BiPAC 6200WZL *R2*/ 6200WZL *R3*

Moblie Broadband Wireless-N Router

User Manual

Version release: v1.04c.dc47

Last revised: October 8, 2012

TABLE OF CONTENTS

Chapter 1: Introduction

Introduction to your Router

Thank you for purchasing the **Mobile Broadband Wireless-N Router**. The router is an economic router ideal for SOHO users, office users and event organizers to have an improved wireless access with a speed of up to 150 Mbps. You can enjoy non-stop wireless access with this economic mobile 3G / 4G embedded router. With Dual-WAN design, you can also have an always-on WAN connection.

Always on connection
The **Mobile Broadband Wireless-N Router** features dual-WAN interface allowing users to connect to the Internet via either wired connectivity of broadband device by pluging into a WAN port, or via 3G / 4G connections via inserting a 3G / 4G SIM card into its built-in SIM slot. The auto fail-over feature ensures maximum connectivity and minimum interruption by quickly and smoothly connecting to a 3G /4G network in the event that your broadband ethernet line fails. The router will then automatically reconnect to the broadband connection when it's restored, minimizing connection costs. These features are perfect for office situations where constant connection is paramount.

Mobility
With the increacing popularity of 3G / 4G standard, communication via **Mobile Broadband Wireless-N Router** is becoming more convenient and wide-available-allowing you to watch movies, download music on the road, run media-intensive application, or access e-mail with your client, team members, friends or family no matter where you are. You can even share your internet with others, whetehr you're in a meeting or speeding across the courtry on a train. The router can even function as a FTP server for network device sharing. The integrated wireless technology allows wireless access up to 150Mbps. The **Mobile Broadband Wireless-N Router** is truely free and mobile.

Upgrated Wireless Access and Security
With an integrated Wireless-N Access Point that supports up to 150Mbps wireless operation rate, yet it can switch compliance with 802.11b/g network devices. Wireless Protected Access (WPA-PSK / WPA2-PSK) and Wired Equivalent Privacy (WEP) features enhance the level of transmission security and access control over your Wireless LAN. If the network requires wider coverage, the built-in Wireless Distribution System (WDS) repeater function allows users to expand the wireless network without the need for any external wires or cables. Built-in with Stateful Packet Inspection (SPI), it enables users to determine whether a data packet is allowed to pass through the firewall to the private LAN. QoS Control prioritizes the traffic and allows users to enjoy smooth traffic flow while running applications such as P2P or multimedia through the Internet.

3G / 4G management Center
With the **Mobile Broadband Wireless-N Router**, monitoring your 3G / 4G connection status is a breeze. unique 3G / 4G Mannagement Center is an utility tool displaying its current 3G / 4G-signal status visually for users to maximize theire connection. You can moitor the bandwidth with the current upload and download speed. This too also calculates the total amount of hours or data traffic used per month, allowing you to manage your 3G / 4G monthly subscripitions.

Features

- 3G / 4G embedded with a built-in SIM card slot
- Dual WAN interfaces for EWAN and 3G / 3.5G / 3.75G / 4G connections
- 150Mbps. Wireless-N AP
- Supports Wi-Fi Protected Setup (WPS) and WPA-PSK / WPA2-PSK
- Supports multiple SSIDs for flexibility of network infrastructure
- High-speed wireless connection up to 150Mbps data rate
- Auto fail-over for always-on connection
- 3G / 4G Management Center for connection monitoring
- SOHO firewall security with DoS prevention and SPI
- Quality of Service control
- Syslog monitoring
- Ideal for SOHO users, Office users, and Event or meeting organizers

Available and Resilience

- Dual-WAN ports (3G / 4G & Ethernet WAN)
- Auto fail-over/fail-back

3G / 4G

- Supports third generation (3G / 3.5G / 3.75G / 4G) digital cellular standards
- Supports multi-band UMTS (HSPA): 800, 850, 900, 1900, 2100 MHz, and AWS(1700/2100 MHz)
- Receive equalizer with antenna diversity on the 800, 850, 900, 1900, 2100 MHz, and AWS(1700/2100 MHz) bands
- Supports quad band EDGE / GPRS / GSM: 850 / 900 / 1800 / 1900MHz
- Web-based GUI for 3G / 4G configuration and 3G / 4G Management Center

Network Protocols and Features

- NAT, static routing and RIP-1 / 2
- NAT supports PAT and multimedia applications
- Transparent bridging
- Virtual server and DMZ
- SNTP, DNS relay and DDNS
- IGMP snooping and IGMP proxy
- File sharing with SMB (Samba) / CIFS

Firewall Management

- Built-in NAT Firewall

- Stateful Packet Inspection (SPI)
- Prevents DoS attacks including Land Attack, Ping of Death, etc.
- Remote access control for web base access
- Packet and URL filtering
- Password protection for system management
- VPN pass-through

Quality of Service Control

- Supports the DiffServ appoarch
- Traffic prorization based-on IP protocol, port number and address

Wireless LAN

- Compliant with IEEE 802.11g and 802.11b standards
- 2.4GHz - 2.484GHz frequency range
- Up to 150Mbps wireless operation rate
- 64 / 128 bits WEP supported for encryption
- WPS (Wi-Fi Protected Setup) for easy setup
- Wireless Security with WPA-PSK / WPA2-PSK support
- WDS repeater function support
- Multiple SSID

Management

- 3G / 4G Management Center
- Quick Installation Wizard
- Web-based for remote and local management
- Firmware upgrades and configuration data upload / download via web-based interface
- SNMP v1 / v2 / v3, MIB-I and MIB-II support
- System Log monitoring
- Supports DHCP server / client / relay
- Mail Alert

Hardware Specifications

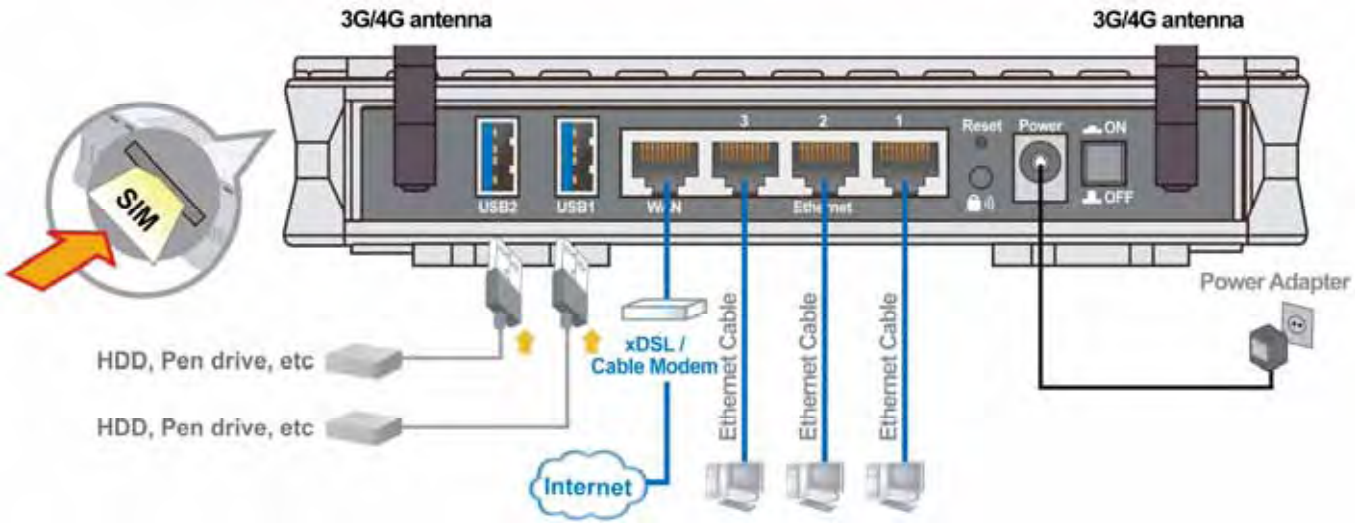
Physical interface

- USB: 2 x USB 2.0 ports
- 3G / 4G: 2 x antennas
- Ethernet: 4 x 10 / 100Mbps Auto-MDI / MDI-X RJ-45 Ethernet ports
- WAN: 1 x 10 / 100Mbps Auto-MDI / MDI-X RJ-45 Ethernet port (port #4 can be configured as WAN port for Broadband connectivity.)
- Reset button
- WPS push button
- Power jack
- Power switch
- SIM slot : (for the SIM card from Telco / ISP)

Physical Specifications

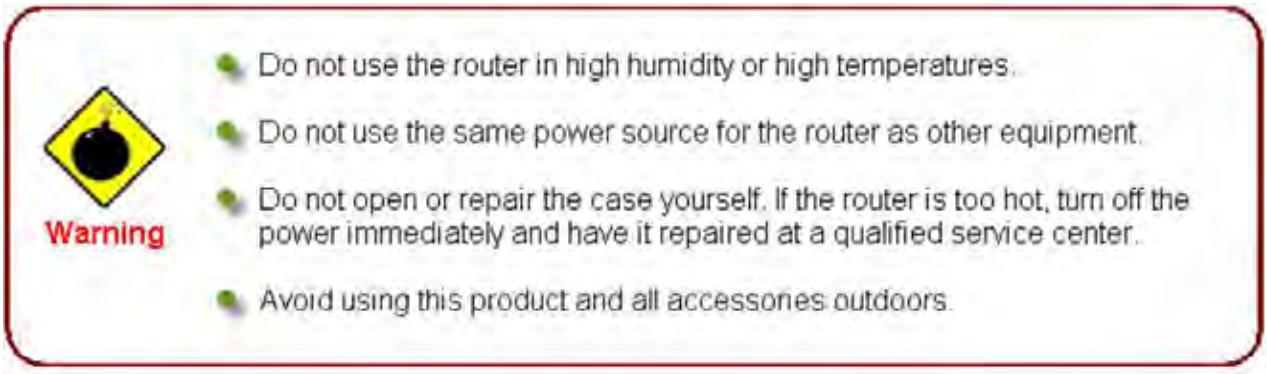
- Dimensions: 7.28" x 4.86" x 1.38"(185mm x 123.5mm x 35mm

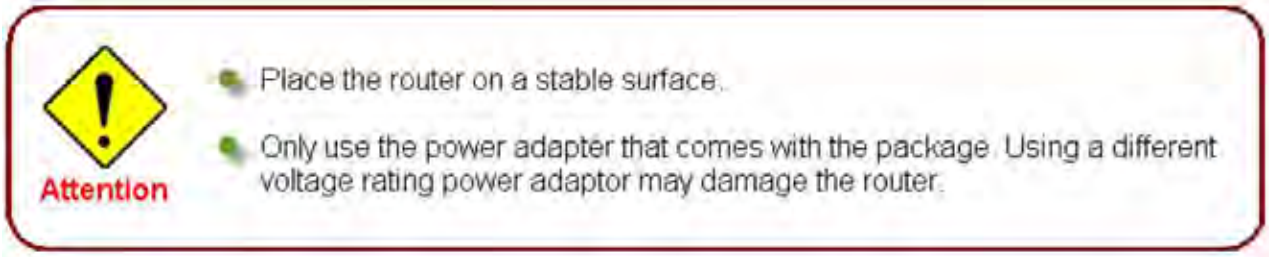
Applications Diagram



Chapter 2: Product Overview

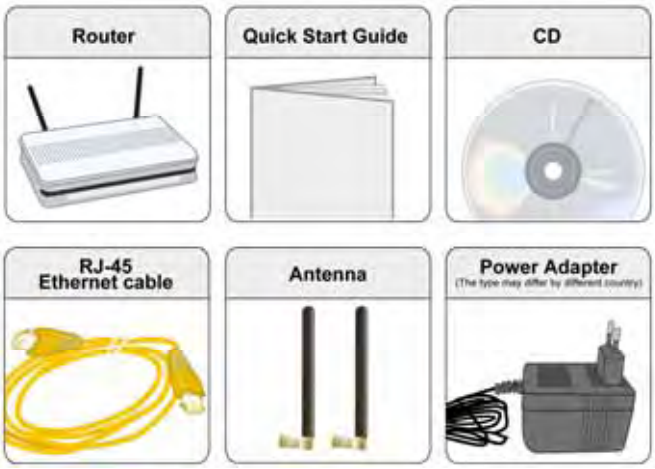
Important note for using this router





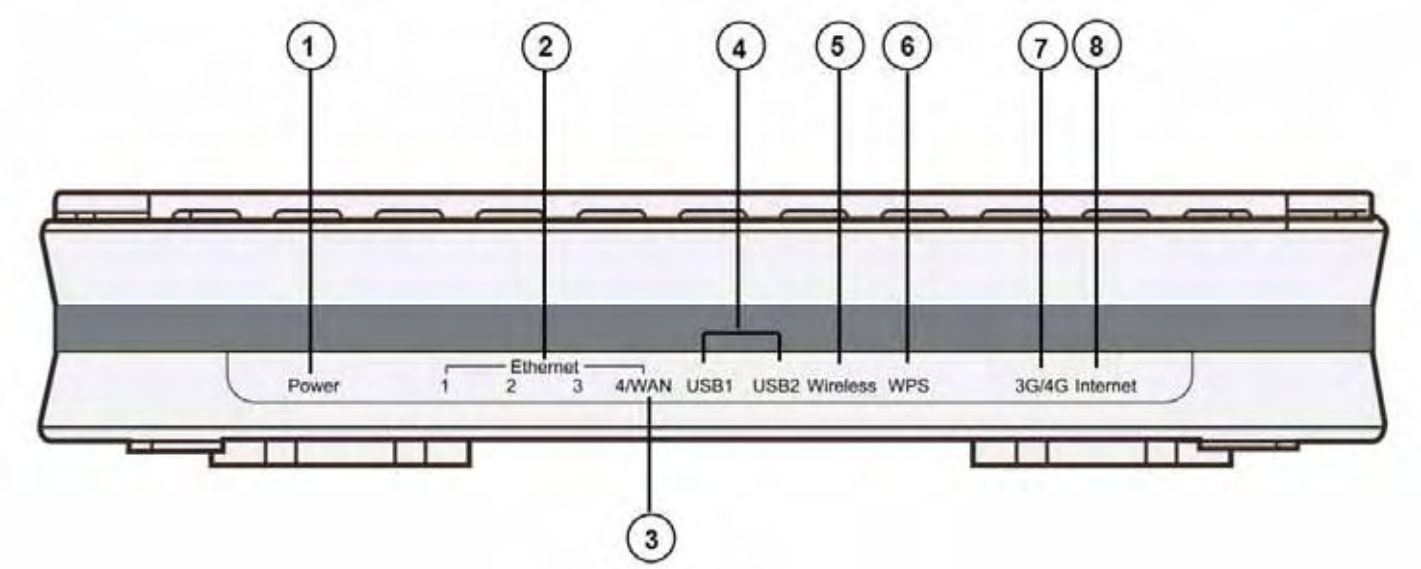
Package Contents

- ✓ **Mobile Broadband Wireless-N Router**
- ✓ **This Quick Installation Guide**
- ✓ **CD containing the user manual**
- ✓ **RJ-45 Ethernet Cable**
- ✓ **Two 3G/4G detachable antenna**
- ✓ **Power adaptor**



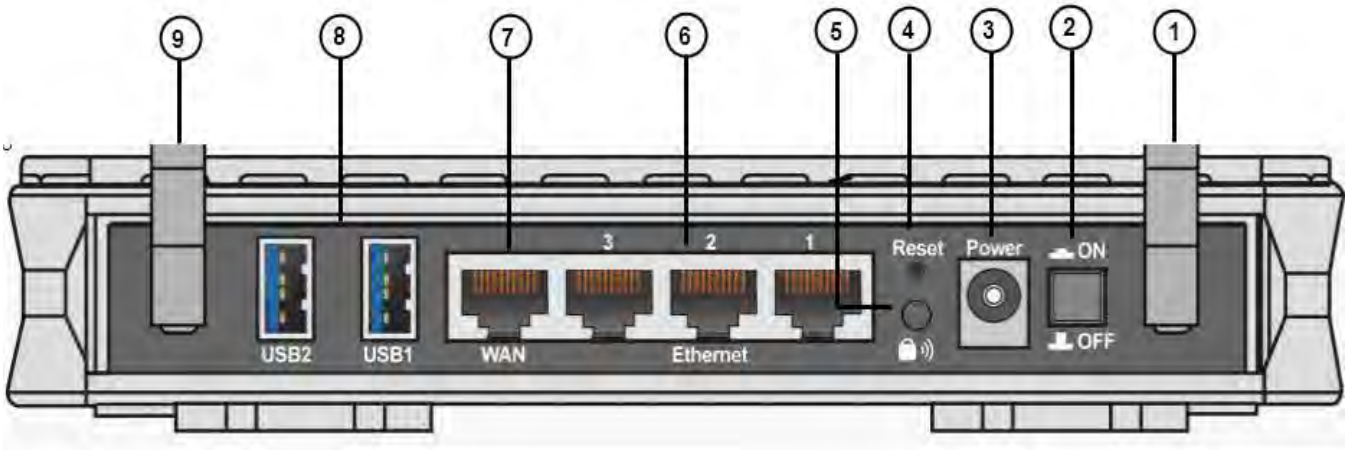
Device Description

The Front LEDs



LED		Meaning
1	**Power**	Lit orange when the device is booting or the device fails to boot. Lit green when the device is ready.
2	**Ethernet (1 - 4)**	Lit green when one of LAN ports is connected to an Ethernet device. Blink when data is being Transmitted / Received.
3	**WAN**	Lit green when connected to a Cable modem, xDSL modem, Fiber (PON) modem's Ethernet port well. **Note:** port #4 can be configured as WAN port for broadband connectivity,
4	**USB***future release	Lit green when the router is connected to a USB device.
5	**Wireless**	Lit green when the wireless connection is enabled. Flashes when the device is sending/receiving data.
6	**WPS**	Flashes green when WPS is enabled and waiting for wireless devices to connect in. Lit green when wireless devices have been successfully connected in.
7	**3G / 4G**	Lit orange when 3G / 4G service is not ready to dial up. Lit green when 3G / 4G service is ready to proceed 3G / 4G dial-up.
8	**Internet**	Lit green when IP connected. Lit orange when device attempted to become IP connected but failed.

The Rear Ports



1	**3G / 4G detachable antenna**	Connect the 3G / 4G detachable antenna to this port.
2	**Power Switch**	Power ON/OFF switch
3	**Power Jack**	Connect the supplied power adapter to this jack.
4	**Reset Button**	Press it to reset the device or restore to factory default settings.
5	**WPS**	Push WPS button to trigger Wi-Fi Protected Setup function.
6	**Ethernet**	Connect your computer to a LAN port, using the included Ethernet cable.
7	**WAN**	Connect to a Cable modem, xDSL modem, Fiber (PON) modem.
8	**USB***future release	Both USB1 and USB2 can be connected to a USB device, such as, HDD. *future release
9	**3G / 4G detachable antenna**	Connect the 3G / 4G detachable antenna to this port.

Cabling

The most common problem associated with Ethernet is bad cabling. Make sure that all connected devices are turned on. In the front of the product is a bank of LEDs. Verify that the LAN Link and WAN Link LEDS are lit. If they are not, verify that you are using the proper cables.

Chapter 3: Basic Installation

You can configure the **Mobile Broadband Wireless-N Router** through the convenient and user-friendly interface of a web browser. Most popular operating systems such as Linux and Windows 98 / NT /2000 / XP / ME / 7 / Vista include a web browser as a standard application.
PCs must have a properly installed Ethernet interface which connects to the router directly or through an external repeater hub. In addition, PCs must have TCP/IP installed and configured to obtain an IP address through a DHCP server or a fixed IP address that must be in the same subnet as the router. The default IP address of the router is **192.168.1.254** and the subnet mask is **255.255.255.0** (i.e. any attached PC must be in the same subnet, and have an IP address in the range between 192.168.1.1 and 192.168.1.253). The easiest way is to configure the PC is to obtain an IP address automatically from the router using DHCP. If you encounter any problems accessing the router's web interface you are advised to **uninstall** any kind of software firewall on your PCs, as they can cause problems when trying to access the 192.168.1.254 IP address of the router.

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

Any TCP/IP capable workstation can be used to communicate with or through the **Mobile Broadband Wireless-N Router**. To configure other types of workstations, please consult the manufacturer's documentation.

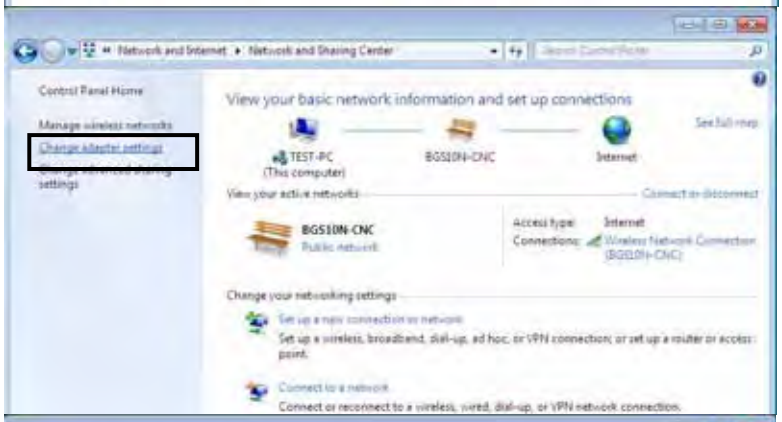
Network Configuration

Configuring a PC in Windows 7

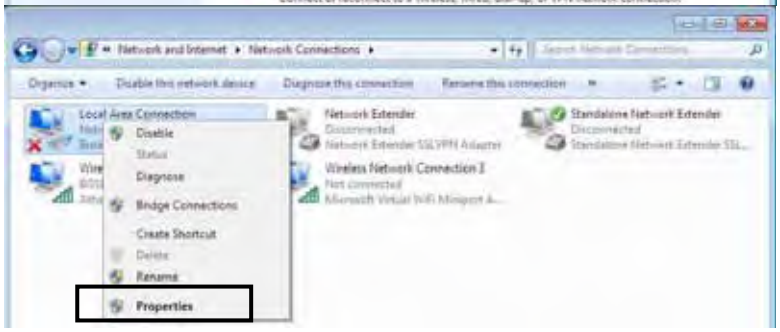
1. Go to **Start**. Click on **Control Panel**.

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

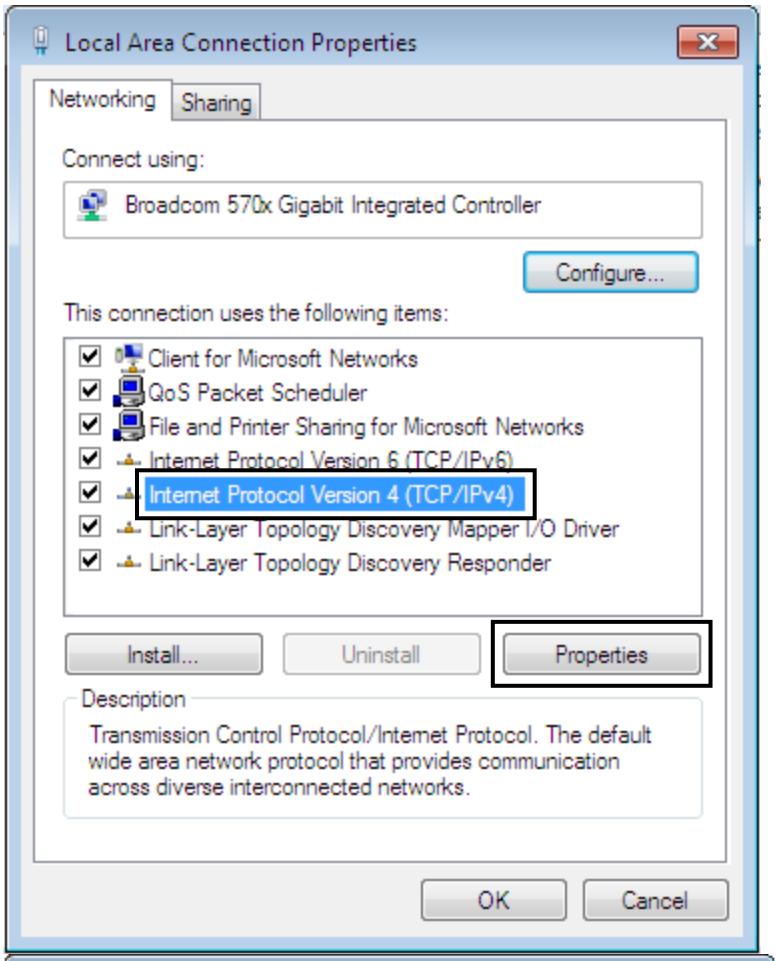
3. When the **Network and Sharing Center** window pops up, select and click on **Change adapter settings** on the left window panel.



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

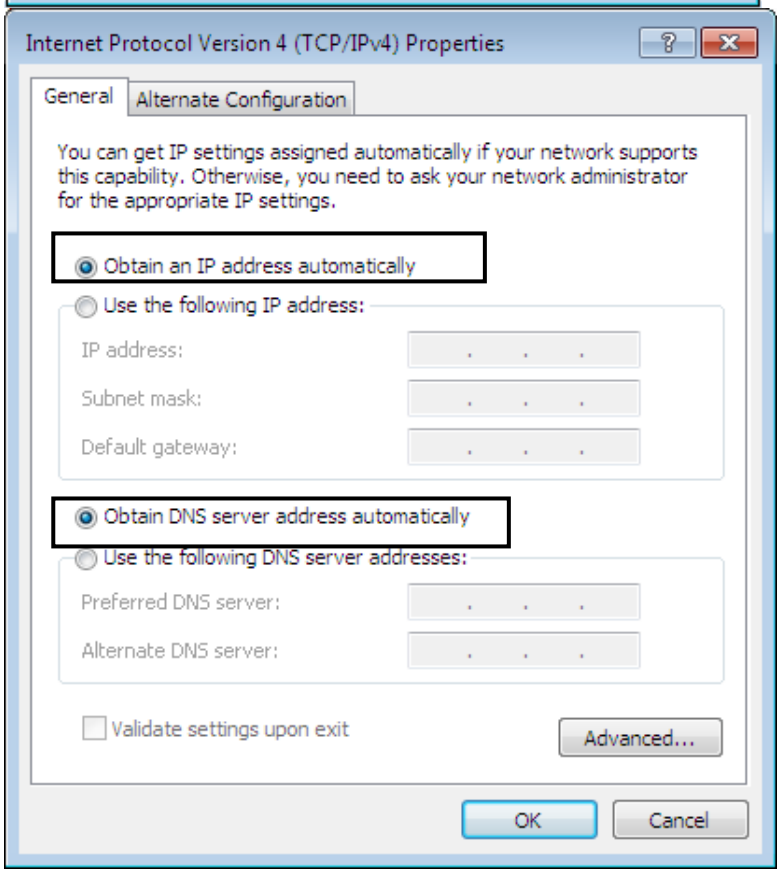


5. Select **Internet Protocol Version 4 (TCP/IPv4)** then click **Properties**.



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.

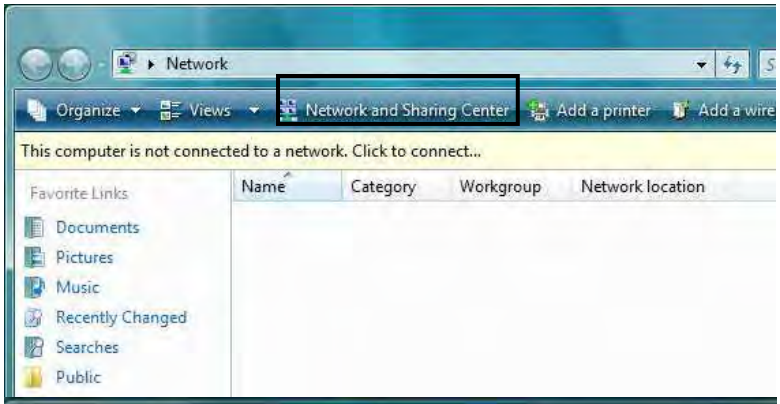
7. Click **OK** again in the **Local Area Connection Properties** window to apply the new configuration.



Configuring a PC in Windows Vista

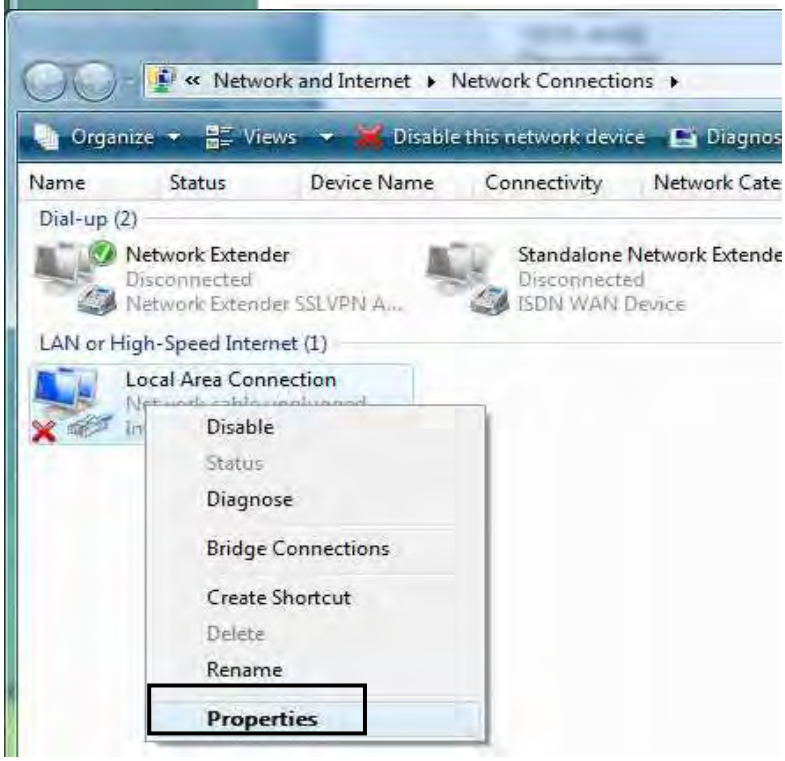
1. Go to **Start**. Click on **Network**.

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

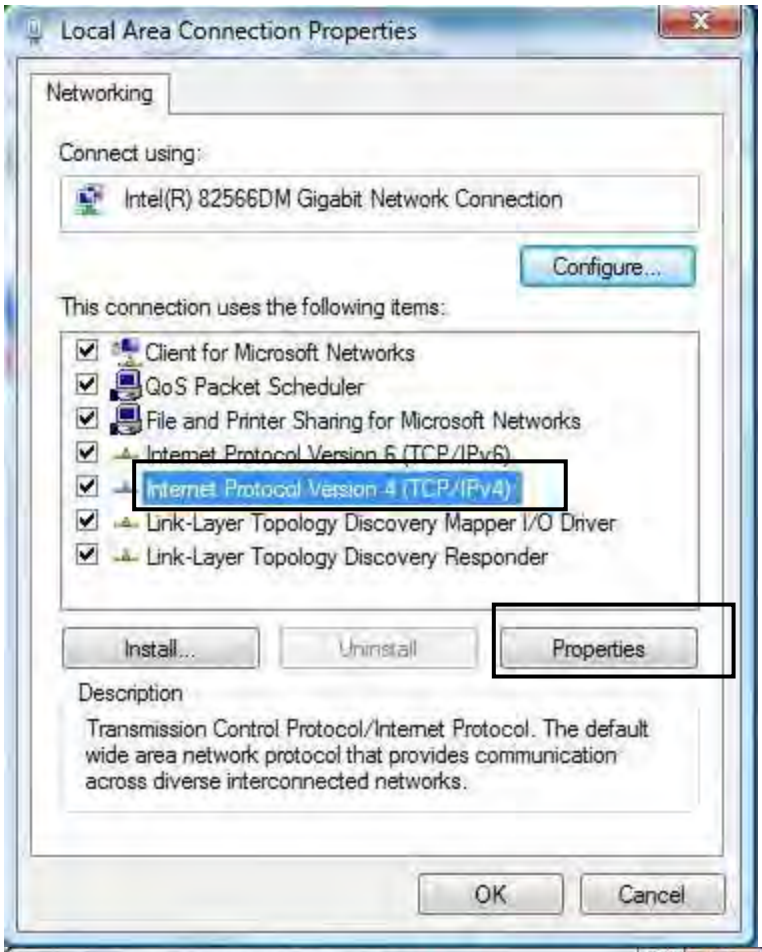


3. When the **Network and Sharing Center** window pops up, select and click on **Manage network connections** on the left window pane.

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

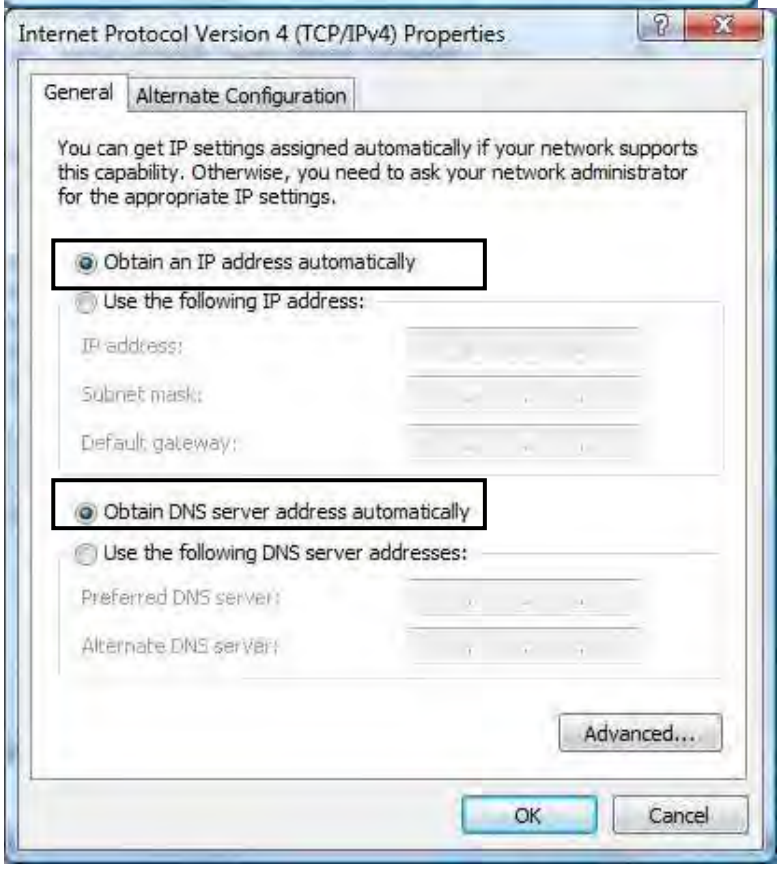


5. Select **Internet Protocol Version 4 (TCP/IPv4)** then click **Properties**.



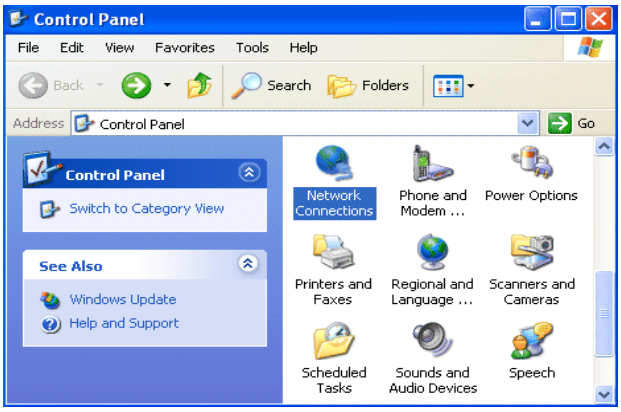
6. In the **TCP/IPv4 properties** window, select the Obtain an **IP address automatically** and **Obtain DNS Server address automatically** radio buttons. Then click **OK** to exit the setting.

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

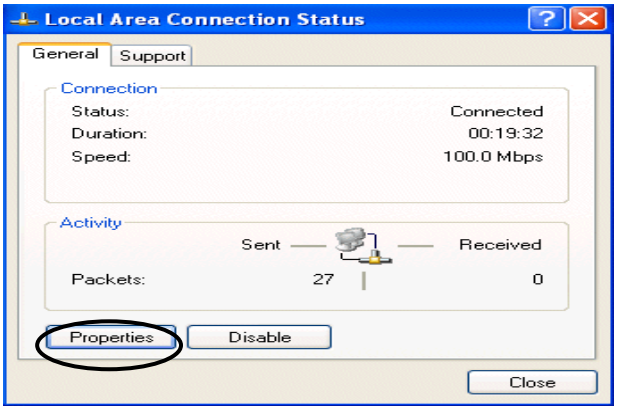


Configuring a PC in Windows XP

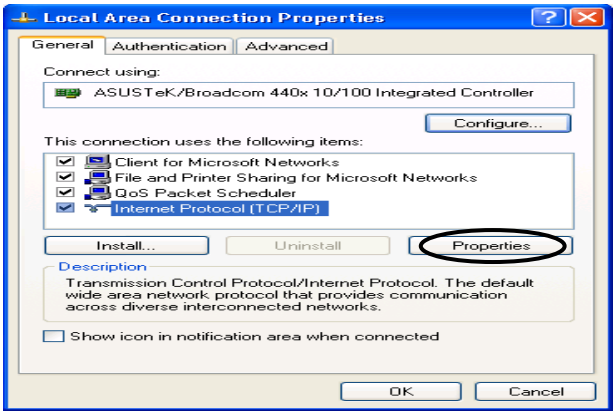
1. Go to **Start**. Click on **Control Panel.**
2. Then click on **Network and Internet**.



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

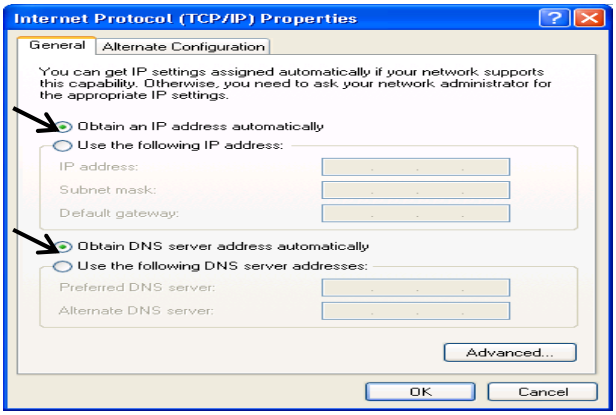


4. Select **Internet Protocol (TCP/IP)** and click **Properties**.



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

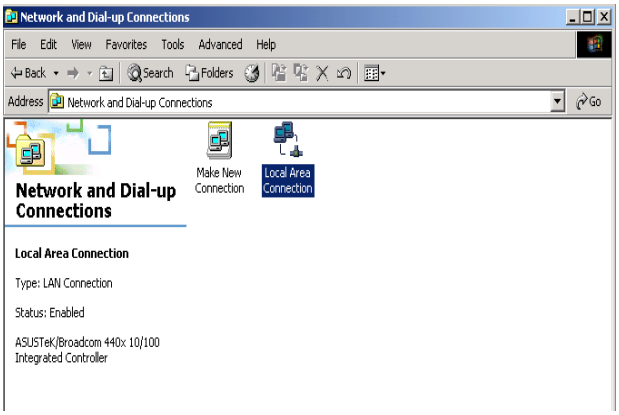
6. Click **OK** to finish the configuration.



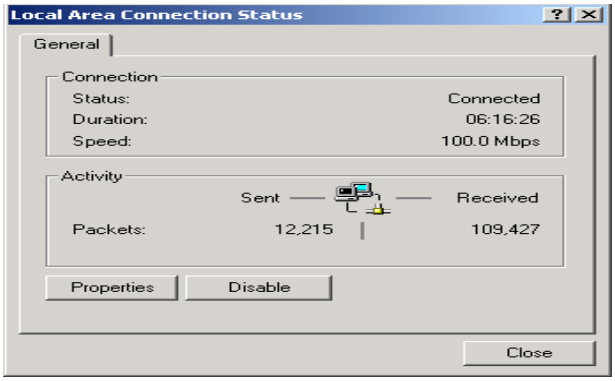
Configuring a PC in Windows 2000

1. Go to **Start / Settings / Control Panel**. In the Control Panel, double-click on **Network and Dial-up Connections**.

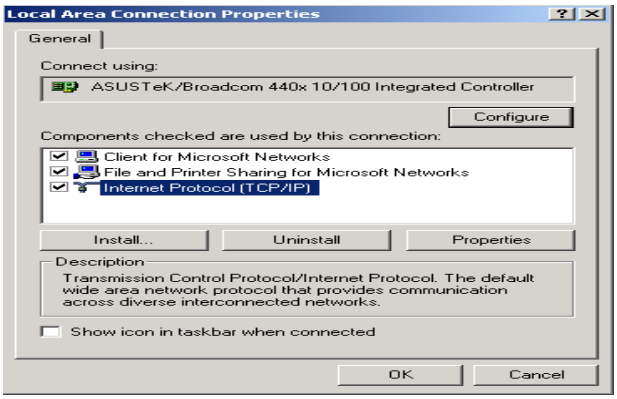
2. Double-click **Local Area Connection**.



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

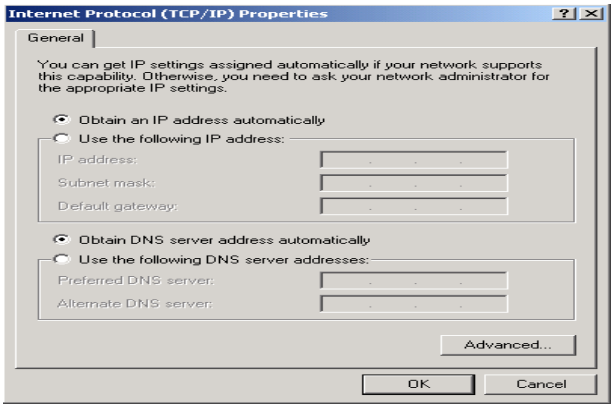


4. Select **Internet Protocol (TCP/IP)** and click **Properties**.



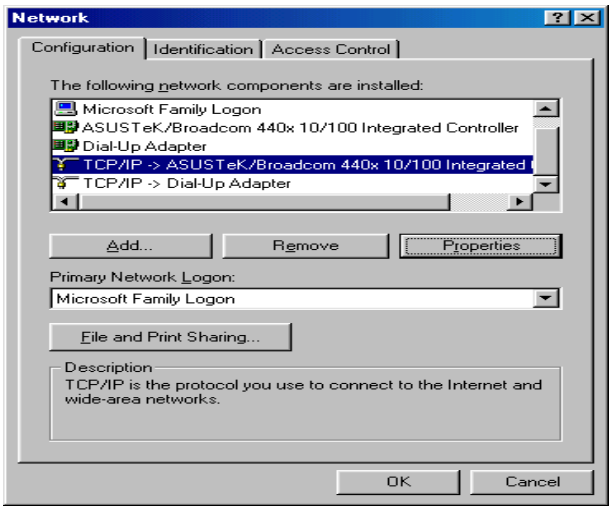
5. Select the **Obtain an IP address automatically** and the **Obtain DNS server address automatically** radio buttons.

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



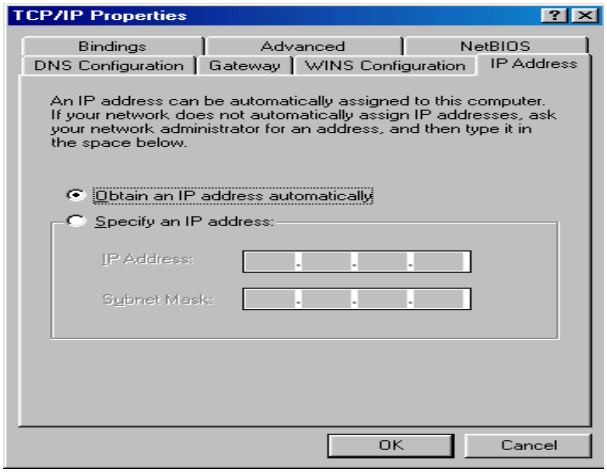
Configuring PC in Windows 98/Me

1. Go to **Start / Settings / Control Panel**. In the Control Panel, double-click on **Network** and choose the **Configuration** tab.



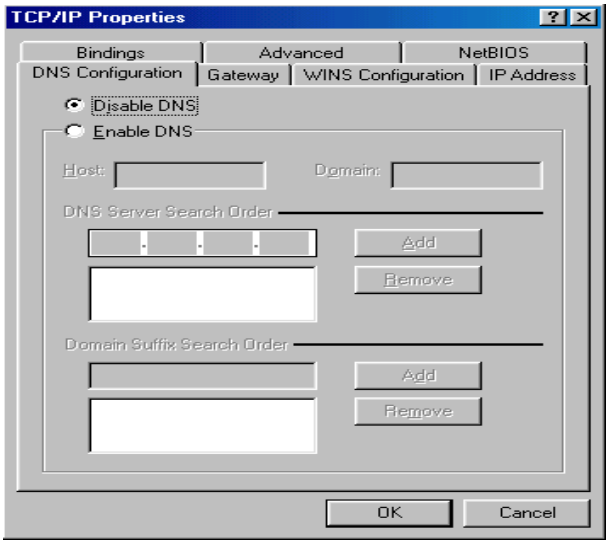
2. Select **TCP/IP ->NE2000 Compatible**, or the name of your Network Interface Card (NIC) in your PC.

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



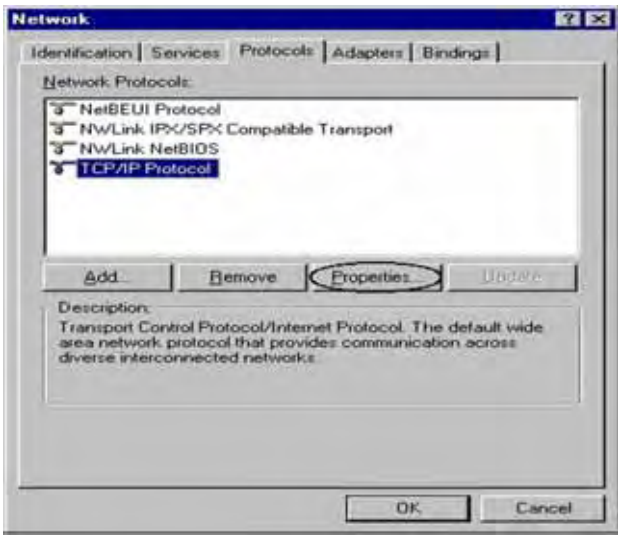
4. Then select the **DNS Configuration** tab.

5. Select the **Disable DNS** radio button and click **OK** to finish the configuration.



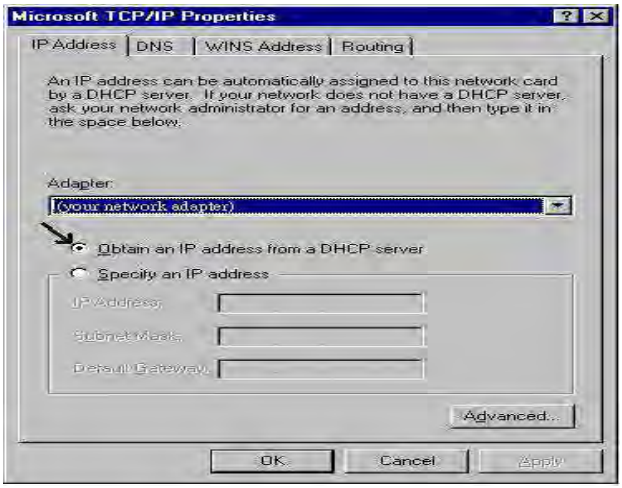
Configuring PC in Windows NT4.0

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

Web Interface: (Username and Password)

- Username: admin
- Password: admin

The default username and password are “**admin**” and “**admin**” respectively.

If you ever forget the username/password to login to the router, you may press the RESET button up to 6 seconds then release it to restore the factory default settings.
Caution: After pressing the RESET button for more than 6 seconds then release it, to be sure you power cycle the device again.

Device LAN IP settings

- IP Address: 192.168.1.254
- Subnet Mask: 255.255.255.0

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 preset at the factory. The default values are shown below.

LAN Port	
IP address	192.168.1.254
Subnet Mask	255.255.255.0
DHCP server function	Enabled in ports 1, 2 and 3
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) what kind of services are provided, such as PPPoE, Obtain an IP Address Automatically, Fixed IP address.

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

PPPoE	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).
Obtain an IP Address Automatically	DHCP Client (it can be automatically assigned by your ISP when you connect or be set manually).
Fixed IP Address	IP address, Subnet mask, Gateway address, and Domain Name System (DNS) IP address (it is fixed IP address).

Configuring with your Web Browser

Open your web browser, enter the IP address of your router, which by default is **192.168.1.254**, and click “**Go**”, a user name and password window prompt appears. Enter the user name and password that your administrator has set for you and select the **Account Type**, then click **Login**. When you are authorised, you will access to the router.The default username and password are **“admin”** and **“admin”** respectively for the Administrator account type.

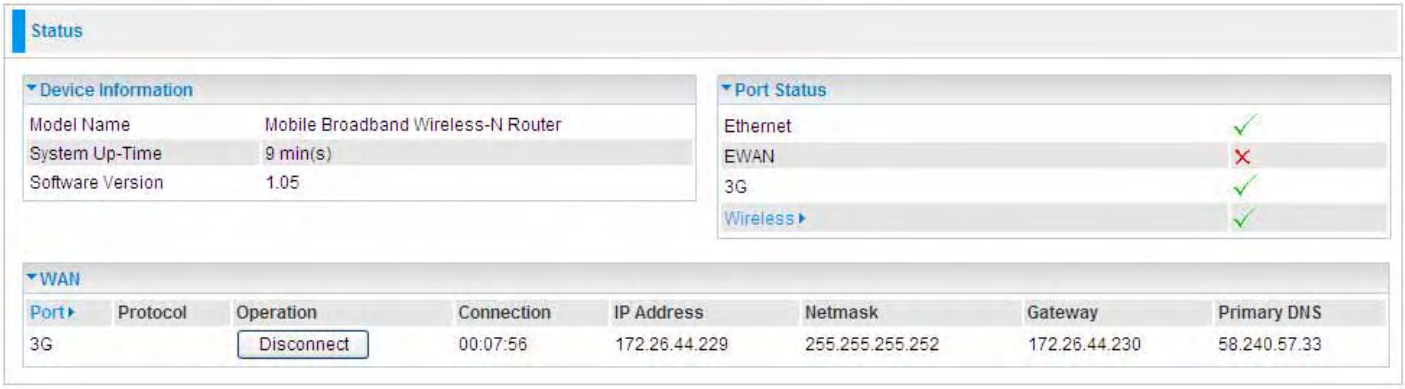
Congratulations! You have successfully logged on to your **Mobile Broadband Wireless-N Router**!

Chapter 4: Basic Configuration

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

- **Advanced** (Switch to Advanced Configuration mode)
- **Status**
- **Quick Start**
- **WAN**
- **WLAN**
- **Language**

Status



Device Information

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

System Up-Time: Record system up-time.

Software Version: Firmware version.

Port Status

Port Status：User can look up to see if they are connected to Ethernet, EWAN, 3G / 4G and Wireless.

WAN

Port: Name of the WAN connection.

Protocol: PPPoE, Dynamic or Fixed.

Operation: Current available operation.

Connection: The current connection status.

Netmask: WAN port IP subnet mask.

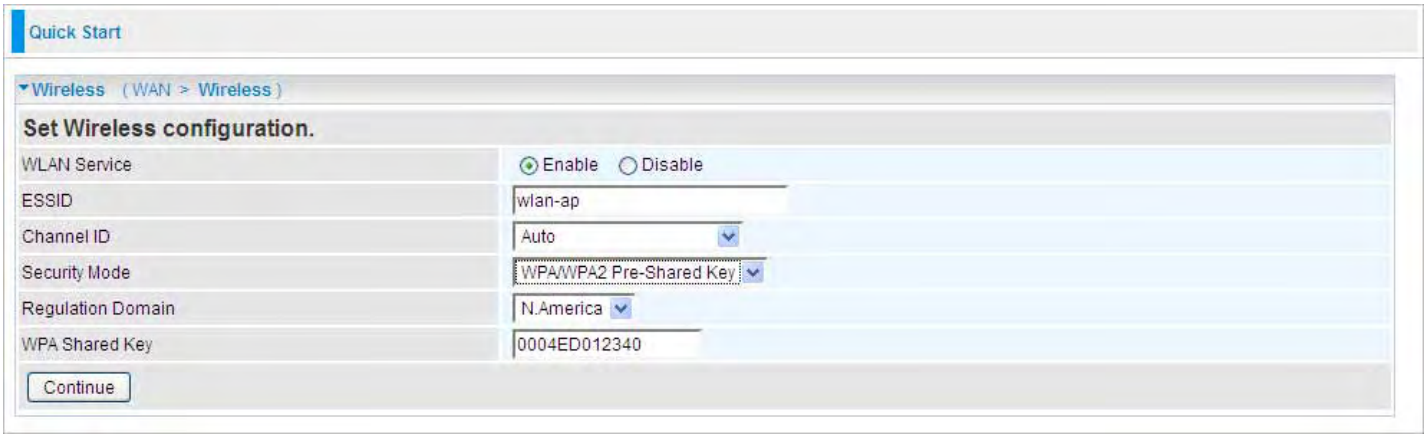
Gateway: The IP address of the default gateway.

IP Address: WAN port IP address.

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

Quick Start

Set Wireless configuration



WLAN Service: Default setting is set to **Enable**.

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

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

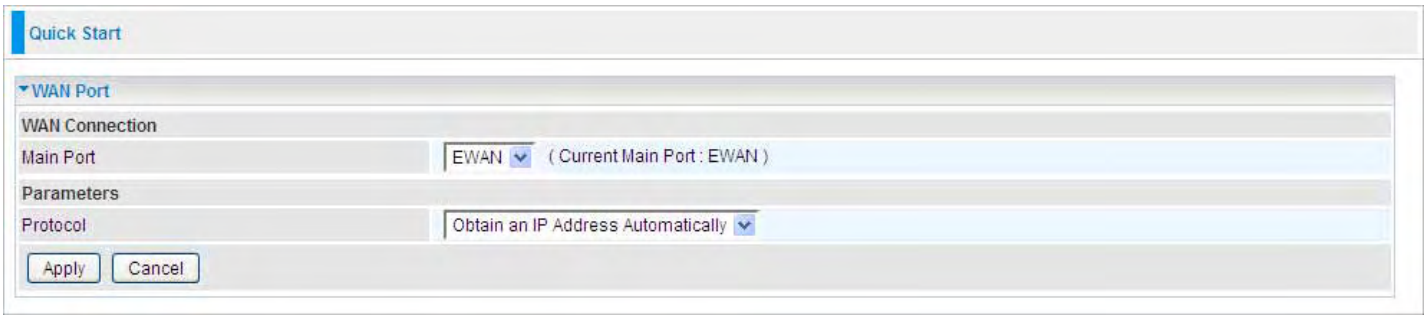
Security Mode: You can disable or enable with WPA or WEP for protecting wireless network. The default mode of wireless security is **Disable**.

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.

For detailed Quick Start configration, turn to **Quick Start** for help.

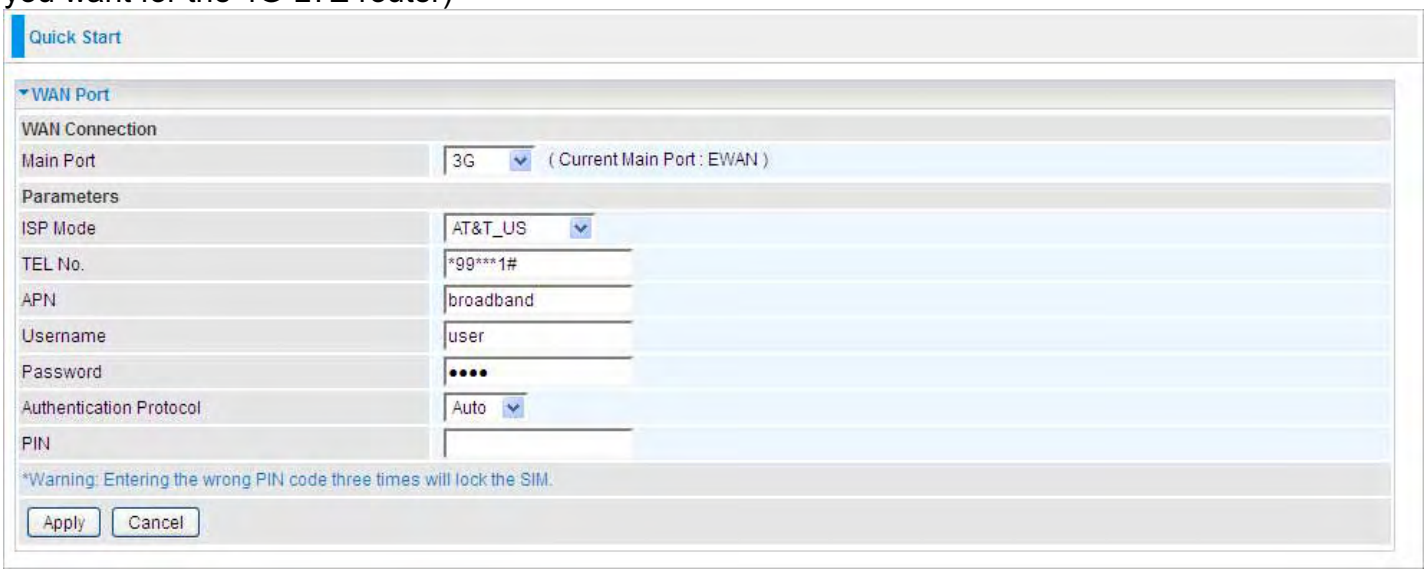
WAN

EWAN



3G / 4G-LTE

(The router also support 4G-LTE network, and user must tell the provider the exact 4G-LTE service you want for the 4G-LTE router)



APN: An APN is similar to a URL on the WWW, it is what the unit makes a GPRS / UMTS / LTE call. The service provider is able to attach anything to an APN to create a data connection. Requirements for APN assignment varies between different service providers. Most service providers have an internet portal which they connect a DHCP Server to, giving you access to the internet i.e. Some 3G / 4G operators use the APN 'internet' for their portal. The default value of APN is "broadband".

Username: Enter the username provided by your service provider.

Password: Enter the password provided by your service provider.

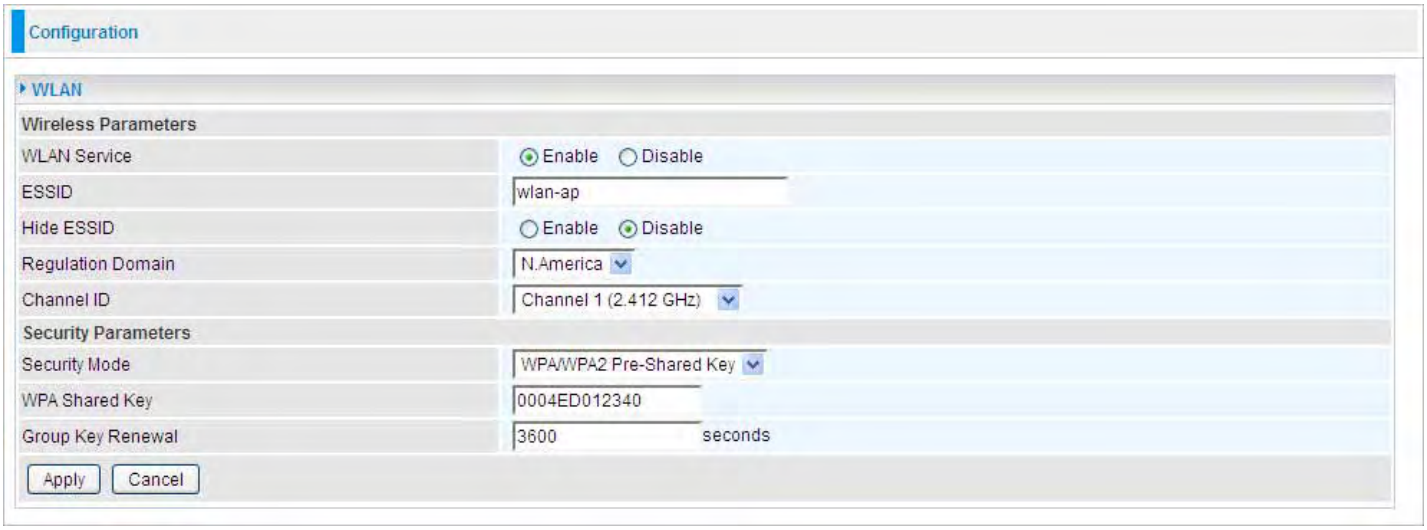
Authentication Protocol: Manually specify CHAP (Challenge Handshake Authentication Protocol) or PAP (Password Authentication Protocol) if you know which authentication type the server is using (when acting as a client), or the authentication type you want the clients to use when tehy are connecting to you (when acting as a server). When using PAP, the password is sent unencrypted, while CHAP encrypts the password before sending, and also allows for challenges at different periods to ensure that an intruder has not replaced the client.

PIN: PIN stands for Personal Identification Number. A PIN code is a numeric value used in certain

systems as a password to gain access, and authentication. In mobile phones a PIN code locks the SIM card until you enter the correct code. If you enter the PIN code incorrectly into the phone 3 times in a row, then the SIM card will be blocked and a PUK code will be required from your network / service provider to unlock it.

Note: when the 3G / 4G-LTE SIM card is pulled out and then insert into again, you should again press **Apply** button to make 3G / 4G-LTE connection take effort, or you can **Save config** and **Restart** the route to reach the same effort.

WLAN



WLAN Service: Default setting is set to **Enable**.

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

Note: ESSID is case sensitive and must not excess 32 characters.

Hide ESSID: It is function in which transmits its ESSID to the air so that when wireless client searches for a network, router can then be discovered and recognized. Default setting is **Disable.**

⊙ **Enable:** Select Enable if you do not want broadcast your ESSID. When select Enable, the ESSID will be hided in stead of broadcasting, thus when wireless client searches for this AP, failure occurs. This ESSID(AP) will be invisible to you. In this case, if you want to join this wireless network, enter the exactly ESSID manually and some security settings.

⊙ **Disable:** When Disable is selected, the router will broadcast the ESSID to allow anybody with a wireless client to be able to identify the Access Point (AP) of your router. Select the specific ESSID scanned, with some security settings, you will join this wireless network.

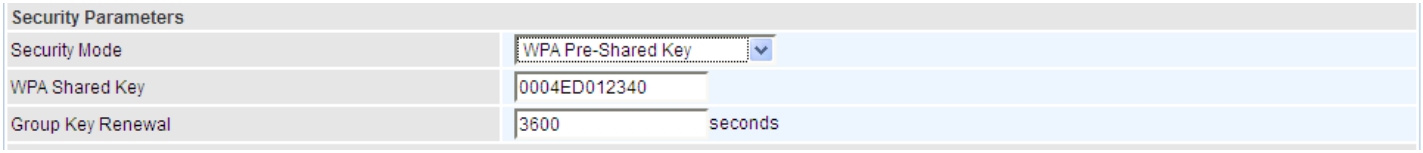
Regulation Domain: There are seven Regulation Domains for you to choose from, including **North America (N.America)**, **Europe**, **France**, etc. The Channel ID will be different based on this setting.

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

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

Security Parameters

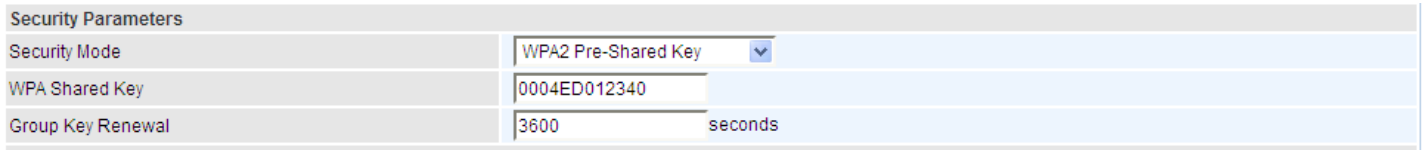
WPA Pre-Shared Key



WPA Shared Key: The key for network authentication. The input format is in character style and the key size should be in the range between 8 and 63 characters (here the default is the router or CPE's MAC address in uppercase).

Group Key Renewal: The period of renewal time for changing the security key between wireless client and Access Point (AP). This process is done automatically.

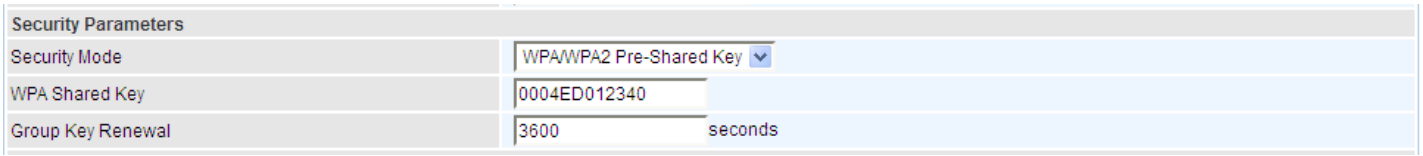
WPA2 Pre-Shared Key



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 (here the default is the router or CPE's MAC address in uppercase).

Group Key Renewal: The period of renewal time for changing the security key between wireless client and Access Point (AP). This process is done automatically.

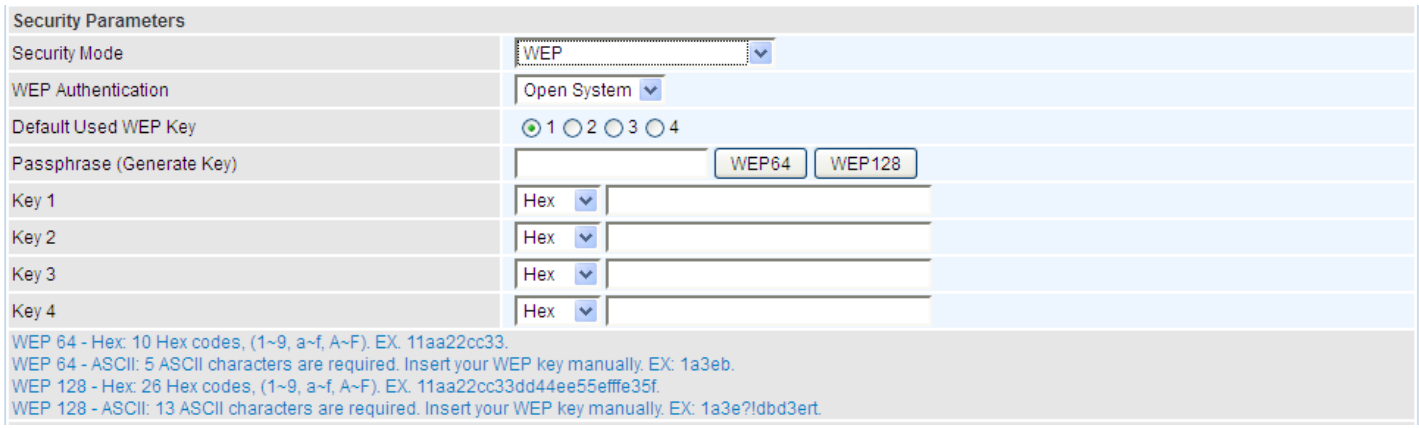
WPA/WPA2 Pre-Shared Key



WAP 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 (here the default is the router or CPE's MAC address in uppercase).

Group Key Renewal: The period of renewal time for changing the security key between wireless client and Access Point (AP). This process is done automatically.

WEP



WEP Authentication: To prevent unauthorized wireless stations from accessing data transmitted over the network, the router offers secure data encryption, known as WEP. If you require high security for transmissions, there are three options to select from: **Open System, Share 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. You can input the same string in both the AP and Client card settings to generate the same WEP keys. Please note that you do not have to enter **Key (1-4)** as below when the **Passphrase** is enabled.

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 is in HEX, 10 or 26 codes or ASCII style, 5 and 13 codes are required for WEP64 and WEP128 respectively-no any separator is included.

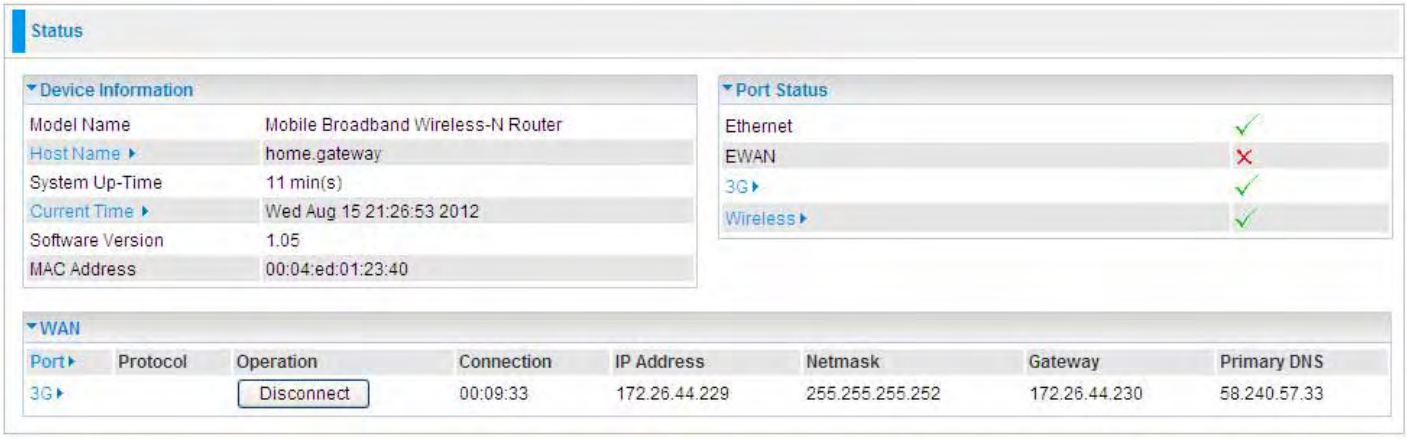
Chapter 5: Advanced Configuration

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

- **Basic** (Switch to Basic Configuration Mode)
- **Status** (3G Status, ARP Table, DHCP Table, System Log, Firewall Log, UPnP Portmap)
- **Quick Start**
- **Configuration** (LAN, WAN, System, USB, Firewall, Download Tool, QoS, Virtual Server, Wake on LAN, Time Schedule and Advanced)
- **Language**

The following sections provide an overview of the settings available for configuring your router.

Status



Device Information

Model Name: Display the model name.

Host Name: Provide a name for the router for identification purposes. Host Name lets you change the router name. Click this link to turn to **Device Management** configuration.

System Up-Time: Record system up-time.

Current time: Set the current time. See the Time Zone section for more information. Click this link to turn to **Time Zone** configuration.

Software Version: Firmware version. **MAC Address:** The LAN MAC address.

Port Status

Port Status：User can look up to see if they are connected to Ethernet, EWAN, 3G (4G-LTE) or Wireless.

WAN

Port: Name of the WAN connection. Click Port to enter **WAN Interface** configuration page. Click EWAN (for example) to enter **WAN Profile** configuration page.

Operation: Current available operation.

Connection: The current connection status.

IP Address: WAN port IP address.

Net mask: WAN port IP subnet mask.

Gateway: The IP address of the default gateway.

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

3G Status

This section displays the 3G / 4G-LTE Card overall status with information such as the current signal strength, statistics of current data transmission and total data transmission.

Status: The current status of the 3G /4G-LTE SIM card. Click this link to configure 3G (4G-LTE). For detail, turn to **3G configuration page** for help.

Signal Strength: The signal strength bar indicates the current 3G(4G-LTE) signal strength.

Network Name: The network name that the device is connected to.

Card Name: The name of the 3G /4G-LTE SIM card.

Card Firmware: The current firmware of the 3G / 4G-LTE card.

Card IMEI: The unique identification number that is used to identify the 3G / 4G-LTE card.

Current TX Bytes / Packets: The statistics of data transmission in bytes / packets during a call.

Current RX Bytes / Packets: The statistics of data received in bytes / packets during a call.

Total TX Bytes / Packets: The statistics of total data transmission in bytes / packets since system ready.

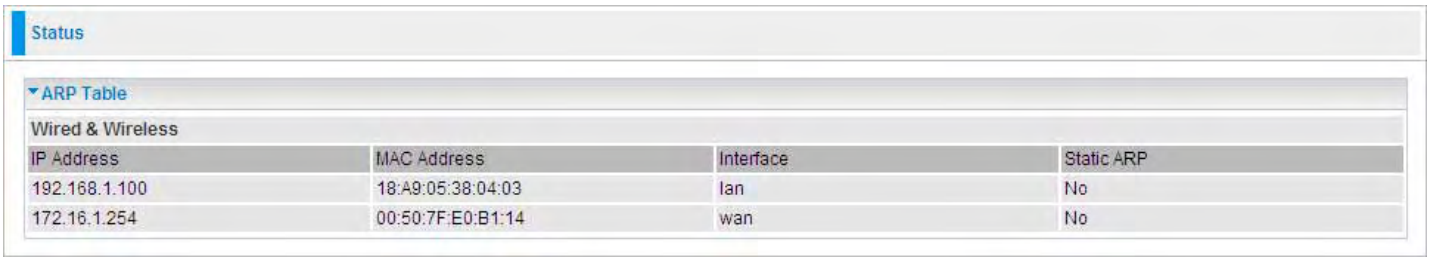
Total RX Bytes / Packets: The statistics of total data received in bytes / packets since system ready.

Amount used: Show the traffic or hours has been used.

Billing preiod: The day from which the fee is charged.

ARP Table

This section displays the router's ARP (Address Resolution Protocol) Table, which shows the mapping of Internet (IP) addresses to Ethernet (MAC) addresses. This is useful as a quick way of determining the MAC address of the network interface of your PCs to use with the router's **Firewall - MAC Address Filter** function. See the Firewall section of this manual for more information on this feature.



IP Address: It is IP Address of internal host that join this network.

MAC Address: The MAC address of internal host.

Interface: indicates which side the IP addresses locate on. WAN means the corresponding IP locates on WAN side.

Static ARP: The state for ARP.

- **"No"** for dynamically-generated ARP table entries.
- **"Yes"** for static ARP table entries added by the user.

DHCP Table

IP Address: The current corresponding DHCP-assigned dynamic IP address of the device. Click this link to configure DHCP Server, for more information, turn to Page 63-64.

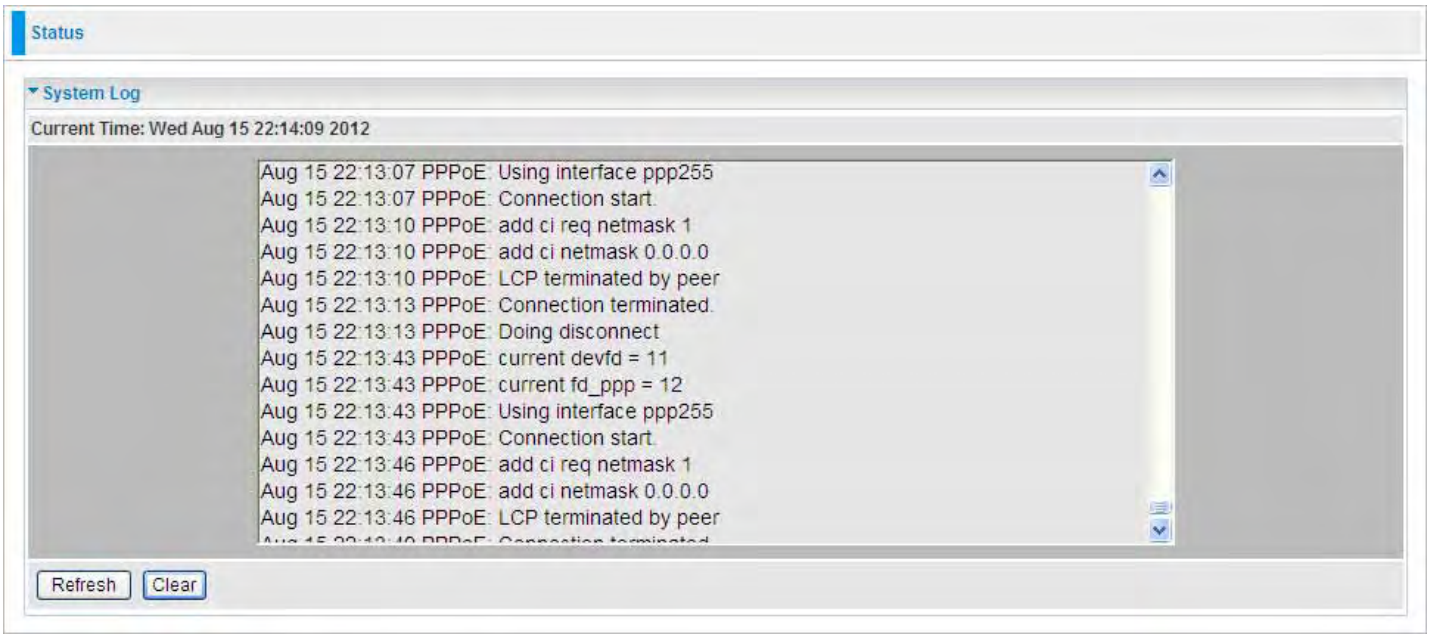
MAC Address: The MAC Address of internal DHCP client host.

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

Register Information: Register time information.

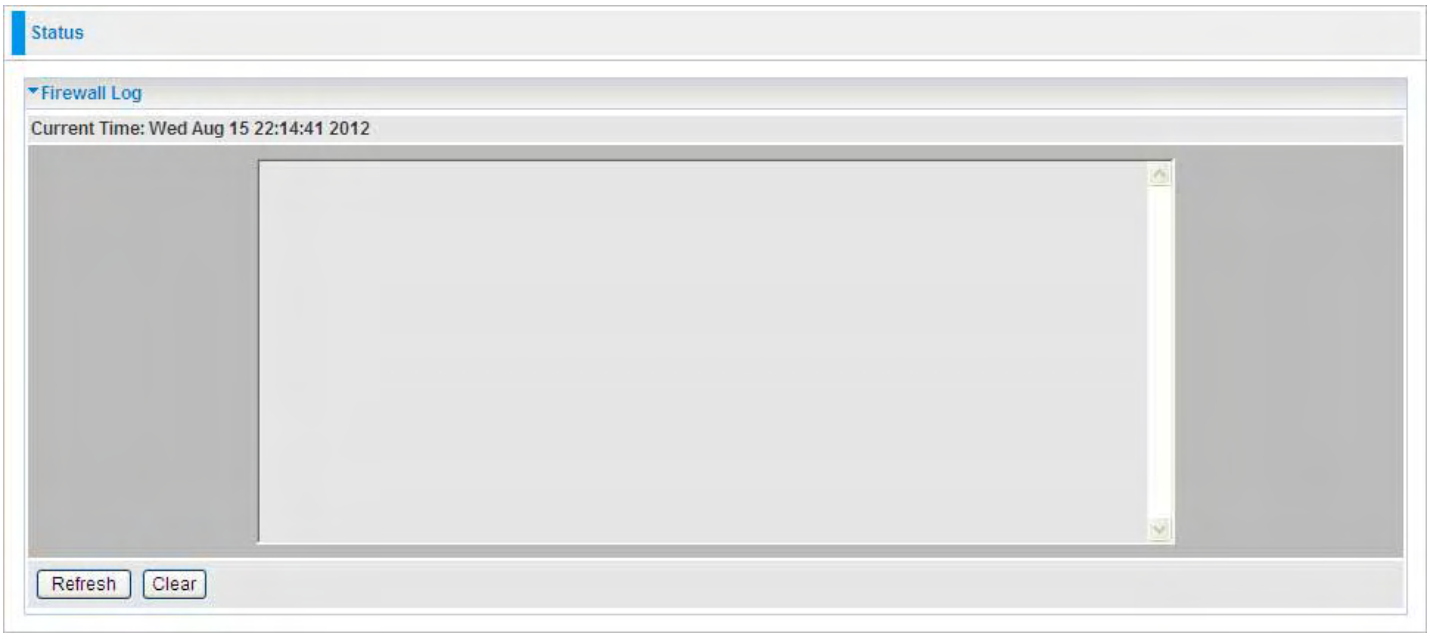
System Log

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



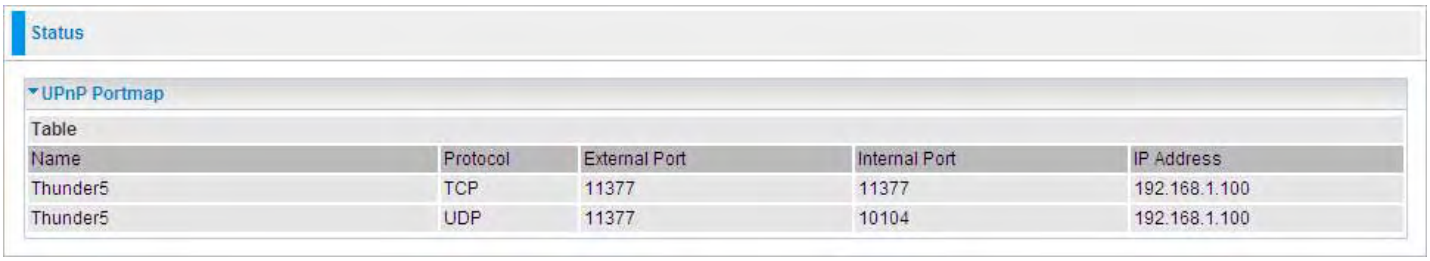
Firewall Log

Firewall Log displays log information of any unexpected action with your firewall settings. This page displays the router's Firewall Log entries. The log shows log entries when you have enabled Intrusion Detection or Block WAN PING in the **Configuration - Firewall** section of the interface. Please see the **Firewall** section of this manual for more details on how to enable Firewall logging.



UPnP Portmap

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



Name: the name of this UPnP mapping.

Protocol: the protocol used by this mapping.

External Port: the external service port the internal port mapped to.

Internal Port: the internal service port.

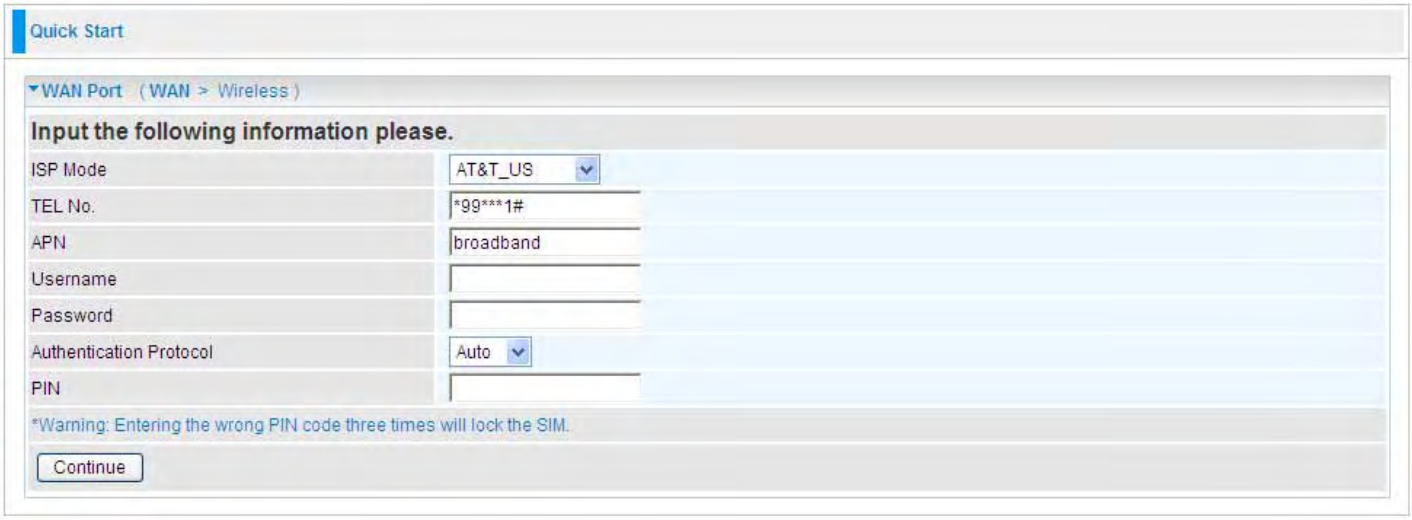
IP Address: the IP Address of the host in LAN.

Quick Start

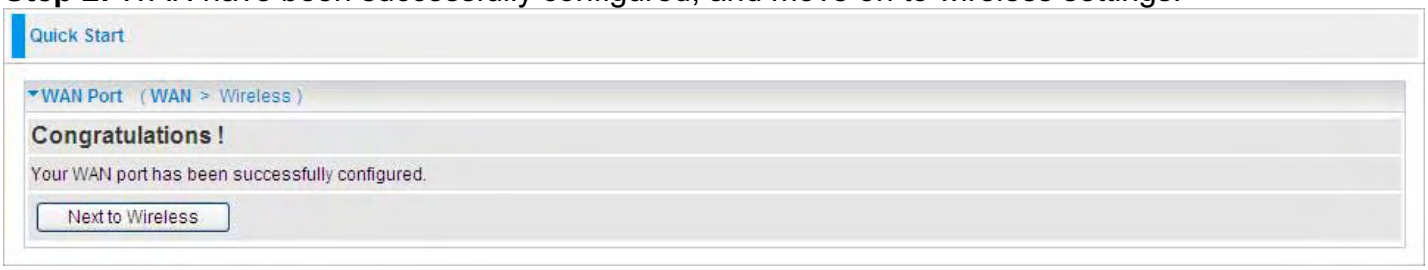
Step 1: Enable and Select the appropriate Time Zone, then click **Continue** to go on to next step. You can turn **Time Zone** to understand more.

3G

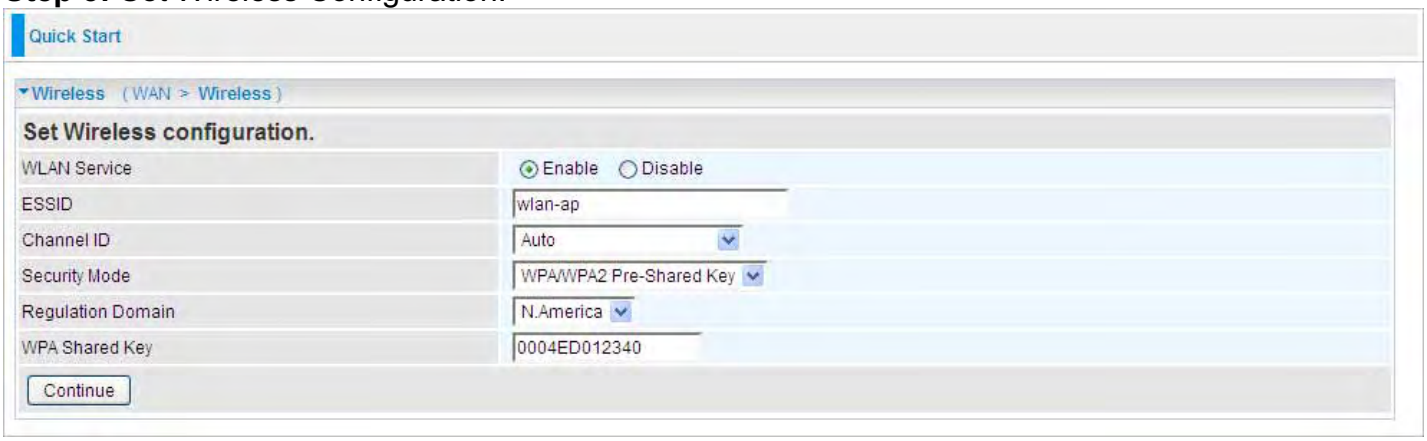
Step 1: Select the connection mode: 3G. Then click **Continue**. If you want directly go to wireless setting, please click **Jump to Wireless setting** and go to step 3.



Step 2: WAN have been successfully configured, and move on to wireless settings.



Step 3: Set Wireless Configuration.



WLAN Service: Default setting is set to **Enable**.

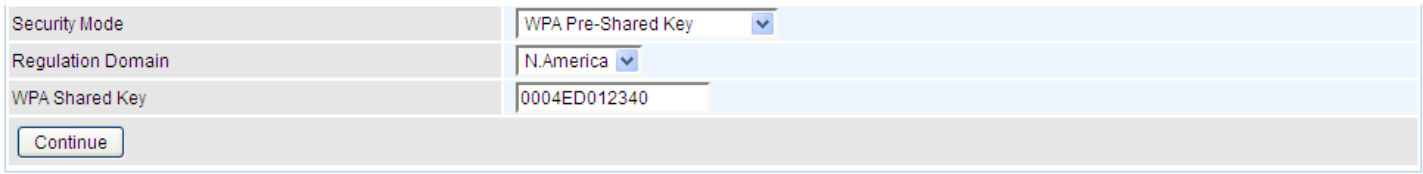
ESSID: The ESSID is the unique name of a wireless access point (AP) to be distinguished from another. For security propose, change to a unique ID name to the AP which is already built-in to the router's wireless interface. It is case sensitive and must not excess 32 characters. Make sure your wireless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

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

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.

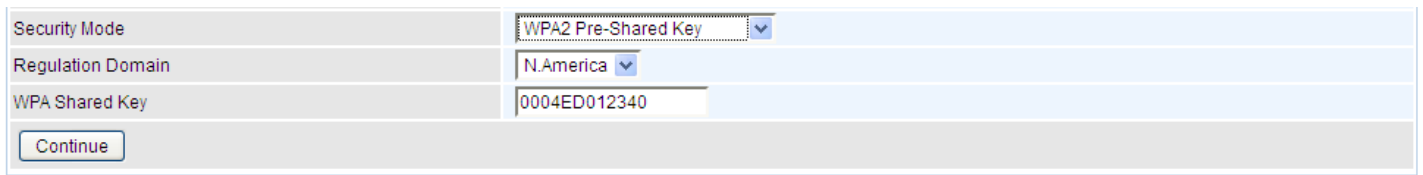
Security Mode: You can disable or enable with WPA or WEP for protecting wireless network. The default mode of wireless security is **Disable**.

WPA Pre-Shared Key



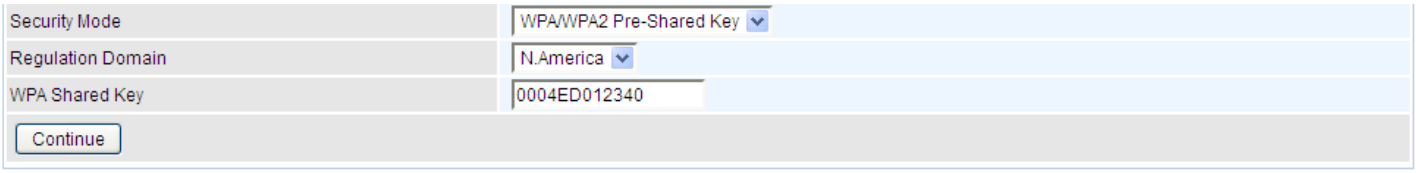
WPA Shared Key: The key for network authentication. The input format is in character style and the key size should be in the range between 8 and 63 characters (here the default is the router or CPE's MAC address in uppercase).

WPA2 Pre-Shared Key



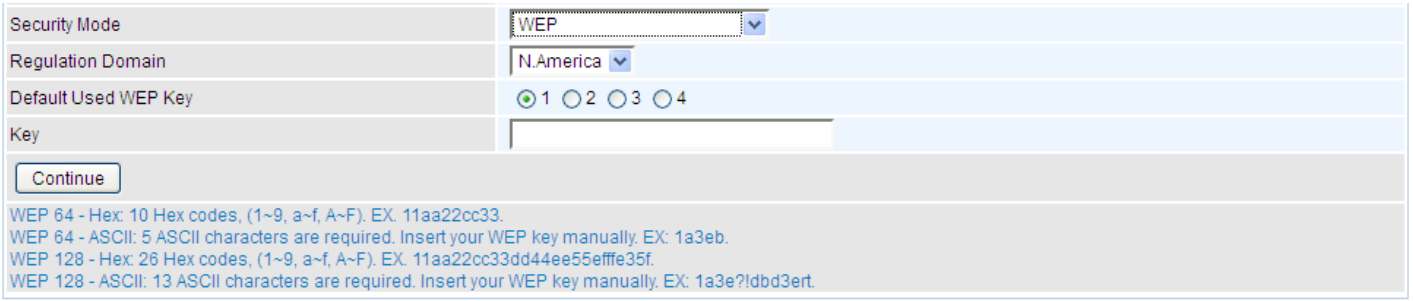
WPA Shared Key: The key for network authentication. The input format is in character style and key size should be in the range between 8 and 63 characters(here the default is the router or CPE's MAC address in uppercase).

WPA/WPA2 Pre-Shared Key



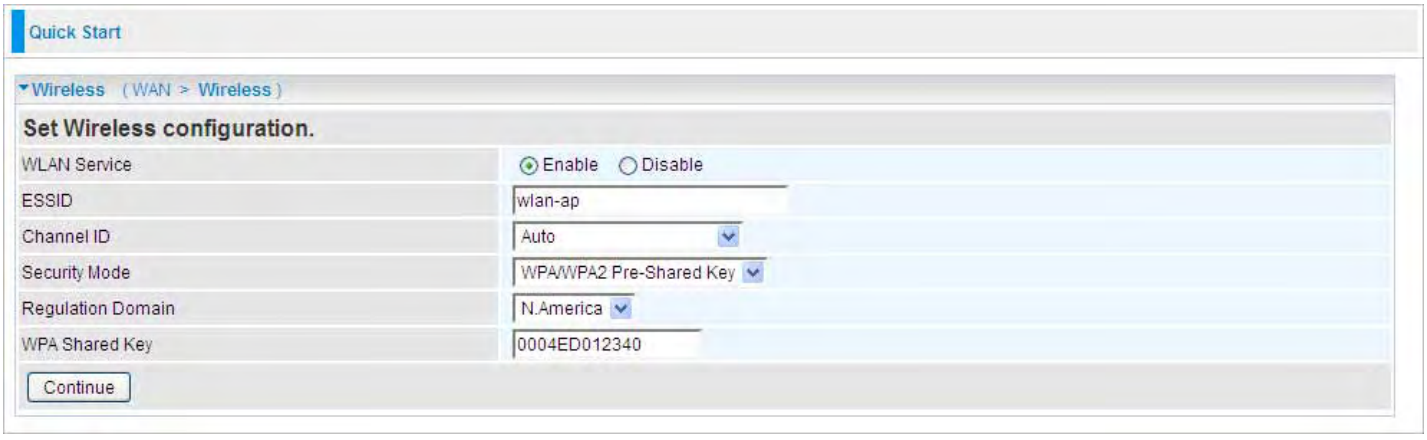
WAP Shared Key: The key for network authentication. The input format is in character style and key size should be in the range between 8 and 63 characters (here the default is the router or CPE's MAC address in uppercase).

WEP

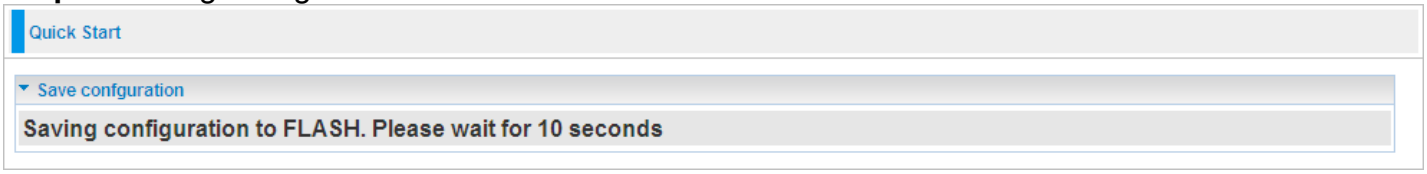


Default Used WEP Key: Select the encryption key ID; please refer to **Key (1~4)** below.

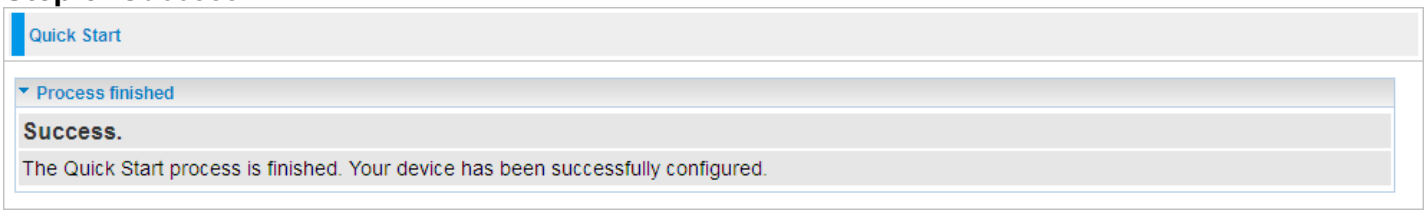
Key: Enter the key to encrypt wireless data. To allow encrypted data transmission, the WEP Encryption Key values on all wireless stations must be the same as the router. There are four keys for your selection. The input format is in HEX or ASCII style, 5 and 13 ASCII codes are required for WEP64 and WEP128 respectively-no any separator is included.



Step 4: Saving configuration.

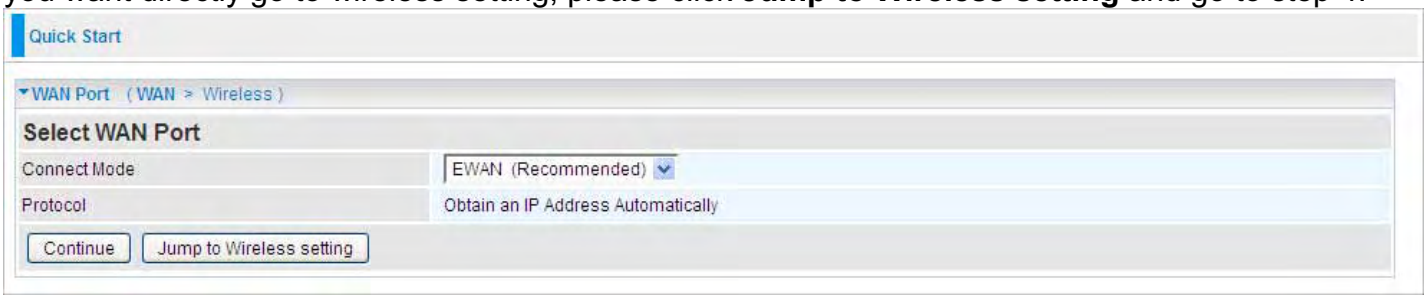


Step 5: Success.



EWAN

Step 1: Select the connection mode:**EWAN**. Then click **Continue**. Here take EWAN for example. If you want directly go to wireless setting, please click **Jump to Wireless setting** and go to step 4.



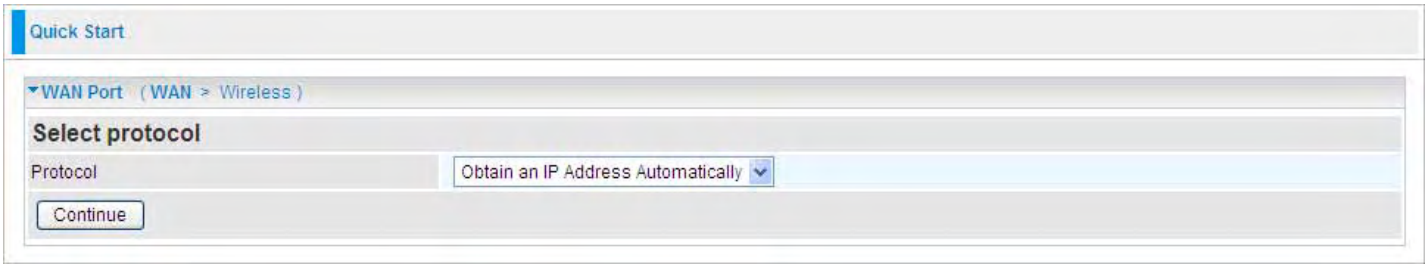
Step 2: Select the Protocol.

Protocol: The current protocol in the device.

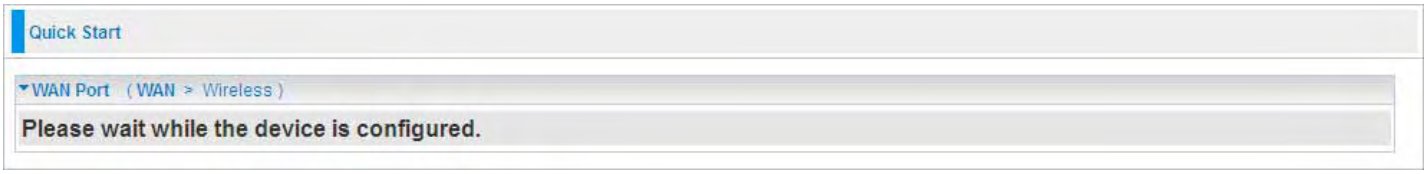
Click on **Continue** to choose the Protocol to connect with EWAN.

Obtain an IP Address Automatically

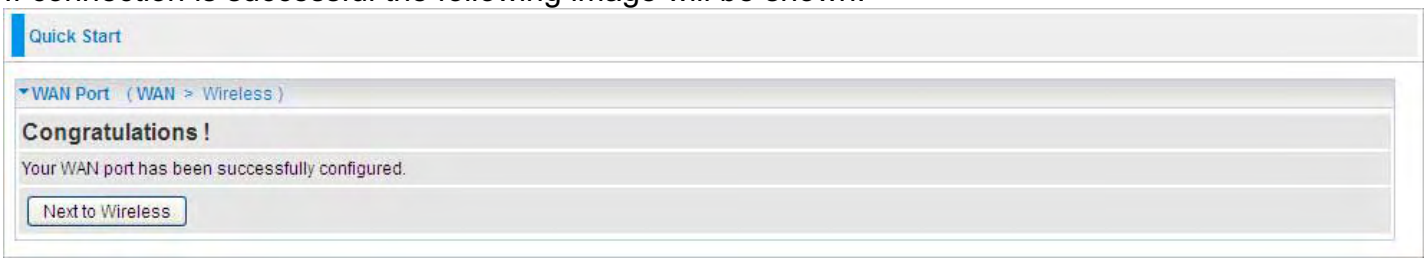
When connecting to the ISP, **Mobile Broadband Wireless-N Router** also functions as a DHCP client. The router can automatically obtain an IP address, subnet mask, gateway address, and DNS server addresses if the ISP assigns this information via DHCP.



Protocol: The current protocol in the device
Click on the **Continue** button and wait for your connection to be connected.

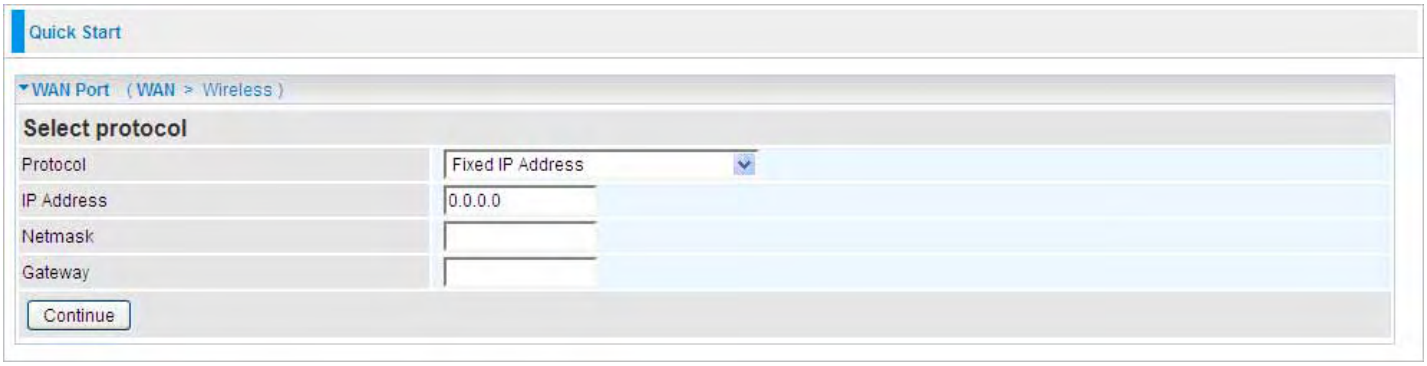


If connection is successful the following image will be shown.



Fixed IP Address

Select this option to set static IP information. You will need to enter in the Connection type, IP address, Netmask, and gateway address, provided to you by your ISP. Each IP address entered in the fields must be in the appropriate IP form, which are four IP octets separated by a dot (x.x.x.x). The Router will not accept the IP address if it is not in this format.



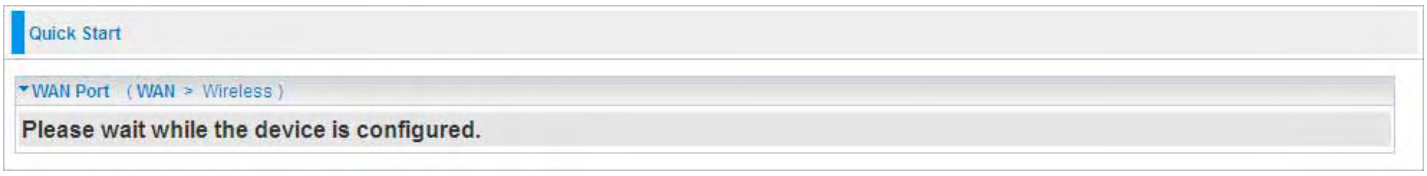
Protocol: The current ATM protocol in the device

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

Netmask: The default is 0.0.0.0. User can change it to other such as 255.255.255.0.Type the subnet mask assigned to you by your ISP (if given).

Gateway: You must specify a gateway IP address (supplied by your ISP)

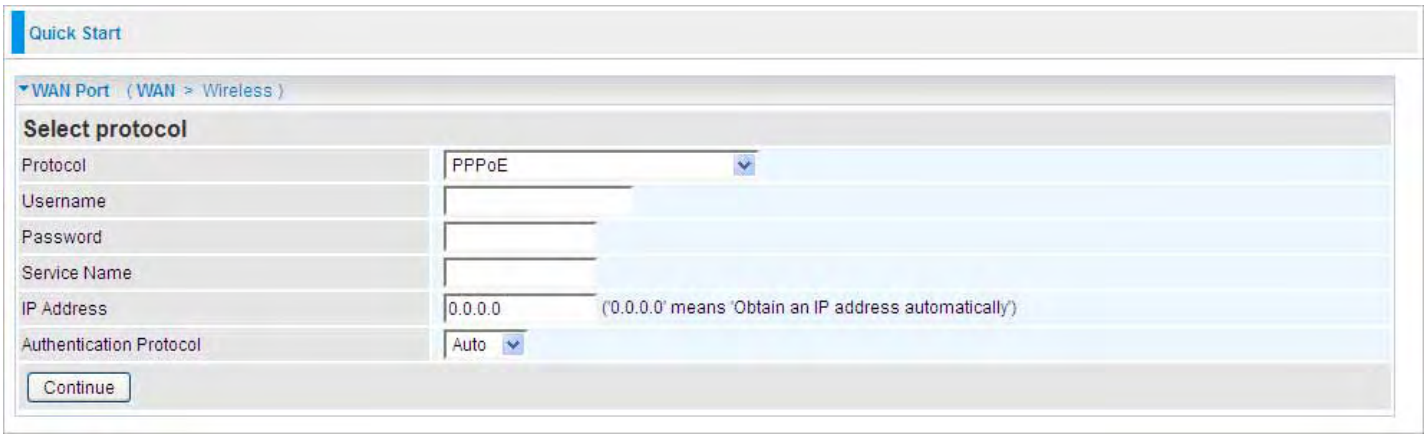
Click on the **Continue** button and wait for your connection to be connected.



If connection is successful the following image will be shown.

PPPoE

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



Protocol: The current ATM protocol in the device

Username: Enter the username provided by your ISP. You can input up to 128 alphanumeric characters (case sensitive). This is in the format of “username@ispname” instead of simply “username”.

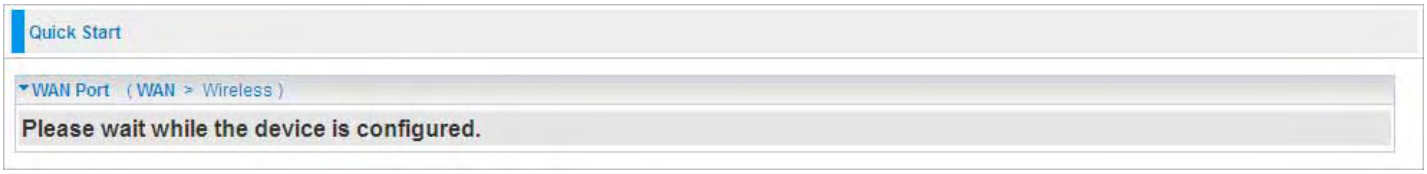
Password: Enter the password provided by your ISP. You can input up to 128 alphanumeric characters (case sensitive).

Service Name: Enter a name for this connection.

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

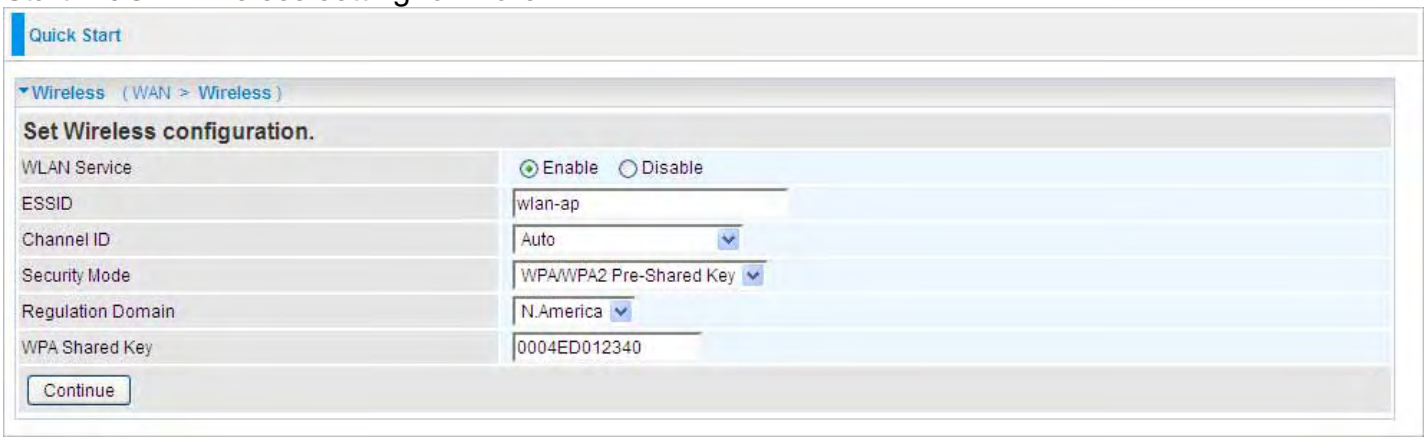
Auth. Protocol: Default is Auto. Your ISP advises on using Chap or Pap.

Click on the **Continue** button and wait for your connection to be connected.

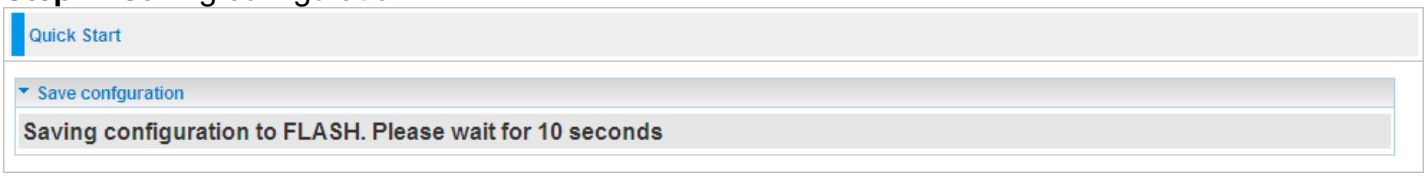


If connection is successful the following image will be shown.

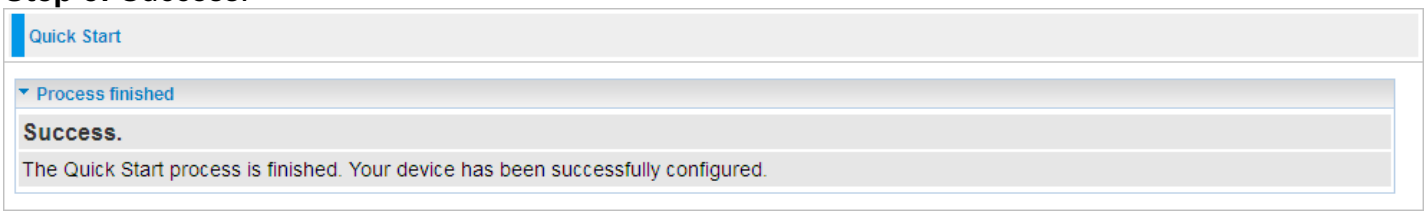
Step 3: In the previous step, press **Next to Wireless** to Set Wireless configuration. Turn to Quick Start > 3G > Wireless setting for more.



Step 4: Saving configuration.



Step 5: Success.



Configuration

Click this item to access the following sub-items that configure the 3G router: **LAN, WAN, System, Firewall, QoS, Virtual Server, Wake on LAN, Time Schedule** and **Advanced.**

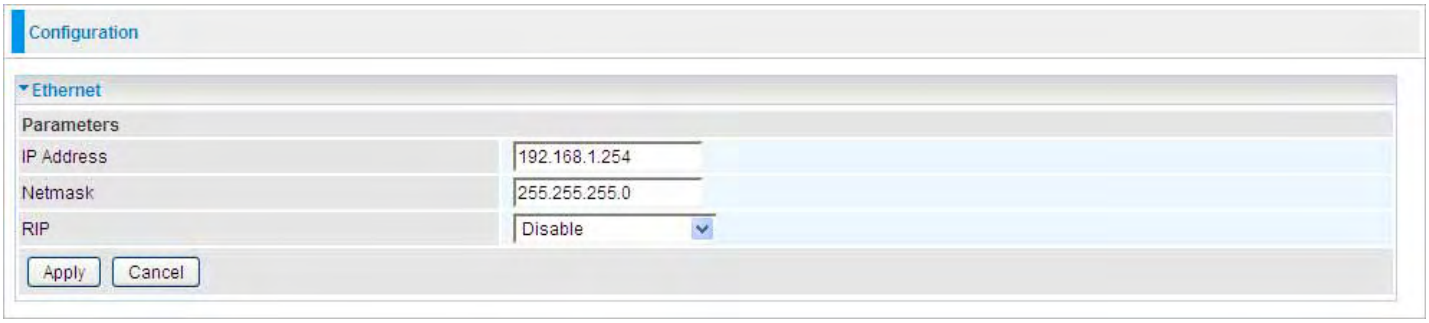
These functions are described in the following sections.

LAN (Local Area Network)

A Local Area Network (LAN) is a shared communication system to which many computers are attached and is limited to the immediate area, usually the same building or floor of a building.

There are six items within the LAN section: **Ethernet, IP Alias, Wireless, Wireless Security, WPS** 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.

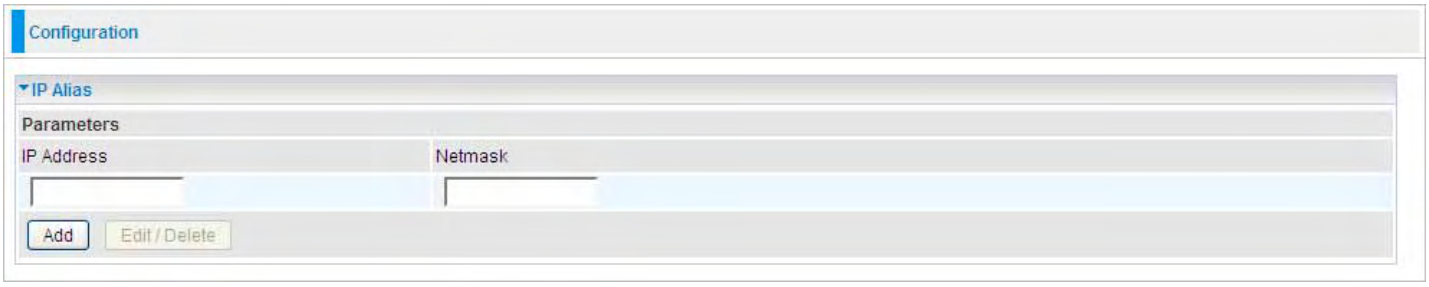
IP Address: The IP on this router, default is 192.168.1.254.

Netmask: The subnet mask on this router.

RIP: RIP v1, RIP v2 Broadcast, RIP v1+v2 Broadcast and RIP v2 Multicast.

IP Alias

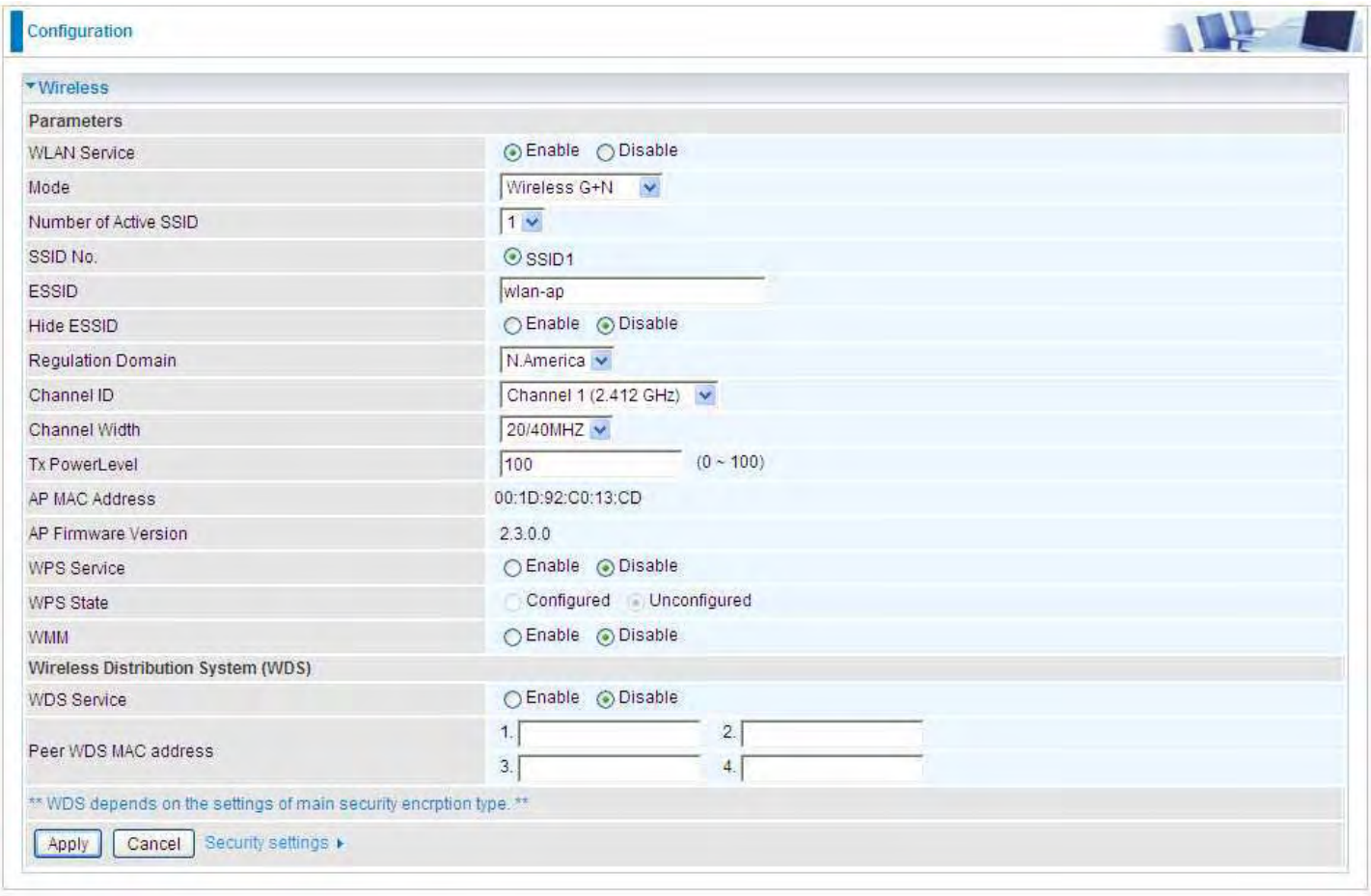
This function allows the creation of multiple virtual IP interfaces on this router. It helps to connect two or more local networks to the ISP or remote node. In this case, an internal router is not required.



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

Netmask: Specify a subnet mask on this virtual interface.

Wireless



Parameters

WLAN Service: Default setting is set to **Enable**.

Mode: The default setting is **Wireless G + N** (Mixed mode). If you do not know or have both 11g and 11n devices in your network, then keep the default in **mixed mode**. From the drop-down manual, you can select **Wireless – G** if you have only 11g card. If you have only 11b card, then select **Wireless – B**. If you have only 11n card, then select **Wireless – N**.

Number of Active SSID: Number of SSID you can choose.

SSID No.: The SSID you choose.

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

Note: ESSID is case sensitive and must not excess 32 characters.

Hide ESSID: It is function in which transmits its ESSID to the air so that when wireless client searches for a network, router can then be discovered and recognized. Default setting is **Disable.**

⊙ **Enable:** Select Enable if you do not want broadcast your ESSID. When select Enable, the ESSID will be hided in stead of broadcasting, thus when wireless client searches for this AP, failure occurs. This ESSID(AP) will be invisible to you. In this case, if you want to join this wireless network, enter the exactly ESSID manually and some security settings.

⊙ **Disable:** When Disable is selected, the router will broadcast the ESSID to allow anybody with a wireless client to be able to identify the Access Point (AP) of your router. Select the specific ESSID

scanned, with some security settings, you will join this wireless network.

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 ID channel that you would like to use.

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

Tx Power Level: It is 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 premises environment and 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: Enable / disable

WPS State: Current WPS state in AP. It is be used for WCN (Windows Connect Now).

- **Configured:** This AP is be configured via WPS. It is not allow to configure via WCN.
- **Unconfigured:** This AP is un-configured via WPS. It can be configure via WCN.

WMM: This feature works concurrently with QoS that enables the system to prioritize the flow of data

packets according to 4 categories: Voice, Video, Best Efforts and Background.

- **Enable:** Click to activate WMM feature.
- **Disable:** Click to deactivate WMM feature.

Wireless Distribution System (WDS)

It is a wireless access point mode that enables wireless link and communication with other access point. It is easy to be installed, simply define the peer's MAC address of the connected AP. WDS takes advantages of 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.

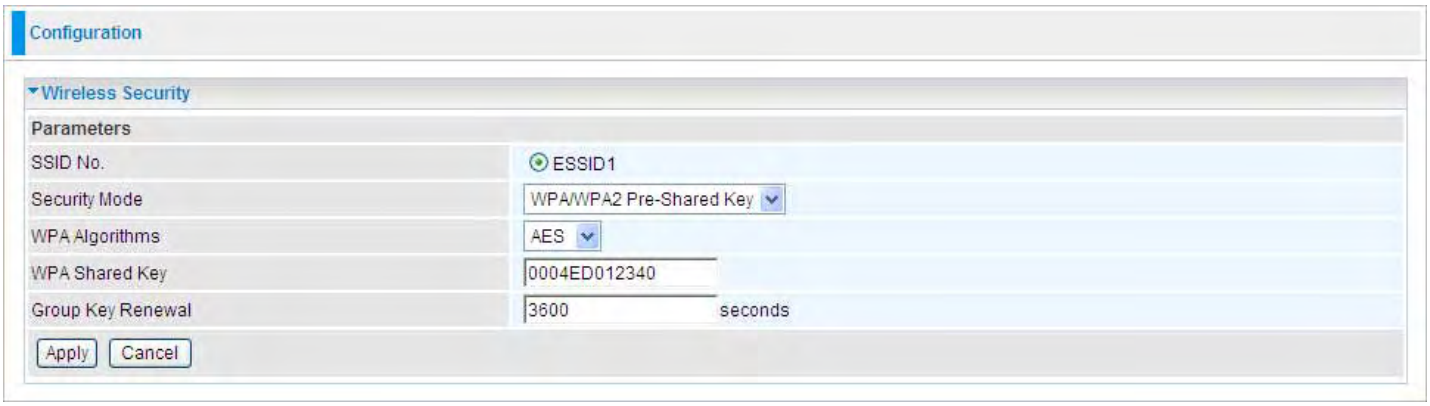
WDS Service: The default setting is **Disable.** Check **Enable** radio button to activate this function.

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, Semicolon (;) or Dash (-) must be included.

Wireless Security

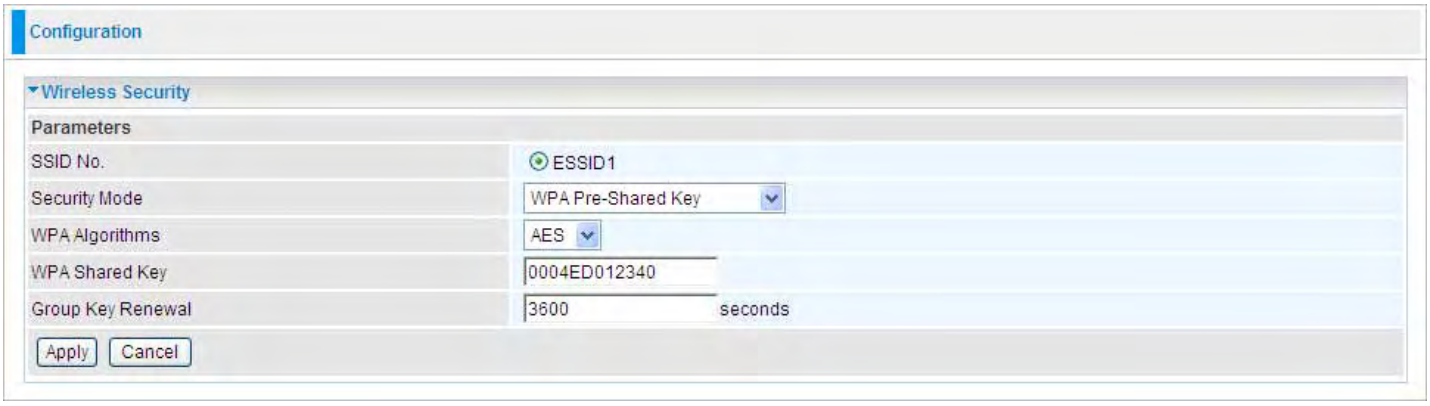
You can disable or enable with WPA or WEP for protecting wireless network.



SSID No.: Choose the SSID you want to set.

Security Mode: There are five security modes for you to choose.

WPA Pre-Shared Key

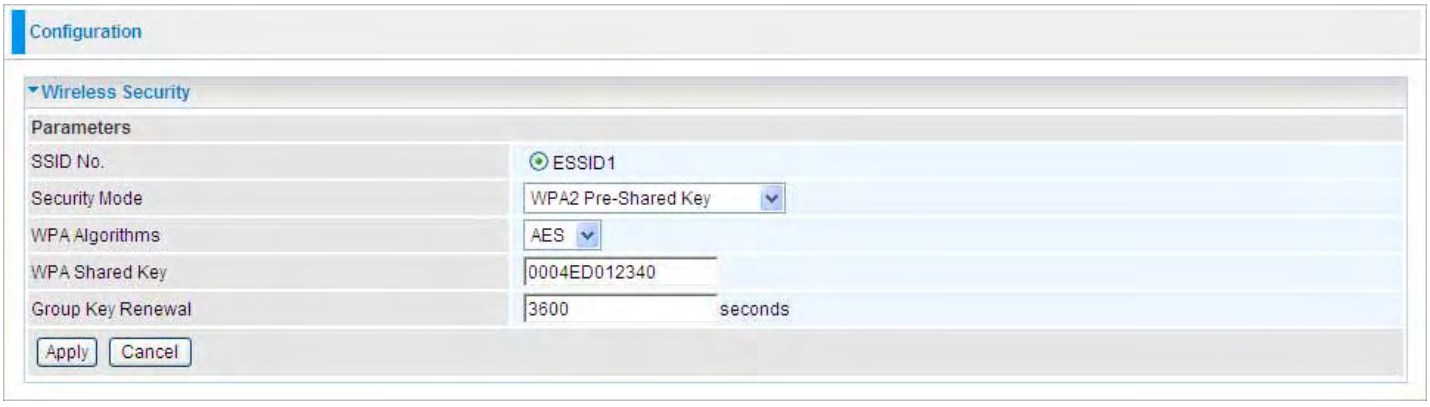


WPA Algorithms: TKIP (Temporal Key Integrity Protocol) / AES (Advanced Encryption Standard) utilizes a stronger encryption method and incorporates Message Integrity Code (MIC) to provide protection against hackers.

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).

WPA2 Pre-Shared Key

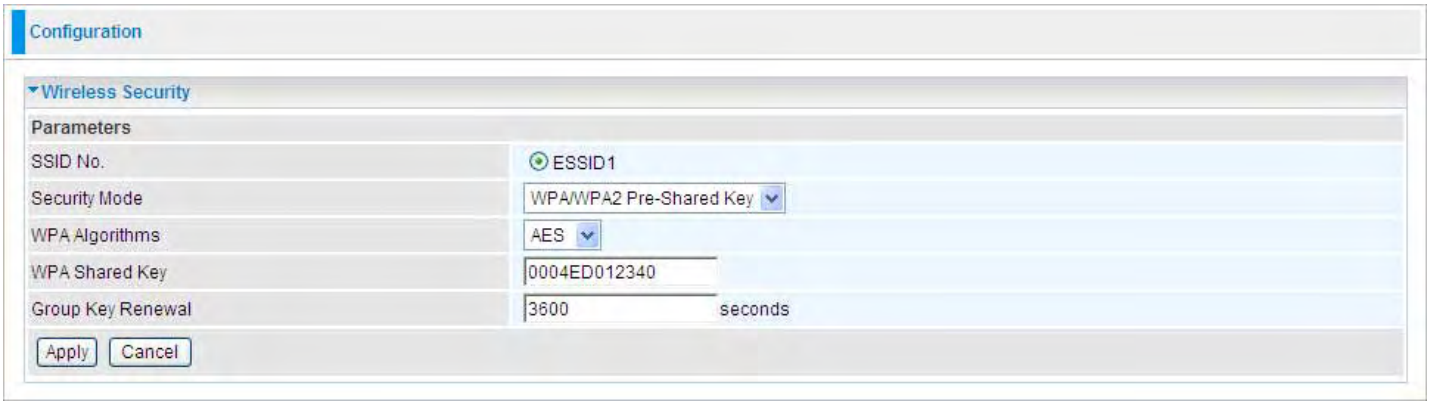


WPA Algorithms: TKIP (Temporal Key Integrity Protocol) / AES (Advanced Encryption Standard) utilizes a stronger encryption method and incorporates Message Integrity Code (MIC) to provide protection against hackers.

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).

WPA/WPA2 Pre-Shared Key

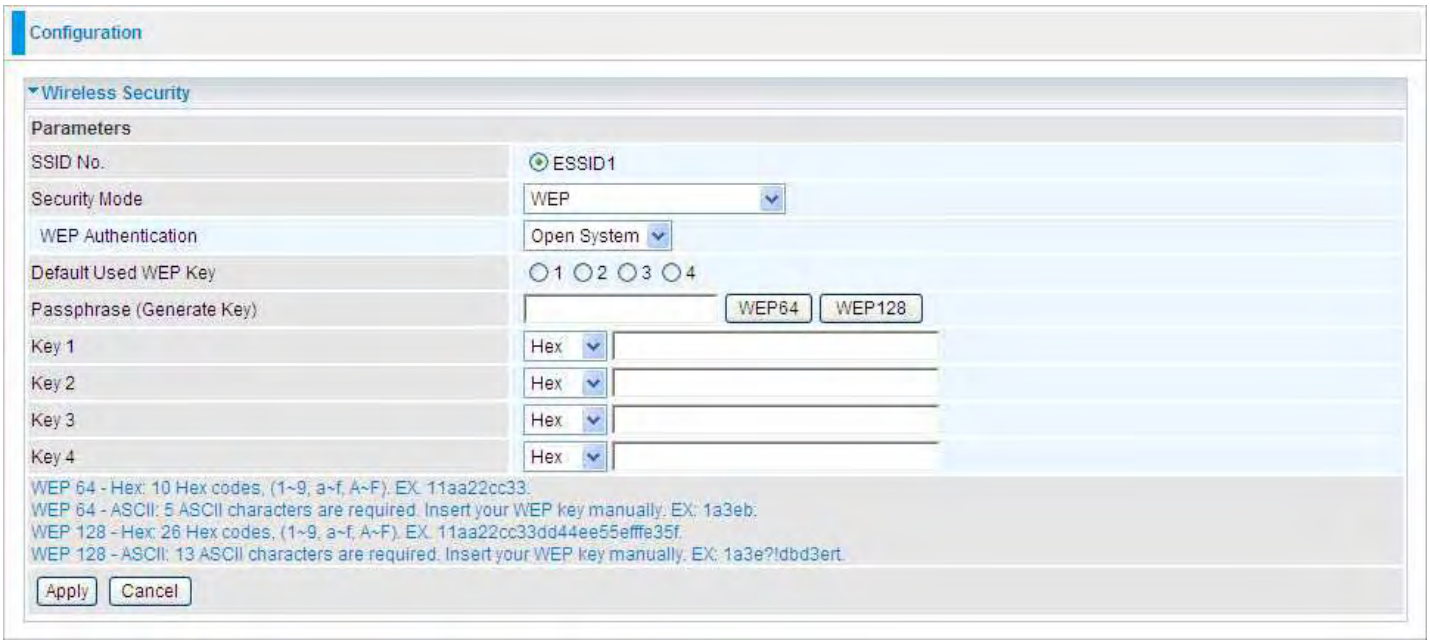


WPA Algorithms: TKIP (Temporal Key Integrity Protocol) / AES (Advanced Encryption Standard) utilizes a stronger encryption method and incorporates Message Integrity Code (MIC) to provide protection against hackers.

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).

WEP



WEP Authentication: To prevent unauthorized wireless stations from accessing data transmitted over the network, the router offers secure data encryption, known as WEP. If you require high security for transmissions, there are three options to select from: **Open System, Share key or Both**.

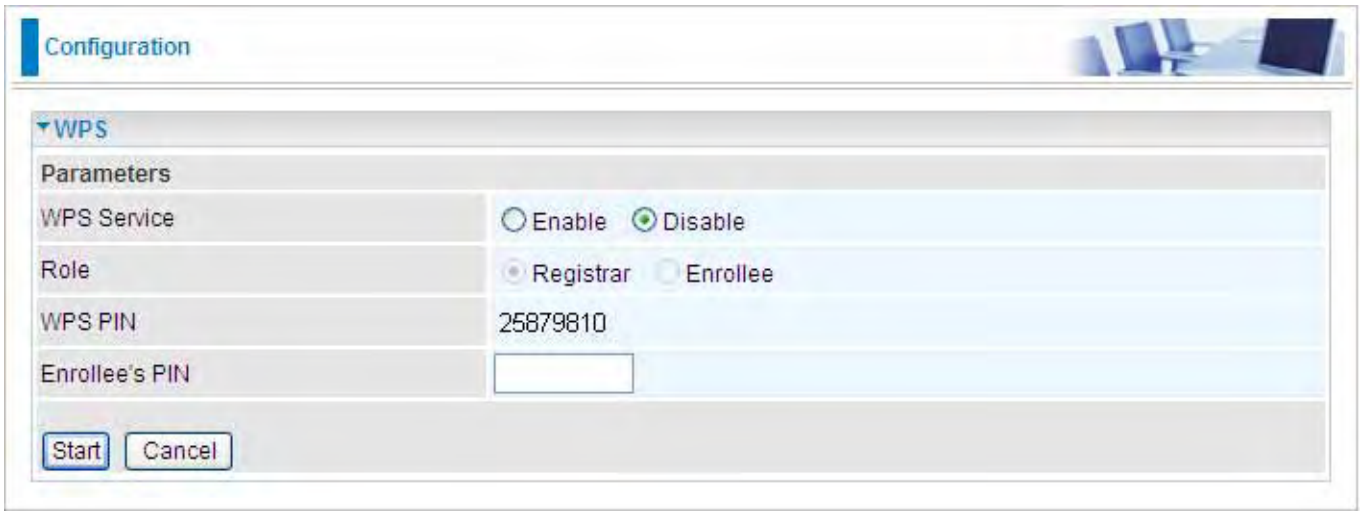
Default Used WEP Key: Select the encryption key ID; please refer to **Key (1~4)** below.

Passphrase: This is used to generate WEP keys automatically based upon the input string and a pre-defined algorithm in WEP64 or WEP128. You can input the same string in both the AP and Client card settings to generate the same WEP keys. Please note that you do not have to enter **Key (1-4)** as below when the **Passphrase** is enabled.

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 is in HEX or ASCII style, 5 and 13 ASCII codes are required for WEP64 and WEP128 respectively-no any separator is included.

WPS

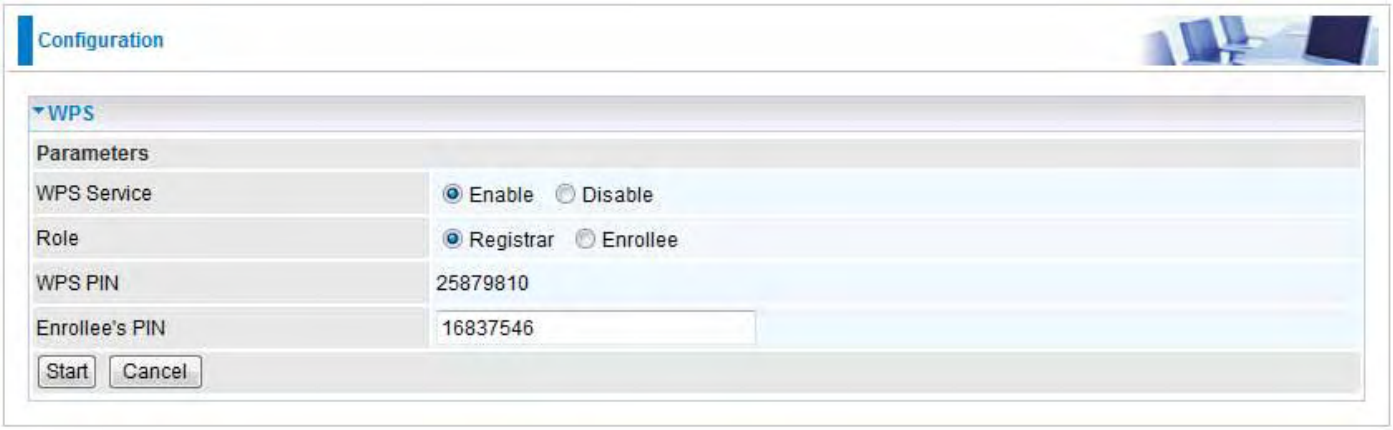
WPS (WiFi Protected Setup) feature is a standard protocol created by Wi-Fi Alliance. This feature greatly simplifies the steps needed to create a Wi-Fi network for a residential or an office setting. WPS supports 2 types of configuration methods which are commonly known among consumers: **PIN Method**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



Wi-Fi Network Setup

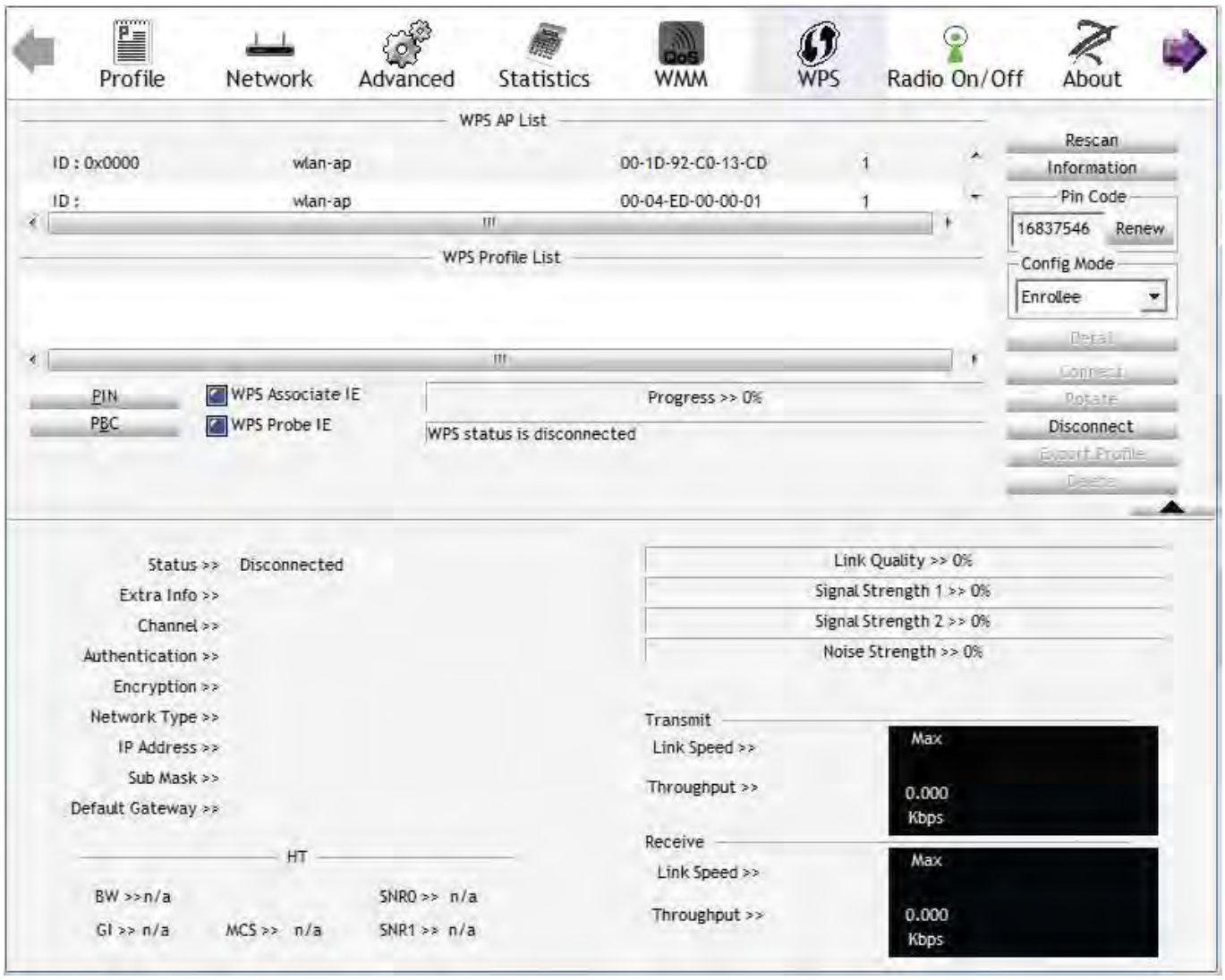
PIN Method: Configure AP as Registrar

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

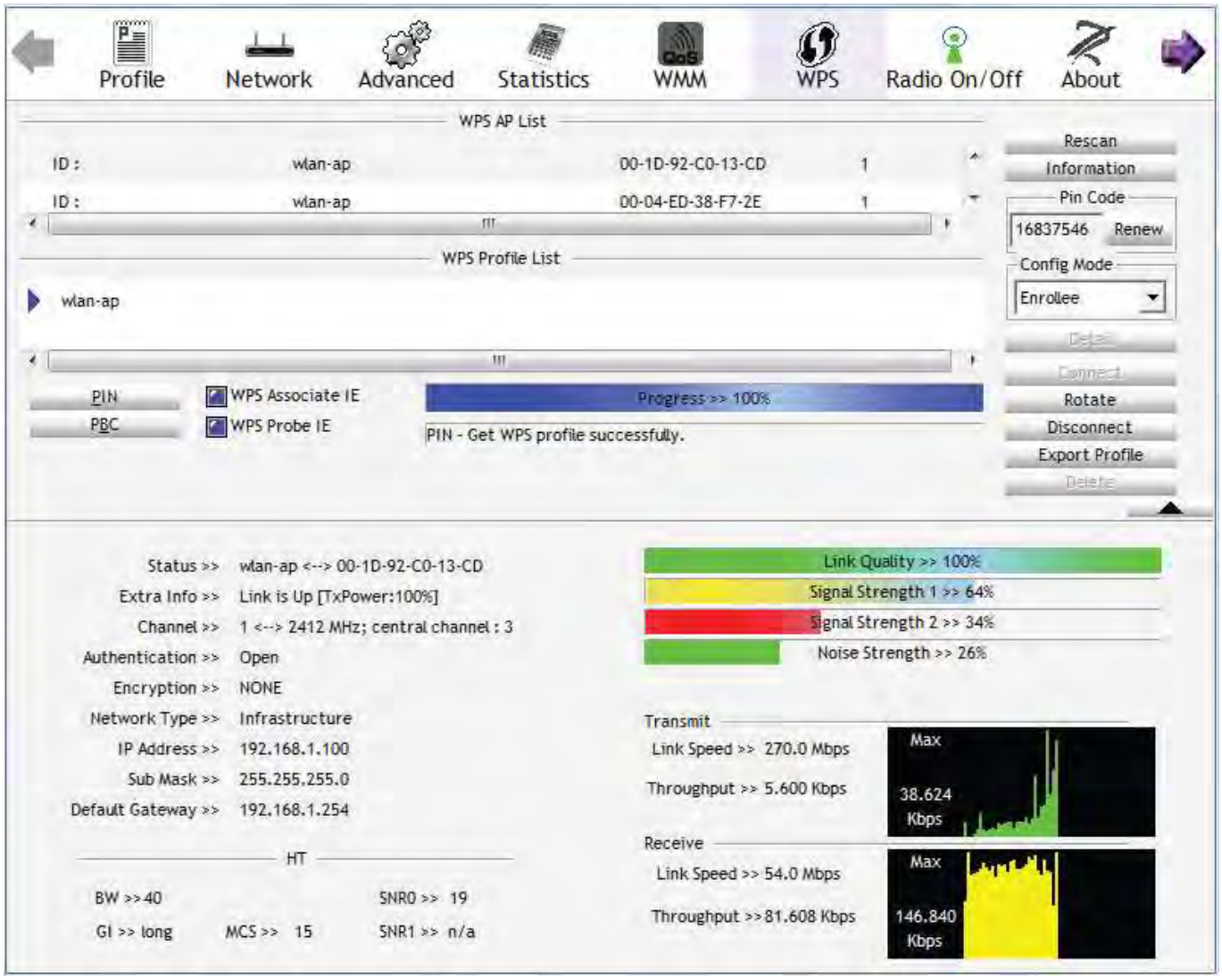


2. Enter the Enrollee's PIN number and then press Start.

3. Launch the wireless client's WPS utility (eg. Ralink Utility). Set the Configure 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.



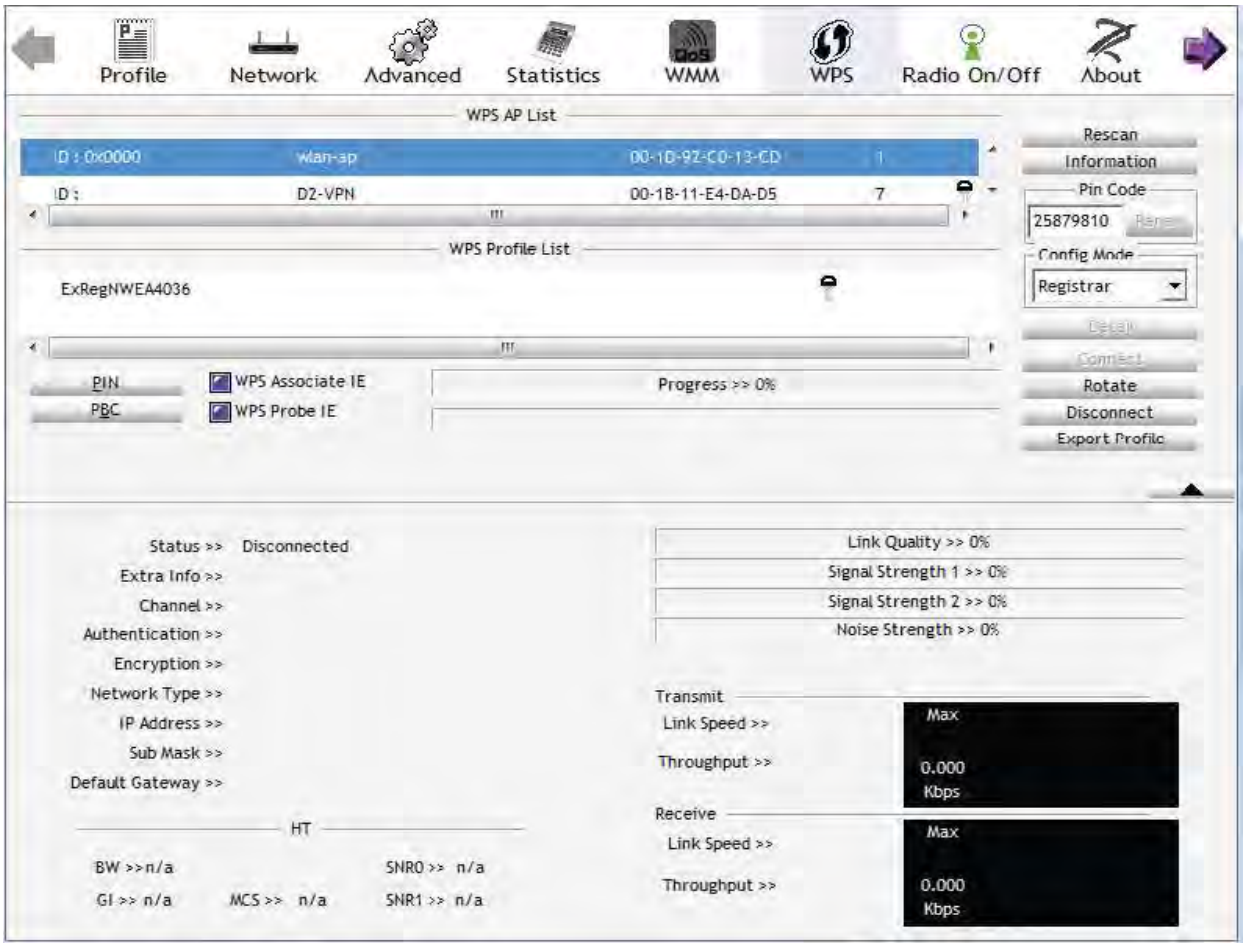
4. The client's SSID and security setting will now be configured to match the SSID and security setting of the registrar.



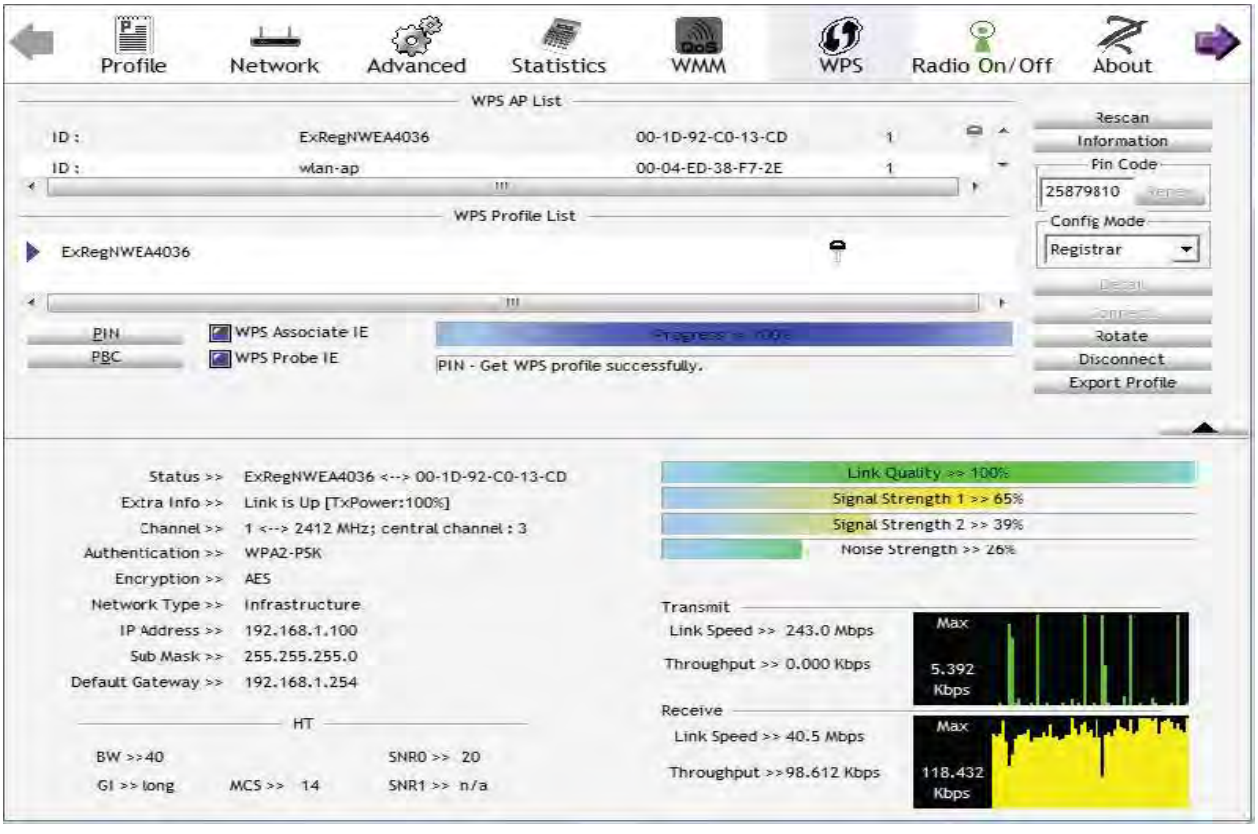
PIN Method: Configure AP as Enrollee

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

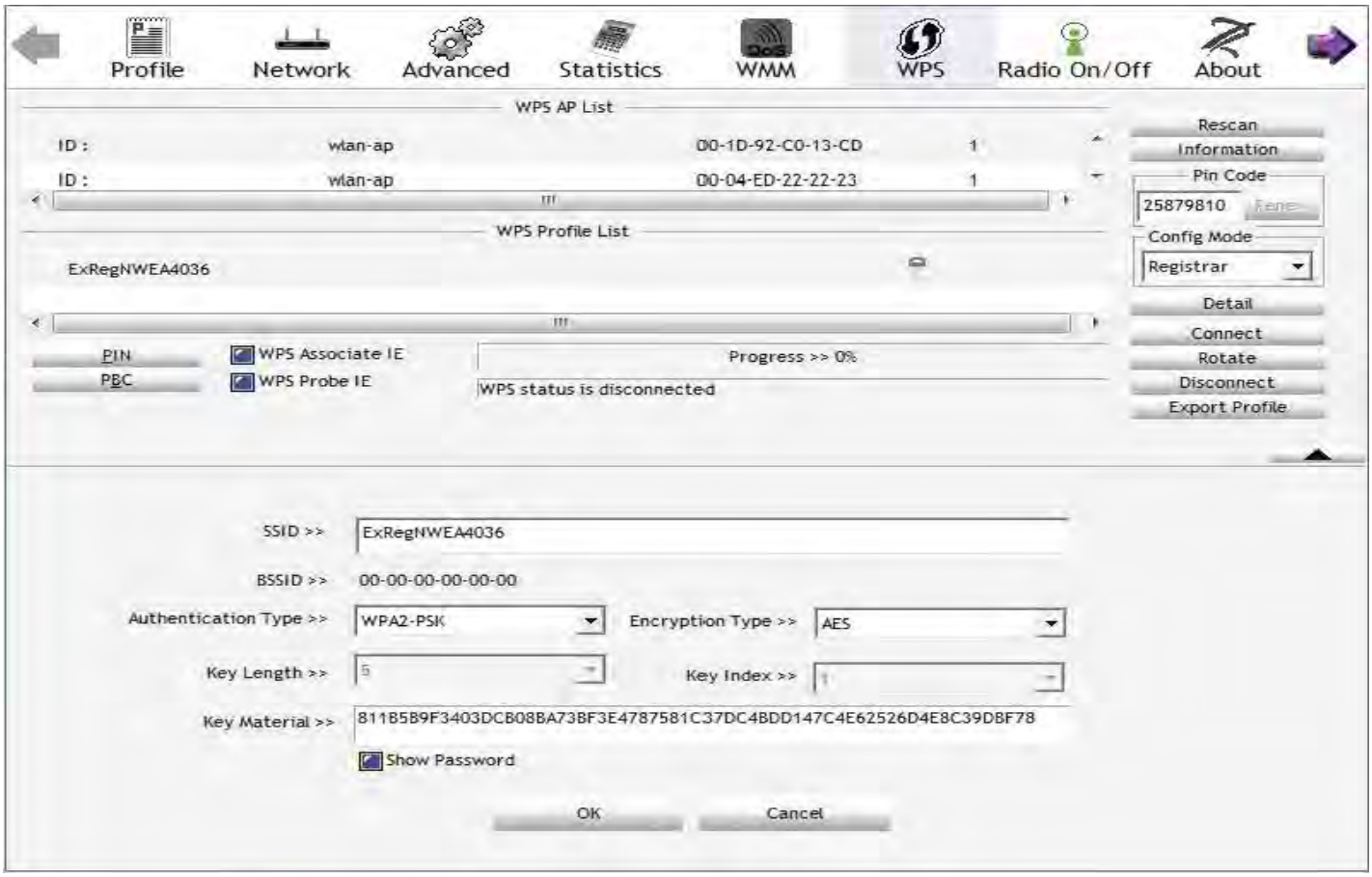
3. Launch the wireless client's WPS utility (e.g. Ralink Utility). Set the Config Mode as Registrar. Enter the PIN number in the PIN Code column then choose the correct AP (eg. wlan-ap) from the WPS AP List section before pressing the PIN button to run the scan.



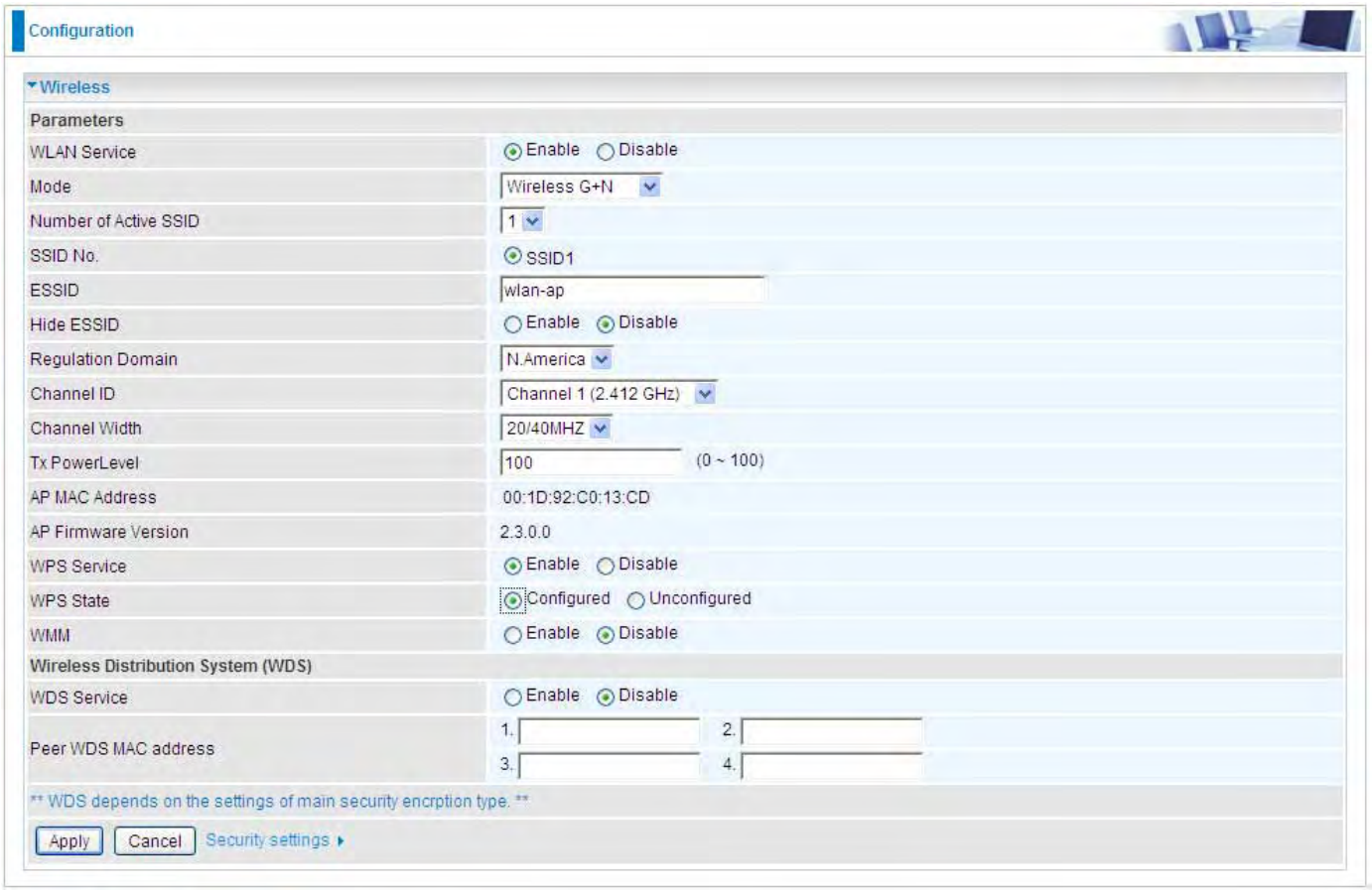
4. The router's (AP's) SSID and security setting will now be configured to match the SSID and security setting of the registrar.

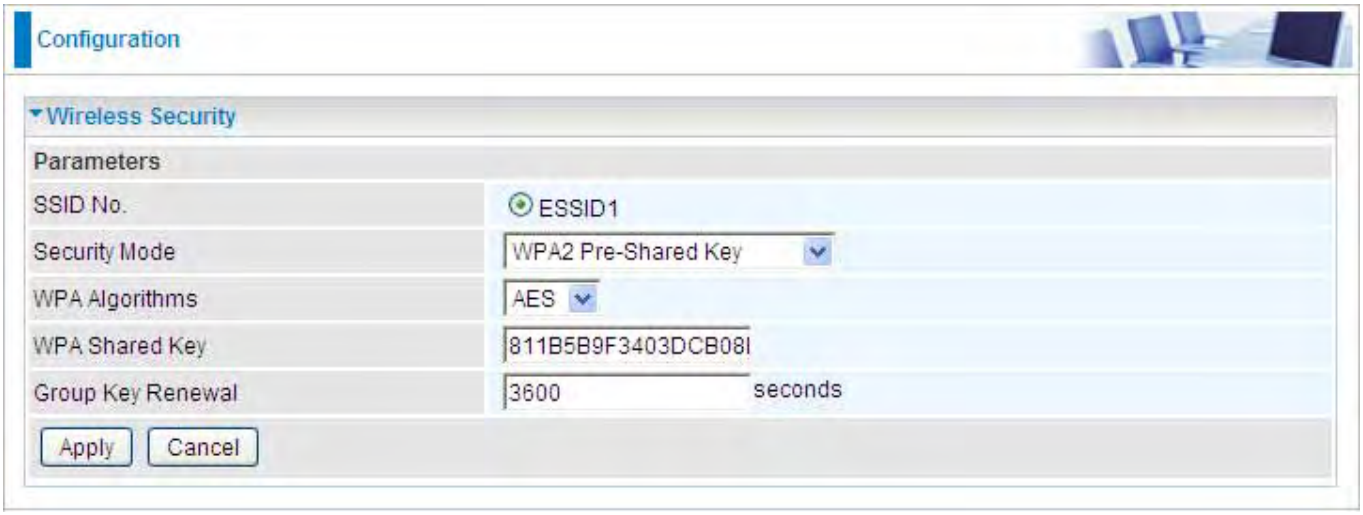


5. Now to make sure that the setup is correctly done, cross check to see if the SSID and the security setting of the registrar setting match with the parameters found on both Wireless Configuration and Wireless Security Configuration page.



The parameters on both Wireless Configuration and Wireless Security Configuration page are as follows:

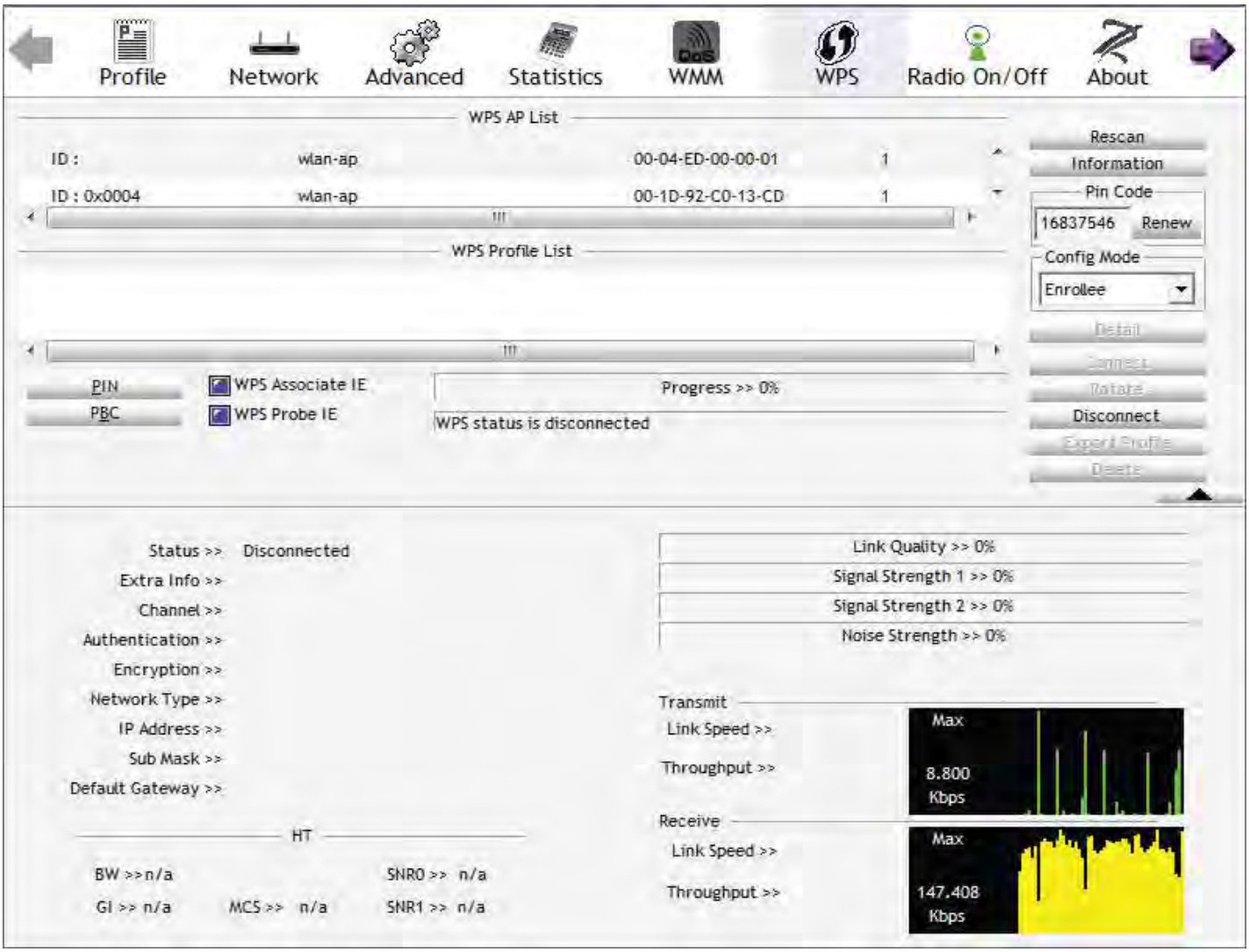




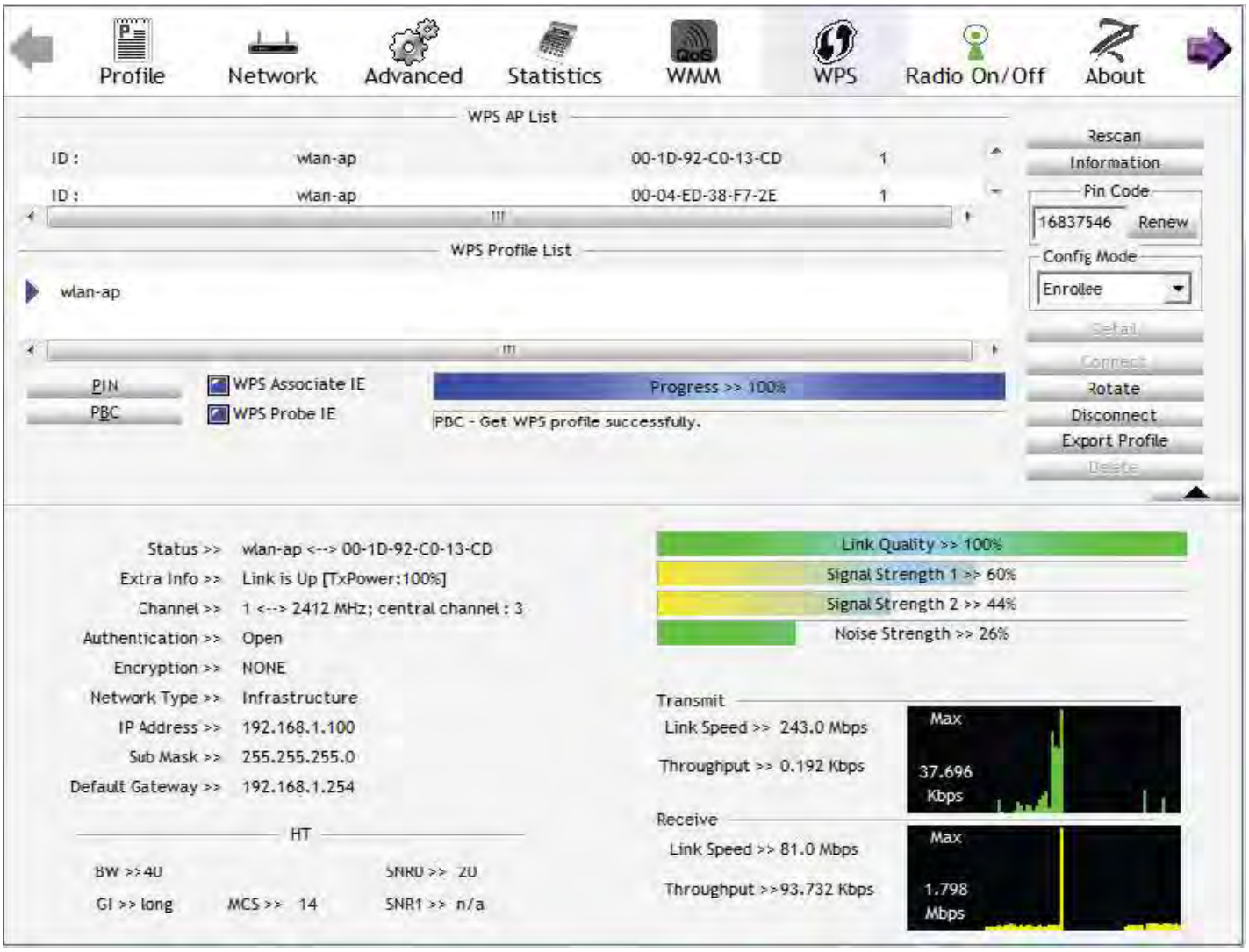
PBC Method:

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.

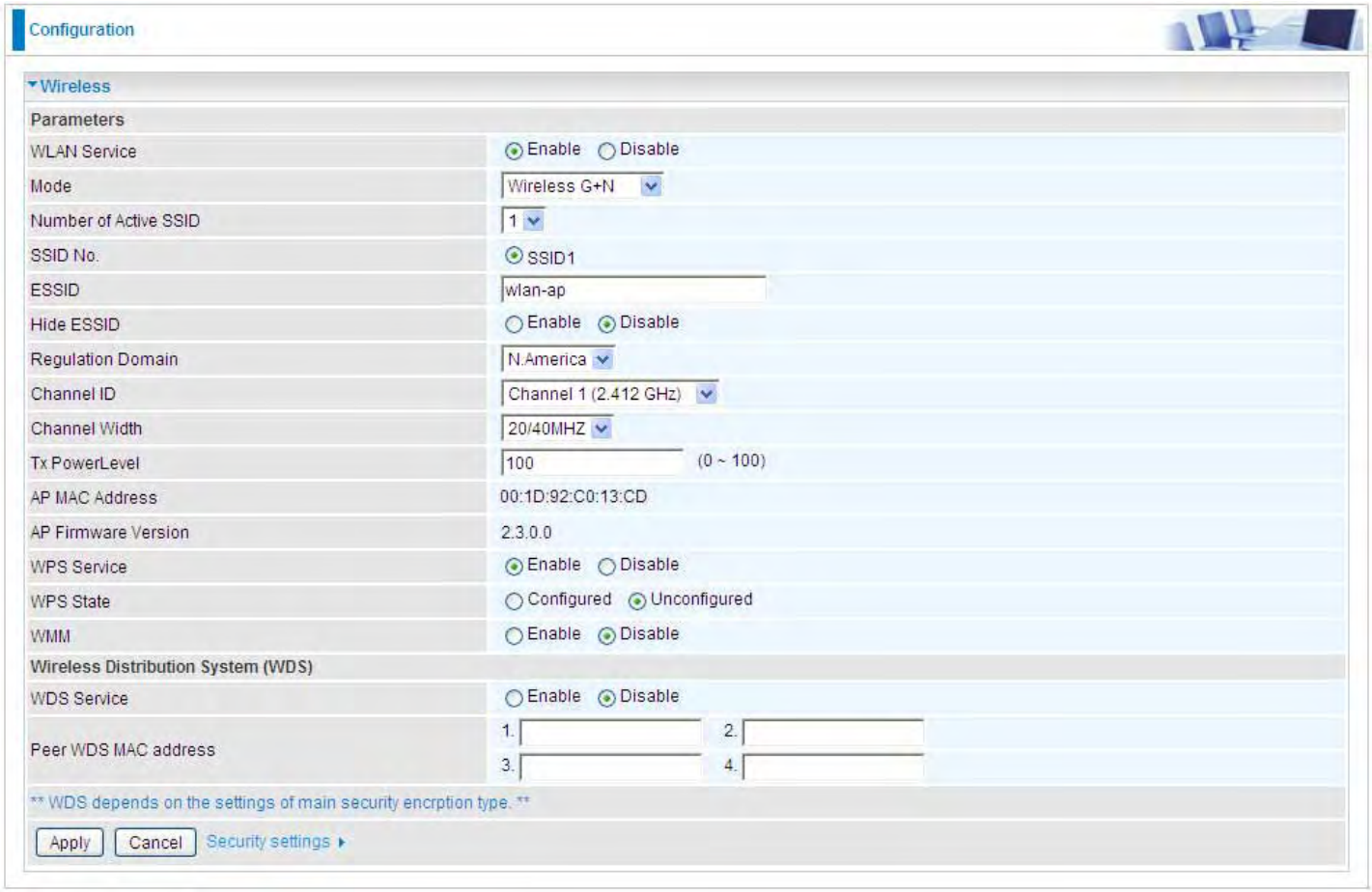


3. When the PBC button is pushed, a wireless communication will be established between your router and the PC. The client's SSID and security setting will now be configured to match the SSID and security setting of the router.

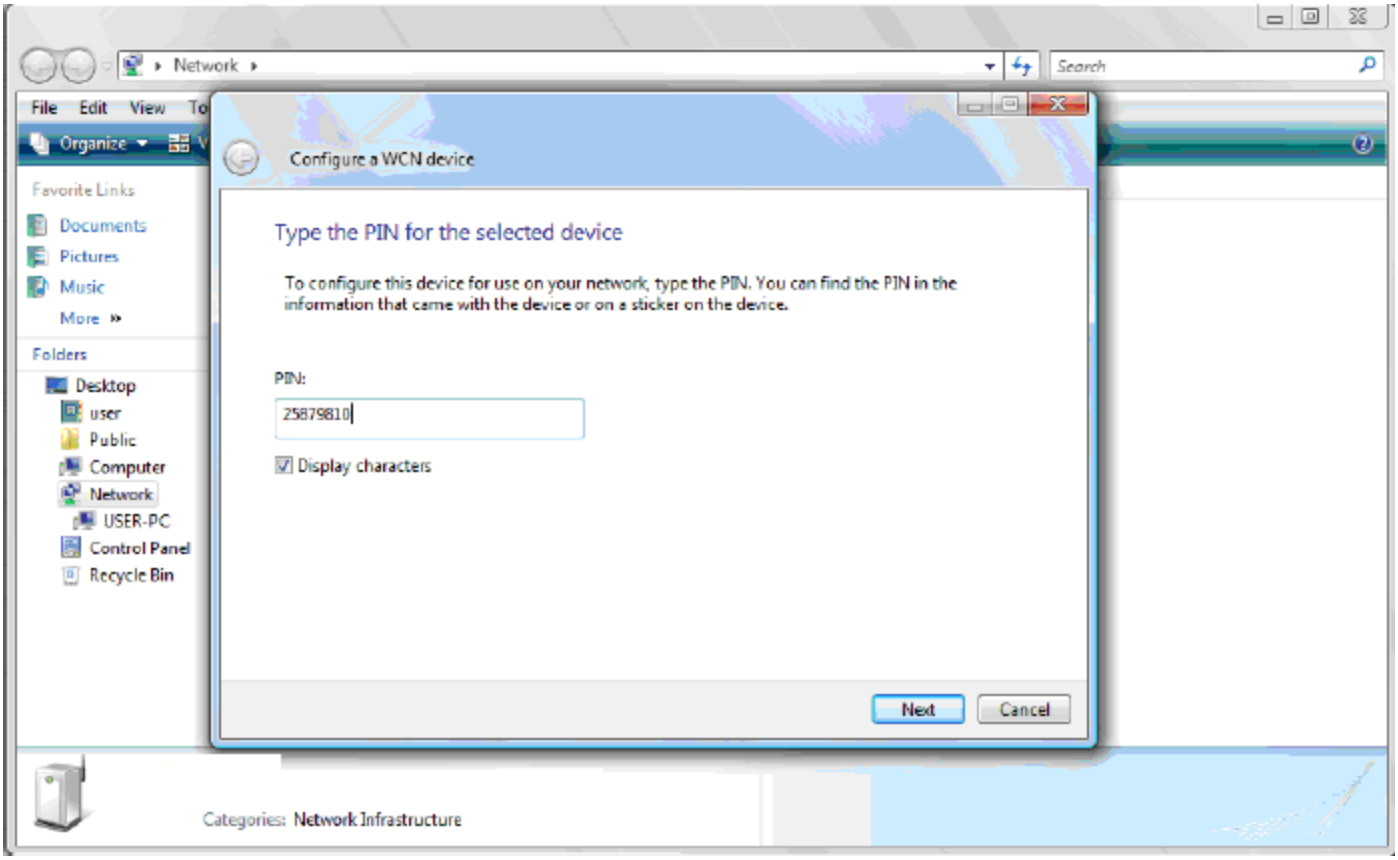


Wi-Fi Network Setup with Windows Vista WCN:

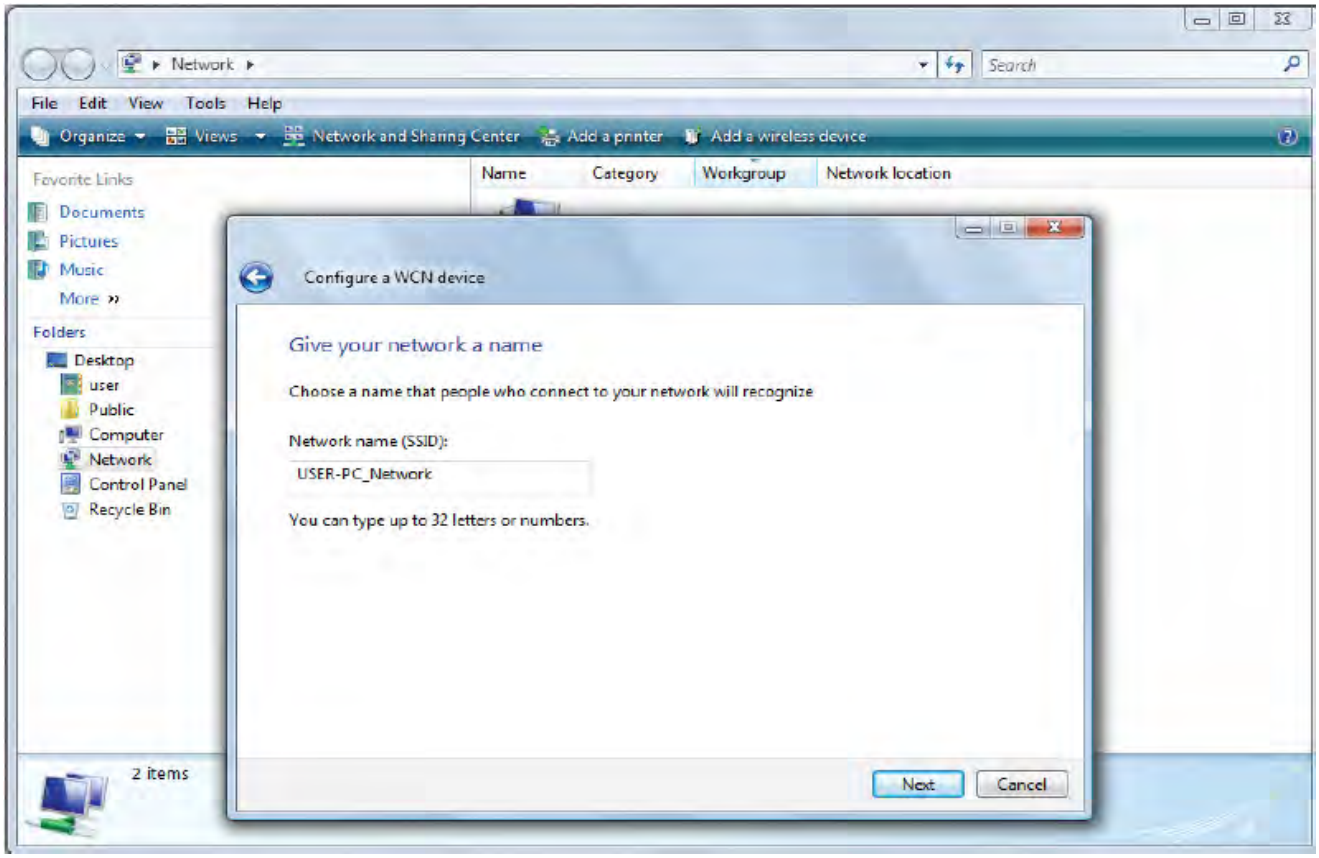
1. Jot down the AP PIN from the Web (eg. 25879810).
2. Access the Wireless configuration of the web GUI. Set the WPS State to **Unconfigured** then click Apply.



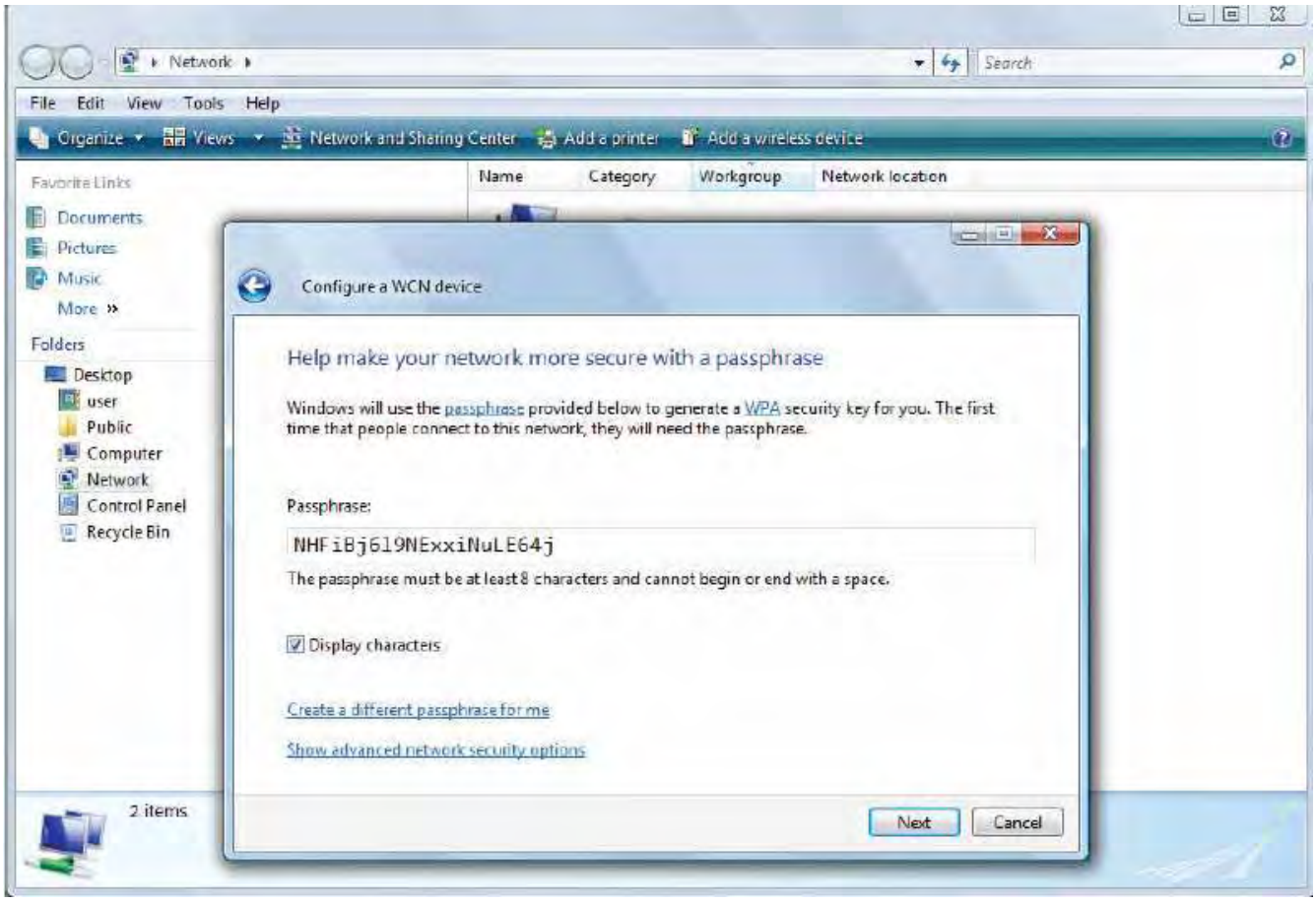
3. In your Vista operating system, access the Control Panel page, then select Network and Internet > View Network Computers and Devices. Double click on the router icon and enter the AP PIN in the column provided then press Next.



4. Enter the AP SSID then click Next.

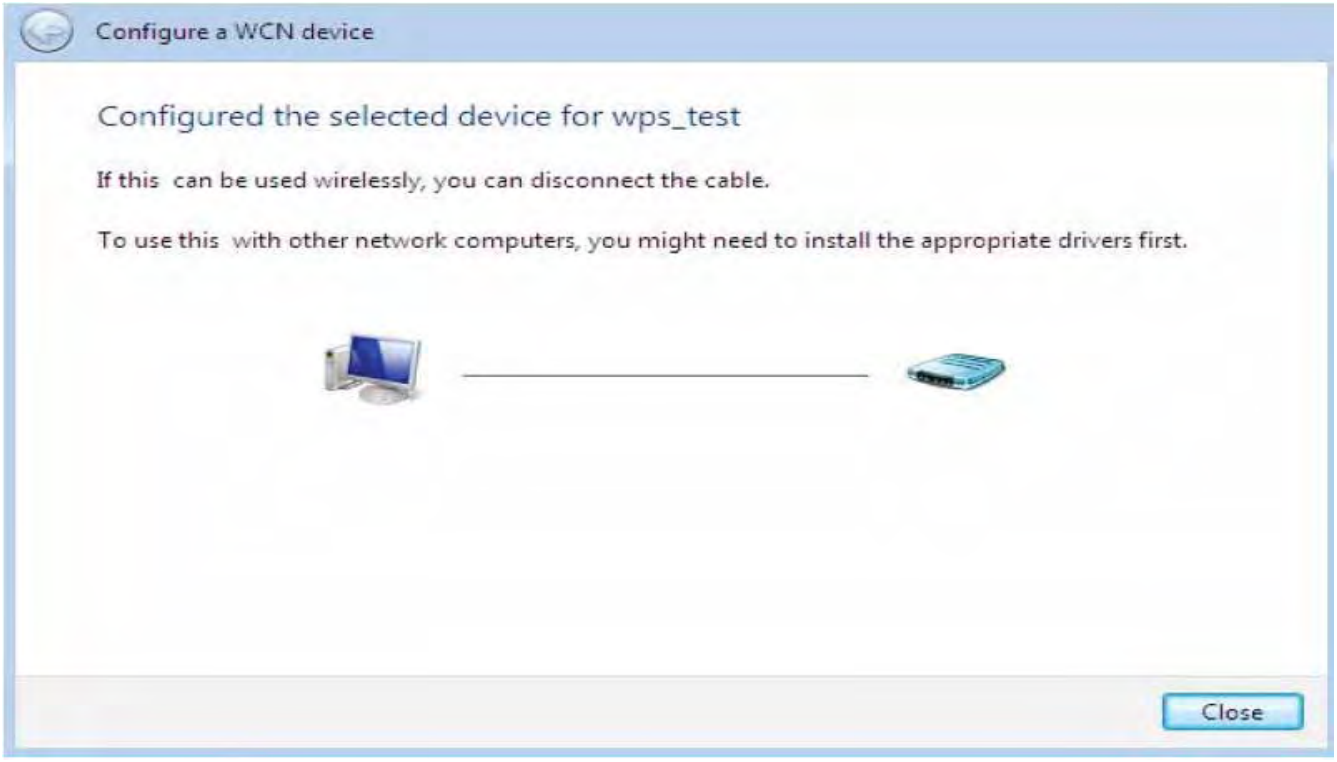


5. Enter the passphrase then click Next.



6. When you have come to this step, you will have completed the Wi-Fi network setup using the

built-in WCN feature in Windows Vista.



DHCP Server

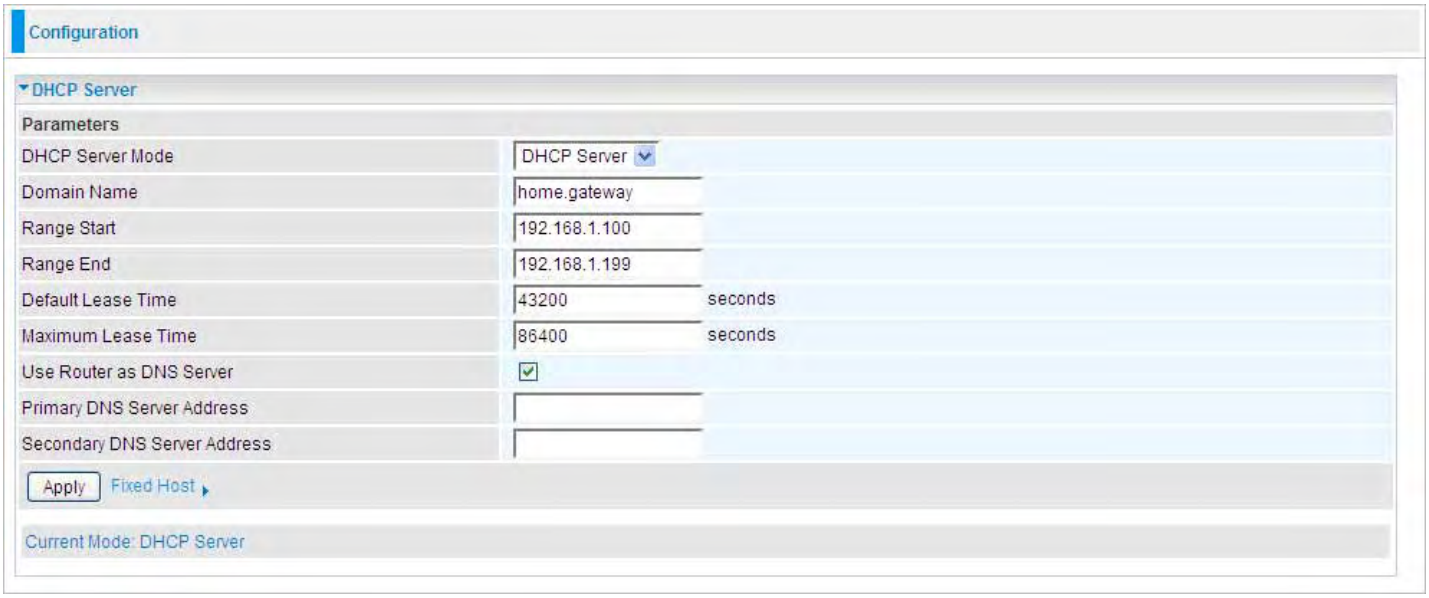
You can disable or enable the DHCP (Dynamic Host Configuration Protocol) server or enable the router's DHCP relay functions. The DHCP protocol allows your router to dynamically assign IP addresses to PCs on your network if they are configured to obtain IP addresses automatically.

DHCP Server Mode: Disable

To disable the router's DHCP Server, check **Disabled** and then click **Apply.** When the DHCP Server is disabled, you will need to manually assign a fixed IP address to each PC on your network, and set the default gateway for each PC to the IP address of the router (the default is 192.168.1.254).

DHCP Server Mode: DHCP Server

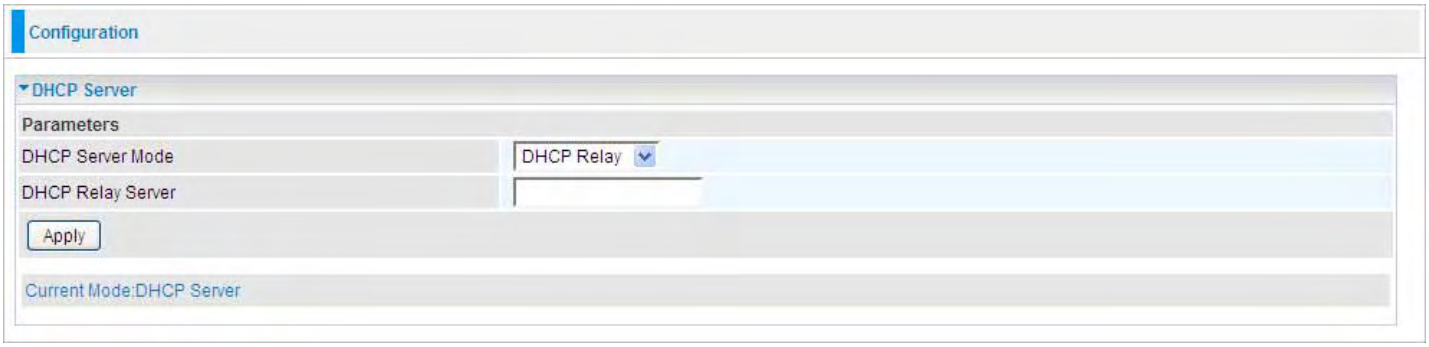
To configure the router's DHCP Server, check **DHCP Server**. You can then configure parameters of the DHCP Server including the IP pool (starting IP address and ending IP address to be allocated to PCs on your network), lease time for each assigned IP address (the period of time the IP address assigned 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. Click **Apply** to enable this function. If you check "**Use Router as a DNS Server**", the 3G Router performs the domain name lookup, finds the IP address from the outside network automatically and forwards it back to the requesting PC in the LAN (your Local Area Network).



DHCP Server Mode: DHCP Relay

If you check **DHCP Relay** and then you must enter the IP address of the DHCP server which assigns an IP address back 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 an outside connection to another network or the Internet. There are two items within the **WAN** section: **WAN interface** and **WAN Profile.**

WAN Interface (EWAN)

Connect Mode: Select the main port from the drop-down menu.

Click Apply to confirm the change.

WAN Interface (3G)

Connect Mode: Select the main port from the drop-down menu.

Click Apply to confirm the change.

WAN Interface (Dual WAN)

Connect Mode: Select the Dual WAN from the drop-down menu.

Main WAN: Choose EWAN or 3G as main WAN. Click the link to go to WAN Profile page to configure its parameters. Click the link beside it to configure the Main WAN connection. Turn to WAN profile in the following part for help.

Backup WAN: Choose the left as backup WAN. Click the link to go to WAN Profile page to configure its parameters. Click the link beside it to configure the backup WAN.

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.

Note: The time values entered in Failover Probe Cycle field is 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).

Faiback Probe Cycle: Set the time for the Faiback Probe Cycle.

Detect Rule (either one):

• **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.

This connection mode supports failover feature so that you can keep your WAN connection always on. You should first configure the main and backup WAN connection profile.

WAN Profile

Main Port – EWAN

Mobile Broadband Wireless-N Router offers a WAN port to connect to Cable Modems and fiber optic lines. This alternative, yet faster method to connect to the internet will provide users with more flexibility to get online.

Obtain an IP Address Automatically (EWAN)

When connecting to the ISP, **Mobile Broadband Wireless-N Router** also functions as a DHCP client. The router can automatically obtain an IP address, Netmask, gateway address, and DNS server addresses if the ISP assigns this information via DHCP.

Line Speed: Set the downstream and upstream of your connection in kilobytes per second. The connection speed is used by QoS settings.

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

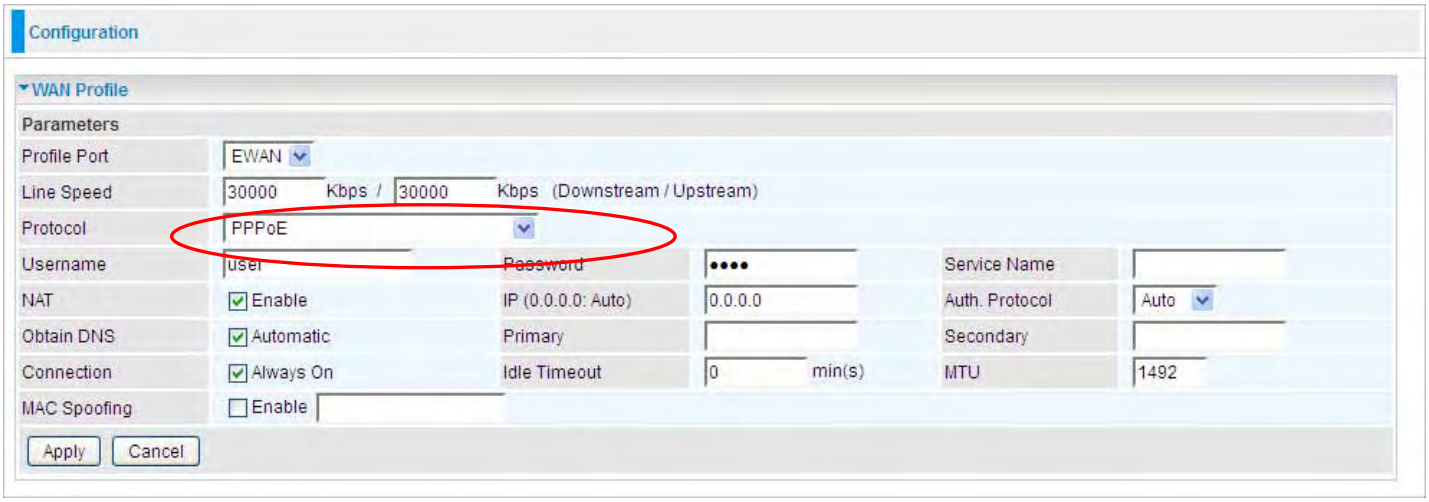
Obtain DNS Automatically: Select this check box to use DNS.

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.

MAC Spoofing: Select Enable and enter a MAC address that will temporarily change your router's MAC address to the one you have specified in this field. Leave it as Disabled if you do not wish to change the MAC address of your router.

PPPoE (EWAN)

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



Username: Enter the username provided by your ISP. You can input up to **128** alphanumeric characters (case sensitive). This is in the format of "username@ispname" instead of simply "username".

Password: Enter the password provided by your ISP. You can input up to **128** alphanumeric characters (case sensitive)

Service Name: This item is for identification purposes. If it is required, your ISP provides you the information. Maximum input is **15** alphanumeric characters.

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

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

Auth. Protocol: Default is **Auto.** Your ISP advises on using **Chap** or **Pap.**

Obtain DNS Automatically: Select this check box to use 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:

⊙ **Always on:** If you want the router to establish a PPPoE session when starting up and to automatically re-establish the PPPoE session when disconnected by the ISP.

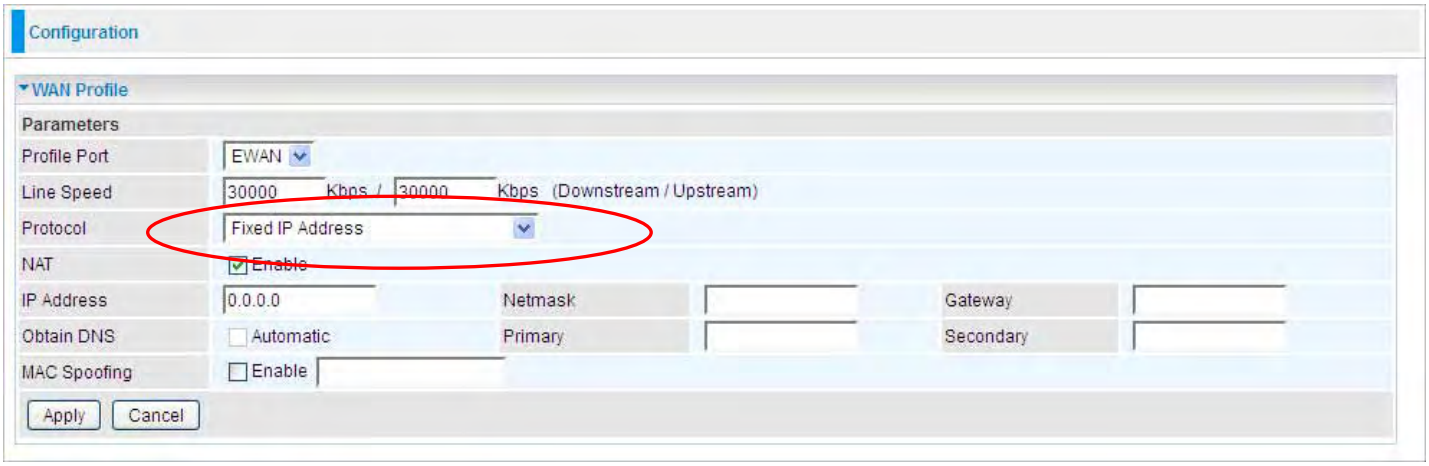
⊙ **Connect to Demand (un-select Always On):** If you want to establish a PPPoE session only when there is a packet requesting access to the Internet (i.e. when a program on your computer attempts to access the Internet). In this mode, you must set Idle Timeout value at same time.

Idle Timeout: Auto-disconnect the broadband firewall gateway when there is no activity on the line for a predetermined period of time. The minimum value is 10 minutes.

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

Fixed IP Address (EWAN)

Select this option to set static IP information. You will need to enter in the Connection type, IP address, netmask, and gateway address, provided to you by your ISP. Each IP address entered in the fields must be in the appropriate IP form, which is four IP octets separated by a dot (x.x.x.x). The Router will not accept the IP address if it is not in this format.



Line Speed: Set the downstream and upstream of your connection in kilobytes per second. The connection speed is used by QoS settings.

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

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

IP Netmask: The default is 0.0.0.0. User can change it to other such as 255.255.255.0.Type the netmask assigned to you by your ISP (if given).

Gateway: You must specify a gateway IP address (supplied by your ISP)

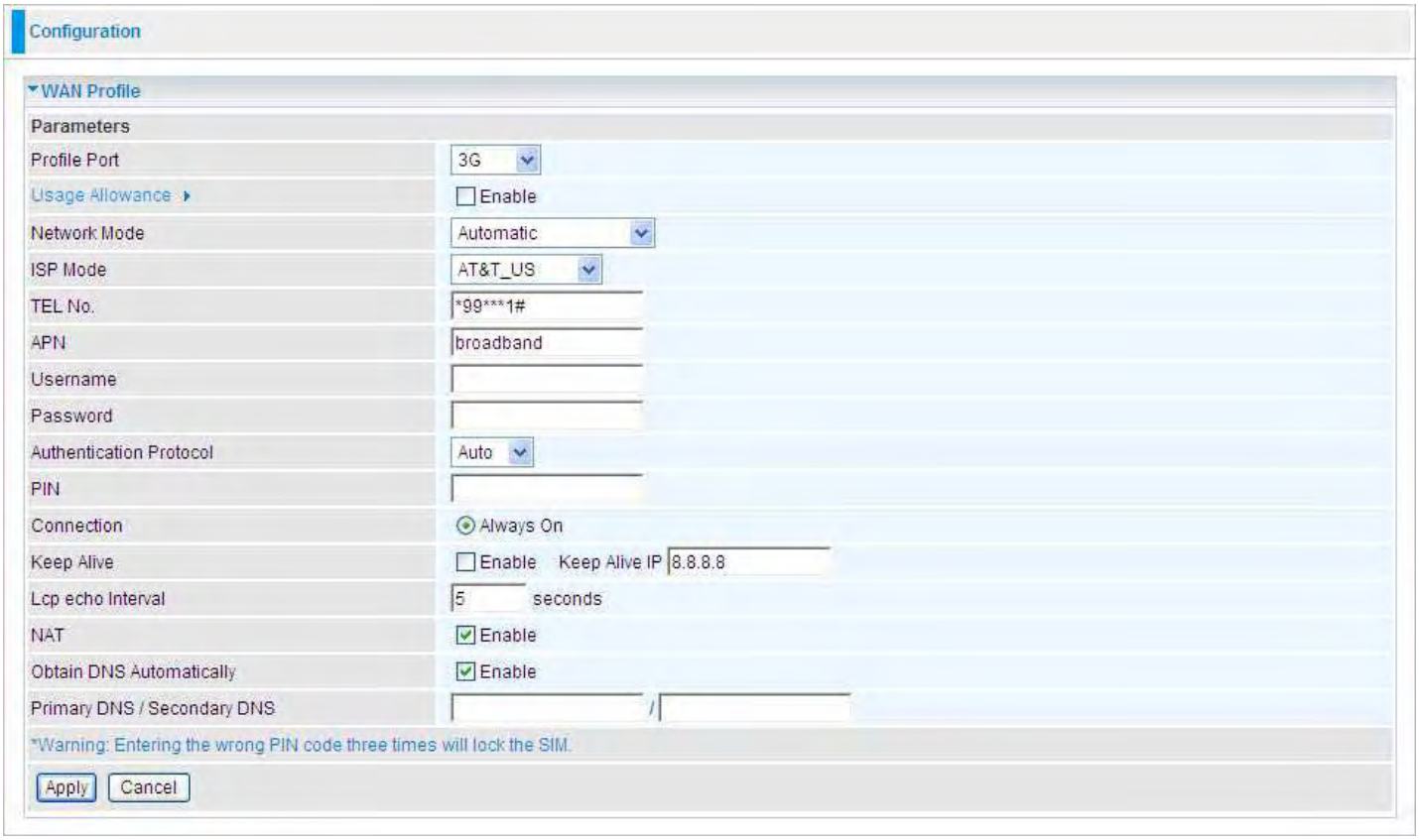
Obtain DNS Automatically: Select this check box to use DNS.

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.

MAC Spoofing: Select Enable and enter a MAC address that will temporarily change your router's MAC address to the one you have specified in this field. Leave it as Disabled if you do not wish to change the MAC address of your router.

Main Port - 3G

The router allows you to insert a 3G/4G-LTE S I M card into to the built-in SIM slot, enabling you to use a, UMTS, GSM, or LTE Internet connection, makes downstream rates of to 14.4 Mbps*.



Usage Allowance: enable when you want to control 3G usage. Click this link to enter **3G Usage Allowance** to configure.

ISP Mode: Choose 3G / 4G-LTE service provider.

TEL No.: The dial string to make a GPRS / 3G user internetworking call. It may be provided by your mobile service provider.

APN: An APN is similar to a URL on the WWW, it is what the unit makes a GPRS / UMTS call. The service provider is able to attach anything to an APN to create a data connection. Requirements for APN assignment varies between different service providers. Most service providers have an internet portal which they connect a DHCP Server to, giving you access to the internet i.e. Some 3G / 4G-LTE operators use the APN 'internet' for their portal. The default value of APN is "internet".

Username: Enter the username provided by your service provider.

Password: Enter the password provided by your service provider.

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

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

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

Note: If you enter an incorrect PIN code three times in a row, your SIM card will be blocked. In this case, please enter your PUK code (it can be supplied by your service provider) and then re-enter your PIN.

Connection:

- **Always On:** The router will make UMTS/GPRS call when starting up. Enabling Always On, will give you an option of Keep Alive.

Keep Alive: Click to enable keep alive mechanism. User should set the Keep Alive IP to necessiate the always on connection. The IP is used for ping operation to examine whether the connection is still on.

Idle Timeout: Auto-disconnect the connection when there is no activity on this call for a predetermined period of time. The default value is 600 seconds.

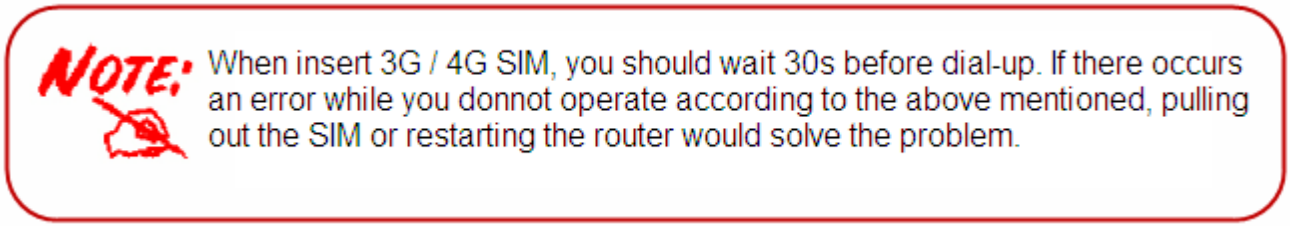
Lcp echo Interval: Set the interval time(seconds), if set to 5, that means the router is allowed to send message out every 5sec to prevent the connection being dropped by ISP.

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

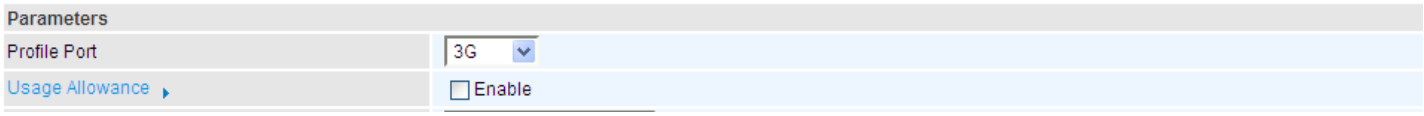
Obtain DNS Automatically: Select this checkbox to use DNS.

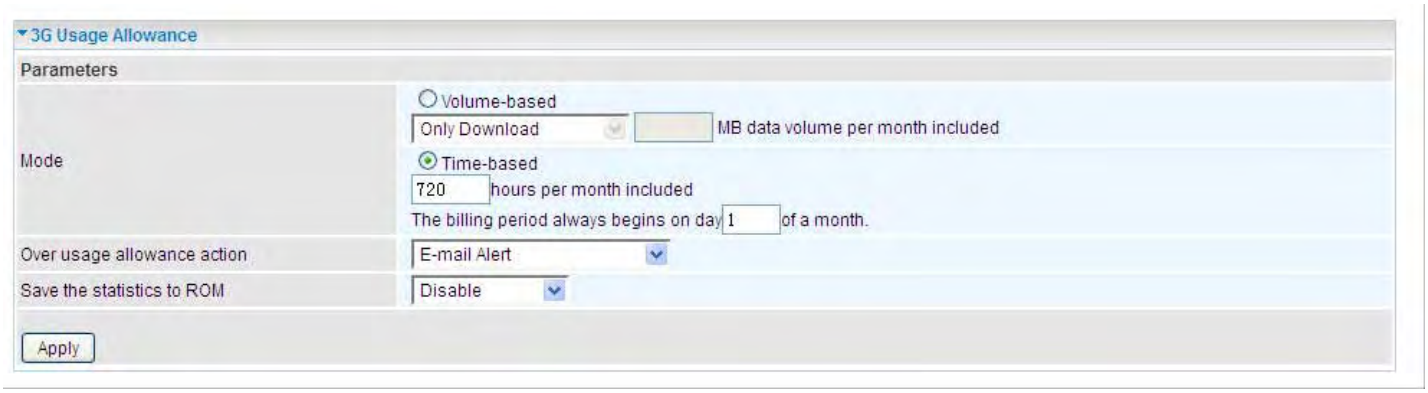
Primary DNS/ Secondary DNS: Enter the IP addresses of the DNS servers. The DNS servers are passed to the DHCP clients along with the IP address and the subnet mask.

Note: If you don't know how to set these values and please keep them untouched.

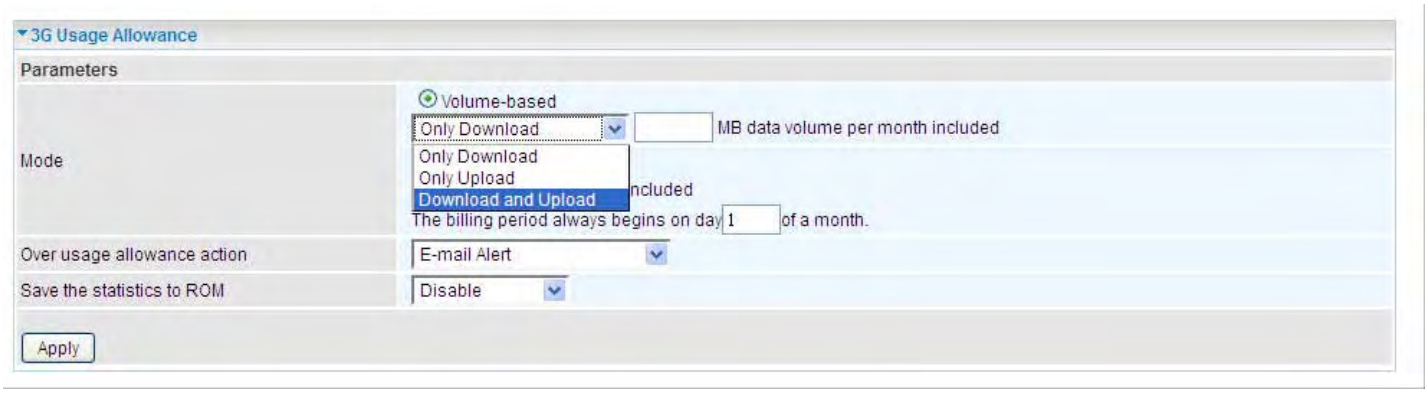


Click **Usage Allowance** to go to the Usage Allowance configuration page.



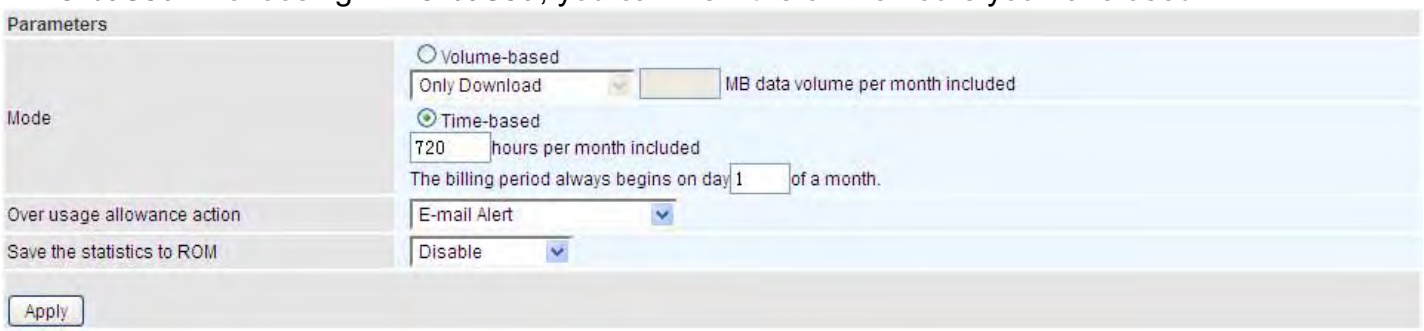


In order to query online time or volume used, you can set the following options.
Mode: Two methods are provided, that is, **Volume-based** and **Time-based**.
Volume-based: If choosing **Volume-based**, you can view the volume you have used.



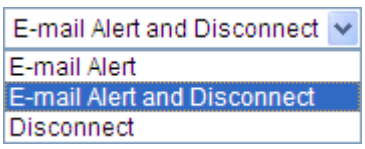
Only Download: Only make statistics of Download Traffic.
Only Upload: Only make statistics of Upload Traffic.
Download and Upload: Make statistics of both Download and Upload Traffic.

Time-based: If choosing **Time-based**, you can view the online hours you have used.



You can also assign the billing period.

Over usage allowance action: If the online time or traffic you have used exceeds the usage allowance you set. The system will do the followings operations.

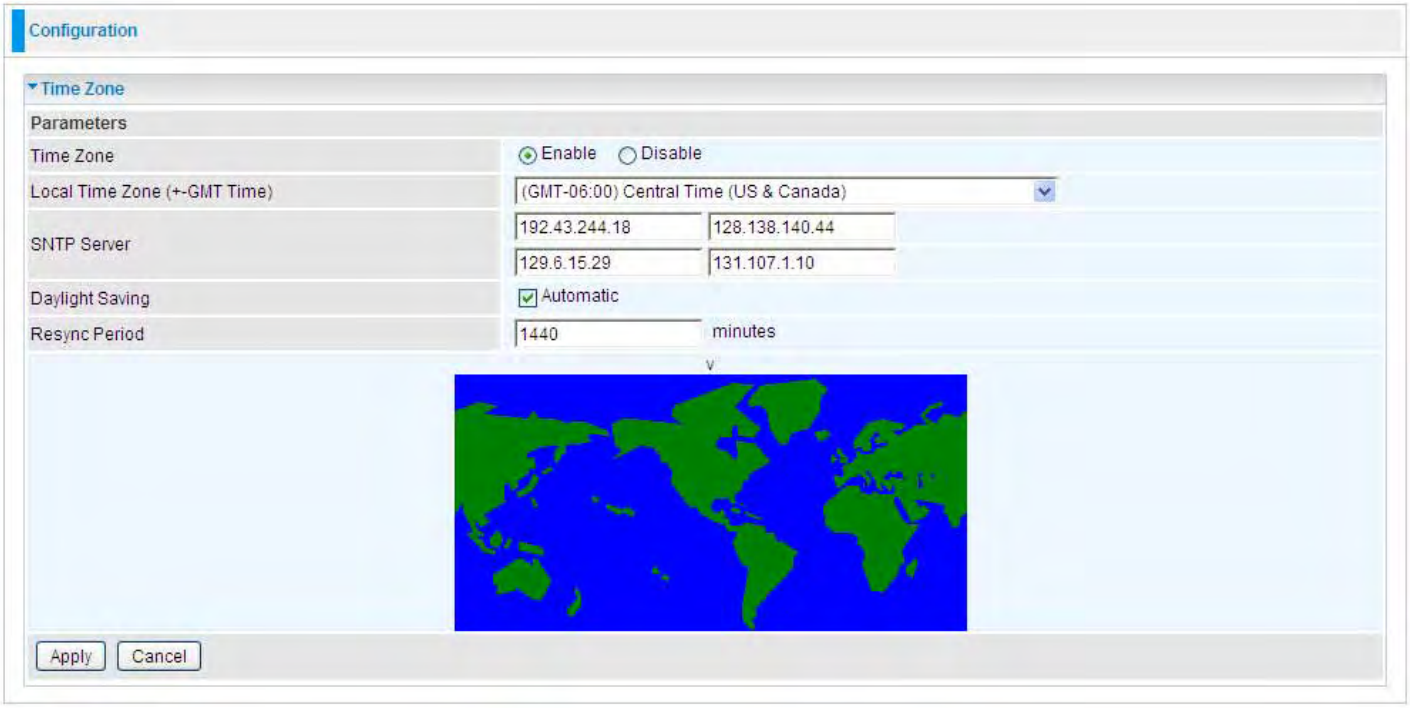


Save the statistics to ROM: Choose the time interval for saving statistics. You can choose to save for **Every one hour** or **Disable** the function**.**

System

There are five items within the **System** section: **Time Zone, Firmware Upgrade, Backup/Restore, Restart**, **User Management** and **Mail Alert.**

Time Zone



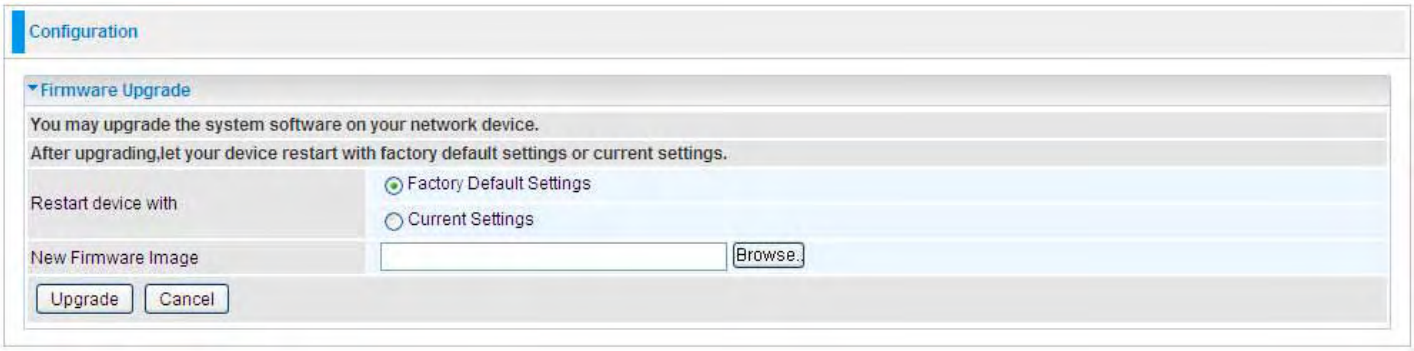
The router does not have a real time clock on board; instead, it uses the Simple Network Time Protocol (SNTP) to get the current time from an SNTP server outside your network. Choose your local time zone, click **Enable** and click the **Apply** button. After a successful connection to the Internet, the router retrieves 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 as shown above. Your ISP may provide an SNTP server for you to use.

Resync Period (in minutes) is the periodic interval the router waits before it resynchronizes the router's time with that of the specified SNTP server. 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.

Firmware Upgrade

Your router's "firmware" is the software that allows it to operate and provides all its functionality. Think of your router as a dedicated computer, and the firmware as the software it runs. Over time this software may be improved and modified. Your router allows you to upgrade the software it runs to take advantage of these changes.

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



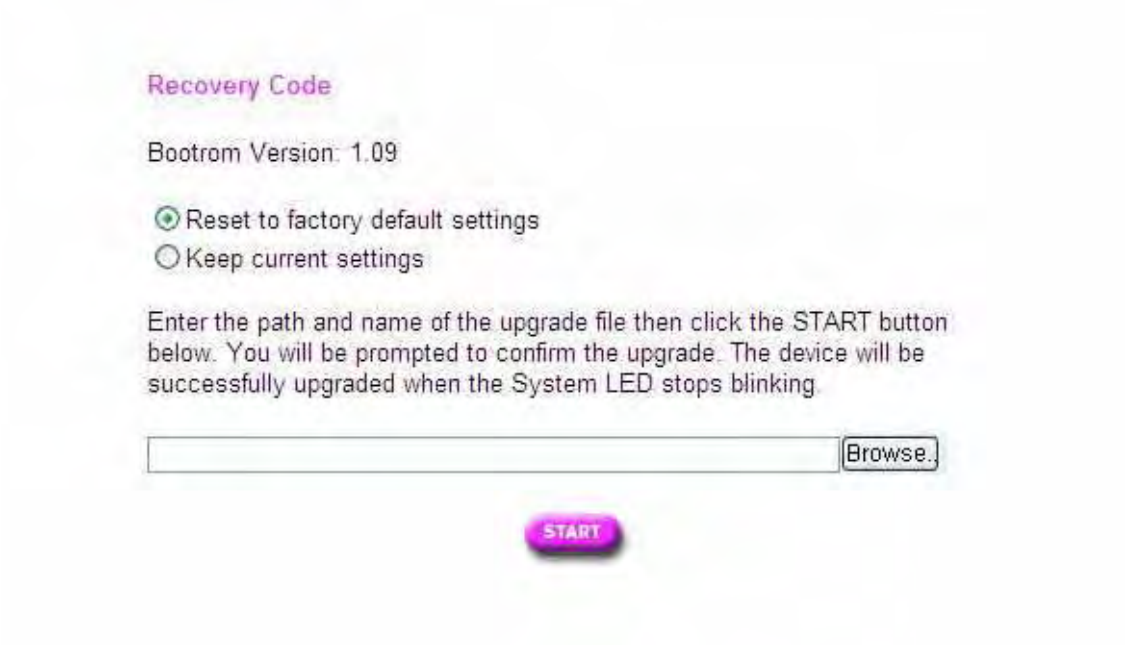
Restart Device with: To choose "Factory Default Settings" or "Current Settings" which uses your current setting on the new firmware (it is highly advised to use Factory Default Settings over Current Settings for a clean firmware upgrade).
New Firmware Image: Type in the location of the file you wish to upload in this field or click **Browse…** to locate it.
Browse…: Click **Browse…** to find the file with the **.afw** file extension that you wish to upload. Remember that you must decompress compressed (.zip) files before you can upgrade from the file.
Upgrade: Click **upgrade** to begin the upload process. This process may take up to three minutes.

Warning

Do not power down the router or interrupt the firmware upgrade while it is still in process. Improper operation may damage the router. If firmware upgrade failure occurs, please refer to operations below for emergency recovery.

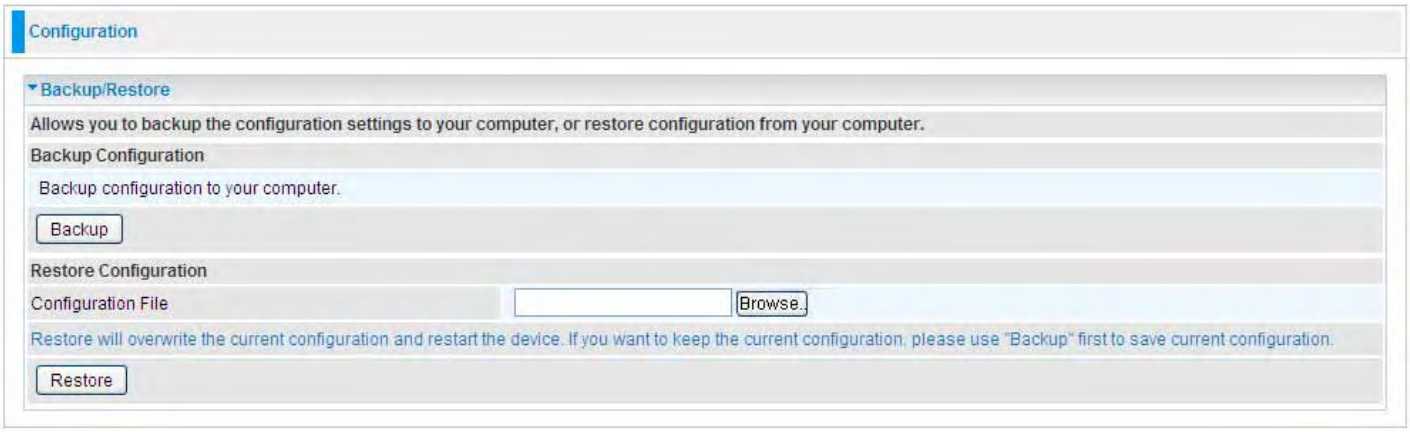
Recovery procedure:

If your device's upgrade failed, then you can take emergency recovery procedure to recover. Usually, if the device failed to upgrade successfully, the recovery page will automatically (or you enter 192.168.1.254 at the address bar) turn to the page showed as below, entering the recovery mode.



Select the correct file used for upgrade, and press **START**.

Backup / Restore



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

Press **Backup** to select where on your local PC to save the settings file. You may also change the name of the file when saving if you wish to keep multiple backups.

Press **Browse…** to select a file from your PC to restore. You should only restore settings files that have been generated by the Backup function, and that were created when using the **current version** of the router's firmware. **Settings files saved to your PC should not be manually edited in any way.**

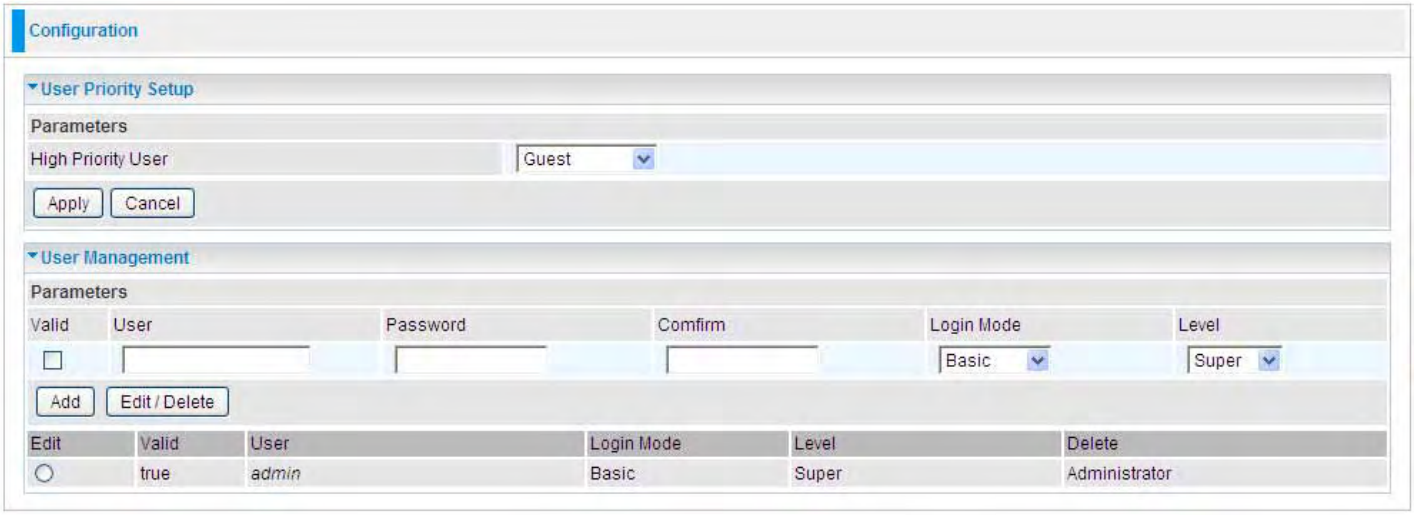
Select the settings files you wish to use, and press **Restore** to load those settings into the router.

Restart Router

Click **Restart** with option **Current Settings** to reboot your router and save the current configuration to device.

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.

User Management

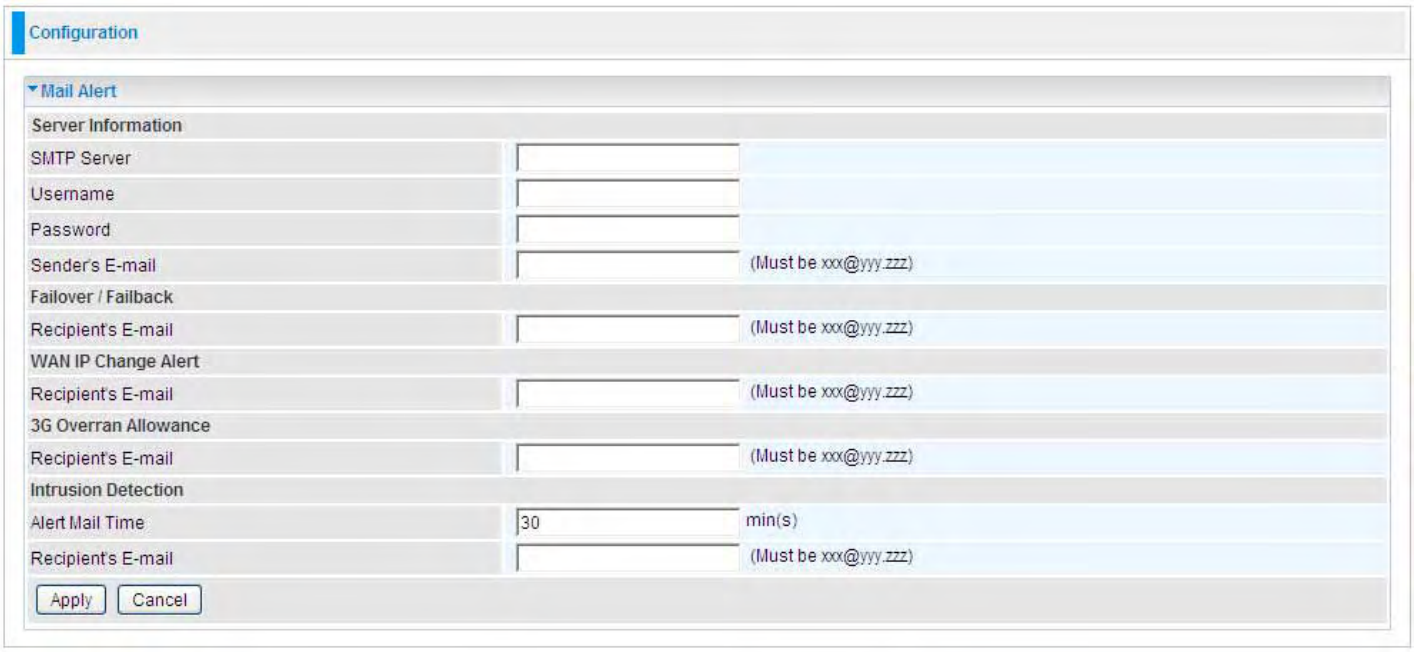


In order to prevent unauthorized access to your router's configuration interface, it requires all users to login with a password. You can set up multiple user accounts, each with their own password.

You are able to **Edit** existing users and **Add** new users who are able to access the device's configuration interface. Once you have clicked **Edit** on the account you want to edit**,** the information of the account will be displayed above. Just go ahead and change the password.
You can change the user's **password**, whether their account is active and **Valid**. These options are the same when creating a user account, with the exception that once created you cannot change the username. You cannot delete the default admin account; however you can delete any other created accounts by clicking ticking the box under **Delete** and then press the **Edit/Delete** button.
You are strongly advised to change the password on the default "**admin**" account when you receive your router, and any time you reset your configuration to Factory Defaults.

Mail Alert

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



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

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

Password: Enter the password of your email account.

Sender's Email: Enter your email address.

Recipient's Email (Failover / Failback): Enter the email address that will receive the alert message once a computer / network server failover occurs.

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

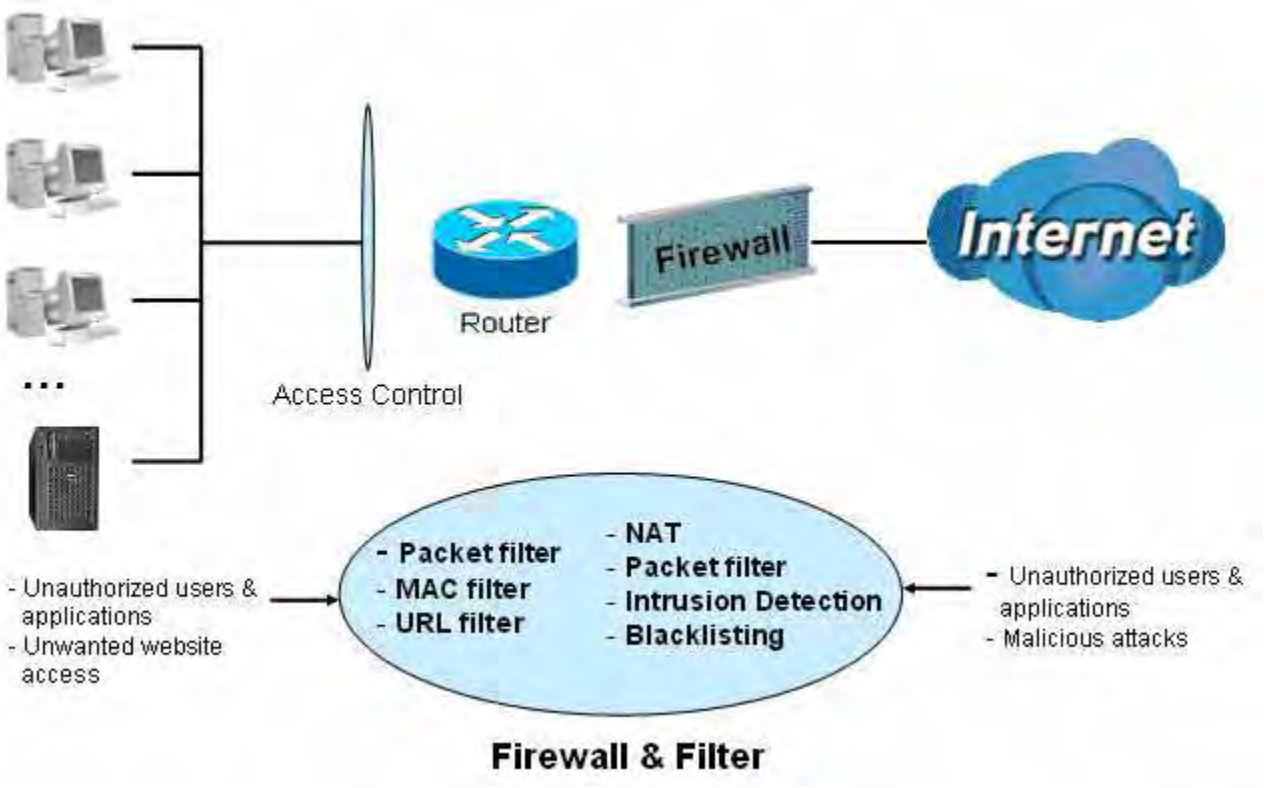
Recipient's Email (3G Overran Allowance): Enter the email address that will receive the alert message once 3G overran allowance was detected.

Alert Mail Time (Intrusion Detection): The time interval of sending Email.

Recipient's Email (Intrusion Detection): Enter the email address that will receive the alert message once intrusion has been detected.

Firewall and Access Control

Your router includes a full SPI (Stateful Packet Inspection) firewall for controlling Internet access from your LAN, as well as helping to prevent attacks from hackers. In addition to this, when using NAT (Network Address Translation) the router acts as a “natural” Internet firewall, since all PCs on your LAN use private IP addresses that cannot be directly accessed from the Internet. See the **WAN** configuration section for more details on NAT.



Firewall: Prevents access from outside your network.

NAT natural firewall: This masks LAN users’ IP addresses, which are invisible to outside users on the Internet, making it much more difficult for a hacker to target a machine on your network. This natural firewall is on when the NAT function is enabled.

When using Virtual Servers (port mapping) your PCs are exposed to the ports specified opened in your firewall packet filter settings.

Firewall Security and Policy (General Settings): Inbound direction of Packet Filter rules prevent unauthorized computers or applications accessing your local network from the Internet.

Intrusion Detection: Enable Intrusion Detection to detect, prevent, and log malicious attacks.

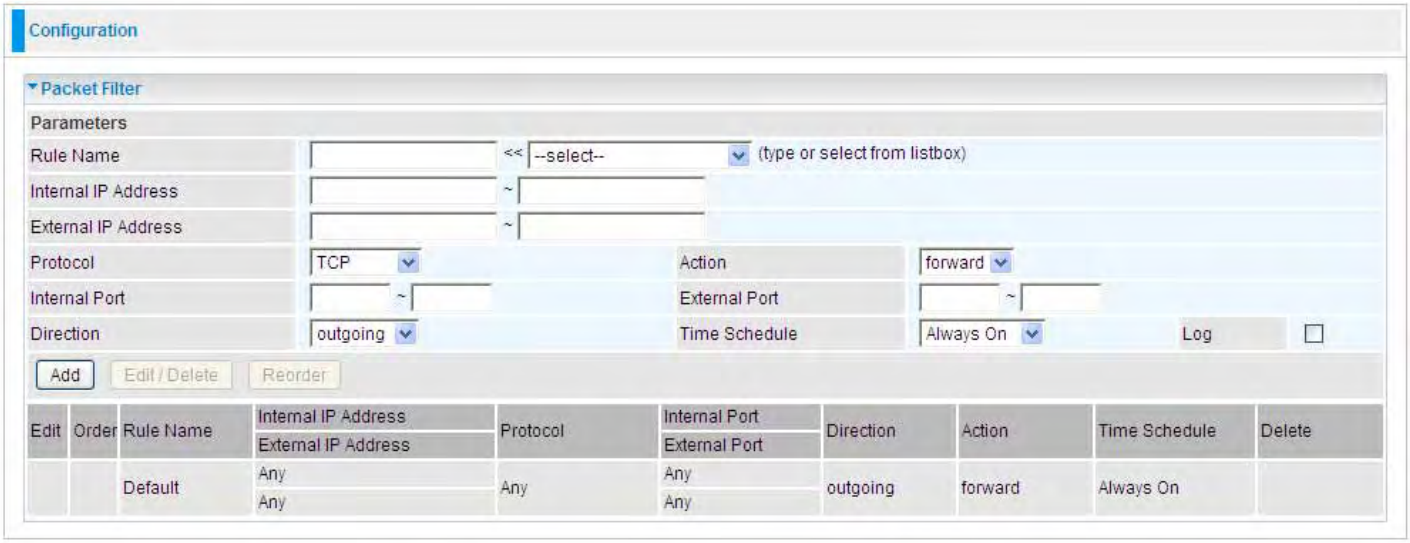
MAC Filter rules: Prevents unauthorized computers accessing the Internet.

URL Filter: Blocks PCs on your local network from unwanted websites.

A detailed explanation of each of the following five items appears in the **Firewall** section below: **Packet Filter**, **MAC Address Filter, Intrusion detection, Block WAN PING** and **URL Filter.**

Packet Filter

Packet filtering enables you to configure your router to block specified internal/external users (**IP address**) from Internet access, or you can disable specific service requests (**Port number**) to /from Internet. This configuration program allows you to set up to 6 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: Users-define description to identify this entry. The maximum name length is 32 characters, and then can choose application that they want from list box.

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

Protocol: Specify the packet type (TCP, UDP, ICMP, etc.) 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.

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 **0 ~ 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: It is self-defined time period. You may specify a time schedule for your prioritization policy. For setup and detail, refer to **Time Schedule** section.

Log: Choose “log” if you wish to generate logs when the filer rule is applied to a packet.

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”.

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	forward	Always On	☐
○	↑	TELNET	Any Any	TCP	Any 23~23	outgoing	forward	Always On	☐
		Default	Any Any	Any	Any Any	outgoing	forward	Always On	

Attention

If the DHCP server option is enabled, you must be very careful in assigning IP addresses of a filtered private IP range to avoid conflicts because you do not know which PC in the LAN is assigned which IP address. The easiest and safest way is that the filtered IP address is assigned to a specific PC that is not allowed to access an outside resource such as the Internet. You configure the filtered IP address manually for this PC, but it stays in the same subnet with the router.

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 to block specific machines from accessing your LAN.

There are no pre-defined MAC address filter rules; you can add the filter rules to meet your requirements.

Action： select to determine how to do with the filter.

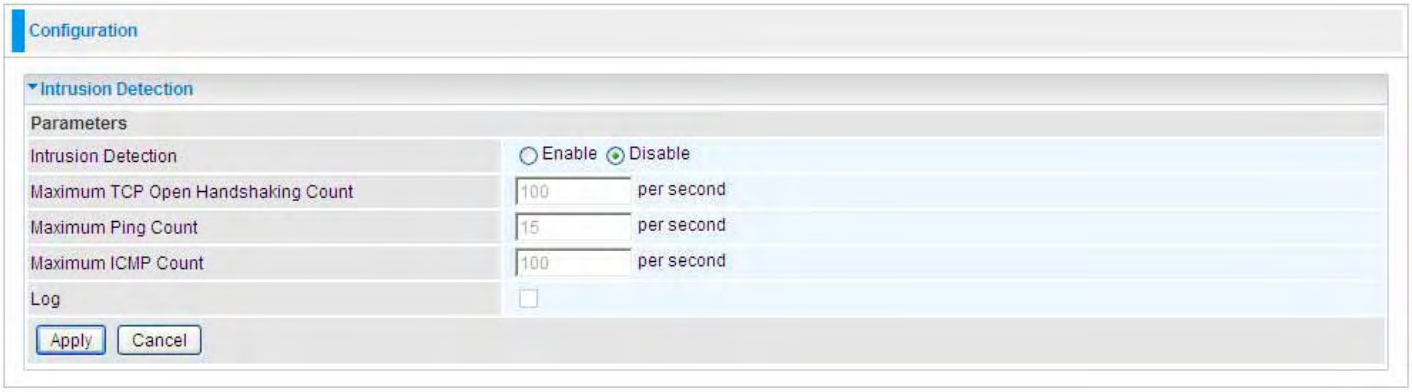
- **Disable:** to disable the MAC filter function.
- **Allow:** to enable the MAC filter function and allow the host of the following set MAC addresses to access.
- **Block:** to enable the MAC filter function and block the host of the following set MAC addresses to access.

MAC Address: Enter the MAC addresses you wish to manage.

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

Intrusion Detection

Check Enable if you wish to detect intruders accessing your computer without permission. The router automatically detects and blocks a DoS (Denial of Service) attack if a user enables this function. This kind of attack is not to access confidential data on the network; instead, it aims to disrupt specific equipment or the entire network. If this happens, users will have trouble accessing the network resources.



Intrusion Detection: Check Enable if you wish to detect intruders accessing your computer without permission.

Maximum 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.

Maximum 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.

Maximum 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: Check Log if you wish to generate logs when the filer rule is applied to the Intrusion Detection.

For SYN Flood, ICMP Echo Storm and ICMP flood, IDS will just warn the user in the Event Log but it will not be able to protect against such attacks.

Hacker attack types recognized by the IDS

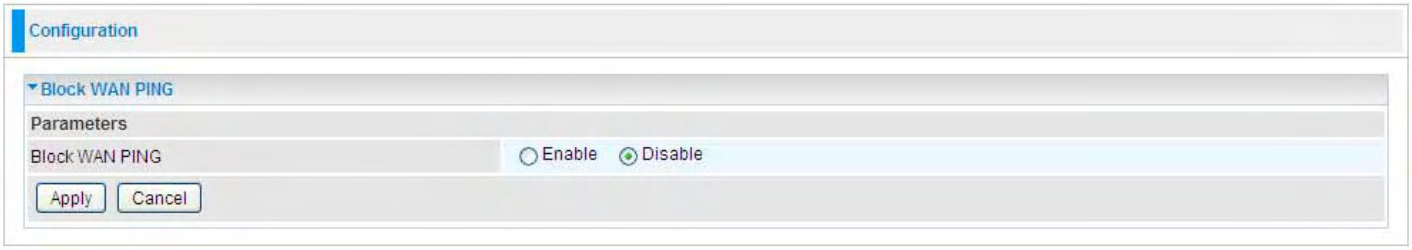
Intrusion Name	Detect Parameter	Blacklist	Type of Block Duration	Drop Packet	Show Log
Ascend Kill	Ascend Kill data	Src IP	DoS	Yes	Yes

WinNuke	TCP Port 135, 137~139, Flag: URG	Src IP	DoS	Yes	Yes
Smurf	ICMP type 8 Des IP is broadcast	Dst IP	Victim Protection	Yes	Yes
Land attack	SrcIP = DstIP			Yes	Yes
Echo/CharGen Scan	UDP Echo Port and CharGen Port			Yes	Yes
Echo Scan	UDP Dst Port = Echo(7)	Src IP	Scan	Yes	Yes
CharGen Scan	UDP Dst Port = CharGen(19)	Src IP	Scan	Yes	Yes
X'mas Tree Scan	TCP Flag: X'mas	Src IP	Scan	Yes	Yes
IMAP SYN/FIN Scan	TCP Flag: SYN/FIN DstPort: IMAP(143) SrcPort: 0 or 65535	Src IP	Scan	Yes	Yes
SYN/FIN/RST/ACK Scan	TCP, No Existing session And Scan Hosts more than five.	Src IP	Scan	Yes	Yes
Net Bus Scan	TCP No Existing session DstPort = Net Bus 12345,12346, 3456	SrcIP	Scan	Yes	Yes
Back Orifice Scan	UDP, DstPort = Orifice Port (31337)	SrcIP	Scan	Yes	Yes
SYN Flood	Max TCP Open Handshaking Count (Default 100 c/sec)				Yes
ICMP Flood	Max ICMP Count (Default 100 c/sec)				Yes
ICMP Echo	Max PING Count (Default 15 c/sec)				Yes

Src IP: Source IP **Src Port:** Source Port
Dst Port: Destination Port **Dst IP:** Destination IP

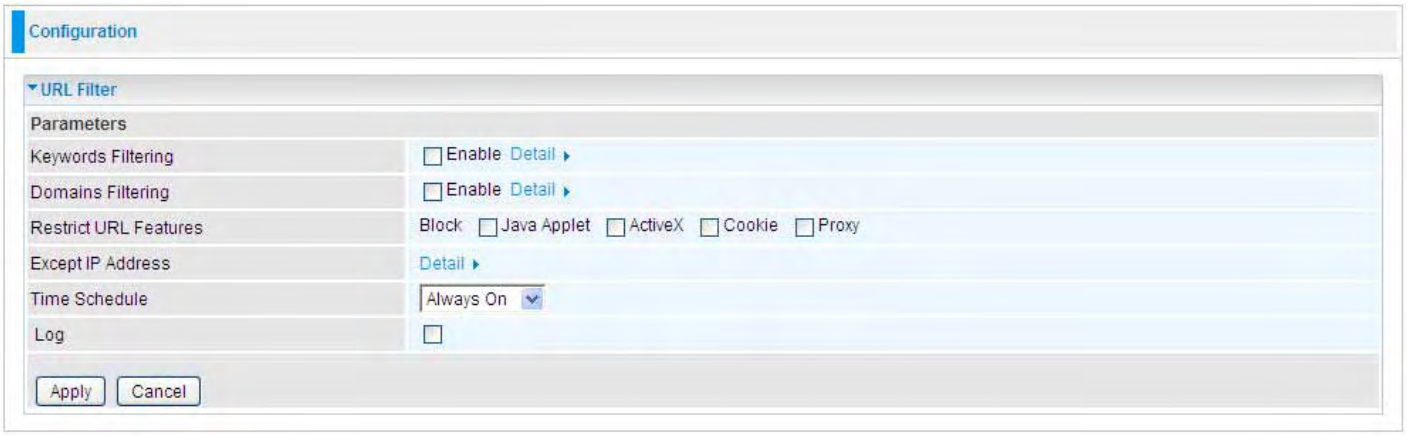
Block WAN PING

Check Enable if you wish to exclude outside PING requests from reaching this router.



URL Filter

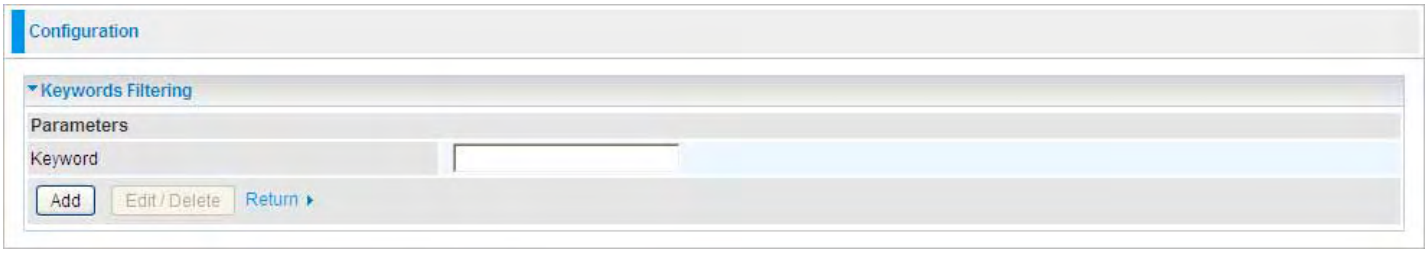
URL (Uniform Resource Locator – e.g. an address in the form of **http://www.example.com**) filter rules allow you to prevent users on your network from accessing particular websites from their URL. There are no pre-defined URL filter rules; you can add filter rules to meet your requirements.



Keywords Filtering

Allows blocking by 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 is checked to see if any keywords are present in URLs accessed to determine if the connection attempt should be blocked. Note that the URL filter blocks web browser (HTTP) connection attempts using port 80 only.

For example, the URL http://www.abc.com/abcde.html would be dropped since the keyword “abcde” occurs in the URL.

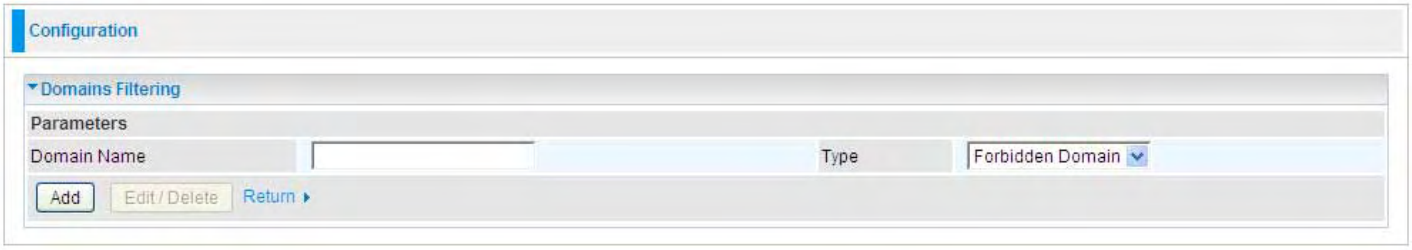


Domains Filtering

Checks the domain name in URLs accessed against your list of domains to block or allow. If it matches, the URL request is sent (Trusted) or dropped (Forbidden). The checking procedure is:

1. Check the domain in the URL to determine if it is in the trusted list. If yes, the connection attempt is sent to the remote web server.
2. If not, it is checked with the forbidden list. If present, the connection attempt is dropped.
3. If the packet matches neither of the above, it is sent to the remote web server.
4. Please be note that the completed URL, “www” + domain name shall be specified. For example

to block traffic to www.google.com.au, enter “www.google” or “www.google.com”



Restrict URL Features

This function enhances the restriction to your URL rules.

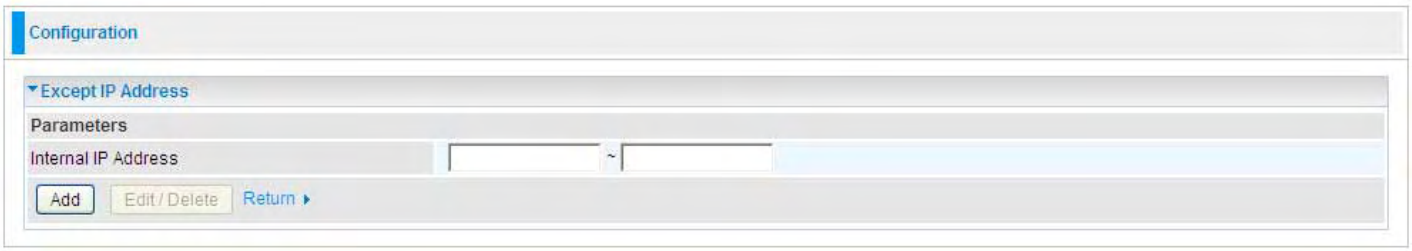
⊙ Block Java Applet: Blocks Web content which includes the Java Applet to prevent someone who wants to damage your system via the standard HTTP protocol.

⊙ **Block ActiveX:** Blocks ActiveX

⊙ **Block Cookies:** Blocks Cookies

⊙ **Block Proxy:** Blocks Proxy

Except IP Address



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

Log: Click “Log” if you wish to generate logs when the filer rule is applied to the URL Filter.

QoS (Quality of Service)

Quality of Service Introduction

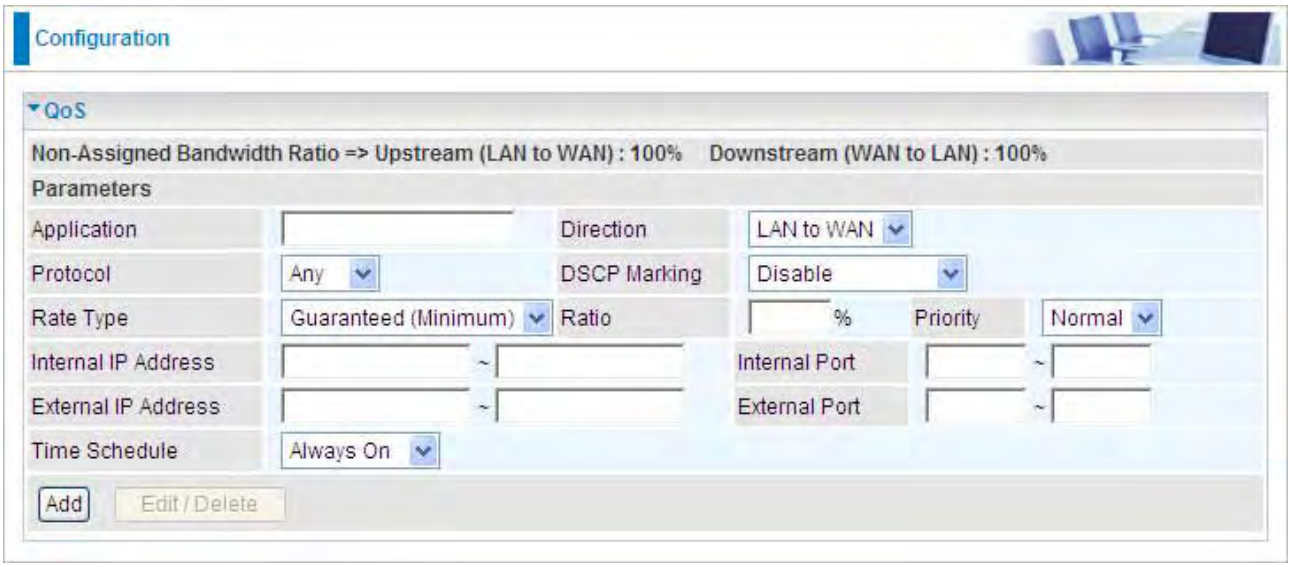
If you've ever found your 'net' speed has slowed to a crawl because another family member is using a P2P file sharing program, you'll understand why the Quality of Service features in the routers is such a breakthrough for home users and office users.

QoS: Keeping Your Net Connection Fast and Responsive

Configurable by internal IP address, external IP address, protocol, and port, the Quality of Service (QoS) gives you full control over which types of outgoing data traffic should be given priority by the router, ensuring bandwidth-consumption data like gaming packets, latency-sensitive application like voice, or even mission critical files, move through the router at lightning speed, even under heavy load. You can throttle the speed at which different types of outgoing data pass through the router. In addition, you can simply change the priority of different types of upload data and let the router sort out the actual speeds.

QoS Setup

Please choose the **QoS** in the **Configuration** item of the left window as depicted below.



After clicking the QoS item, you can Add/Edit/Delete a QoS policy. This page will show the brief information for policies you have added or edited. This page will also display the total available (Non-assigned) bandwidth, in percentage, can be assigned.

Application: A name that identifies an existing policy.

Direction: The traffic flow direction to be controlled by the QoS policy.

There are two settings to be provided in the Router:

⊙ **LAN to WAN:** You want to control the traffic flow from the local network to the outside world. e.g., you have a FTP server inside the local network and you want to have a limited traffic rate controlled by the QoS policy. So, you need to add a policy with LAN to WAN direction setting.

⊙ **WAN to LAN**: Control Traffic flow from the WAN to LAN. The connection maybe either issued

from LAN to WAN or WAN to LAN.)

Protocol: The Protocol will be controlled. For GRE protocol, there is no need to specify the IP addresses or Application ports in this page. For other protocols, at least one value shall be given.

⊙ **ANY:** No protocol type is specified.

⊙ **TCP**

⊙ **UDP**

⊙ **ICMP**

⊙ **GRE**

DSCP Marking: Differentiated Services Code Point (DSCP), it is the first 6 bits in the ToS byte. DSCP Marking allows users to classify traffic based on DSCP value and send packets to next Router.

Note: To be sure the router(s) in the backbones network have the capability in executing and checking the DSCP through-out the QoS network.

The DSCP Mapping Table

DSCP Mapping Table	
3G / 4G-LTE Router	**Standard DSCP**
Disabled	None
Best Effort	Best Effort (000000)
Premium	Express Forwarding (101110)
Gold service (L)	Class 1, Gold (001010)
Gold service (M)	Class 1, Silver (001100)
Gold service (H)	Class 1, Bronze (001110)
Silver service (L)	Class 2, Gold (010010)
Silver service (M)	Class 2, Silver (010100)
Silver service (H)	Class 2, Bronze (010110)
Bronze service (L)	Class 3, Gold (011010)
Bronze service (M)	Class 3, Silver (011100)
Bronze service (H)	Class 3, Bronze (011110)

Rate Type: 2 types are provided:

⊙ **Limited (Maximum):** Specify a limited data rate for this policy. It also is the maximal rate for this policy. 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.

⊙ **Guaranteed (Minimum):** Specify a minimal data rate for this policy. For example, you want to provide a guaranteed data rate for your outside customers to access your internal FTP server with, say at least, 20% of your total bandwidth. You can use this type. Then, if there is available bandwidth that is not used, it will be given to this policy by following priority assignment.

Ratio: Assign the data ratio for this policy to be controlled. For examples, we want to only allow 20% of the total data transfer rate for the LAN-to-WAN direction to be used for FTP server. Then we can specify here with data ratio = 20.

Priority: Specify the priority for the bandwidth that is not used. For examples, you may specify two different QoS policies for different applications. Both applications need a minimal bandwidth and need more bandwidth, beside the assigned one, if there is any available/non-used one available. So, you may specify which application can have higher priority to acquire the non-used bandwidth.

- ⊙ **High**
- ⊙ **Normal**: The default is normal priority.
- ⊙ **Low**

For the sample priority assignment for different policies, it is served in a First-In-First-Out way.

Internal IP Address: The IP address values for Local LAN machines you want to control. (For IP packets from LAN to WAN, it is the source IP address. For IP packages from WAN to LAN, it is the destination IP address.)

Internal Port: The Application port values for local LAN machines you want to control. (For TCP/UDP packets from LAN to WAN, it is the source port value. For TCP/UDP packets from WAN to LAN, it is the destination port value.)

External IP Address: The IP address values for Remote WAN machines you want to control. (For IP packets from LAN to WAN, it is the destination IP address. For IP packages from WAN to LAN, it is the source IP address.)

External Ports: The Application port values for remote machines you want to control. (For TCP/UDP packets from LAN to WAN, it is the destination port value. For TCP/UDP packets from WAN to LAN, it is the source port value.)

Time Schedule: Scheduling your prioritization policy.

Example: QoS for your Network

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 and bandwidth ratio for the different applications that members of your network will be using to avoid bandwidth traffic from getting overloaded.

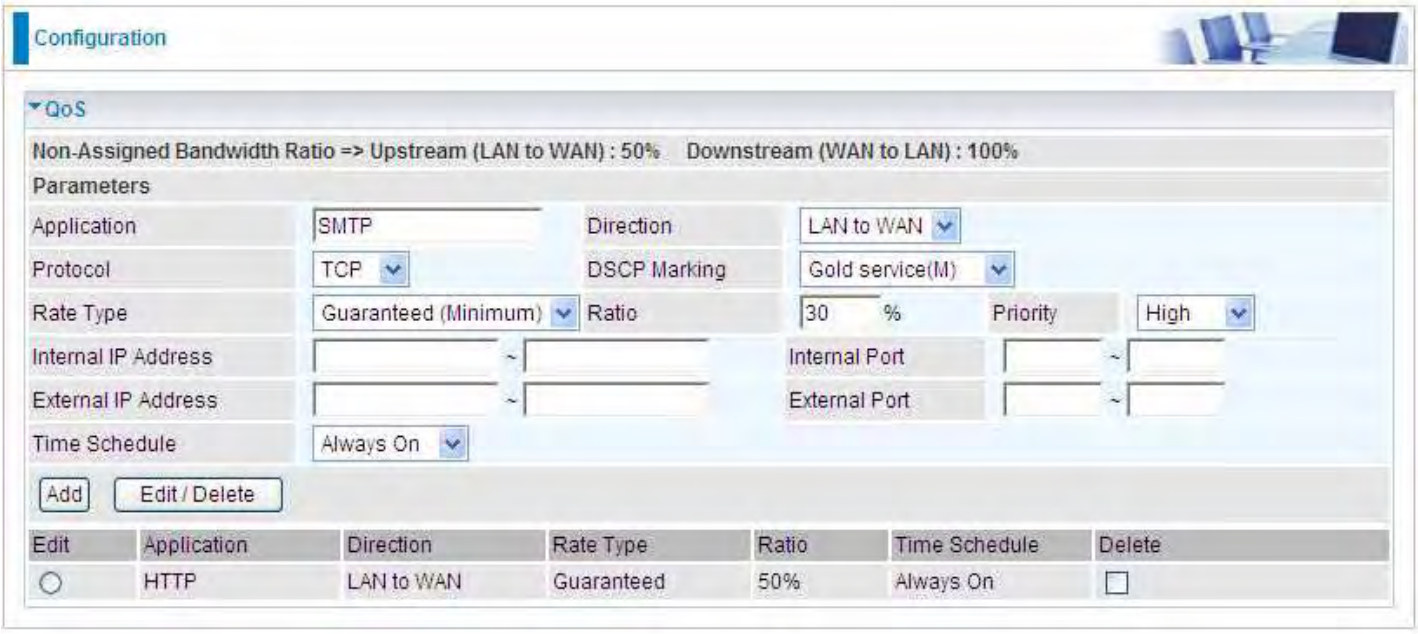
The figures below are a simple example to show the different settings for Web Browsing and Email sending to assure the bandwidth for these applications.

For Web Browsing

Here we guarantee 50% of the traffic for Http application.

For Mail Sending

Here we guarantee 30% of the traffic for Mail application.



Edit	Application	Direction	Rate Type	Ratio	Time Schedule	Delete
○	HTTP	LAN to WAN	Guaranteed	50%	Always On	☐
○	SMTP	LAN to WAN	Guaranteed	30%	Always On	☐

thus, 20% of LAN to WAN (upsteam) traffic is reserved for other uses and those applications' bandwidths are guaranteed.

For downstream traffic bandwidth, just the direction changes and the configuration is similar.

That's just a simple example for QoS application, for more please refer to FAE.

Virtual Server

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.

The reason is that when using NAT, your publicly accessible IP address is used by and points to your router, which needs to deliver all traffic to the private IP addresses used by your PCs. Please see the **WAN** configuration section of this manual for information on NAT.

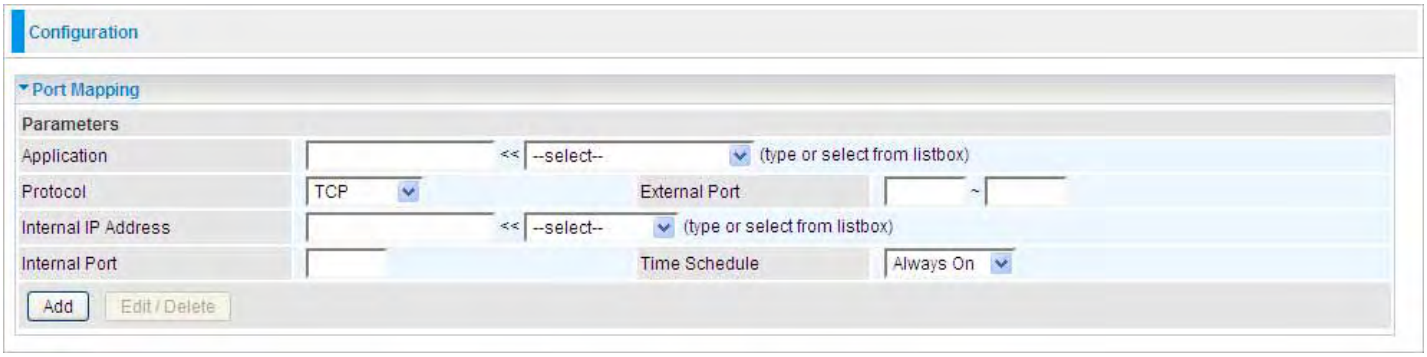
The Internet Assigned Numbers Authority (IANA) is the central coordinator for the assignment of unique parameter values for Internet protocols. Port numbers range from 0 to 65535, but only port numbers 0 to 1023 are reserved for privileged services and are designated as “well-known ports”. The registered ports are numbered from 1024 through 49151. The remaining ports, referred to as dynamic ports, or private ports, are numbered from 49152 through 65535.

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	RealAudio

Port Mapping



Application: Select the service you wish to configure.

Protocol: Automatic when you choose Application from list-box or select a protocol type which you want.

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.

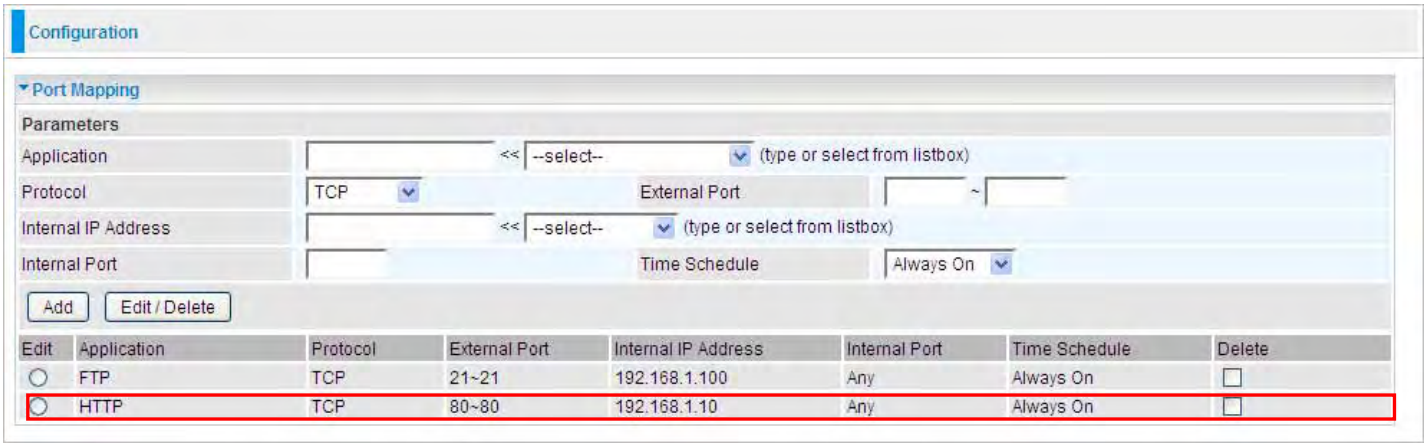
Add: Click to add a new virtual server rule. Click again and the next figure appears.

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

Delete: Check the Rule No. you wish to delete then click “Edit/Delete”.

Since NAT acts as a “natural” Internet firewall, your router protects your network from access 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 to 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.

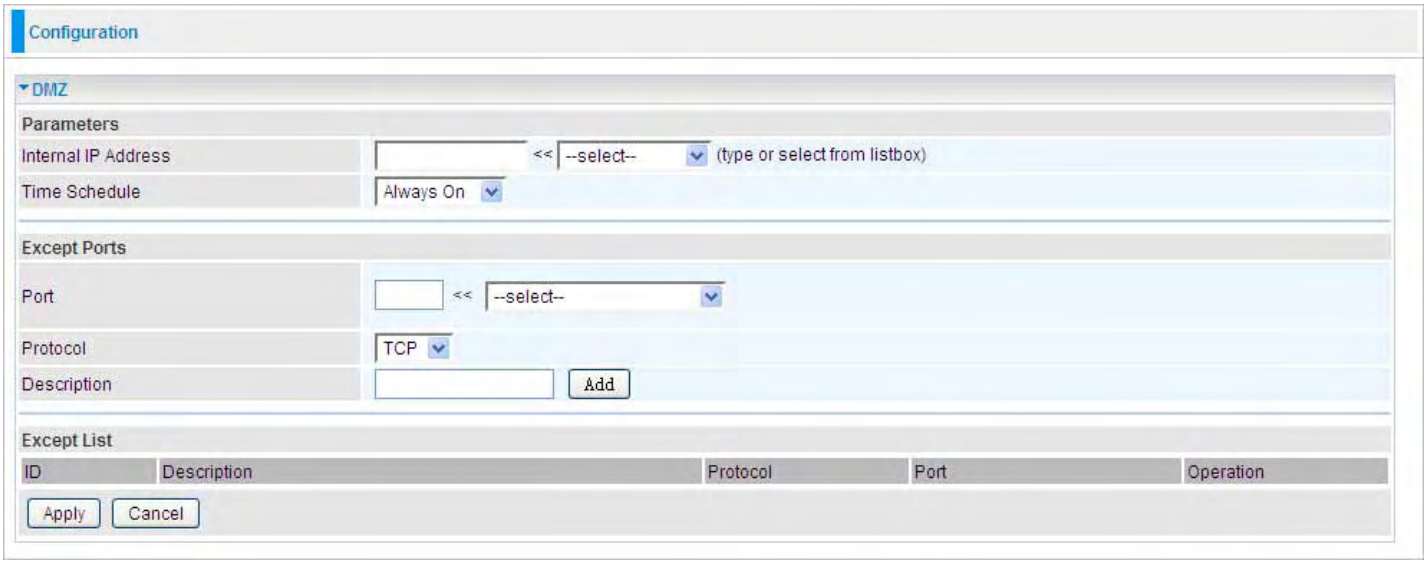


In addition to specifying the port number used, you also need to specify the protocol used. The

protocol is determined by the particular application. Most applications use TCP or UDP, however you can 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 are checked by the Firewall and NAT algorithms, it is then passed to the DMZ host when a packet received does not use a port number in use by any other Virtual Server entries.



Internal IP Address: Enter the IP address of a specific internal server to which will be the DMZ Host.

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

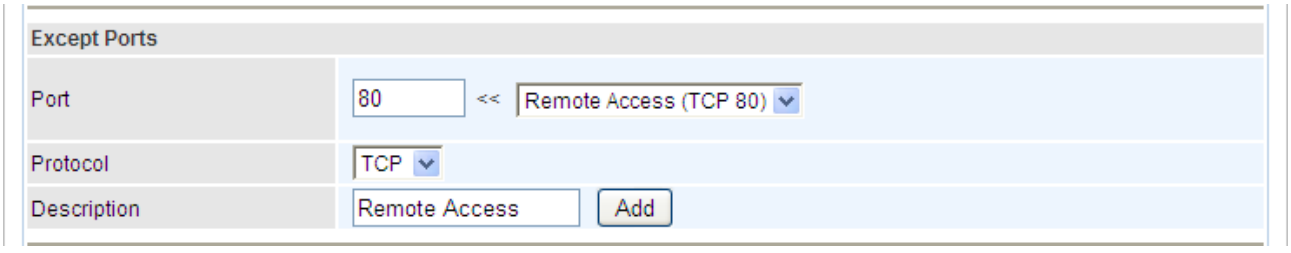
Port: The except port number. Default is set from range 1 ~ 65535.You can select from the drop down list and also can enter manually.

Protocol: Select the TCP or UDP protocol from the drop down list.

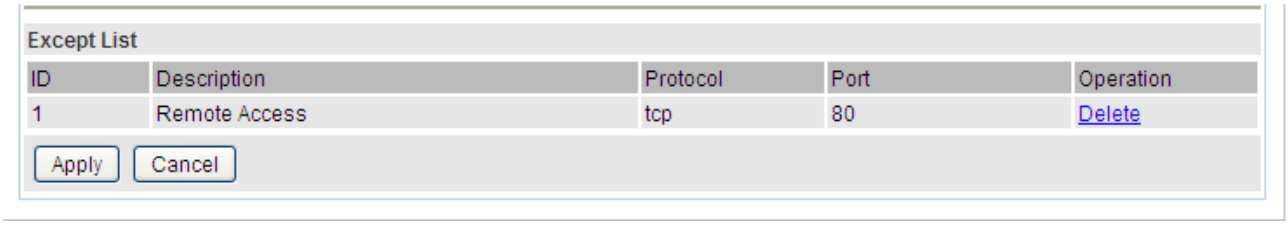
Description: The description of the port's function.

Add/Delete Except Ports

1. Enter except port number in the port field or choose from the drop down list. Select the port and describe the port.



2. Click **Add**. The new except port will display below.

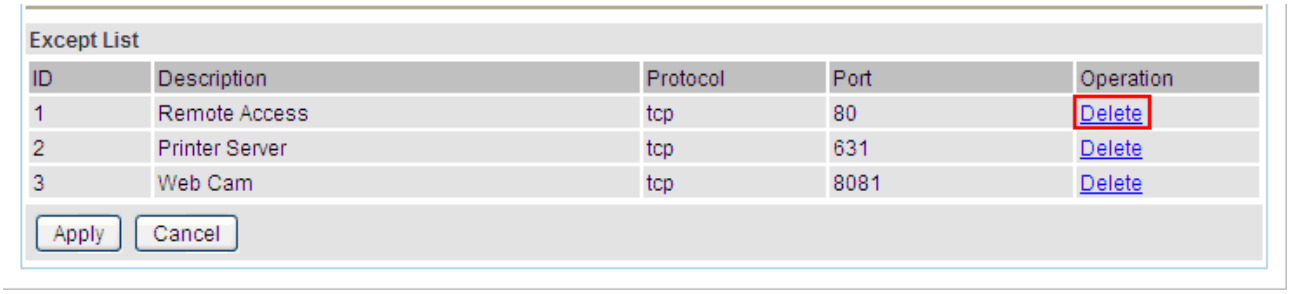


Except List

ID	Description	Protocol	Port	Operation
1	Remote Access	tcp	80	Delete

Apply Cancel

3. Click **Delete** to delete the one which you want to remove from the except list.



Except List

ID	Description	Protocol	Port	Operation
1	Remote Access	tcp	80	Delete
2	Printer Server	tcp	631	Delete
3	Web Cam	tcp	8081	Delete

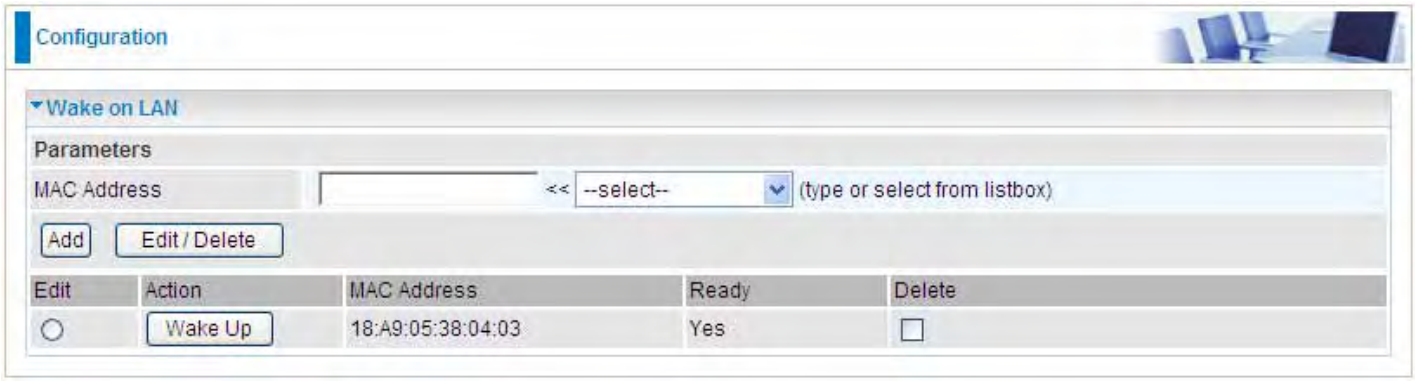
Apply Cancel

Using port mapping does have security implications, since outside users are able to connect to PCs on your network. For this reason you are advised to use specific Virtual Server entries just for the ports your application requires instead of simply using DMZ or creating a Virtual Server entry for “All” protocols, as doing so results in all connection attempts to your public IP address accessing the specified PC

If you have disabled the NAT option in the WAN-ISP section, the Virtual Server will hence become invalid. If the DHCP option is disabled, you have to to be very careful in assigning the Ip addresses of the valid servers in order to aviod conflcits. The easiest way of configuring Virtual Servers is to manually assign static IP addresses to each virtual server PC,with an address that dees not fall into the range of IP address that are issued by the DHCP server. You can configure the virtual server IP address maually, but it must still be in the same subnet as the router.

Wake on LAN

Wake on LAN (WOL, sometimes WoL) is an Ethernet computer networking standard that allows a computer to be turned on or woken up remotely by a network message.



Select: Select MAC address of the computer that you want to wake up or turn on remotely.

Add: After selecting, click **Add** then you can perform the Wake-up action.

Edit/Delete: Click to edit or delete the selected MAC address.

Ready: "**Yes**" indicating the remote computer is ready for your waking up.

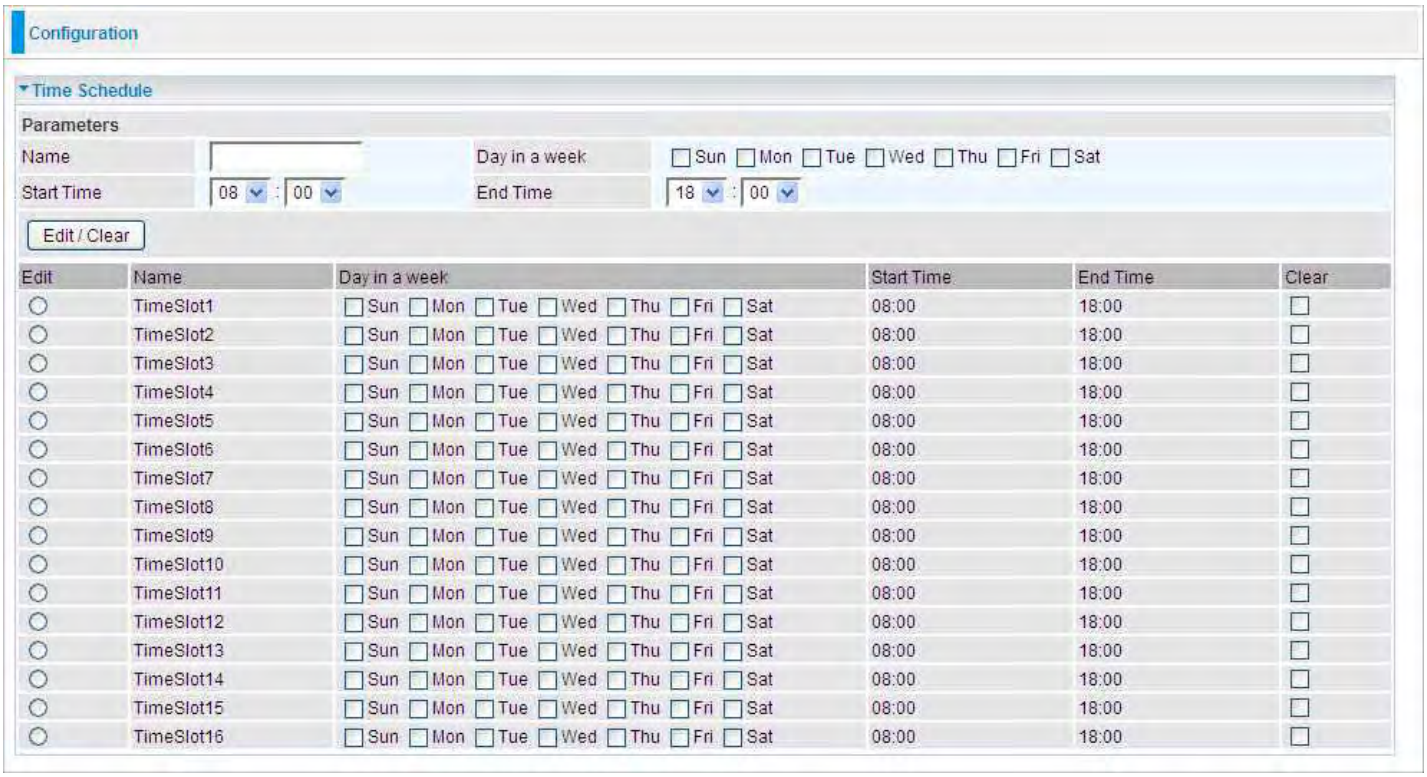
"**No**" indicating the machine is not ready for your waking up.

Delete: Delete the selected MAC address.

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 allowing the usage of the Internet by users or applications.

This Time Schedule correlates closely with router's time, since router does not have a real time clock on board; it uses the Simple Network Time Protocol (SNTP) to get the current time from an SNTP server from the Internet. Refer to **Time Zone** for details. You router time should correspond with your local time. If the time is not set correctly, your Time Schedule will not function properly.



Name: A user-define description to identify this time portfolio.

Day in a week: The default is set from Sunday through Saturday. You may specify the days for the schedule to be applied.

Start Time: The default is set at 8:00 AM. You may specify the start time of the schedule.

End Time: The default is set at 18:00 (6:00PM). You may specify the end time of the schedule. Select the Apply button to apply your changes.

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.

There are seven items within the **Advanced** section: **Static Route, Static ARP, Dynamic DNS, Device Management, SIP_ALG, IGMP, SNMP Access Control, TR-069 client** and **Remote Access.**

Static Route

Destination: The destination subnet IP address.

Netmask: Subnet mask of the destination IP addresses based on above destination.

Gateway: The gateway IP address to which packets are forwarded.

Interface: Select the interface through which packets are forwarded.

Cost: Represents the cost of transmission for routing purposes. The number need not be precise, but it must be between 0 and 65535.

Static ARP

IP Address: Fill in the IP address of the host computer that is sending the data packet.

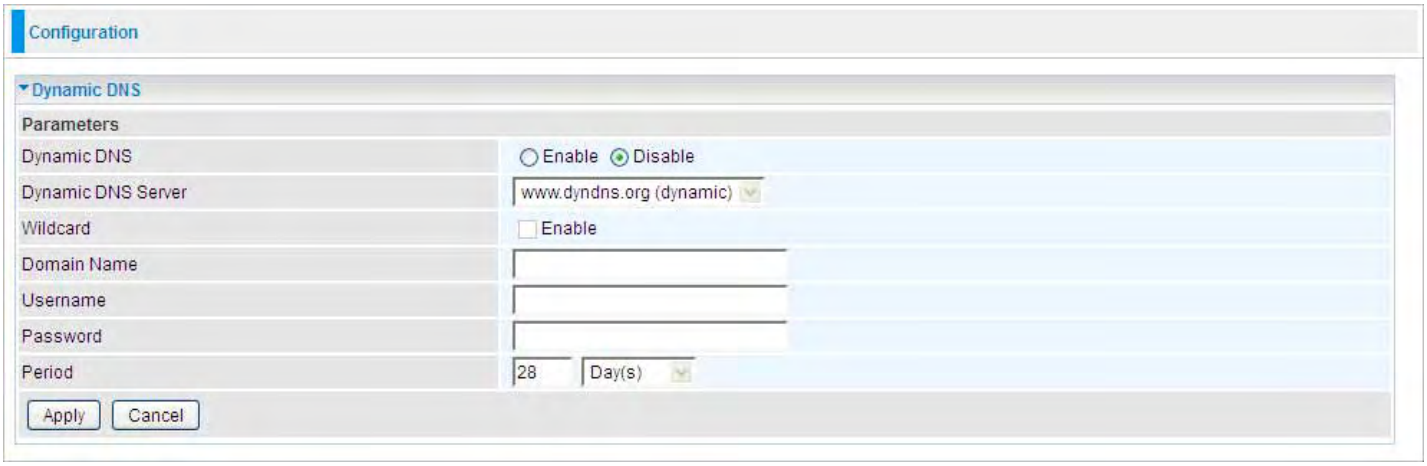
MAC Address: Fill in the MAC address of the computer that the incoming data packets are to be forwarded.

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 for hosting servers via your 3G 4G-LTE connection, so that anyone wishing to connect to you may use your domain name, rather than having to use your dynamic IP address, which changes from time to time. This dynamic IP address is the WAN IP address of the router, which is assigned to you by your ISP.

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



Disable: Check to disable the Dynamic DNS function.

Enable: Check to enable the Dynamic DNS function. The fields following are activated and required.

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

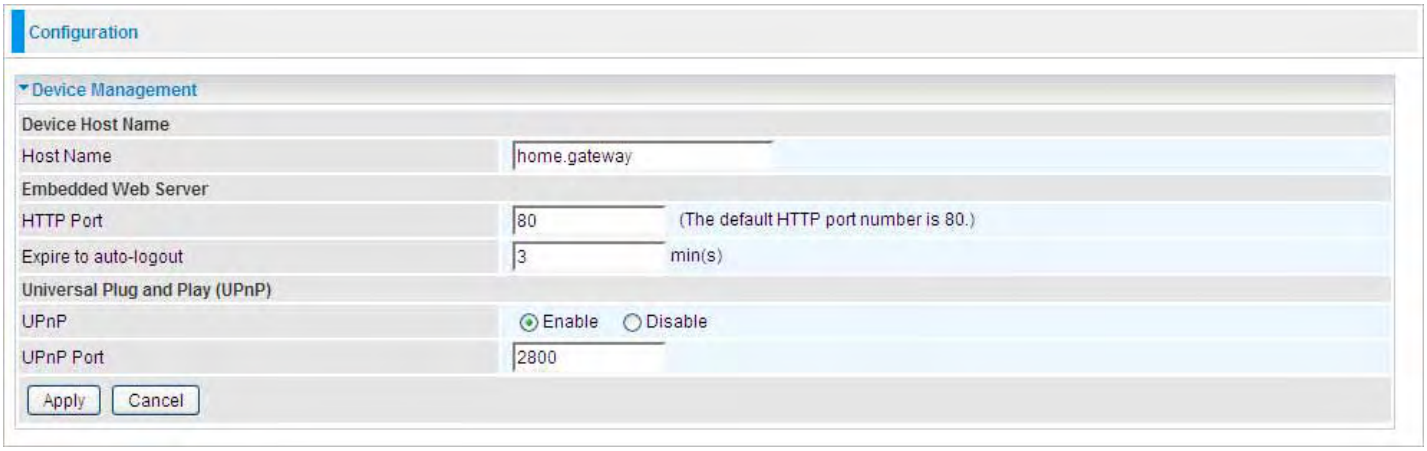
Wildcard: Select this check box to enable the DYNDNS Wildcard.

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

Period: Set the time period between updates, for the Router to exchange information with the DDNS server. In addition to updating periodically as per your settings, the router will perform an update when your dynamic IP address changes.

Device Management

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



Embedded Web Server

HTTP Port: The port number of the router's embedded web server (for web-based configuration uses. The default value is the standard HTTP port, 80. You may specify an alternative if, for example, you are running a web server on a PC within your LAN.

For Example: User A changes HTTP port number to **100**, specifies their own IP address of **192.168.1.55**, and sets the logout time to be **100** minutes. The router only allows User A access from the IP address **192.168.1.55** to logon to the Web GUI by typing: **http://192.168.1.254:100** in their web browser. After 100 minutes, the device automatically logs out User A.

Universal Plug and Play (UPnP)

UPnP offers peer-to-peer network connectivity for PCs and other network devices, along with control and data transfer between devices. UPnP offers many advantages for users running NAT routers through UPnP NAT Traversal, and on supported systems makes tasks such as port forwarding much easier by letting the application control the required settings, removing the need for the user to control advanced configuration of their device.

Both the user's Operating System and the relevant application must support UPnP in addition to the router. Windows XP and Windows Me natively support UPnP (when the component is installed), and Windows 98 users may install the Internet Connection Sharing client from Windows XP in order to support UPnP. Windows 2000 does not support UPnP.

Disable: Check to disable the router's UPnP functionality.
Enable: Check to enable the router's UPnP functionality.
UPnP Port: The Default setting is 2800. It is highly recommended you use this port value.
If this value conflicts with other ports already in use you may wish to change the port.

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.

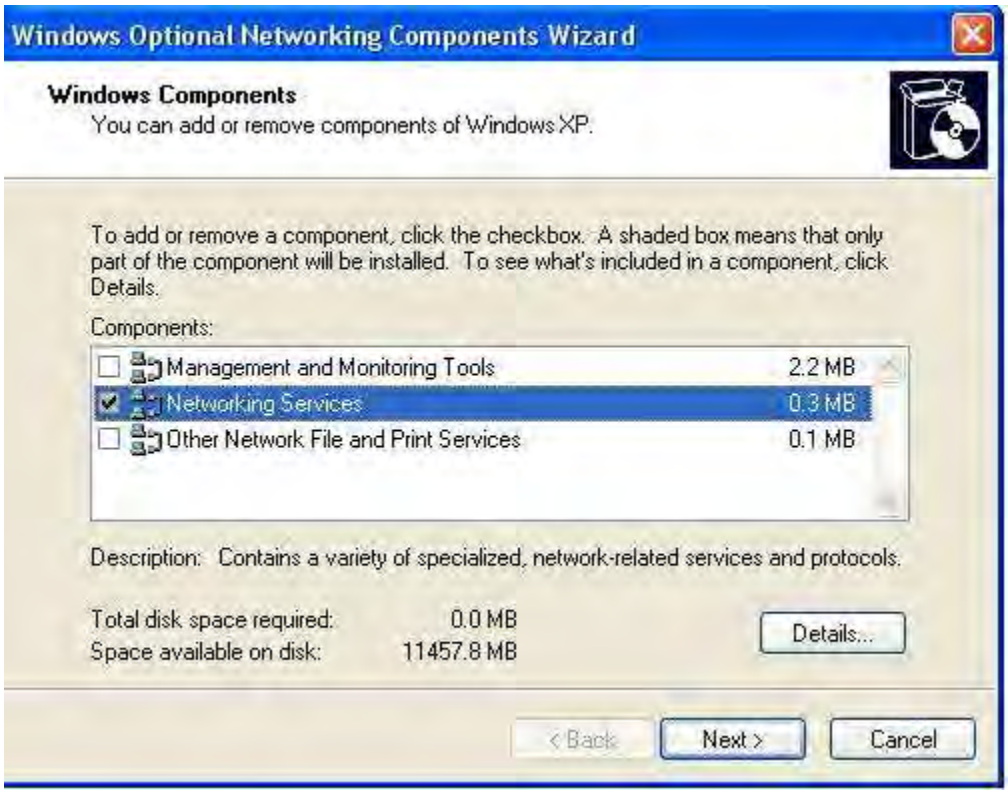
Step 4: Click OK to go back to the Add/Remove Programs Properties window. Click Next.
Step 5: Restart the computer when prompted.

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 ….

The Windows Optional Networking Components Wizard window displays.

Step 4: Select Networking Service in the Components selection box and click Details.



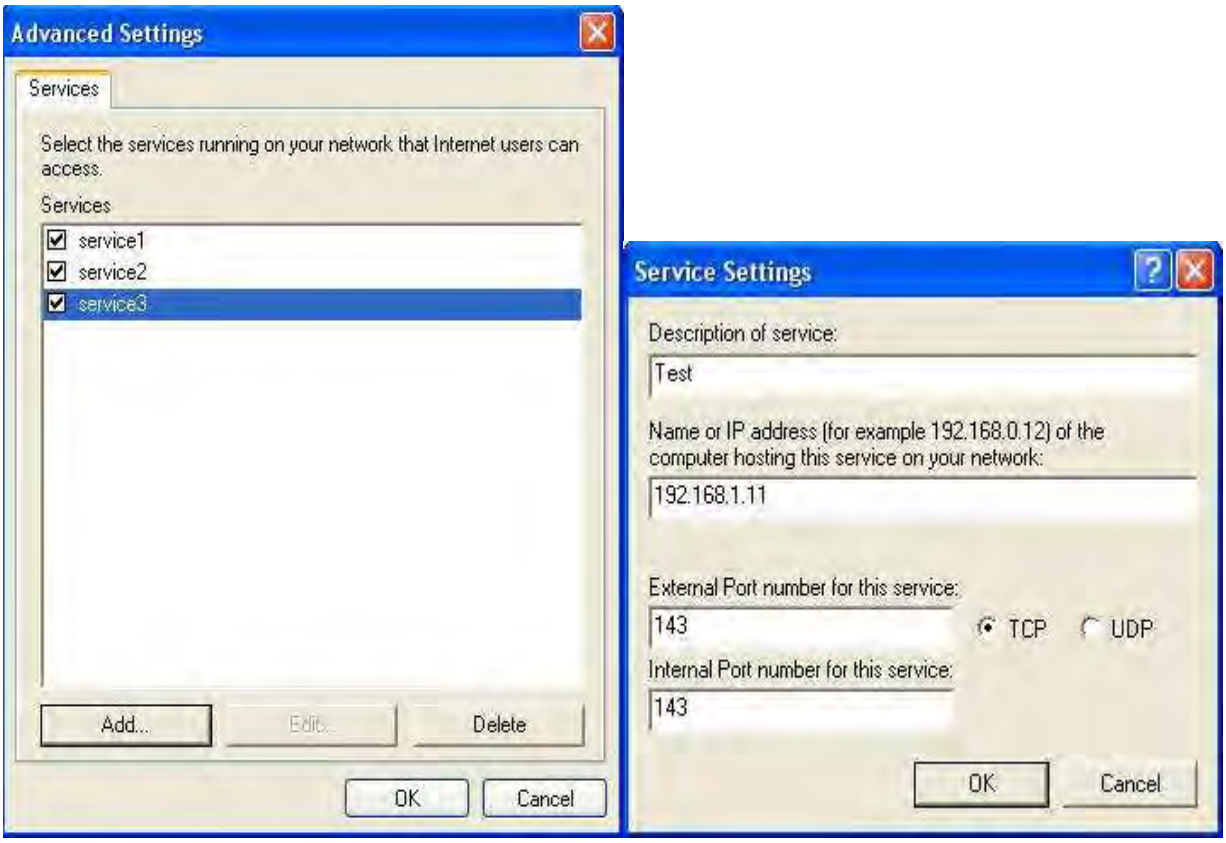
Step 5: In the Networking Services window, select the Universal Plug and Play check box.
Step 6: Click **OK** to go back to the Windows Optional Networking Component Wizard window and click **Next**.

Auto-discover Your UPnP-enabled Network Device

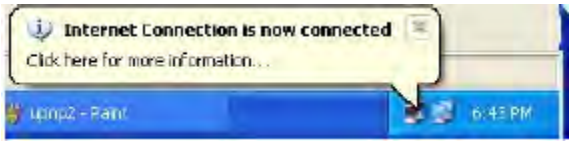
Step 1: Click start and Control Panel. Double-click Network Connections. An icon displays under Internet Gateway.
Step 2: Right-click the icon and select Properties.

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

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



Step 5: Select Show icon in notification area when connected option and click OK. An icon displays in the system tray



Step 6: Double-click on the icon to display your current Internet connection status.

Web Configurator Easy Access

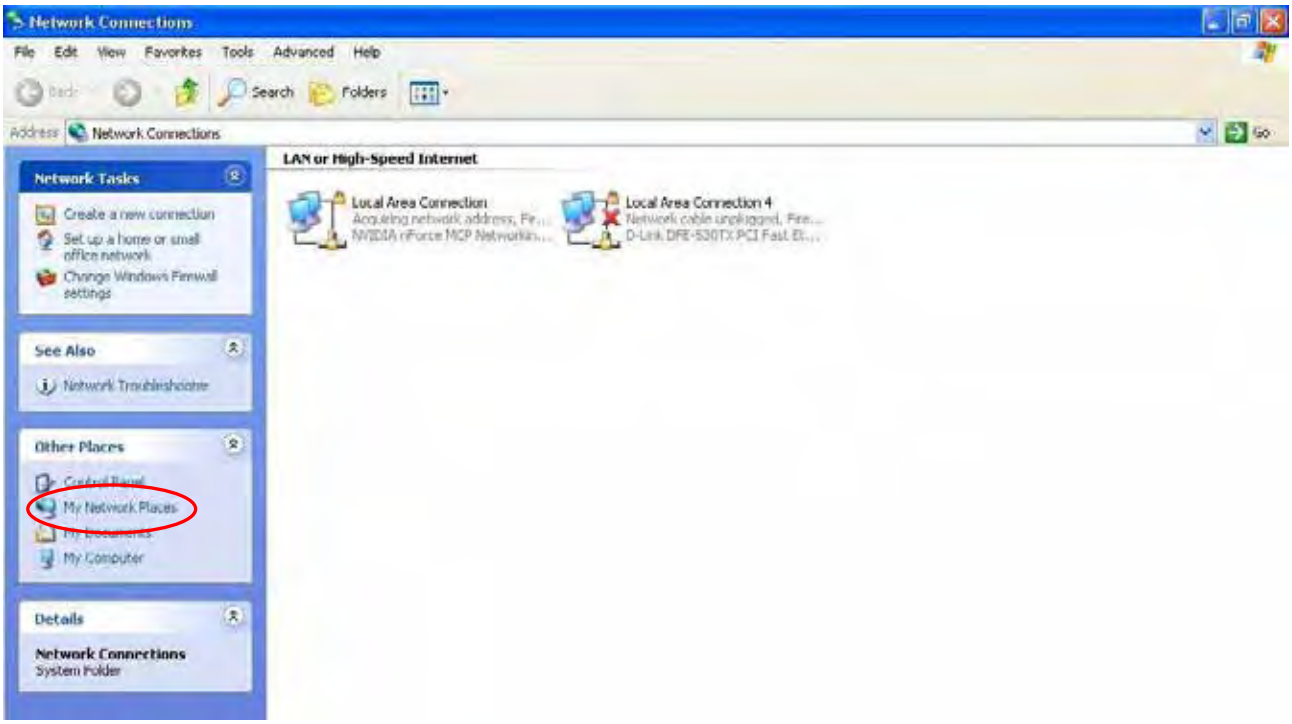
With UPnP, you can access web-based configuration for the **Mobile Broadband Wireless-N**

Router 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.



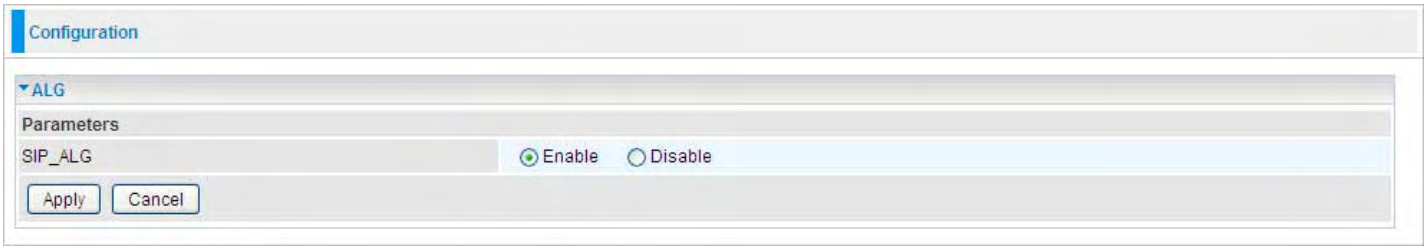
Step 4: An icon describing each UPnP-enabled device shows under Local Network.

Step 5: Right-click on the icon of your **Mobile Broadband Wireless-N Router** and select Invoke. The web configuration login screen displays.

Step 6: Right-click on the icon of your **Mobile Broadband Wireless-N Router** and select Properties. A properties window displays basic information about the router.

SIP_ALG

Select **Enable** to activate **SIP ALG** feature or Disabled to disable this feature.
The Session Initiation Protocol (SIP) is an IETF-defined signaling protocol, widely used for controlling multimedia communication sessions such voice and video calls over Internet protocol (IP). The protocol can be used for creating, modifying and terminating two-party (unicast) or multiparty (multicast) sessions consisting of one or several media streams. It is a text-based Application Layer protocol.
But as many use NAT to communicate with the public networks, and the IP address and port combination in SIP packets are needed for addressing, we must come up with an effective way to deal with SIP NAT traversal. SIP ALG is an easy solution with which you are only required to enable SIP ALG on NAT application in this router to easily experience the smooth SIP connection between private networks and public networks or even in two private networks with your VoIP devices.



IGMP

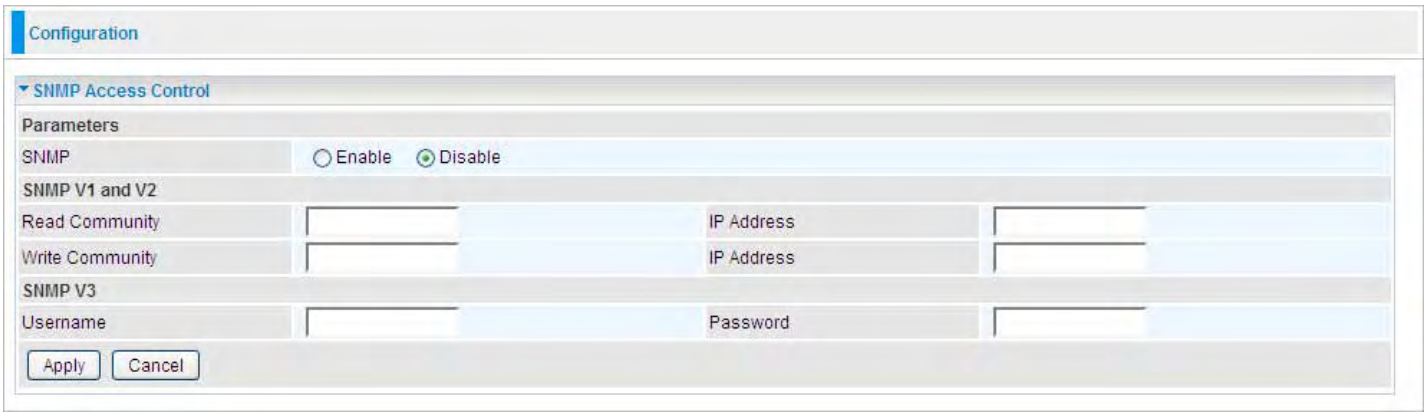
IGMP, known as Internet Group Management Protocol, is used to management hosts from multicast group.

IGMP Proxy: Accepting multicast packet. Default is set to **Disable.**

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

SNMP Access Control

Software on a PC within the LAN is required in order to utilize this function - Simple Network Management Protocol.



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.

Trap Community: Specify a name to be identified as the Trap 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 sent SNMP Traps.

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.

SNMP Version: SNMPV2c and SNMPv3

SNMPv2c is the combination of the enhanced protocol features of SNMPv2 without the SNMPv2 security. The "c" comes from the fact that SNMPv2c uses the SNMPv1 community string paradigm for "security", but is widely accepted as the SNMPv2 standard.

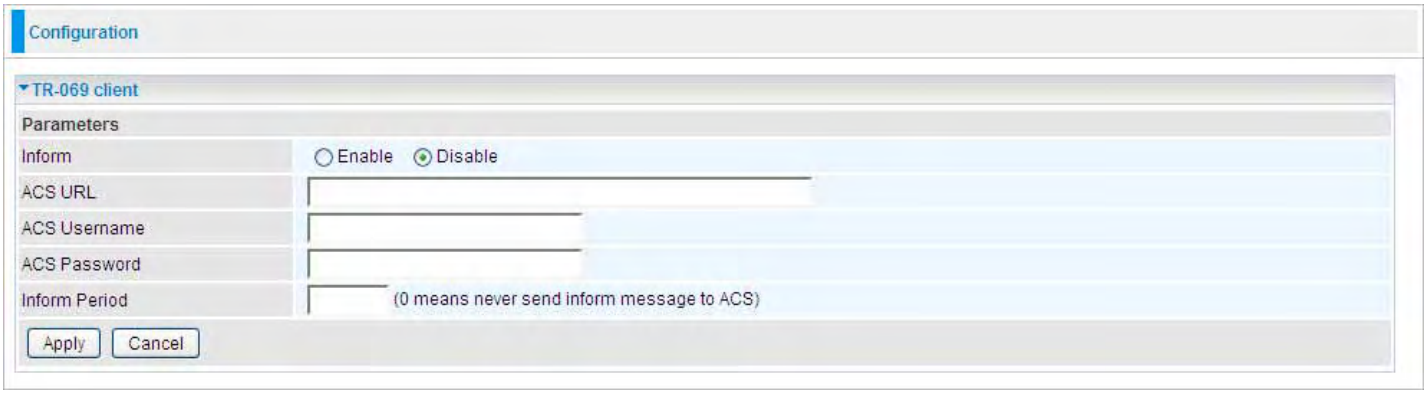
SNMPv3 is a strong authentication mechanism, authorization with fine granularity for remote monitoring.

Traps supported: Cold Start, Authentication Failure.

TR-069 Client

TR069, (short for Technical Report 069) is a DSL Forum (which was later renamed as Broadband Forum) technical specification entitled CPE WAN Management Protocol (CWMP). It defines an application layer protocol for remote management of end-user devices. It defines an application layer protocol for remote management of end-user devices.

As a bidirectional SOAP/HTTP based protocol it can provides the communication between customer premises equipment (CPE) and Auto Configuration Server (ACS). It includes both a safe configuration and the control of other CPE management functions within an integrated framework. In the course of the booming broadband market, the number of different internet access possibilities grew as well (e.g. modems, routers, gateways, set-top box, VoIP-phones).At the same time the configuration of this equipment became more complicated –too complicated for end-users. For this reason, TR-069 was developed. It provides the possibility of auto configuration of the access types. Using TR-069 the terminals can get in contact with the Auto Configuration Servers (ACS) and establish the configuration automatically and let ACS configure CPE automatically.



Inform: Enable to authorize CPE to send Inform message to automatically connect to ACS.

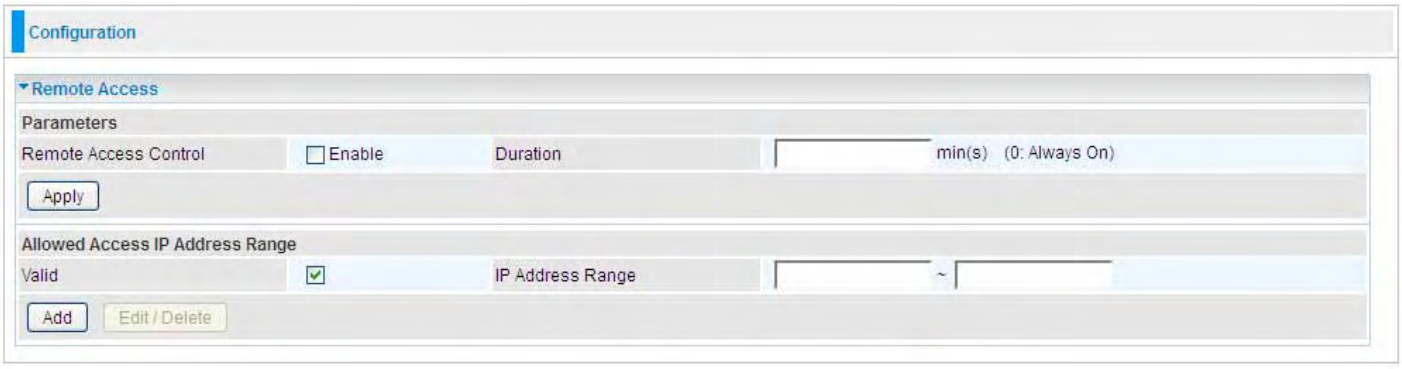
ACS URL: Enter the ACS server accessing URL.

ACS Username: Set the ACS user name for ACS authentication to the connection from CPE.

ACS Password: Set the ACS server login password.

Inform Period: Specify the inform interval time (sec) which CPE used to periodically send inform message to automatically connect to ACS.

Remote Access



Remote Access Control

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

Duration: Set how many minutes to allow management access from remote side. Zero means always on.

Allowed Access IP Address Range

Valid: Select Valid to allow remote management from these IP ranges.

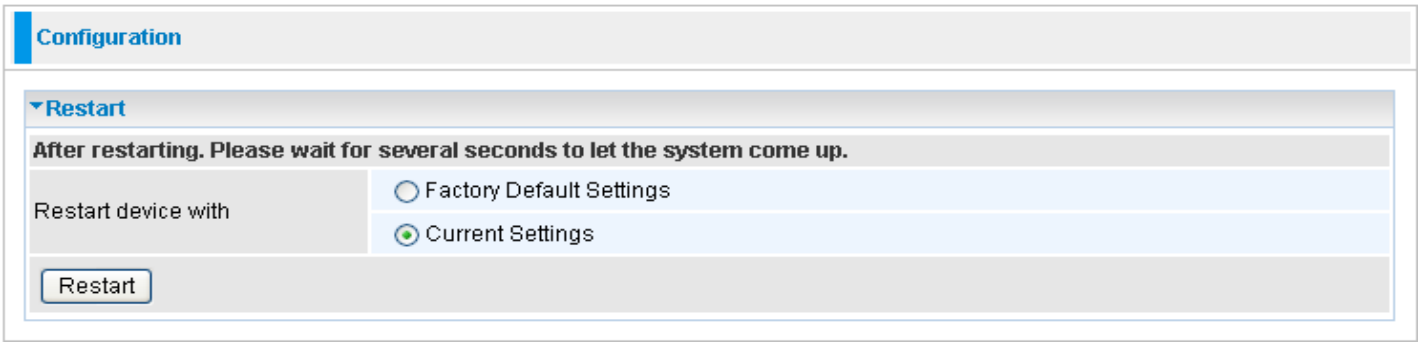
IP Address Range: Specify what IP address to be allowed to access device from remote side. Clink Add to insert management IP address list.

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.

Logout

To exit the router's web interface, choose **Logout**. Please ensure that you have saved the configuration settings before you logout.

Be aware that the router is restricted to only one PC accessing the configuration web pages at a time. Once a PC has logged into the web interface, other PCs cannot get access until the current PC has logged out of the web interface. If the previous PC forgets to logout, the second PC can access the page after a user-defined period, by default 3 minutes. You can modify this value using the **Advanced - Device Management** section of the web interface. Please see the **Advanced** section of this manual for more information.

Chapter 6: Troubleshooting

If your Router is not functioning properly, you can refer first to this chapter for simple troubleshooting before contacting your service provider support. This can save you time and effort but if symptoms persist, consult your service provider.

Problems starting up the router

Problem	Corrective Action
None of the LEDs are on when you turn on the router.	Check the connection between the adapter and the router. If the error persists, you may have a hardware problem. In this case you should contact technical support.

Problems with the LAN Interface

Problem	Corrective Action
Can't ping any PCs on the LAN.	Check the Ethernet LEDs on the front panel. The LED should be on for a port that has a PC connected. If it is off, check the cables between your router and the PC. Make sure you have uninstalled any software firewall for troubleshooting. Verify that the IP address and the subnet mask are consistent between the router and the workstations.

Appendix: Product Support & Contact

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

Federal Communication Commission Interference Statement

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

FCC Caution:

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions:

(1) This device may not cause harmful interference

(2) This device must accept any interference received, including interference that may cause undesired operation.

RF Radiation Exposure and Hazard Statement:

To ensure compliance with FCC RF exposure requirements, this device must be installed in a location such that the antenna of the device will be greater than 20cm (8 in.) away from all persons. Using higher gain antennas and types of antennas not covered under the FCC certification of this product is not allowed. Installers of the radio and end users of the product must adhere to the installation instructions provided in this manual. This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

Non-modification Statement:

Use only the integral antenna supplied by the manufacturer when operating this device. Unauthorized antennas, modifications, or attachments could damage the TI Navigator access point and violate FCC regulations. Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate this equipment.

MAC OS is a registered Trademark of Apple Computer, Inc.

Windows 7/98, Windows NT, Windows 2000, Windows Me, Windows XP and Windows Vista are registered Trademarks of Microsoft Corporation.