TW-EF600

802.11n Fiber Optical Router

User Manual

Model a = 100MB SPF
Model b = 1000MB SPF

Table of Contents

Chapter 1: Product

Introduction to your Router

Thank you for purchasing TW-EF600 802.11n Fiber Optical Router. Your new router is a point-to-point fiber gateway that allows you to experience very super fast broadband point-to-point connectivity for FTTH applications.

The 802.11n Fiber Optical Router is a point-to-point (P2P) Fiber Gateway – featuring a 4-port Gigabit Ethernet Switch, Firewall and Wi-Fi 802.11n access point. The device can be used for fiber-to-the-home (FTTH) applications and offers four different optical connectors of Fiber WAN interface transceiver: 100/1000BASE-BX (single-mode single fiber transceiver), 100/1000BASELX (single-mode dual fiber), 100BASE-FX (multi-mode dual fiber), and 100/1000BASE Small Form Factor Pluggable (SFP).

Moreover, the 802.11n Fiber Optical Router supports remote management on end-user devices, which is available upon request for Telco's/ISPs projects to tightly manage FTTH service delivery. The router is also equipped with a built-in 4-port Gigabit Switch, enabling amazingly fast LAN transmissions for bandwidth-consuming applications such as video streaming and file sharing. The integrated 802.11n Wireless Access Point ensures the router offers faster wireless speeds (up to 300Mbps) while three built-in antennae maximize wireless signals.

The 802.11n Fiber Optical Router automatically adopts the optimal connection to deliver smooth and constant signal reception even if obstacles are present. Users can easily enjoy high bandwidth applications such as High Definition IPTV services without changing their home network. A robust Firewall is also built in to provide protection against intrusion attacks while the Quality of Service feature prioritizes queues and traffic or manages bandwidth for applications such as music downloads and online gaming.

802.11n Wireless AP with WPA Support (802.11n Fiber Optical Router Only)

With integrated 802.11n Wireless Access Point in the router, the device offers a quick and easy access among wired network, wireless network and broadband connection (VDSL) with single device simplicity, and as a result, mobility to the users. In addition to 300 Mbps 802.11n data rate, it also interoperates backward with existing 802.11g and 802.11b equipment. The Wi-Fi Protected Access (WPA) and Wired Equivalent Privacy (WEP) supported features enhance the security level of data protection and access control via Wireless LAN.

Fast Ethernet Switch

A 4-port 10/100/1000Mbps fast Ethernet switch is built in with automatic switching between MDI and MDI-X for 10Base-T, 100Base-TX and 1000Base-TX ports. An Ethernet straight or crossover cable can be used directly for auto detection.

PPP over Ethernet (PPPoE)

This device provides an embedded PPPoE client function to establish a connection. You get greater access speed without changing the operation concept, while sharing the same ISP account and paying for one access account. No PPPoE client software is required for the local computer. Automatic Reconnect and Disconnect Timeout (Idle Timer) functions are also provided.

Quick Installation Wizard

It supports a WEB GUI page to install this device quickly. With this wizard, end users can enter the

Information easily which they get from their ISP, then surf the Internet immediately.

Universal Plug and Play (UPnP) and UPnP NAT Traversal

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

Network Address Translation (NAT)

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

Domain Name System (DNS) Relay

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

Dynamic Domain Name System (DDNS)

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

Rich Management Interfaces

It supports flexible management interfaces with local console port, LAN port, and WAN port. Users can use terminal applications through the console port to configure and manage the device, or Telnet, WEB GUI, and SNMP through LAN or WAN ports to configure and manage the device.

Quality of Service (QoS)

QoS gives you full control over which types of outgoing data traffic should be given priority by the router, ensuring important data like gaming packets, customer information, or management Information move through the router ay lightning speed, even under heavy load. The QoS features are configurable by source IP address, destination IP address, protocol, and port. You can throttle the speed at which different types of outgoing data pass through the router, to ensure P2P users don't saturate upload bandwidth, or office browsing doesn't bring client web serving to a halt. In addition, or alternatively, you can simply change the priority of different types of upload data and let the router sort out the actual speeds.

Virtual Server

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

Rich Packet Filtering

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

Dynamic Host Configuration Protocol (DHCP) Client and Server

In the WAN site, the DHCP client can get an IP address from the Internet Service Provider (ISP) automatically. In the LAN site, the DHCP server can allocate a range of client IP addresses and distribute them including IP address, subnet mask as well as DNS IP address to local computers. It provides an easy way to manage the local IP network.

Static and RIP1/2 Routing

It has routing capability and supports easy static routing table or RIP1/2 routing protocol.

Simple Network Management Protocol (SNMP)

It is an easy way to remotely manage the router via SNMP.

Web based GUI

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

Firmware Upgradeable

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

Features

- Fiber WAN interface
- 4-port Gigabit Switch
- Supports 802.11n Wireless Access Point with WPA-PSK / WPA2-PSK (802.11n Fiber Optical Router Only)
- WPS (Wi-Fi Protected Setup) for Easy Setup (802.11n Fiber Optical Router Only)
- Wireless Speed up to 300Mbps and 3 Times the Coverage of Standard 802.11b/g (802.11n Fiber Optical Router Only)
- Quality of Service Control for Traffic Prioritization and Bandwidth Management
- SOHO Firewall Security with DoS Prevention and Packet Filtering
- Easy Sign-On (EZSO)
- Universal Plug and Play (UPnP) Compliance
- Dynamic Domain Name System (DDNS)
- Available Syslog
- Supports IPTV Applications (IPTV application may require subscription to IPTV services from a Telco / ISP.)

Hardware Specifications

Physical Interface

Please refer to the instructions on the label of the outer box to get the specification of your device.

- Optical SC-connector with options:

- 100BASE-LX dual fiber single-mode WAN (Tx/Rx1310nm)

- 100BASE-BX single-strand single-mode WAN (Tx1310nm/Rx1550nm)

- 100BASE-FX dual fiber multimode WAN (Tx/Rx1310nm)

- 1000BASE-LX dual fiber single-mode WAN (Tx/Rx1310nm)

- 1000BASE-BX single-strand single-mode WAN (Tx1310nm/Rx1490nm)

- 100/1000BASE Optical SFP Optical convector
- WLAN: 3 x detachable antennae (802.11n Fiber Optical Router only)
- Ethernet: 4-port 10/100/1000M auto-crossover (MDI / MDI-X) Switch
- Factory default reset button
- WPS push button (802.11n Fiber Optical Router only)
- Power jack
- Power switch

Operating Environment

Operating temperature: 0 – 40°C

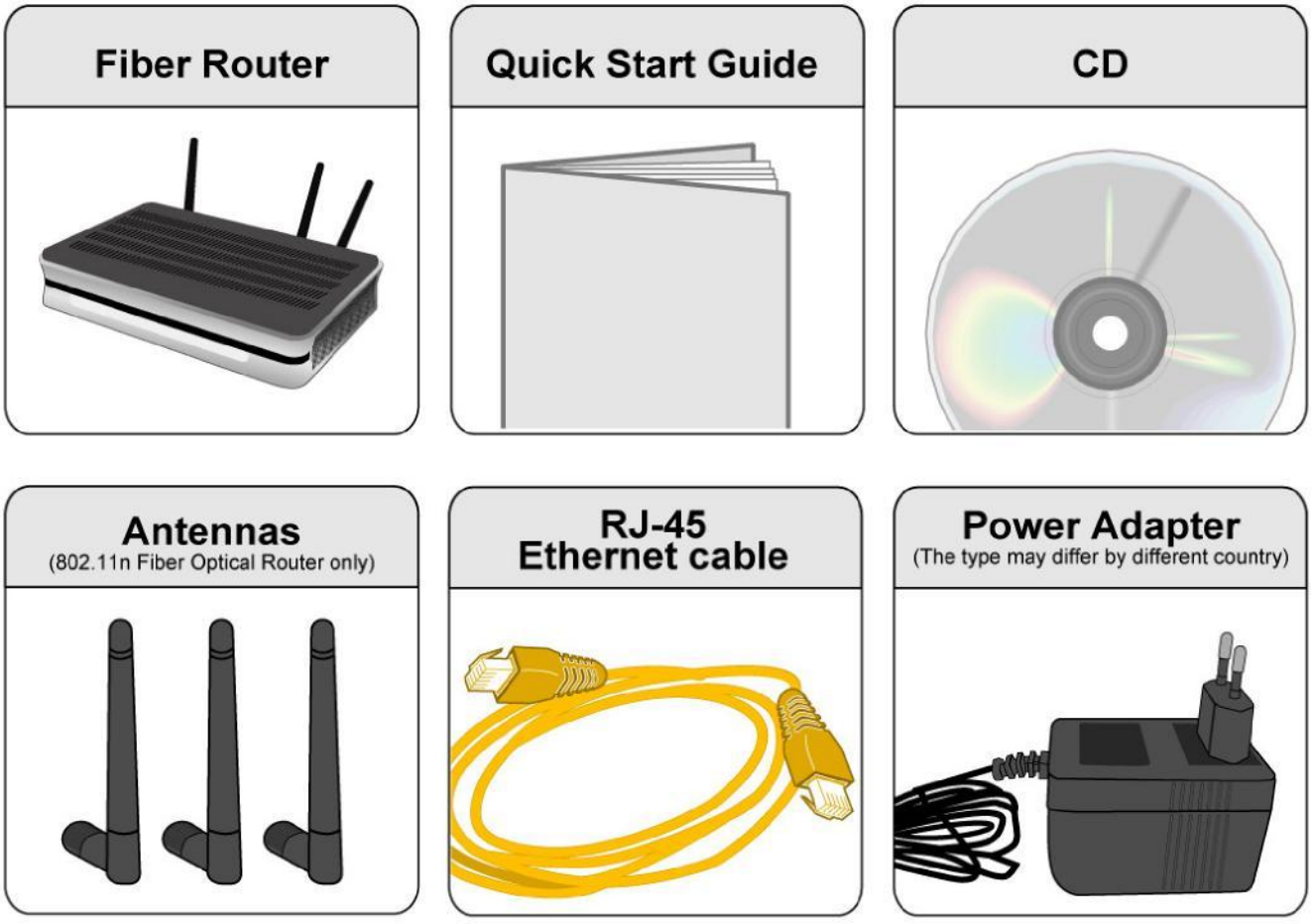
Storage temperature: -20 – 70°C

Humidity: 20 – 95% non-condensing

Chapter 2: Installing the Router

Package Contents

- **TW-EF600 802.11n Fiber Optical Router**
- **Quick Start Guide**
- **CD containing the online manual**
- **Three 2dBi detachable antennae (802.11n Fiber Optical Router only)**
- **Ethernet (RJ-45) cable**
- **Power adapter**



Important note for using this router

Warning

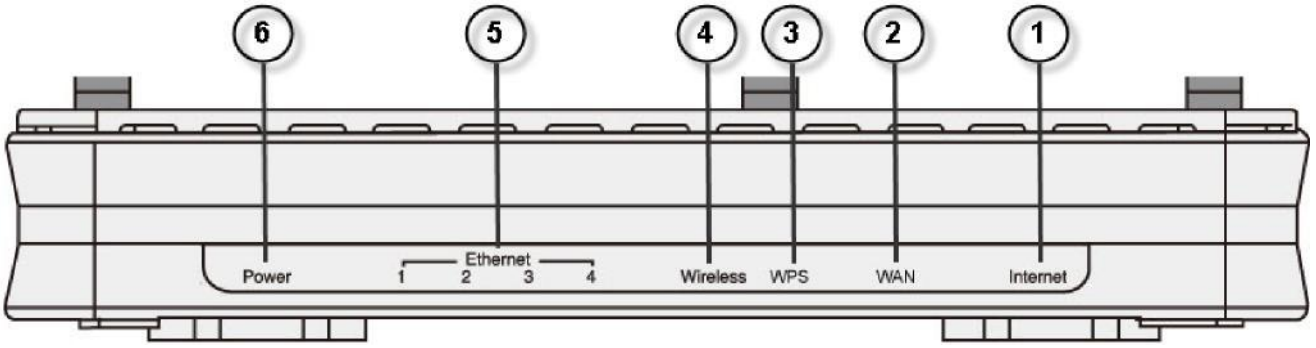
- Do not use the router in high humidity or high temperatures.
- Do not use the same power source for the router as other equipment.
- Do not open or repair the case yourself. If the router is too hot, turn off the power immediately and have it repaired at a qualified service center.
- Avoid using this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

Attention

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

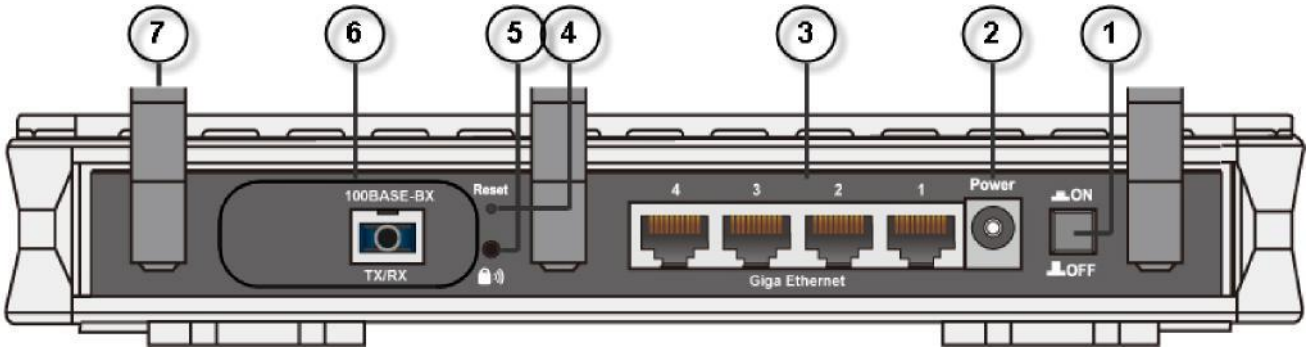
Device Description

The Front LEDs



LED		Meaning
1	**Internet**	Lit orange when WAN port fails to get IP address. Lit green when WAN port gets IP address successfully. Lit off when the device is in bridge mode or when WAN connection absent.
2	**WAN**	Lit green when the device is connected to a broadband connection device. Blinking when data is transmitted/received.
3	**WPS (802.11n Fiber Optical Router only)**	Flash green when WPS configuration is in progress. However, if WPS fails, the LED will only lit for 1 min before goes off.
4	**Wireless (802.11n Fiber Optical Router only)**	Lit green when a wireless connection is established. Flash green when data is transmitted/received.
5	**Ethernet port 1X — 4X (RJ-45 connector)**	Lit orange when one of LAN ports is connected to an Ethernet device. Lit green when the speed of transmission hits 1000Mbps; Lit orange when the speed of transmission hits 10/100Mbps. Blinking when data is transmitted/received.
6	**Power**	When the device is booting, the green light will lit while the orange light will flash. When the system is ready, it will lit green. Lit orange when the device fails to boot or when the device is in emergency mode.

The Rear Ports



Port		Meaning
1	**Power Switch**	Power ON/OFF switch.
2	**Power**	Connect it with the supplied power adapter.
3	**Giga Ethernet**	Connect a PC or another home network of 10Mbps, 100Mbps or 1000Mbps using the provided RJ-45 Ethernet cables.
4	**RESET**	Press this button for more than 5 seconds to restore the device to its default mode.
5	**WPS (802.11n Fiber Optical Router only)**	Push this button to trigger Wi-Fi Protected Setup function.
6	**WAN**	***specification*** • **100BASE-BX** • **1000BASE-BX** Ports: 100BASE Several options for fiber WAN interface and they do not coexist. ***Refer to the instructions on the label of the outer box to of your device.*** Port: A single strand of optical fiber. Single-mode fiber used (Tx1310nm/Rx1550nm). It supports SC connector. A single strand of optical fiber. Single-mode is used (Tx1310nm/Rx1490nm). It supports SC connector. According to transmission method, the dual fiber WANS separated into single mode and multi mode. • **100BASE-LX/SMF** & **1000BASE-LX/SMF** Two strands of optical fiber, one for receive (RX) and the other for transmit (TX). Single-mode fiber is used (Tx/Rx1310nm). It supports SC connector. • **100BASE-FX/MMF** Two strands of optical fiber, one for receive (RX) and the other for transmit (TX). Multimode fiber is used (Tx/Rx1310nm). It supports SC connector.
7	**Antenna (802.11n Fiber Optical Router only)**	Connect the detachable antenna to this port.

The detail instruction in Reset Button

Recovery procedures for non-working routers (e.g. after a failed firmware upgrade flash):

Hold the Reset Button on the back of the modem in. Keep this button held in and turn on the modem. Once the Power LED lights orange, release the Reset Button. The modem's emergency-reflash web interface will then be accessible via http://192.168.1.254 where you can upload a firmware image to restore the modem to a functional state. Please note that the modem will only respond via its web interface at this address, and will not respond to ping requests from your PC or to telnet connections.

Before the router is turned on to initiate its recovery process, please configure the IP address of the PC to 192.168.1.100 and then proceed with the following steps:
1. Turn off the router.
2. Hold the "Reset Button".
3. Turn on the router. The IP of the router will reset to an Emergency IP address (like 192.168.1.254).
4. Download the firmware.

Cabling

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

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

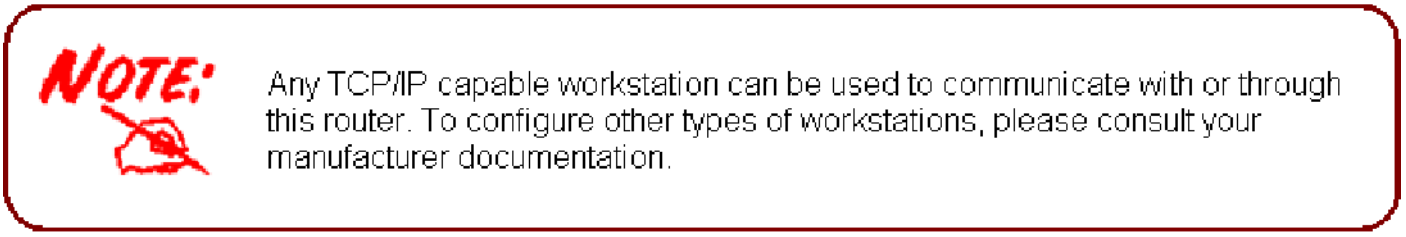
Chapter 3: Basic Installation

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

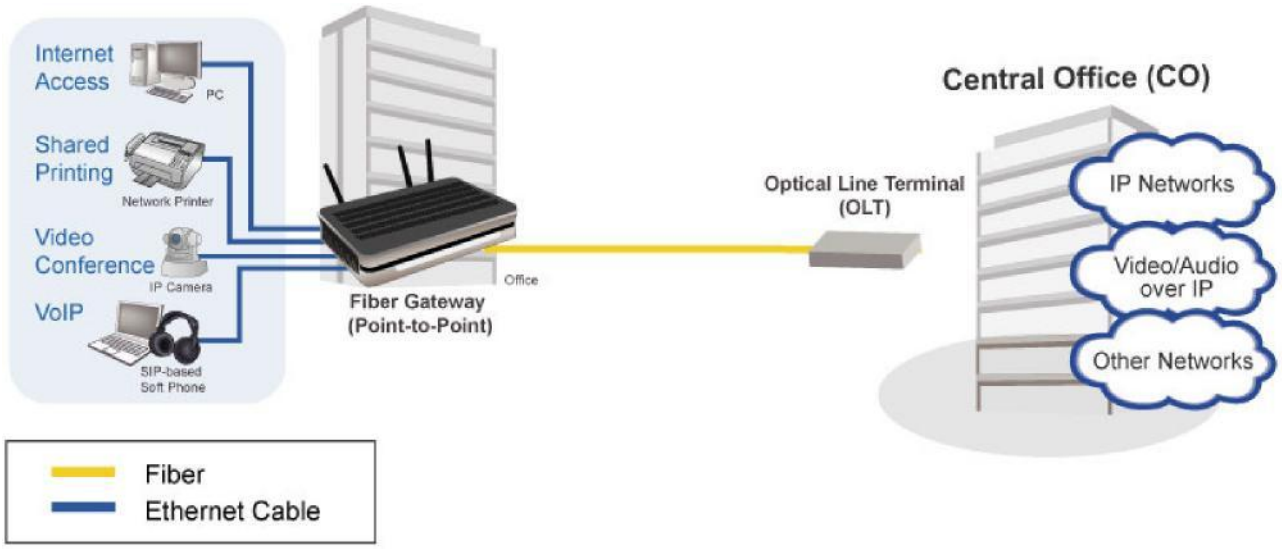
Please check your PC network components. The TCP/IP protocol stack and Ethernet network adapter must be installed. If not, please refer to your Windows-related or other operating system manuals.

There are ways to connect the router, either through an external repeater hub or connect directly to your PCs. However, make sure that your PCs have an Ethernet interface installed properly prior to connect the router device. You ought to configure your PCs to obtain an IP address through a DHCP server or a fixed IP address that must be in the same subnet as the router. The default IP address of the router is 192.168.0.254 and the subnet mask is 255.255.255.0 (i.e. any attached PC must be in the same subnet, and have an IP address in the range of 192.168.0.1 to 192.168.0.253). The best and easiest way is to configure the PC to get an IP address automatically from the router using DHCP. If you encounter any problem accessing the router web interface it is advisable to uninstall your firewall program on your PCs, as they can cause problems accessing the IP address of the router. Users should make their own decisions on what is best to protect their network.

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



Applications of the device

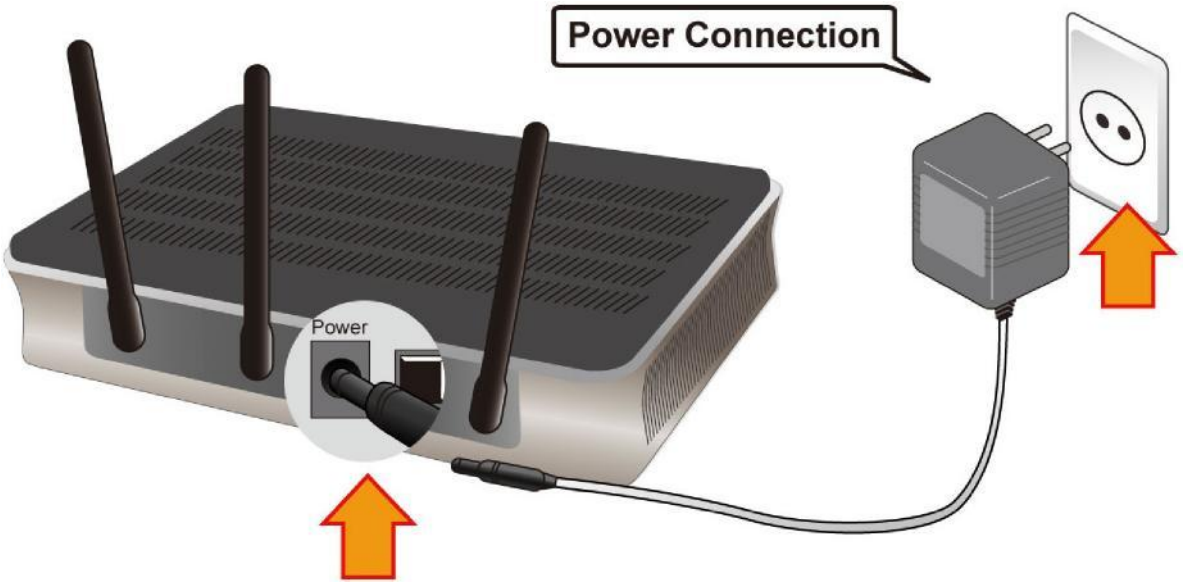


Hardware Installation

It is easy to connect the Fiber Optical Router simply by performing the following instructions:

Power Connection

Plug the supplied power adapter into the wall jack and the other side to the router. Please note that the plug type may differ according to country.



LAN Connection

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

Fiber Connection

Please follow the illustrations below to connect the fiber cable or module and the router.

Attention

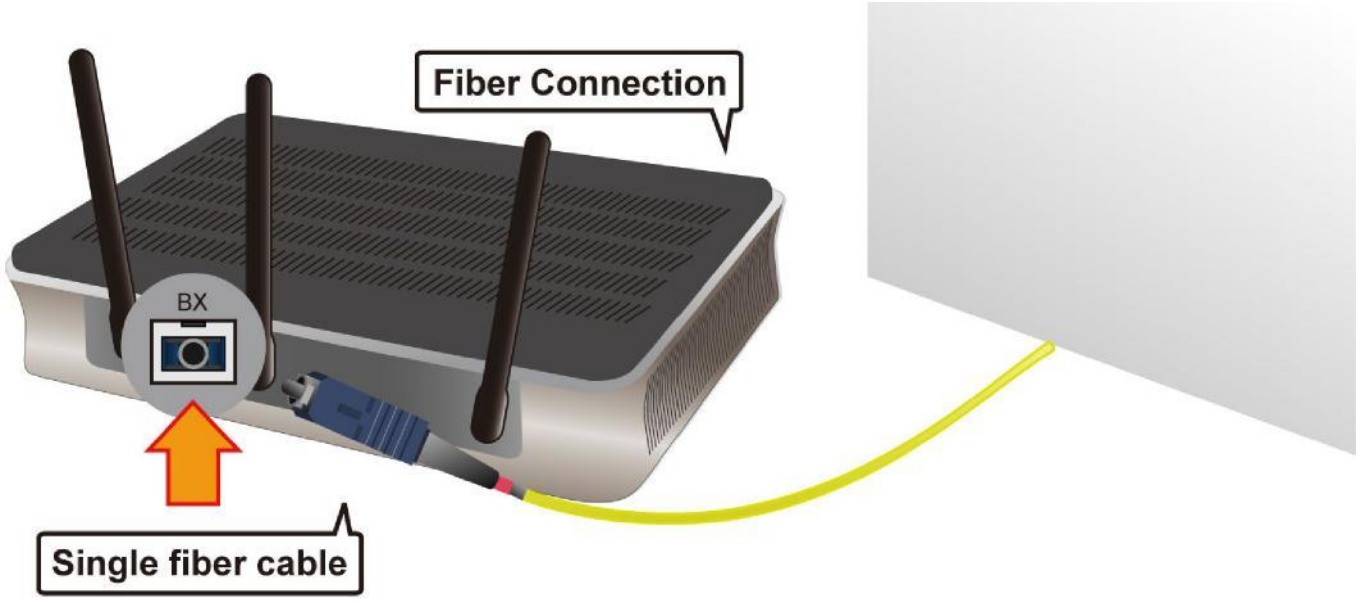
The type of fiber interface varies from device models provided by your ISP. Please refer to the instructions on the label of the outer box to get the specification of your device and follow the instructions of hardware installation

NOTE:

Please do not look steadily at the fiber port when you connect the fiber, because the invisible light may harm your vision.

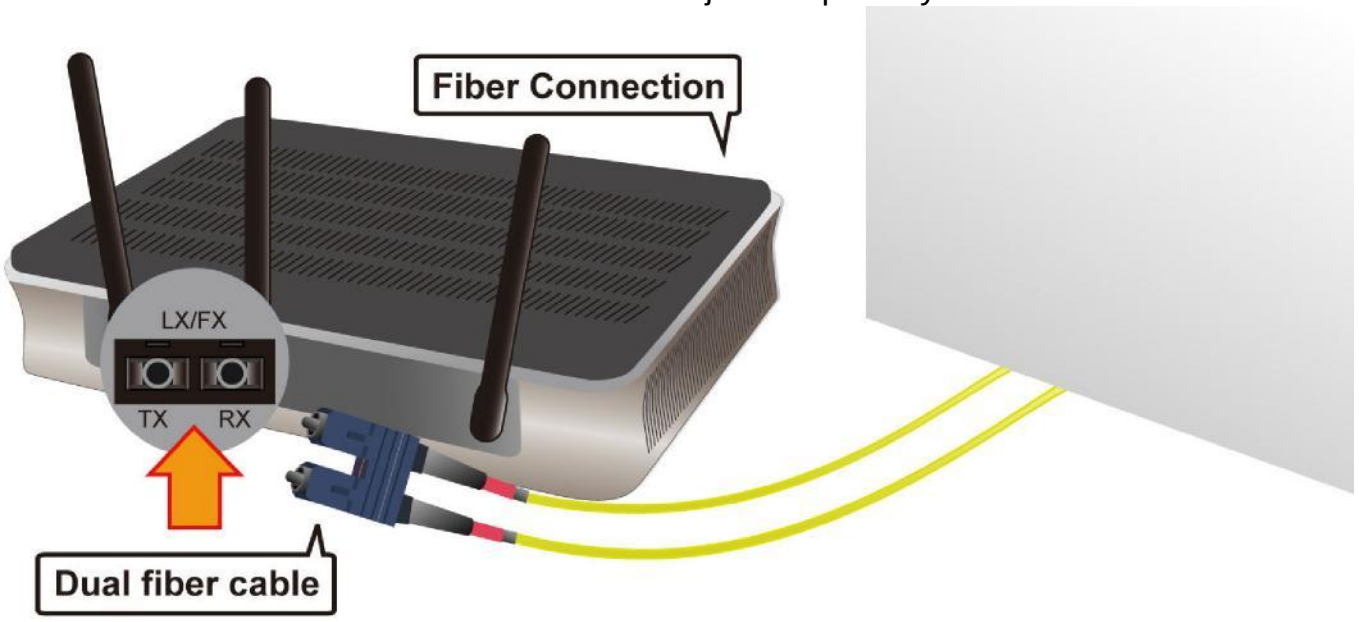
BX

Insert the single fiber cable into the BX jack of the router.



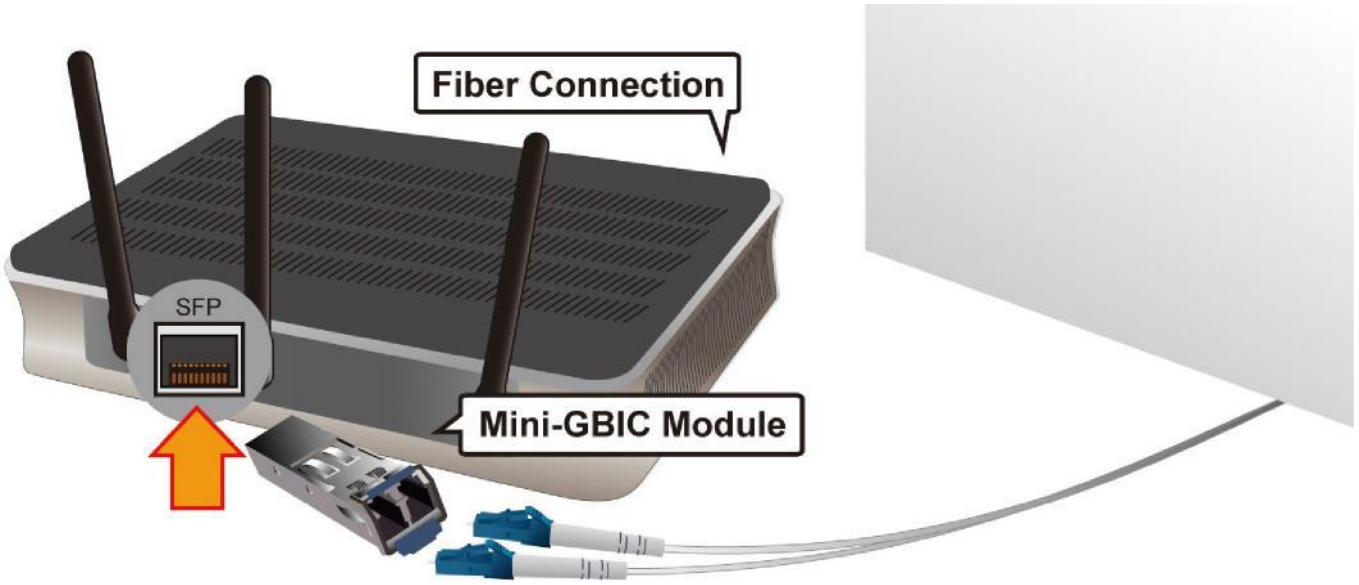
LX/ FX

Insert the dual fiber cable into the LX/FX TX and RX jacks separately of the router.



SFP

Set the M-GBIC module in the SFP port of your device, and then connect the fiber cable to the module.

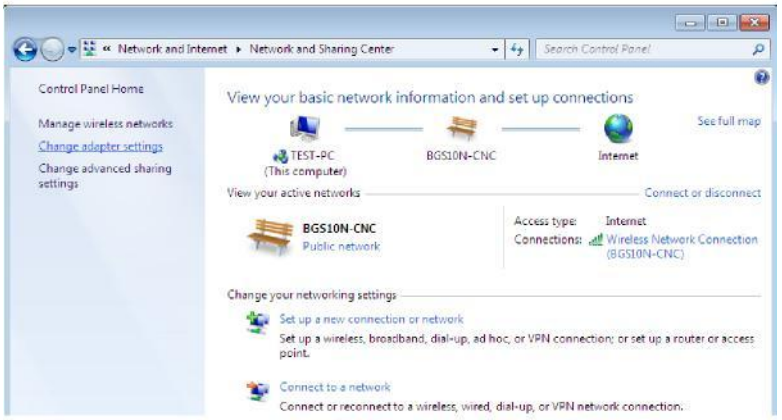


Network Configuration

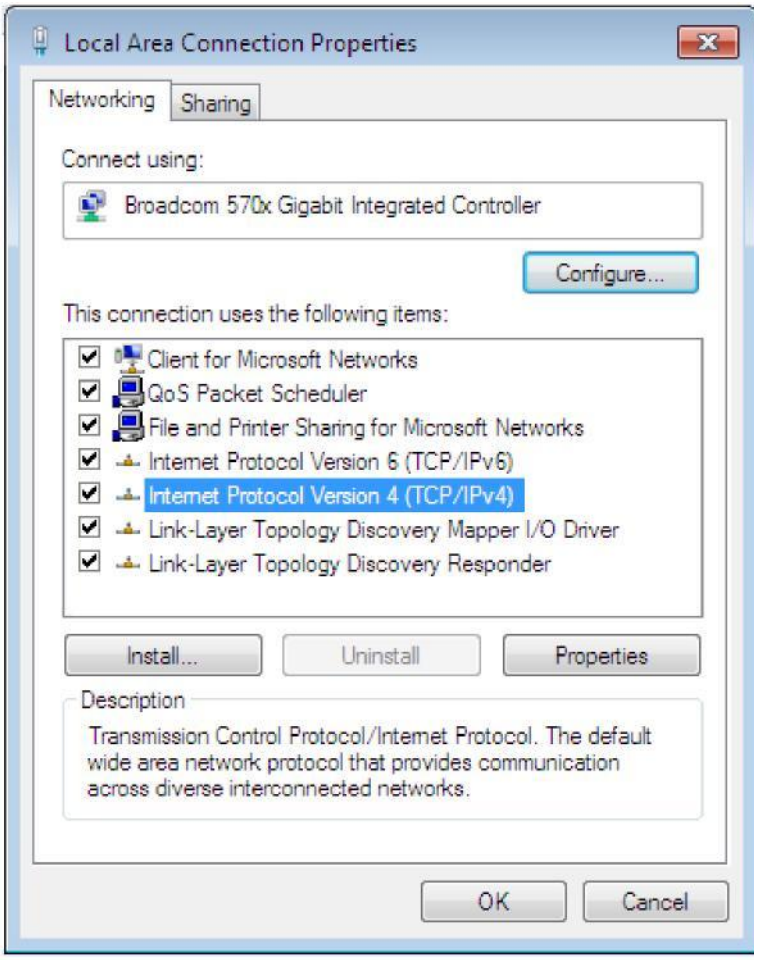
Configuring PC in Windows 7

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

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

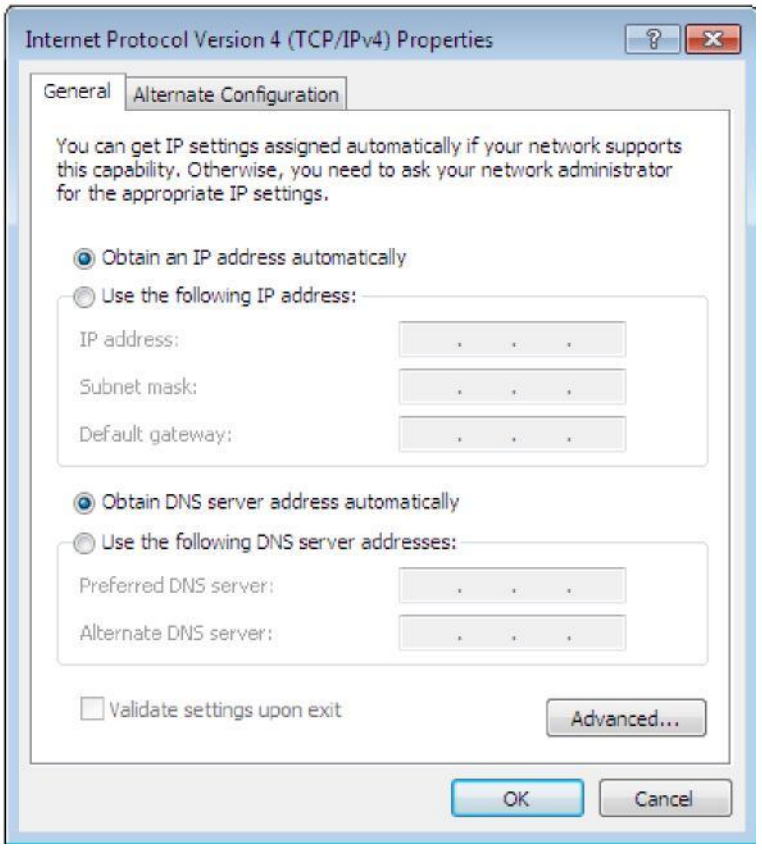


4. Select the Local Area Connection, and right click the icon to select Properties.



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

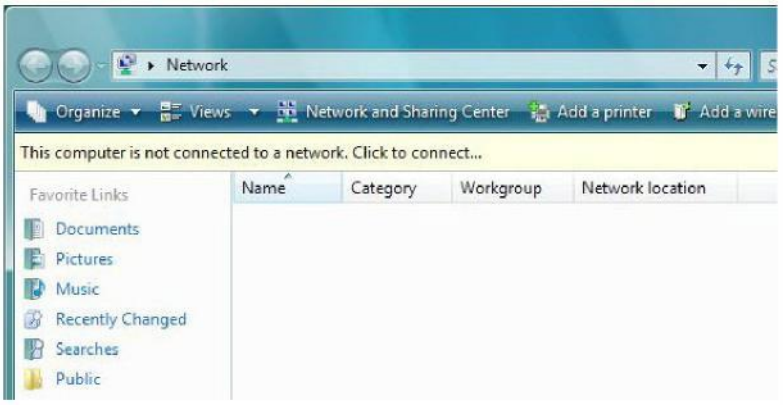
7. Click OK again in the Local Area Connection Properties window to apply the new configuration.



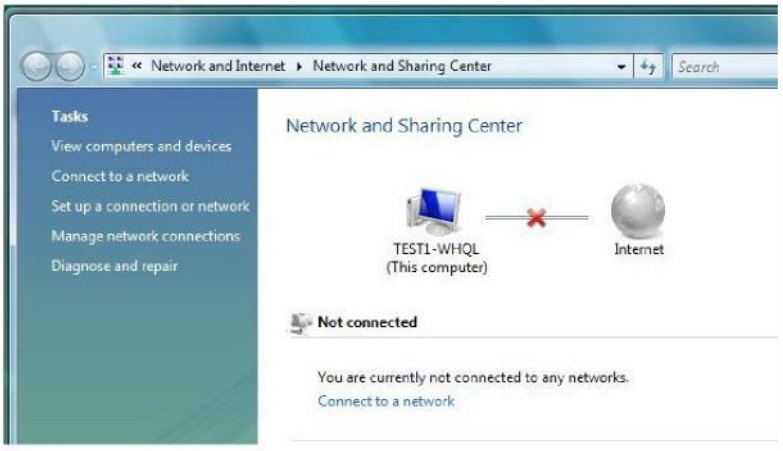
Configuring PC in Windows Vista

1. Go to Start. Click on Network.

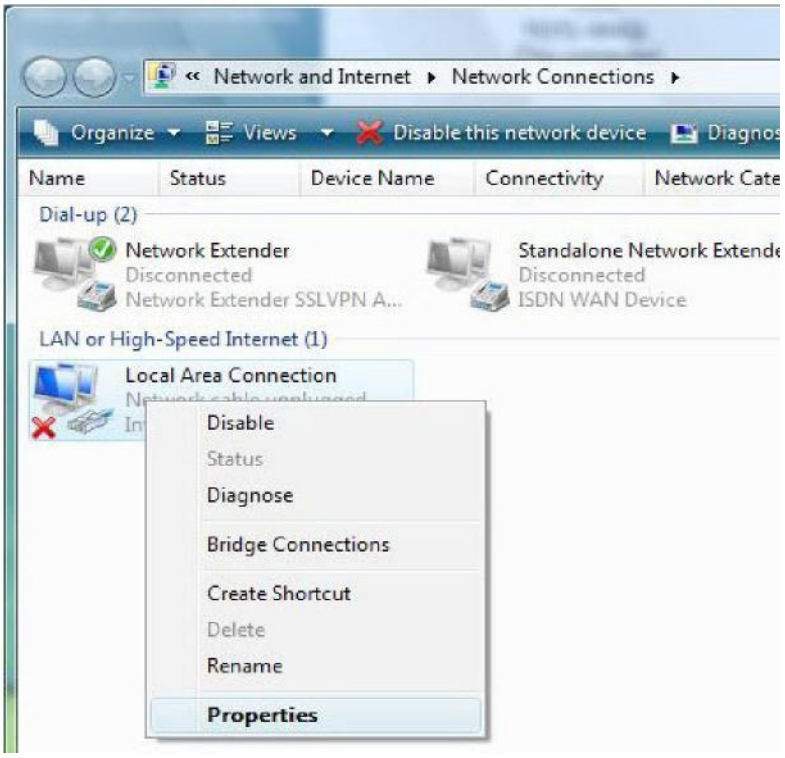
2. Then click on Network and Sharing Center at the top bar.



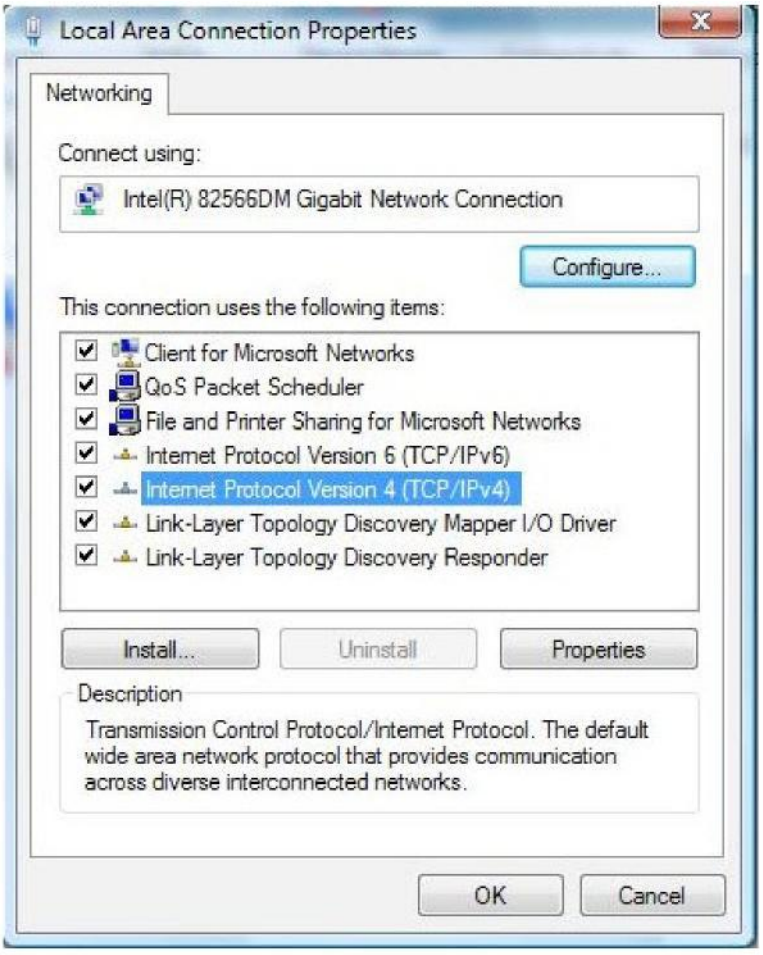
3. When the Network and Sharing Center window pops up, select and click on Manage network connections on the left window column.



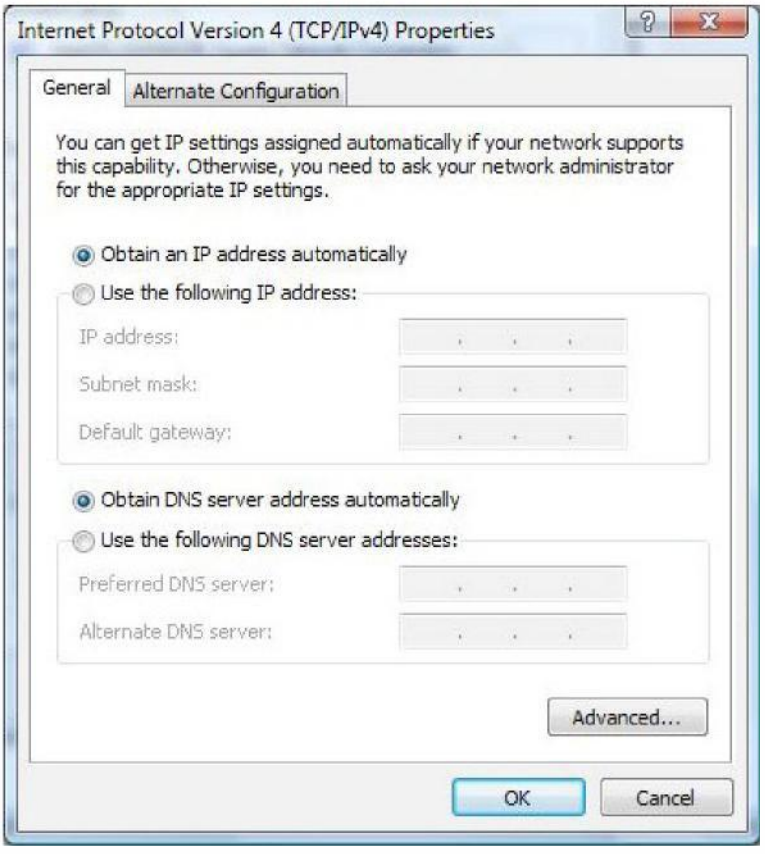
4. Select the Local Area Connection, and right click the icon to select Properties.



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



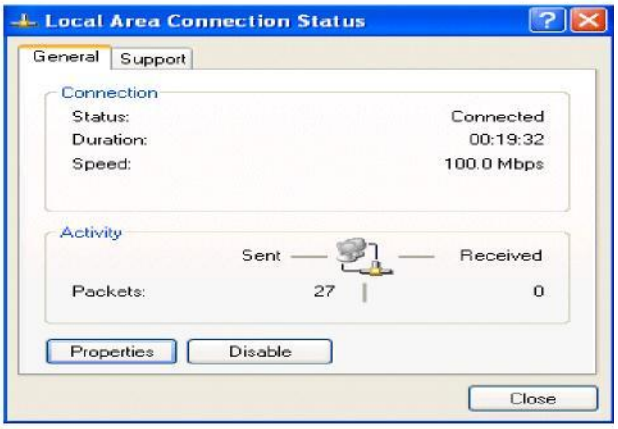
6. In the TCP/IPv4 properties window, select the Obtain an IP address automatically and Obtain DNS Server address automatically radio buttons. Then click OK to exit the setting.
7. Click OK again in the Local Area Connection Properties window to apply the new configuration.



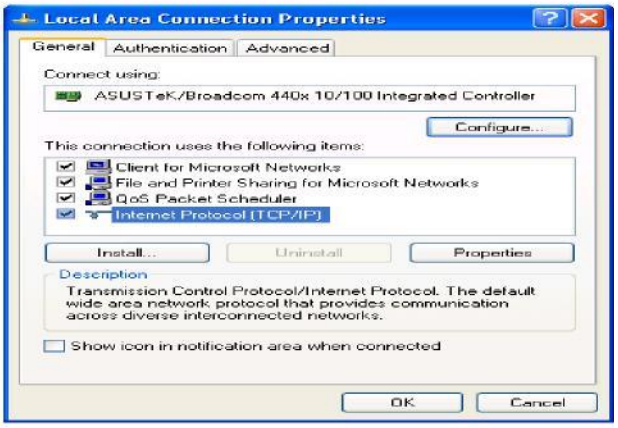
Configuring PC in Windows XP

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

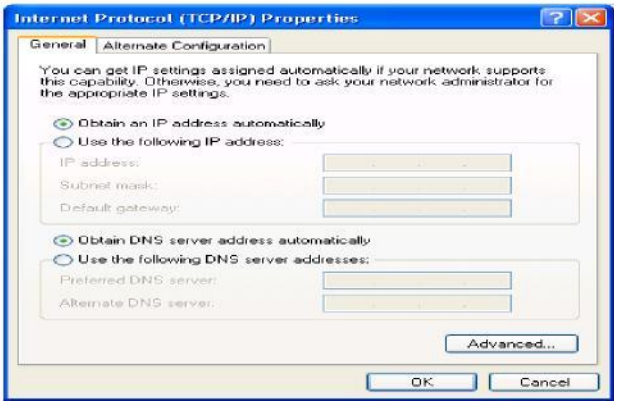
3. In the Local Area Connection Status window, click Properties.



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

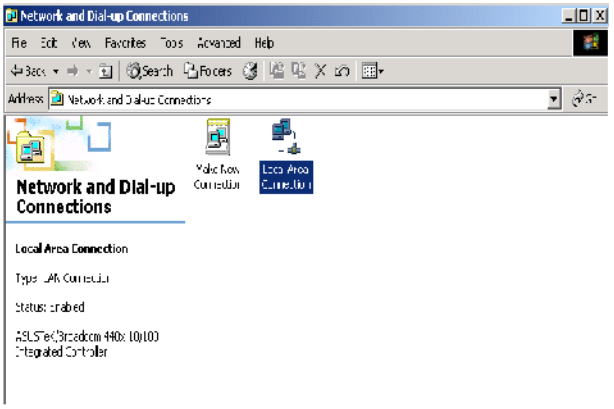


5. Select the Obtain an IP address automatically and the Obtain DNS server address automatically radio buttons.
6. Click OK to finish the configuration.

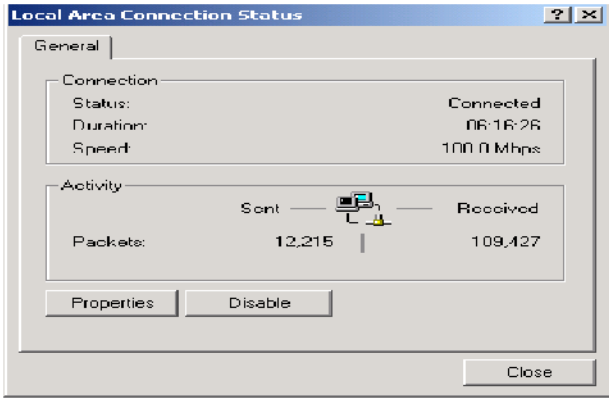


Configuring PC in Windows 2000

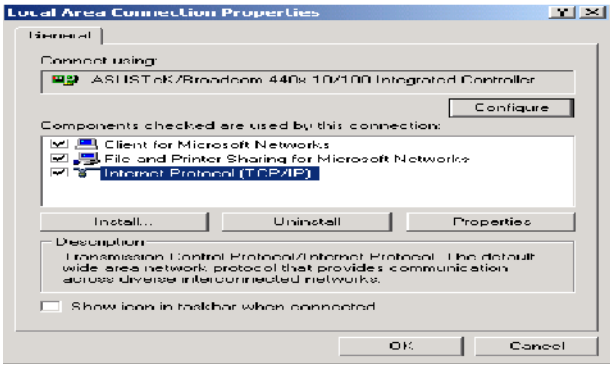
1. Go to Start > Settings > Control Panel. In the Control Panel, double-click on Network and Dial-up Connections.
2. Double-click Local Area Connection.



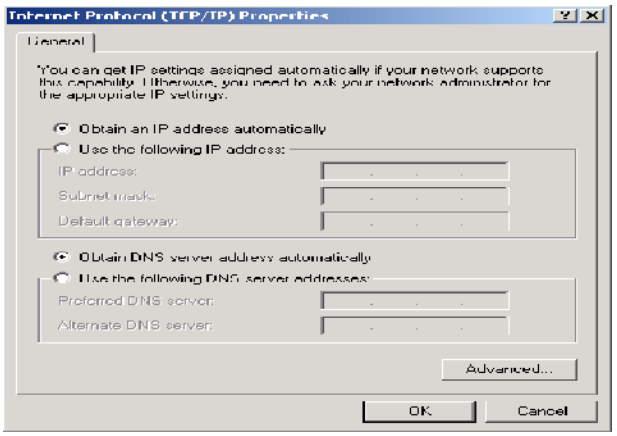
3. In the Local Area Connection Status window click Properties.



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

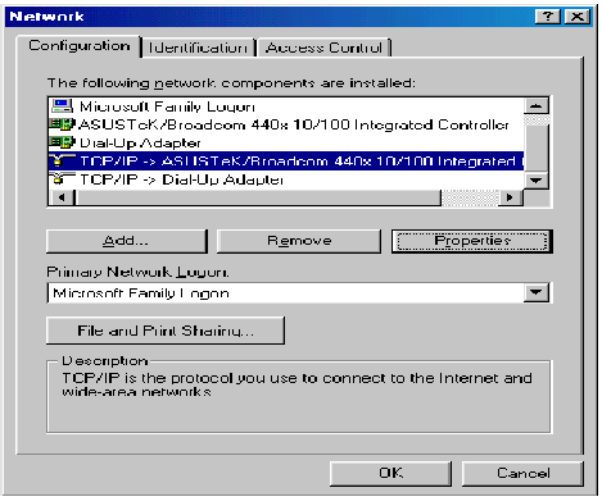


5. Select the Obtain an IP address automatically and the Obtain DNS server address automatically radio buttons.
6. Click OK to finish the configuration.

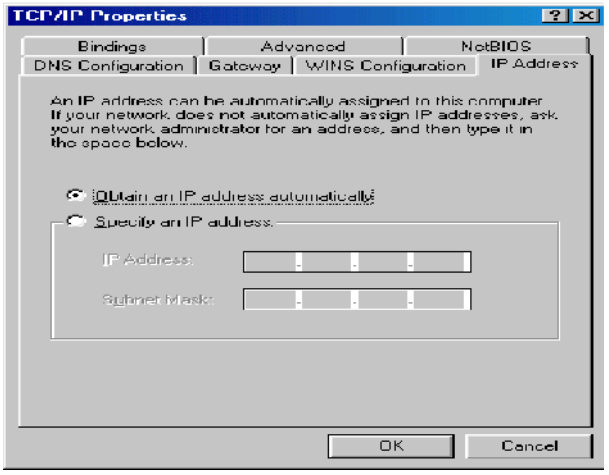


Configuring PC in Windows 95/98/Me

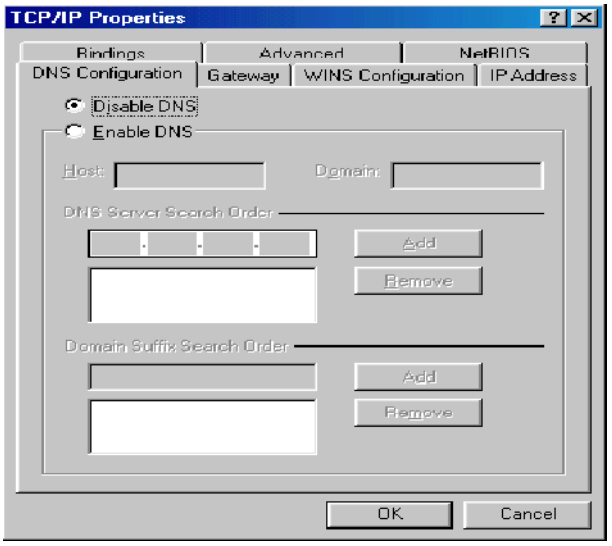
1. Go to Start > Settings > Control Panel. In the Control Panel, double-click on Network and choose the Configuration tab.
2. Select TCP/IP > NE2000 Compatible, or the name of your Network Interface Card (NIC) in your PC.



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

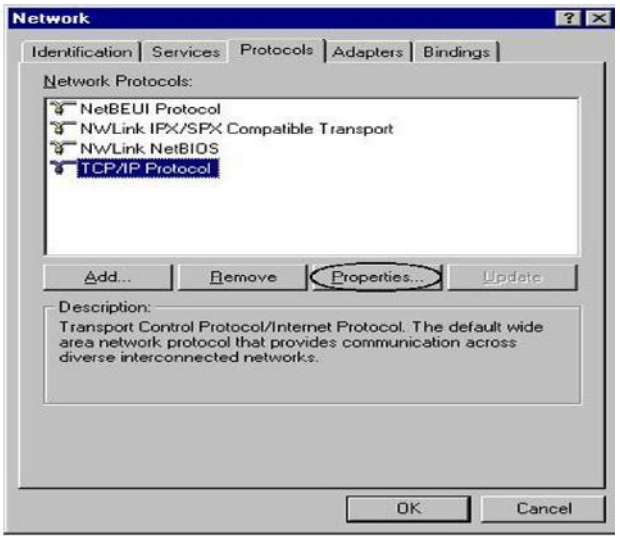


4. Then select the DNS Configuration tab.
5. Select the Disable DNS radio button and click OK to finish the configuration.

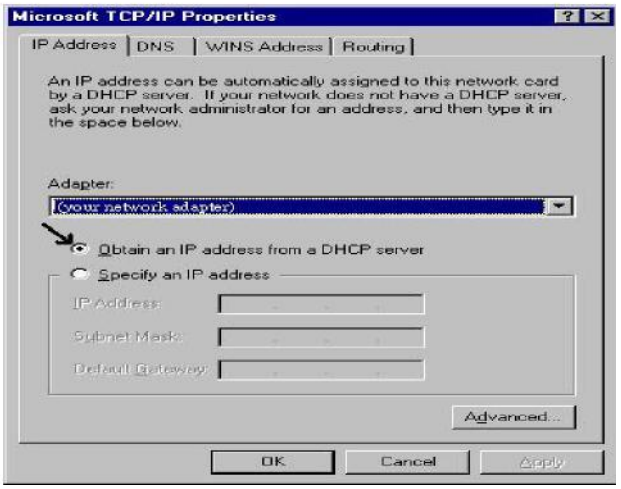


Configuring PC in Windows NT4.0

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 your 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 have forgotten your username or password for the router, you can restore your device to its default setting by pressing the Reset button for more than 1 second.

Device LAN IP settings

- IP Address: 192.168.0.254
- Subnet Mask: 255.255.255.0

ISP setting in WAN site

- PPPoE **DHCP server**

  DHCP server is enabled.

- Start IP Address: 192.168.0.100
- IP pool counts: 100
-

LAN and WAN Port Addresses

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

LAN Port		WAN Port
IP address	192.168.0.254	The PPPoE function is enabled to automatically get the WAN port configuration from the ISP.
Subnet Mask	255.255.255.0	
DHCP server function	Enabled	
IP addresses for distribution to PCs	100 IP addresses continuing from 192.168.0.100 through 192.168.0.200	

Information from your ISP

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

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

PPPoE(RFC2516)	VPI/VCI, VC / LLC-based multiplexing, Username, Password, Service Name, and Domain Name System (DNS) IP address (it can be automatically assigned by your ISP when you connect or be set manually).

Chapter 4: Configuration

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

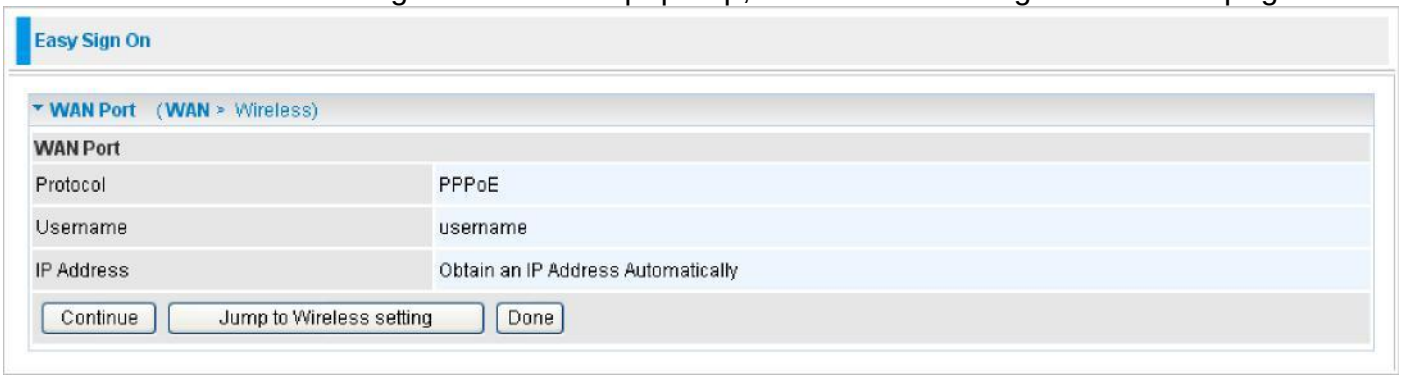
Easy Sign-On (EZSO)

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

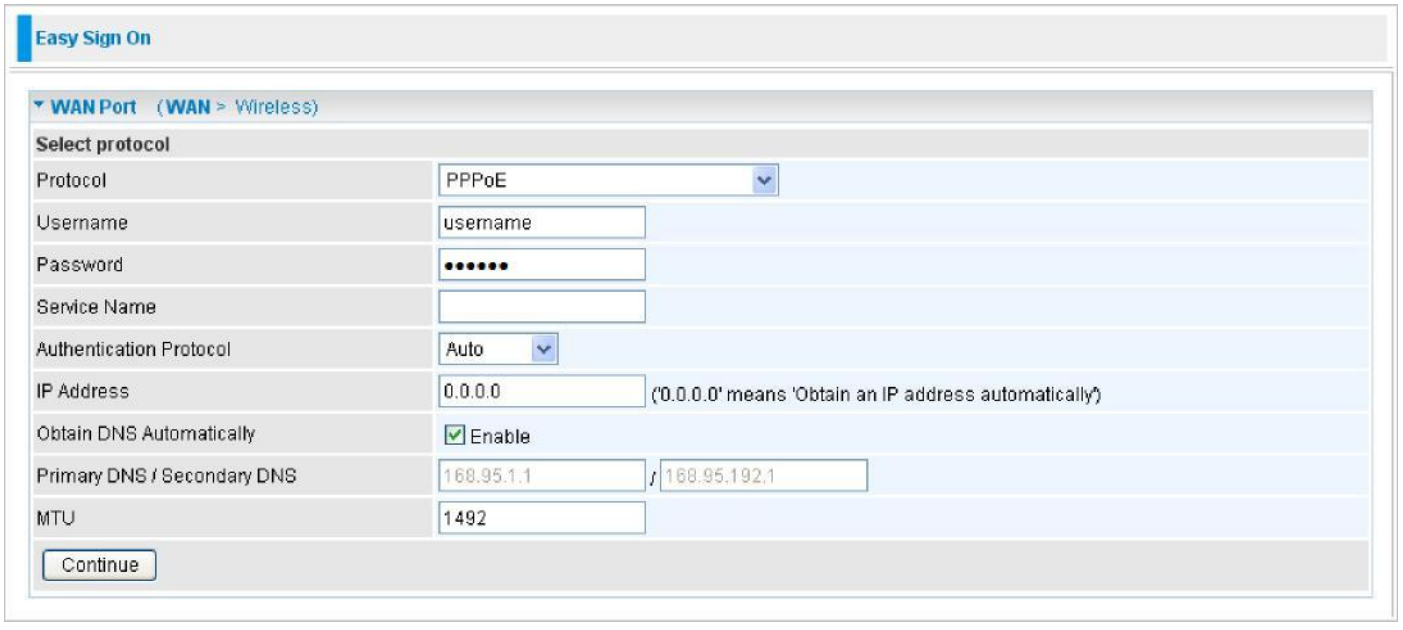
After setting up the router with all the appropriate cables plugged-in, open up your IE browser, the EZSO WEB GUI will automatically pop up and request that you enter some basic information That you have obtained from your ISP. By following the instructions given carefully and through the information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

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

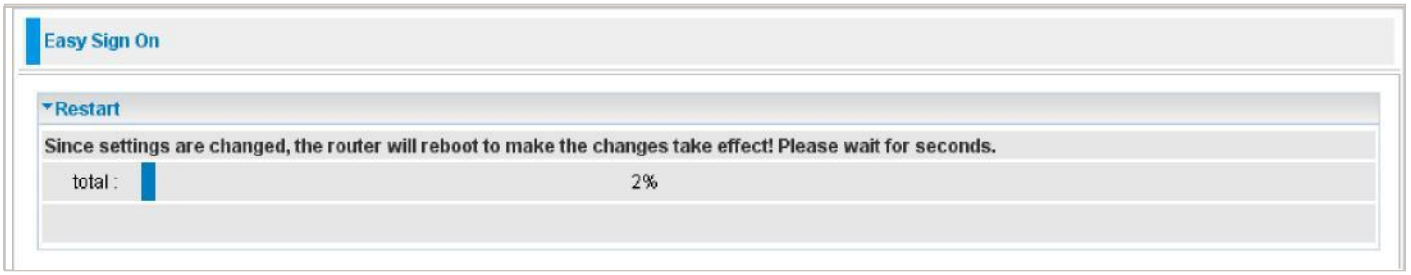
1. Connect your router with all the appropriate cables. Then, load your IE / Netscape browser.
2. When the EZSO configuration wizard pops up, click Continue to go to the next page.

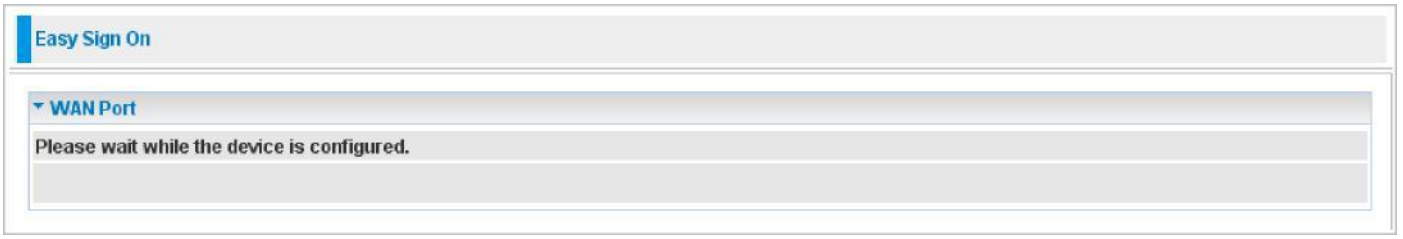


3. Please enter all the information in the blanks provided and then click Continue.

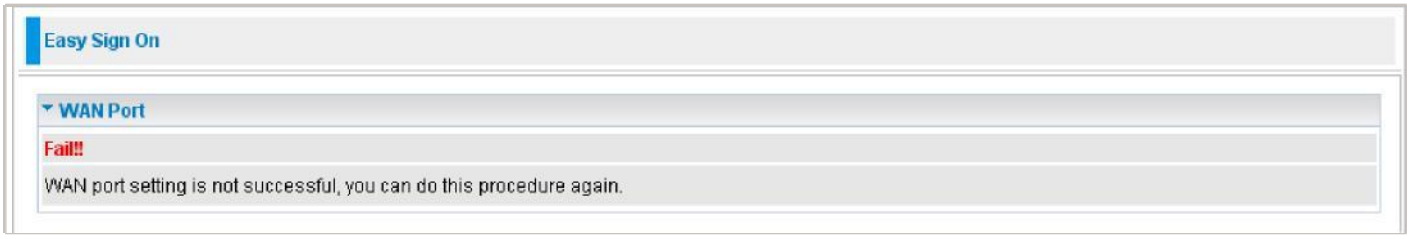


4. The device will reboot and then load the new configuration.

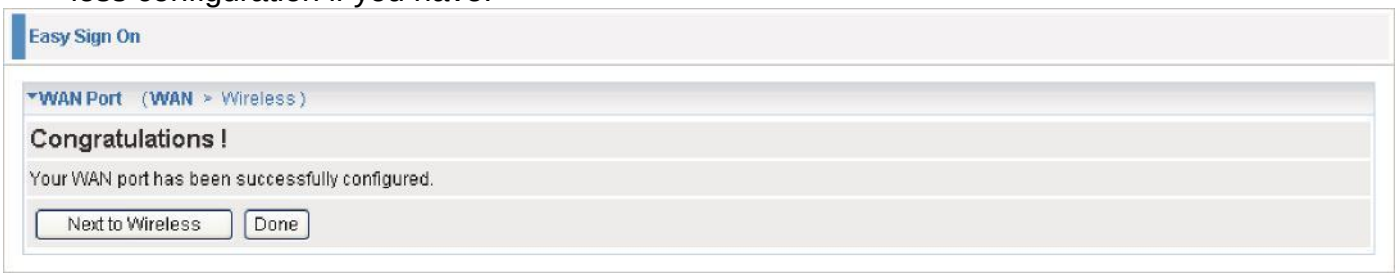




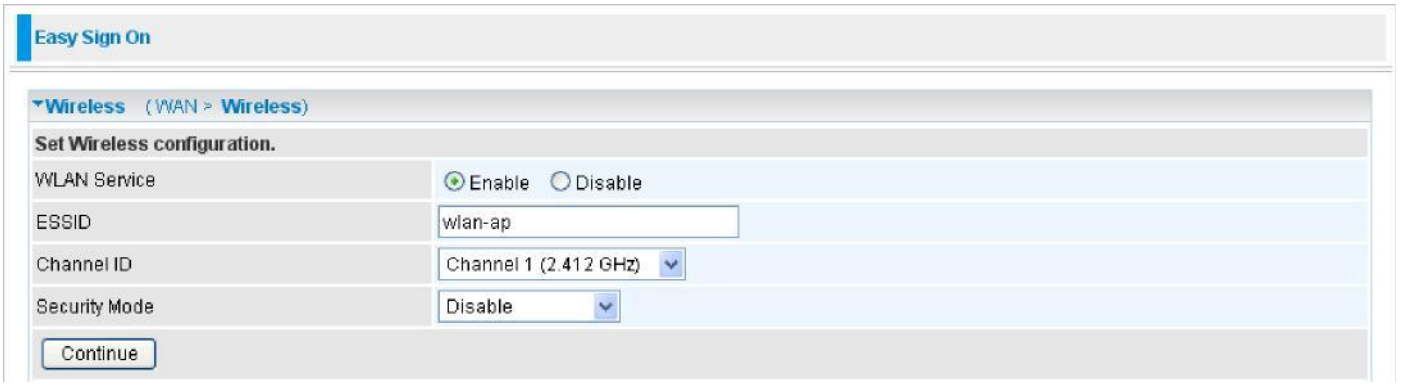
Note: If any error occurs during device configuration that results in WAN connection failure, the system will prompt that the setup has failed.



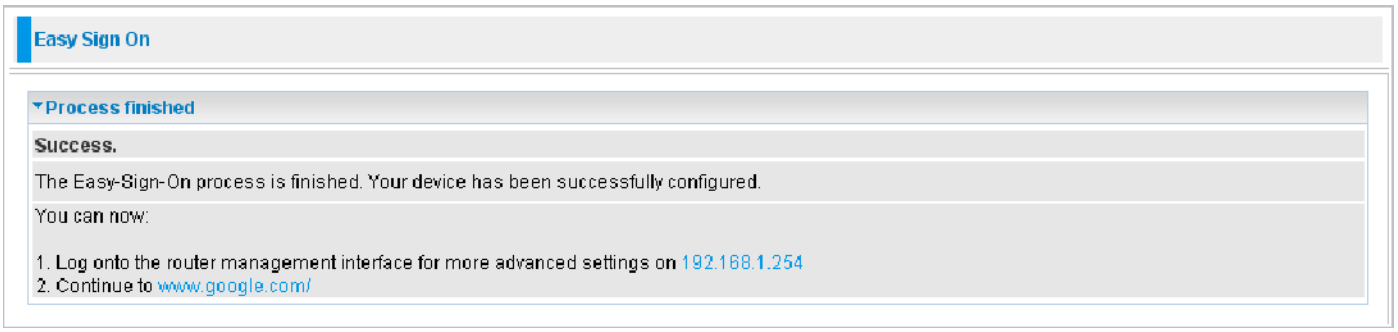
5. If all information provided is valid and the device successfully connects to WAN, a dialog box will appear to signify the completion of the WAN port setup. At this point you can either click done to finish the EZSO configuration or you can click Next to wireless to proceed to the wireless configuration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



6. Select Enable and enter the necessary information in the blanks provided for the Wireless LAN setting (wireless setting is only available for 802.11n Fiber Optical Router) if you would like to use this feature and then click Continue.



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

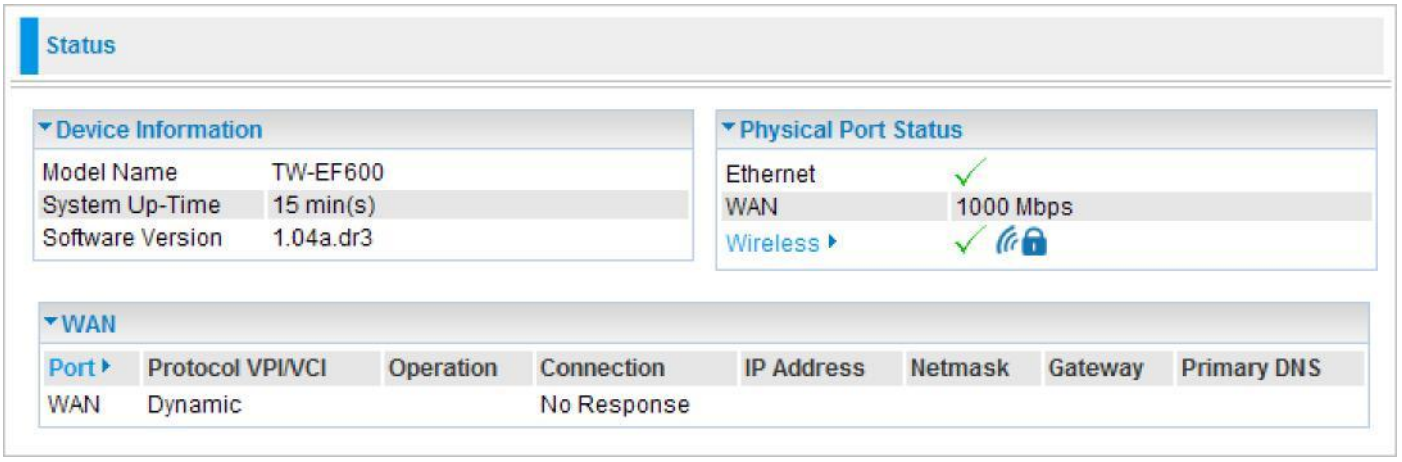


Configuration via Web Interface

Open your web browser; enter the IP address of your router, which by default is 192.168.0.254, and click “Go”, a login window prompt will appear. The default username and password are “admin” and “admin” respectively.

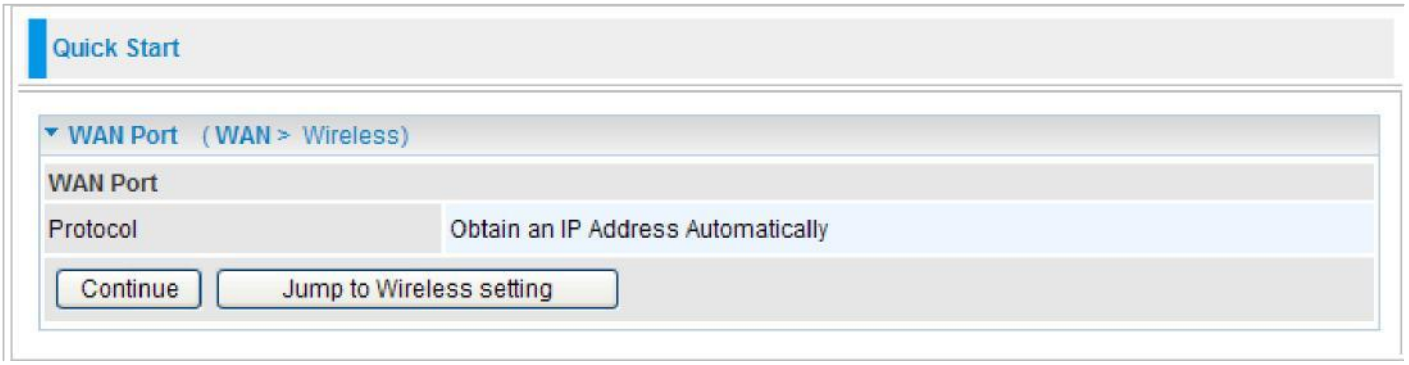
Congratulations! You are now successfully logon to the Router!

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

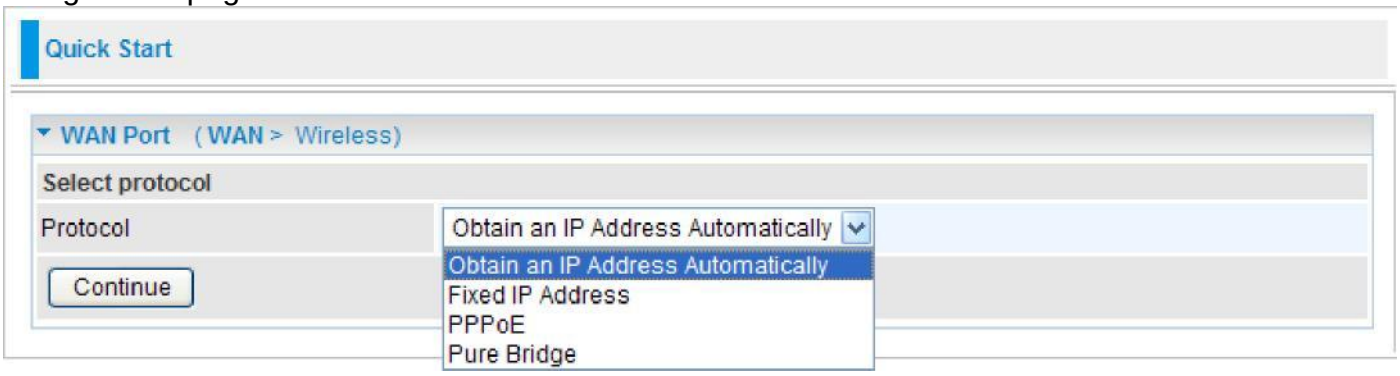


Quick Start

Whether on the Basic or Advanced Configuration Mode, click Quick Start link to WAN Port setup pages.

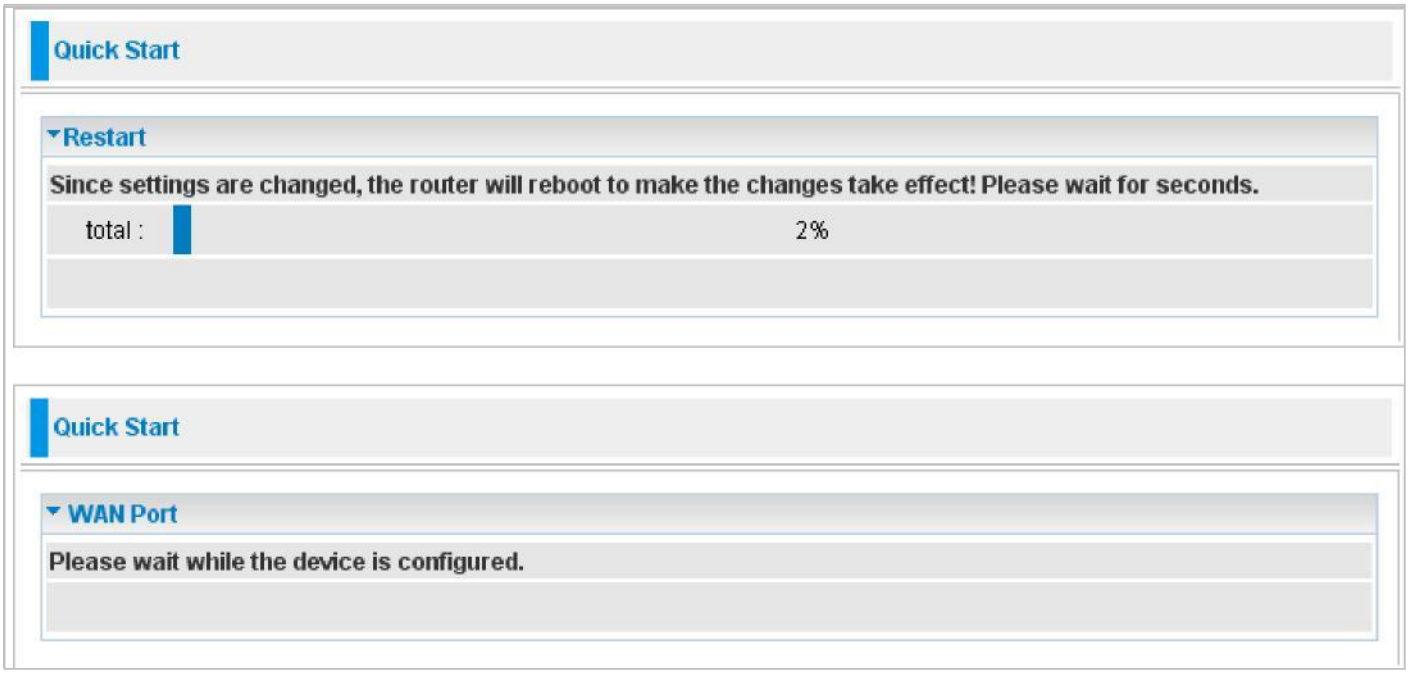


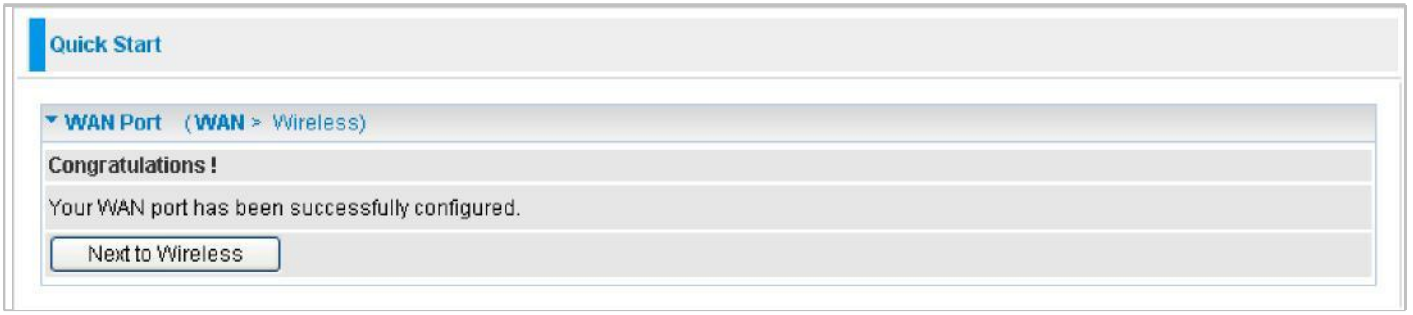
Step 1: This screen displays some information for WAN port. Press Continue to go to the next configuration page.



Step 2: There are 3 types of connection protocols available for WAN connect mode. ***Each type of connection mode is described in the following sections of WAN Connect mode.***

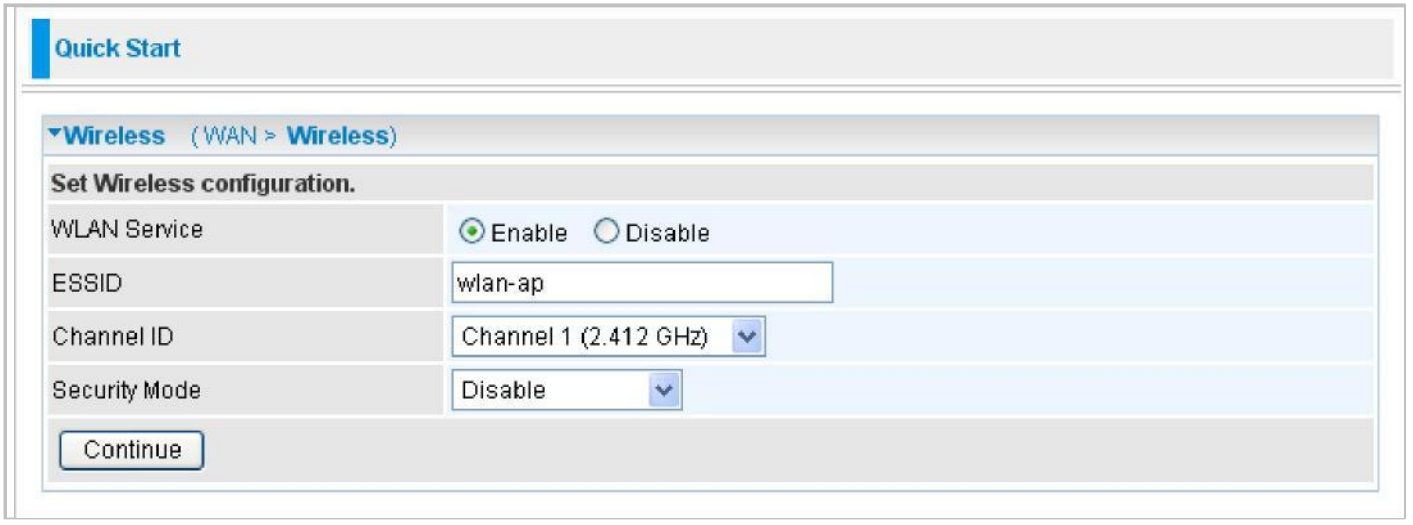
Step 3: After finishing configuring the WAN port connection, click Continue to proceed. The system will upload and apply the new WAN port configuration to the device.





Note: If the WAN line is not ready, a page will display as below and your new configuration can not be saved.

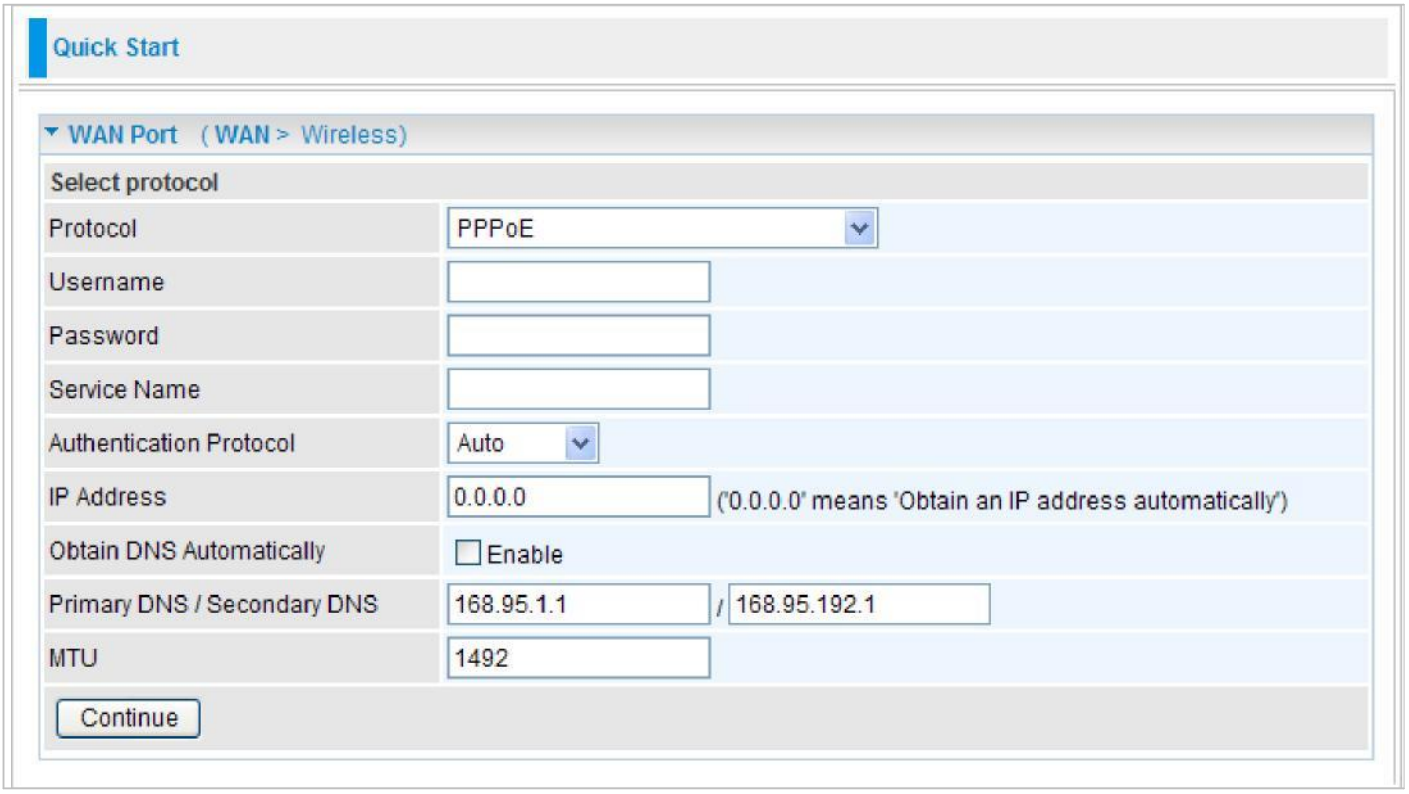
Step 4: After the configuration is successful, click Next to Wireless button and you may proceed to configure the Wireless setting. There are 4 types of security mode: WPA, WPA2, and WPA/ WPA2 Pre-Shared Key and WEP. Please refer to the **Wireless Setting Mode** section for detail description of each security mode.



Step 5: After finishing configuring the WLAN setting, press Continue to finish the Quick Start.

WAN Connect Mode

PPPoE connection



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

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

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

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

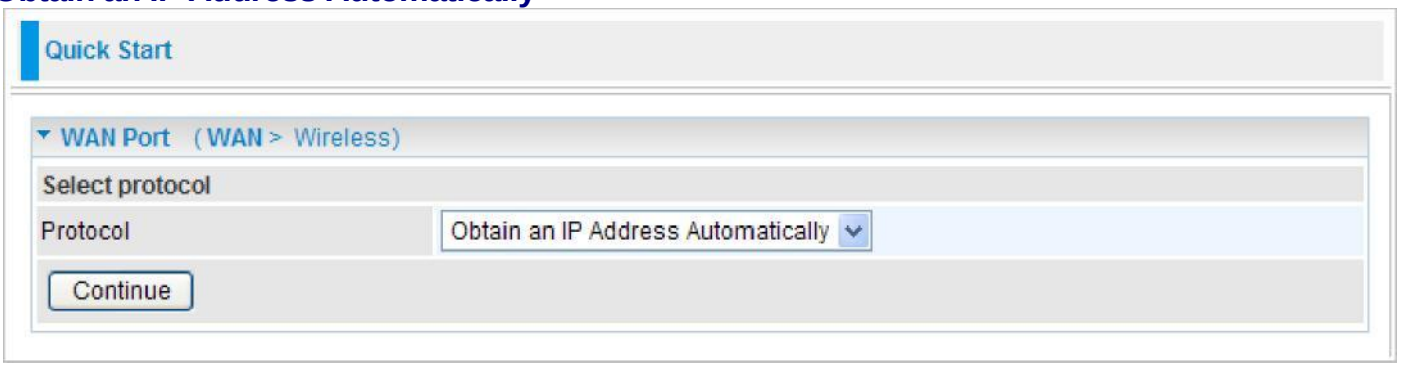
IP Address: Enter your fixed IP address.

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

Primary DNS / Secondary DNS: Available when **Obtain DNS automatically** is disable. Enter the IP addresses of the DNS servers. The DNS servers are passed to the DHCP clients along with the IP address and the net mask.

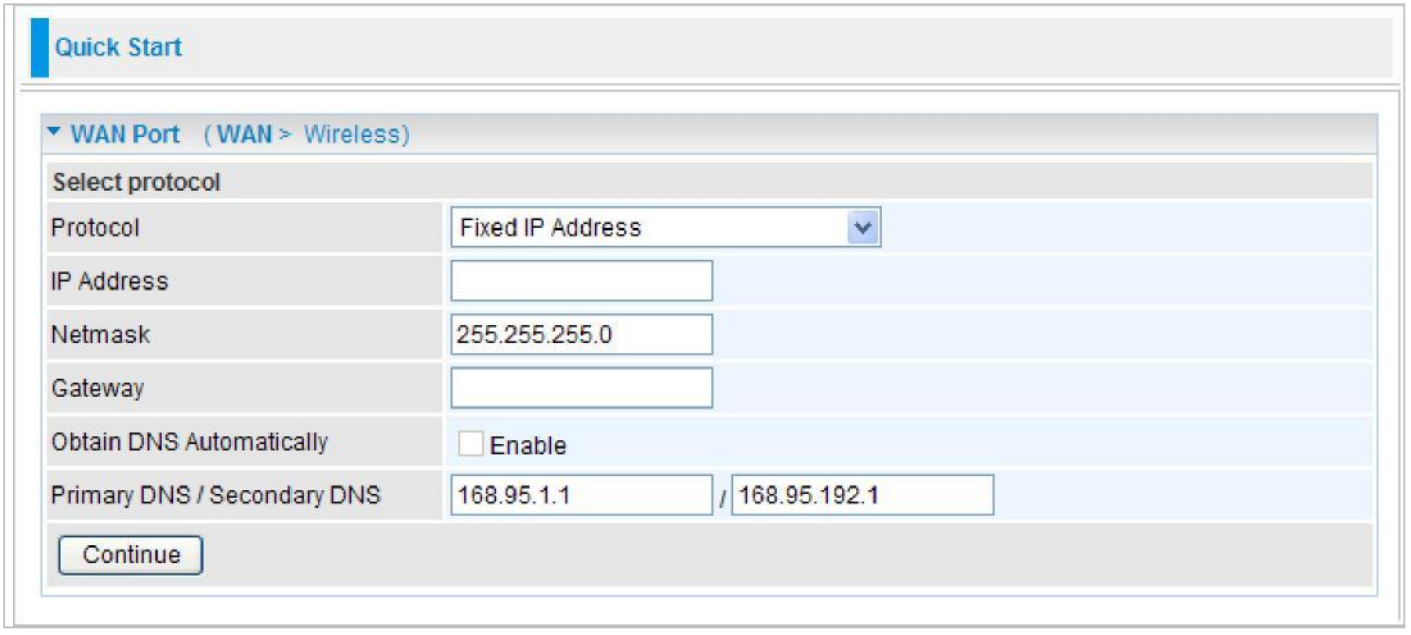
MTU: Maximum Transmission Unit. The size of the largest datagram (excluding media-specific headers) that IP will attempt to send through the interface.

Obtain an IP Address Automatically



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

Fixed IP Address



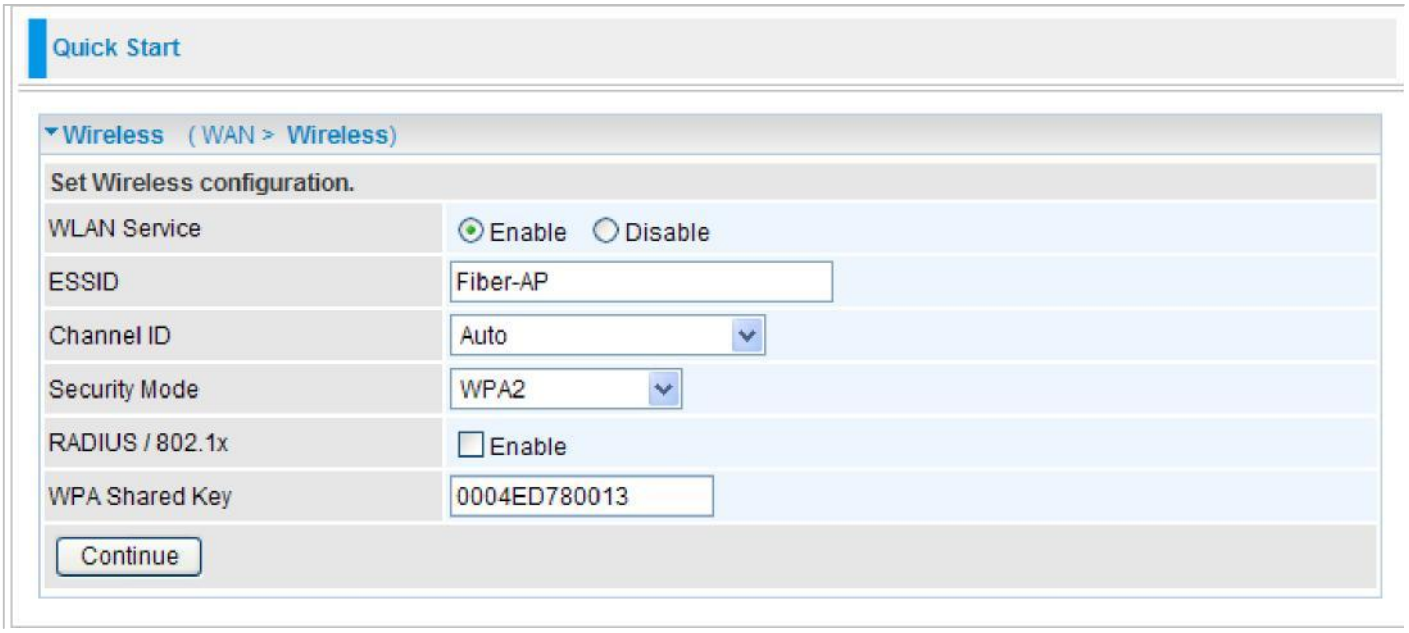
Net mask: User can change it to others such as 255.255.255.128. Type the net mask assigned to you by your ISP (if given).

Gateway: Enter the IP address of the default gateway.

Pure Bridge

Wireless Setting Mode

WPA / WPA2



WLAN Service: Default setting is Enable. If you want to use wireless, you can select Enable.

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

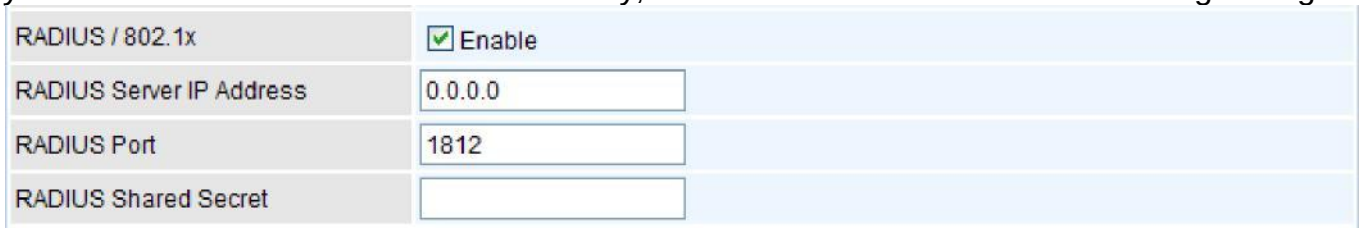
Channel ID: Select the channel ID that you would like to use.

Security Mode: You can disable or enable with WPA or WEP to protect wireless network.

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

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

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



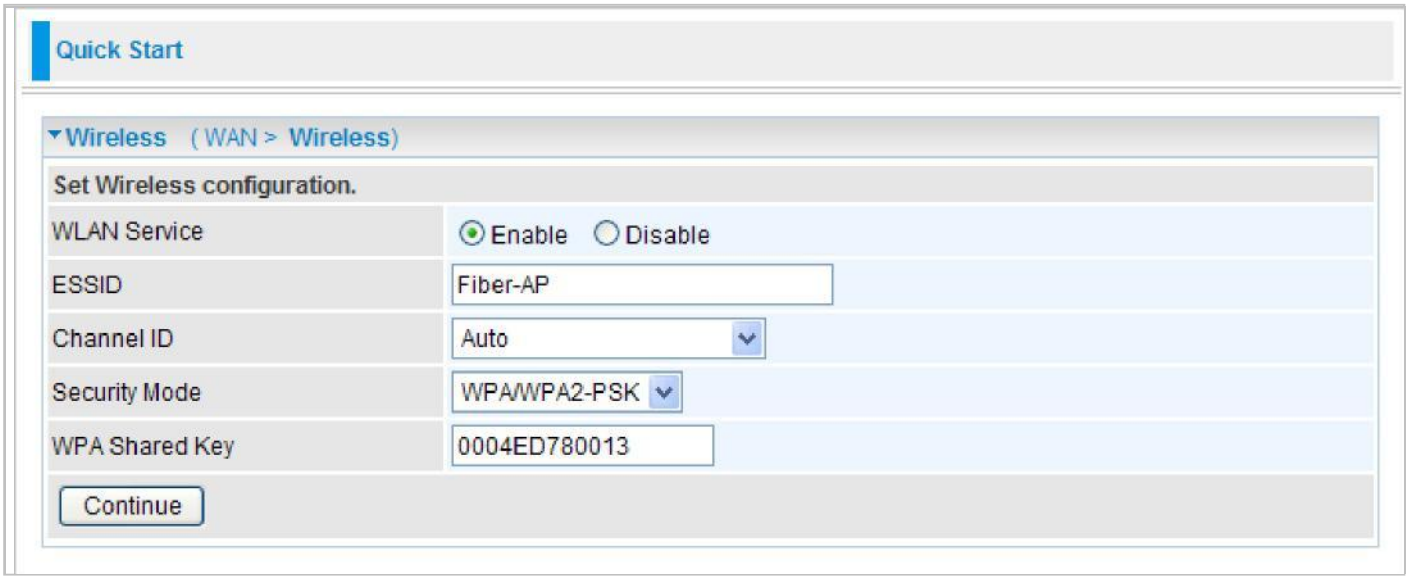
RADIUS Server IP Address: The IP address of RADIUS authentication server.

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

RADIUS Shared Secret: The password of RADIUS authentication server.

WPA/WPA2-PSK

WPA and WPA2 pre-shared keys are authentication mechanisms in which users provide some form of credentials to verify that they should be allowed access to a network. This requires a single password entered into each WLAN node (Access Points, Wireless Routers, client adapters, bridges). As long as the passwords match, a client will be granted access to a WLAN.



WLAN Service: Default setting is Enable. If you want to use wireless, you can select Enable.

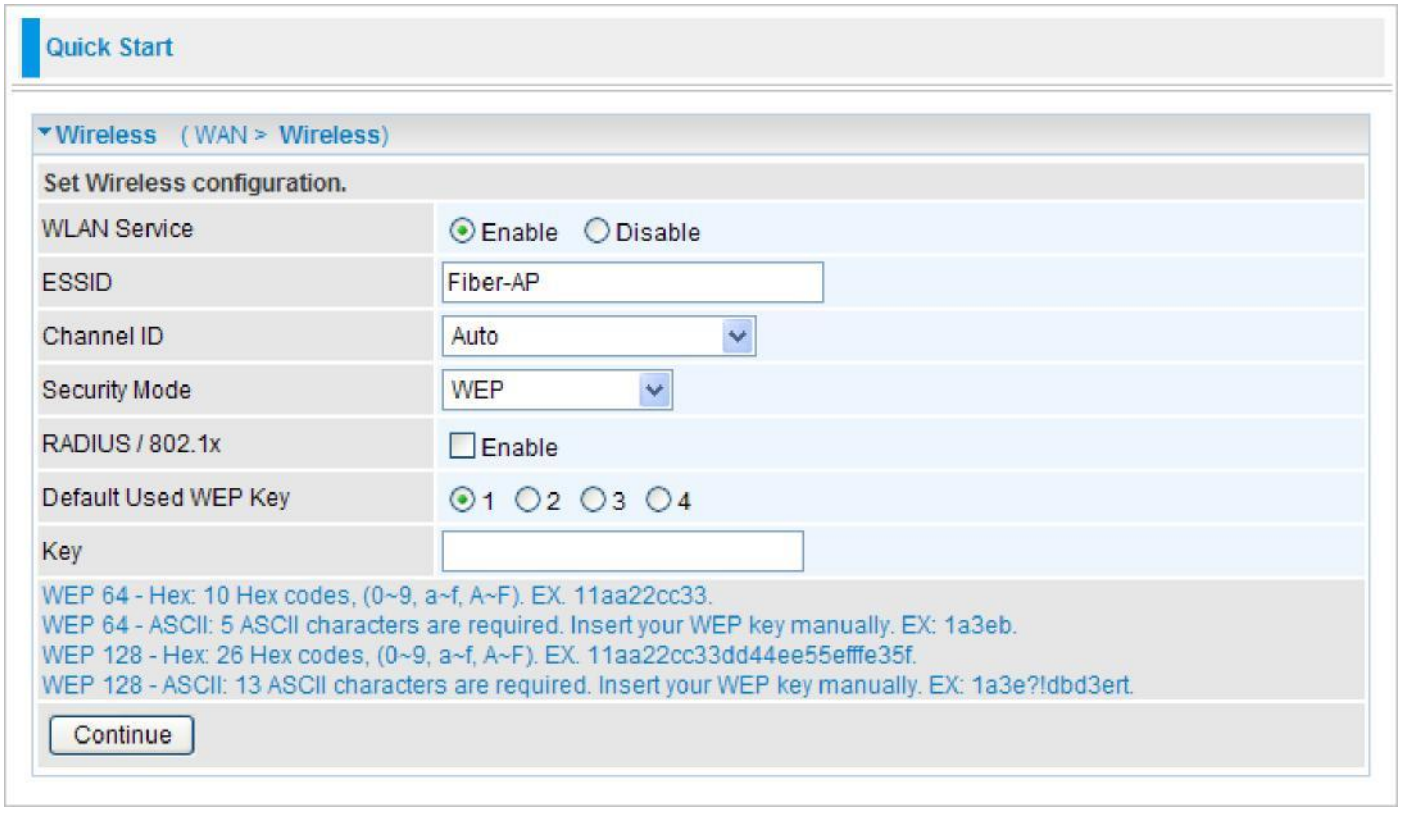
ESSID: The ESSID is the unique name of a wireless access point (AP) used to distinguish one from another. For security propose, change to a unique ID name which is already built into the router wireless interface. It is case sensitive and must not exceed 32 characters. Make sure your wireless clients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

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

Security Mode: You can disable or enable with WPA or WEP to protect wireless network.

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.

WEP



WLAN Service: Default setting is set to enable. If you want to use wireless, you can select Enable.

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

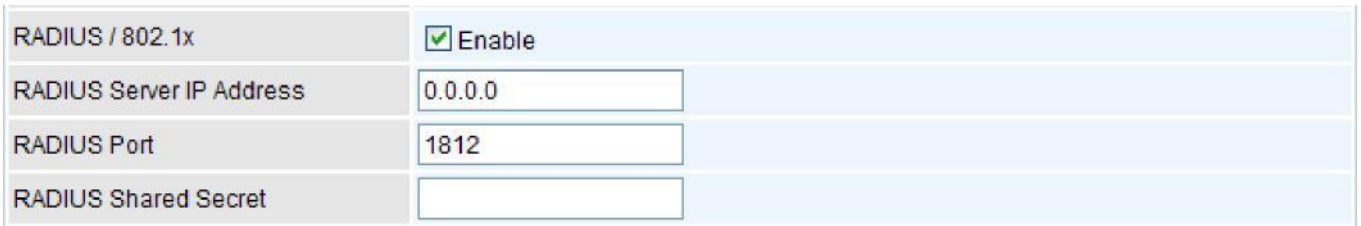
Channel ID: Select the channel ID that you would like to use.

Security Mode: You can disable or enable with WPA or WEP to protect wireless network.

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

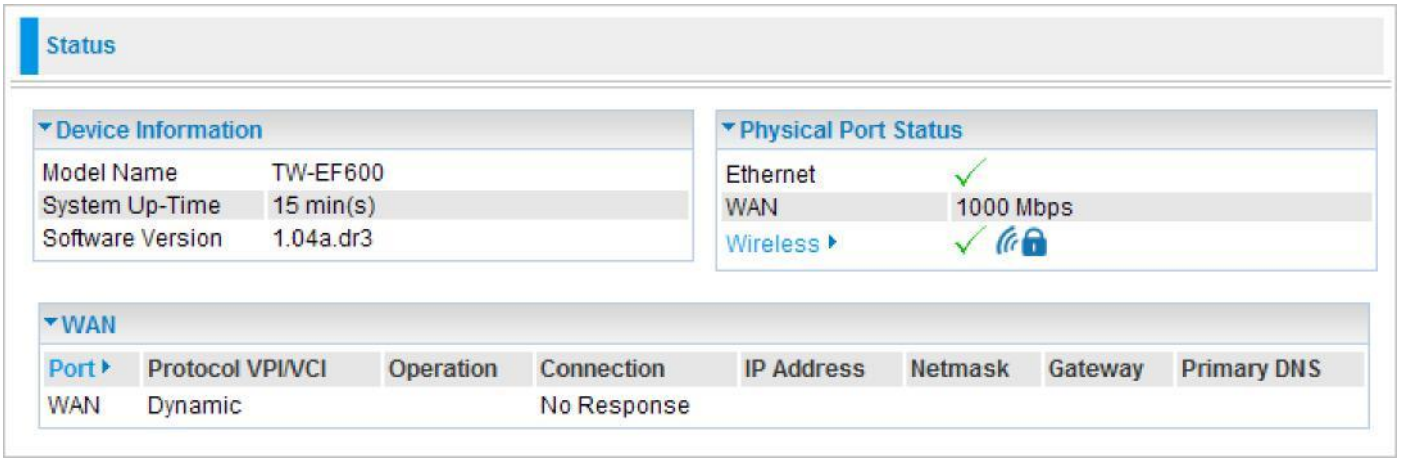
Key (1-4): Enter the key to encrypt wireless data. To allow encrypted data transmission, the WEP Encryption Key values on all wireless stations must be the same as the router. There are four keys for your selection. The input format can either be HEX style or ASCII format, 10 and 26 HEX codes or 5 and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

If you want to enable the RADIUS functionality, check Enable and then do the following settings as WPA/WPA2.



Basic Configuration Mode

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.

Physical Port Status

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

WAN

Port: Name of the WAN connection.

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

Operation: Current status in WAN interface.

Connection: Current connection status.

IP Address: WAN port IP address.

Net mask: WAN port IP subnet mask.

Gateway: IP address of the default gateway.

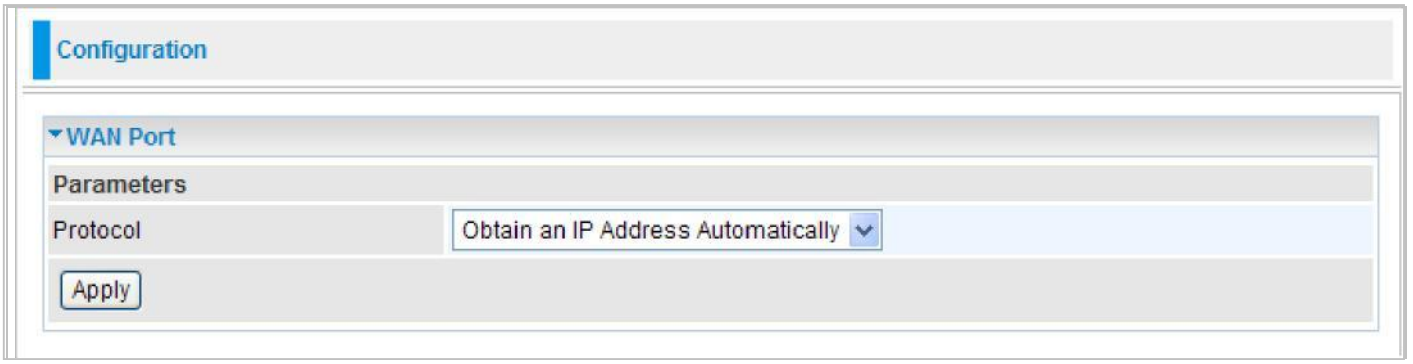
Primary DNS: IP address of the primary DNS server.

WAN

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

Obtain IP Address Automatically

By configuring these settings, the device is able to obtain IP settings automatically from the ISP.

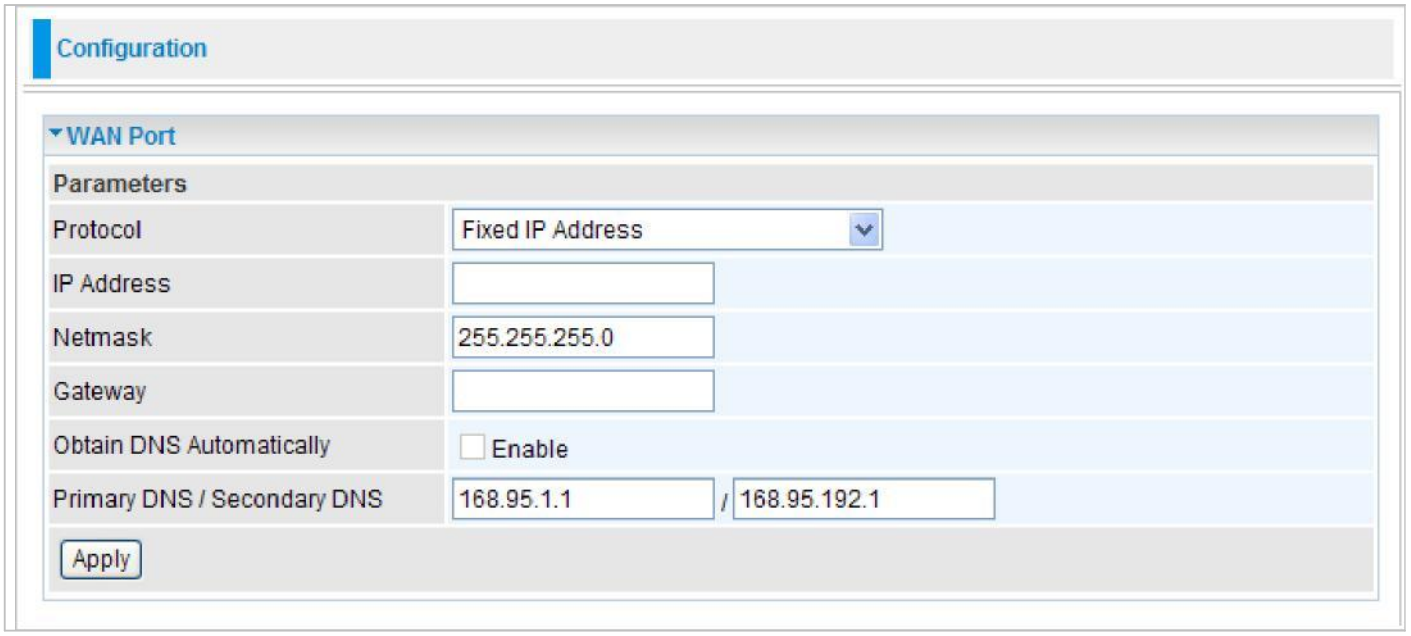


Protocol: Select the protocol you will use in the device.

Click Apply to confirm the settings.

Fixed IP Address

A Static WAN connection will be configured according to the IP properties defined by your ISP.



IP Address: Enter your fixed IP address.

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

Gateway: Enter the IP address of the default gateway (if given).

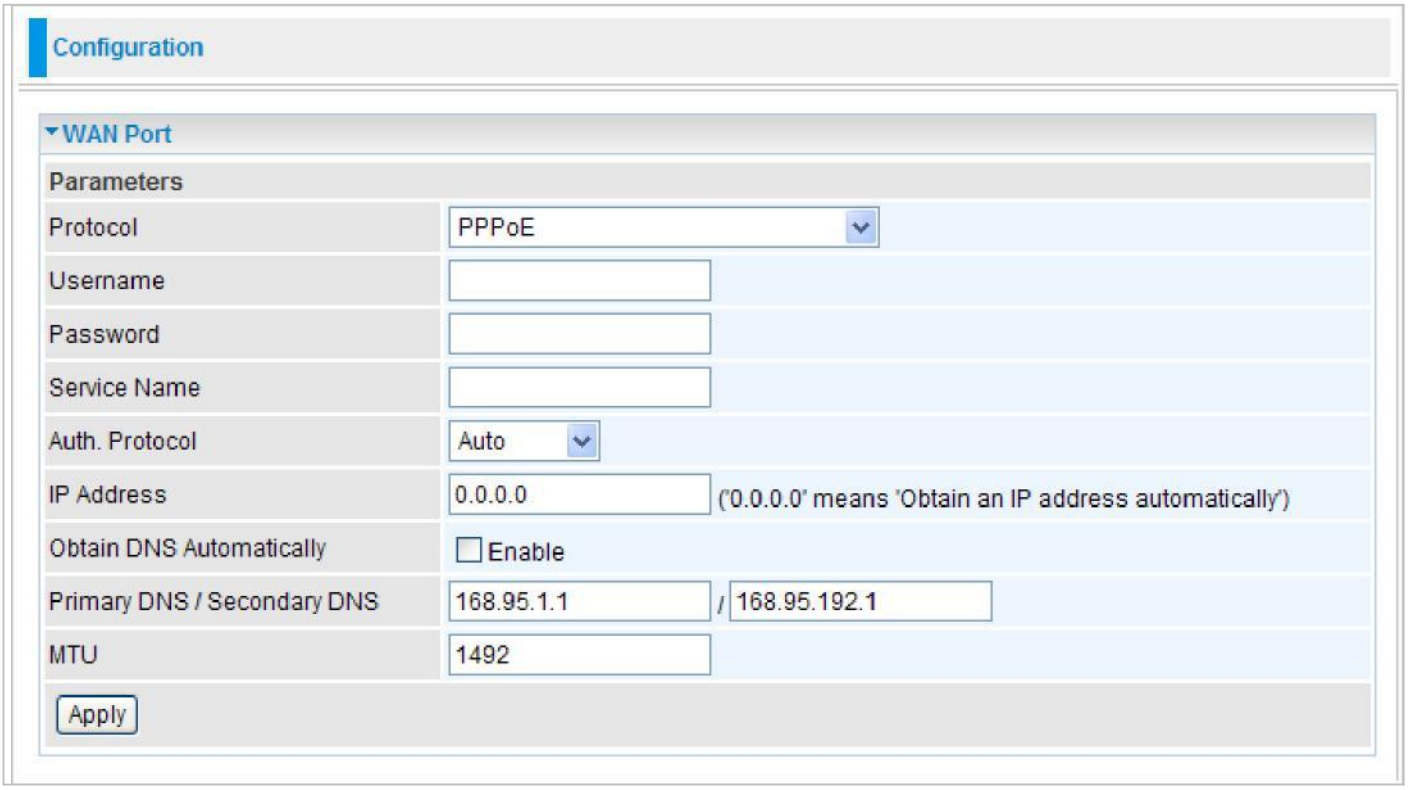
Obtain DNS automatically: Click to activate DNS and to enable the system to automatically detect DNS.

Primary DNS / Secondary DNS: Available when **Obtain DNS automatically** is disable. Enter the IP addresses of the DNS servers. The DNS servers are passed to the DHCP clients along with the IP address and the netmask.

Click Apply to confirm the settings.

PPPoE

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



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

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

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

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

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

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

Primary DNS / Secondary DNS: Available when **Obtain DNS automatically** is disable. Enter the IP addresses of the DNS servers. The DNS servers are passed to the DHCP clients along with the IP address and the netmask.

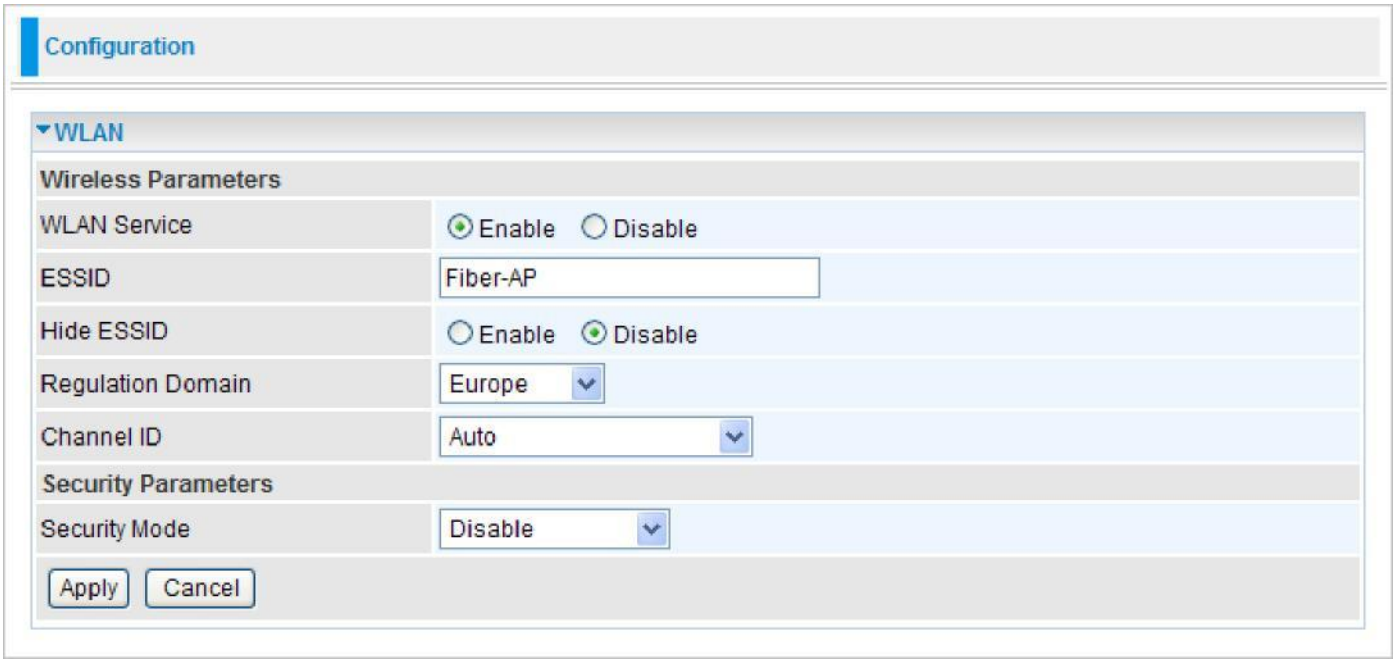
MTU: Maximum Transmission Unit. The size of the largest datagram (excluding media-specific headers) that IP will attempt to send through the interface.

Click Apply to confirm the settings.

Pure Bridge

Click Apply to confirm the settings.

WLAN



Wireless Parameters

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

ESSID: The ESSID is a unique name of a wireless access point (AP) used to distinguish one from another. For security purpose, change the default wlan-ap to a unique ID name that is already built into the router wireless interface. Make sure your wireless clients have exactly the ESSID as the device in order to connect to your network.

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

Hide ESSID: It is used to broadcast its ESSID on the network so that when a wireless client searches for a network, the router can be discovered and recognized. Default setting is Disable.

> **Enable:** When enabled, you do not broadcast your ESSID. Therefore, no one will be able to locate the Access Point (AP) of your router.
>
> **Disable:** When disabled, you allow anybody with a wireless client to be able to locate the Access Point (AP) of your router.

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

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

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

Security Parameters

Security Mode: You can disable or enable the function with WPA or WEP to protect the wireless network.

Click Apply to confirm the settings.

Security Mode

WPA / WPA2

Security Parameters	
Security Mode	WPA2
RADIUS / 802.1x	Enable
WPA Shared Key	0004ED780013
Group Key Renewal	3600 seconds

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

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

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

Group Key Renewal: The period of renewal time for changing the security key automatically between wireless client and Access Point (AP). Default value is 3600 seconds.

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

Security Mode	WPA2
RADIUS / 802.1x	Enable
Group Key Renewal	3600 seconds
RADIUS Server IP Address	0.0.0.0
RADIUS Port	1812
RADIUS Shared Secret	

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

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

RADIUS Shared Secret: The password of RADIUS authentication server.

WPA/WPA2 -PSK

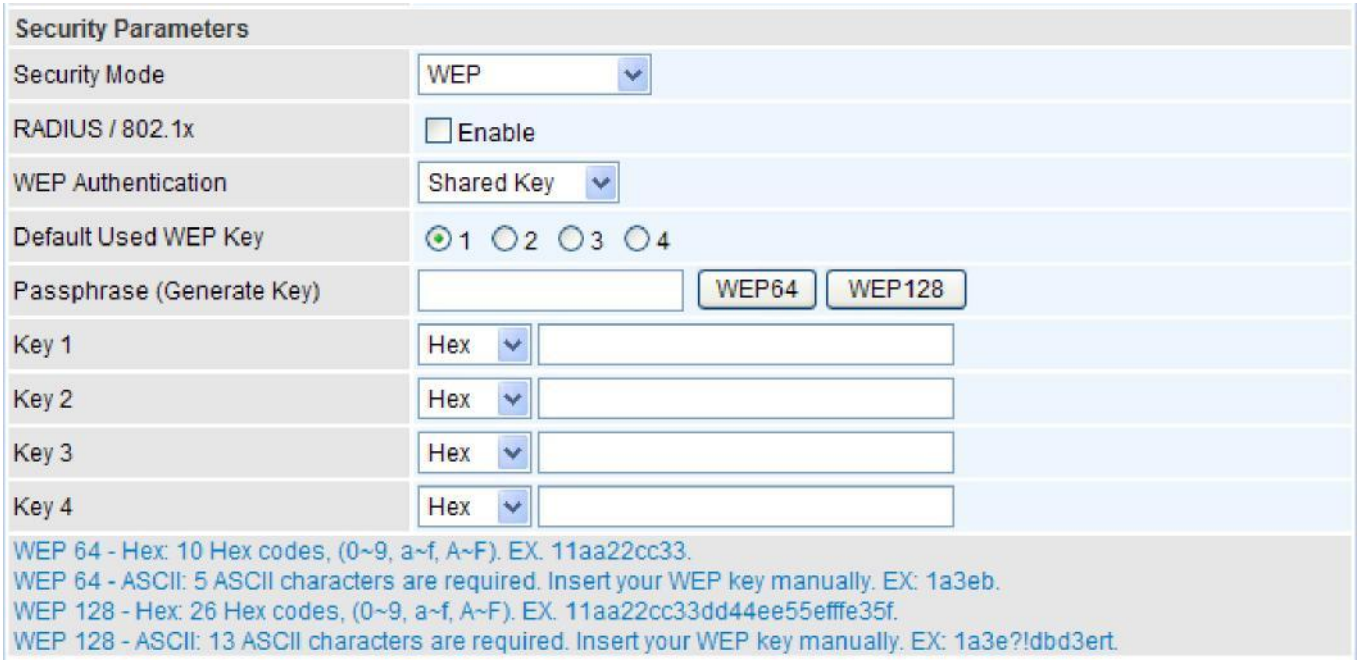
WPA Shared Key: The key for network authentication. The input format is in character style and

Security Parameters	
Security Mode	WPA/WPA2-PSK
WPA Shared Key	0004ED780013
Group Key Renewal	3600 seconds

key size should be in the range between 8 and 63 characters.

Group Key Renewal: The period of renewal time for changing the security key automatically between wireless client and Access Point (AP). Default value is 3600 seconds.

WEP



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

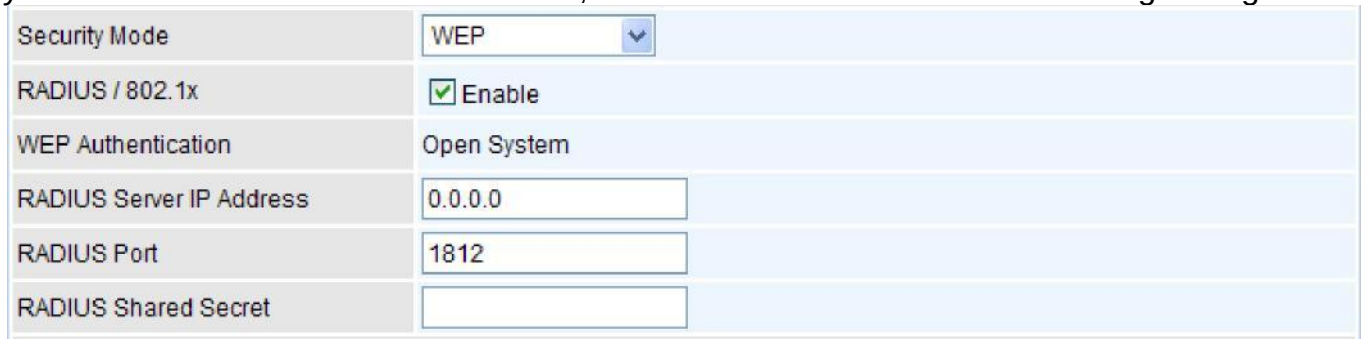
WEP Authentication: To prevent unauthorized wireless stations from accessing data transmitted over the network, the router offers secure data encryption, known as WEP. If you require high security for transmissions, there are 3 options to select from: **Open System, Share Key** and **Both**.

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

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

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

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



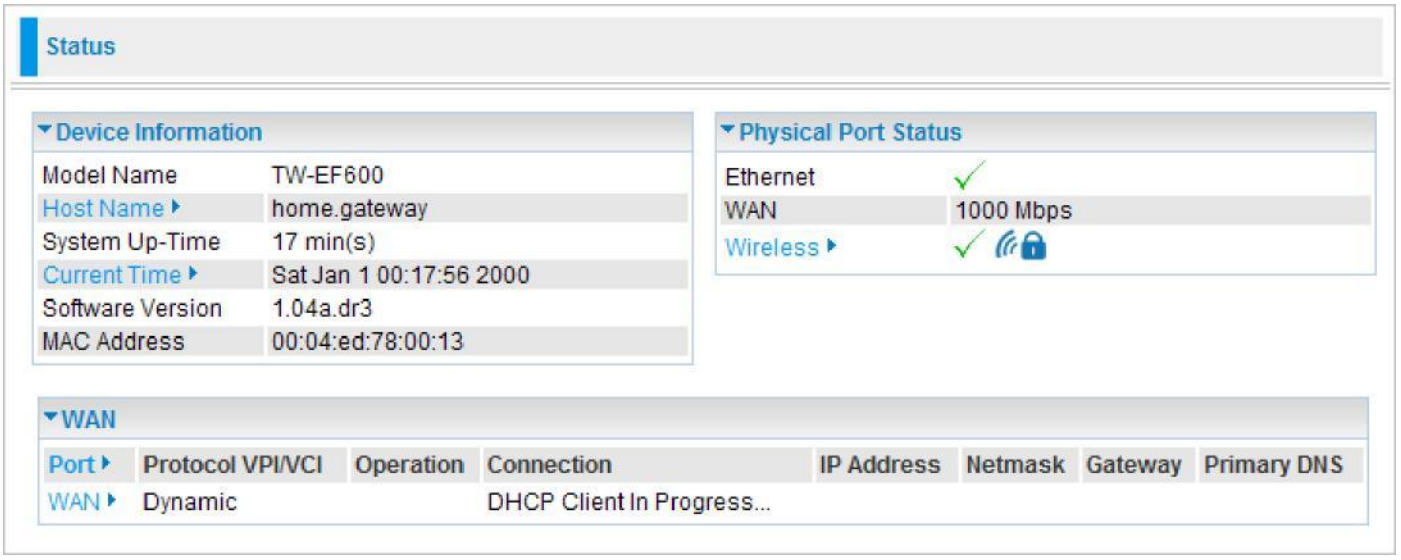
RADIUS Server IP Address: The IP address of RADIUS authentication server.

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

RADIUS Shared Secret: The password of RADIUS authentication server.

Advanced Configuration Mode

Status



Device Information

Model Name: Displays the model name.

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

System Up-Time: Records system up-time.

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

Software Version: Firmware version.

MAC Address: The LAN MAC address.

Physical Port Status

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

WAN

Port: Name of the WAN connection.

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

Operation: The current status in WAN interface.

Connection: The current connection status.

IP Address: WAN port IP address.

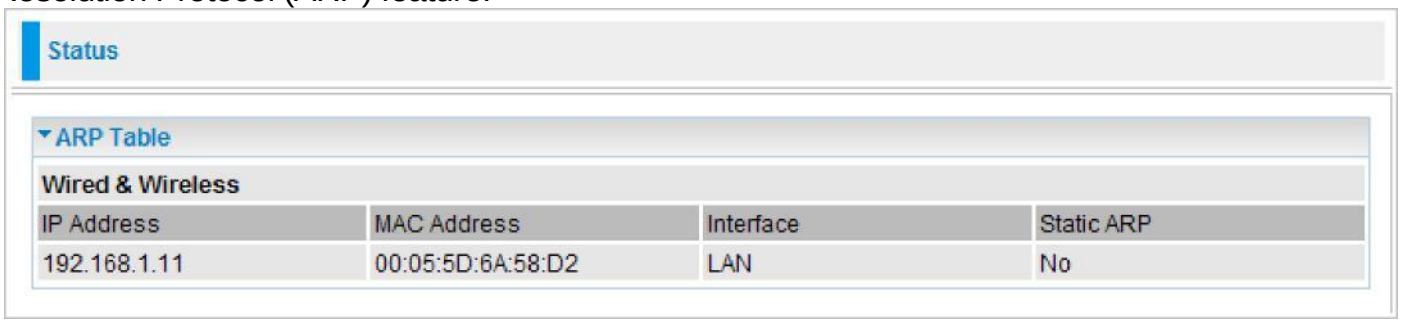
Netmask: WAN port IP subnet mask.

Gateway: The IP address of the default gateway.

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

ARP Table

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



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

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

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

Static ARP: Shows the status of static ARP.

DHCP Table

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

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

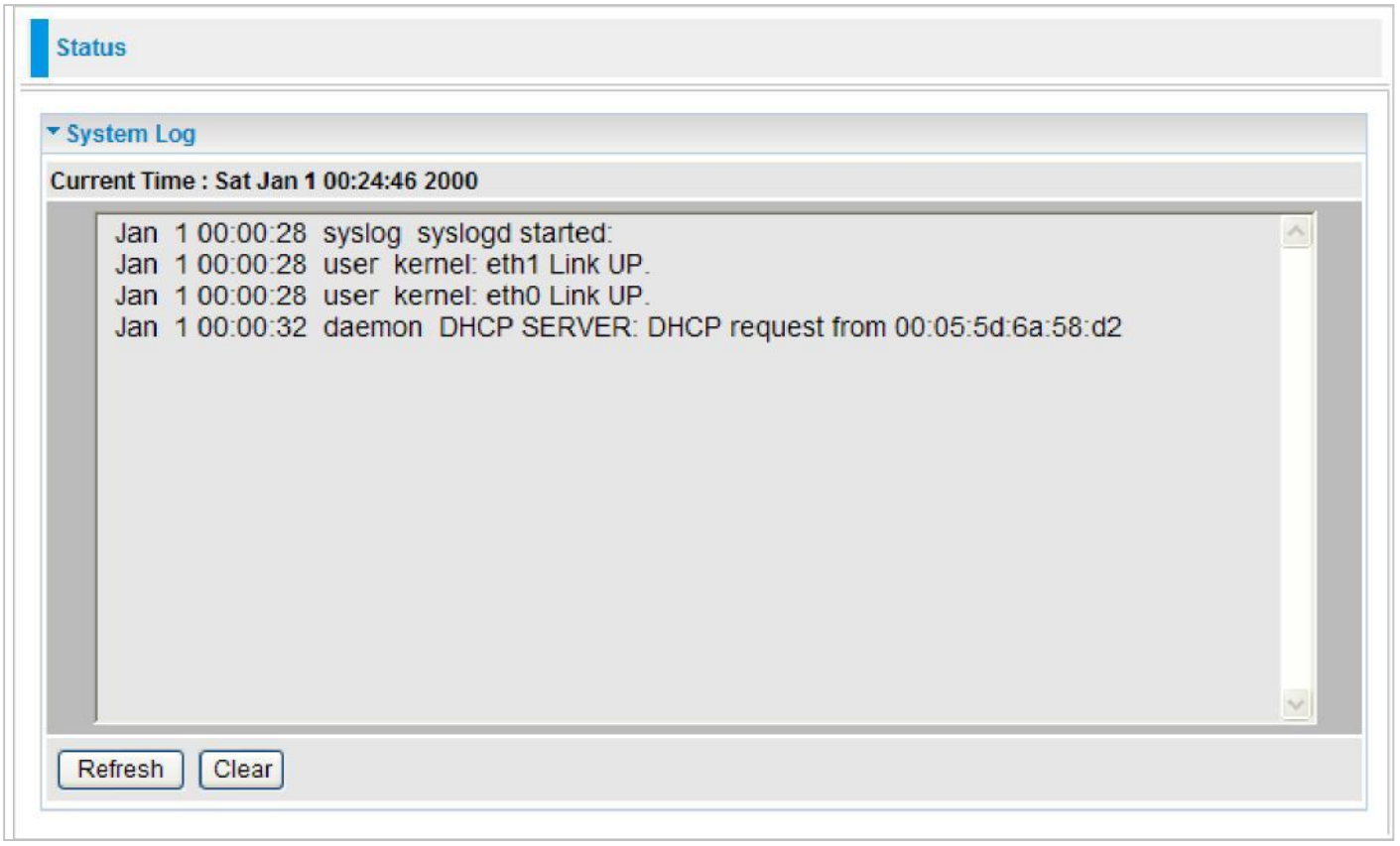
MAC Address: The MAC Address of internal dhcp client host.

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

Register Information: Shows the information provided during registration.

System Log

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



Refresh: Click to update the system log.

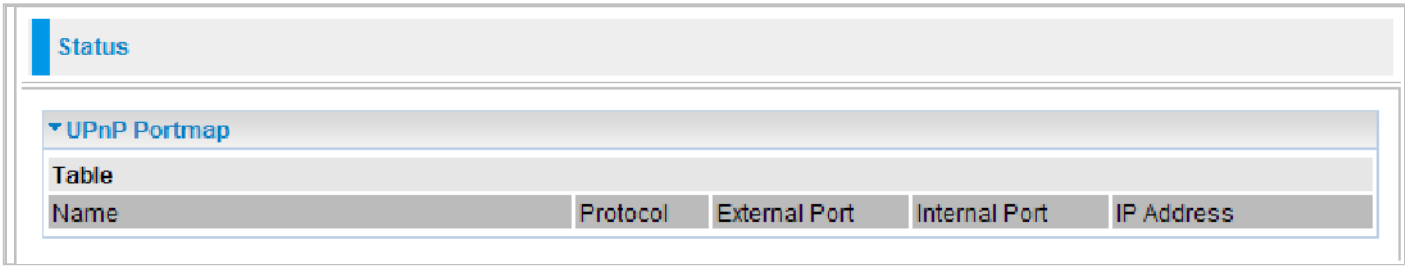
Clear: Click to clear the current log from the screen.

Firewall Log

Firewall Log displays the log information of any unexpected events that occurs to your firewall settings. This page displays the router Firewall Log entries which have been recorded 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 event logging.

UPnP Port map

This section lists all the established port-mapping using UPnP (Universal Plug and Play).



Name: The Host Name of the internal UPNP client.

Protocol: The connection protocol of the UPNP client.

External Port: The external port for this connection.

Internal Port: The internal port for this connection.

IP Address: IP of the internal UPNP client.

Configuration

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

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

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

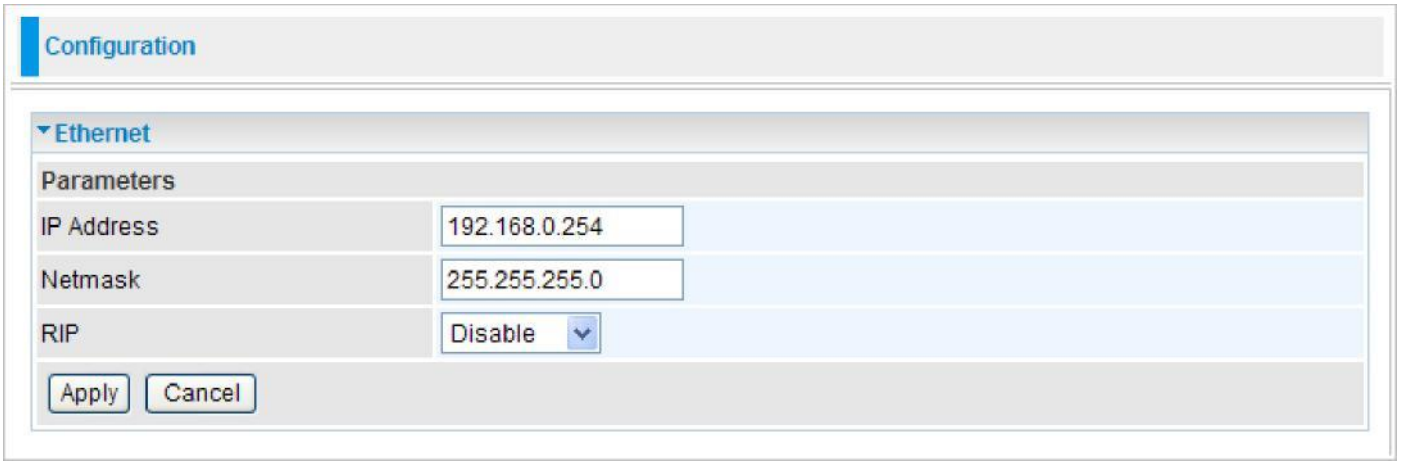
LAN - Local Area Network

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

There are 6 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 that supports multiple internet access at the same time. Users usually only have one subnet in their LAN. The default IP address for the router is 192.168.0.254.



IP Address: The default IP on this router.

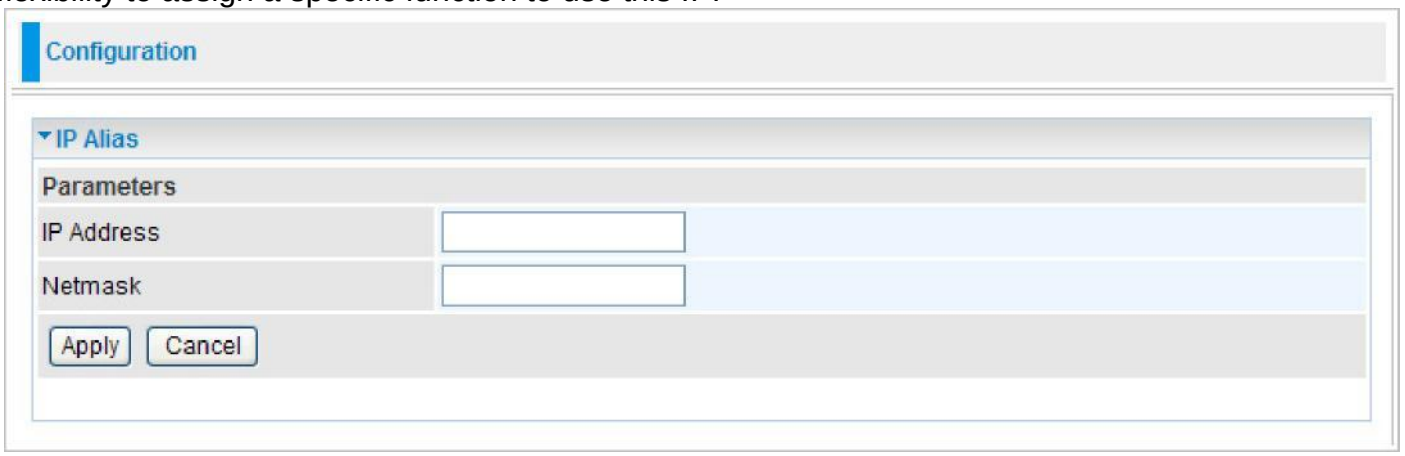
Netmask: The default subnet mask on this router.

RIP: RIP v1, RIP v2 and RIP v1+v2. Check to enable RIP function.

Click Apply to confirm the settings.

IP Alias

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



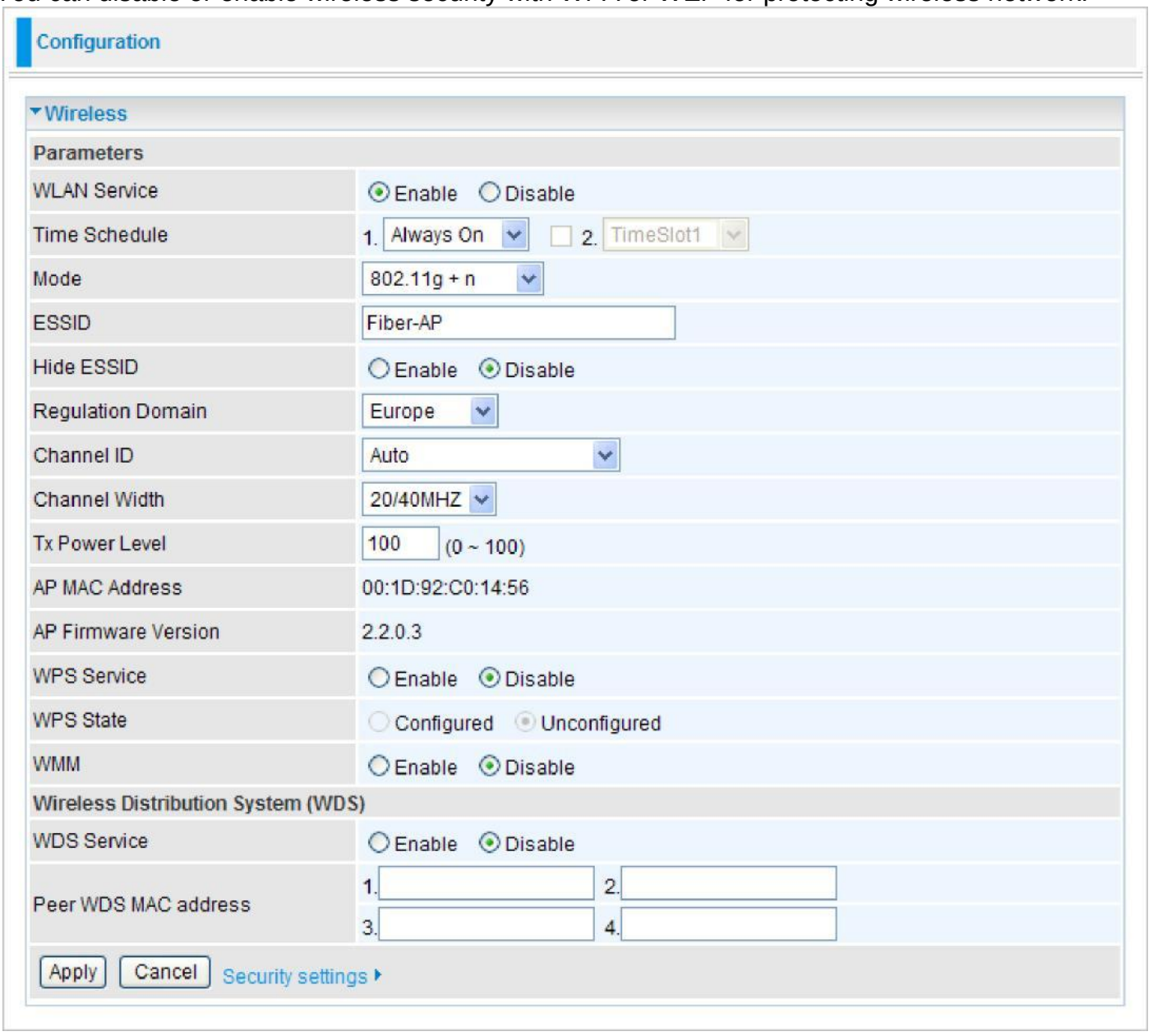
IP Address: Enter the IP address to be added to the network.

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

Click Apply to confirm the settings.

Wireless

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



Parameters

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

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.

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

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

Hide ESSID: This function enables the router to become invisible on the network. Thus, any

Clients using the wireless setting to search for available or specific router on the network will not be able to discover the router whose Hide ESSID function is set to enabled. The default setting is disabled.

Enable: When enabled, you do not broadcast your ESSID. Therefore, no one will be able to locate the Access Point (AP) of your router.

Disable: When disabled, you allow anybody with a wireless client to be able to locate the Access Point (AP) of your router.

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

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

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

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

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

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

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

AP Firmware Version: The Access Point firmware version.

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

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

WMM: This feature is used to control the prioritization of traffic according to 4 Access categories: Voice, Video, Best Effort and Background. Default is set to disable.

Wireless Distribution System (WDS)

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

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

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

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

2. **Peer WDS MAC Address:** It is the second associated AP's MAC Address.
3. **Peer WDS MAC Address:** It is the third associated AP's MAC Address.
4. **Peer WDS MAC Address:** It is the fourth associated AP's MAC Address. ***Note:***

For MAC Address, the format can be:..... xxxxxxxxxxxxxxxxxxxxxx

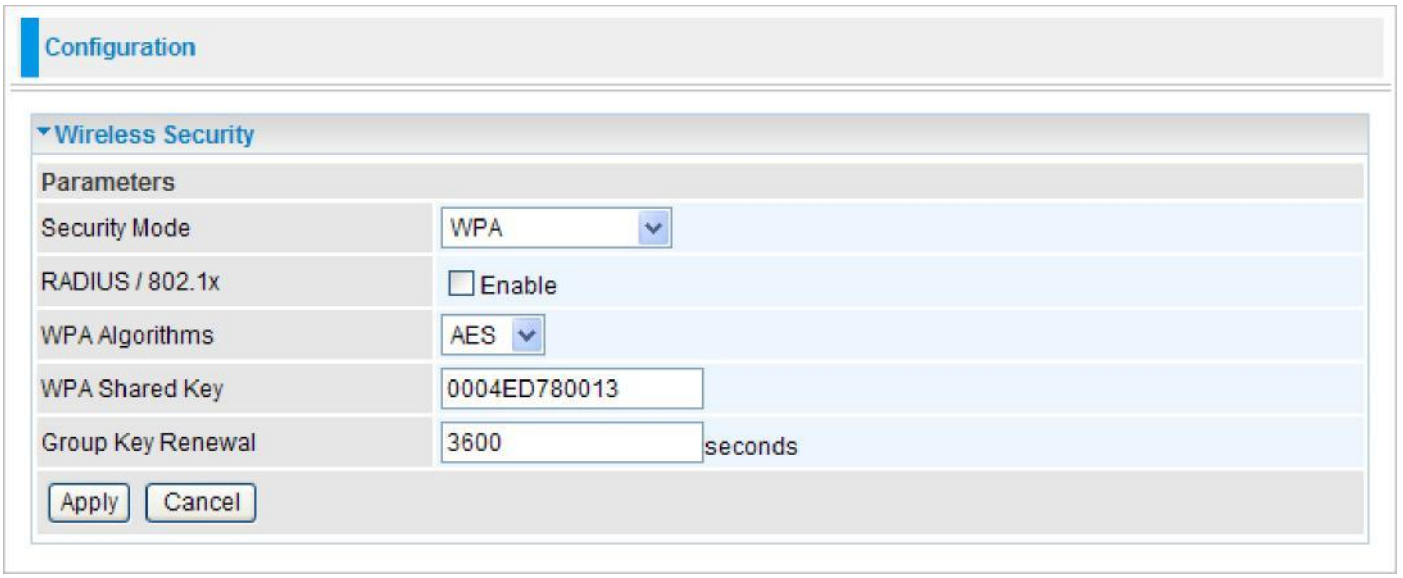
Click Apply to confirm the settings.

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

Wireless Security

You can disable or enable wireless security function using WPA or WEP for protecting wireless network.

WPA / WPA2 / WPA/WPA2-PSK



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

RADIUS/802.1x: Whether to enable RADIUS function or not (Available for WPA and WPA2 encryption).

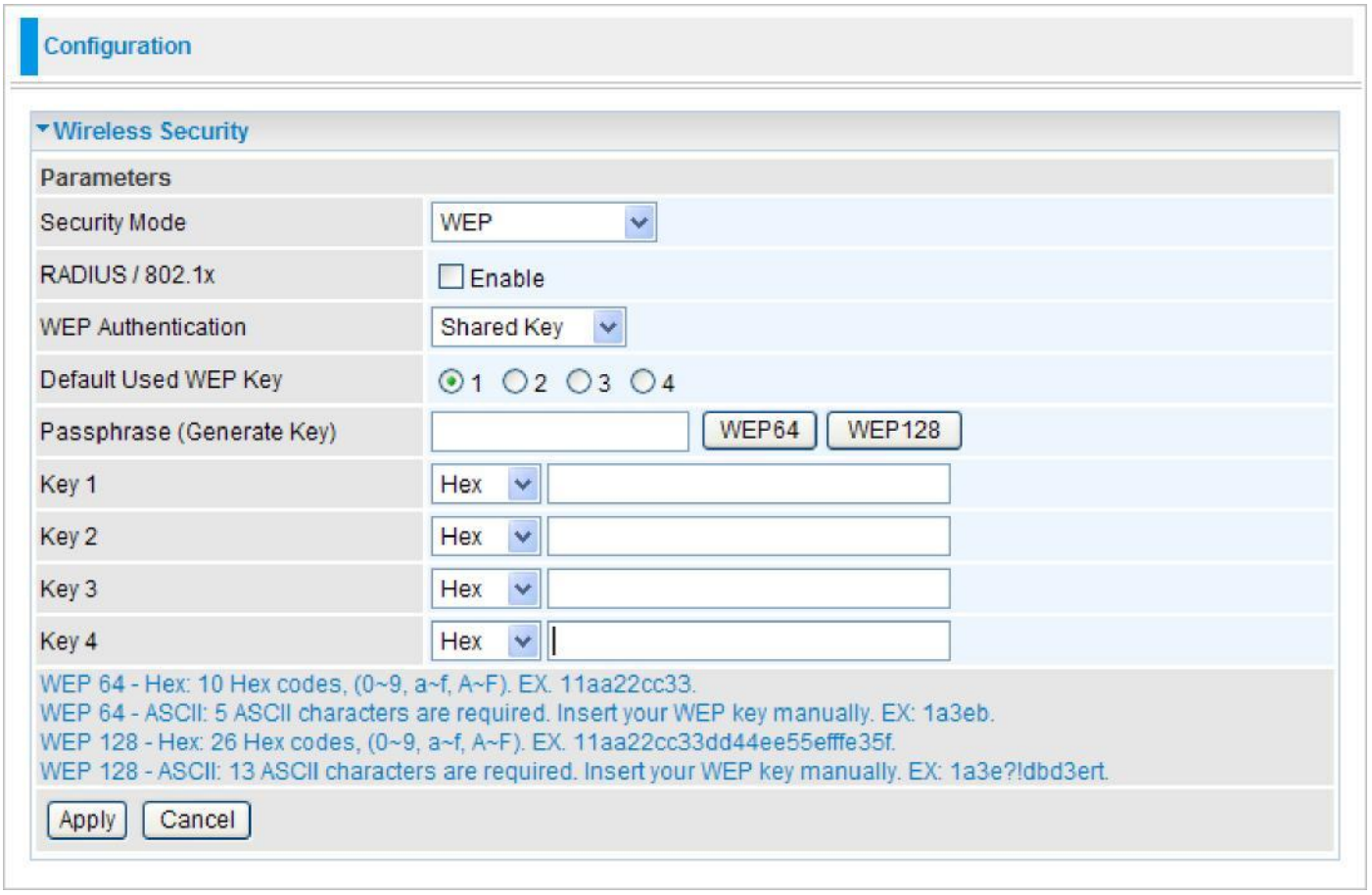
WPA Algorithms: There are 3 types of the WPA-PSK, WPA2-PSK and WPA/WPA2-PSK. The WPA-PSK adapts the TKIP (Temporal Key Integrity Protocol) encrypted algorithms, which incorporates Message Integrity Code (MIC) to provide protection against hackers. The WPA2-PSK adapts CCMP (Cipher Block Chaining Message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

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

Group Key Renewal: The period of renewal time for changing the security key automatically between wireless client and Access Point (AP). Default value is 3600 seconds.

Click Apply to confirm the settings.

WEP



Security Mode: Choose the type of security mode **WEP** from the drop-down menu.

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

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

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

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

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

Click Apply to confirm the settings.

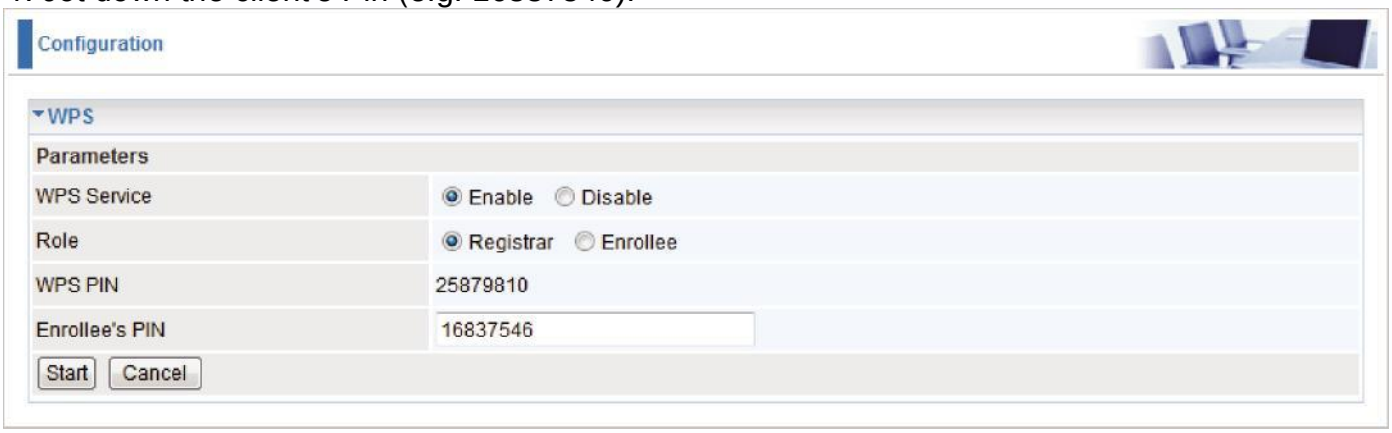
Note: For information about settling Radius/802.1x, please refer to WLAN setup section.

WPS

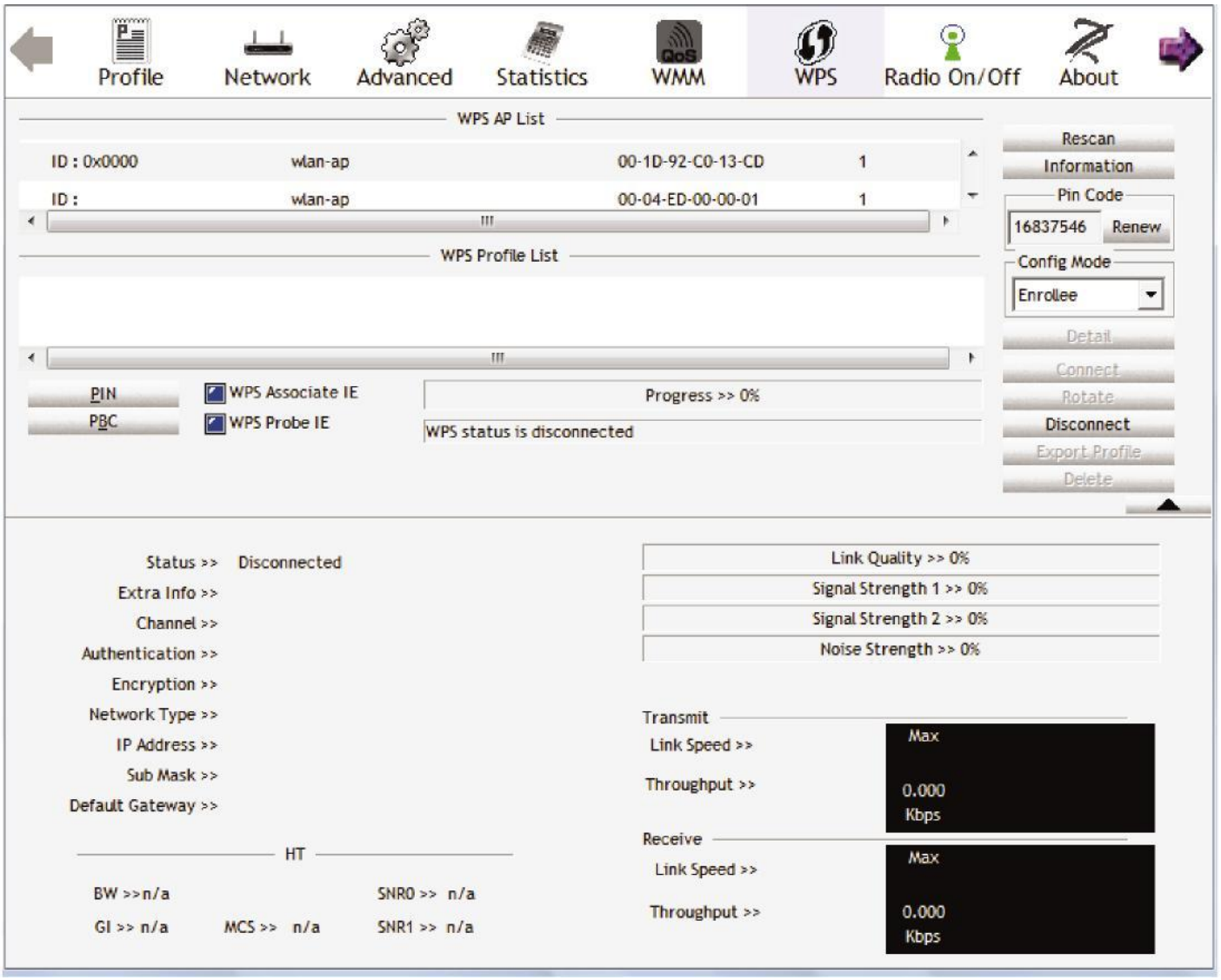
WPS (Wifi Protected Setup) feature is a standard protocol created by Wi-Fi Alliance. This feature greatly simplifies the steps needed to create Wi-Fi networks for a residential or an office setting. WPS supports 2 types of configuration methods which are commonly known among consumers: **PIN Method**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

PIN Method: Configure AP as Registrar

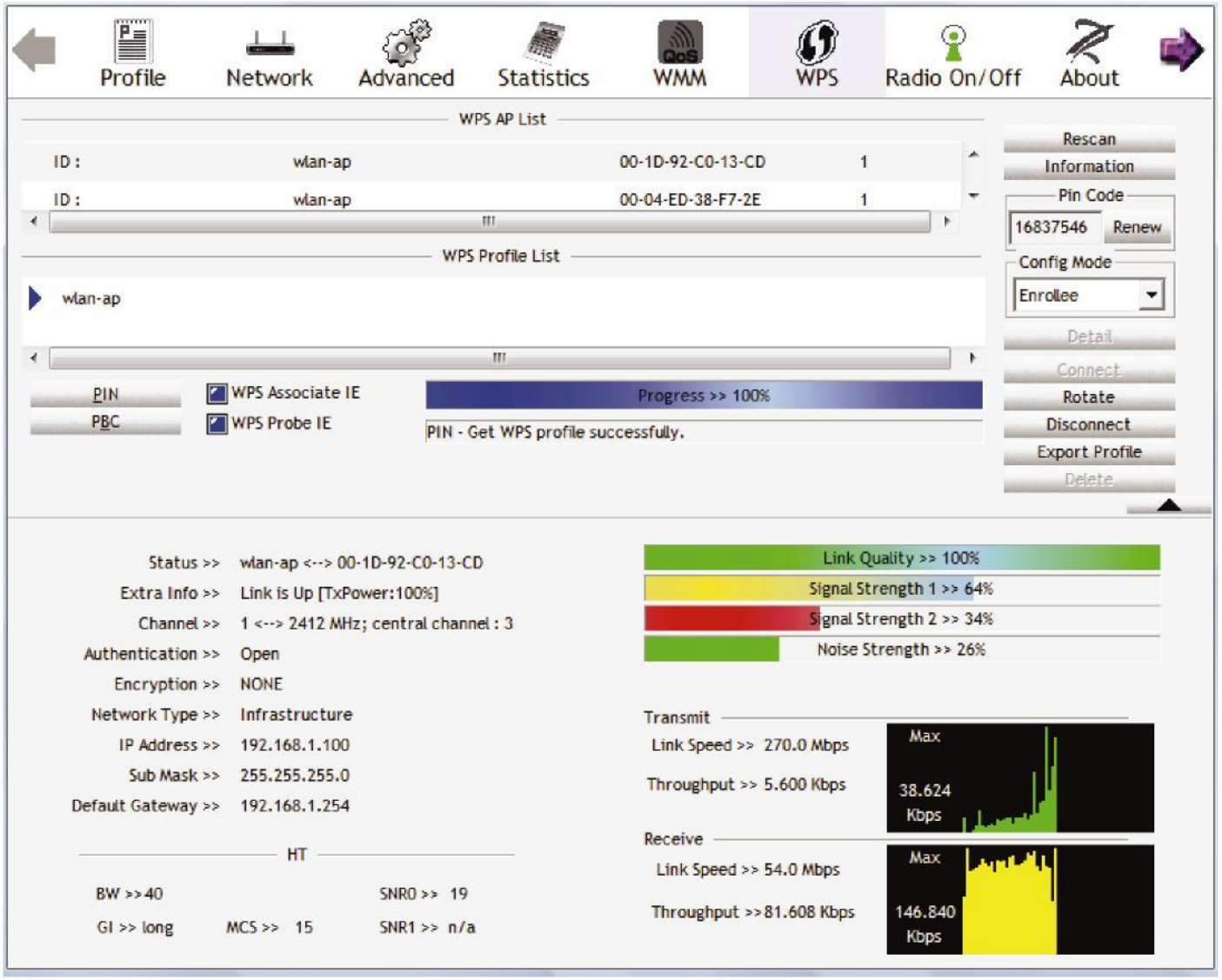
1. Jot down the client's Pin (e.g. 16837546).



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



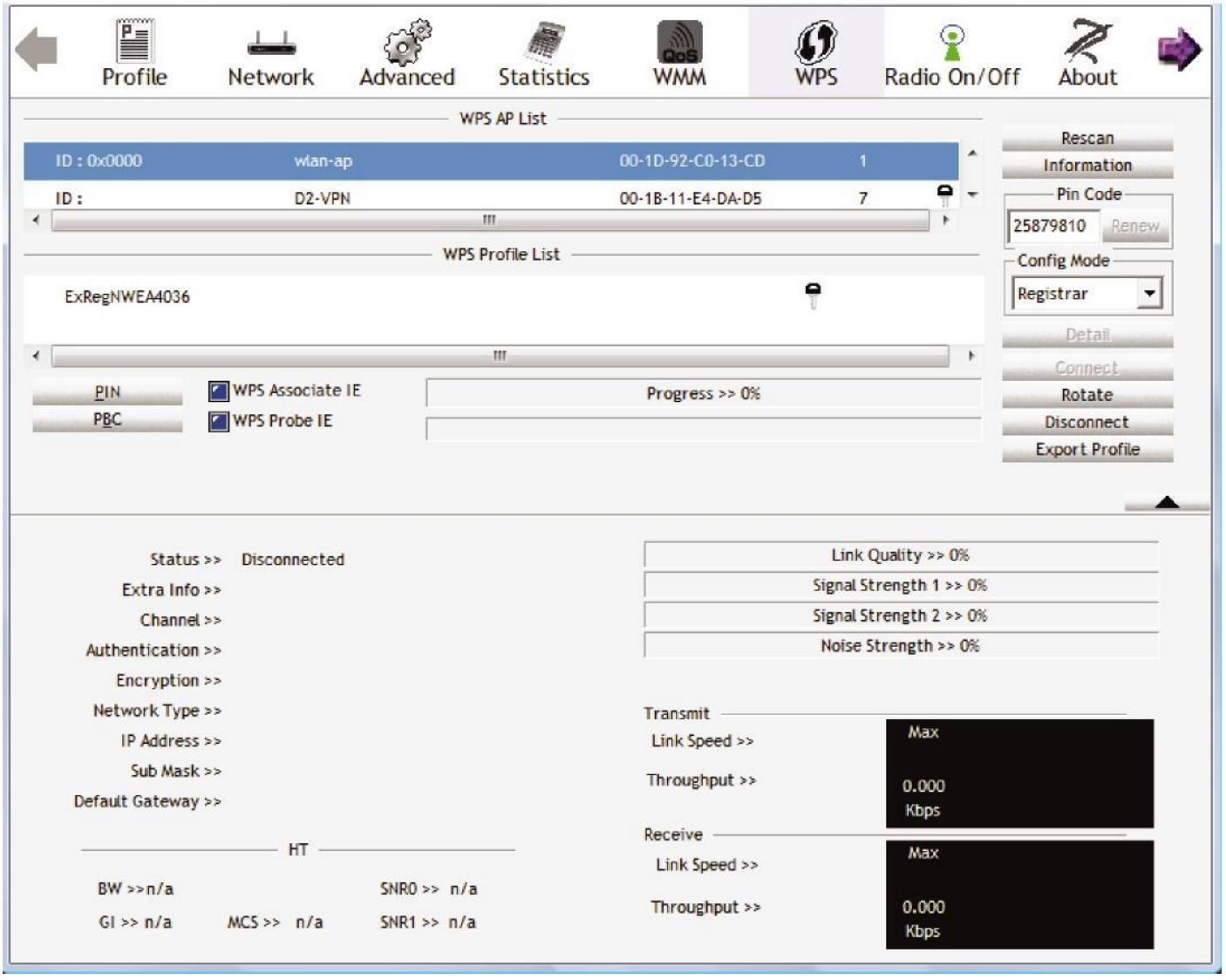
4. The client's SSID and security setting will now be configured to match the SSID and security setting of the registrar.



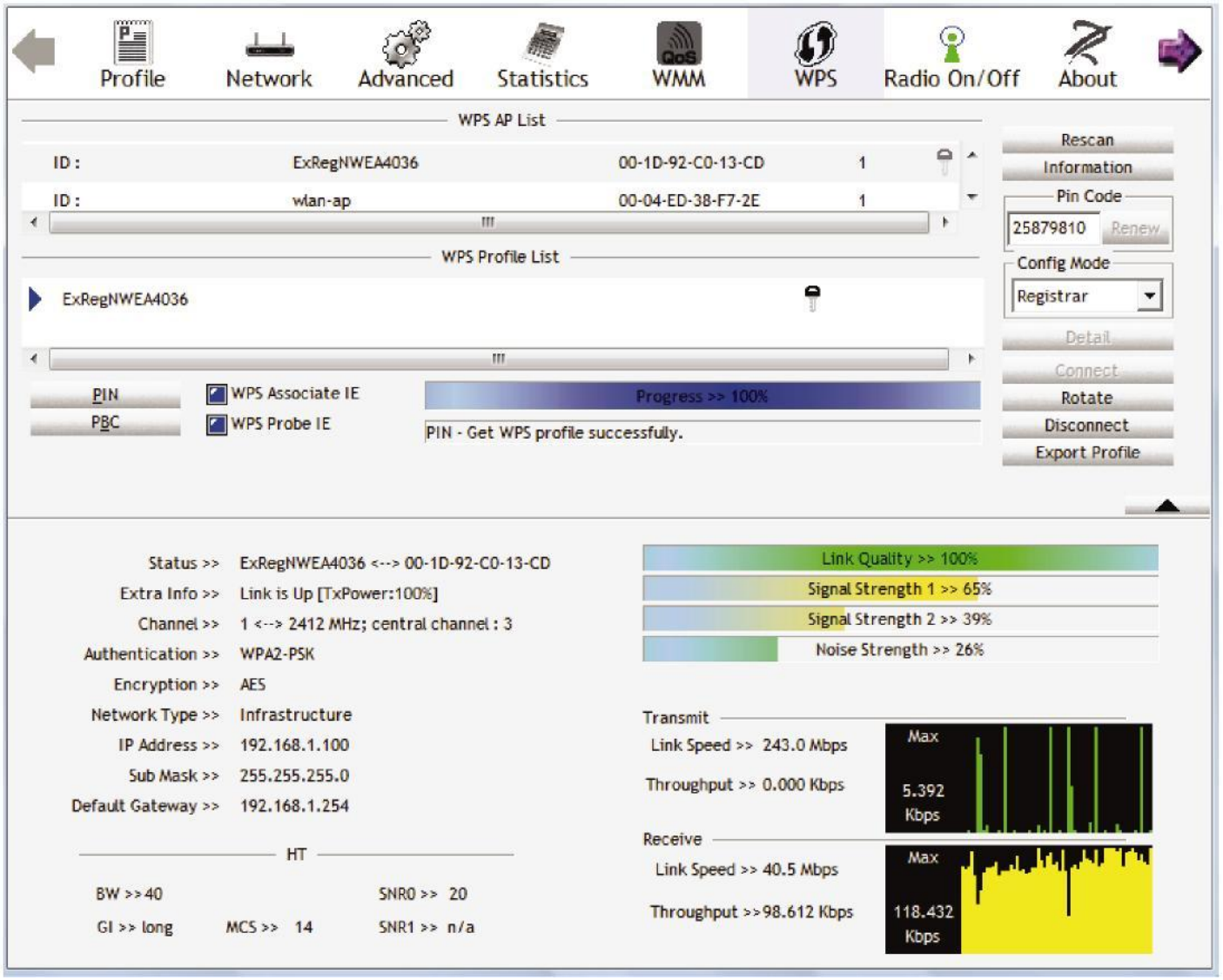
PIN Method: Configure AP as Enrollee

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

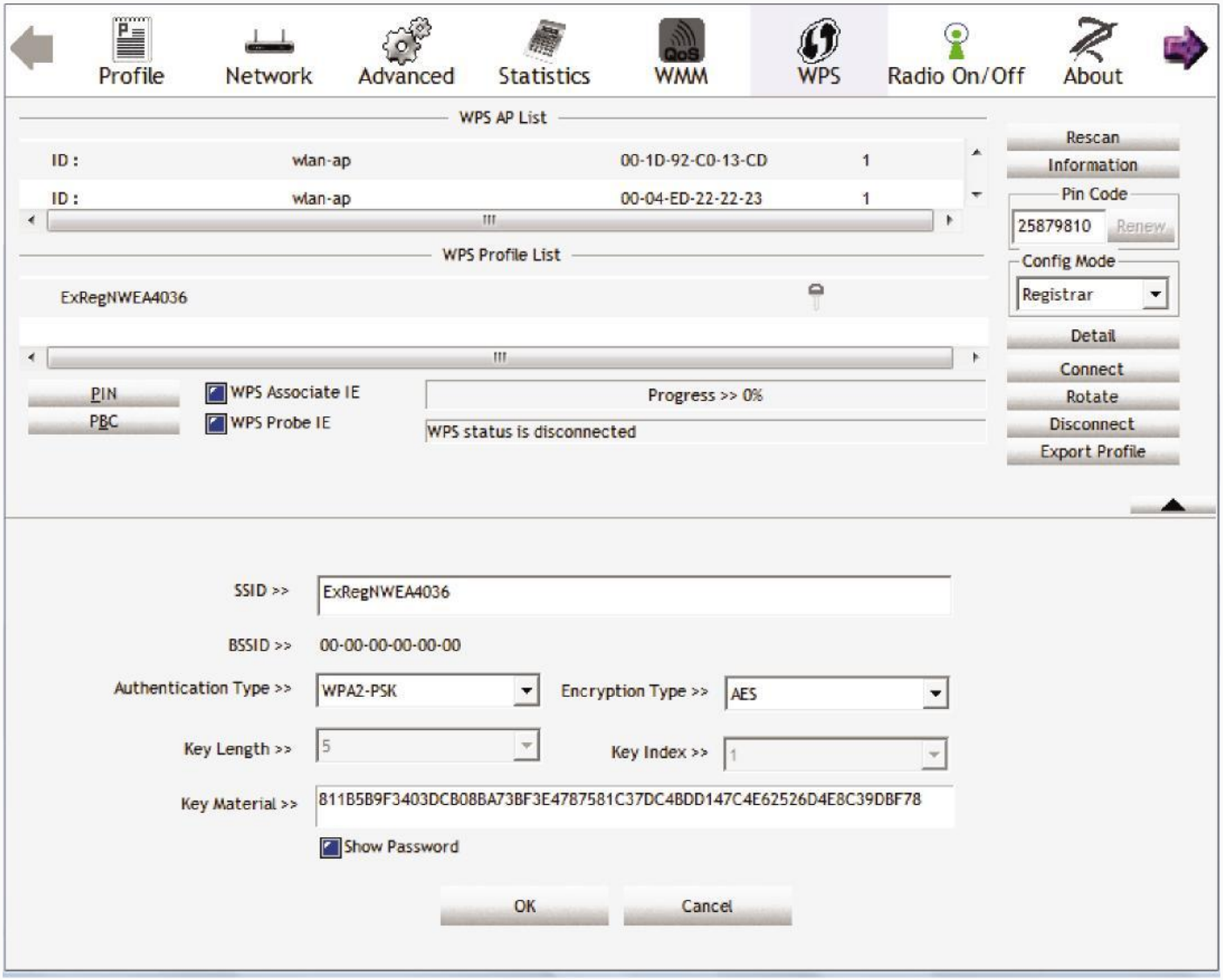
3. Launch the wireless client's WPS utility (e.g. Ralink Utility). Set the Config Mode as Registrar. Enter the PIN number in the PIN Code column then choose the correct AP (e.g. wlan-ap) from the WPS AP List section before pressing the PIN button to run the scan.

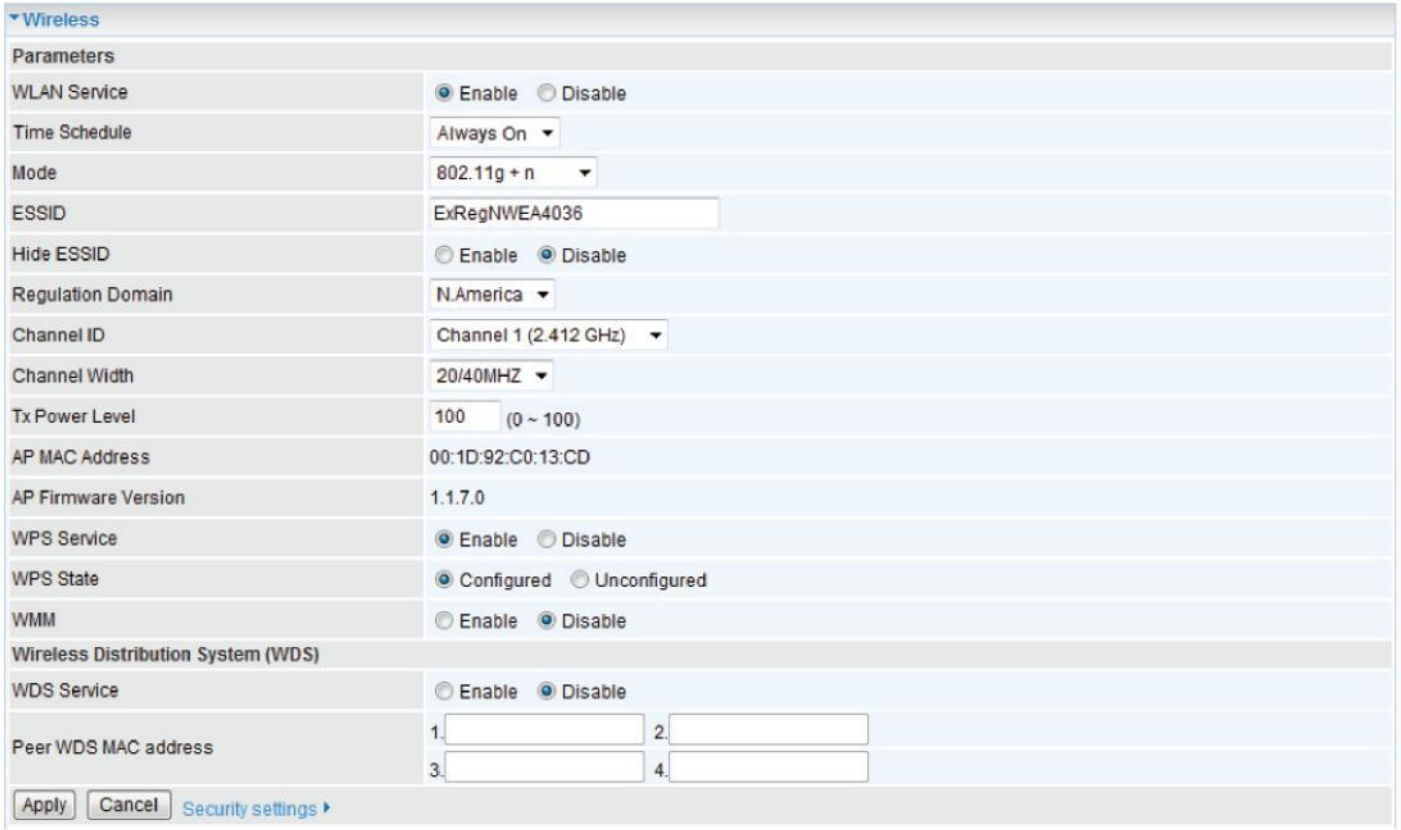


4. The router's (AP's) SSID and security setting will now be configured to match the SSID and security setting of the registrar.



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.

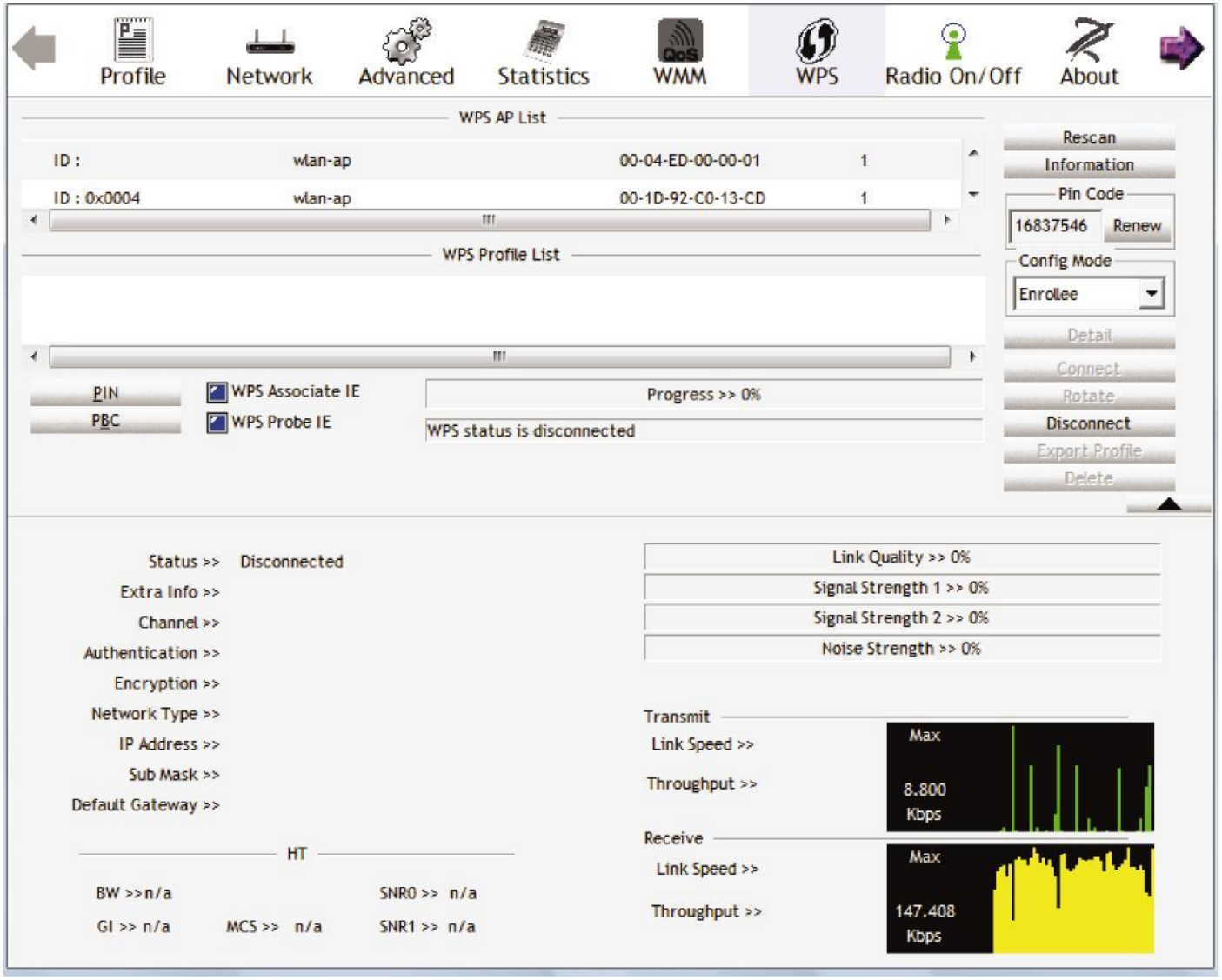

Profile
Network
Advanced
Statistics
WMM
WPS
Radio On/Off
About
WPS AP List
ID : wlan-ap 00-1D-92-C0-13-CD 1
ID : wlan-ap 00-04-ED-22-22-23 1
Rescan
Information
Pin Code
25879810
Renew
Config Mode
Registrar
WPS Profile List
ExRegNWEA4036
Detail
Connect
Rotate
Disconnect
Export Profile
PIN
PBC
WPS Associate IE
WPS Probe IE
Progress >> 0%
WPS status is disconnected
SSID >> ExRegNWEA4036
BSSID >> 00-00-00-00-00-00
Authentication Type >> WPA2-PSK
Encryption Type >> AES
Key Length >> 5
Key Index >> 1
Key Material >> 811B5B9F3403DCB08BA73BF3E4787581C37DC4BDD147C4E62526D4E8C39DBF78
Show Password
OK
Cancel


Wireless
Parameters
WLAN Service Enable Disable
Time Schedule Always On
Mode 802.11g + n
ESSID ExRegNWEA4036
Hide ESSID Enable Disable
Regulation Domain N.America
Channel ID Channel 1 (2.412 GHz)
Channel Width 20/40MHZ
Tx Power Level 100 (0 ~ 100)
AP MAC Address 00:1D:92:C0:13:CD
AP Firmware Version 1.1.7.0
WPS Service Enable Disable
WPS State Configured Unconfigured
WMM Enable Disable
Wireless Distribution System (WDS)
WDS Service Enable Disable
Peer WDS MAC address 1. 2. 3. 4.
Apply
Cancel
Security settings

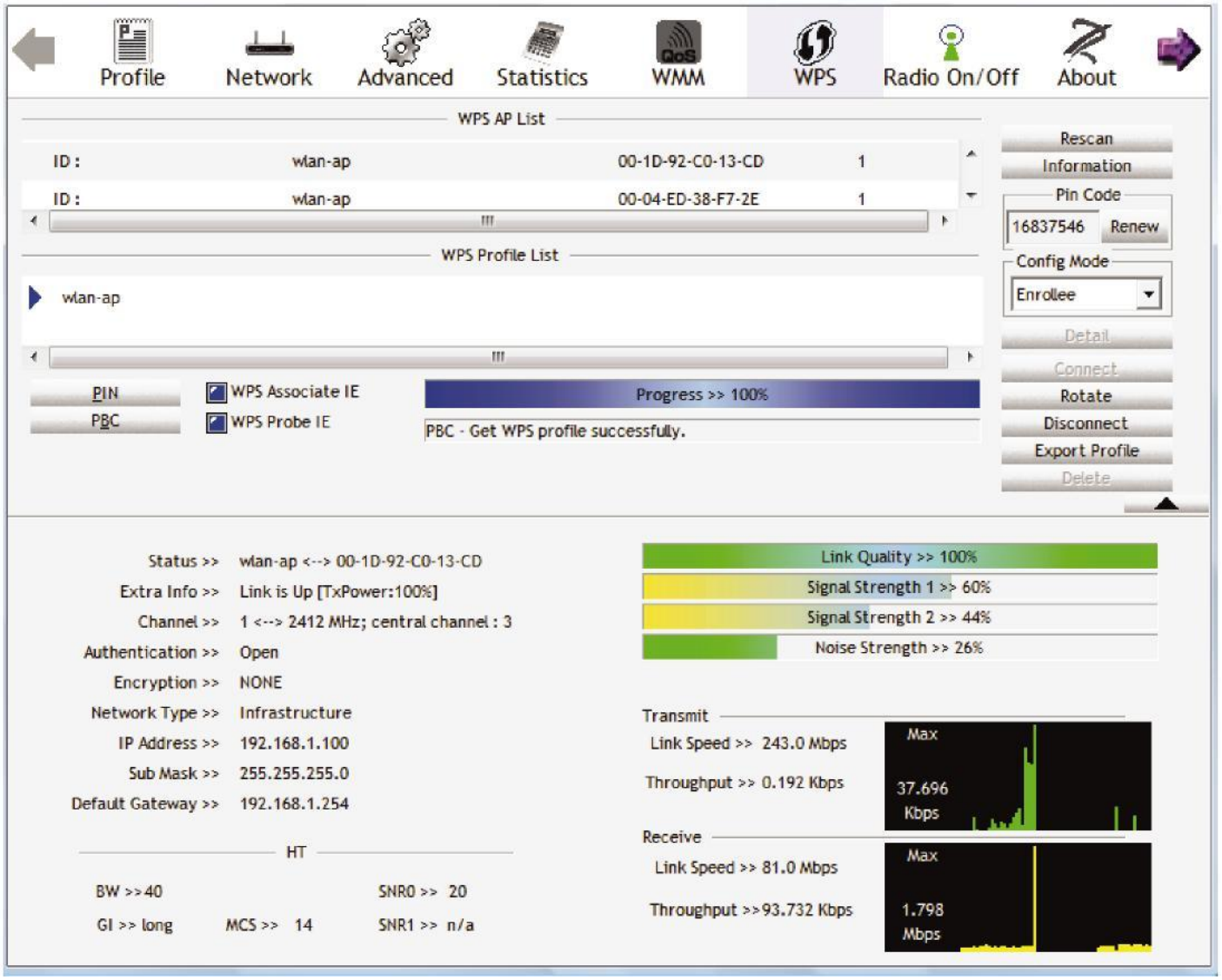

Wireless Security
Parameters
Security Mode
WPA2
WPA Algorithms
AES
WPA Shared Key
811B5B9F3403DCB08I
Group Key Renewal
3600
seconds
Apply
Cancel

PBC Method:

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

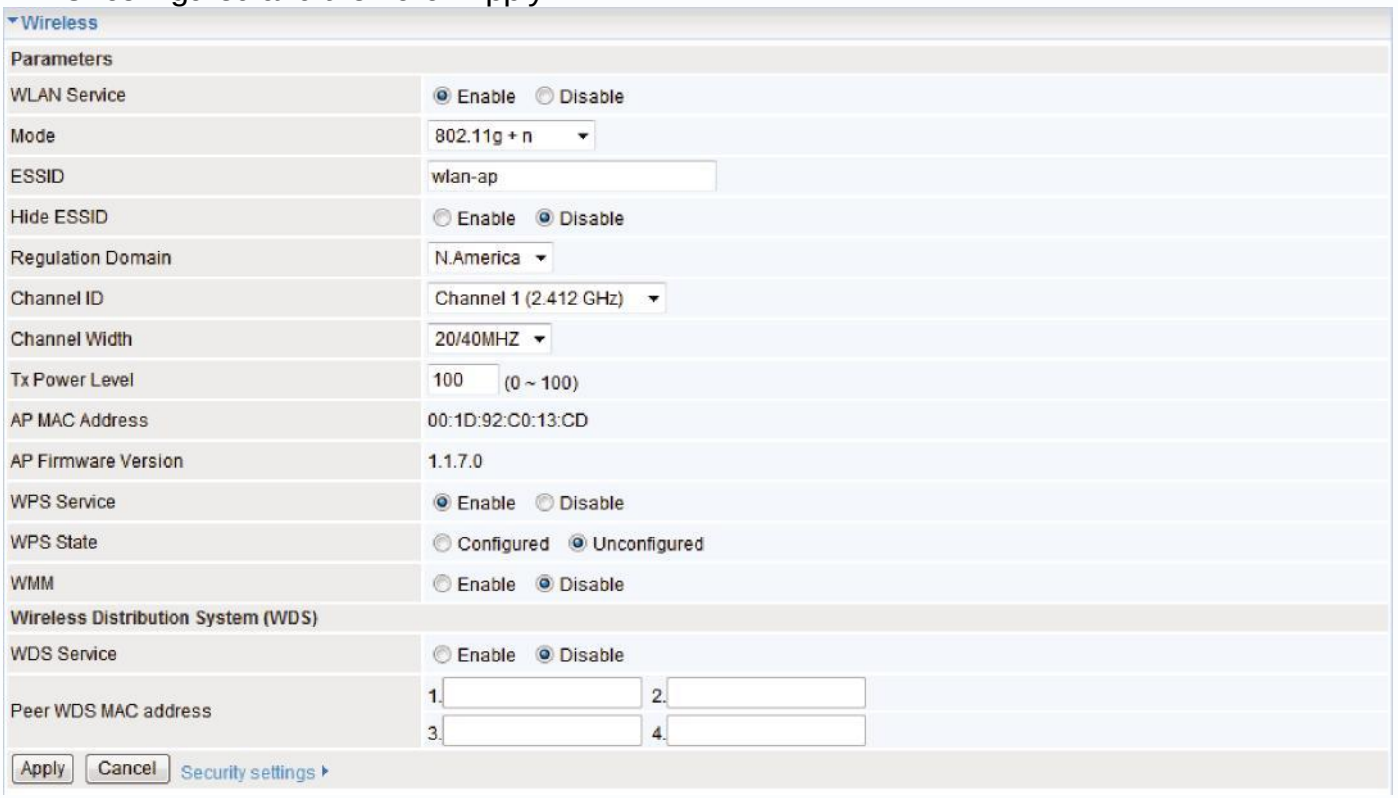


3. When the PBC button is pushed, a wireless communication will be established between your router and the PC. The client's SSID and security setting will now be configured to match the SSID and security setting of the router.

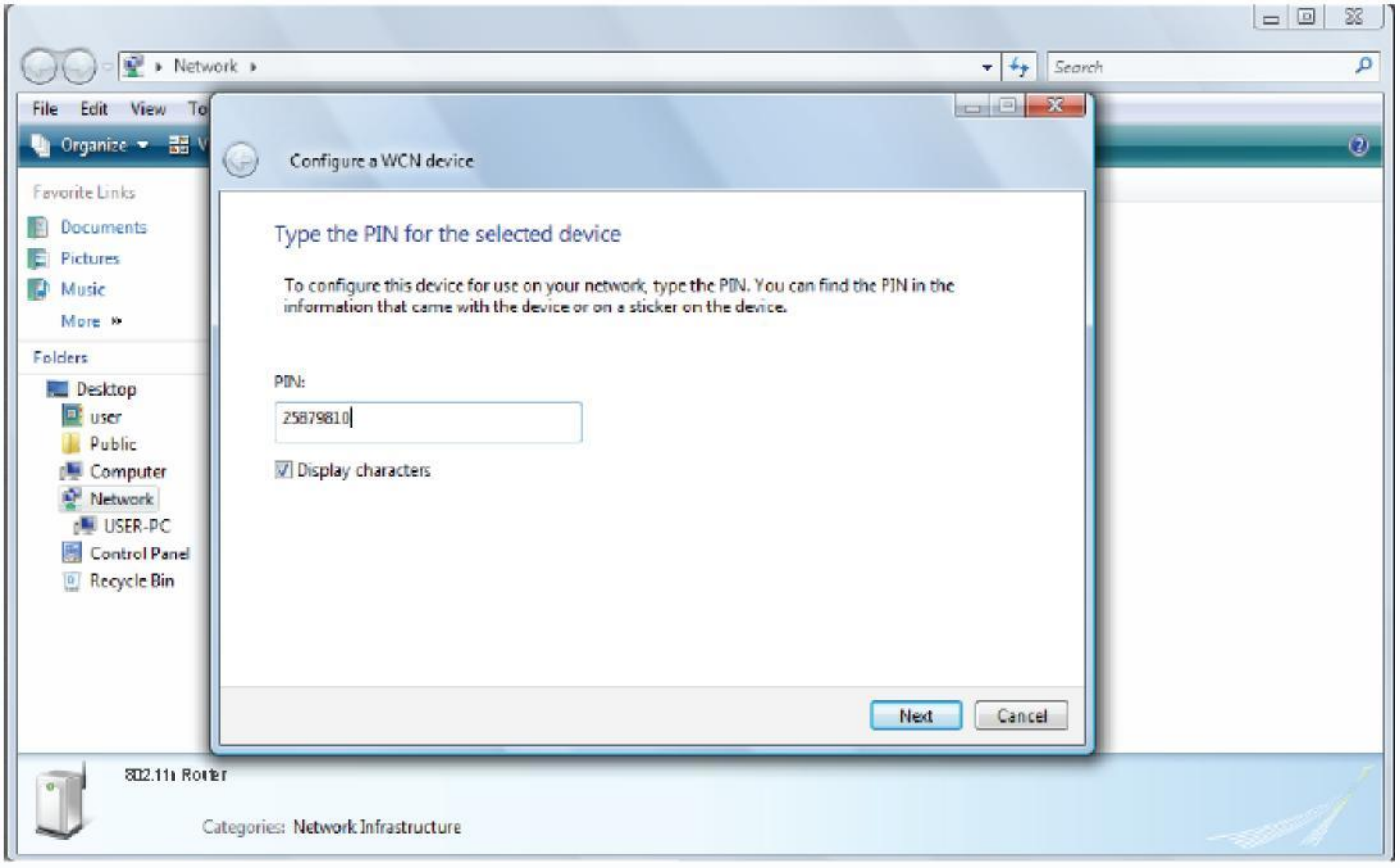


Wi-Fi Network Setup with Windows Vista WCN:

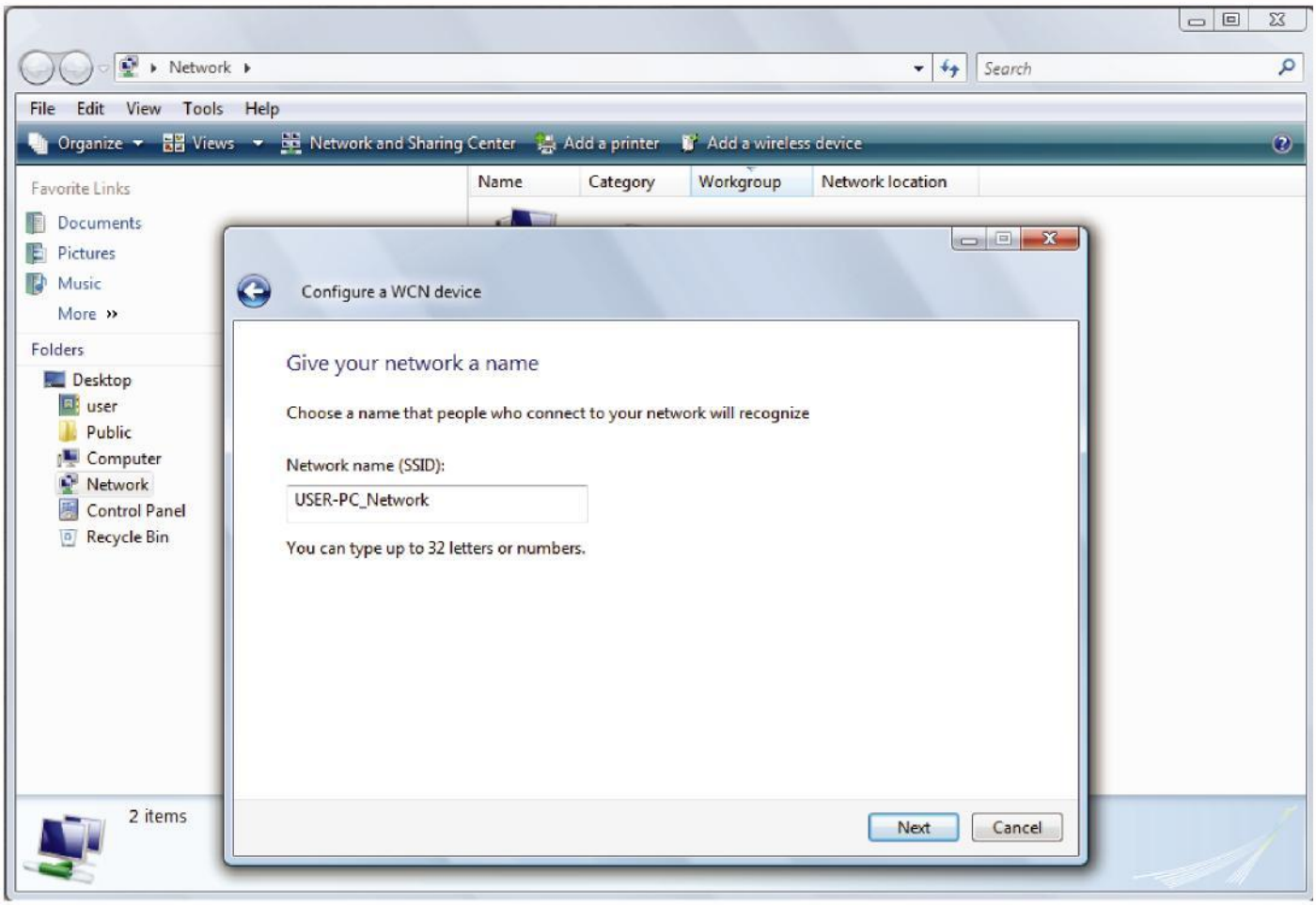
1. Jot down the AP PIN from the Web (e.g. 25879810).
2. Access the Wireless configuration of the web GUI. Enable WPS service, set the WPS State to Unconfigured and then click Apply.



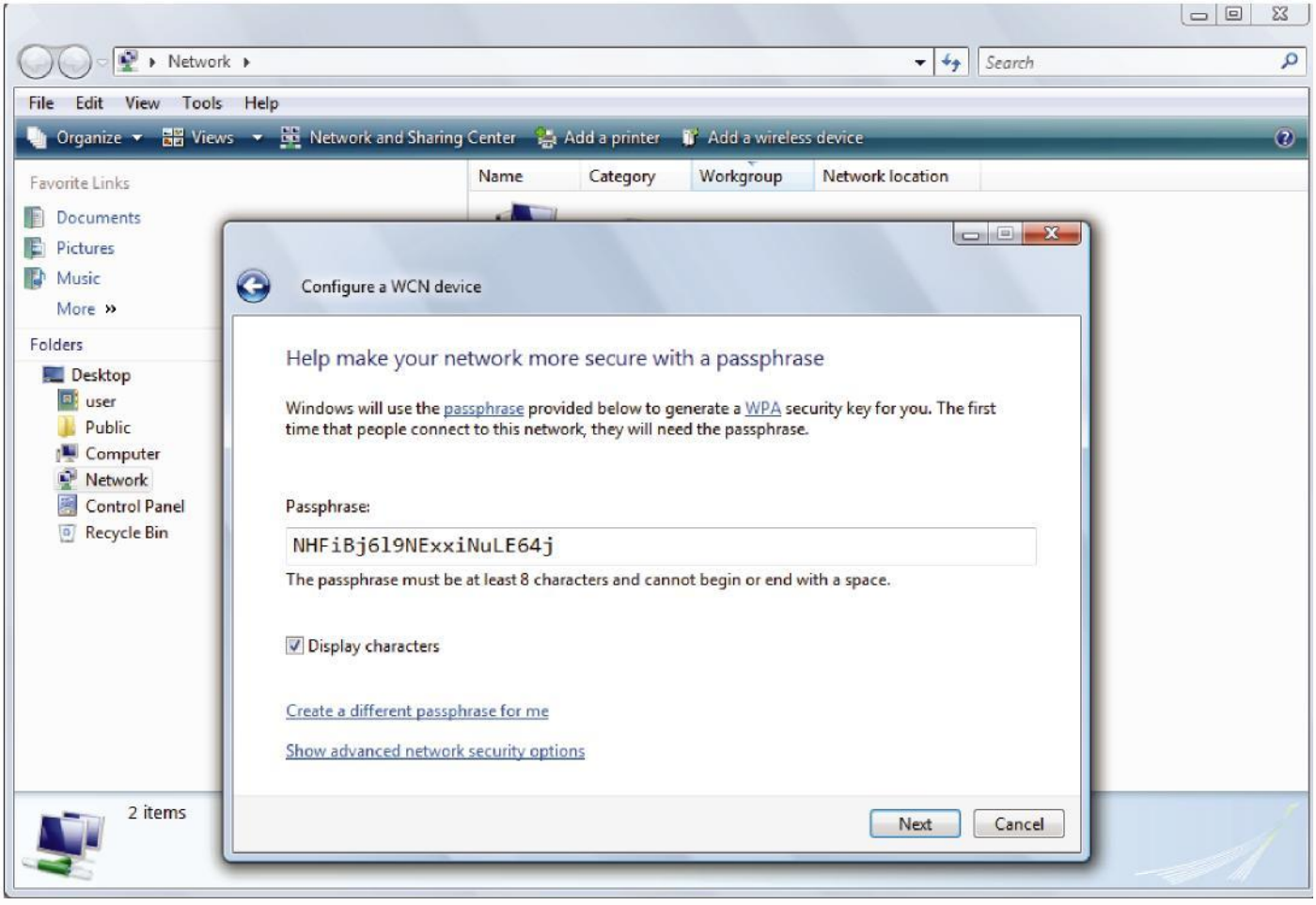
3. In your Vista operating system, access the Control Panel page, then select Network and Internet > View Network Computers and Devices. Double click on the Fiber Optical Router icon and enter the AP PIN in the column provided then press next.



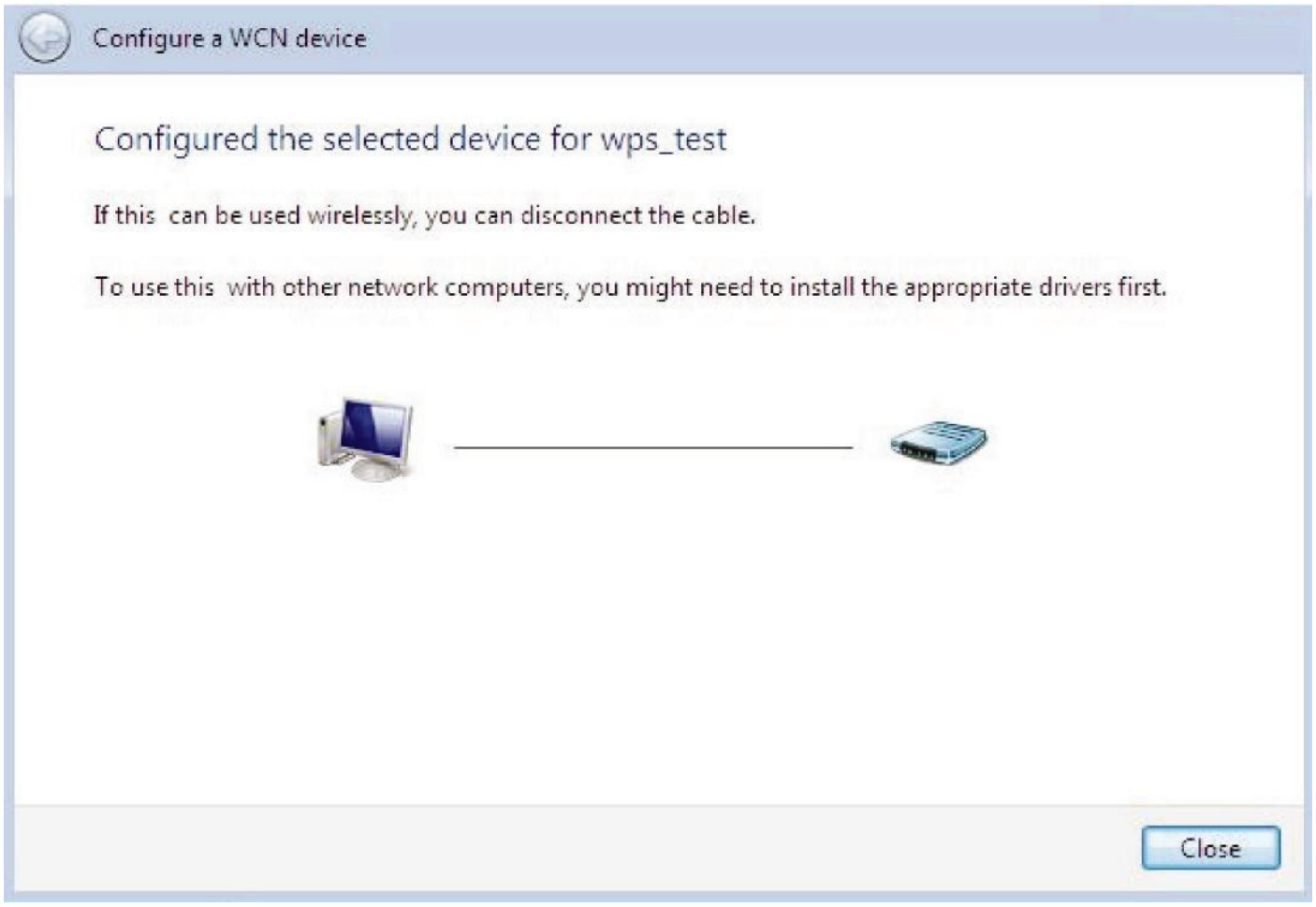
4. Enter the AP SSID then click Next.



5. Enter the passphrase then click Next.

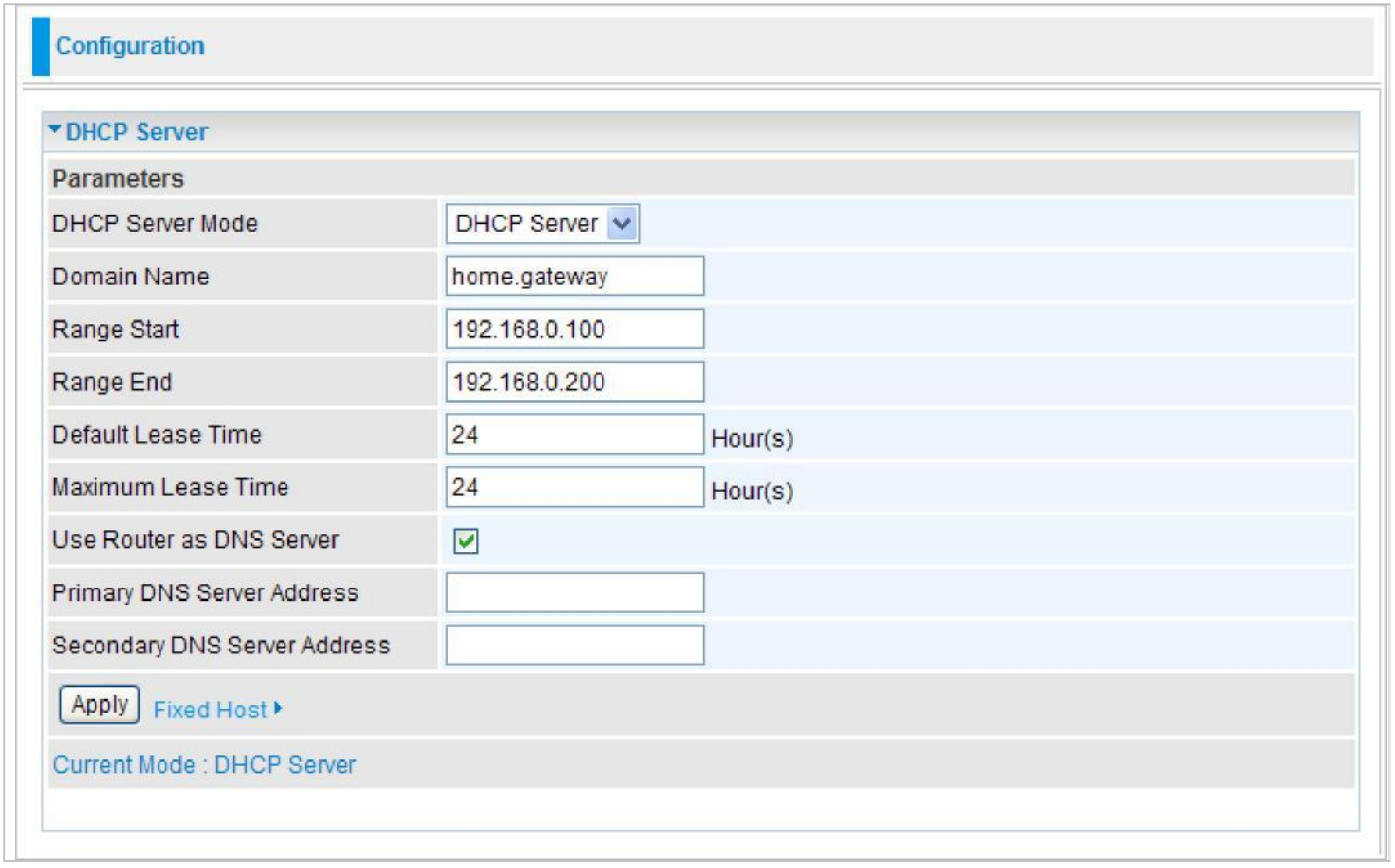


6. When you have come to this step, you will have completed the Wi-Fi network setup using the built-in WCN feature in Windows Vista.



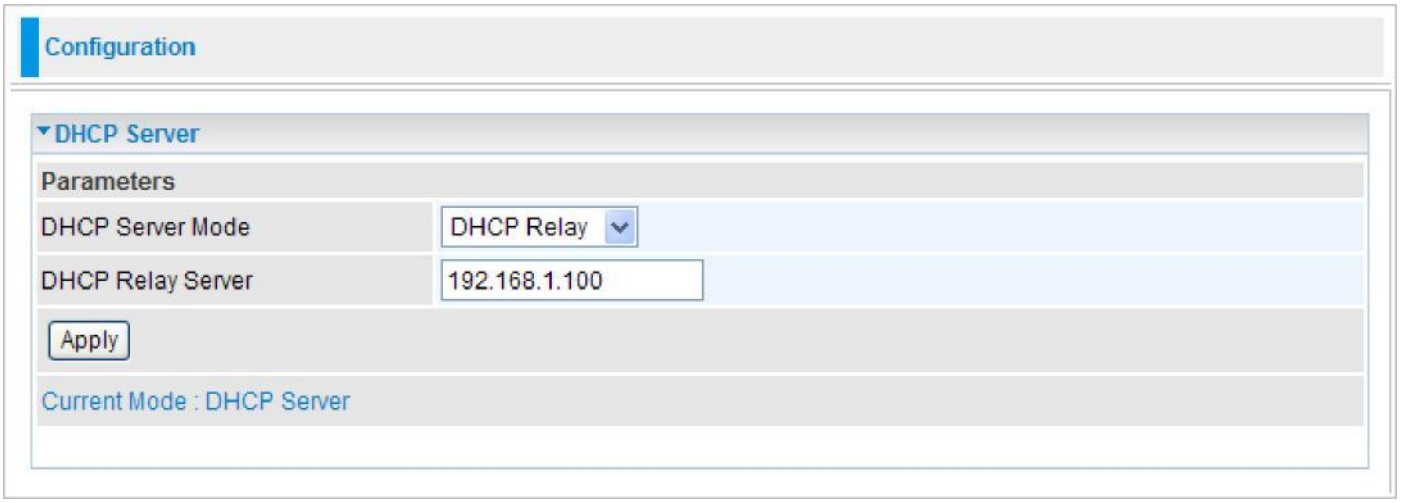
DHCP Server

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



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

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



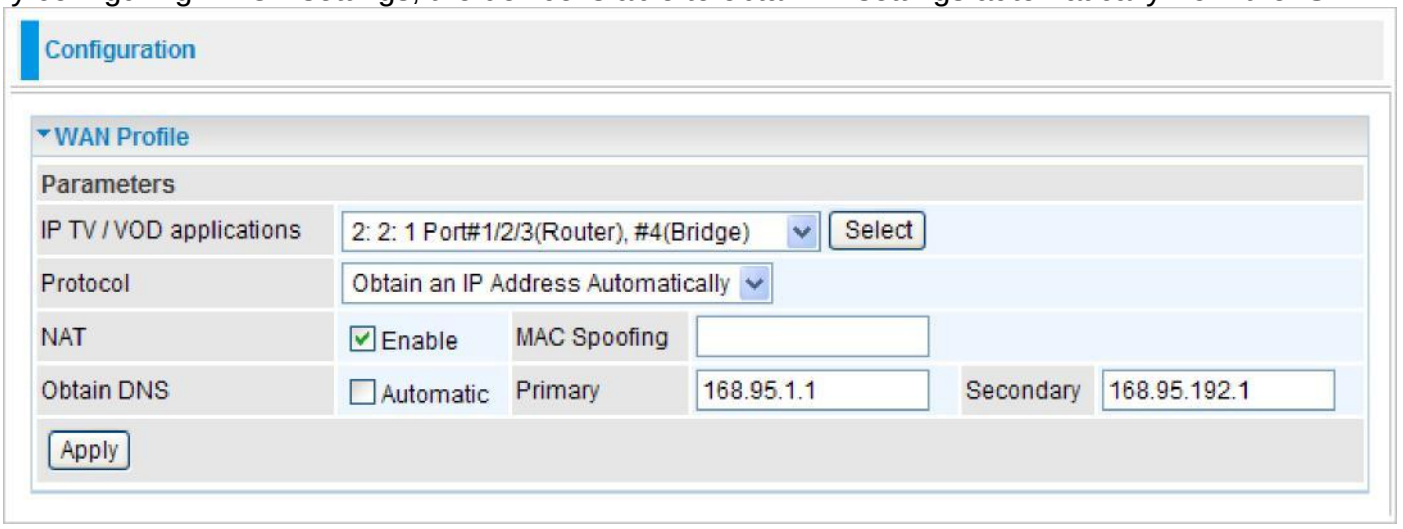
WAN - Wide Area Network

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

WAN Profile

Obtain an IP Address Automatically

By configuring DHCP settings, the device is able to obtain IP settings automatically from the ISP.



IP TV / VOD applications: Select the application you will use in the device and then click Select to save the change.

Protocol: Select the protocol you will use in the device.

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

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

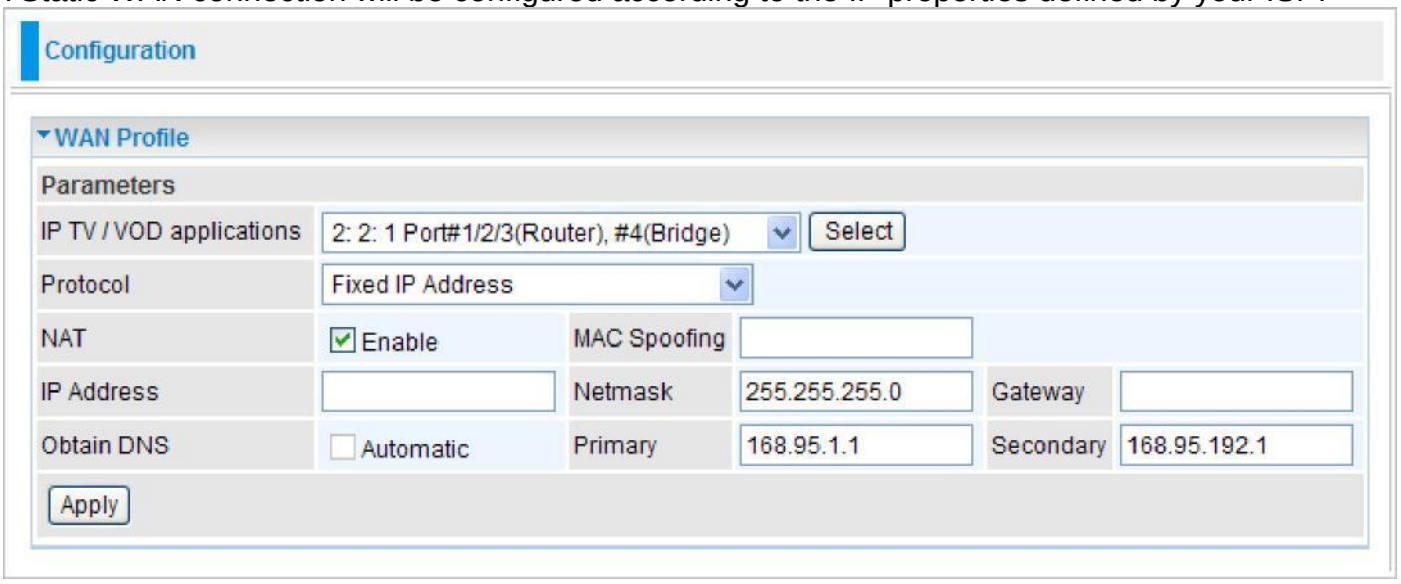
Obtain DNS: Select this check box to activate DNS.

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

Click Apply to confirm the settings.

Fixed IP Address

A Static WAN connection will be configured according to the IP properties defined by your ISP.



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

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

IP Address: Enter your fixed IP address.

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

Gateway: Enter the IP address of the default gateway (if given).

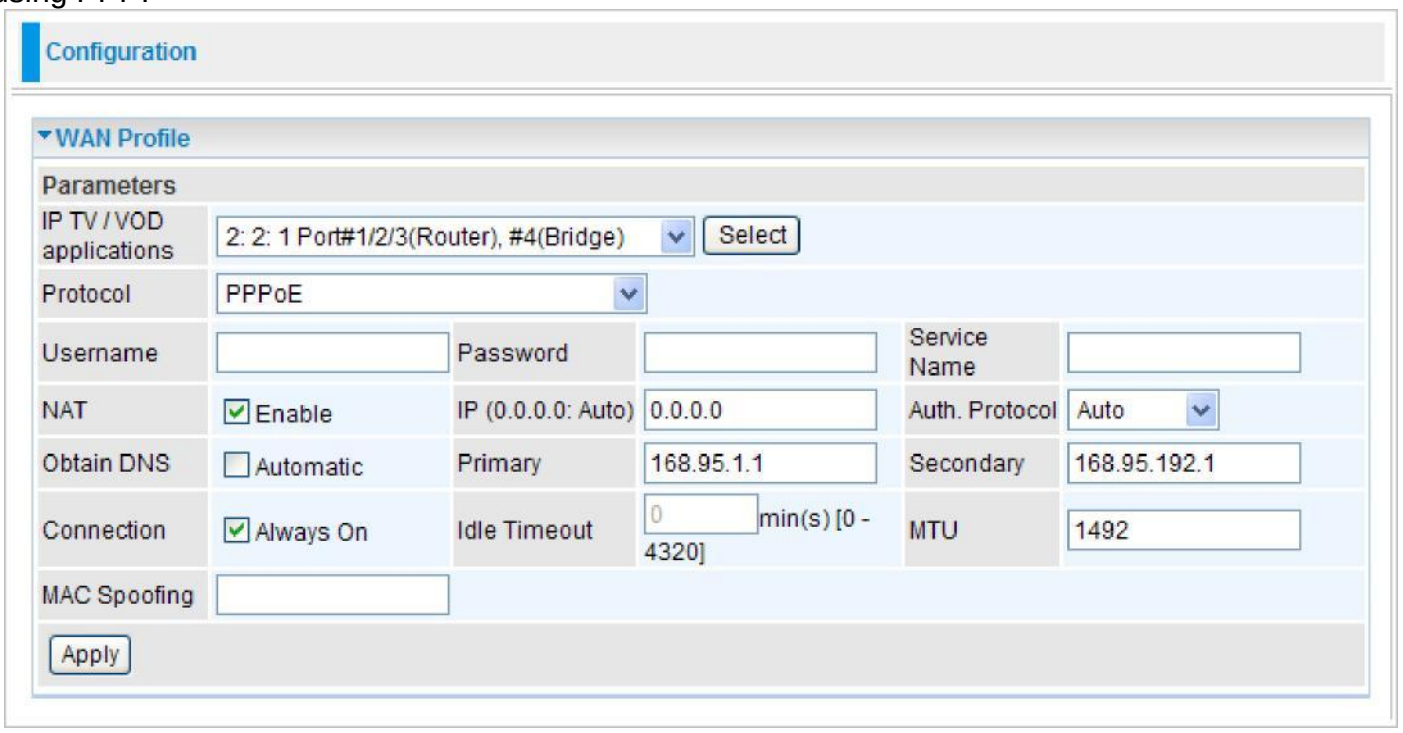
Obtain DNS: Select this check box to activate DNS.

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

Click Apply to confirm the settings.

PPPoE

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



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

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

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

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

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

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

Obtain DNS: Select this check box to activate DNS.

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

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

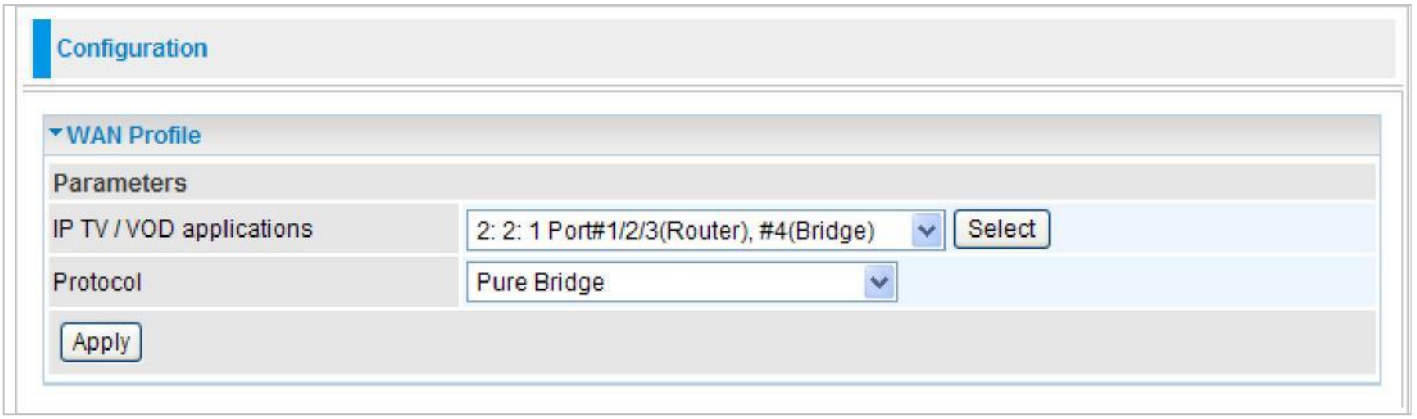
Idle Timeout: Auto-disconnect the broadband firewall gateway when there is no activity on the line for a predetermined period of time.

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

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

Click Apply to confirm the settings.

Pure Bridge

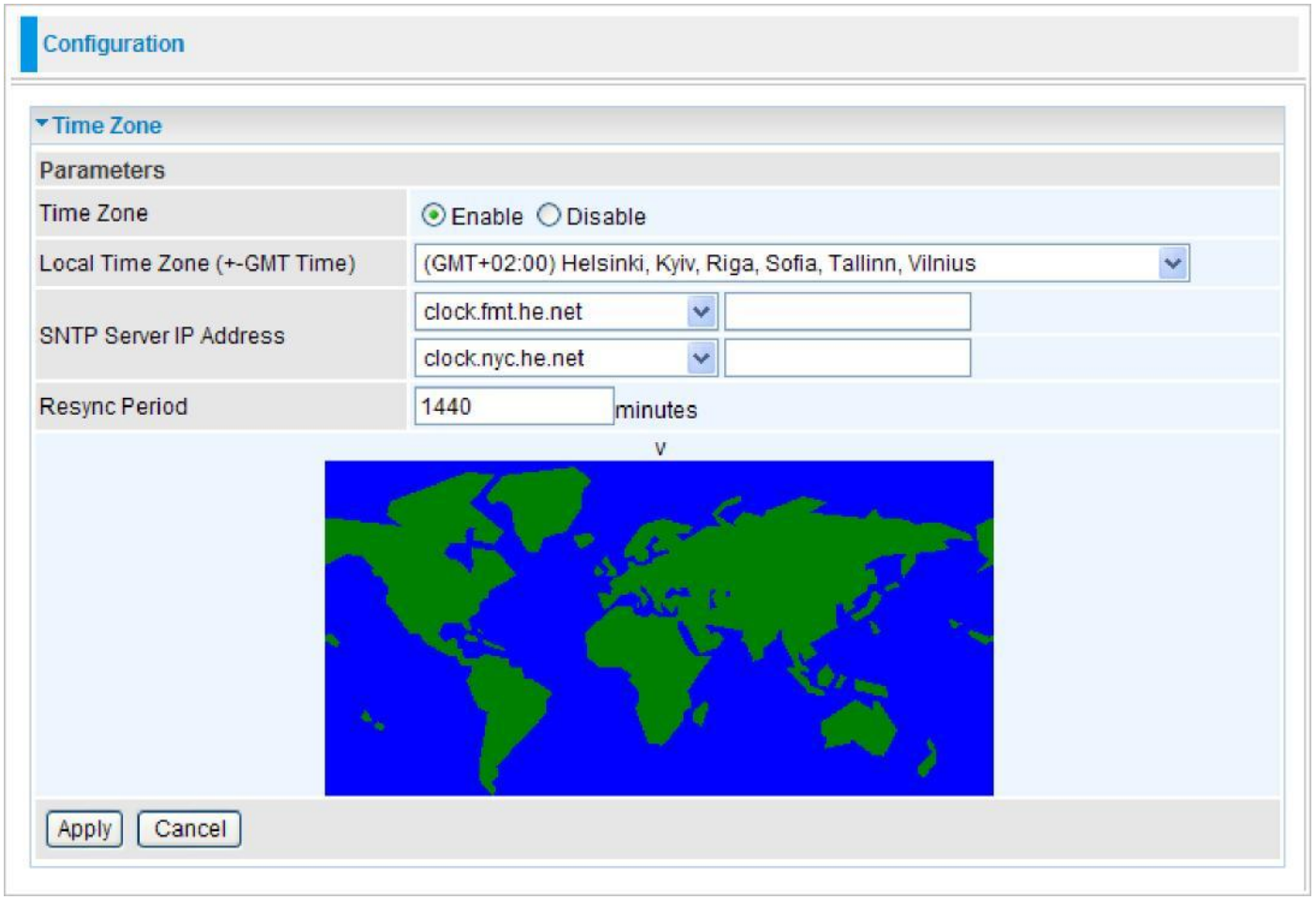


Click Apply to confirm the settings.

System

There are 5 items within the System section: **Time Zone** **Firmware Upgrade** **Backup/Restore** **Restart** **User Management** **Mail Alert** **Syslog** and **Diagnostics Tools**.

Time Zone



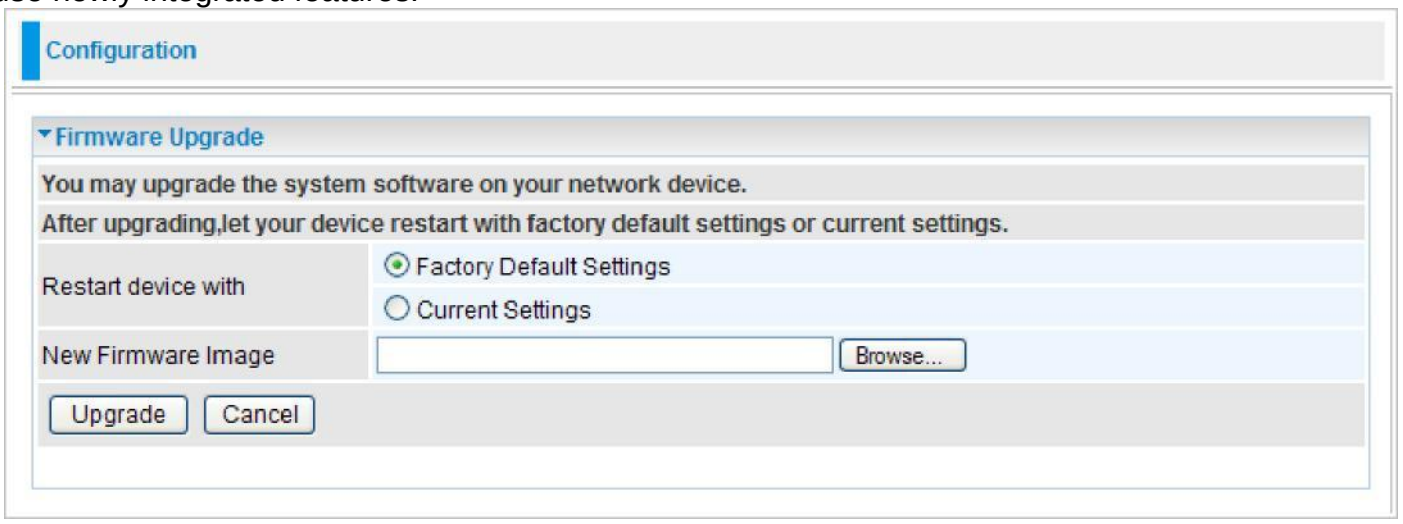
The router does not have a real time clock on board; instead, it uses the Simple Network Time Protocol (SNTP) to get the most current time from an SNTP server outside your network. Choose your local time zone from the drop down menu. To apply the selected local time zone, click Enable and click the Apply button. After a successful connection to the Internet, the router will retrieve the correct local time from the SNTP server you have specified. If you prefer to specify an SNTP server other than those in the drop-down list, simply enter its IP address in their appropriate blanks provided as shown above. Your ISP may also provide an SNTP server for you to use.

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

Click Apply to confirm the settings.

Firmware Upgrade

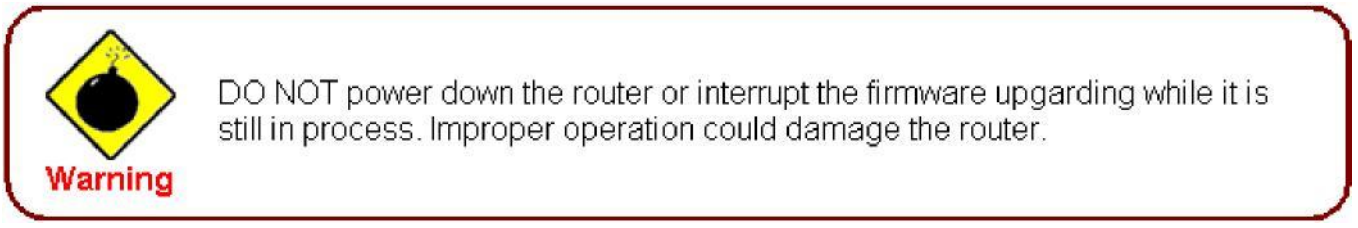
Your router's firmware is the software that enables it to operate and provides all its functionality. Think of your router as a dedicated computer, and the firmware as the software that runs in your router. Thus, by upgrading the newly improved version of the firmware allows you the advantage to use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



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

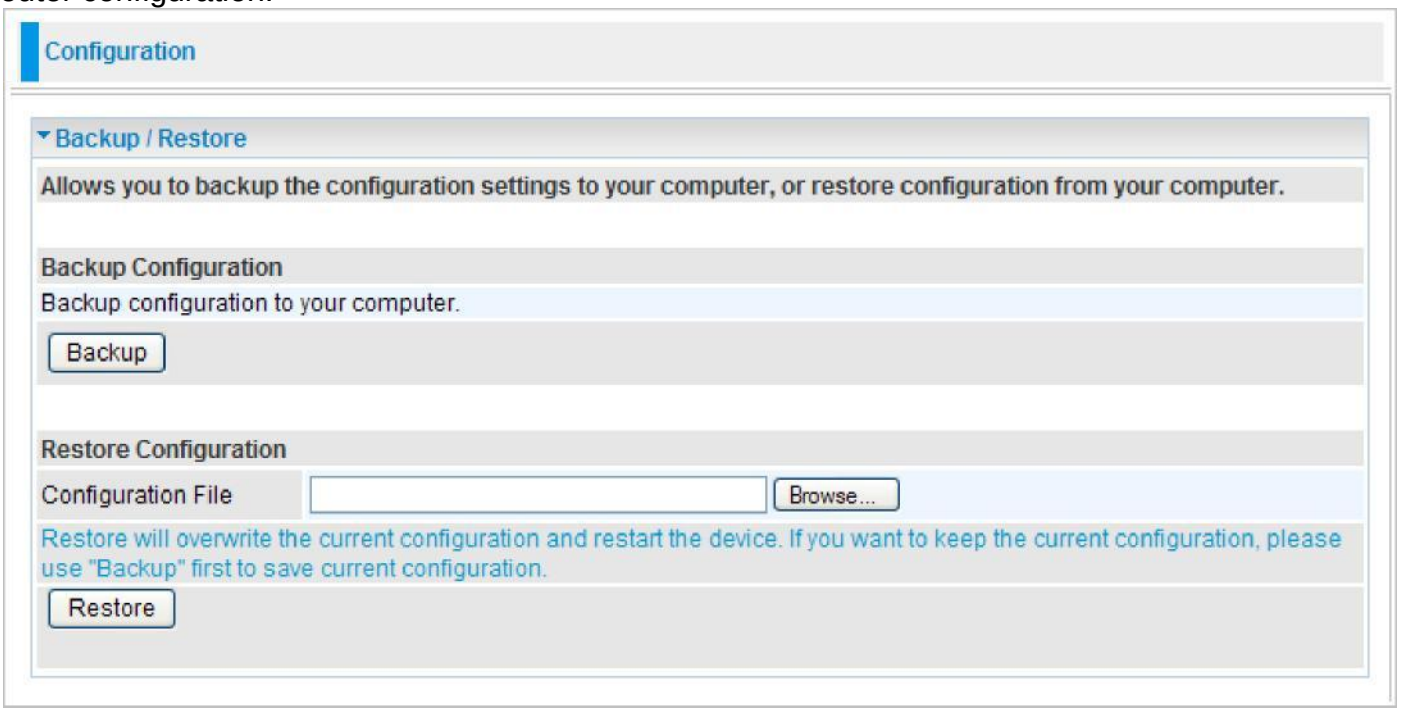
Current Settings: If select this setting, the device will reboot and retain the customized settings of all applications.

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



Backup / Restore

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



Backup Configuration

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

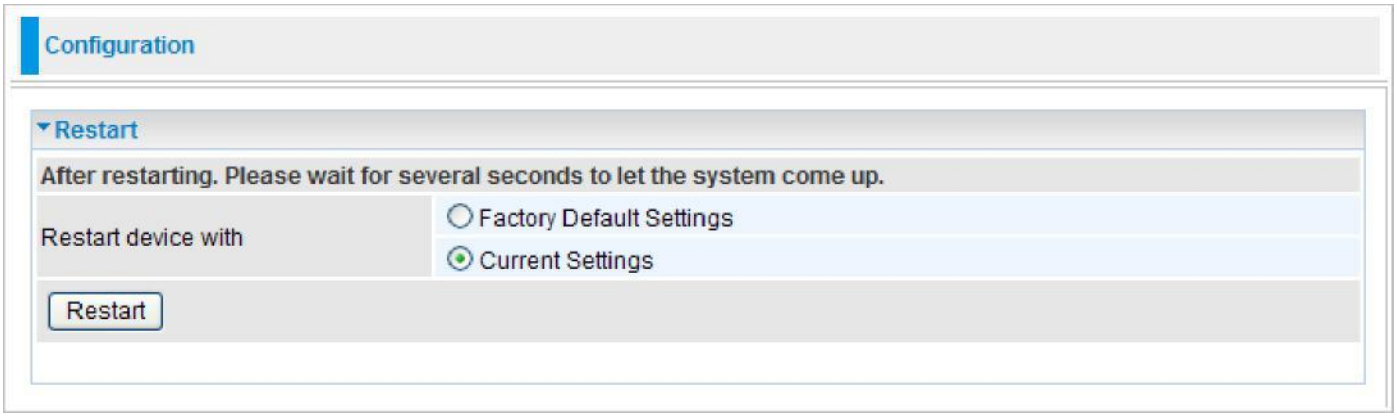
Restore Configuration

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

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

Restart

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



If you wish to restart the router using the factory default settings (for example, after a firmware upgrade or if you have saved an incorrect configuration), select Factory Default Settings to reset to factory default settings.

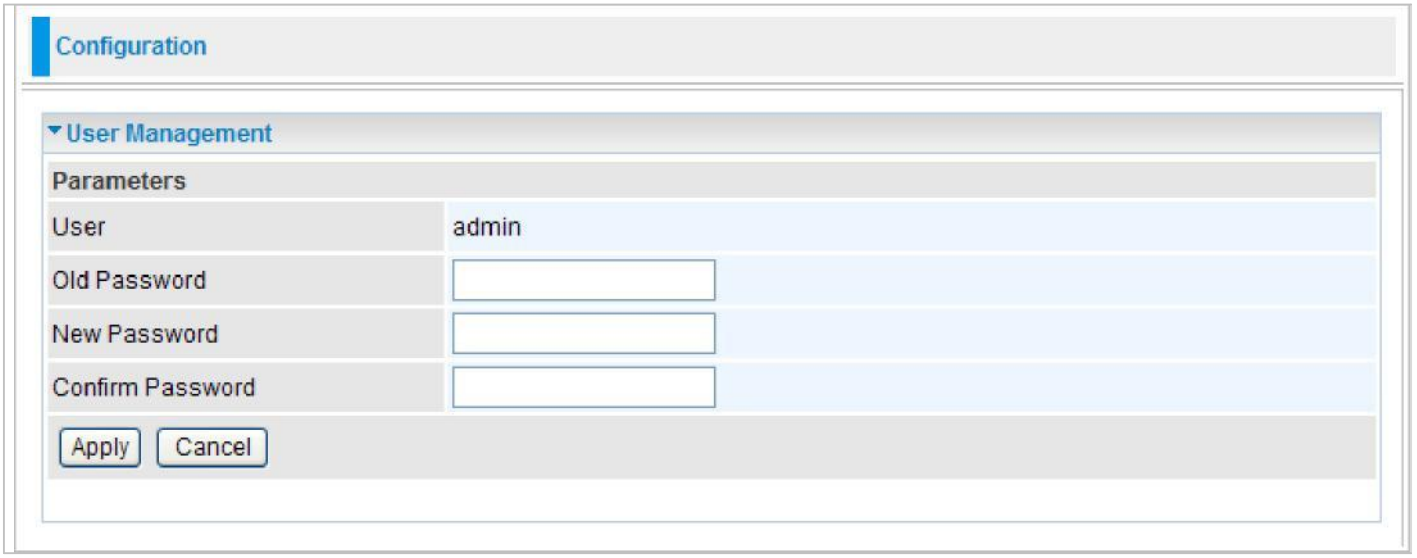
Click Restart with option Current Settings to reboot your router (and restore your last saved configuration).

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

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

User Management

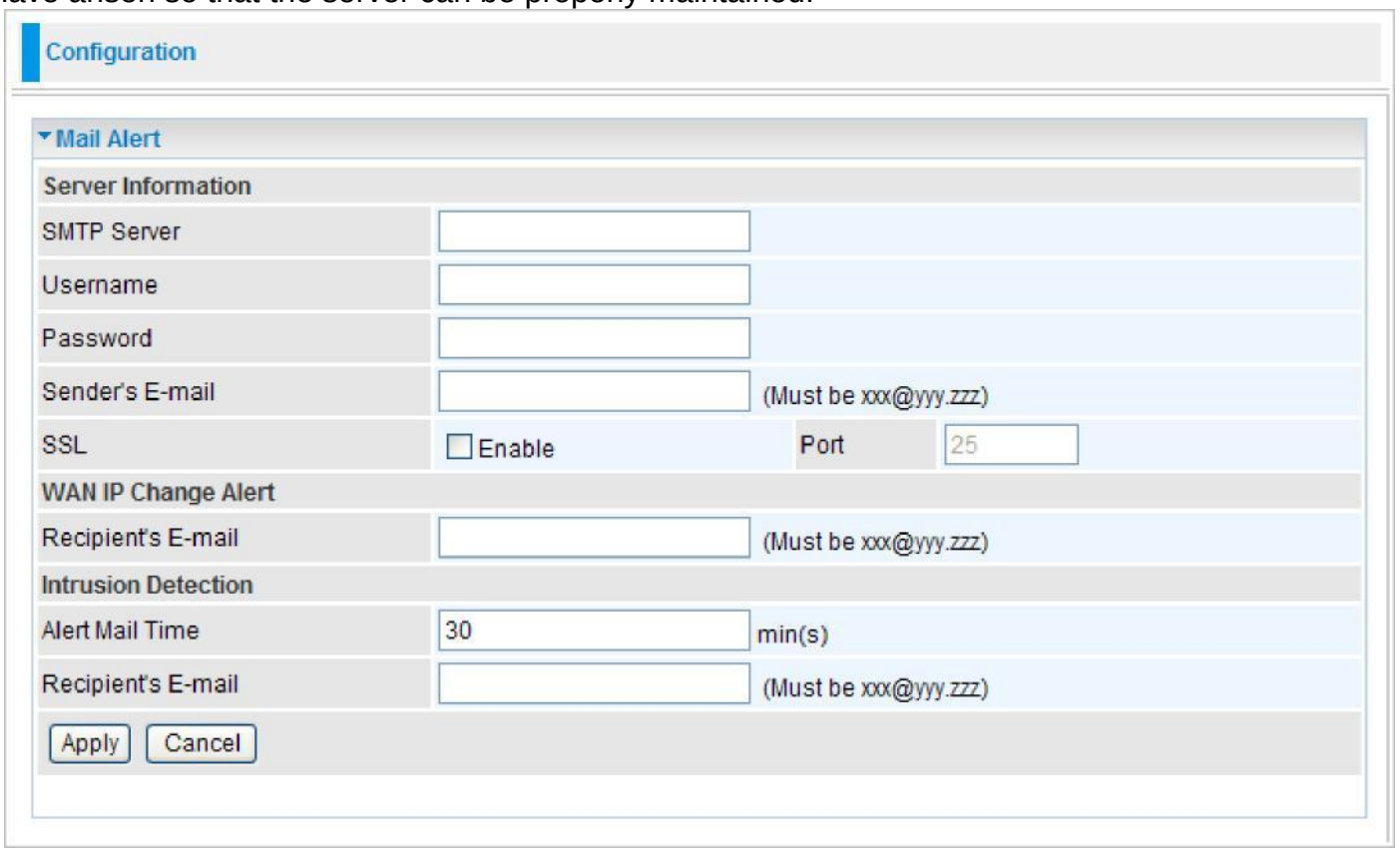
In order to prevent unauthorized access to your router configuration interface, it requires all users to login with a username and password. Therefore only system administrator can access the system. It is highly recommended that you change your password upon receiving your router. The default password is “admin”.



To change your password, simply enter the old password in the Old Password blank. Then enter your new password in the New Password and Confirm Password blanks provided. When this is done, press Apply to save changes.

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.



Server Information

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

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

Password: Enter the password of your email account.

Sender's Email: Enter your email address.

SSL: Tick this box if you want to enable SSL function.

Port: Enter the port number.

WAN IP Change Alert

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

Intrusion Detection

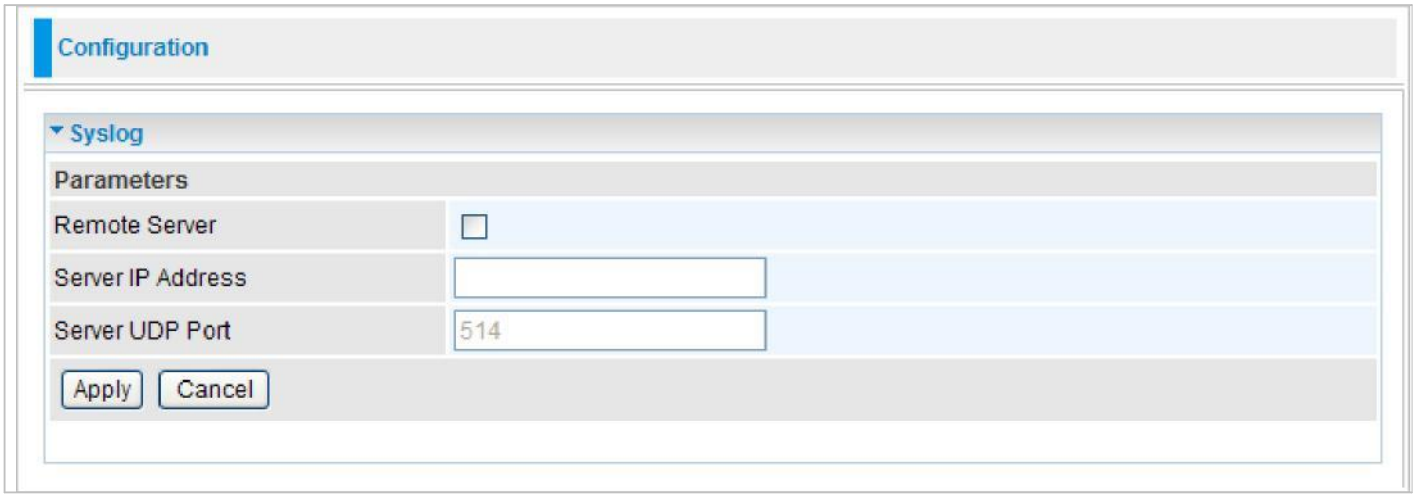
Alert Mail Time: Designate frequency of alerts.

Recipient's Email: Enter the email address that will receive the alert message once an WAN IP change has been detected.

Click Apply to confirm the settings.

Syslog

The Syslog (system log) Server enables the router to transmit event and alert messages across the network to a server using the Syslog protocol. The operating system sends messages at the start or end of a process to report the process status.



Remote Server: Tick to enable system logs to be sent to an external Syslog server. When it is enabled, the following fields are available.

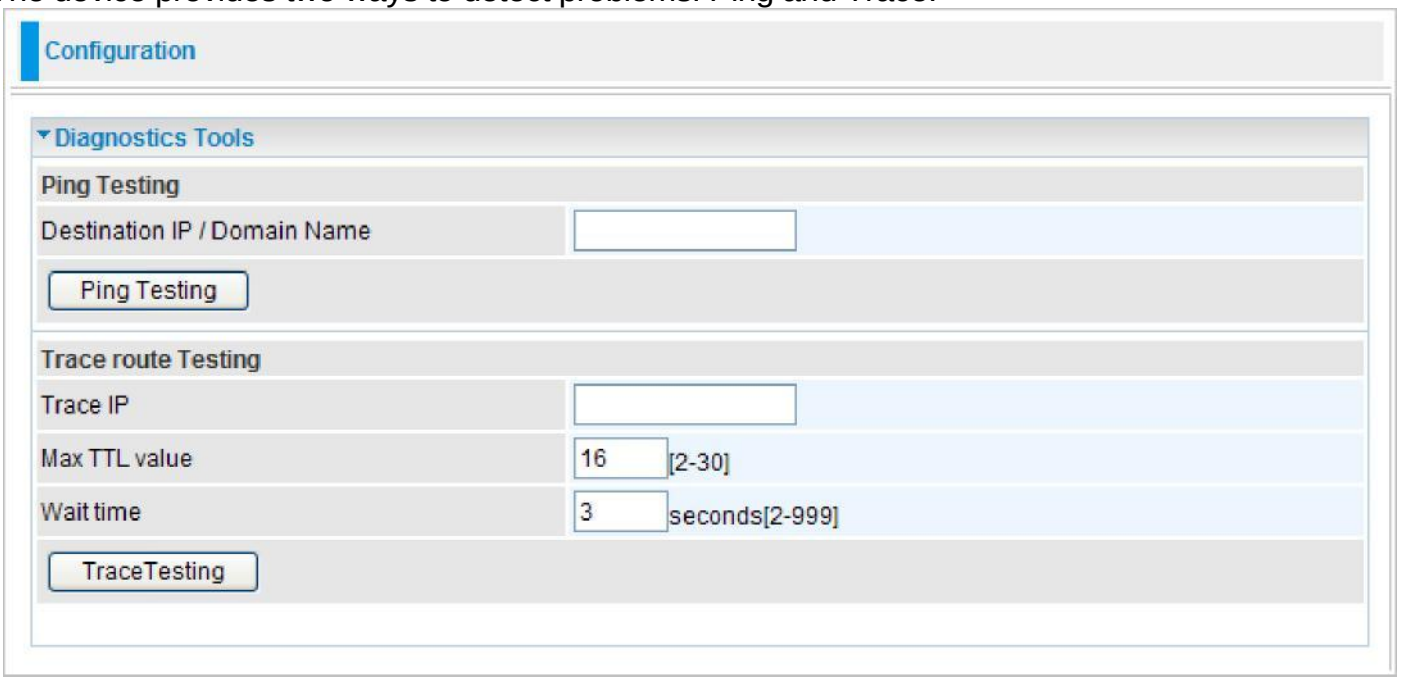
Server IP Address: Enter the server IP address where the Syslog will be saved.

Server UDP Port: Enter the UDP port number.

Click Apply to confirm the settings.

Diagnostics Tools

Diagnostics feature refers to ability to check for problems associated with network connections. The device provides two ways to detect problems: Ping and Trace.



Ping Testing

Ping is a utility that verifies connections to one or more remote hosts. It is a computer network tool used to test whether a particular host is reachable across an IP network.

Destination IP / Domain Name: Enter an IP address or domain name.

Press **Ping Testing** button and the result will be shown on a pop-up screen.

Trace route Testing

Traceroute (Trace for short) is to execute a program in such a way that the sequence of statements being executed can be observed. It is a computer network tool used to determine the route taken by packets across an IP network.

Trace IP: Enter an IP address.

Max TTL value: Enter the

Wait time: Enter the

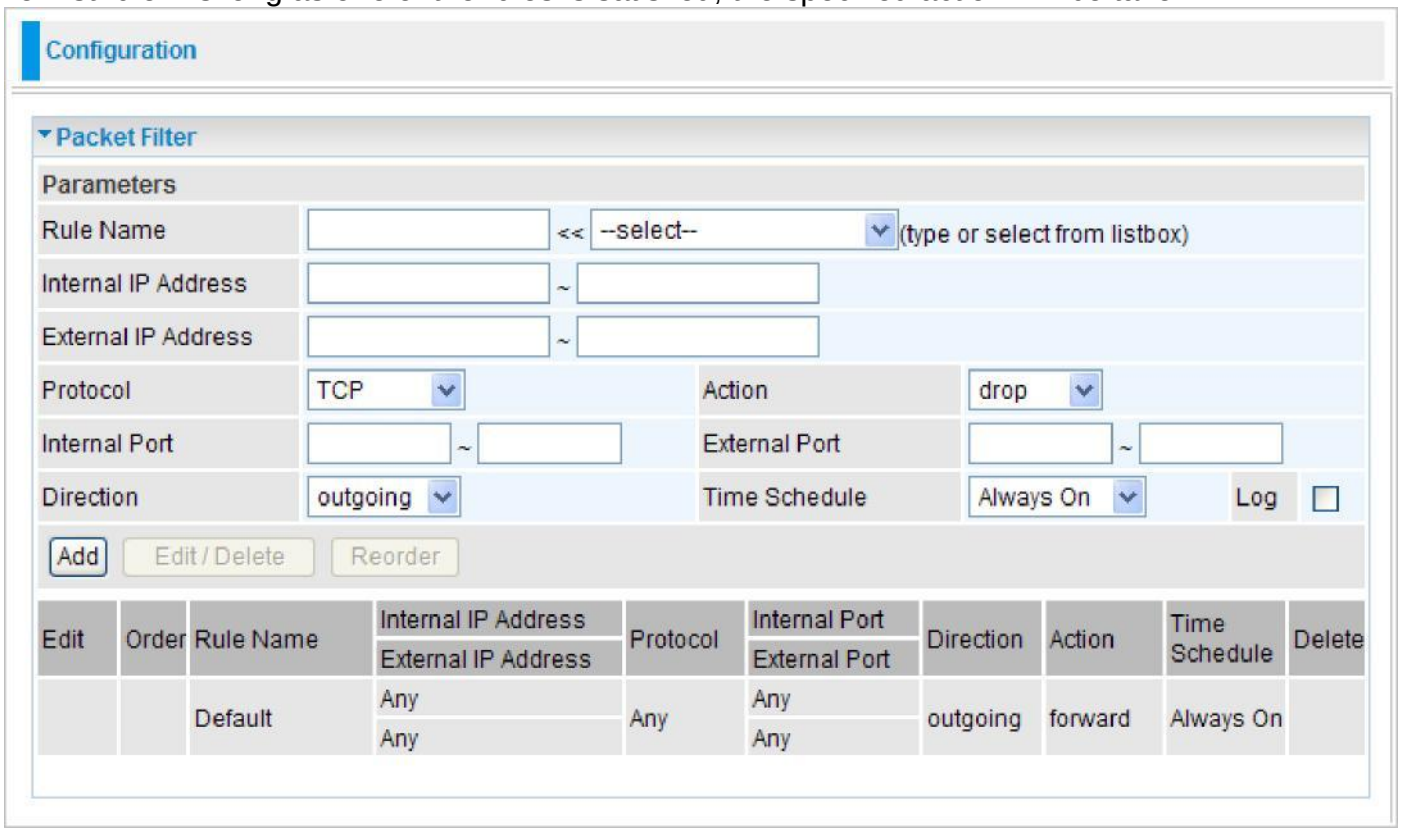
Press **Trace Testing** button and the result will be shown on a pop-up screen.

Firewall

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

Packet Filter

Packet filtering enables you to configure your router to block specific internal / external users (IP address) from Internet access, or disable specific service requests (Port number) to / from the Internet. This configuration program allows you to set up different filter rules for different users based on their IP addresses or their network Port number. The relationship among all filters is “or” operation, which means that the router checks these different filter rules one by one, starting from the first rule. As long as one of the rules is satisfied, the specified action will be taken.



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

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

Protocol: Specify the packet type (TCP, UDP, TCP/UDP) 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 the range from 1 to 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: Check the checking box 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 Edit next to the item you wish to edit, and then change parameters as desired. Complete it by press “Edit/Delete”.

Delete: Check Edit next to the item you wish to delete, and press “Edit/Delete” to remove this rule.

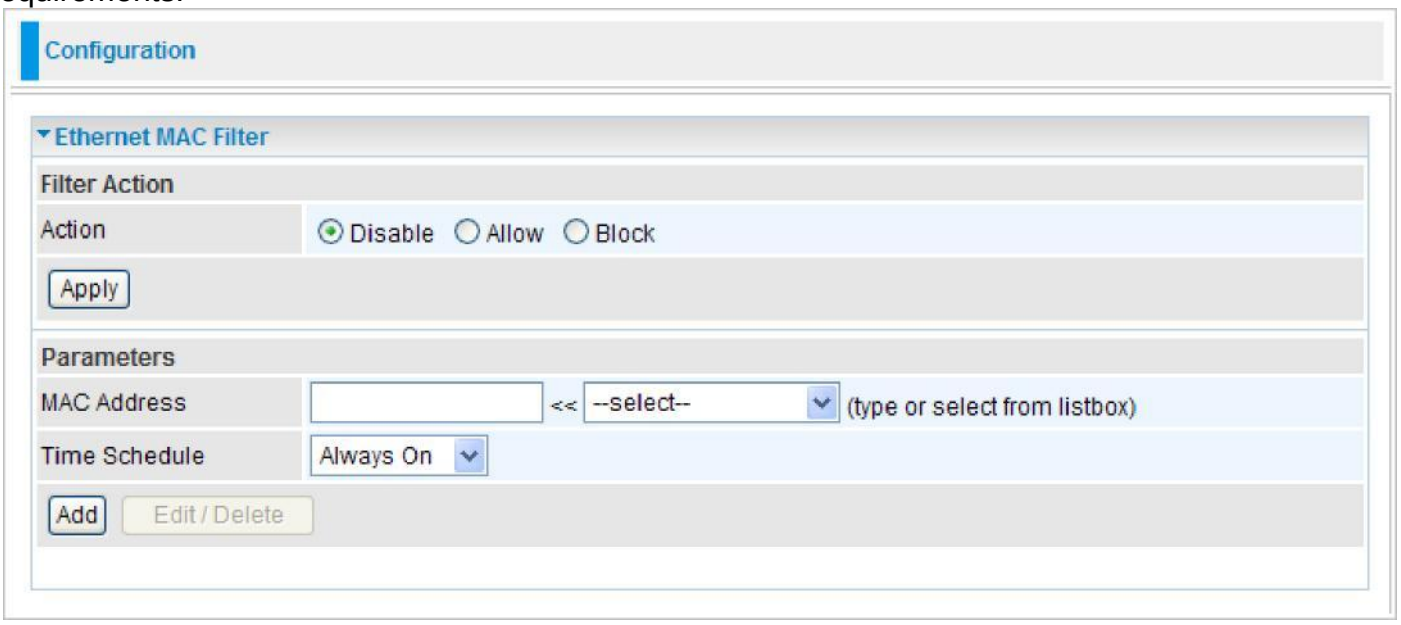
Order: Be aware that packet filtering parameters appear in priority order i.e. the first one takes precedence over all other rules. There is a sort function next to the Rule Name column, you can move the rule to higher or lower priority by clicking the Order arrow, and press “Reorder” to save the new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

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

Ethernet MAC Filter

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

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



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

Filter Action

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

Parameters

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

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

Click Add to apply the settings.

Wireless MAC Filter

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

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

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

Filter Action

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

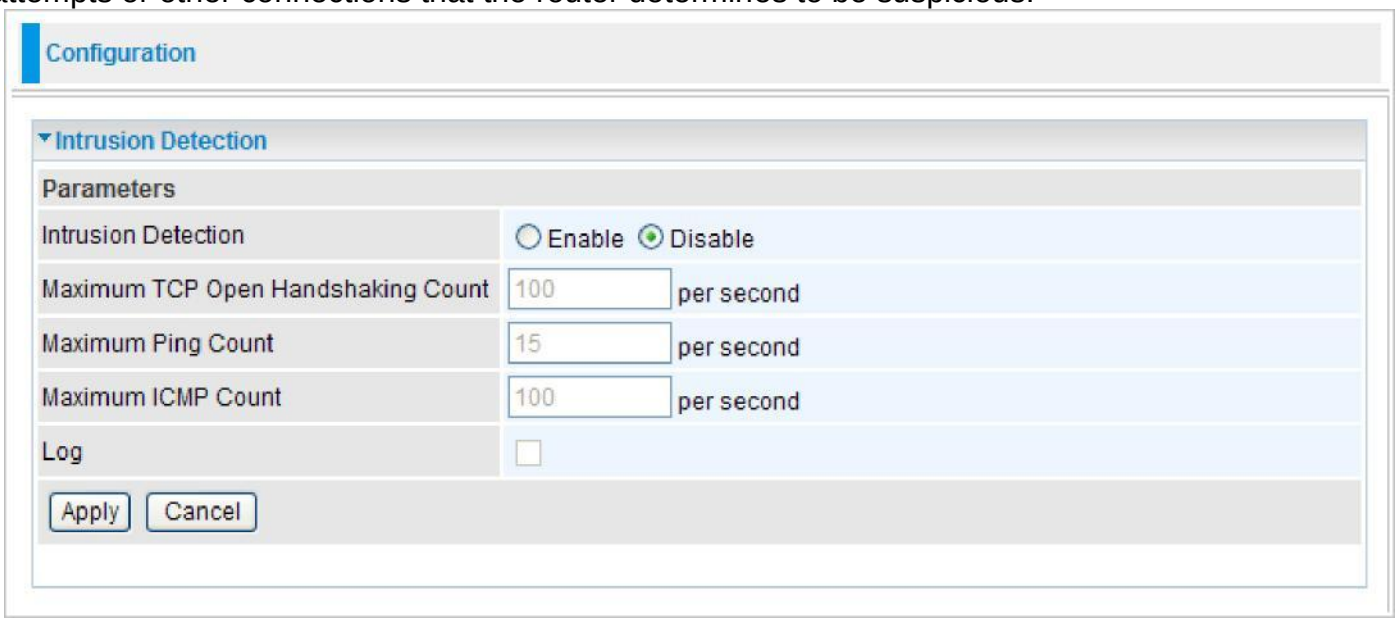
Parameters

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

Click Add to apply the settings.

Intrusion Detection

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



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.

Click Apply to confirm the settings.

Block WAN Ping

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

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

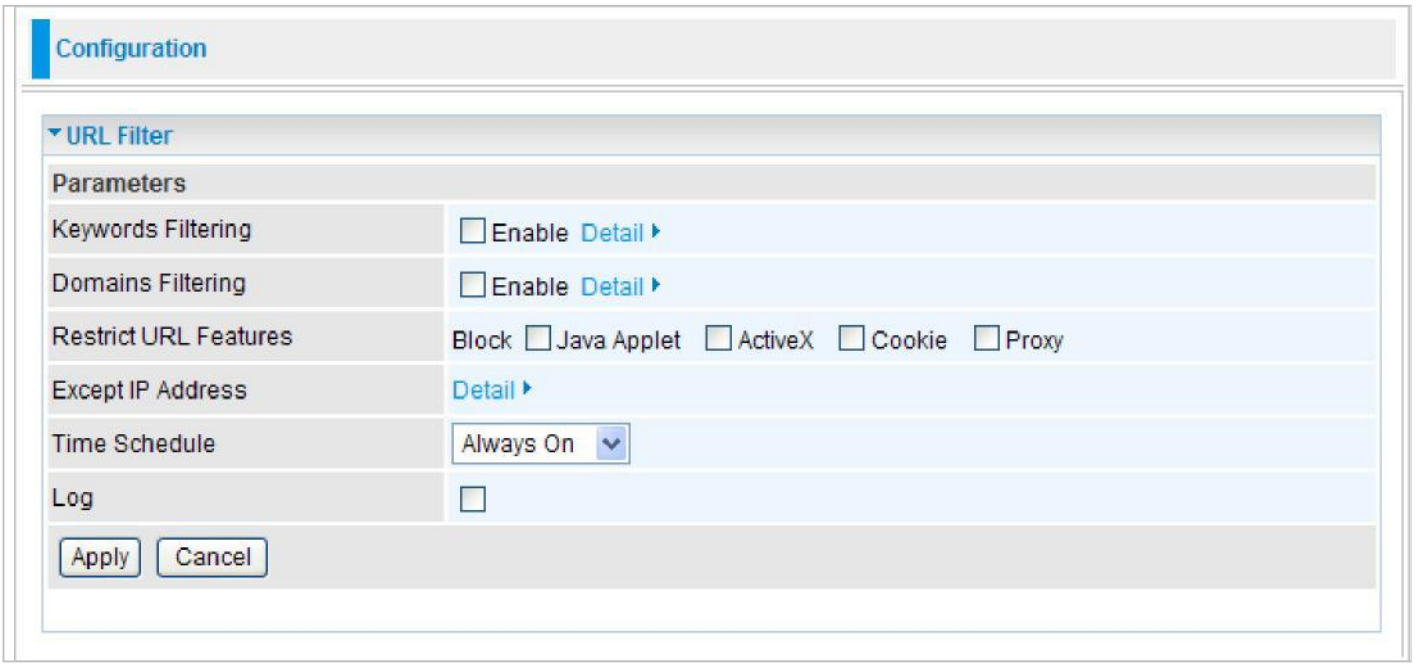
Table: Hacker attack types recognized by the IDS

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

URL Filter

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



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

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

Restrict URL Features: Click Block Java Applet to filter web access with Java Applet components. Click Block ActiveX to filter web access with ActiveX components. Click Block Cookie to filter web access with Cookie components. Click Block Proxy to filter web proxy access.

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

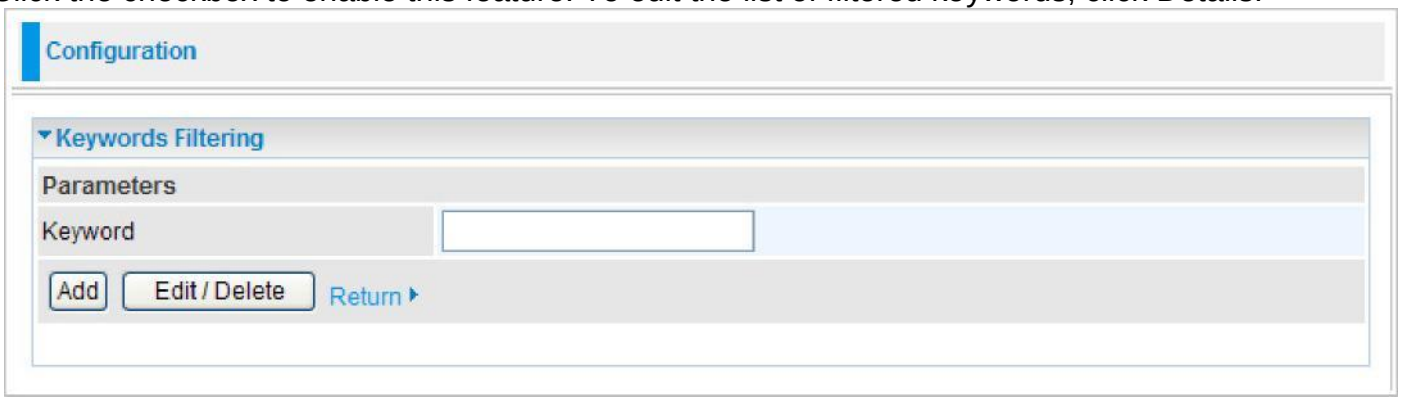
Time Schedule: A self defined time period. You may specify a time schedule for your prioritization policy. For setup and detail, refer to Time Schedule section.

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

Click Apply to confirm the settings.

Keywords Filtering

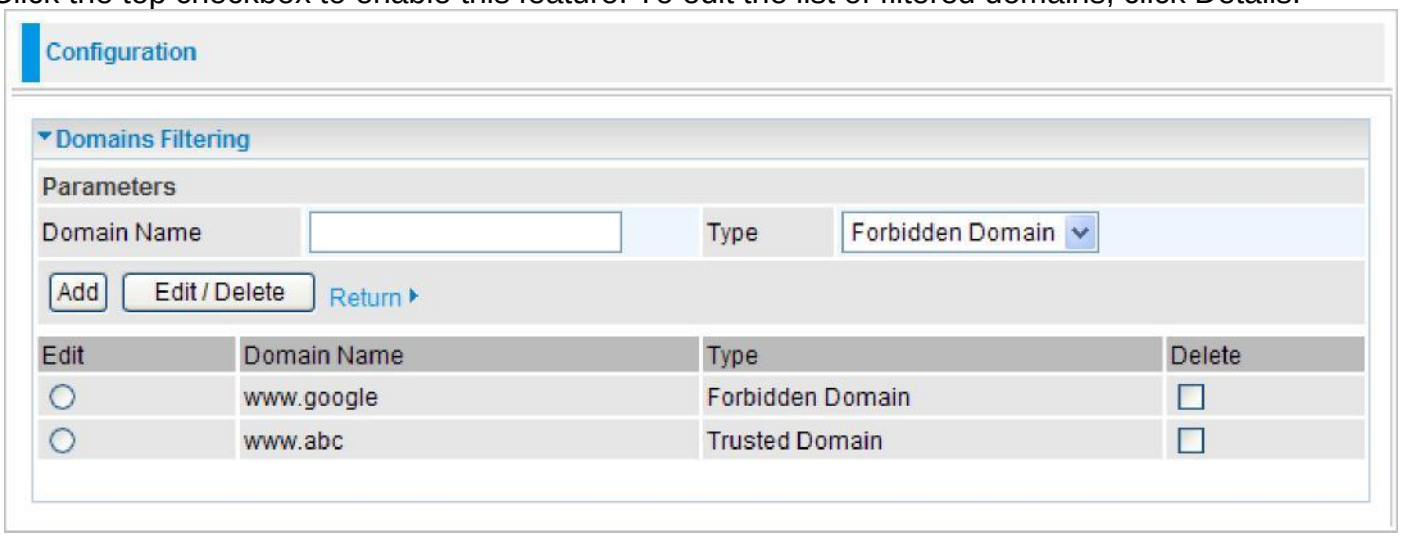
Click the checkbox to enable this feature. To edit the list of filtered keywords, click Details.



Enter a keyword to be filtered and click Apply. Your new keyword will be added to the filtered keyword listing. For example, if the URL is **http://www.abc.com/abcde.html** it will be dropped as the keyword “abcde” occurs in the URL.

Domains Filtering

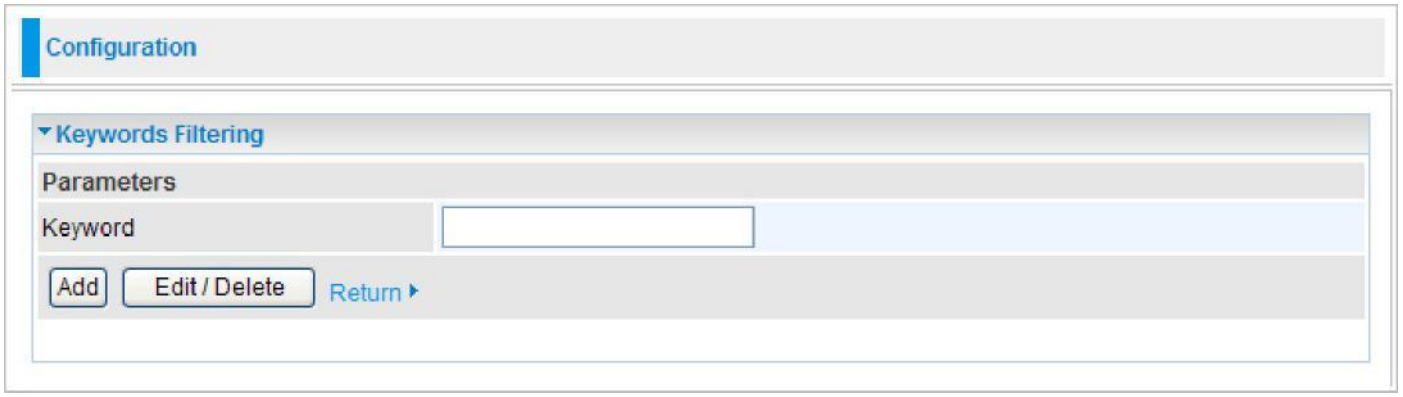
Click the top checkbox to enable this feature. To edit the list of filtered domains, click Details.



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

Except IP Address

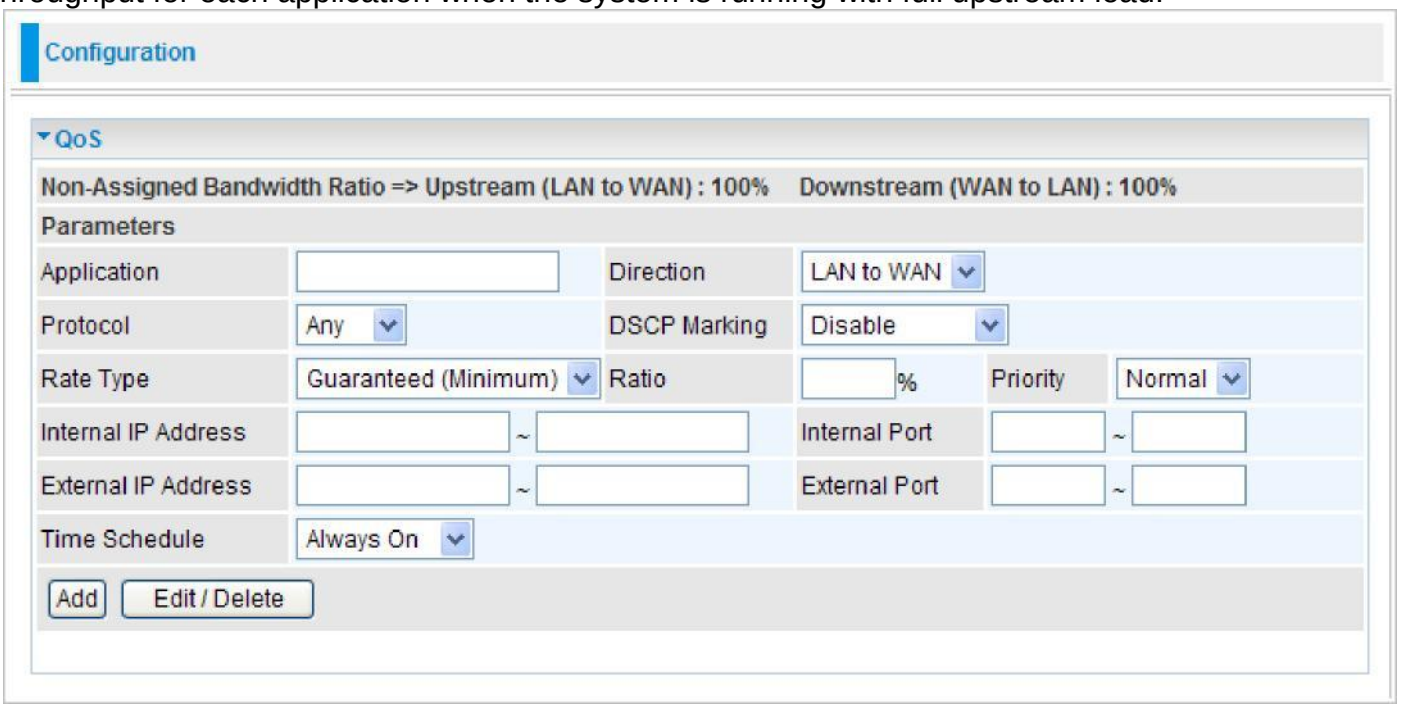
You may also designate which IP addresses are to be excluded from these filters by adding them to the Exception List. To do so, click Details.



Enter the except IP address. Click Add to save your changes. The IP address will be entered into the Exception List, and excluded from the URL filtering rules in effect.

QoS - Quality of Service

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



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

Direction: Select the direction mode of the QoS application.

Protocol: Select the supported protocol from the drop down list.

DSCP Marking: Differentiated Services Code Point (DSCP), it is the first 6 bits in the ToS byte. DSCP Marking allows users to classify the traffic of the application to be executed according to the DSCP value.

Priority: The priority given to each policy/application. Its default setting is set to Normal. You may adjust this setting to fit your policy / application.

Internal IP Address / External IP Address: This is used to classify the traffic of a specific range of internal/external IP address(es). Input the range you want to classify. If only the first IP block is filled, only that IP will be classified. If you leave these four fields empty, it means any classify IP address.

Internal Port: The Port number on the LAN side.

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

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

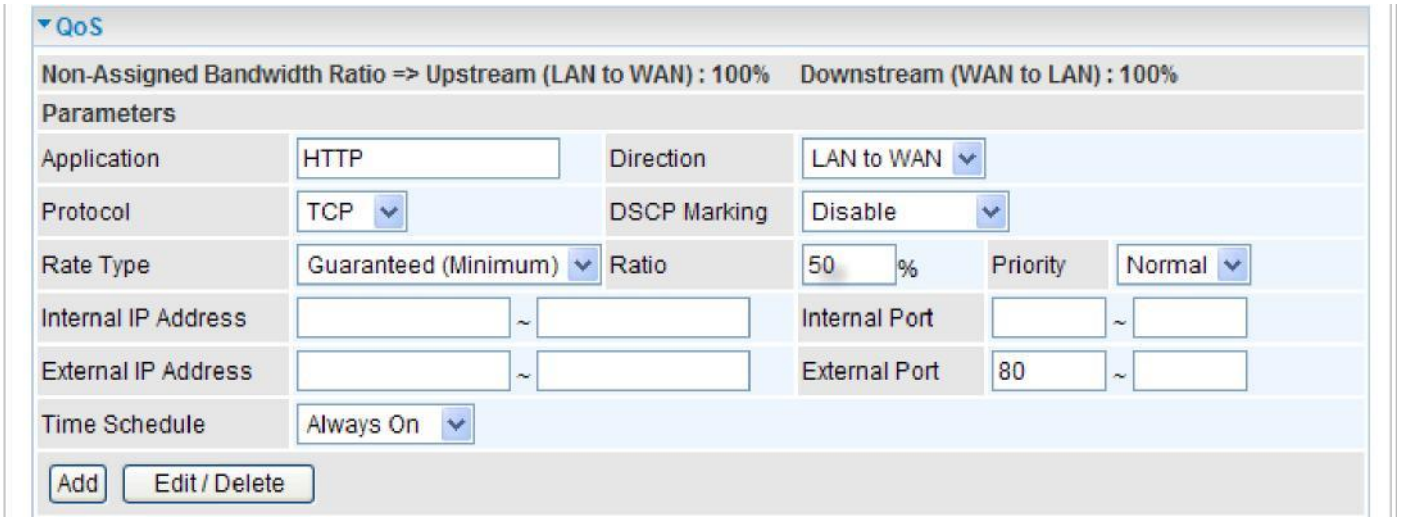
Example 1: Optimize Your Home Network with QoS

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

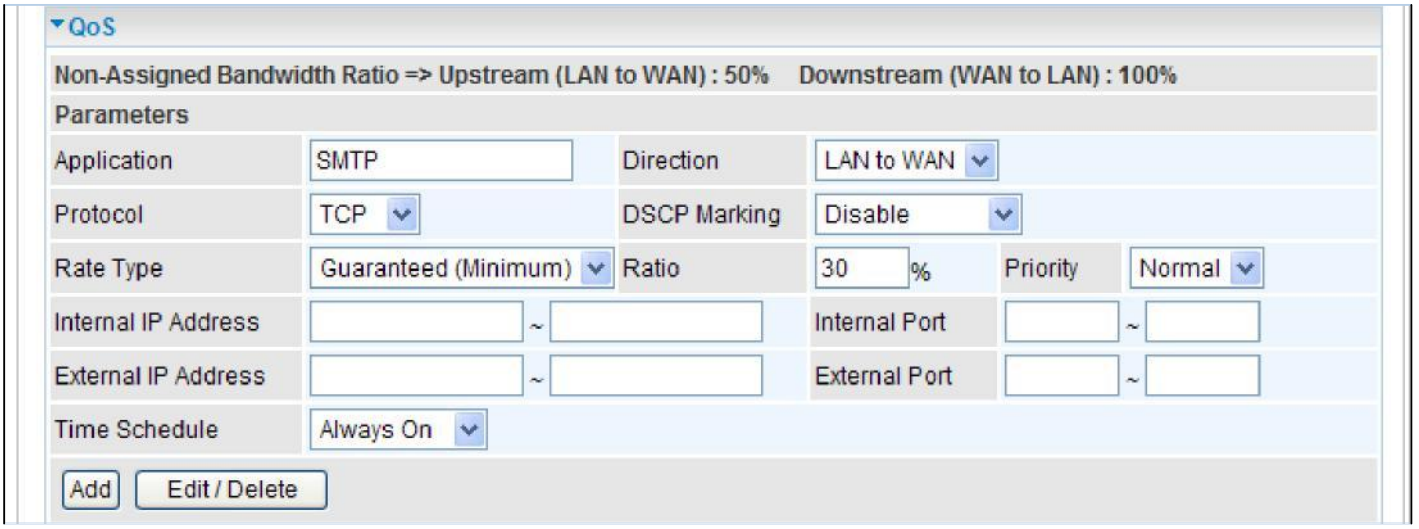
Therefore, in order to assign the priority status of each application, we must first create a new QoS rule for each application.

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

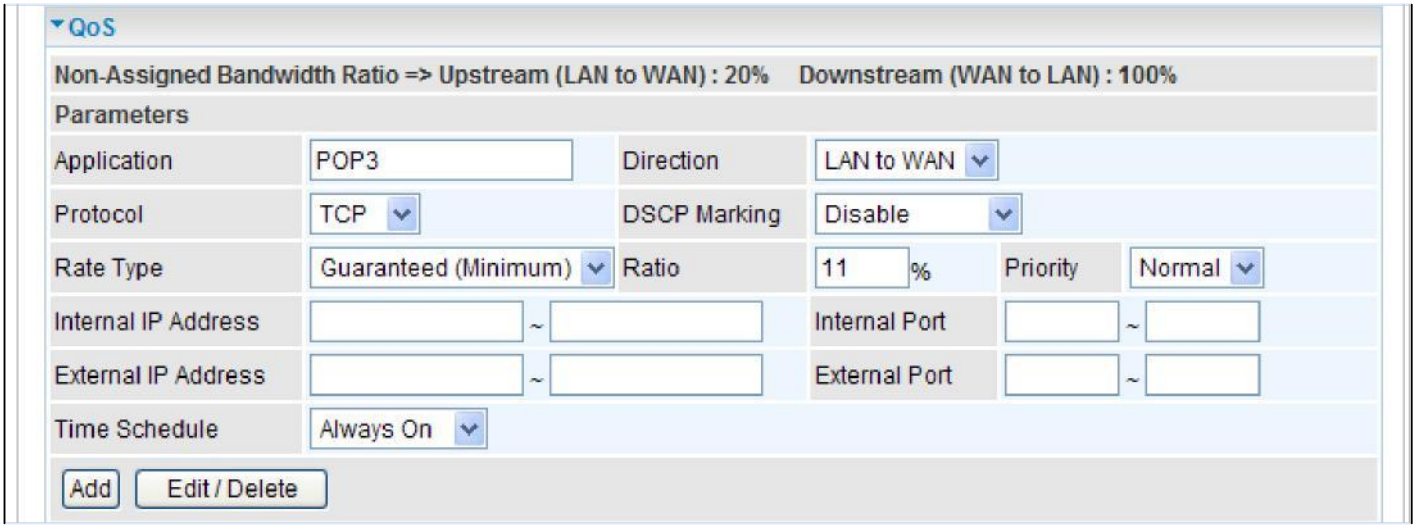
For Web Browsing



For Mail Sending



For Mail Receiving

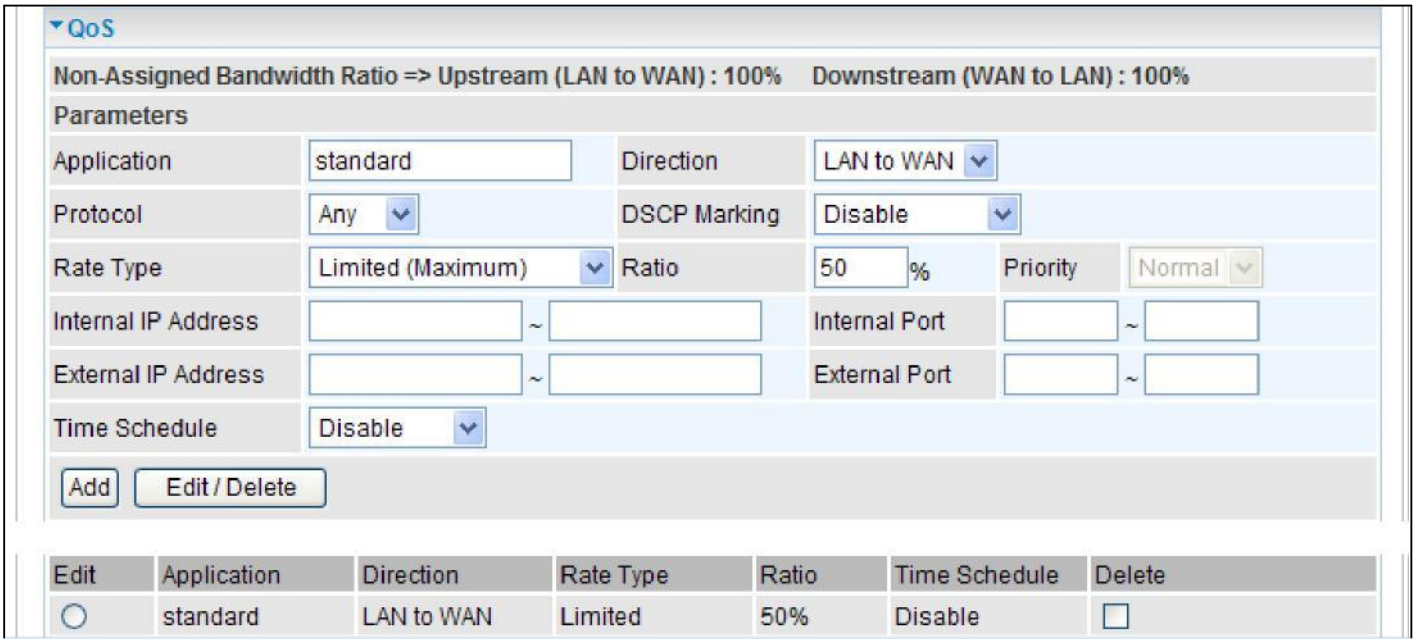


QoS Rules created

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	☐
○	POP3	LAN to WAN	Guaranteed	11%	Always On	☐

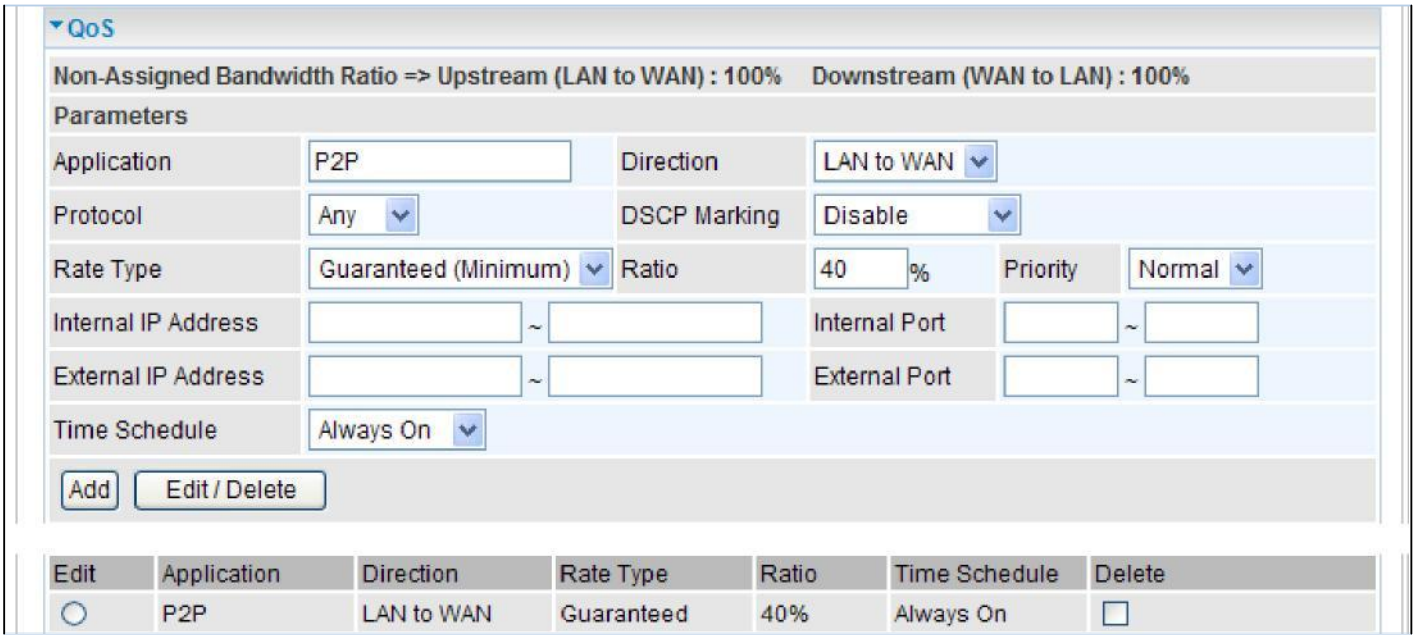
Example 2: Optimize Your Home Network with QoS

If you are running a lot of standard applications you cn just create a QoS rule that has its port range set from 1 ~ 1024 and its priority set to High. This port range is defined in RFC and so it can be used by all standard applications like FTP, Telnet, HTTPS etc.



Example 3: Optimize Your Home Network with QoS

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



Virtual Server

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

The device can be configured as a virtual server so that remote users accessing services such as Web or FTP services via the public (WAN) IP address can be automatically redirected to local servers in the LAN network. Depending on the requested service (TCP/UDP port number), the device redirects the external service request to the appropriate server within the LAN network.

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.

Example: List of some well-known and registered port numbers.

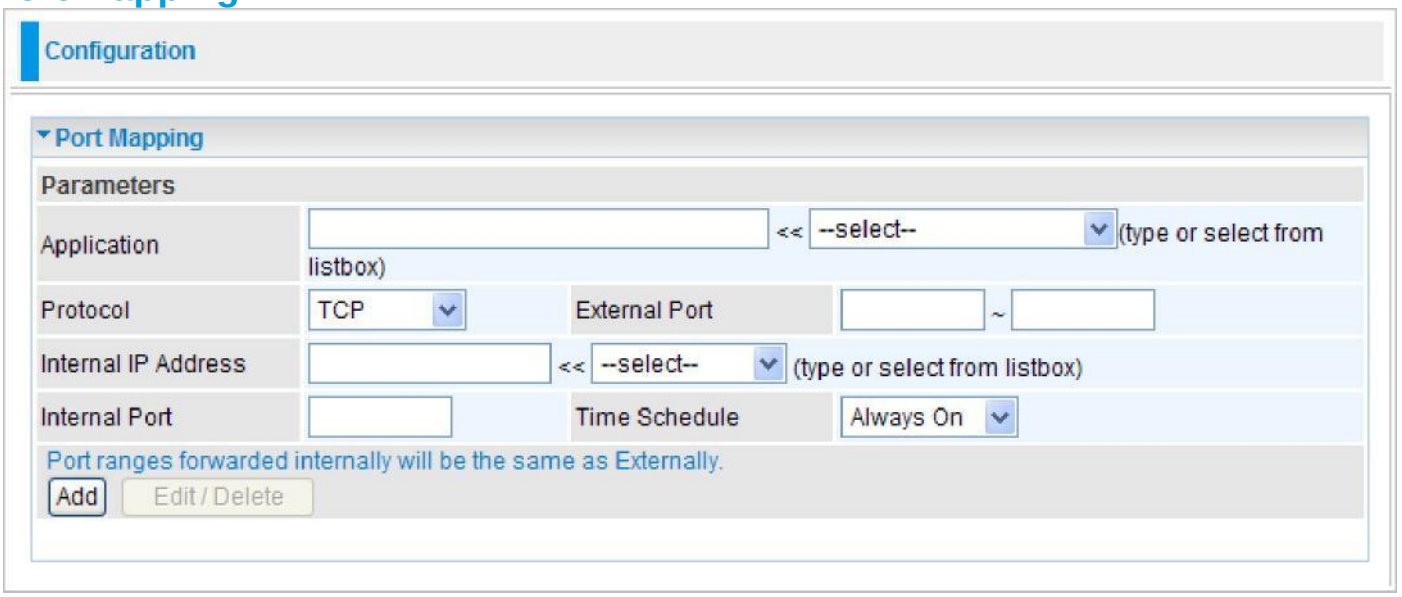
The Internet Assigned Numbers Authority (IANA) is the central coordinator for the assignment of unique parameter values for Internet protocols. Port numbers range from 0 to 65535, but only ports numbers 0 to 1023 are reserved for privileged services and are designated as “well-known ports” (Please refer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

Port Mapping



Application: Select the service you wish to configure.

Protocol: A protocol is automatically applied when an Application is selected from the listbox or you may select a protocol type which you want.

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.

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

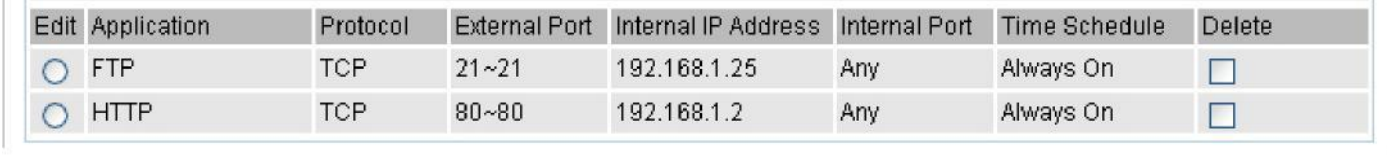
Add: Click to add a new virtual server rule. Click again and the next figure appears.

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

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

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

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

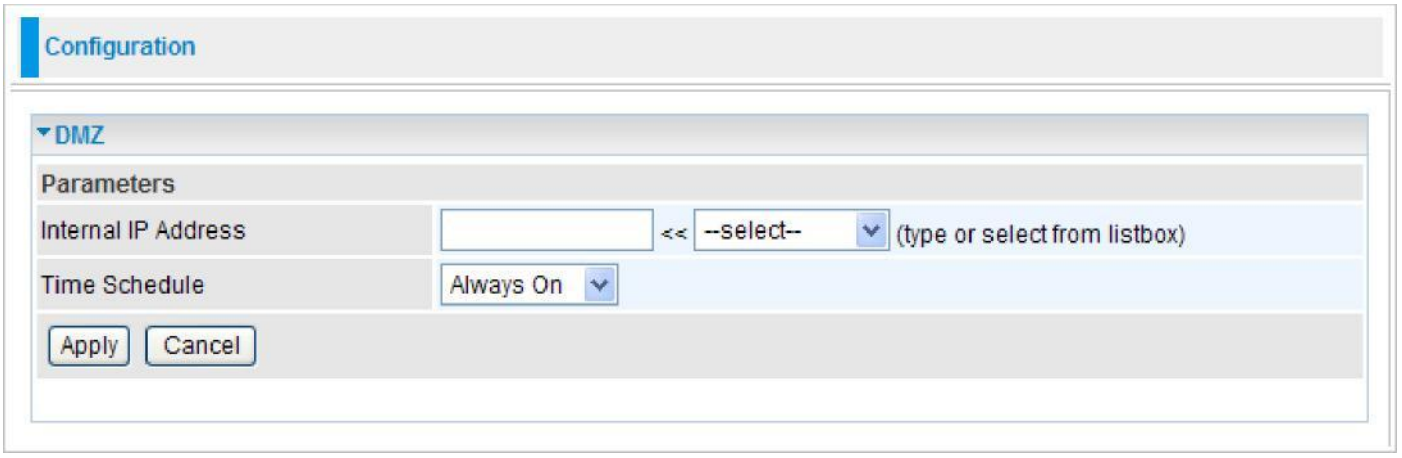


Edit	Application	Protocol	External Port	Internal IP Address	Internal Port	Time Schedule	Delete
○	FTP	TCP	21~21	192.168.1.25	Any	Always On	☐
○	HTTP	TCP	80~80	192.168.1.2	Any	Always On	☐

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

DMZ

The DMZ Host is a local computer exposed to the Internet. When setting a particular internal IP address as the DMZ Host, all incoming packets that do not use a port number which is already used by any other Virtual Server entries will first be checked by the Firewall and NAT algorithms before it is passed to the DMZ host. When this is done, press Apply to save changes.

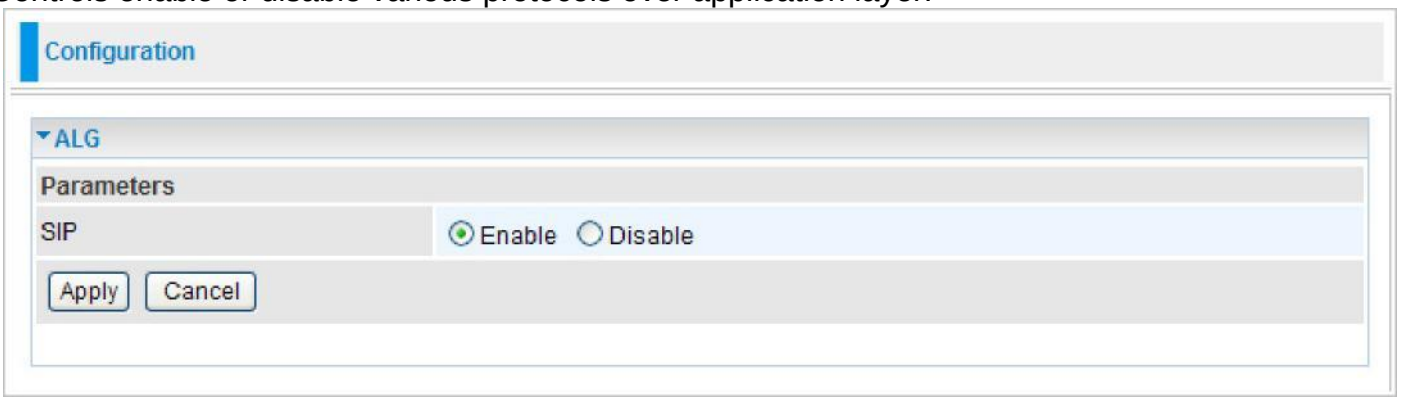


If you have disabled the NAT option in the WAN-ISP section, the Virtual Server will hence become invalid. If the DHCP option is enabled, you have to be very careful in assigning the IP addresses of the virtual servers in order to avoid conflicts. The easiest way of configuring Virtual Servers is to manually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

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

ALG

Controls enable or disable various protocols over application layer.



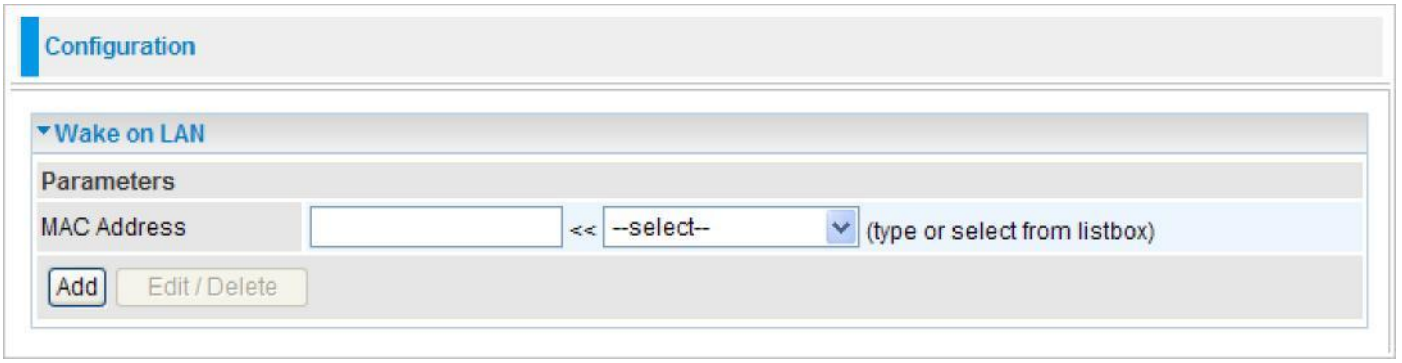
For example, SIP ALG:

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

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

Wake on LAN

WOL allows the router to set a command to turn on a particular computer that can support this feature.



MAC Address: Enter the MAC address of the target computer or you can select the MAC address directly from the **Select** drop down menu on the right. Click Add to save the setting.

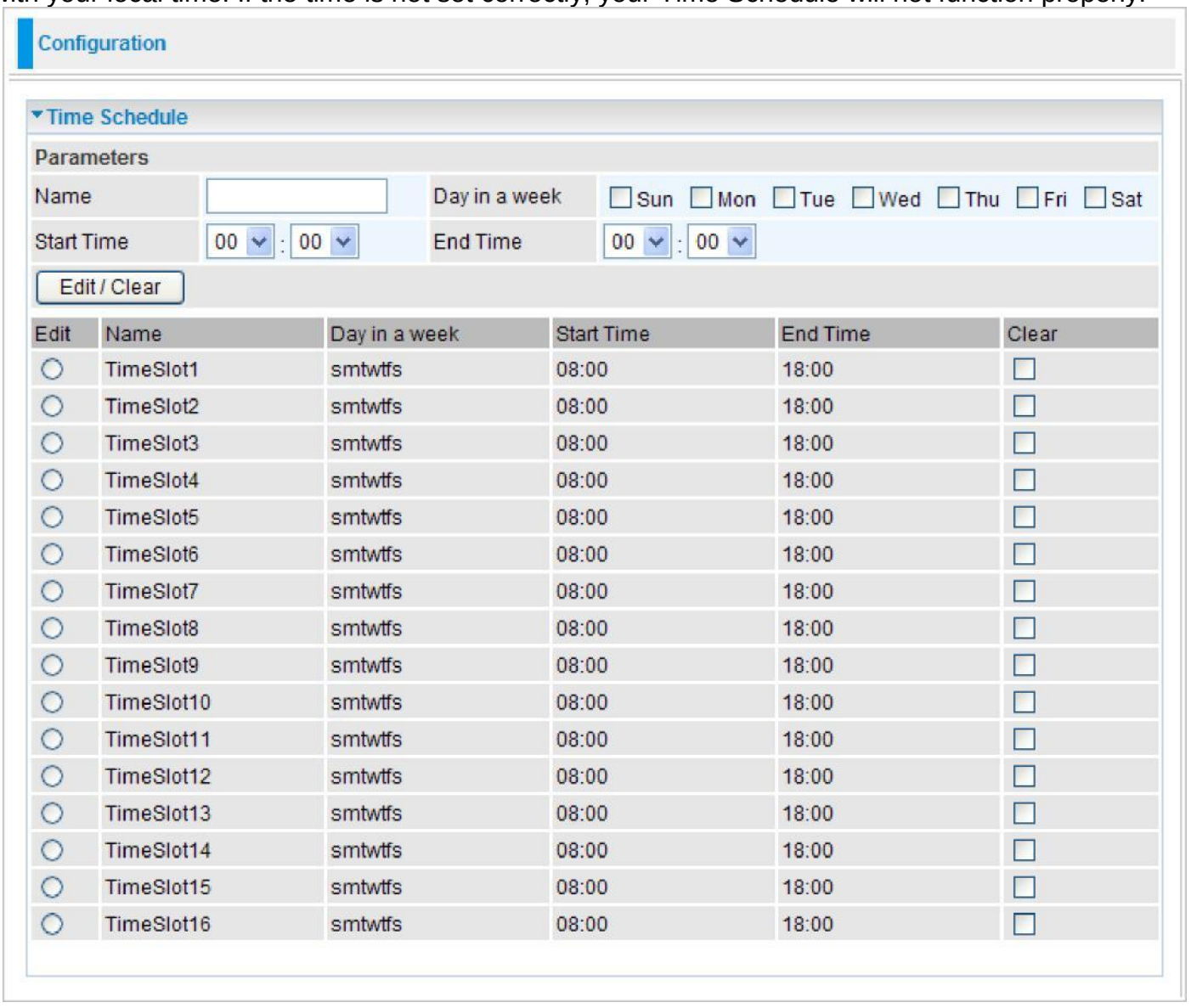
Edit: Check the Edit radio button to display the parameter of the selected entry, then after changing the parameters click the "Edit/Delete" button to apply the changes.

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

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.

Click the Edit/Clear button to save 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.

Here are the items within the Advanced section: **Static Route** **Static ARP** **Dynamic DNS** **VLAN** **Device Management** **IGMP** **TR-069 client** **SNMP** **Access Control** and **Remote Access**

Static Route

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

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

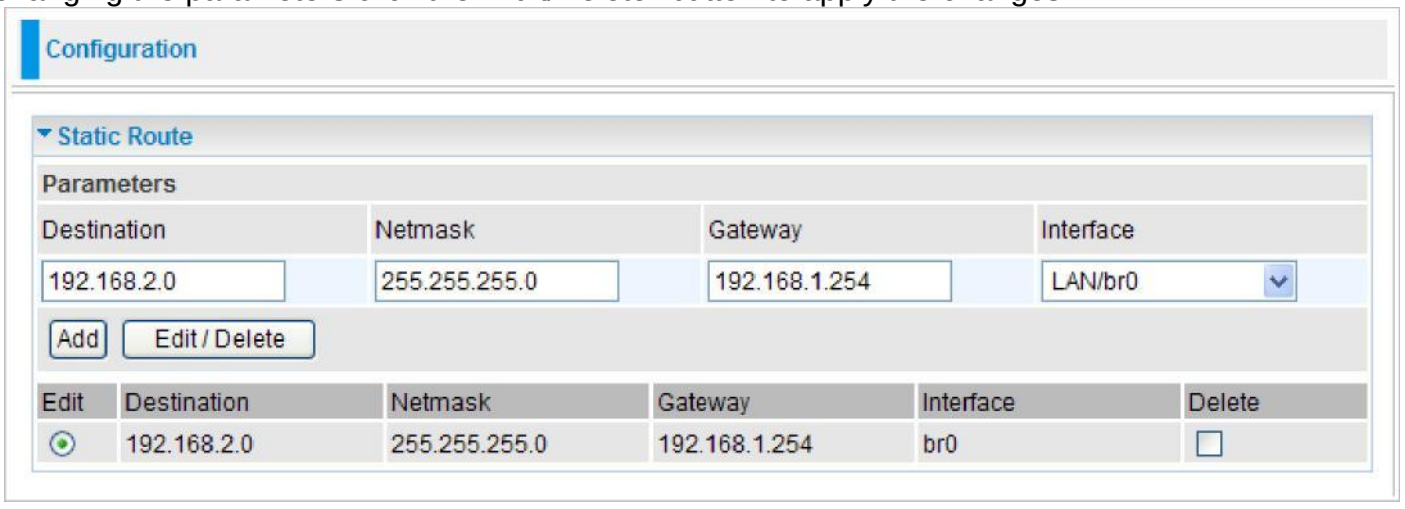
Netmask: Enter the netmask of the destination.

Gateway: Enter the gateway address for the traffic.

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

Click Add to confirm the settings.

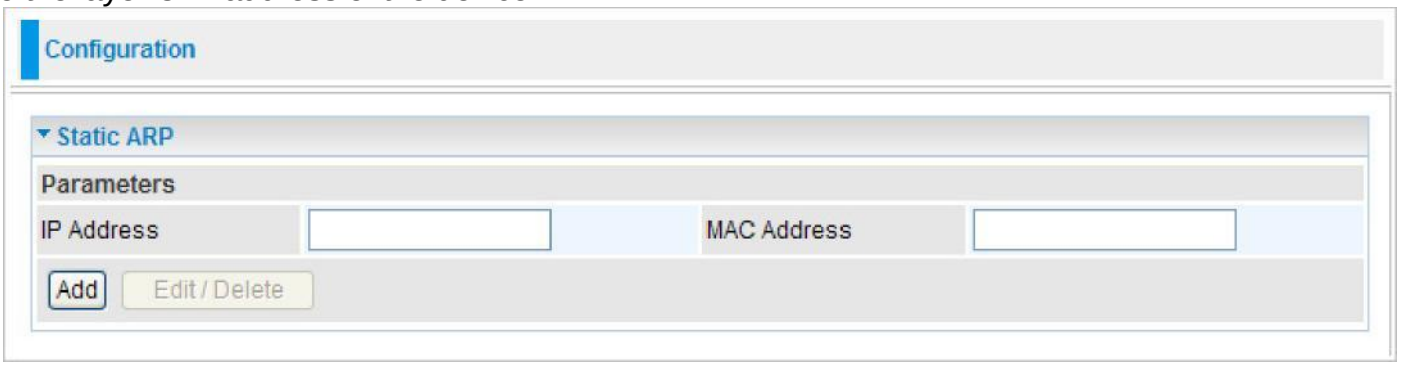
Edit: Check the Edit radio button to display the parameter of the selected application, then after changing the parameters click the "Edit/Delete" button to apply the changes.



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

Static ARP

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

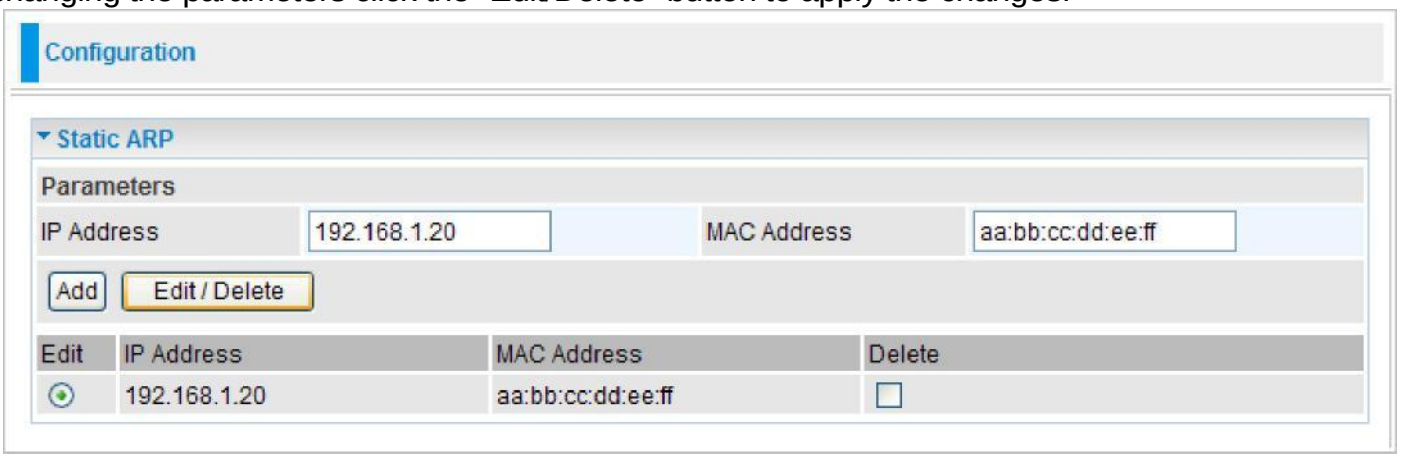


IP Address: Enter the IP of the device that the corresponding MAC address will be mapped to.

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

Click Add to confirm the settings.

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

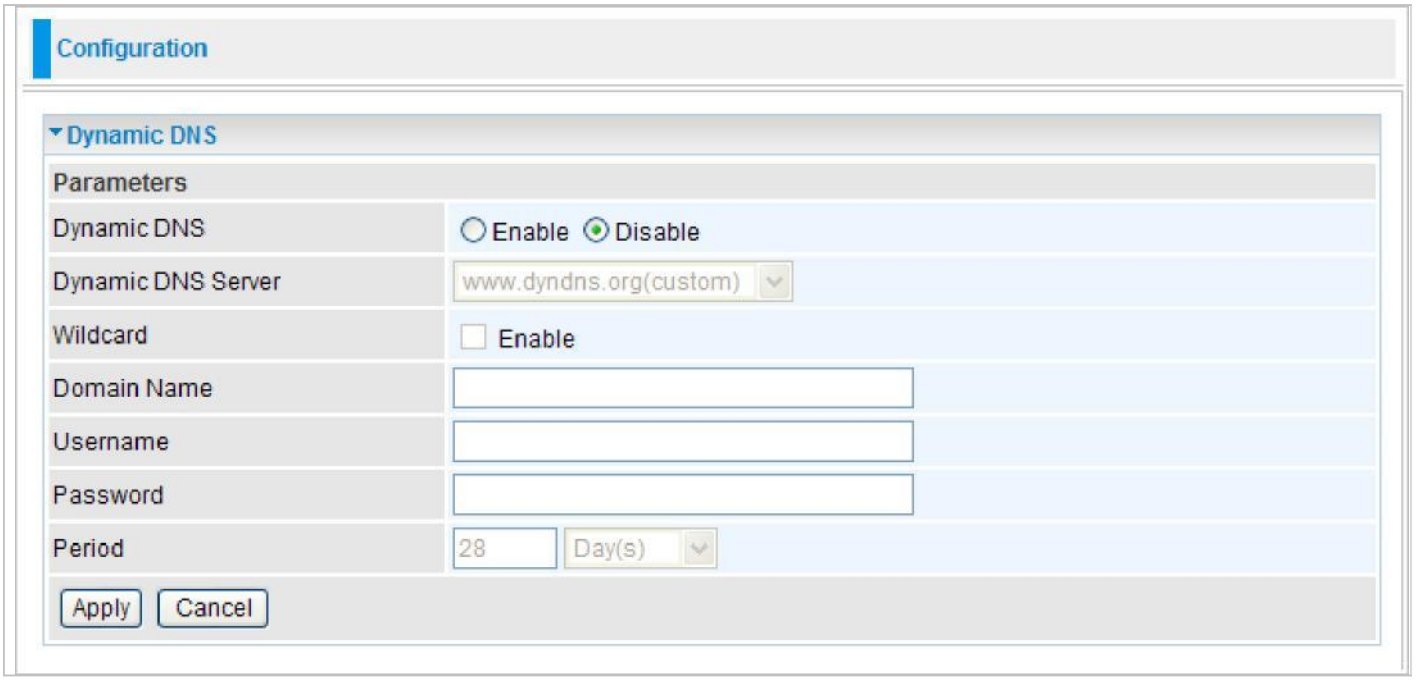


Delete: To remove a static ARP entry, check the Delete box of the selected entry then click the "Edit/Delete" button.

Dynamic DNS

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

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



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

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

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

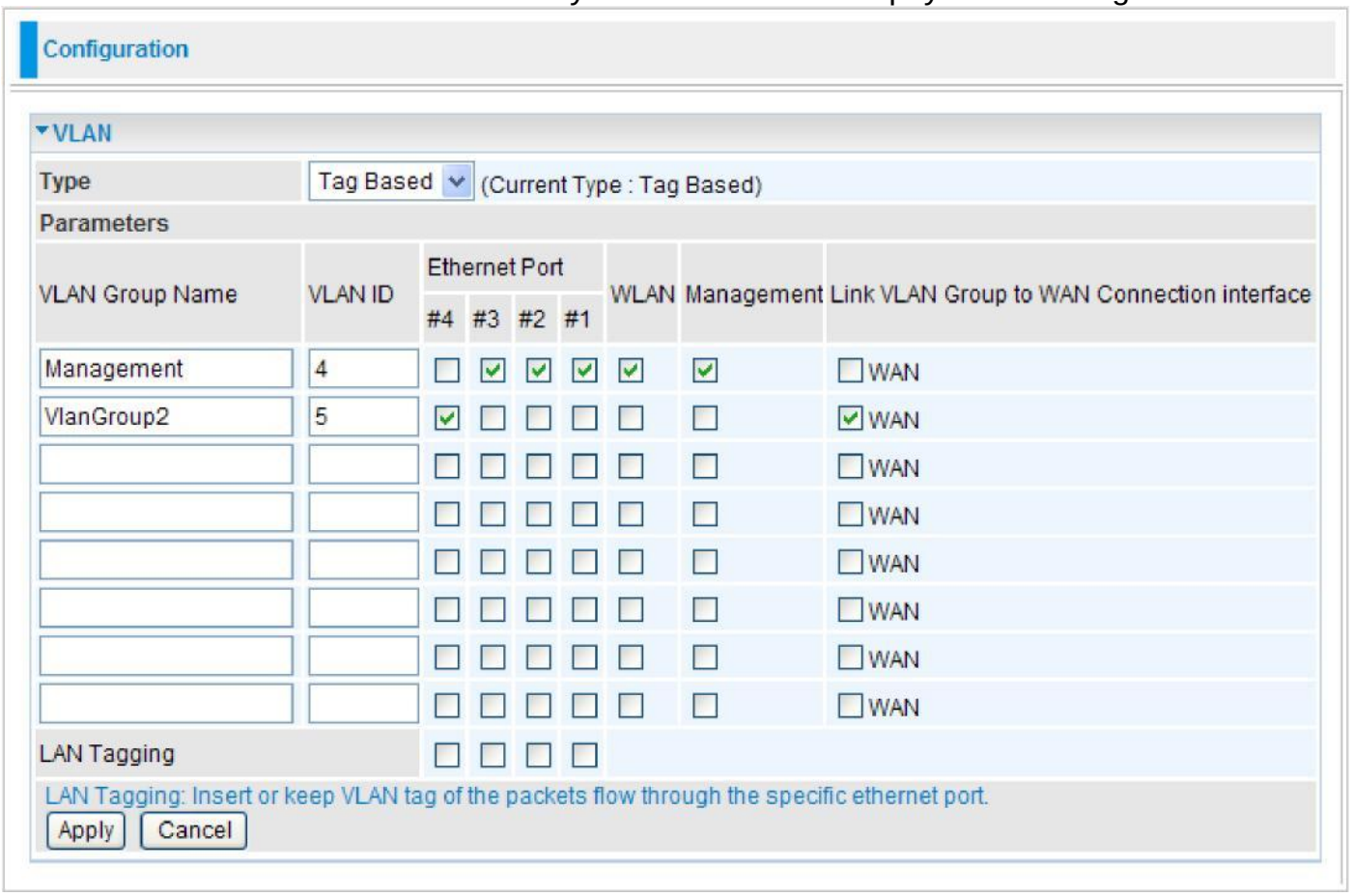
Domain Name, **Username** and **Password:** Enter your registered domain name and your username and password for this service.

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

Click Apply to confirm the settings.

VLAN

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

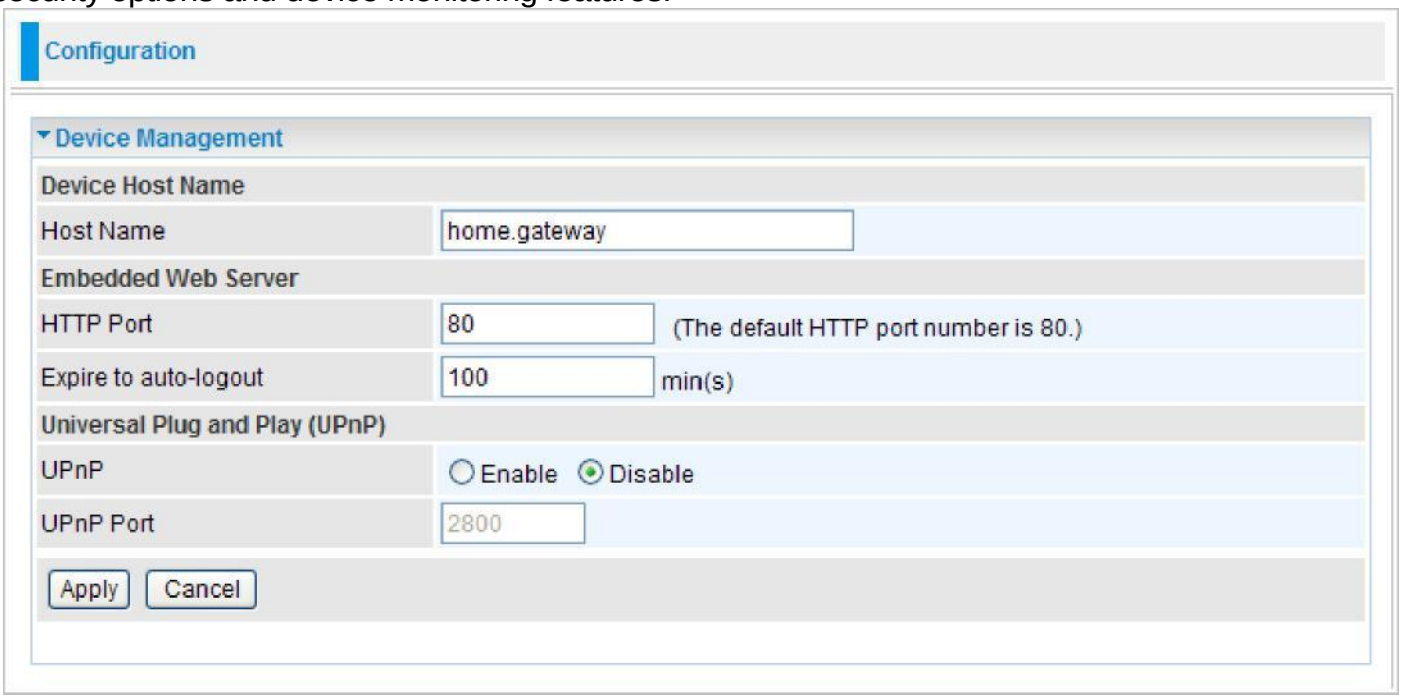


Type: Select the VLAN type from the drop-down menu.

Then enter the parameters in the fields of the table. Click Apply to confirm the settings.

Device Management

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



Device Host Name

Host Name: Assign it a name**.**

(The Host Name cannot be used with one word only. There are two words should be connected with a '.' at least.

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

Embedded Web Server

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

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

Example:

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

Universal Plug and Play (UPnP)

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

of their device will make tasks such as port forwarding become easier.

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

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

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

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

Click Apply to confirm the settings.

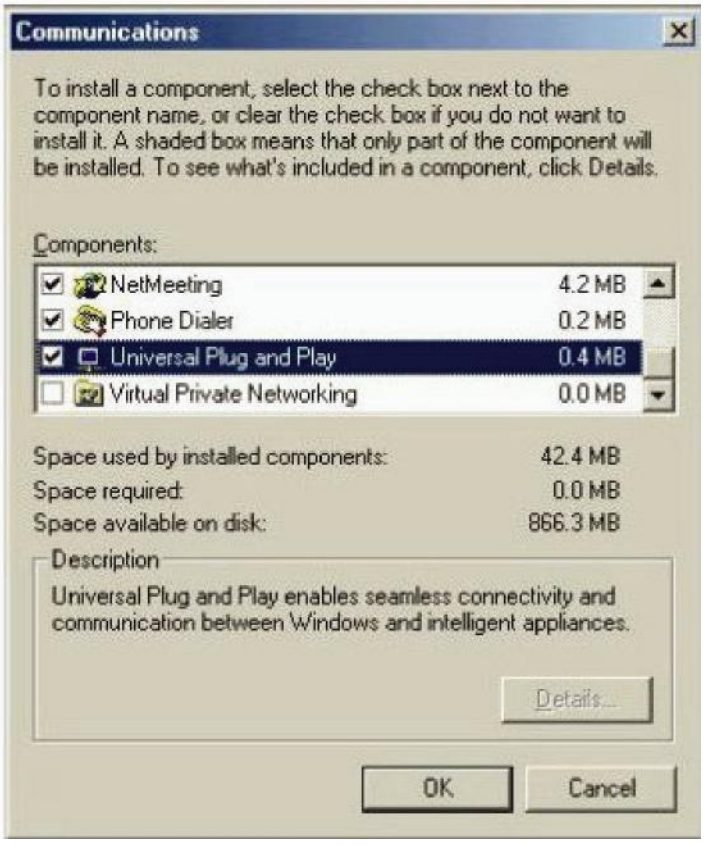
Installing UPnP in Windows Example

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

Step 1: Click Start and Control Panel. Double-click Add/Remove Programs.

Step 2: Click on the Windows Setup tab and select Communication in the Components selection box. Click Details.

Step 3: In the Communications window, select the Universal Plug and Play check box in the Components selection box.



Step 4: Click OK to go back to the Add/Remove Programs Properties window. Click Next.

Step 5: Restart the computer when prompted.

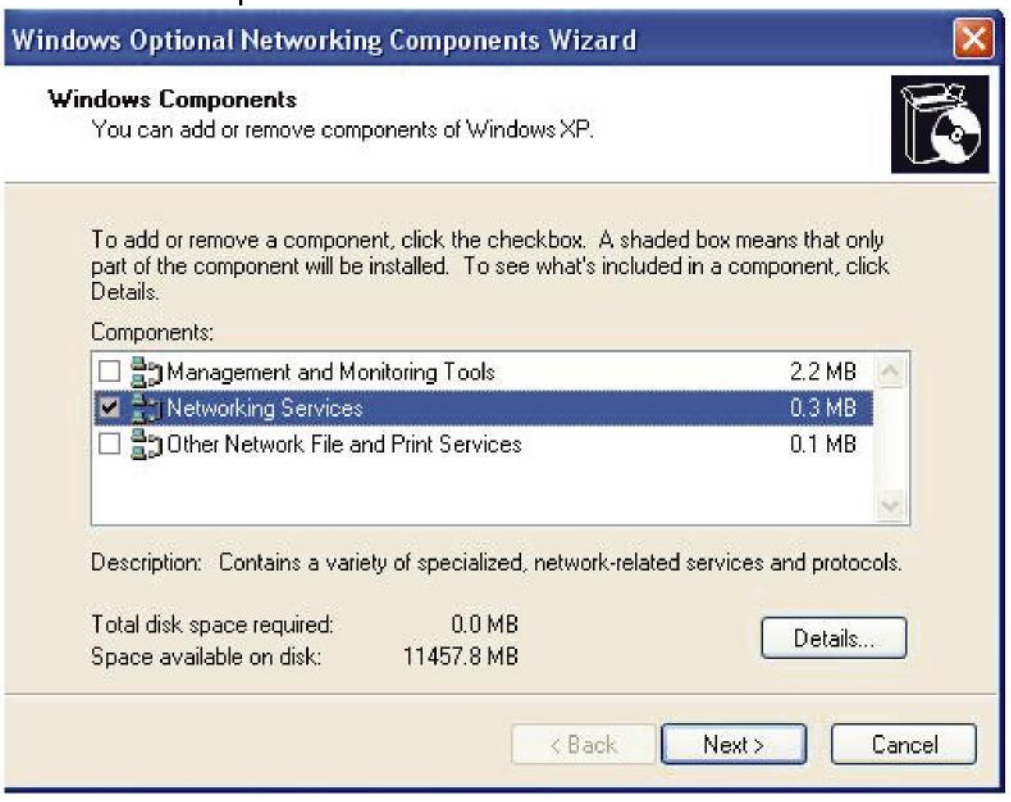
Follow the steps below to install the UPnP in Windows XP.

Step 1: Click Start and Control Panel.

Step 2: Double-click Network Connections.

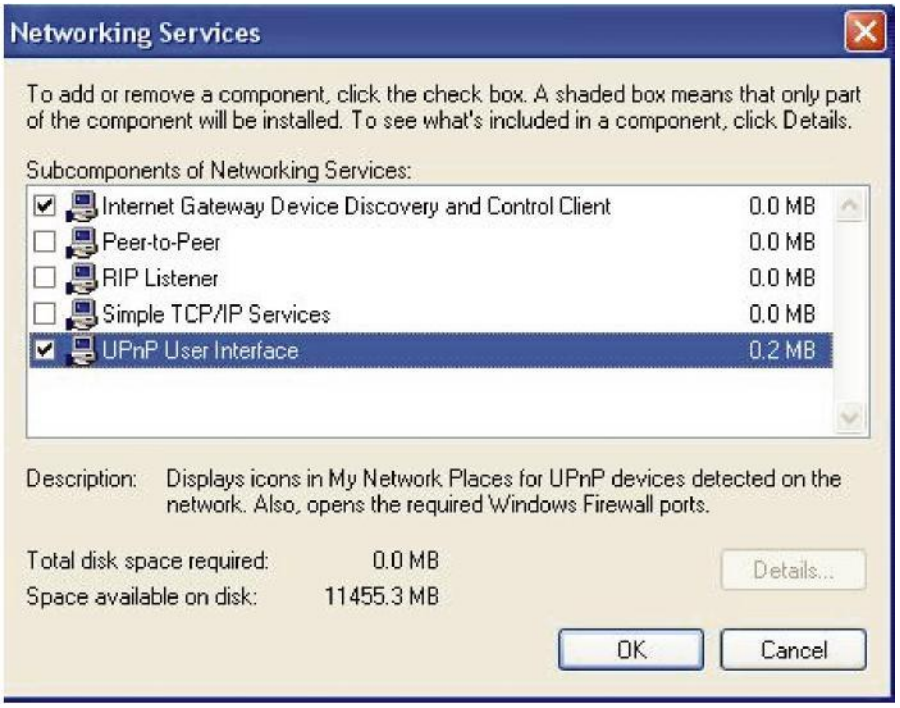
Step 3: In the Network Connections window, click Advanced in the main menu and select Optional Networking Components ....

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



Step 5: In the Networking Services window, select the Universal Plug and Play check box.

Step 6: Click OK to go back to the Windows Optional Networking Component Wizard window and click Next.

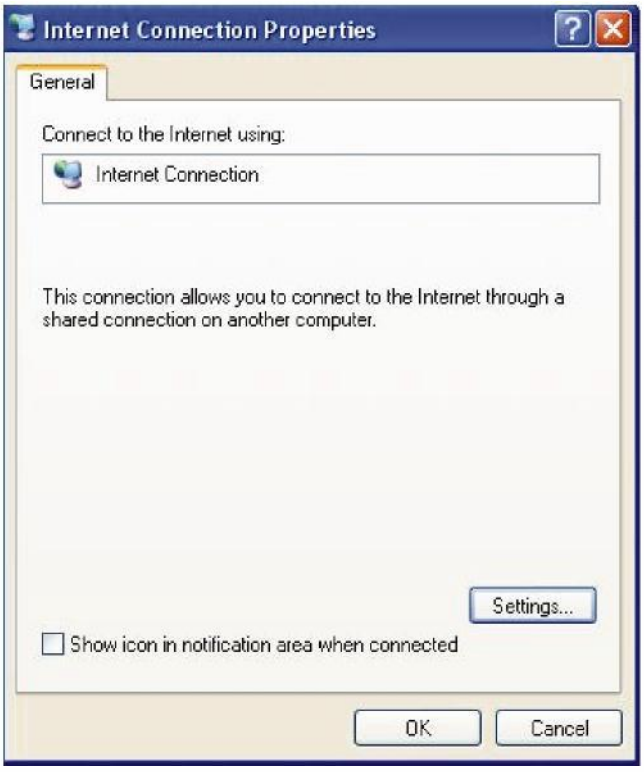


Auto-discover Your UPnP-enabled Network Device

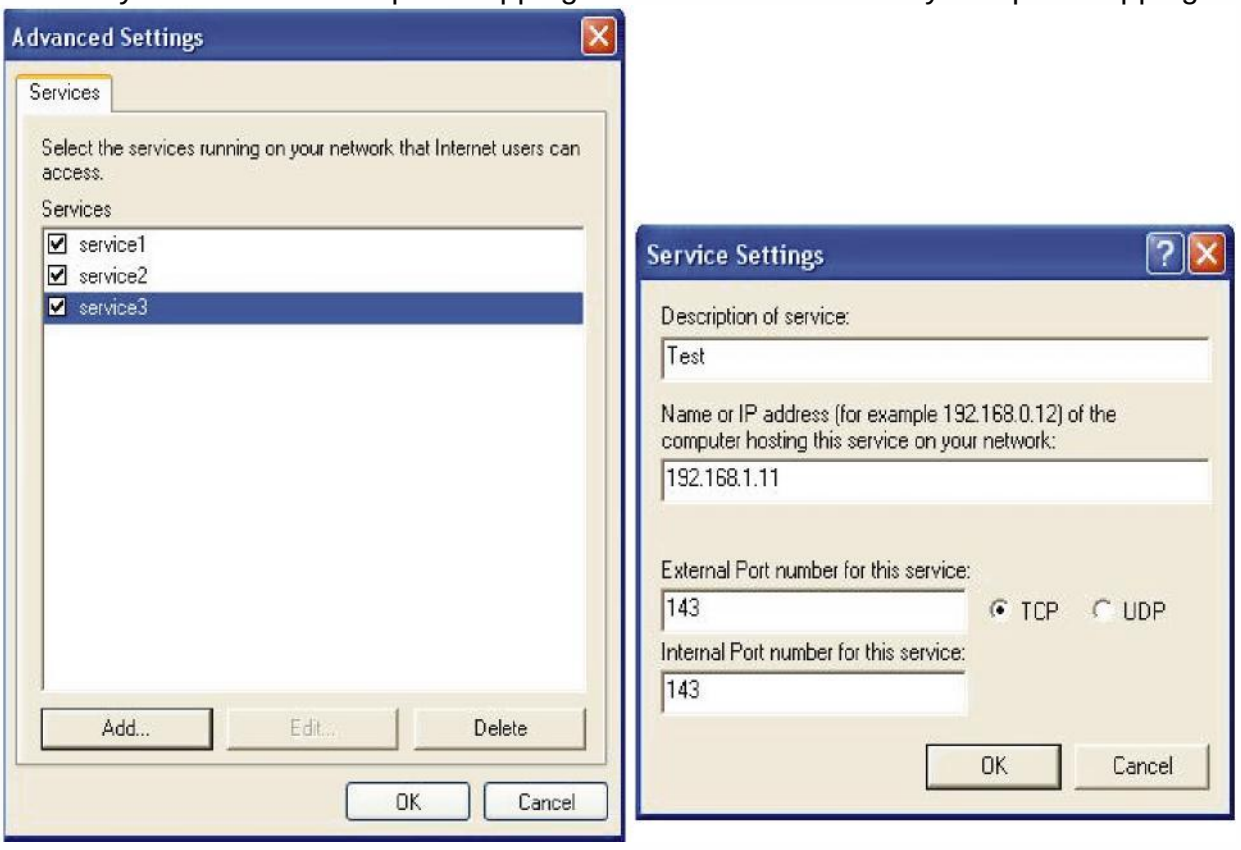
Step 1: Click start and Control Panel. Double-click Network Connections. An icon displays under Internet Gateway.

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

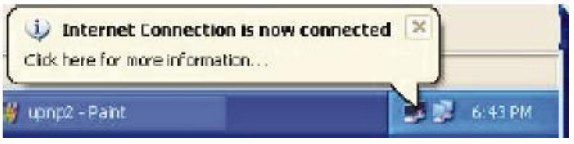
Step 3: In the Internet Connection Properties window, click Settings to see the port mappings that were automatically created.



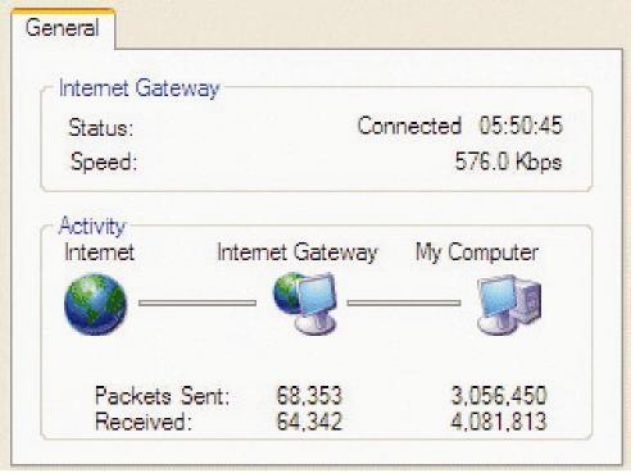
Step 4: You may edit or delete the port mappings or click Add to manually add port mappings.



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



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



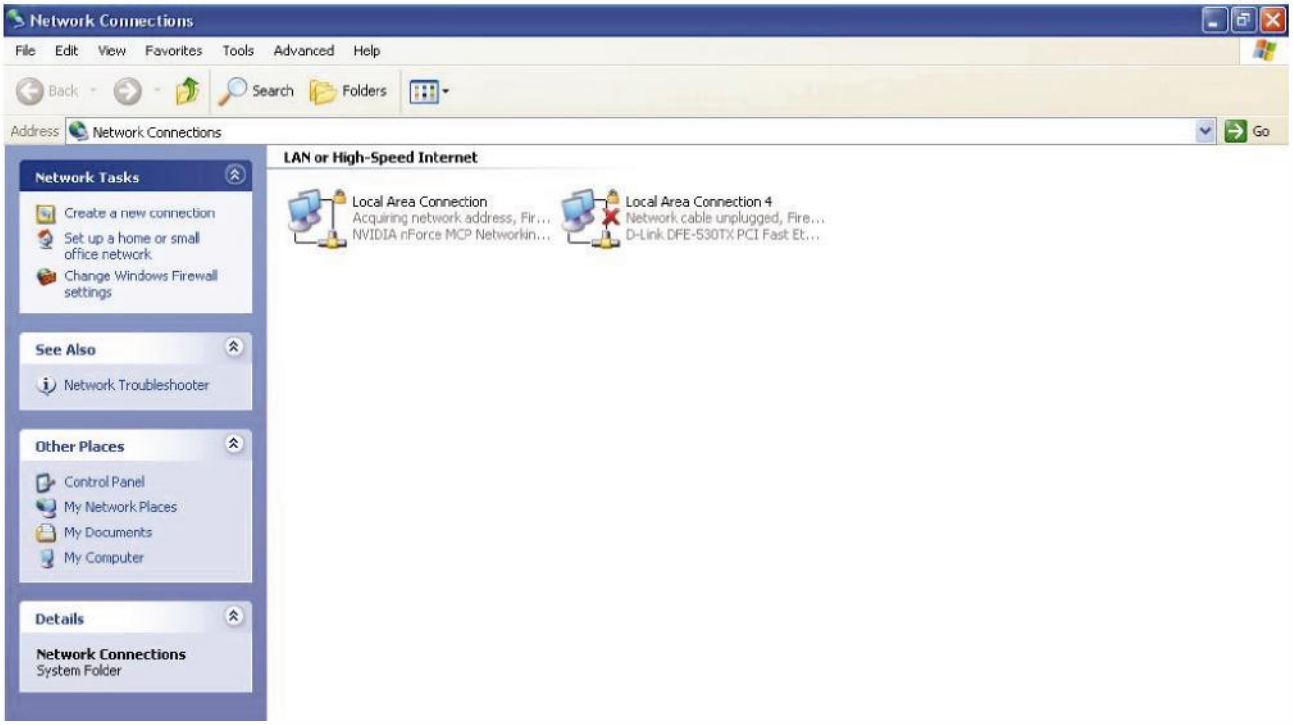
Web Configuration Easy Access

With UPnP, you can access web-based configuration for the 802.11n Fiber Optical 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.

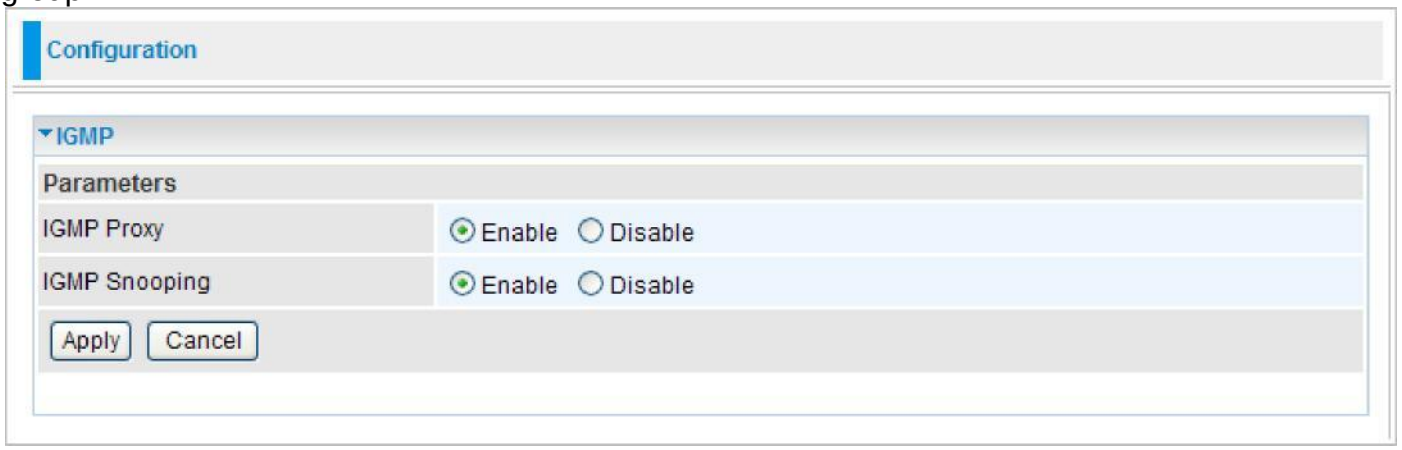
Step 4: An icon describing each UPnP-enabled device shows under Local Network.

Step 5: Right-click on the icon of your 802.11n Fiber Optical Router and select Invoke. The web configuration login screen displays.

Step 6: Right-click on the icon of your 802.11n Fiber Optical Router and select Properties. A properties window displays basic information about the 802.11n Fiber Optical Router.

IGMP

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



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

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

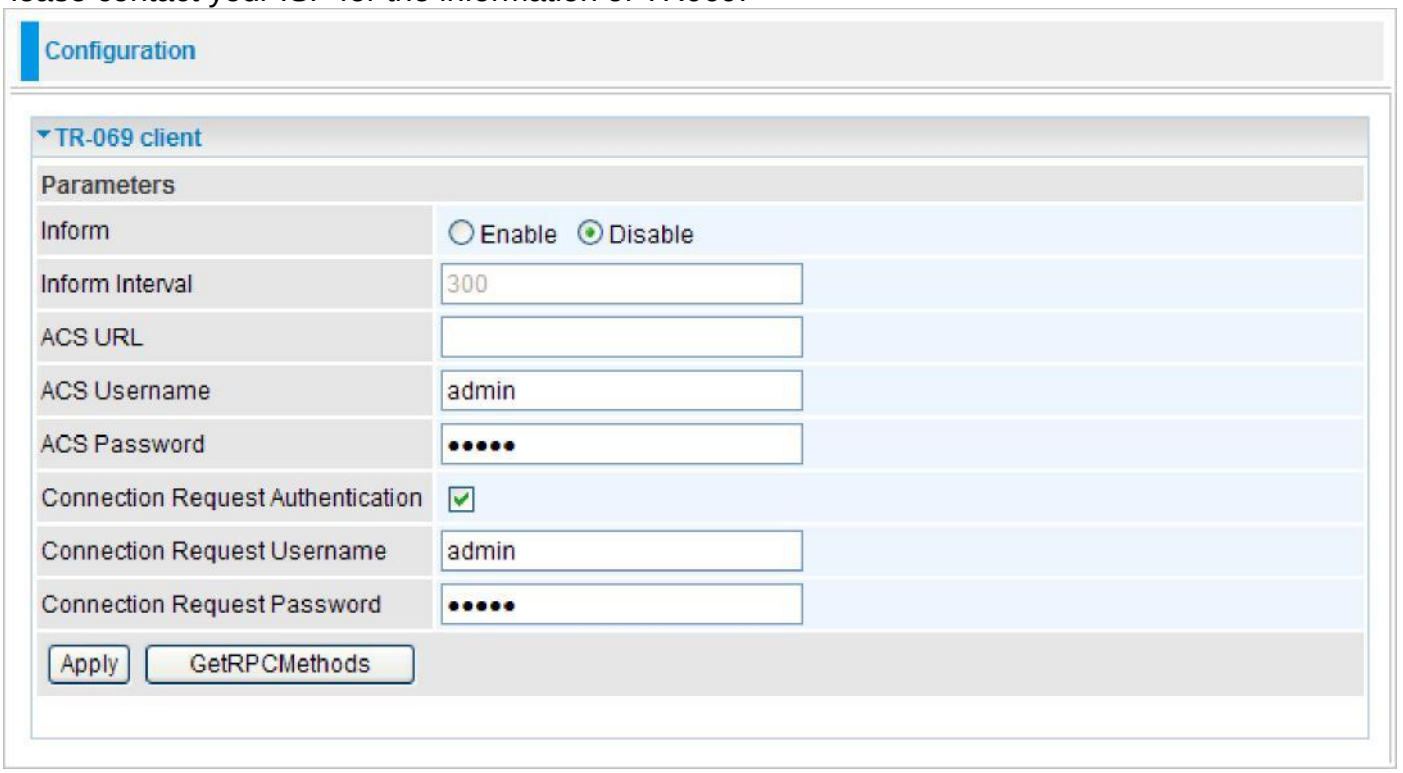
Click Apply to confirm the settings.

Example:

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

TR-069 Client

Please contact your ISP for the information of TR069.



Inform: You may enable or disable the periodic inform feature.

Inform Interval: Enter the length of the periodic inform interval (unit: seconds).

ACS URL: Enter the ACS URL address.

ACS Username: Enter the ACS server login name.

ACS Password: Enter the ACS server login password.

Connection Request Authentication: Check to enable connection request authentication feature.

Connection Request Username: Enter the username for ACS server to make connection request.

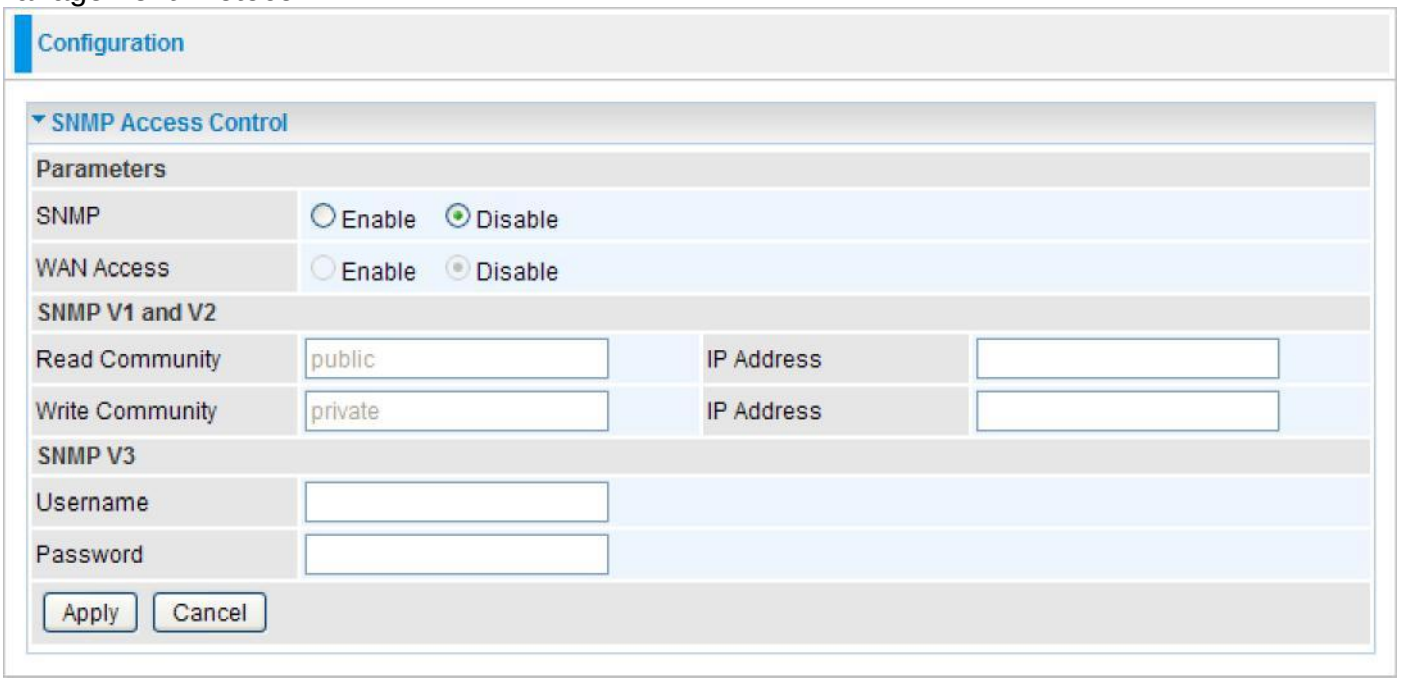
Connection Request Password: Enter the password for ACS server to make connection request.

GetRPCMethods: Detect the types of methods that ACS supports and is in communication with.

Click Apply to confirm the settings.

SNMP Access Control

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



Parameters

SNMP: Select Enable/Disable to activate/inactivate this function.

WAN Access: Select Enable/Disable to activate/inactivate this function.

SNMP V1 and V2

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

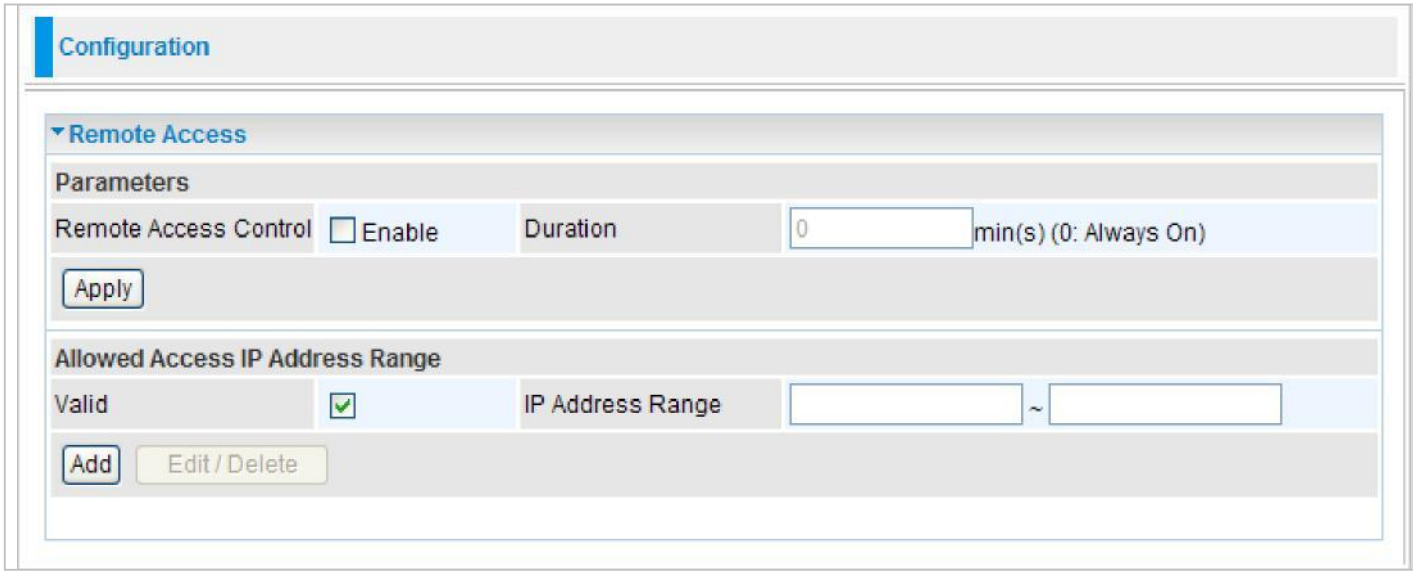
Write Community: Specify a name to be identified as the Write Community, and an IP address. This community string will be checked against the string entered in the configuration file. Once the string name is matched, users from this IP address will be able to view and modify the data.

SNMP V3

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

Click Apply to confirm the settings.

Remote Access



Parameters

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

Click Apply to confirm the settings.

Allowed Access IP Address Range

"Allowed Access IP Address Range" was used to restrict which IP address could login to access system webGUI.

Valid: Tick to enable the IP address Range limitation.

IP Address Range: Enter the IP address Range.

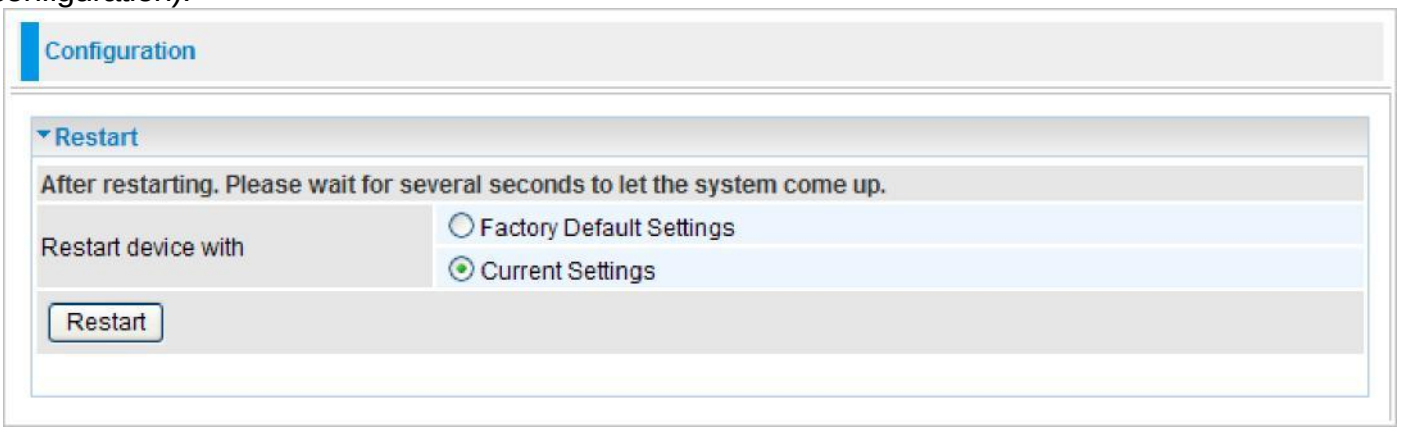
Click Add to add an IP Range to allow remote access.

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 web interface, click “Logout”. Please save your configuration setting before

logging out of the system. A Warning screen will appear as below.

Click OK and a message displays. Click Yes to close the window.

Be aware that the router configuration interface can only be accessed by one PC at a time. Therefore when a PC has logged into the system interface, the other users cannot access the system interface until the current user has logged out of the system. If the previous user forgets to logout, the second PC can only access the router web interface after a user-defined auto logout period which is by default 3 minutes. You can however modify the value of the auto logout period using the Advanced > Device Management section of the router web interface. Please see the **Advanced** section of this manual for more information.

Chapter 5: Troubleshooting

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

Problems with the router

Problem	Suggested Action
None of the LEDs lit when the router is turned on	Examine the connection between the router and the adapter. If the problem persists, most likely it is due to the malfunction of your hardware. Please contact your service provider for technical support.
Fail to make fiber connection	Ensure the fiber cable or the mini-GBIC module has been connected correctly and the fiber cable has not become damaged or bent. Ensure that you apply right fiber cable(s) into right port(s) and right SFP module into right device as well. If these steps do not resolve the problem, please contact your service provider for technical support.
You have forgotten your login username or password	Try the default username & password (Please refer to Chapter 3). If this fails, restore your router to its default setting by pressing the reset button for 1~2 seconds.

Problem with LAN interface

Problem	Suggested Action
Cannot PING any PC on LAN	Examine the Ethernet LEDs on the front panel. The LED should be on for the port that has a PC connected. If it does not light, check to see whether the cable between your router and the PC is properly connected. Make sure you have first uninstalled your firewall program before troubleshooting.

Appendix: Product Support & Contact

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