.

Wireless N Broadband Router

User's Manual

Version: 1.0

(August, 2009)

COPYRIGHT

Federal Communication Commission Interference Statement

FCC Part 15

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

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

FCC Caution

This equipment must be installed and operated in accordance with provided instructions and a minimum 20 cm spacing must be provided between computer mounted antenna and person's body (excluding extremities of hands, wrist and feet) during wireless modes of operation.

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) this device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

Any changes or modifications not expressly approved by the party responsible for compliance could void the authority to operate equipment.

Federal Communication Commission (FCC) Radiation Exposure Statement

This equipment complies with FCC radiation exposure set forth for an uncontrolled environment. In order to avoid the possibility of exceeding the FCC radio frequency exposure limits, human proximity to the antenna shall not be less than 20cm (8 inches) during normal operation.

The antenna(s) used for this transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

The equipment version marketed in US is restricted to usage of the channels 1-11 only.

R&TTE Compliance Statement

This equipment complies with all the requirements of DIRECTIVE 1999/5/EC OF THE EUROPEAN PARLIAMENT AND THE COUNCIL of March 9, 1999 on radio equipment and telecommunication terminal Equipment and the mutual recognition of their conformity (R&TTE).

The R&TTE Directive repeals and replaces in the directive 98/13/EEC (Telecommunications Terminal Equipment and Satellite Earth Station Equipment) As of April 8, 2000.

Safety

This equipment is designed with the utmost care for the safety of those who install and use it. However, special attention must be paid to the dangers of electric shock and static electricity when working with electrical equipment. All guidelines of this and of the computer manufacture must therefore be allowed at all times to ensure the safe use of the equipment.

EU Countries Intended for Use

The ETSI version of this device is intended for home and office use in Austria, Belgium, Denmark, Finland, France, Germany, Greece, Ireland, Italy, Luxembourg, the Netherlands, Portugal, Spain, Sweden, and the United Kingdom.

The ETSI version of this device is also authorized for use in EFTA member states: Iceland, Liechtenstein, Norway, and Switzerland.

EU Countries Not intended for use

None.

C A T A L O G

Chapter 1 Introduction

Thank you for purchasing this wireless broadband router! This high cost-efficiency router is the best choice for Small office / Home office users, all computers and network devices can share a single xDSL / cable modem internet connection at high speed. Easy install procedures allows any computer users to setup a network environment in very short time - within minutes, even inexperienced. When the number of your computers and network-enabled devices grow, you can also expand the number of network slot by simple attach a hub or switch, to extend the scope of your network!

With built-in IEEE 802.11b/g/Draft-N wireless network capability, all computers and wireless-enabled network devices (including PDA, cellular phone, game console, and more!) can connect to this wireless router without additional cabling. New Draft-N wireless capability also gives you the highest speed of wireless experience ever! With a compatible wireless card installed in your PC, you can transfer file for up to 300Mbps (transfer data rate)! The radio coverage is also doubled, so don't worry if your office or house is really big!

1.1 Features

- High Internet Access throughput
- Allow multiple users to share a single Internet line
- Supports up to 253 users
- Share a single Cable or xDSL internet connection
- Access private LAN servers from the internet
- Four wired LAN ports (10/100M) and one WAN port (10/100M)
- Provides IEEE 802.11b/g/Draft-N wireless LAN capability
- Support DHCP (Server/Client) for easy IP-address setup
- Support multiple wireless modes like: AP, Client, WDS and AP with WDS.
- Advanced network and security features like: QoS, DMZ, Virtual Servers, Access Control, Firewall.
- Easy to use Web-based GUI for network configuration and management purposes
- Auto MDI / MDI-X function for all wired Ethernet ports.

1.2 Safety Information

In order to keep the safety of users and your properties, please follow the following safety instructions:

1. This router is designed for indoor use only; DO NOT place this router outdoor.

2. DO NOT put this router at or near hot or humid places, like kitchen or bathroom. Also, do not left this router in the car in summer.

3. DO NOT pull any connected cable with force; disconnect it from the router first.

4. If you want to place this router at high places or hang on the wall, please make sure the router is firmly secured. Falling from high places would damage the router and its accessories, and warranty will be void.

5. Accessories of this router, like antenna and power supply, are danger to small children under 3 years old. They may put the small parts in their nose or month and it could cause serious damage to them. KEEP THIS ROUTER OUT THE REACH OF CHILDREN!

6. The router will become hot when being used for long time (This is normal and is not a malfunction). DO NOT put this router on paper, cloth, or other flammable materials.

7. There's no user-serviceable part inside the router. If you found that the router is not working properly, please contact your dealer of purchase and ask for help. DO NOT disassemble the router, warranty will be void.

8. If the router falls into water when it's powered, DO NOT use your hand to pick it up. Switch the electrical power off before you do anything, or contact an experienced technician for help.

9. If you smell something strange, or even see some smoke coming out from the router or power supply, remove the power supply or switch the electrical power off immediately, and call dealer of purchase for help.

1.3 Minimum Requirements

- Computer or network devices with wired or wireless network interface card.
- Web browser (Microsoft Internet Explorer 4.0 or above, Netscape Navigator 4.7 or above, Opera web browser, or Safari web browser).
- An available AC power socket (100 – 240V, 50/60Hz)

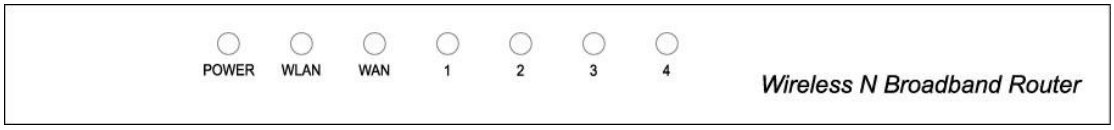
1.4 Package Content

Before you starting to use this router, please check if there's anything missing in the package, and contact your dealer of purchase to claim for missing items:

- Broadband router (main body, 1 pcs)…… 1
- Quick installation guide (1 pcs) …… 2
- User manual CDROM (1 pcs) …….. 3
- A/C power adapter (1 pcs) ……..... 4

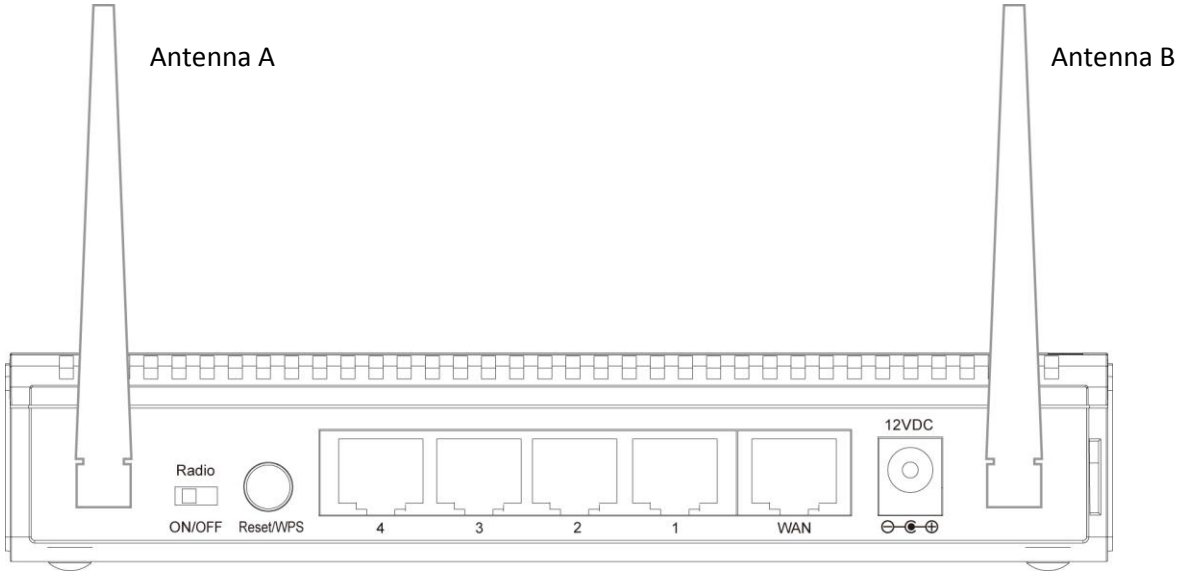
1.5 Familiar with your new wireless broadband router

Front Panel



LED Name	Light Status	Description
PWR	On	Router is switched on and correctly powered.
WLAN	On	Wireless WPS function is enabled.
	Off	Wireless network is switched off.
	Flashing	Wireless LAN activity (transferring or receiving data).
WAN LNK/ACT	On	WAN port is connected.
	Off	WAN port is not connected.
	Flashing	WAN activity (transferring or receiving data).
LAN 1-4 LNK/ACT	On	LAN port is connected.
	Off	LAN port is not connected.
	Flashing	LAN activity (transferring or receiving data).

Back Panel



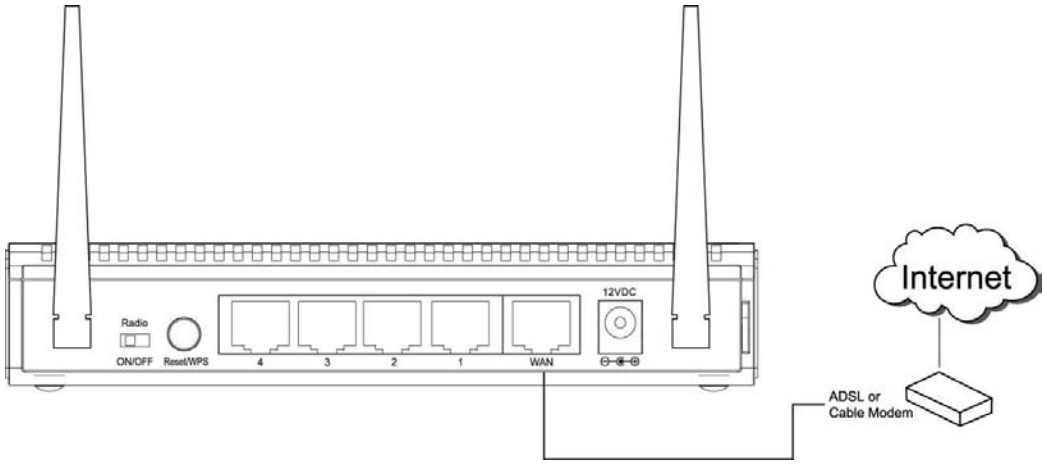
Item Name	Description
Antenna A/B	These antennas are 3dBi dipole antennas.
Radio ON/OFF	Switch the button to activate or deactivate the wireless functions.
Reset / WPS	Reset the router to factory default settings (clear all settings) or start WPS function. Press this button and hold for 10 seconds to restore all settings to factory defaults, and press this button for less than 5 seconds to start WPS function.
1 - 4	Local Area Network (LAN) ports 1 to 4.
WAN	Wide Area Network (WAN / Internet) port.
Power	Power connector, connects to A/C power adapter.

Chapter 2 System and Network Setup

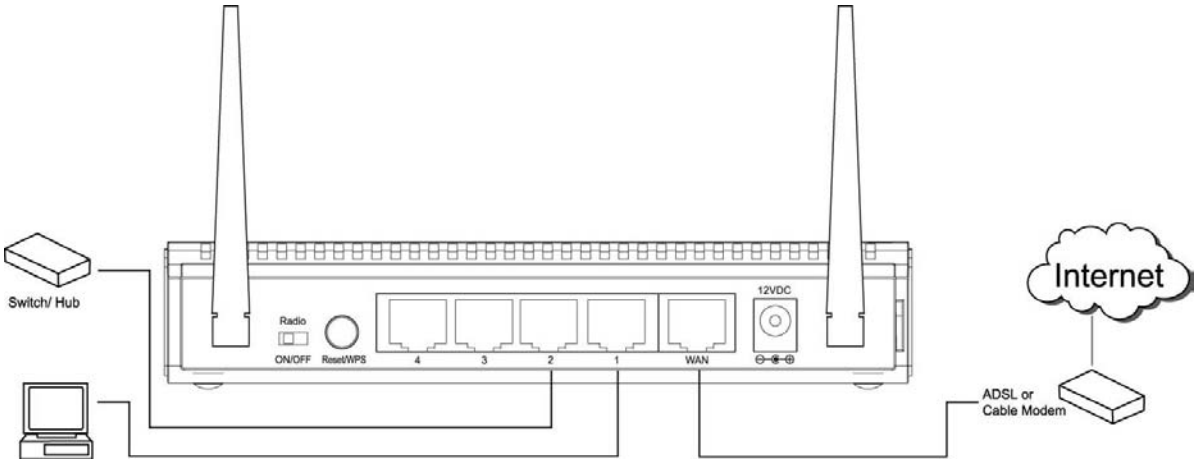
2.1 Build Network Connection

Please follow the following instruction to build the network connection between your new WIRELESS router and your computers, network devices:

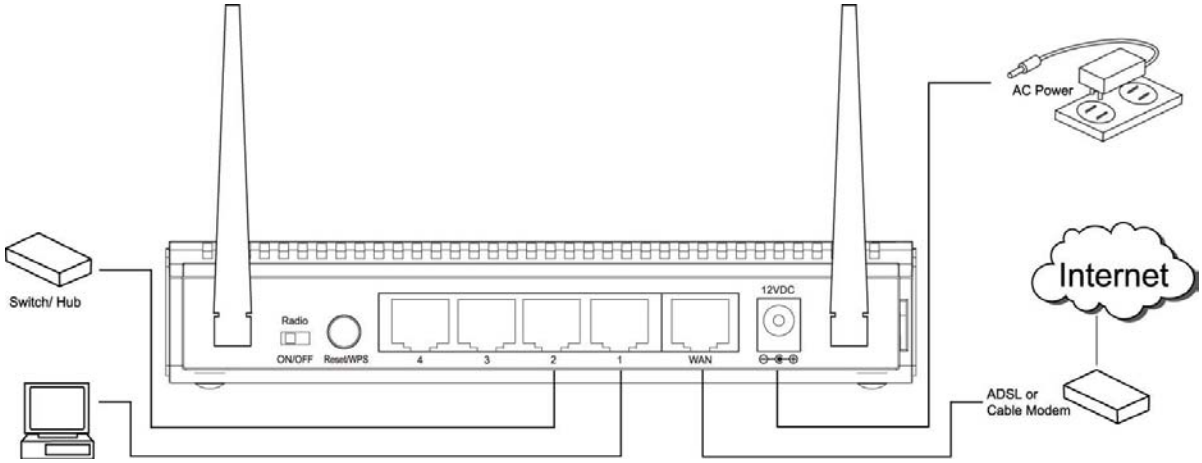
1. Connect your xDSL / cable modem to the WAN port of router by Ethernet cable.



2. Connect all your computers, network devices (network-enabled consumer devices other than computers, like game console, or switch / hub) to the LAN port of the router.



3. Connect the A/C power adapter to the wall socket, and then connect it to the ‘Power’ socket of the router.



Please check all LEDs on the front panel. ‘PWR’ LED should be steadily on, WAN and LAN LEDs should be on if the computer / network device connected to the respective port of the router is powered on and correctly connected.

2.2 Connecting to wireless broadband router by web browser

This is a step-by-step instruction on how to start using the router and get connected to the Internet.

1) Setup your network as shown in the setup diagram above (fig 1.1).

2) You then need to set your LAN PC clients so that it can obtain an IP address automatically. All LAN clients require an IP address. Just like an address, it allows LAN clients to find one another. (If you have already configured your PC to obtain an IP automatically then proceed to step 3, page 11)
Configure your PC to obtain an IP address automatically

By default the broadband router's DHCP is on, this means that you can obtain an IP address automatically once you've configured your PC to obtain an IP address automatically. This section will show you how to configure your PC's so that it can obtain an IP address automatically for either Windows 95/98/Me, 2000 or NT operating systems. For other operating systems (Macintosh, Sun, etc.), follow the manufacturer's instructions. The following is a step-by-step illustration on how to configure your PC to obtain an IP address automatically for 2a) **Windows 95/98/Me**, 2b) **Windows XP**, 2c) **Windows 2000,** 2d) **Windows NT**, and 2e) **Windows Vista**.

2a) Windows 95/98/Me

1: Click the *Start* button and select *Settings*, then click *Control Panel*. The *Control Panel* window will appear.

2: Double-click *Network* icon. The *Network* window will appear.

3: Check your list of Network Components. If TCP/IP is not installed, click the *Add* button to install it now. If TCP/IP is installed, go to **step 6**.

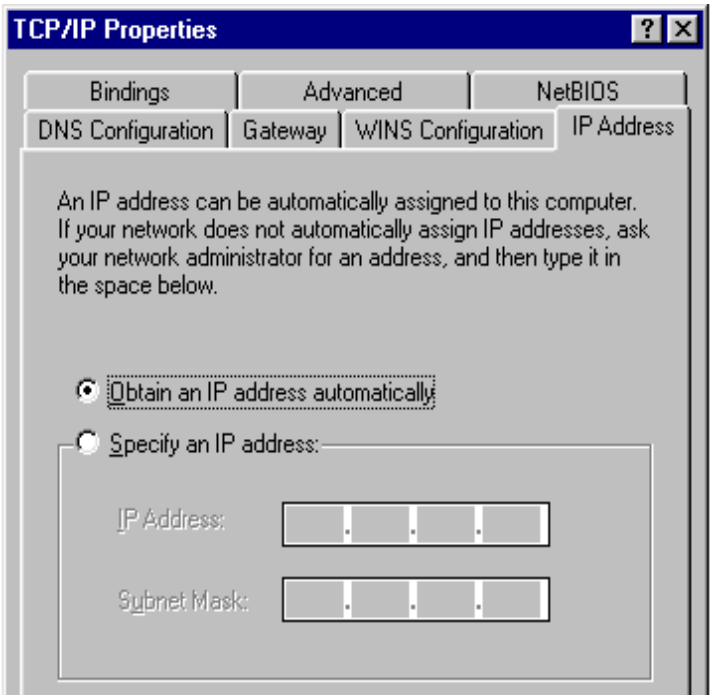
4: In the *Network Component Type* dialog box, select *Protocol* and click *Add* button.

5: In the *Select Network Protocol* dialog box, select *Microsoft* and *TCP/IP* and then click the *OK* button to start installing the TCP/IP protocol. You may need your Windows CD to complete the installation.

6: After installing TCP/IP, go back to the *Network* dialog box. Select *TCP/IP* from the list of *Network Components* and then click the *Properties* button.

7: Check each of the tabs and verify the following settings:

- **Bindings**: Check *Client for Microsoft Networks* and *File and printer sharing for Microsoft Networks*.
- **Gateway**: All fields are blank.
- **DNS Configuration**: Select *Disable DNS.*
- **WINS Configuration**: Select *Disable WINS Resolution.*
- **IP Address**: Select *Obtain IP address automatically*.



8: Reboot the PC. Your PC will now obtain an IP address automatically from your Broadband Router's DHCP server.

Note: Please make sure that the Broadband router's DHCP server is the only DHCP server available on your LAN.

Once you've configured your PC to obtain an IP address automatically, please proceed to Step 3

2b) Windows 2000

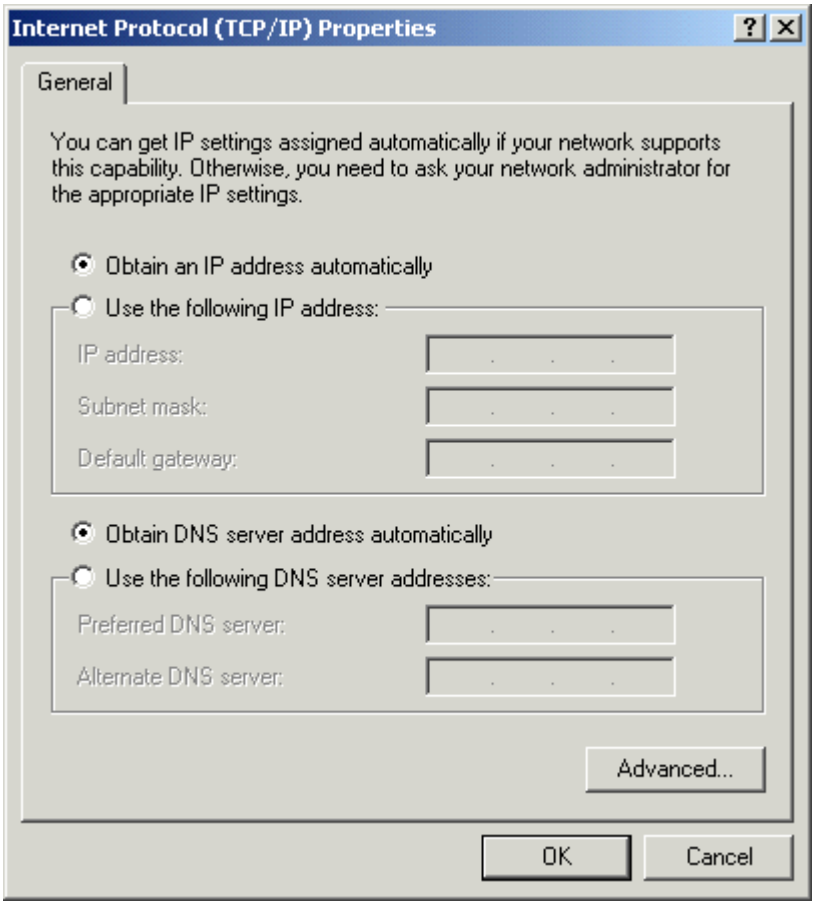
1: Click the *Start* button and select *Settings*, then click *Control Panel*. The *Control Panel* window will appear.

2: Double-click *Network and Dial-up Connections* icon. In the *Network and Dial-up Connection* window, double-click *Local Area Connection* icon. The *Local Area Connection* window will appear.

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

4: Check your list of Network Components. You should see *Internet Protocol [TCP/IP]* on your list. Select it and click the *Properties* button.

5: In the Internet Protocol (TCP/IP) Properties window, select *Obtain an IP address automatically* and *Obtain DNS server address automatically* as shown on the following screen.



6: Click *OK* to confirm the setting. Your PC will now obtain an IP address automatically from your Broadband Router's DHCP server.

Note: Please make sure that the Broadband router's DHCP server is the only DHCP server available on your LAN.

Once you've configured your PC to obtain an IP address automatically, please proceed to Step 3.

2c) Windows NT

1: Click the *Start* button and select *Settings*, then click *Control Panel*. The *Control Panel* window will appear.

2: Double-click *Network* icon. The *Network* window will appear. Select the *Protocol* tab from the *Network* window.

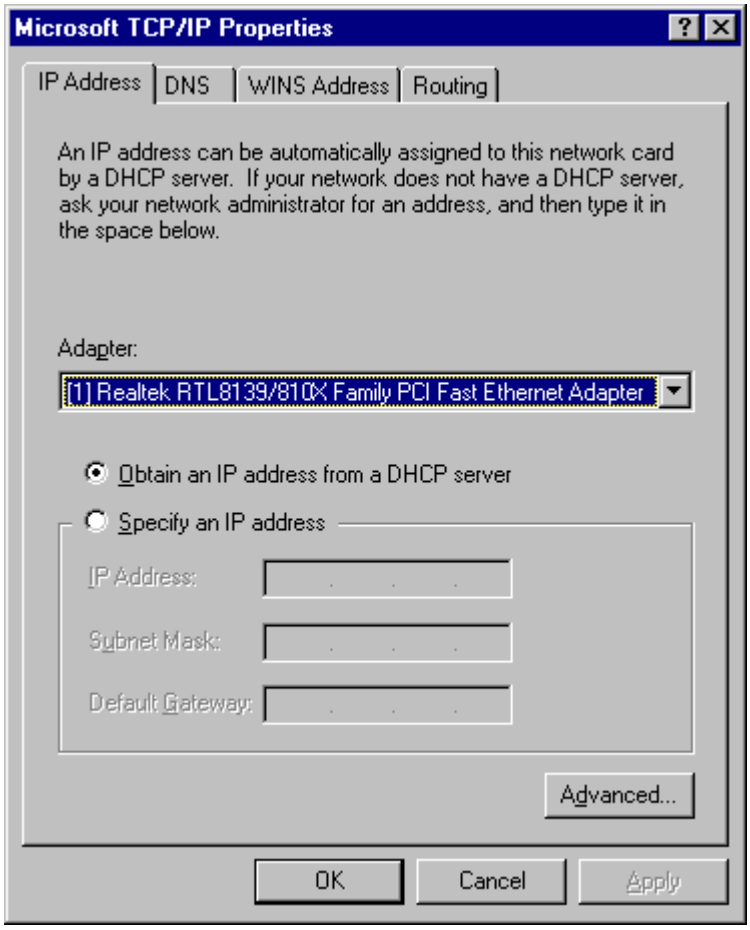
3: Check if the *TCP/IP Protocol* is on your list of *Network Protocols*. If TCP/IP is not installed, click the *Add* button to install it now. If TCP/IP is installed, go to **step 5**.

4: In the *Select Network Protocol* window, select the *TCP/IP Protocol* and click the *Ok* button to start installing the TCP/IP protocol. You may need your Windows CD to complete the installation.

5: After you install TCP/IP, go back to the *Network* window. Select *TCP/IP* from the list of *Network Protocols* and then click the *Properties* button.

6: Check each of the tabs and verify the following settings:

- **IP Address:** Select *Obtain an IP address from a DHCP server*.
- **DNS:** Let all fields are blank.
- **WINS:** Let all fields are blank.
- **Routing:** Let all fields are blank.



7: Click *OK* to confirm the setting. Your PC will now obtain an IP address automatically from your Broadband Router's DHCP server.

Note: Please make sure that the Broadband router's DHCP server is the only DHCP server available on your LAN.

Once you've configured your PC to obtain an IP address automatically, please proceed to Step 3.

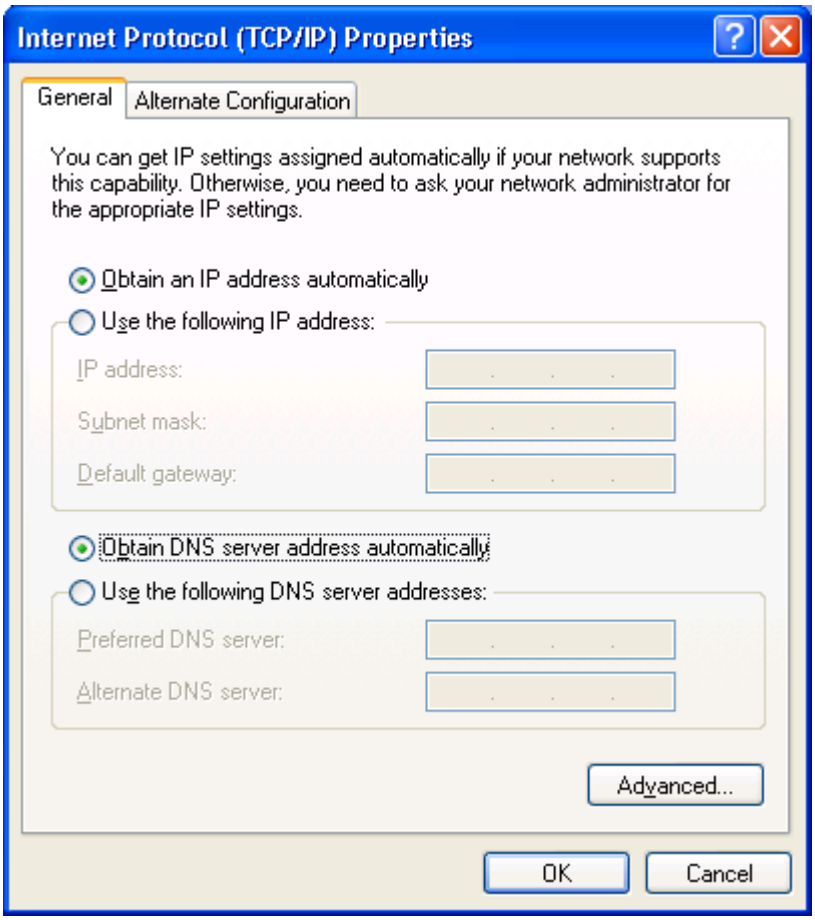
2d) Windows XP

1: Click the *Start* button and select *Settings*, then click *Network Connections.* The *Network Connections* window will appear.

2: Double-click *Local Area Connection* icon. The *Local Area Connection* window will appear.

3: Check your list of Network Components. You should see *Internet Protocol [TCP/IP]* on your list. Select it and click the *Properties* button.

4: In the Internet Protocol (TCP/IP) Properties window, select *Obtain an IP address automatically* and *Obtain DNS server address automatically* as shown on the following screen.



5: Click *OK* to confirm the setting. Your PC will now obtain an IP address automatically from your Broadband Router's DHCP server.

Note: Please make sure that the Broadband router's DHCP server is the only DHCP server available on your LAN.

Once you've configured your PC to obtain an IP address automatically, please proceed to Step 3.

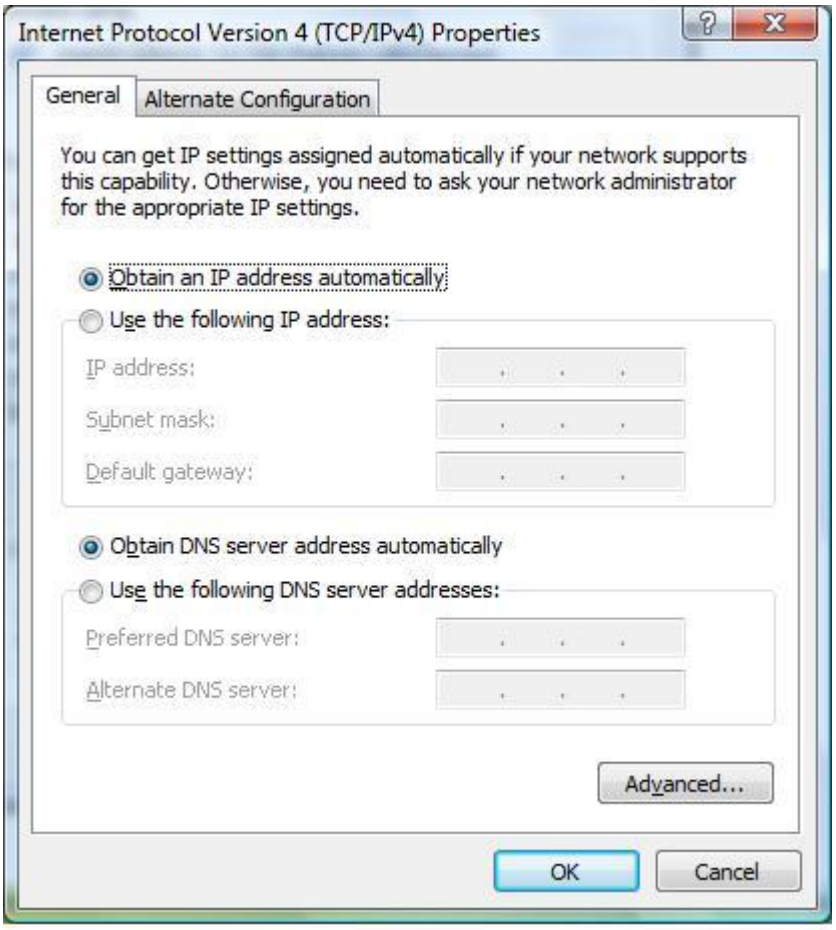
2e) Windows Vista

1: Click the Start button and select Settings and then select Control Panel. Double click Network and Sharing Center, the Network and Sharing Center window will appear.

2: Click Manage network connections and right click on the Local Area Connection icon and select Properties. The Local Area Connection window will appear.

3: Check your list of Network Components. You should see Internet Protocol Version 4 (TCP/IPv4) on your list. Select it and click the Properties button.

4: In the Internet Protocol Version 4 (TCP/IPv4) Properties window, select Obtain an IP address automatically and Obtain DNS server address automatically as shown on the following screen.



5: Click OK to confirm the setting. Your PC will now obtain an IP address automatically from your router's DHCP server.

Note: Please make sure that the Broadband router's DHCP server is the only DHCP server available on your LAN.

Once you've configured your PC to obtain an IP address automatically, please proceed to Step 3.

3) Once you have configured your PCs to obtain an IP address automatically, the router's DHCP server will automatically give your LAN clients an IP address. By default the Broadband Router's DHCP server is enabled so that you can obtain an IP address automatically. To see if you have obtained an IP address, see Appendix A.

   Note: Please make sure that the Broadband router's DHCP server is the only DHCP server available on your LAN. If there is another DHCP on your network, then you'll need to switch one of the DHCP servers off. (To disable the Broadband router's DHCP server see chapter 3 LAN Port)

4) Once your PC has obtained an IP address from your router, enter the default IP address **192.168.2.1** (broadband router's IP address) into your PC's web browser and press <enter>

5) The login screen below will appear. Enter the "User Name" and "Password" and then click <OK> to login.

   Note: By default the user name is "admin" and the password is "1234". For security reasons it is recommended that you change the password as soon as possible (in General setup/system/password, see chapter 3)

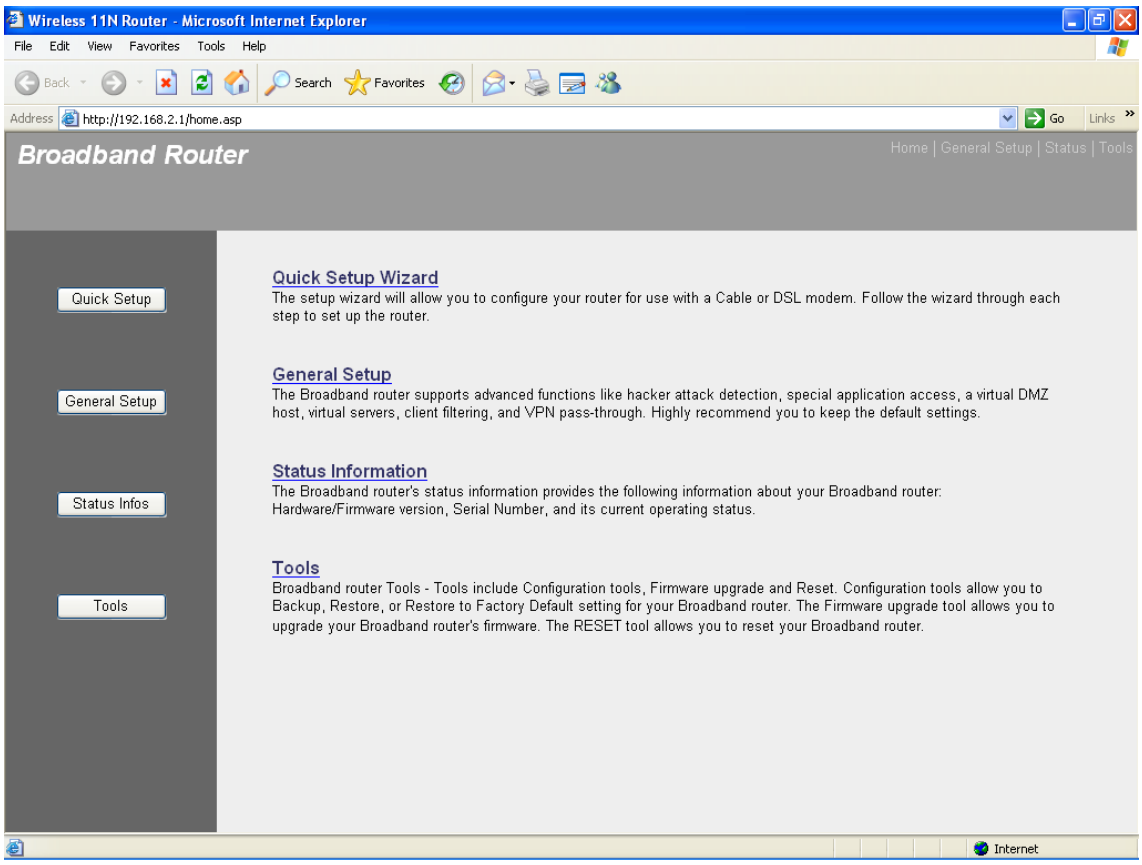
6) The **HOME** page screen below will appear. The **Home** Page is divided into four sections, **Quick Setup Wizard**, **General Setup**, **Status Information** and **Tools.**

Quick Setup Wizard *(Chapter 2)*
If you only want to start using the broadband router as an Internet Access device then you ONLY need to configure the screens in the Quick Setup Wizard section.

General Setup *(Chapter 3)*
If you want to use more advanced features that the broadband router has to offer, then you'll need to configure the Quick Setup Wizard and the General Setup section. Alternatively, you can just configure the General Setup section, since the General Setup/WAN and the Quick Setup Wizard contain the same configurations.

Status Information *(Chapter 4)*
The Status Information section is for you to monitor the router's current status information only.

Tools *(Chapter 5)*
If you want to Reset the router (because of problems) or save your configurations or upgrade the firmware then the Tools section is the place to do this.



Menu	Description
Quick Setup Wizard *(Chapter 2)*	Setup your Internet connection type and then input the configurations needed to connect to your Internet Service Provider (ISP). Here you can also configure the wireless settings of the router.
General Setup *(Chapter 3)*	This section contains configurations for the Broadband router's advance functions such as: Address Mapping, Access Control, Hacker Attack Prevention, DMZ, Special applications and other functions to meet your LAN requirements.
Status Information *(Chapter 4)*	In this section you can see the Broadband router's system information, Internet Connection,

	Device Status, System Log, Security Log and DHCP client information.
Tools *(Chapter 5)*	This section contains the broadband router's Tools - Tools include Configuration tools, Firmware upgrade and Reset. Configuration tools allow you to Backup (save), Restore, or Restore to Factory Default configuration for your Broadband router. The Firmware upgrade tool allows you to upgrade your Broadband router's firmware. The RESET tool allows you to reset your Broadband router.

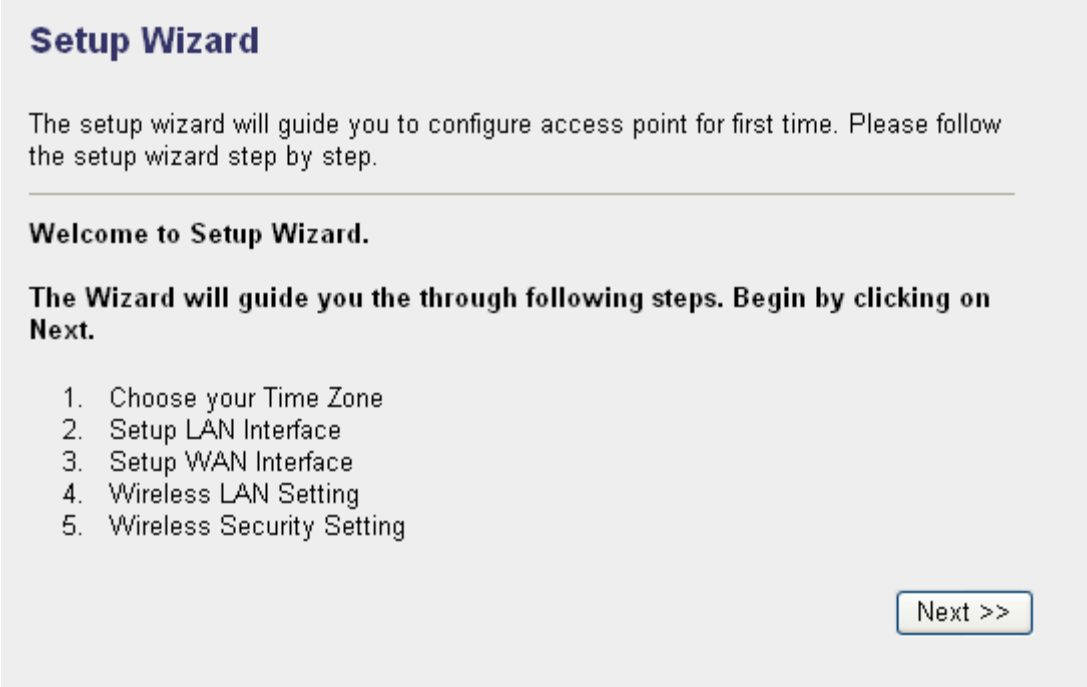
---

7) Click on **Quick Setup Wizard** (see chapter 2) to start configuring settings required by your ISP so that you can start accessing the Internet. The other sections (General Setup, Status Information and Tools) do not need to be configured unless you wish to implement/monitor more advance features/information.

Select the section (Quick Setup Wizard, General Setup, Status Information and Tools) you wish to configure and proceed to the corresponding chapter. Use the selections on the web management's top right hand page (see below) to navigate around the web-based management User Interface.

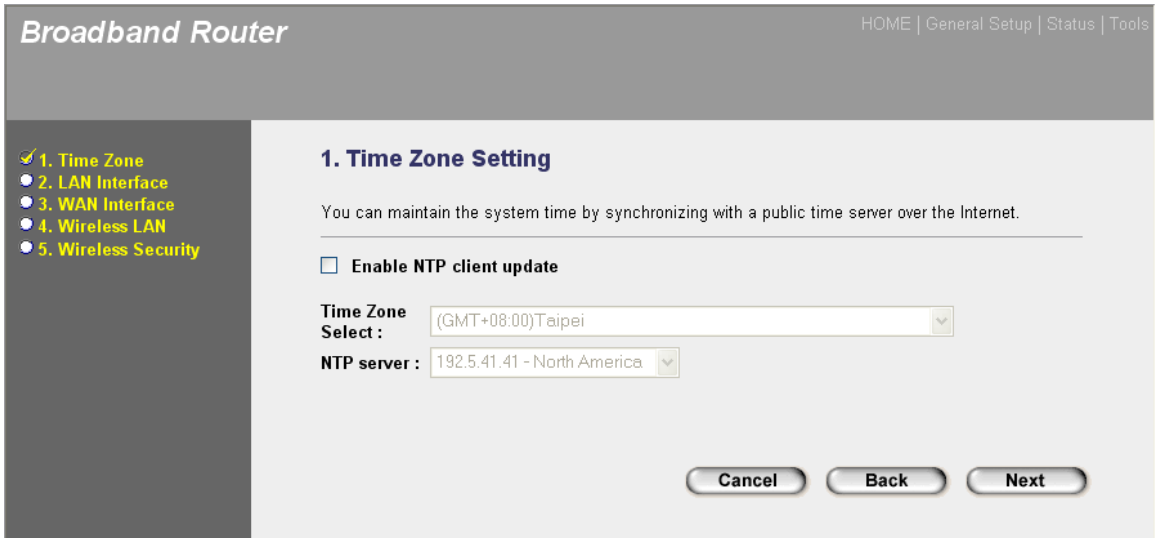
Chapter 2 Quick Setup

The Quick Setup section is designed to get you using the broadband router as quickly as possible. In the Quick Setup you are required to fill in only the information necessary to access the Internet. Once you click on the **Quick Setup Wizard** in the HOME page, you should see the following screen. Follow the setup procedures described below.



2.1 Time Zone

The Time Zone allows your router to base its time on the settings configured here, this will affect functions such as Log entries and Firewall settings.



Parameter	Description
Enable NTP client update	Check this box to enable the auto time synchronization function. The router will set its time based on your selection.
Automatically Adjust Daylight Saving	If the country you live uses daylight saving, please check this box.
Time Zone Select	You can select your local time zone here. The router will sync time according to your time zone selection.
NTP server	Select the time server to synchronize with.

Click on **NEXT** to proceed to the next page (step 2) LAN Interface.

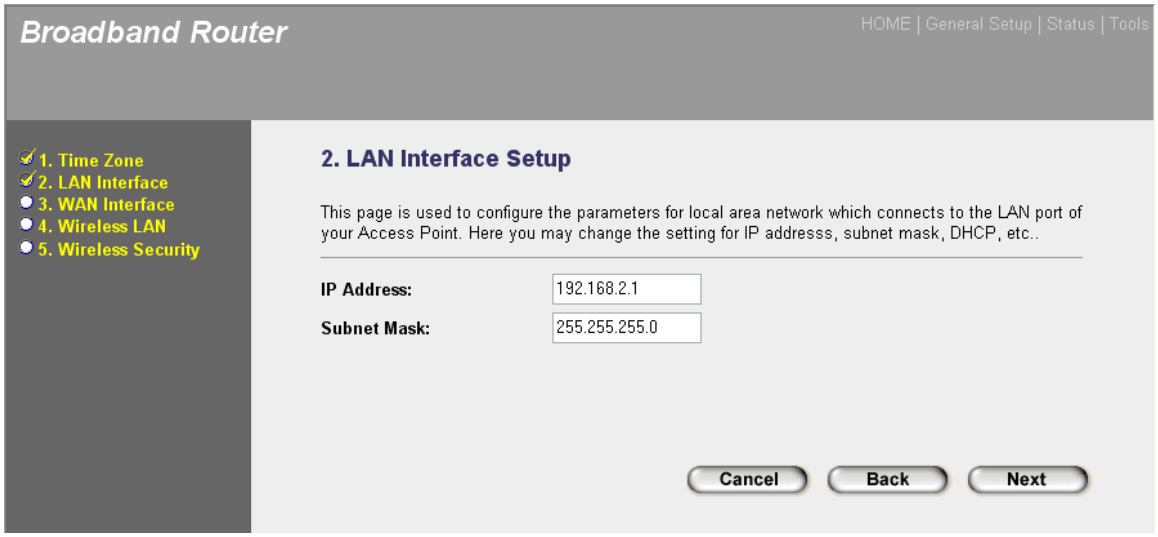
NOTE: There are several time servers available on internet:

129.6.15.28 (time-a.nist.gov)

132.163.4.101 (time-a.timefreq.bldrdoc.gov)

131.107.1.10 (time-nw.nist.gov)

If you found that the time of router is incorrect, try another time server.



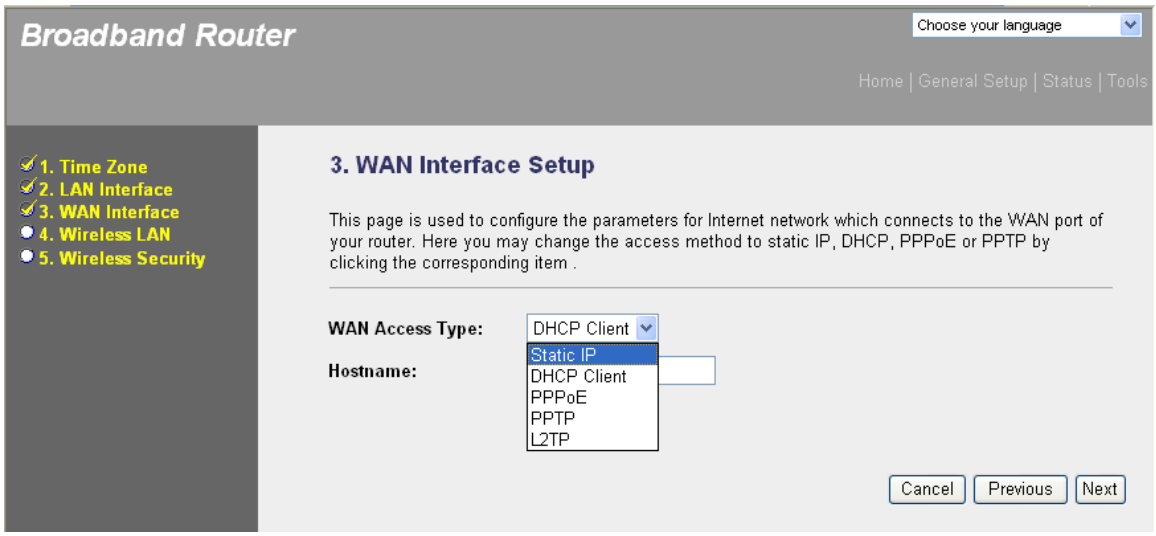
Parameter	Description
IP Address	This is the router's LAN port IP address (Your LAN clients default gateway IP address). The default IP Address is '192.168.2.1'.
Subnet Mask	Specify a Subnet Mask for your LAN segment. The default subnet mask is '255.255.255.0'.

Click on **NEXT** to proceed to the next page (step 3) WAN Interface.

2.3 WAN Interface

In this section you have to select one of five types of connections that you will be using to connect your broadband router's WAN port to your ISP (see screen below).

Note: Different ISP's require different methods of connecting to the Internet, please check with your ISP as to the type of connection it requires.

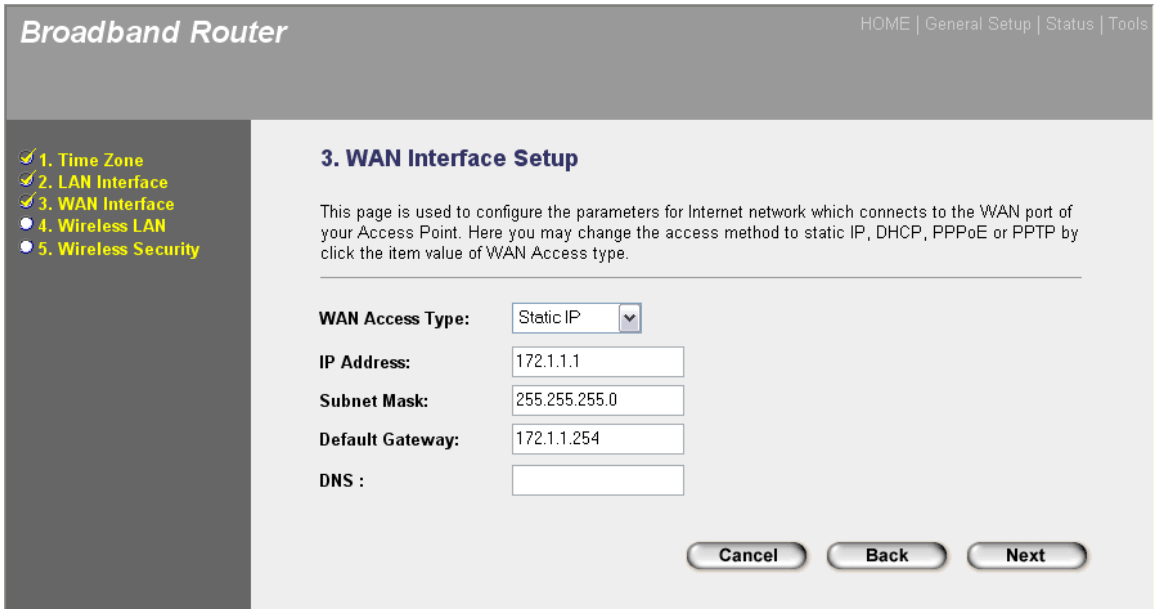


Menu	Description
2.3.1 Static IP	Your ISP will give a static IP address to you while you subscribe the service.
2.3.2 DHCP Client	Your ISP will automatically give you an IP address.
2.3.3 PPPoE	Your ISP requires you to use a Point-to-Point Protocol over Ethernet (PPPoE) connection.
2.3.4 PPTP	Your ISP requires you to use a Point-to-Point Tunneling Protocol (PPTP) connection.
2.3.5 L2TP	Your ISP requires you to use a Point-to-Point Tunneling Protocol (L2TP) connection.

Select one of the WAN types and set the manual's relevant sub-section (**2.3.1**, **2.3.2**, **2.3.3**, or **2.3.4**). Click on **Back** to return to the previous screen.

2.3.1 Static IP

Select Static IP if your ISP has given you a specific IP address for you to use. Your ISP should provide all the information required in this section.

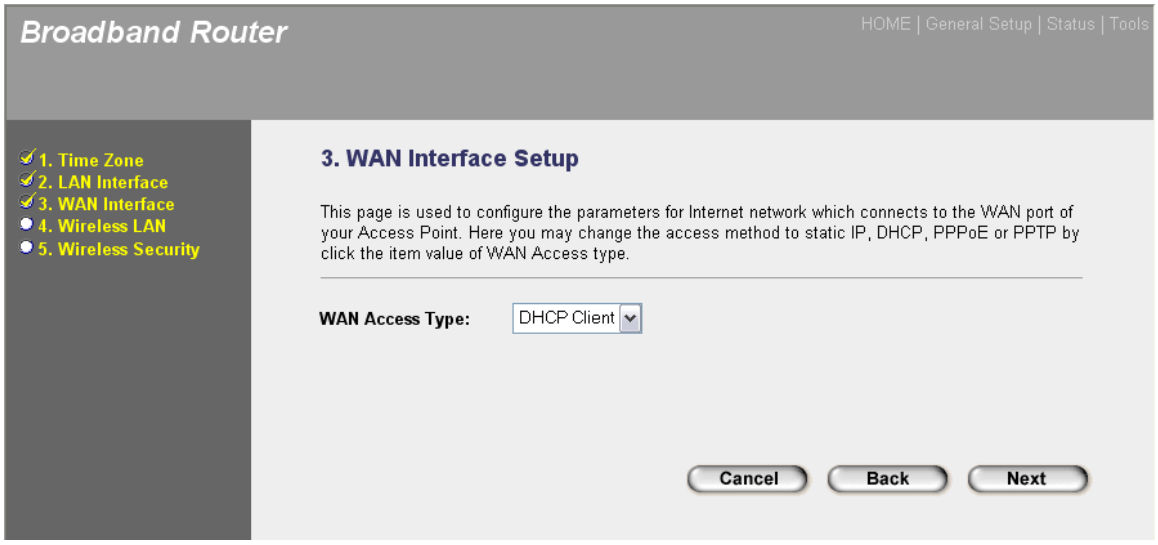


Parameters	Description
IP Address	This is the IP address that your ISP has given you.
Subnet Mask (e.g. 255.255.255.0)	Enter the Subnet Mask provided by your ISP.
Default Gateway IP	This is the ISP's IP address gateway.
DNS	This is the ISP's DNS server IP address.

Click on **NEXT** to proceed to the next page (step 4) Wireless Basic Settings.

2.3.2 DHCP Client

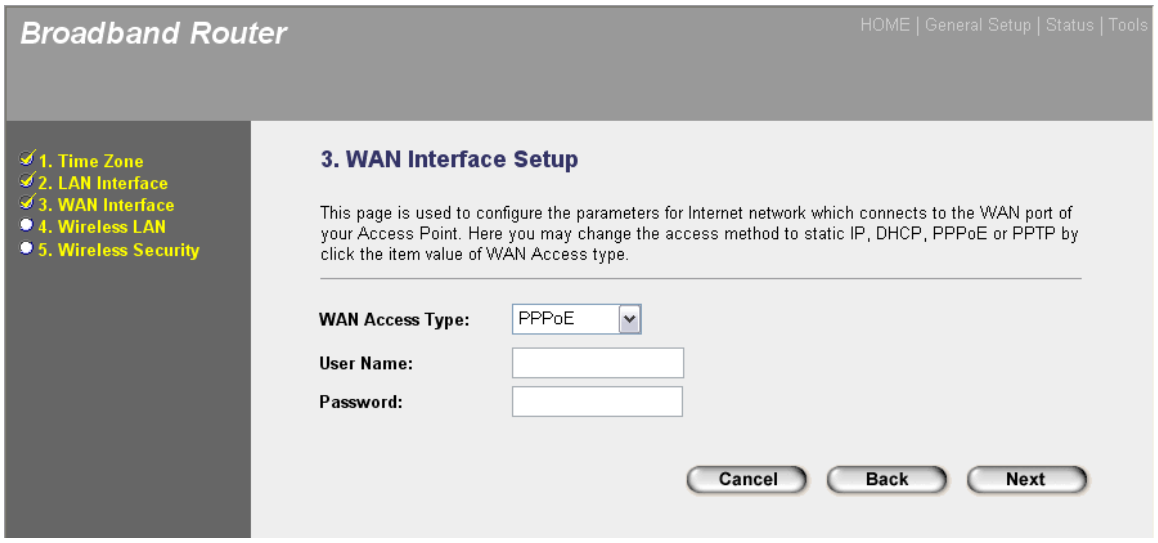
Choose DHCP Client if your ISP will automatically give you an IP address.



Click on **NEXT** to proceed to the next page (step 4) Wireless Basic Settings.

2.3.3 PPPoE

Select PPPoE if your ISP requires the PPPoE protocol to connect you to the Internet. Your ISP should provide all the information required in this section.



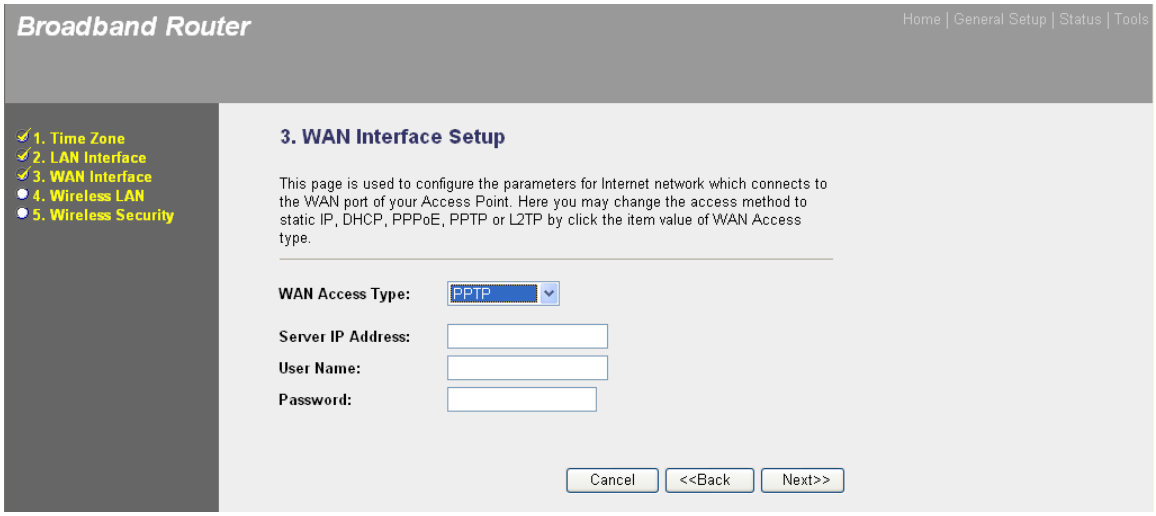
Parameter	Description
User Name	Enter the User Name provided by your ISP for the PPPoE connection.
Password	Enter the Password provided by your ISP for the PPPoE connection.

Click on **NEXT** to proceed to the next page (step 4) Wireless Basic Settings.

Note
The WAN "idle timeout" auto-disconnect function may not work due to abnormal activities of some network application software, computer virus or hacker attacks from the Internet. For example, some software sends network packets to the Internet in the background, even when you are not using the Internet. So please turn off your computer when you are not using it. This function also may not work with some ISP. So please make sure this function can work properly when you use this function in the first time, especially your ISP charge you by time used.

2.3.4 PPTP

Select PPTP if your ISP requires the PPTP protocol to connect you to the Internet. Your ISP should provide all the information required in this section.

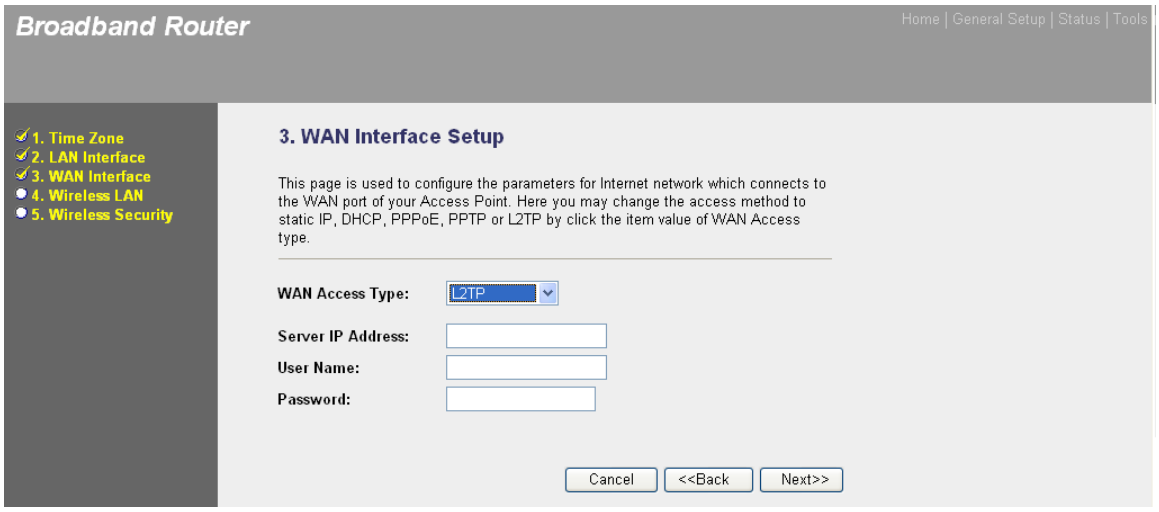


Parameter	Description
Server IP Address	Enter the IP address of the ISP Gateway.
User Name	Enter the User Name provided by your ISP for the PPTP connection. Sometimes called a Connection ID.
Password	Enter the Password provided by your ISP for the PPTP connection.

Click on **NEXT** to proceed to the next page (step 4) Wireless Basic Settings.

2.3.5 L2TP

Select L2TP if your ISP requires the L2TP protocol to connect you to the Internet. Your ISP should provide all the information required in this section.



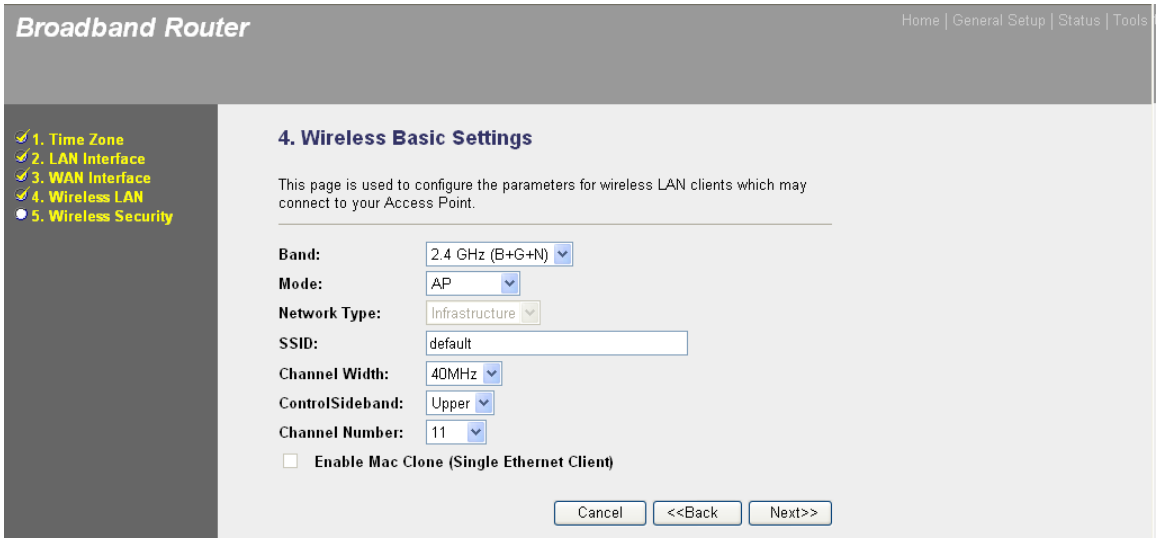
Parameter	Description
Server IP Address	Enter the IP address of the ISP Gateway.
User Name	Enter the User Name provided by your ISP for the L2TP connection. Sometimes it is called a Connection ID.

Password	Enter the Password provided by your ISP for the L2TP connection.

Click on **NEXT** to proceed to the next page (step 4) Wireless Basic Settings.

2.4 Wireless Basic Settings

Wireless Access Point builds a wireless LAN and can let all PCs equipped with IEEE 802.11b or 801.11g wireless network adaptor connect to your Intranet. It supports WEP and WPA2 encryption to enhance the security of your wireless network.



Menu	Description
Band	Please select the radio band from one of the following options. 2.4GHz(B): 2.4GHz band, only allows 802.11b wireless network client to connect this router (maximum transfer rate 11Mbps). 2.4 GHz (N): 2.4GHz band, only allows 802.11n wireless network client to connect this router (maximum transfer rate 150Mbps). 2.4 GHz (B+G):2.4GHz band, only allows 802.11b and 802.11g wireless network client to connect this router (maximum transfer rate 11Mbps for 802.11b clients, and maximum 54Mbps for 802.11g clients).

	2.4 GHz (G): 2.4GHz band, only allows 802.11g wireless network client to connect this router (maximum transfer rate 54Mbps). 2.4 GHz (B+G+N): 2.4GHz band, allows 802.11b, 802.11g, and 802.11n wireless network client to connect this router (maximum transfer rate 11Mbps for 802.11b clients, maximum 54Mbps for 802.11g clients, and maximum 150Mbps for 802.11n clients).
Mode	It allows you to set the router to AP, Client, WDS or AP + WDS mode.
Network Type	In client mode, you can specify your client to connect as an infrastructure client or an ad hoc client.
SSID	This is the name of wireless router. You can type any alphanumerical characters here, maximum 32 characters. SSID is used to identify your own wireless router from others when there are other wireless routers in the same area. Default SSID is 'default', it's recommended to change default SSID value to the one which is meaningful to you, like myhome, office_room1, etc.
Channel Width	Set channel width of wireless radio. Do not modify default value if you don't know what it is, default setting is '40 MHz'.
ControlSideBand	Select the upper band or lower band for your radio frequency. While upper band is selected, the channel number you can select is from channel 5 to channel 11. While lower band is selected, the channel number you can select is from channel 1 to channel 7.
Channel Number	Please select a channel from the dropdown list of 'Channel Number', available channel numbers are 1 to 13 for European countries, 1 to 11 for USA. You can choose any channel number you want to use, and almost all wireless clients can locate the channel you're using automatically without any problem. However, it's still useful to remember the channel number you use, some wireless client supports manual channel number select, and this would help in certain scenario when there is some radio communication problem.

Enable MAC Clone (Single Ethernet Client)	Check the check box will let router copy the first seen MAC address to the WLAN MAC.

Click on **NEXT** to proceed to the next page (step 5) Wireless Security.

2.5 Wireless Security Settings

This page allows you setup the wireless security. Turn on WEP or WPA by using Encryption Keys could prevent any unauthorized access to your wireless network.

Menu	Description
None	Do not apply any encryption to wireless usage. Everyone can access the wireless without permission.
2.5.1 WEP	You can select the WEP key length for encryption, 64-bit or 128-bit. Larger WEP key length will provide higher level of security, but the throughput will be lower.
2.5.2 WPA(TKIP)	You can use a pre-shared key to authenticate wireless stations and encrypt data during communication. And use TKIP to change the encryption key frequently.

2.5.3 WPA2(AES)	You can use a pre-shared key to authenticate wireless stations and encrypt data during communication. And use CCMP(AES) to change the encryption key frequently.
2.5.4 WPA2 Mixed	This will use TKIP or AES based on the other communication peer automatically.

Select one of the Security types and set the manual's relevant sub-section (**2.5.1**, **2.5.2**, **2.5.3**, or **2.5.4**). Click on **Back** to return to the previous screen.

2.5.1 WEP

When you select 64-bit or128-bit WEP key, you have to enter WEP keys to encrypt data. You can generate the key by yourself and enter it. You can enter four WEP keys and select one of them as default key. Then the router can receive any packets encrypted by one of the four keys.

Parameters	Description
Key Length	You can select the WEP key length for encryption, 64-bit or 128-bit. Larger WEP key length will provide higher level of security, but the throughput will be lower.

Key Format	You may select to select ASCII Characters (alphanumeric format) or Hexadecimal Digits (in the "A-F", "a-f" and "0-9" range) to be the WEP Key. For example: ASCII Characters: guest Hexadecimal Digits: 12345abcde
Key Setting	The WEP key are used to encrypt data transmitted in the wireless network. Fill the text box by following the rules below. 64-bit WEP: input 10-digit Hex values (in the "A-F", "a-f" and "0-9" range) or 5-digit ASCII character as the encryption keys. 128-bit WEP: input 26-digit Hex values (in the "A-F", "a-f" and "0-9" range) or 13-digit ASCII characters as the encryption keys.

Clicking on **OK** to save and active all the settings. Now, you can start to use the router as your internet gateway.

2.5.2 WPA(TKIP)

Wi-Fi Protected Access (WPA) is an advanced security standard. You can use a pre-shared key to authenticate wireless stations and encrypt data during communication. It uses TKIP to change the encryption key frequently. So the encryption key is not easy to be broken by hackers. This can improve security very much.

Parameters	Description
Pre-shared Key Format	You may select to select Passphrase (alphanumeric format) or Hexadecimal Digits (in the “A-F”, “a-f” and “0-9” range) to be the Pre-shared Key. For example: Passphrase: iamguest Hexadecimal Digits: 12345abcde
Pre-shared Key	The Pre-shared key is used to authenticate and encrypt data transmitted in the wireless network. Fill the text box by following the rules below. Hex: input 64-digit Hex values (in the “A-F”, “a-f” and “0-9” range) or at least 8 character pass phrase as the pre-shared keys.

Clicking on **OK** to save and active all the settings. Now, you can start to use the router as your internet gateway.

2.5.3 WPA2(AES)

Wi-Fi Protected Access 2(WPA2) is an advanced security standard. You can use a pre-shared key to authenticate wireless stations and encrypt data during communication. It uses CCMP(AES) to change the encryption key frequently. So the encryption key is not easy to be broken by hackers. This can improve security very much.

Parameters	Description
Pre-shared Key Format	You may select to select Passphrase (alphanumeric format) or Hexadecimal Digits (in the “A-F”, “a-f” and “0-9” range) to be the Pre-shared Key. For example: Passphrase: iamguest Hexadecimal Digits: 12345abcde
Pre-shared Key	The Pre-shared key is used to authenticate and encrypt data transmitted in the wireless network. Fill the text box by following the rules below. Hex: input 64-digit Hex values (in the “A-F”, “a-f” and “0-9” range) or at least 8 character pass phrase as the pre-shared keys.

Clicking on **OK** to save and active all the settings. Now, you can start to use the router as your internet gateway.

2.5.4 WPA2 Mixed

Wi-Fi Protected Access 2(WPA2) is an advanced security standard. You can use a pre-shared key to authenticate wireless stations and encrypt data during communication. It uses TKIP or CCMP(AES) to change the encryption key frequently. So the encryption key is not easy to be broken by hackers. This can improve security very much.

Parameters	Description
Pre-shared Key Format	You may select to select Passphrase (alphanumeric format) or Hexadecimal Digits (in the “A-F”, “a-f” and “0-9” range) to be the Pre-shared Key. For example: Passphrase: iamguest Hexadecimal Digits: 12345abcde
Pre-shared Key	The Pre-shared key is used to authenticate and encrypt data transmitted in the wireless network. Fill the text box by following the rules below. Hex: input 64-digit Hex values (in the “A-F”, “a-f” and “0-9” range) or at least 8 character pass phrase as the pre-shared keys.

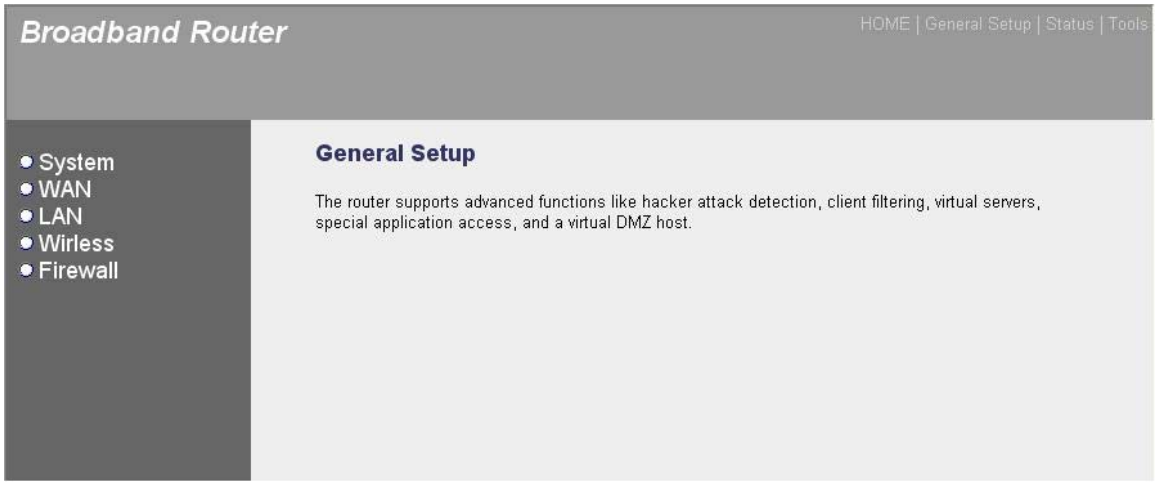
Clicking on **OK** to save and active all the settings. Now, you can start to use the router as your internet gateway.

Chapter 3 General Settings

Once you click on the **General Setup** button at the Home Page, you should see the screen below.

If you have already configured the Quick Setup Wizard you do NOT need to configure anything thing in the General Setup screen for you to start using the Internet.

The General Setup contains advanced features that allow you to configure the router to meet your network's needs such as: Wireless, Address Mapping, Access Control, Hacker Attack Prevention, Special Applications, DMZ and other functions.



Below is a general description of what advance functions are available for this broadband router.

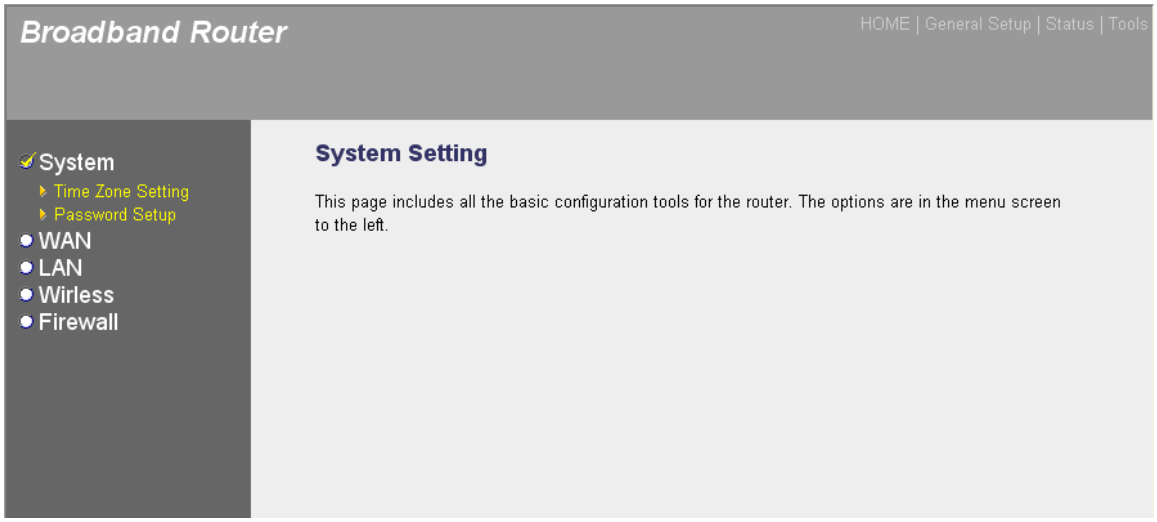
Menu	Description
3.1 System	This section allows you to set the Broadband router's system Time Zone, Password and Remote Management Administrator.
3.2 WAN	This section allows you to select the connection method in order to establish a connection with your ISP. (same as the Quick Setup Wizard section)
3.3 LAN	You can specify the LAN segment's IP address, subnet Mask, enable/disable DHCP and select an IP range for your LAN
3.4 Wireless	You can setup the wireless LAN's SSID, WEP key, MAC filtering.

3.5 Firewall	The Firewall section allows you to configure Access Control, Hacker Prevention and DMZ.
3.6 QoS	If you need to setup the bandwidth control for high priority network traffic, please go to this section.

Select one of the above six General Setup selections and proceed to the manual's relevant sub-section

3.1 System

The system screen allows you to specify a time zone, to change the system password and to specify a remote management user for the broadband router.

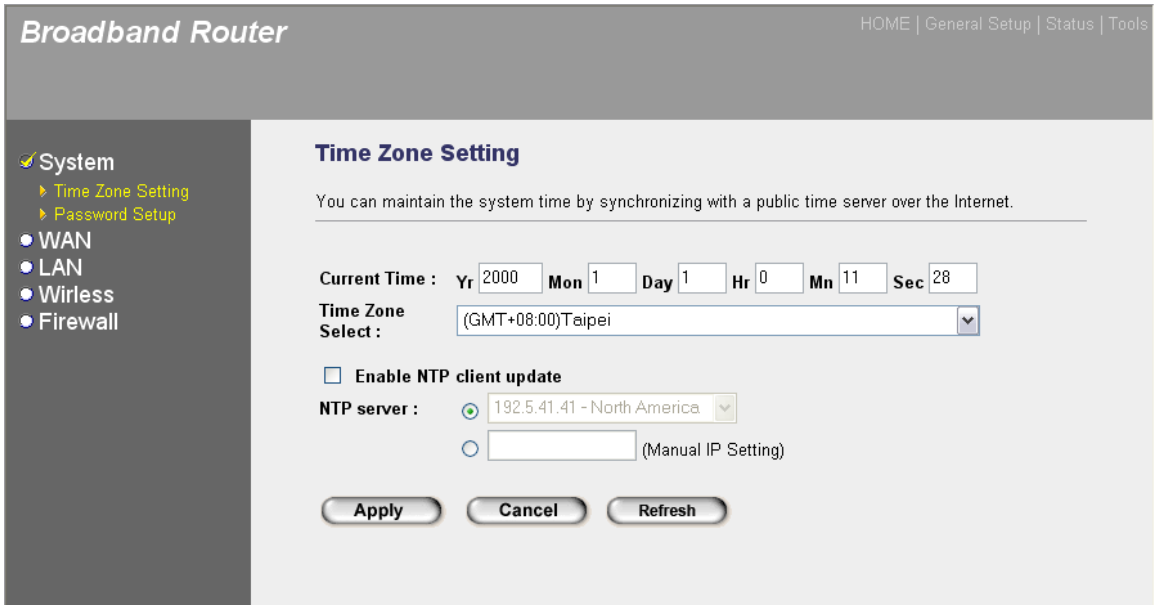


Parameters	Description
3.1.1 Time Zone Setting	Select the time zone of the country you are currently in. The router will set its time based on your selection.
3.1.2 Password Setup	Allows you to select a password in order to access the web-based management website.

Select one of the above three system settings selections and proceed to the manual's relevant sub-section

3.1.1 Time Zone Setting

The Time Zone Setting allows your router to reference or base its time on the settings configured here, which will affect functions such as Log entries and Firewall settings.

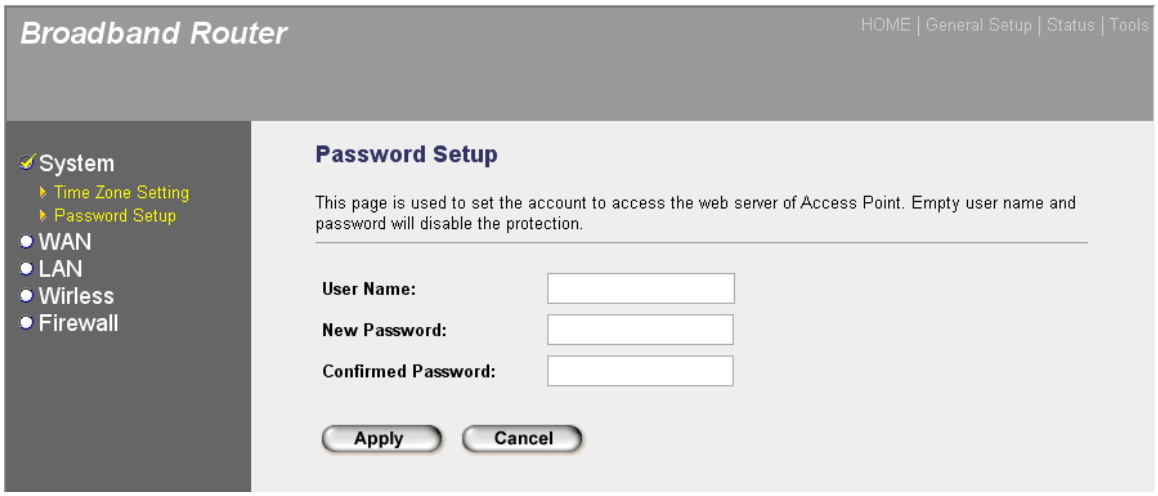


Parameter	Description
Current Time	Set the current time.
Time Zone Select	Select the time zone of the country you are currently in. The router will set its time based on your selection.
Enable NTP client update	Check the box to enable router to update time from NTP server.
Automatically Adjust Daylight Saving	If the country you live uses daylight saving, please check this box.
NTP Server	Select one preset time server or manual input a server IP.

Click <**Apply>** at the bottom of the screen to save the above configurations. You can now configure other advance sections or start using the router (with the advance settings in place)

3.1.2 Password Setup

You can change the password required to log into the broadband router's system web-based management. By default, there is no password. So please assign a password to the Administrator as soon as possible, and store it in a safe place. Passwords can contain 0 to 12 alphanumeric characters, and are case sensitive.

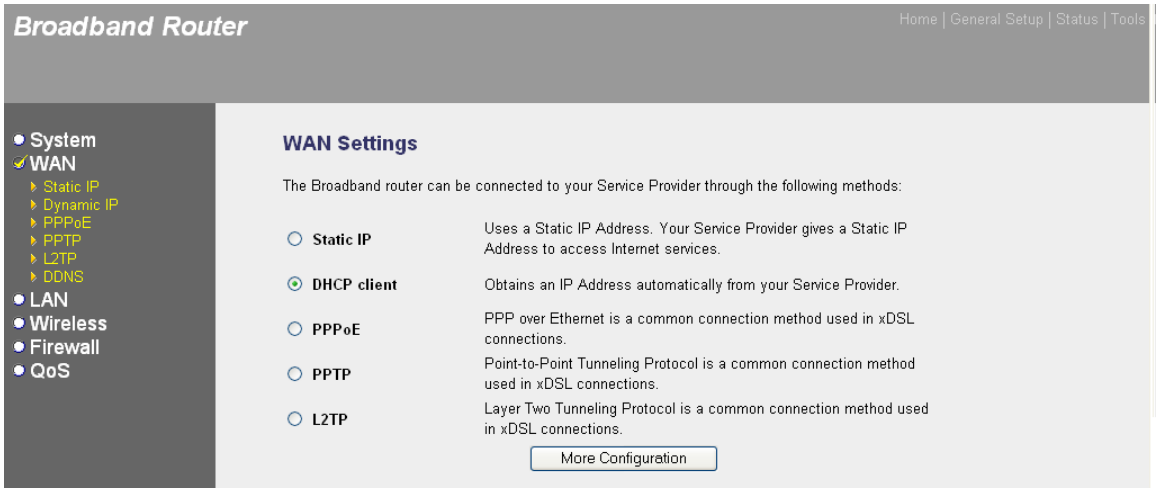


Parameters	Description
User Name	Change your login user name.
New Password	Enter your new password
Confirmed Password	Enter your new password again for verification purposes **Note**: If you forget your password, you'll have to reset the router to the factory default (No password) with the reset button (see router's back panel)

Click <**Apply>** at the bottom of the screen to save the above configurations. You can now configure other advance sections or start using the router (with the advance settings in place)

3.2 WAN

Use the WAN Settings screen if you have already configured the Quick Setup Wizard section and you would like to change your Internet connection type. The WAN Settings screen allows to specify the type of WAN port connect you want to establish with your ISP. The WAN settings offer the following selections for the router's WAN port, **Static IP Address**, **DHCP Client**, **PPPoE**, **PPTP**, **L2TP** and **DDNS**. Please choose one type and click 'More Configuration'.

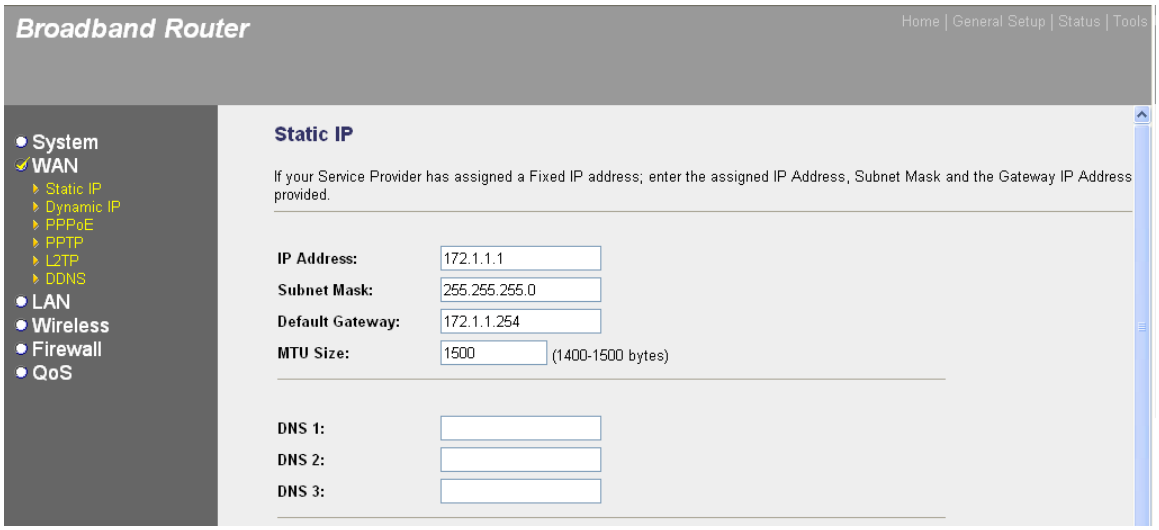


Parameters	Description
3.2.1 Static IP	Your ISP has given you an IP address already.
3.2.2 DHCP Client	Your ISP will automatically give you an IP address.
3.2.3 PPPoE	Your ISP requires PPPoE connection.
3.2.4 PPTP	Your ISP requires you to use a Point-to-Point Tunneling Protocol (PPTP) connection.
3.2.5 L2TP	Your ISP requires L2TP connection.

Once you have made a selection, proceed to the manual's relevant sub-section.

3.2.1 Static IP

Select Static IP address if your ISP has given you a specific IP address for you to use. Your ISP should provide all the information required in this section.



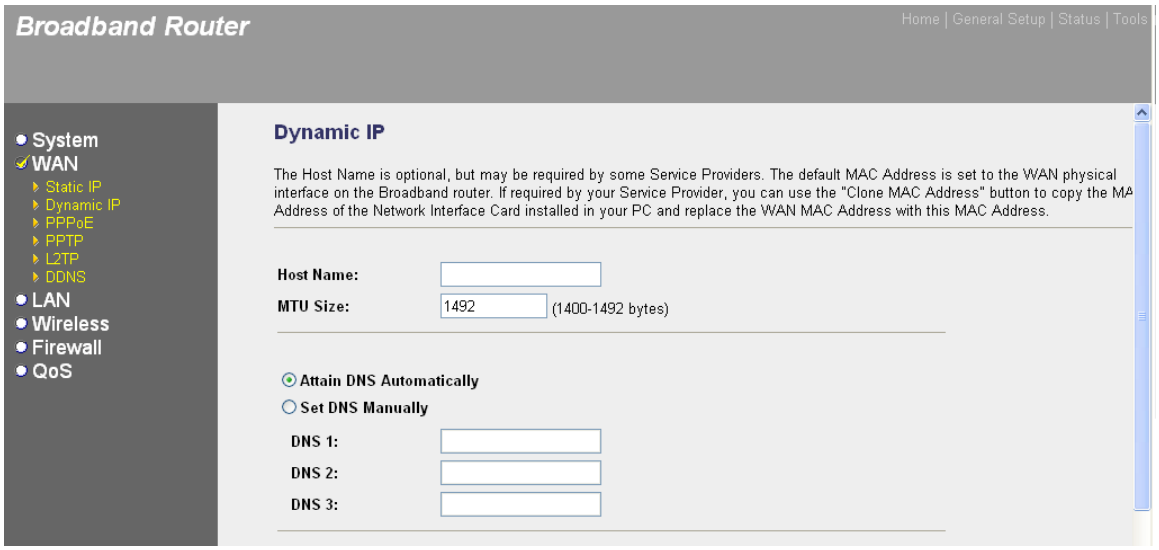
Parameters	Description
IP Address	This is the IP address that your ISP has given you.
Subnet Mask	Enter the Subnet Mask provided by your ISP. (e.g. 255.255.255.0)
Default Gateway	This is the IP address of ISP's gateway.
MTU Size	MTU (Maximum Transmission Unit) determine the maximum size of each packet in any transmission within the network. Please specify the MTU range from 1400 to 1500 bytes. Please input the MTU value of your network connection here. If you don't know, you can use default value.
DNS 1	Please input the IP address of DNS server provided by your service provider.
DNS 2	Please input the IP address of additional DNS server provided by your service provider.

DNS 3	Please input the IP address of additional DNS server provided by your service provider.

Click <**Apply Changes>** at the bottom of the screen to save the above configurations. If you want to configure other advanced settings in this web page, please go to section 3.2.6 for more information.

3.2.2 DHCP Client

Choose the Dynamic IP selection if your ISP will automatically give you an IP address. Some ISP's may also require that you fill in additional information such as Host Name, Domain Name and MAC address.



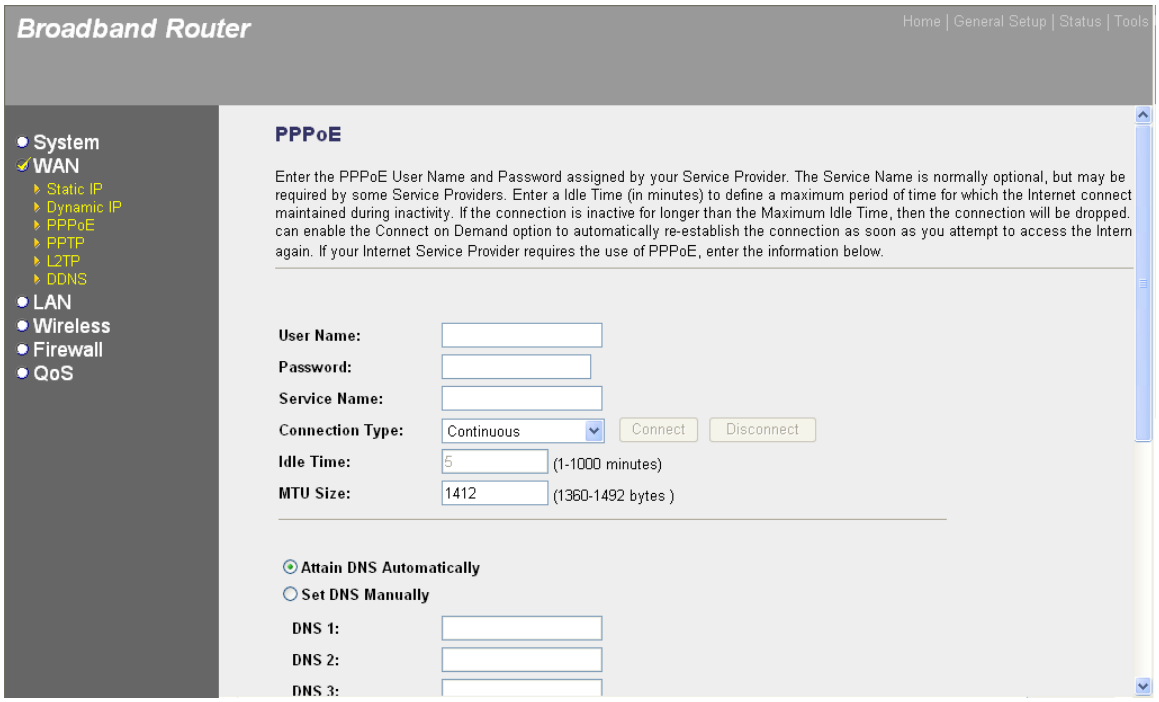
Parameters	Description
Host Name	Please input host name of your computer, this is optional, and only required if your service provider asks you to do so.
MTU Size	MTU (Maximum Transmission Unit) determine the maximum size of each packet in any transmission within the network. Please specify the MTU range from 1400 to 1492 bytes. Please input the MTU value of your network connection here. If you don't know, you can use default value.

Obtain DNS Automatically	The ISP requires you to obtain a DNS by DHCP server before you connecting to the internet.
Set DNS Manually	If your ISP gives you a static DNS server to be used to connect to the internet, please select this option.
DNS 1	Please input the IP address of DNS server provided by your service provider.
DNS 2	Please input the IP address of additional DNS server provided by your service provider.
DNS 3	Please input the IP address of additional DNS server provided by your service provider.

Click <**Apply Changes>** at the bottom of the screen to save the above configurations. If you want to configure other advanced settings in this web page, please go to section 3.2.6 for more information.

3.2.3 PPPoE (PPP over Ethernet)

Select PPPoE if your ISP requires the PPPoE protocol to connect you to the Internet. Your ISP should provide all the information required in this section. (See chapter 2 “PPPoE” for more detail)



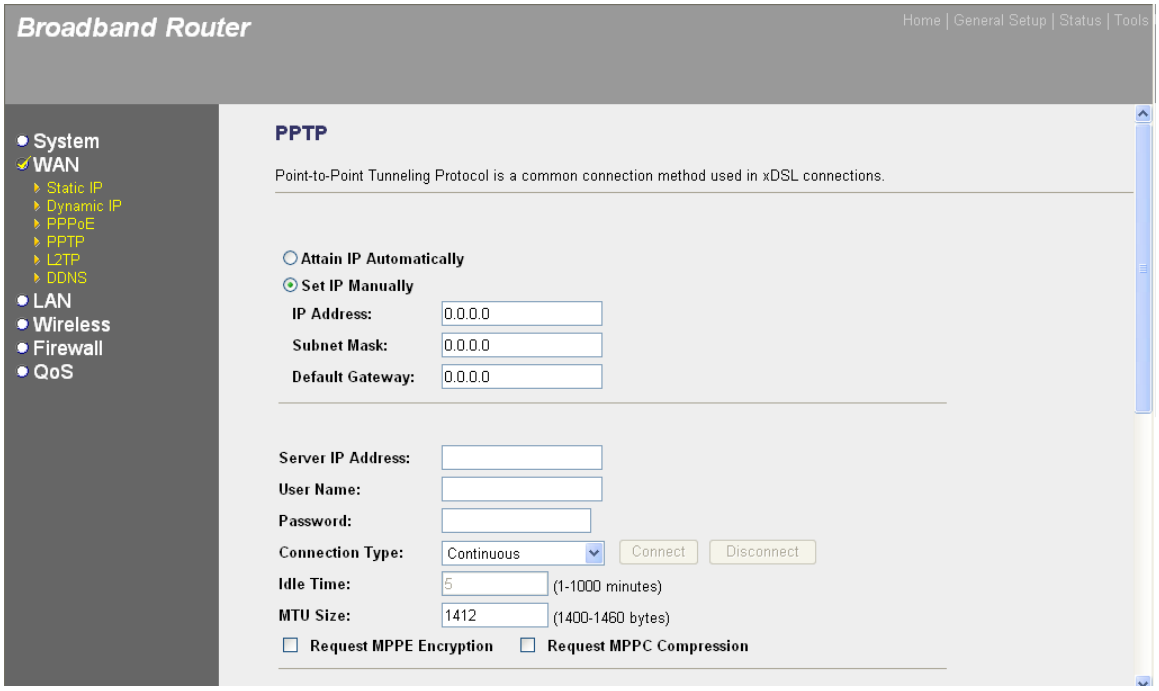
Parameters	Description
User Name	Please input user name assigned by your Internet service provider here.
Password	Please input the password assigned by your Internet service provider here.
Service Name	Please give a name to this Internet service, this is optional
Connection Type	Please select the connection type of Internet connection you wish to use. There are 3 options: “**Continuous**” - keep internet connection alive, do not disconnect, “**connect on Demand**“ - only connects to Internet when there’s a connect attempt, and “**Manual**” - only connects to Internet when ‘Connect’ button on this page is pressed, and disconnects when ‘Disconnect button is pressed.

Idle Time	Please input idle time out. Specify the time to shutdown internet connection after no internet activity is detected after a while. This option is only available when connection type is 'Connect on Demand'.
MTU Size	MTU (Maximum Transmission Unit) determine the maximum size of each packet in any transmission within the network. Please specify the MTU range from 1360 to 1492 bytes. Please input the MTU value of your network connection here. If you don't know, you can use default value.
Obtain DNS Automatically	The ISP requires you to obtain a DNS by DHCP server before you connecting to the internet.
Set DNS Manually	If your ISP gives you a static DNS server to be used to connect to the internet, please select this option.
DNS 1	Please input the IP address of DNS server provided by your service provider.
DNS 2	Please input the IP address of additional DNS server provided by your service provider.
DNS 3	Please input the IP address of additional DNS server provided by your service provider.

Click <**Apply Changes>** at the bottom of the screen to save the above configurations. If you want to configure other advanced settings in this web page, please go to section 3.2.6 for more information.

3.2.4 PPTP

Select PPTP if your ISP requires the PPTP protocol to connect you to the Internet. Your ISP should provide all the information required in this section.



Parameters	Description
Attain IP Automatically	Select this option if your ISP will assign IP Address to your router directly. Please contact your ISP if you don't know what you should select.
Set IP Address	This is the IP address that your ISP has given you.
Subnet Mask	Enter the Subnet Mask provided by your ISP. (e.g. 255.255.255.0)
Default Gateway	This is the IP address of ISP's gateway.
Server IP Address	Please input the IP address of PPTP gateway assigned by your Internet service provider here.

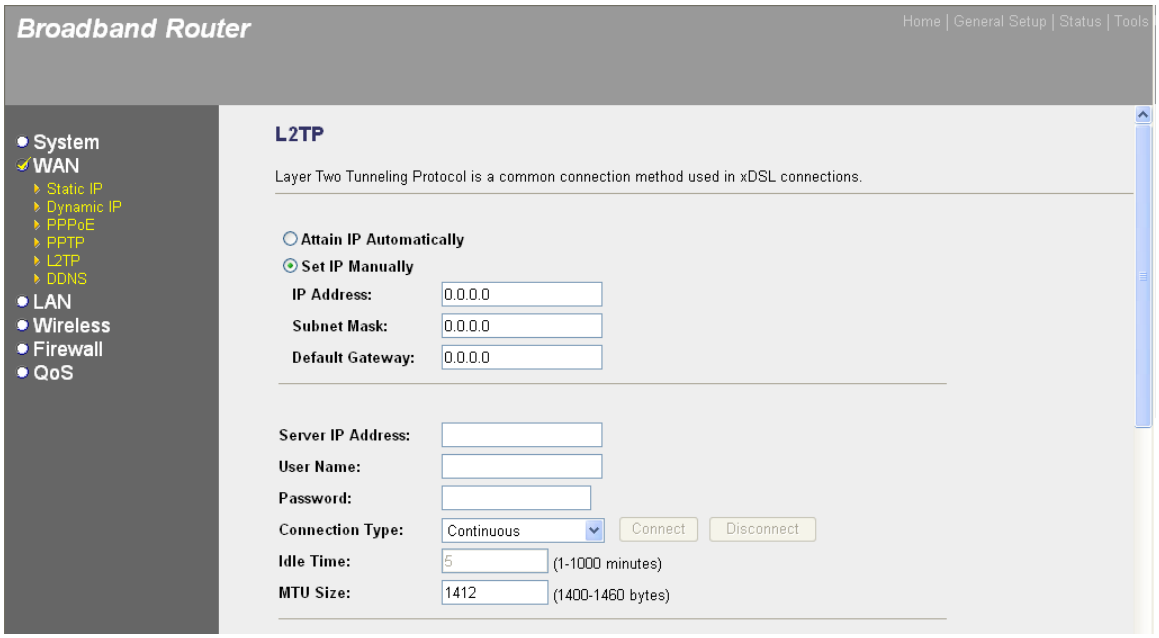
User Name	Please input user name assigned by your Internet service provider here.
Password	Please input the password assigned by your Internet service provider here.
Connection Type	Please select the connection type of Internet connection you wish to use. There are 3 options: "**Continuous**" - keep internet connection alive, do not disconnect, "**connect on Demand**" - only connects to Internet when there's a connect attempt, and "**Manual**" - only connects to Internet when 'Connect' button on this page is pressed, and disconnects when 'Disconnect button is pressed.
Idle Time	Please input idle time out. Specify the time to shutdown internet connection after no internet activity is detected after a while. This option is only available when connection type is 'Connect on Demand'.
MTU Size	MTU (Maximum Transmission Unit) determine the maximum size of each packet in any transmission within the network. Please specify the MTU range from 1400 to 1460 bytes. Please input the MTU value of your network connection here. If you don't know, you can use default value.
Request MPPE Encryption	MPPE (Microsoft Point-to-Point Encryption) is a method of encrypting data across PPTP virtual private network connections. Check this box if it is needed for your virtual private network links.
Request MPPC Encryption	MPPC (Microsoft Point-to-Point Compression) which compresses data across virtual private network links. Check this box if it is needed.
Obtain DNS Automatically	The ISP requires you to obtain a DNS by DHCP server before you connecting to the internet.
Set DNS Manually	If your ISP gives you a static DNS server to be used to connect to the internet, please select this option.
DNS 1	Please input the IP address of DNS server provided by your service provider.

DNS 2	Please input the IP address of additional DNS server provided by your service provider.
DNS 3	Please input the IP address of additional DNS server provided by your service provider.

Click <**Apply Changes>** at the bottom of the screen to save the above configurations. If you want to configure other advanced settings in this web page, please go to section 3.2.6 for more information.

3.2.5 L2TP

Select L2TP if your ISP requires the L2TP protocol to connect you to the Internet. Your ISP should provide all the information required in this section.



Parameters	Description
Attain IP Automatically	Please select the type of how you obtain IP address from your service provider here. You can choose "**Attain IP automatically**" or use the "**Set IP Manually**"

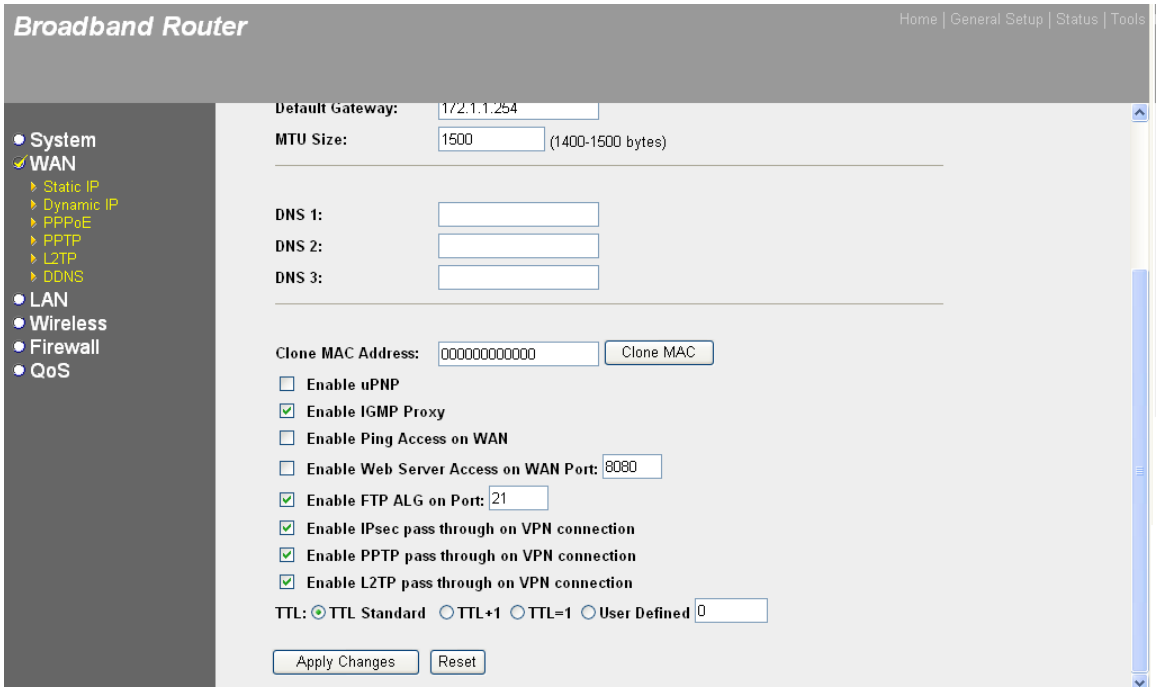
Set IP Manually	If you select the "**Set IP Manually**", please fill in these fields of the "**IP Address**" and "**Subnet Mask**"
IP Address	This is the IP address that your ISP has given you.
Subnet Mask	Enter the Subnet Mask provided by your ISP. (e.g. 255.255.255.0)
Default Gateway	This is the IP address of ISP's gateway.
Server IP Address	Please input the IP address of L2TP gateway assigned by your Internet service provider here.
User Name	Please input user name assigned by your Internet service provider here.
Password	Please input the password assigned by your Internet service provider here.
Connection Type	Please select the connection type of Internet connection you wish to use. There are 3 options: "**Continuous**" - keep internet connection alive, do not disconnect, "**connect on Demand**" - only connects to Internet when there's a connect attempt, and "**Manual**" - only connects to Internet when 'Connect' button on this page is pressed, and disconnects when 'Disconnect button is pressed.
Idle Time	Please input idle time out. Specify the time to shutdown internet connection after no internet activity is detected after a while. This option is only available when connection type is 'Connect on Demand'.
MTU Size	MTU (Maximum Transmission Unit) determine the maximum size of each packet in any transmission within the network. Please specify the MTU range from 1400 to 1460 bytes. Please input the MTU value of your network connection here. If you don't know, you can use default value.
Obtain DNS Automatically	The ISP requires you to obtain a DNS by DHCP server before you connecting to the internet.

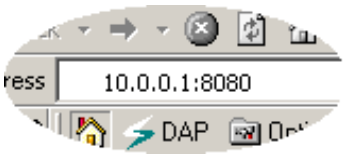
Set DNS Manually	If your ISP gives you a static DNS server to be used to connect to the internet, please select this option.
DNS 1	Please input the IP address of DNS server provided by your service provider.
DNS 2	Please input the IP address of additional DNS server provided by your service provider.
DNS 3	Please input the IP address of additional DNS server provided by your service provider.

Click <**Apply Changes>** at the bottom of the screen to save the above configurations. If you want to configure other advanced settings in this web page, please go to section 3.2.6 for more information.

3.2.6 WAN Advanced Settings

There are some advanced settings for different WAN connection types. Please refer to the description as below.



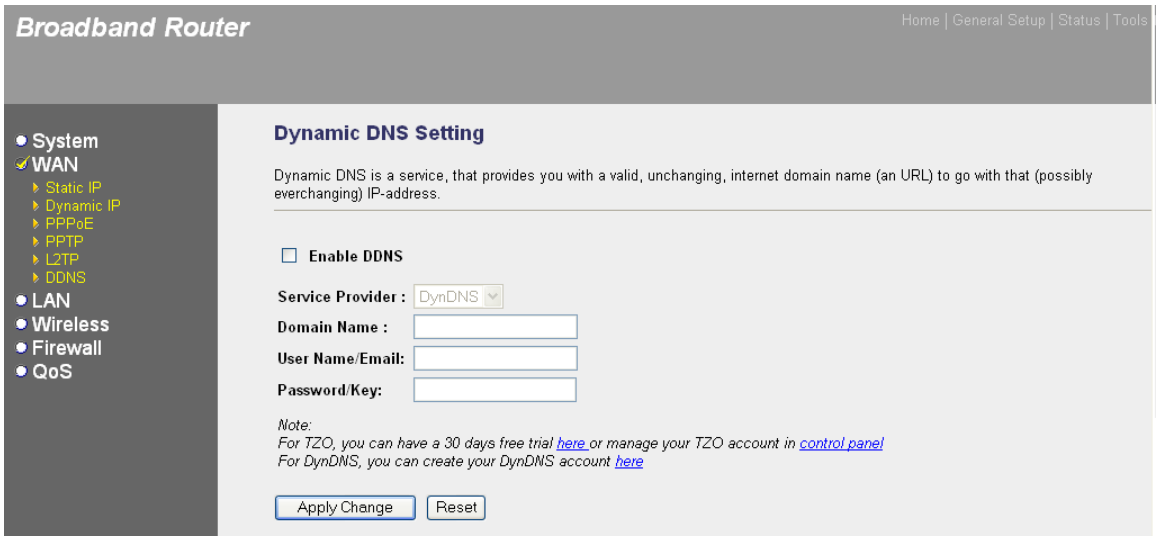
Parameters	Description
Clone MAC Address	For some applications, you may need to designate a specific MAC address for the router. Please enter the MAC address here. If you are connecting the router to a computer, you can simply press 'Clone Mac' button to fill the MAC address field with the MAC address of your computer.
Enable UPnP	Check this box to enable UPnP feature here. After you enable the UPnP feature, all client systems that support UPnP, like Windows XP, can discover this router automatically and access the Internet through this router without any configuration. The NAT Traversal function provided by UPnP can let applications that support UPnP smoothly connect to Internet sites without any incompatibility problem due to the NAPT port translation.
Enable IGMP Proxy	Check this box if you want to enable the router as IGMP proxy to implement multicast routing.
Enable Ping Access on WAN	When this function is enabled, you will be allowed to ping the IP address of the router given by ISP from a remote site.
Enable Web Server Access on WAN Port	Please check this box to start the Web Server Access on WAN when you want to access the web-based management from a remote site. Enter the port number of your Web Server. Note: When you want to access the web-based management from a remote site, you must enter the router's WAN IP address (e.g. 10.0.0.1) into your web-browser followed by port number 8080, e.g. 10.0.0.1:8080 (as below). 
Enable FTP ALG on Port	If you have built up a FTP server in your network, you can enable this function to let the FTP traffics correctly pass though the NAT gateway of the router. Enter the port number of your FTP server.

Enable IPsec pass through On VPN connection	Check this box and the router will enable IPsec packets pass through the router for VPN connection.
Enable PPTP pass through On VPN connection	Check this box and the router will enable PPTP packets pass through the router for VPN connection
Enable L2TP pass through On VPN connection	Check this box and the router will enable L2TP packets pass through the router for VPN connection.
TTL	For some special applications, you might need to change the TTL value for the packets routing to your router. Please select 'TTL Standard', 'TTL+1', 'TTL=1' or 'User Defined" to define a value. If you don't know what it is / not sure if you need it, it's safe to set this option to 'TTL Standard'.

Click <**Apply Changes>** at the bottom of the screen to save the above configurations. You can now configure other advance sections or start using the router.

3.2.7 DDNS

DDNS allows you to map the static domain name to a dynamic IP address. You must get an account, password and your static domain name from the DDNS service providers. This router supports DynDNS, and TZO.

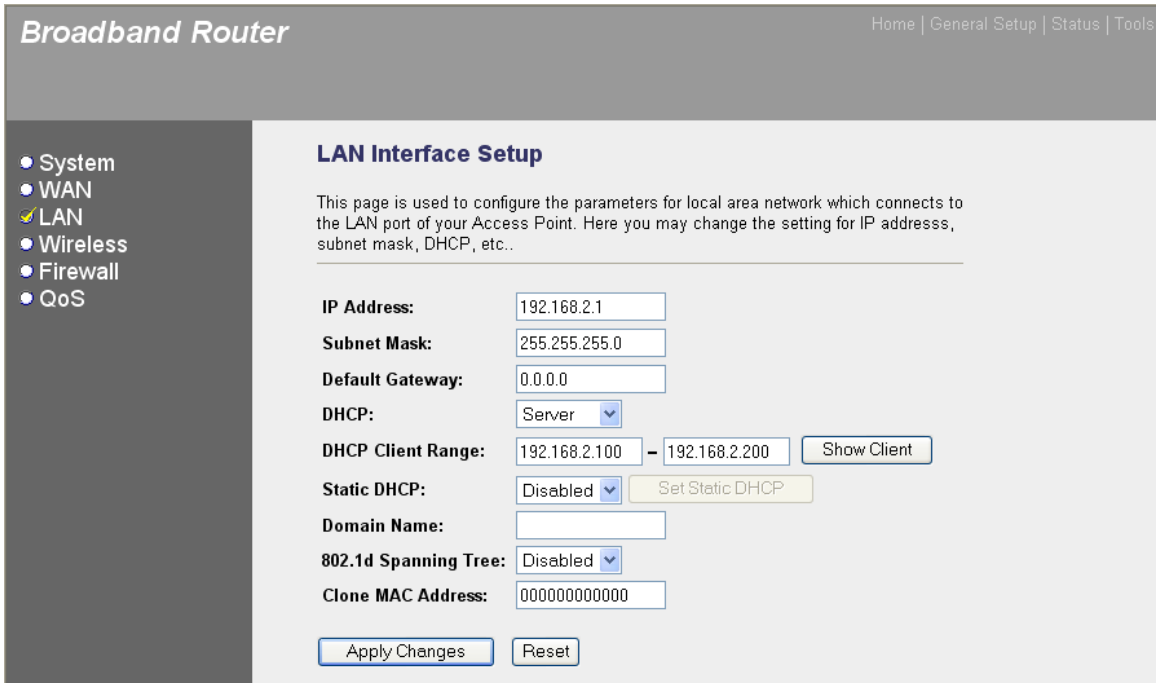


Parameters	Default	Description
Enable DDNS	Disable	Enable/Disable the DDNS function of this router.
Service Provider		Select a DDNS service provider.
Domain name		Your static domain name that use DDNS.
User Name/Email		The account that your DDNS service provider assigned to you.
Password/Key		The password you set for the DDNS service account above.

Click <**Apply Changes**> at the bottom of the screen to save the above configurations. You can now configure other advance sections or start using the router (with the advance settings in place)

3.3 LAN

The LAN Port screen below allows you to specify a private IP address for your router's LAN ports as well as a subnet mask for your LAN segment.



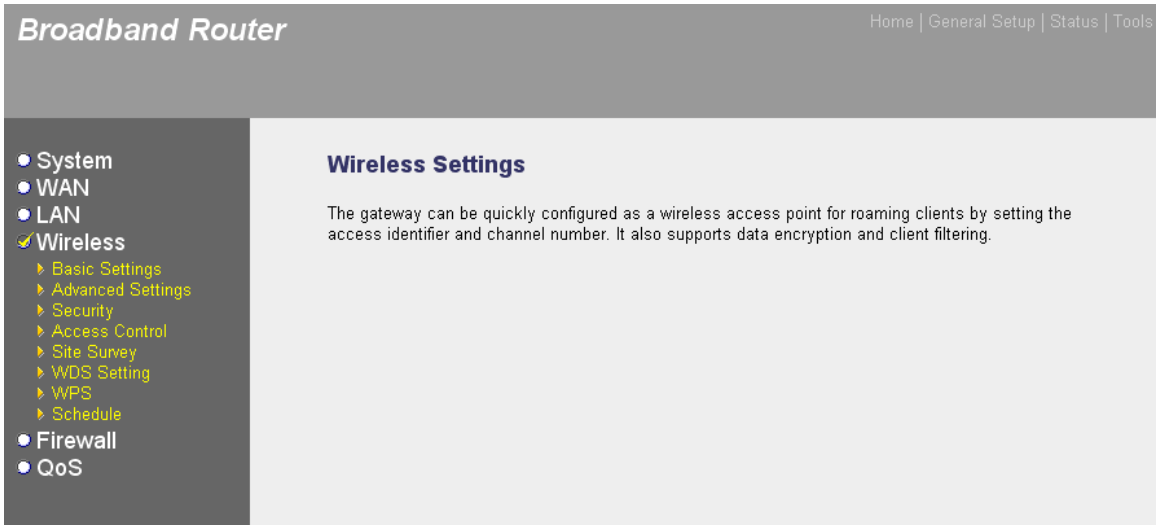
Parameters	Default	Description
IP address	192.168.2.1	This is the router's LAN port IP address (Your LAN clients default gateway IP address).
Subnet Mask	255.255.255.0	Specify a Subnet Mask for your LAN segment.
Default Gateway		Specify the default gateway for LAN segment.
DHCP	Server	You can select the DHCP type for LAN segment. By selecting the DHCP server, the router will automatically give your LAN clients an IP address. By selecting the DHCP client, the router will get an IP address from LAN DHCP server automatically. If the DHCP server is not enabled then you'll have to manually set your LAN client's IP addresses; make sure the LAN Client is in the same subnet as this broadband

		router if you want the router to be your LAN client's default gateway.
DHCP Client Range		You can select a particular IP address range for your DHCP server to issue IP addresses to your LAN Clients. **Note:** By default the IP range is from: Start IP **192.168.2.100** to End IP **192.168.2.199**. If you want your PC to have a static/fixed IP address then you'll have to choose an IP address outside this IP address Pool.
802.1d Spanning Tree	Disabled	If 802.1d Spanning Tree function is enabled, this router will use the spanning tree protocol to prevent from network loop happened in the LAN ports.
Clone MAC Address		Specify the MAC Address for your LAN interface.

Click <**Apply Changes**> at the bottom of the screen to save the above configurations. You can now configure other advance sections or start using the router (with the advance settings in place)

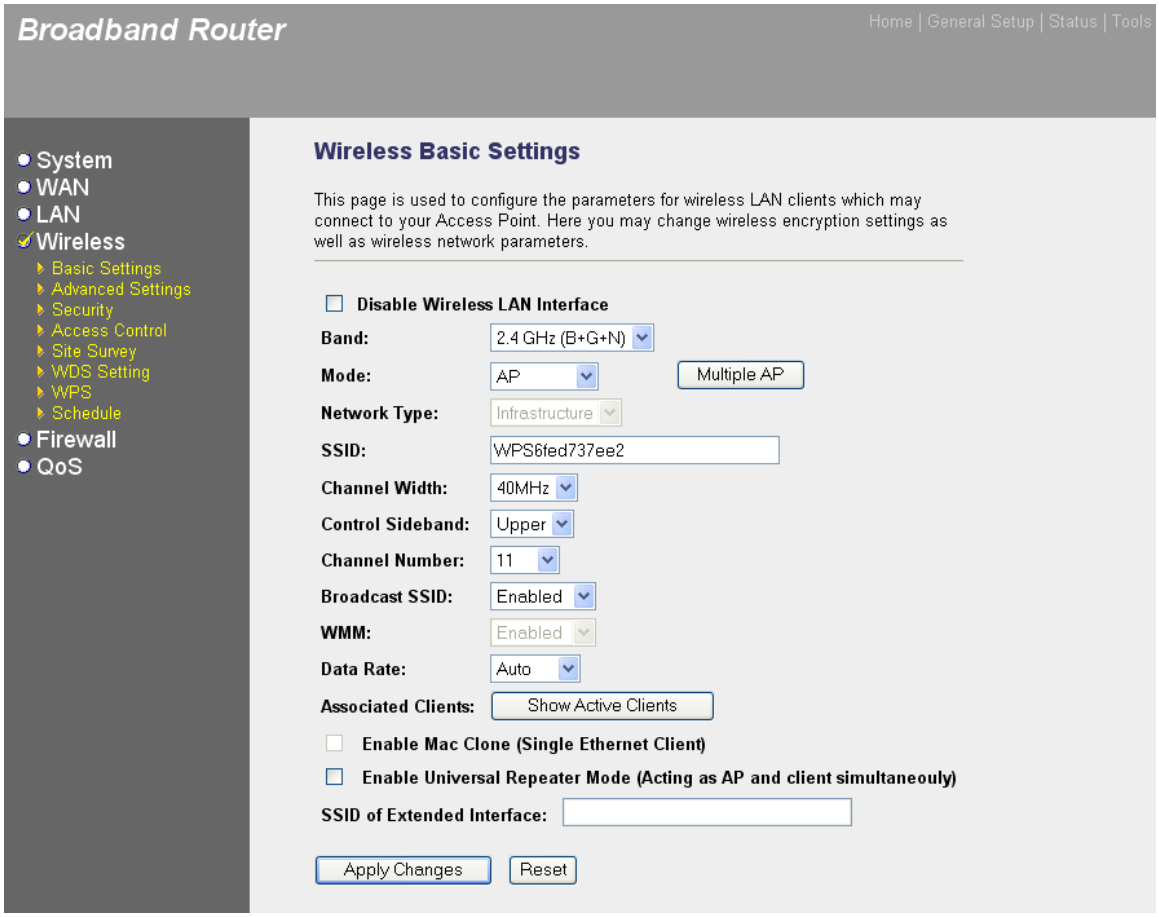
3.4 Wireless

Wireless Access Point builds a wireless LAN and can let all IEEE 802.11b, IEEE 801.11g or IEEE 802.1n wireless stations connect to your Intranet. It supports WEP, WPA and WPA2 encryption to enhance the security of your wireless network. It also support WPS function for you to easy setup the wireless connection between the Access Point with other stations.



3.4.1 Basic Settings

You can set parameters that are used for the wireless stations to connect to this router. The parameters include Mode, ESSID, Channel Number and Associated Client.



Parameters	Default	Description
Disable Wireless LAN Interface		Check this box to disable wireless LAN.
Band		Please select the radio band from one of the following options. 2.4GHz(B): 2.4GHz band, only allows 802.11b wireless network client to connect this router (maximum transfer rate 11Mbps).

	2.4 GHz (N): 2.4GHz band, only allows 802.11n wireless network client to connect this router (maximum transfer rate 150Mbps). 2.4 GHz (B+G):2.4GHz band, only allows 802.11b and 802.11g wireless network client to connect this router (maximum transfer rate 11Mbps for 802.11b clients, and maximum 54Mbps for 802.11g clients). 2.4 GHz (G): 2.4GHz band, only allows 802.11g wireless network client to connect this router (maximum transfer rate 54Mbps). 2.4 GHz (B+G+N): 2.4GHz band, allows 802.11b, 802.11g, and 802.11n wireless network client to connect this router (maximum transfer rate 11Mbps for 802.11b clients, maximum 54Mbps for 802.11g clients, and maximum 150Mbps for 802.11n clients).
Mode	It allows you to set the wireless mode of the router to AP, Client, WDS or AP+WDS mode. **AP** : standard wireless access point. **Client** : Configure the router to Ethernet device such us TV, Game player, HDD&DVD to enable the Ethernet device be a wireless station. **WDS** : Connect this router with other WDS-capable wireless routers, to expand the scope of network. **AP + WDS (Universal Repeater)** : The router can act as Station and AP at the same time. It can use Station function to connect to a Root AP and use AP function to service all wireless stations within its coverage.
Multiple AP	This access point supports multiple APs function. Please go to section 3.4.1.1 for more information.
Network Type	You can set the client mode to Infrastructure or Ad Hoc mode here.

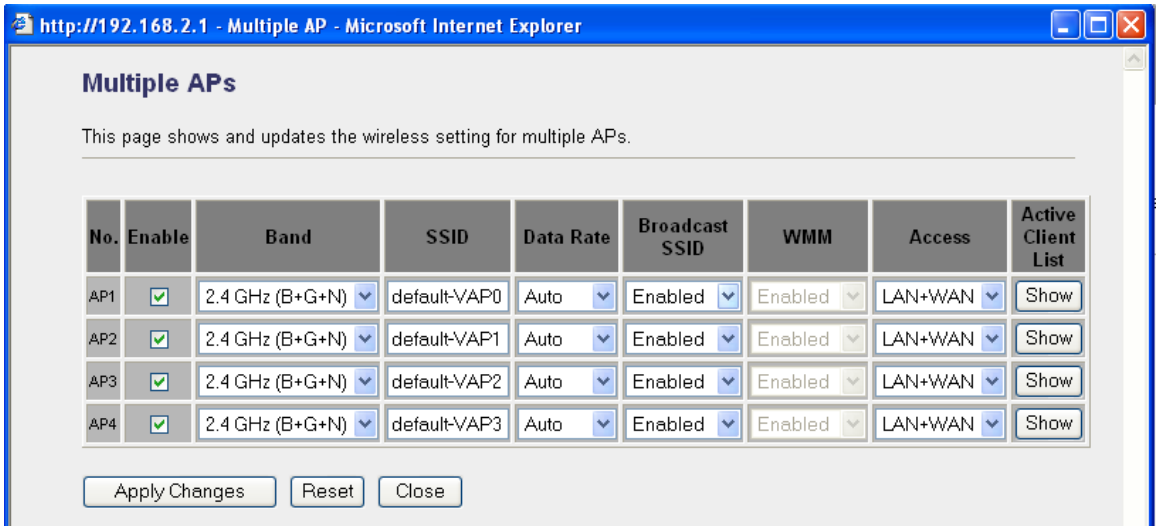
SSID	default	This is the name of wireless router. You can type any alphanumerical characters here, maximum 32 characters. SSID is used to identify your own wireless router from others when there are other wireless routers in the same area. Default SSID is ‘default’, it’s recommended to change default SSID value to the one which is meaningful to you, like myhome, office_room1, etc.
Channel Width		Set channel width of wireless radio. Do not modify default value if you don’t know what it is, default setting is ‘40 MHz’.
ControlSideBand		Select the upper band or lower band for your radio frequency. While upper band is selected, the channel number you can select is from channel 5 to channel 11. While lower band is selected, the channel number you can select is from channel 1 to channel 7.
Channel Number		Please select a channel from the dropdown list of ‘Channel Number’, available channel numbers are 1 to 13 for European countries, 1 to 11 for USA. You can choose any channel number you want to use, and almost all wireless clients can locate the channel you’re using automatically without any problem. However, it’s still useful to remember the channel number you use, some wireless client supports manual channel number select, and this would help in certain scenario when there is some radio communication problem.
Broadcast SSID		Decide if the wireless router will broadcast its own SSID or not. You can hide the SSID of your wireless router (set the option to ‘Disable’), so only people those who know the SSID of your wireless router can get connected.
WMM		The short of Wi-Fi MultiMedia, it will enhance the data transfer performance of multimedia contents when they’re being transferred over wireless network. If you don’t know what it is /

	not sure if you need it, it's safe to set this option to 'Enable'.
Data Rate	Set the wireless data transfer rate to a certain value. Since most of wireless devices will negotiate with each other and pick a proper data transfer rate automatically, it's not necessary to change this value unless you know what will happen after modification.
Associated Clients	Click "Show Active Clients" button, then an "Active Wireless Client Table" will pop up. You can see the status of all active wireless stations that are connecting to the access point.
Enable MAC Clone (Single Ethernet Client)	Check the check box will copy the MAC address of your PC to wireless Interface when the first packet was received.
Enable Universal Repeater Mode (Acting as AP and client simultaneously)	By enable the universal repeater mode, the router will act as AP and client simultaneously.
SSID of Extended Interface	Set the SSID for the extended wireless interface.

Click <**Apply Changes**> at the bottom of the screen to save the above configurations. You can now configure other advance sections or start using the router (with the advance settings in place)

3.4.2.1 Multiple AP

This access point supports multiple APs function. With different SSID names, you can separate to four wireless networks with different wireless security, WMM, access control and etc.



Parameters	Default	Description
Enable		Check this box if you want to enable multiple access points.
Band		Please select the radio band from one of the following options. 2.4GHz(B): 2.4GHz band, only allows 802.11b wireless network client to connect this router (maximum transfer rate 11Mbps). 2.4 GHz (N): 2.4GHz band, only allows 802.11n wireless network client to connect this router (maximum transfer rate 150Mbps). 2.4 GHz (B+G):2.4GHz band, only allows 802.11b and 802.11g wireless network client to connect this router (maximum transfer rate 11Mbps for 802.11b clients, and maximum 54Mbps for 802.11g clients).

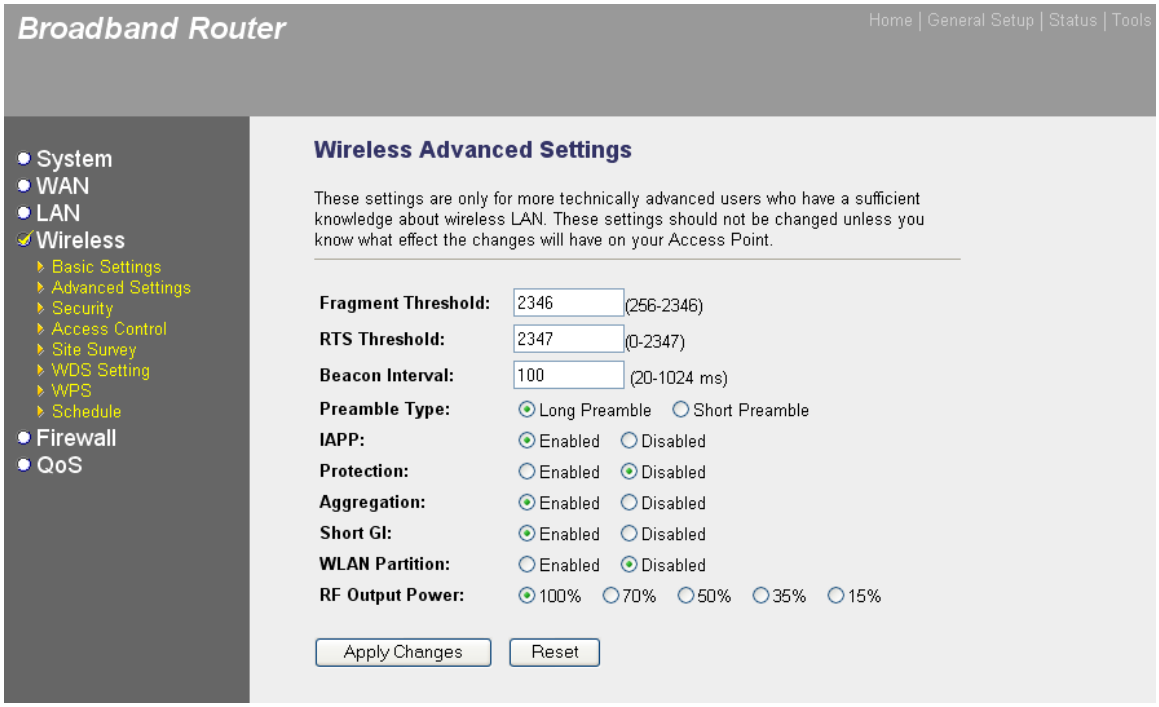
	2.4 GHz (G): 2.4GHz band, only allows 802.11g wireless network client to connect this router (maximum transfer rate 54Mbps). 2.4 GHz (B+G+N): 2.4GHz band, allows 802.11b, 802.11g, and 802.11n wireless network client to connect this router (maximum transfer rate 11Mbps for 802.11b clients, maximum 54Mbps for 802.11g clients, and maximum 150Mbps for 802.11n clients).
SSID	This is the name of wireless router. You can type any alphanumerical characters here, maximum 32 characters. SSID is used to identify your own wireless router from others when there are other wireless routers in the same area. Default SSID is 'default-VAP0/1/2/3', it's recommended to change default SSID value to the one which is meaningful to you, like myhome, office_room1, etc.
Data Rate	Set the wireless data transfer rate to a certain value. Since most of wireless devices will negotiate with each other and pick a proper data transfer rate automatically, it's not necessary to change this value unless you know what will happen after modification.
Broadcast SSID	Decide if the wireless router will broadcast its own SSID or not. You can hide the SSID of your wireless router (set the option to 'Disable'), so only people those who know the SSID of your wireless router can get connected.
WMM	The short of Wi-Fi MultiMedia, it will enhance the data transfer performance of multimedia contents when they're being transferred over wireless network. If you don't know what it is / not sure if you need it, it's safe to set this option to 'Enable'.
Access	If you want to limit stations connect to the specific access point with the right to access Internet only, please select 'WAN'. By default, it is not enabled the access control.

Active Client List	Click “Show” button, then an “Active Wireless Client Table” will pop up. You can see the status of all active wireless stations that are connecting to the access point.

Click <**Apply Changes**> at the bottom of the screen to save the above configurations. You can now configure other advance sections or start using the router (with the advance settings in place)

3.4.2 Advanced Settings

You can set advanced wireless LAN parameters of this router. The parameters include Authentication Type, Fragment Threshold, RTS Threshold, Beacon Interval, Preamble Type, etc. You should not change these parameters unless you know what effect the changes will have on this router.



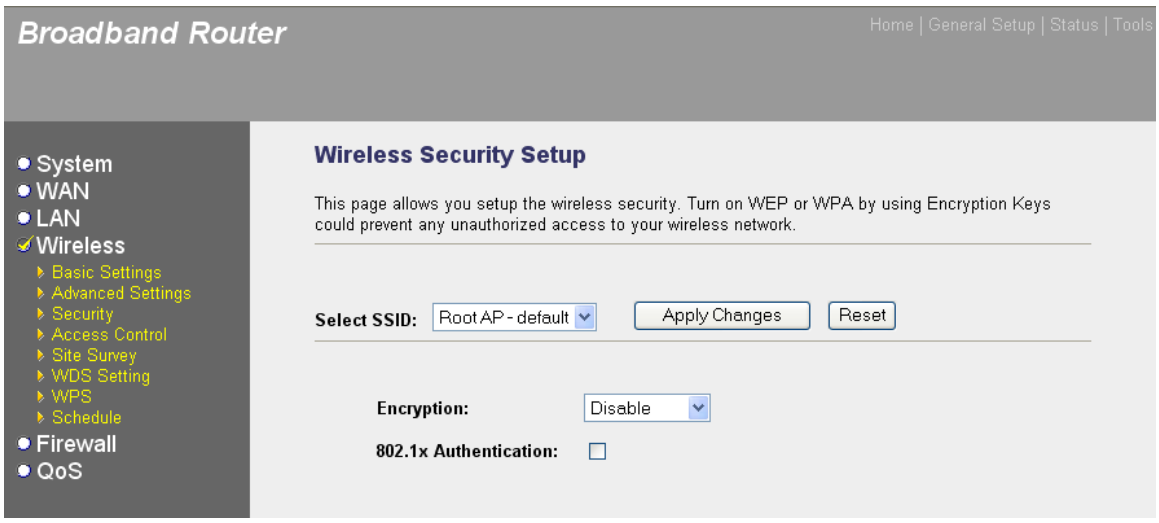
Parameters	Default	Description
Fragment Threshold		"Fragment Threshold" specifies the maximum size of packet during the fragmentation of data to be transmitted. If you set this value too low, it will result in bad performance.
RTS Threshold		When the packet size is smaller than the RTS threshold, the wireless router will not use the RTS/CTS mechanism to send this packet.
Beacon Interval		The interval of time that this wireless router broadcast a beacon. Beacon is used to synchronize the wireless network.
Preamble Type		The “Long Preamble” can provide better wireless LAN compatibility while the “Short Preamble” can provide better wireless LAN performance.
IAPP		If you enable “IAPP”, it will allow wireless station roaming between IAPP enabled access points within the same wireless LAN.
Protection		This is also called CTS Protection. It is recommended to enable the protection mechanism. This mechanism can decrease the rate of data collision between 802.11b and 802.11g/802.11n wireless stations. When the protection mode is enabled, the throughput of the AP will be a little lower due to many of frame traffic should be transmitted.
Aggregation		This function is used to join multiple data packets for transmission as a single unit to increase network efficiency.
Short GI		The 802.11n draft specifies two guard intervals: 400ns (short) and 800ns (long). Support of the 400ns GI is optional for transmit and receive. Enable this function will increase network efficiency.
WLAN Partition		Enable this function and all the wireless clients cannot access to each other.

RF Output Power	You can set the output power of wireless radio. Unless you're using this wireless router in a really big space, you may not have to set output power to 100%. **This will enhance security (malicious / unknown users in distance will not be able to reach your wireless router).**

Click <**Apply Changes**> at the bottom of the screen to save the above configurations. You can now configure other advance sections or start using the router.

3.4.3 Security

This Access Point provides complete wireless LAN security functions, include WEP, IEEE 802.11x, IEEE 802.11x with WEP, WPA with pre-shared key and WPA with RADIUS. With these security functions, you can prevent your wireless LAN from illegal access. Please make sure your wireless stations use the same security function.



Parameters	Default	Description
Select SSID		If you have configure multiple access points, please select the access point you want to configure.

Encryption	You can choose no encryption, WEP, WPA, WPA2 or WPA2 mixed mode for security.
Use 802.1x Authentication	IEEE 802.1x is an authentication protocol. Every user must use a valid account to login to this Access Point before accessing the wireless LAN. The authentication is processed by a RADIUS server. Check this box to authenticates user by IEEE 802.1x.

Click <**Apply Changes**> at the bottom of the screen to save the above configurations. You can now configure other advance sections or start using the router (with the advance settings in place)

3.4.3.1 WEP

When you select 64-bit or128-bit WEP key, you have to enter WEP keys to encrypt data. You can generate the key by yourself and enter it. You can enter four WEP keys and select one of them as default key. Then the router can receive any packets encrypted by one of the four keys.

Parameters	Description
Authentication	There are two authentication types: "Open System" and "Shared Key". When you select "Open System", wireless stations can associate with this wireless router without WEP encryption. When you select "Shared Key", you should also setup WEP key in the "Security" page and wireless stations should use WEP encryption in the authentication phase to associate with this wireless router. If you select "Auto", the wireless client can associate with this wireless router by using any one of these two authentication types.
Key Length	You can select the WEP key length for encryption, 64-bit or 128-bit. Larger WEP key length will provide higher level of security, but the throughput will be lower.
Key Format	You may select to select ASCII Characters (alphanumeric format) or Hexadecimal Digits (in the "A-F", "a-f" and "0-9" range) to be the WEP Key. For example: ASCII Characters: guest Hexadecimal Digits: 12345abcde
Encryption Key	The WEP key are used to encrypt data transmitted in the wireless network. Fill the text box by following the rules below. 64-bit WEP: input 10-digit Hex values (in the "A-F", "a-f" and "0-9" range) or 5-digit ASCII character as the encryption keys. 128-bit WEP: input 26-digit Hex values (in the "A-F", "a-f" and "0-9" range) or 13-digit ASCII characters as the encryption keys.

Click <**Apply Changes**> at the bottom of the screen to save the above configurations. You can now configure other advance sections or start using the router (with the advance settings in place)

3.4.3.2 WPA

Wi-Fi Protected Access (WPA) is an advanced security standard. You can use a pre-shared key to authenticate wireless stations and encrypt data during communication. It uses TKIP to change the encryption key frequently. So the encryption key is not easy to be broken by hackers. This can improve security very much.

Parameters	Description
WPA Authentication Mode	WPA can authenticate by Enterprise (RADIUS) or by Personal (Pre-Shared key). If you enable 'Enterprise (RADIUS)', please go to section 3.4.3.5 for more information.
WPA/WPA2 Cipher Suite	You can choose TKIP or AES for WPA/WPA2 key method.
Pre-shared Key Format	You may select to select Passphrase (alphanumeric format) or Hexadecimal Digits (in the "A-F", "a-f" and "0-9" range) to be the Pre-shared Key. For example: Passphrase: iamguest Hexadecimal Digits: 12345abcde
Pre-shared Key	The Pre-shared key is used to authenticate and encrypt data transmitted in the wireless network. Fill the text box by following the rules below.

	Hex: input 64-digit Hex values (in the “A-F”, “a-f” and “0-9” range) or at least 8 character pass phrase as the pre-shared keys.

Click <**Apply Changes**> at the bottom of the screen to save the above configurations. You can now configure other advance sections or start using the router (with the advance settings in place)

3.4.3.3 WPA2(AES)

Wi-Fi Protected Access 2(WPA2) is an advanced security standard. You can use a pre-shared key to authenticate wireless stations and encrypt data during communication. It uses CCMP(AES) to change the encryption key frequently. So the encryption key is not easy to be broken by hackers. This can improve security very much.

Parameters	Description
WPA Authentication Mode	WPA can authenticate by Enterprise (RADIUS) or by Personal (Pre-Shared key). If you enable ‘Enterprise (RADIUS)’, please go to section 3.4.3.5 for more information.
WPA/WPA2 Cipher Suite	You can choose TKIP or AES for WPA/WPA2 key method.

Pre-shared Key Format	You may select to select Passphrase (alphanumeric format) or Hexadecimal Digits (in the “A-F”, “a-f” and “0-9” range) to be the Pre-shared Key. For example: Passphrase: iamguest Hexadecimal Digits: 12345abcde
Pre-shared Key	The Pre-shared key is used to authenticate and encrypt data transmitted in the wireless network. Fill the text box by following the rules below. Hex: input 64-digit Hex values (in the “A-F”, “a-f” and “0-9” range) or at least 8 character pass phrase as the pre-shared keys.

Click <**Apply Changes**> at the bottom of the screen to save the above configurations. You can now configure other advance sections or start using the router (with the advance settings in place)

3.4.3.4 WPA2Mixed

Wi-Fi Protected Access 2(WPA2) is an advanced security standard. You can use a pre-shared key to authenticate wireless stations and encrypt data during communication. It uses TKIP or CCMP(AES) to change the encryption key frequently. So the encryption key is not easy to be broken by hackers. This can improve security very much.

Parameters	Description
WPA Authentication Mode	WPA can authenticate by Enterprise (RADIUS) or by Personal (Pre-Shared key). If you enable 'Enterprise (RADIUS)', please go to section 3.4.3.5 for more information.
WPA Cipher Suite	You can choose TKIP or AES for WPA key method.
WPA2 Cipher Suite	You can choose TKIP or AES for WPA2 key method.
Pre-shared Key Format	You may select to select Passphrase (alphanumeric format) or Hexadecimal Digits (in the "A-F", "a-f" and "0-9" range) to be the Pre-shared Key. For example: Passphrase: iamguest Hexadecimal Digits: 12345abcde
Pre-shared Key	The Pre-shared key is used to authenticate and encrypt data transmitted in the wireless network. Fill the text box by following the rules below. Hex: input 64-digit Hex values (in the "A-F", "a-f" and "0-9" range) or at least 8 character pass phrase as the pre-shared keys.

Click <**Apply Changes**> at the bottom of the screen to save the above configurations. You can now configure other advance sections or start using the router (with the advance settings in place)

3.4.3.5 RADIUS Server

IEEE 802.1x is an authentication protocol. Every user must use a valid account to login to this wireless router before accessing the wireless LAN. The authentication is processed by a RADIUS server. This mode only authenticates user by IEEE 802.1x, but it does not encryption the data during communication. If there is a RADIUS server in you environment, please enable this function. Check this box and another sub-menu will appear.

Parameters	Description
Radius Server IP Address	The IP address of external RADIUS server.
Radius Server Port	The service port of the external RADIUS server.
Radius Server Password	The password used by external RADIUS server.

Click <**Apply Changes**> at the bottom of the screen to save the above configurations. You can now configure other advance sections or start using the router (with the advance settings in place)

3.4.4 Access Control

This function will help you to prevent unauthorized users from connecting to your wireless router; only those wireless devices who have the MAC address you assigned here can gain access to your wireless router. You can use this function with other security measures described in previous section, to create a safer wireless environment.

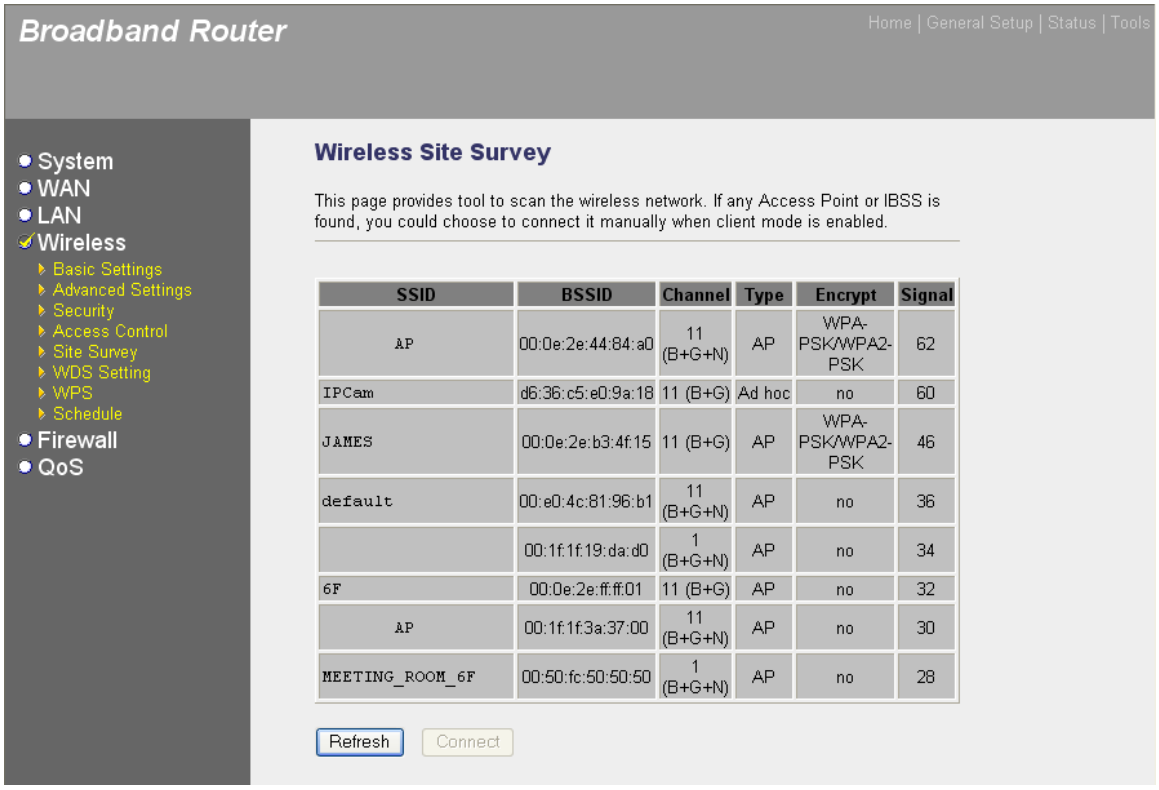
Parameters	Description
Wireless Access Control Mode	Enable/Disable wireless access control. You can choose 'Allow Listed' if you allow the MAC Addresses listed in the following table to connect to the router; choose 'Deny Listed' if you deny the MAC Addressed listed in the following table to connect to the router.
MAC Address	Input the MAC address of your wireless devices here, dash (-) or colon (:) are not required. (i.e. If the MAC address label of your wireless device indicates 'aa-bb-cc-dd-ee-ff' or aa:bb:cc:dd:ee:ff', just input 'aabbccddeeff'.

Comment	You can input any text here as the comment of this MAC address, like ‘ROOM 2A Computer’ or anything.
Current Access Control List	From the table, you can check the access control settings.
Delete Selected	If you want to delete a specific MAC address entry, check the ‘select’ box of the MAC address you want to delete, then click ‘Delete Selected’ button. (You can select more than one MAC addresses).
Delete All	If you want to delete all MAC addresses listed here, please click ‘Delete All’ button.
Reset	You can also click ‘Reset’ button to unselect all.

Click <**Apply Changes**> at the bottom of the screen to save the above configurations. You can now configure other advance sections or start using the router (with the advance settings in place)

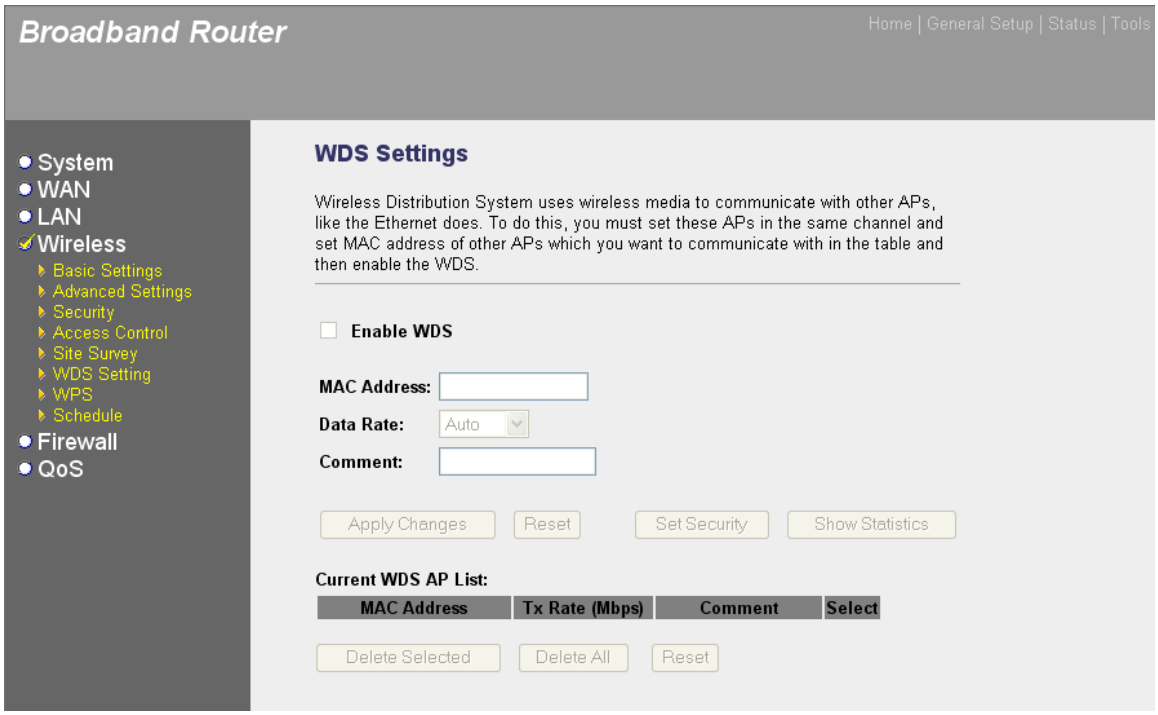
3.4.5 Site Survey

This page provides tool to scan the wireless network. If any Access Point or IBSS is found, you could choose to connect it manually when client mode is enabled.



3.4.6 WDS Settings

In this mode, you can expand the scope of network by combining up to other access points together, and every access point can still accept wireless clients.



Parameters	Description
Enable WDS	Check this box to enable Wireless Distribution System.
MAC Address	Input the MAC address of other wireless routers.
Data Rate	Designate the transmit data rate for the routers in the WDS network.
Comment	You can input any text here as the comment of this MAC address, like 'ROOM 2A AP' or anything.
Set Security	Click this button to configure the security used in the WDS network.

Show Statistics	Click this button and a table will pop up. This table shows the MAC Address, transmission, reception packet counters and state information for each configured WDS AP.
Current WDS AP List	From the table, you can check the settings for each WDS AP.
Delete Selected	If you want to delete a specific WDS AP, check the 'select' box of the WDS AP you want to delete, then click 'Delete Selected' button. (You can select more than one WDS AP).
Delete All	If you want to delete all WDS APs listed here, please click 'Delete All' button.
Reset	You can also click 'Reset' button to unselect all.

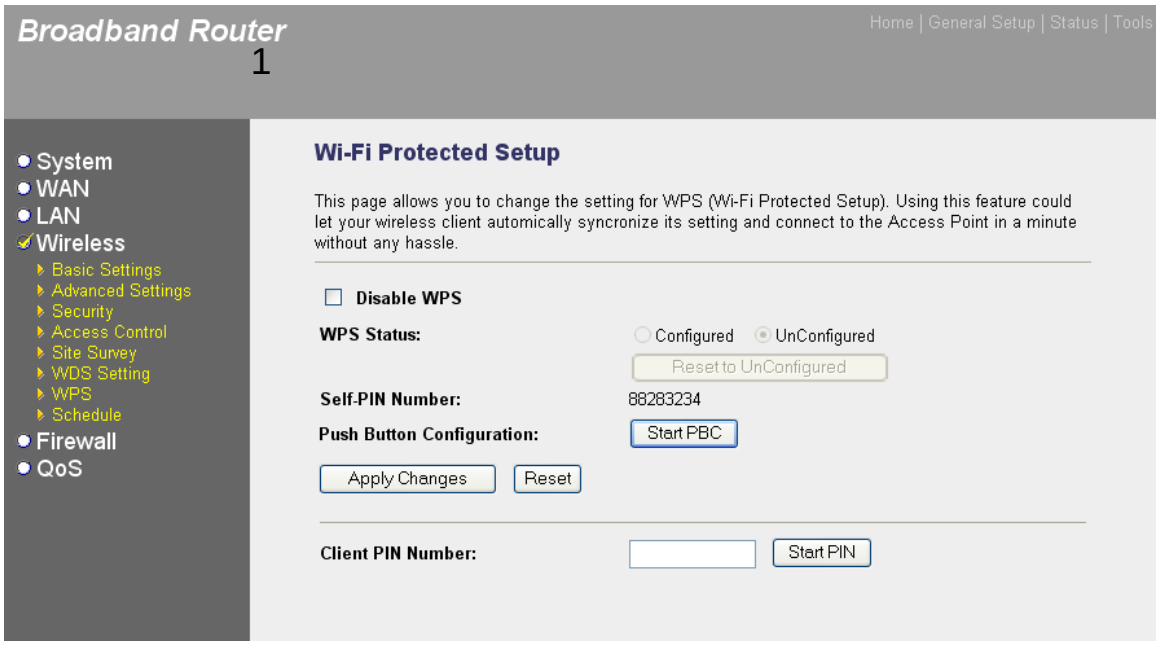
Click <**Apply Changes**> at the bottom of the screen to save the above configurations. You can now configure other advance sections or start using the router (with the advance settings in place)

3.4.7 WPS

Wi-Fi Protected Setup (WPS) is the simplest way to build connection between wireless network clients and this wireless router. You don't have to select encryption mode and input a long encryption passphrase every time when you need to setup a wireless client, you only have to press a button on wireless client and this wireless router, and the WPS will do the rest for you.

This wireless router supports two types of WPS: Push-Button Configuration (PBC), and PIN code. If you want to use PBC, you have to push a specific button on the wireless client to start WPS mode, and switch this wireless router to WPS mode too. You can push Reset/WPS button of this wireless router, or click 'Start PBC' button in the web configuration interface to do this; if you want to use PIN code, you have to know the PIN code of wireless client and switch it to WPS mode, then provide the PIN code of the wireless client you wish to connect to this wireless router. The detailed instructions are listed follow:

Please click 'Wireless' menu on the left of web management interface, then click 'WPS', and the following message will be displayed on your web browser:



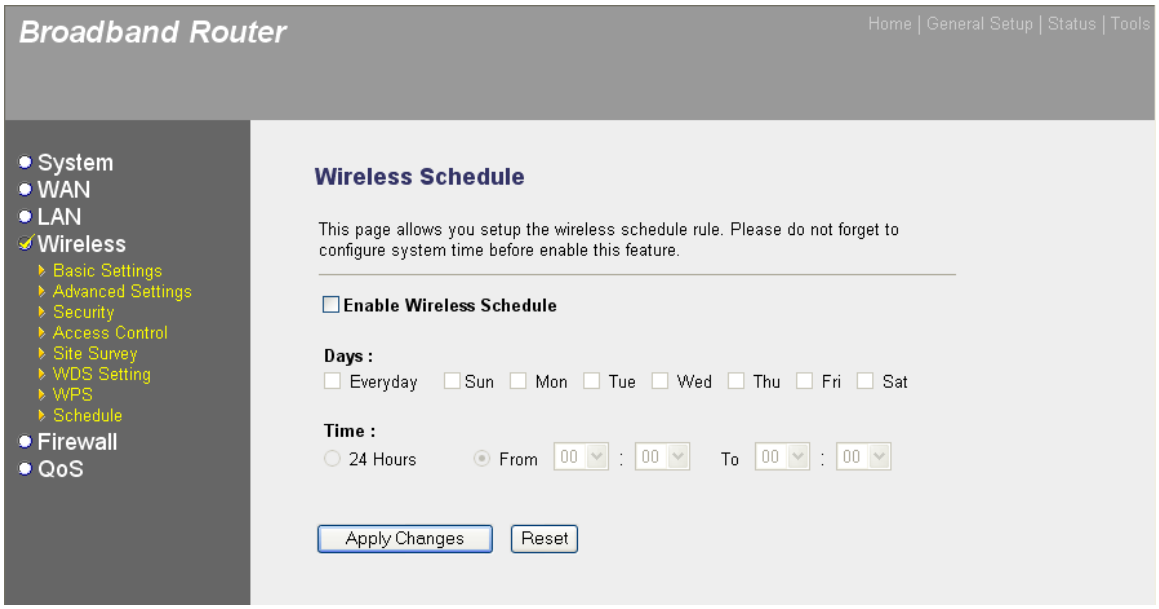
Parameters	Description
Enable WPS	Check this box to enable WPS function.
WPS Status	If the wireless security (encryption) function of this wireless router is properly set, you'll see 'Configured' message here. If wireless security function has not been set, you'll see 'unConfigured'.
Reset to UnConfigured	Reset the WPS status to unconfigured, please click this button.
Self-PIN Number	This is the WPS PIN code of this wireless router. This code is useful when you need to build wireless connection by WPS with other WPS-enabled wireless devices.
Push Button Configuration	Click 'Start PBC' to start Push-Button style WPS setup procedure. This wireless router will wait for WPS requests from wireless clients for 2 minutes. The 'WLAN' LED on the wireless router will be steady on for 2 minutes when this wireless router is waiting for incoming WPS request.

Client PIN Number	Please input the PIN code of the wireless client you wish to connect, and click 'Start PIN' button. The 'WLAN' LED on the wireless router will be steady on when this wireless router is waiting for incoming WPS request.

Click <**Apply Changes**> at the bottom of the screen to save the above configurations. You can now configure other advance sections or start using the router (with the advance settings in place)

3.4.8 Schedule

This page allows you to set up the wireless schedule rule. You can designate to enable wireless access point by time or day.



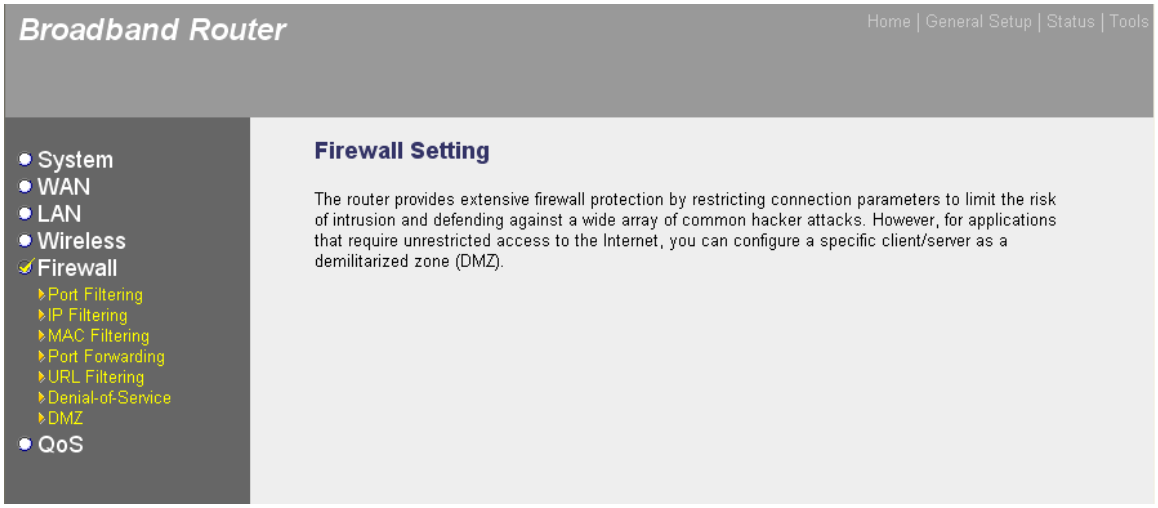
Parameters	Description
Enable Wireless Schedule	Check this box to enable wireless schedule.
Days	Select to enable the wireless access point every day or some other weekdays.

Time	Designate a period of hours in a day to enable the wireless access point.

Click <**Apply Changes**> at the bottom of the screen to save the above configurations. You can now configure other advance sections or start using the router (with the advance settings in place)

3.5 Firewall

The Broadband router provides extensive firewall protection by restricting connection parameters, thus limiting the risk of hacker attack, and defending against a wide array of common Internet attacks. However, for applications that require unrestricted access to the Internet, you can configure a specific client/server as a Demilitarized Zone (DMZ).



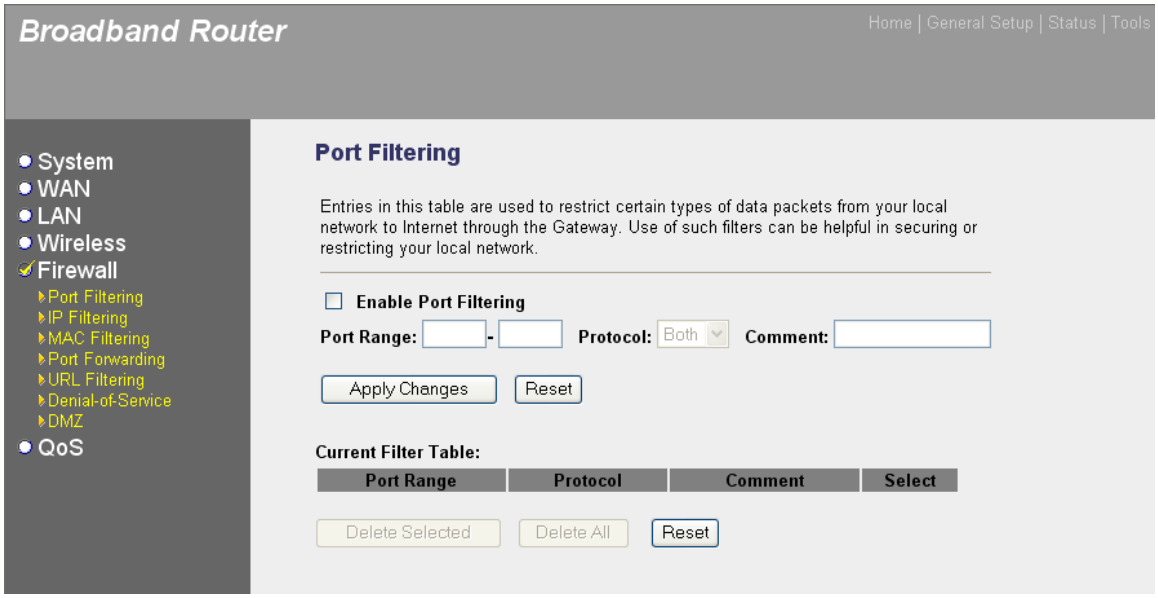
Parameters	Description
3.5.1 Port Filtering	Entries in this table are used to restrict certain types of data packets from your local network to Internet through the Gateway.
3.5.2 IP Filtering	IP Filtering allows you to specify which IP can or can not be used to access to internet.
3.5.3 MAC Filtering	MAC Filtering allows you to specify which MAC Address can or can not be used to access to internet.

3.5.4 Port Forwarding	You can have different services (e.g. email, FTP, Web etc.) going to different service servers/clients in your LAN. The Port Forwarding allows you to re-direct a particular range of service port numbers (from the Internet/WAN Ports) to a particular LAN IP address.
3.5.5 URL Filtering	You can enable this function to block specific web sites.
3.5.6 Denial-of-Service	Denial of Service (DoS) is a common attack measure, by transmitting a great amount of data or request to your Internet IP address and server, the Internet connection will become very slow, and server may stop responding because it is not capable to handle too much traffics.
3.5.7 DMZ	The DMZ function allows you to re-direct all packets going to your WAN port IP address to a particular IP address in your LAN.
3.5.8 Static Routing	You can enable Static Routing to turn off NAT function of your router and let the router forward packets by your routing policy.
3.5.9 Virtual Server	This function allows you to redirect a port on Internet IP address (on WAN port) to a specified port of an IP address on local network, so you can setup an Internet service on the computer on local network, without exposing it on Internet directly. You can also build many sets of port redirection, to provide many different Internet services on different local computers via a single Internet IP address.

Click on one of the firewall selections and proceed to the manual's relevant sub-section

3.5.1 Port Filtering

If you want to restrict users from accessing certain Internet applications/services (e.g. Internet websites, email, FTP etc.), then this is the place to set that configuration. Entries in this table are used to restrict certain types of data packets from your local network to Internet through the Gateway. Use of such filters can be helpful in securing or restricting your local network.



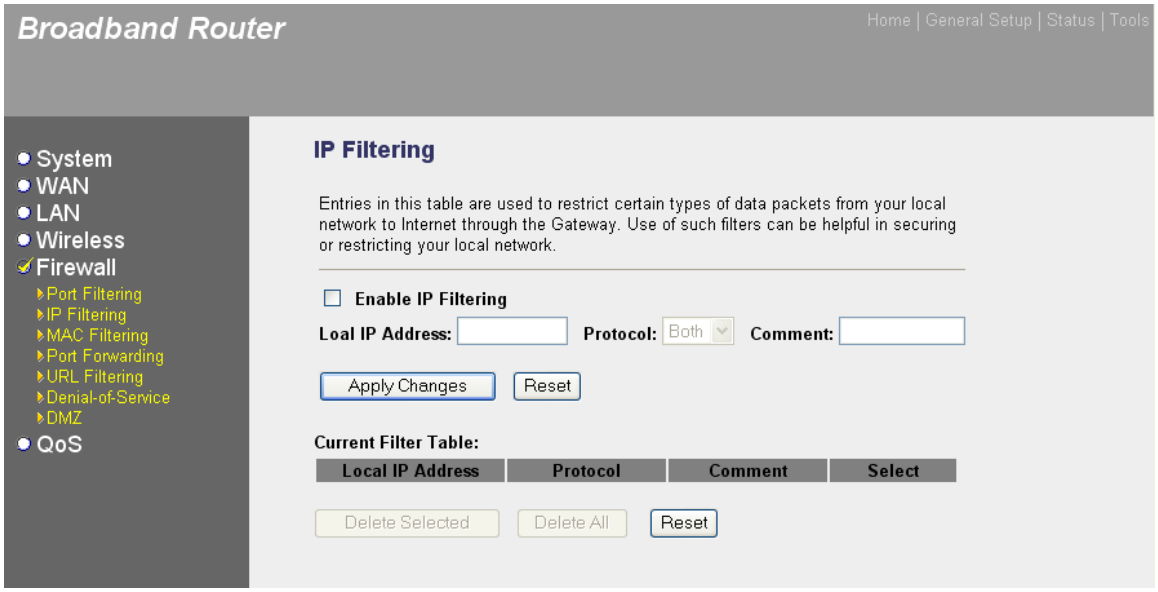
Parameters	Description
Enable Port Filtering	Check this box to enable the port filtering function.
Port Range	The range of ports to be forward to the private IP.
Protocol	Choose ‘TCP’ or ‘UDP’ or ‘Both’ protocols for port filtering.
Comment	You can input any text here as the comment of this settings.
Current Filter Table	From the table, you can check each port filter setting.
Delete Selected	If you want to delete a specific setting, check the ‘select’ box of the setting you want to delete, then click ‘Delete Selected’ button. (You can select more than one setting).

Delete All	If you want to delete all settings listed here, please click 'Delete All' button.
Reset	You can also click 'Reset' button to unselect all.

Click <**Apply Changes**> at the bottom of the screen to save the above configurations. You can now configure other advance sections or start using the router (with the advance settings in place)

3.5.2 IP Filtering

If you want to restrict users from accessing certain Internet applications/services (e.g. Internet websites, email, FTP etc.), then this is the place to set that configuration. Entries in this table are used to restrict certain types of data packets from your local network to Internet through the Gateway. Use of such filters can be helpful in securing or restricting your local network.



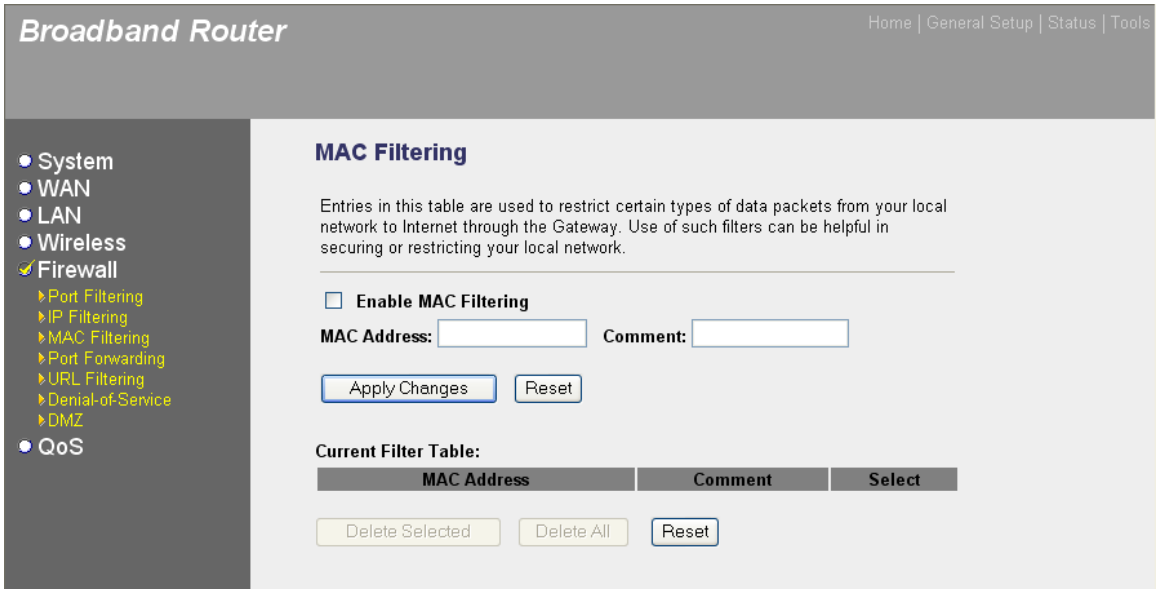
Parameters	Description
Enable IP Filtering	Check this box to enable the IP filtering function.
Local IP Address	Input the IP Address you want to filter.
Protocol	Choose 'TCP' or 'UDP' or 'Both' protocols for port filtering.

Comment	You can input any text here as the comment of this settings.
Current Filter Table	From the table, you can check each IP filter setting.
Delete Selected	If you want to delete a specific setting, check the 'select' box of the setting you want to delete, then click 'Delete Selected' button. (You can select more than one setting).
Delete All	If you want to delete all settings listed here, please click 'Delete All' button.
Reset	You can also click 'Reset' button to unselect all.

Click <**Apply Changes**> at the bottom of the screen to save the above configurations. You can now configure other advance sections or start using the router (with the advance settings in place)

3.5.3 MAC Filtering

If you want to restrict users from accessing certain Internet applications/services (e.g. Internet websites, email, FTP etc.), then this is the place to set that configuration. Entries in this table are used to restrict certain types of data packets from your local network to Internet through the Gateway. Use of such filters can be helpful in securing or restricting your local network.

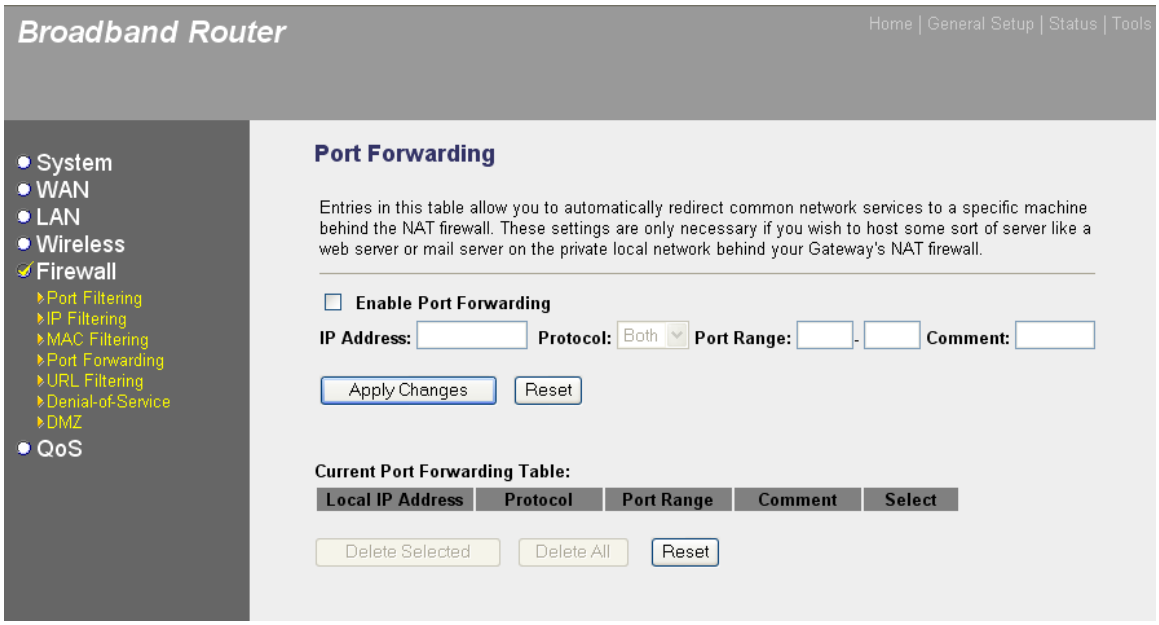


Parameters	Description
Enable MAC Filtering	Check this box to enable the MAC filtering function.
MAC Address	Input the MAC address of the devices you want to filter, dash (-) or colon (:) are not required. (i.e. If the MAC address label of your wireless device indicates 'aa-bb-cc-dd-ee-ff' or aa:bb:cc:dd:ee:ff', just input 'aabbccddeeff'.
Comment	You can input any text here as the comment of this MAC address, like 'ROOM 2A Computer' or anything.
Current Filter Table	From the table, you can check each MAC Address filter setting.
Delete Selected	If you want to delete a specific MAC address entry, check the 'select' box of the MAC address you want to delete, then click 'Delete Selected' button. (You can select more than one MAC addresses).
Delete All	If you want to delete all MAC addresses listed here, please click 'Delete All' button.
Reset	You can also click 'Reset' button to unselect all.

Click <**Apply Changes**> at the bottom of the screen to save the above configurations. You can now configure other advance sections or start using the router (with the advance settings in place)

3.5.4 Port Forwarding

The Port Forwarding allows you to re-direct a particular range of service port numbers (from the Internet/WAN Ports) to a particular LAN IP address. It helps you to host some servers behind the router NAT firewall.



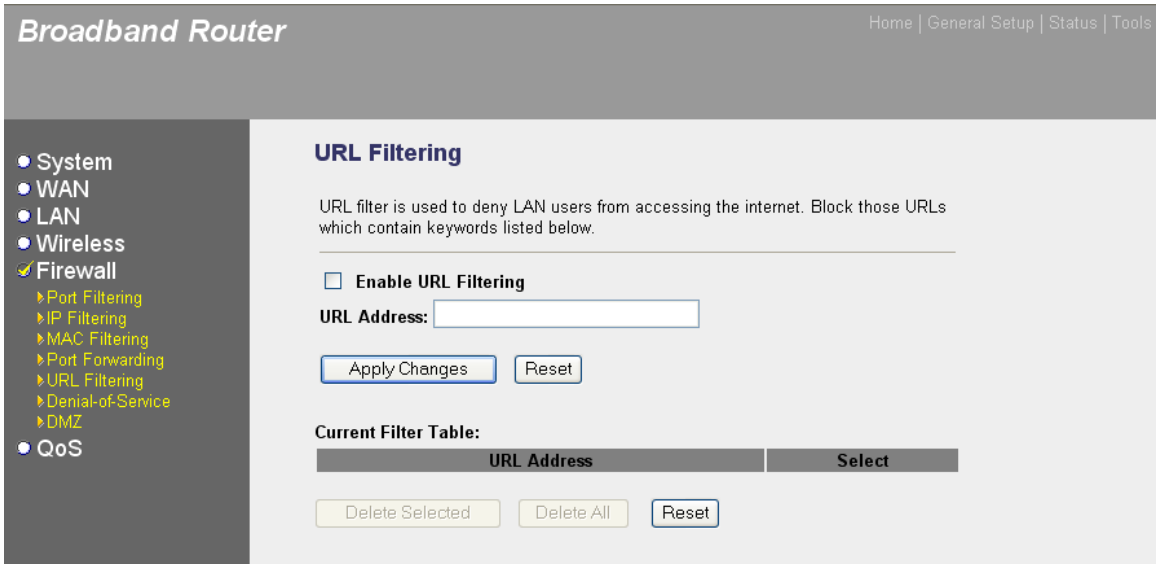
Parameter	Description
Enable Port Forwarding	Enable Port Forwarding
IP Address	This is the private IP of the server behind the NAT firewall. Note: You need to give your LAN PC clients a fixed/static IP address for Port Forwarding to work properly.
Protocol	This is the protocol type to be forwarded. You can choose to forward “TCP” or “UDP” packets only or select “both” to forward both “TCP” and “UDP” packets.
Port Range	The range of ports to be forward to the private IP.
Comment	The description of this setting.

Current Port Forwarding Table	From the table, you can check each Port forwarding setting.
Delete Selected	If you want to delete a setting, check the 'select' box of the setting you want to delete, then click 'Delete Selected' button. (You can select more than one setting).
Delete All	If you want to delete all settings listed here, please click 'Delete All' button.
Reset	You can also click 'Reset' button to unselect all.

Click <**Apply Changes**> at the bottom of the screen to save the above configurations. You can now configure other advance sections or start using the router (with the advance settings in place)

3.5.5 URL Filtering

You can block access to some Web sites from particular PCs by entering a full URL address or just keyword of the Web site.



Parameter	Description
Enable URL Filtering	Enable/disable URL Blocking.

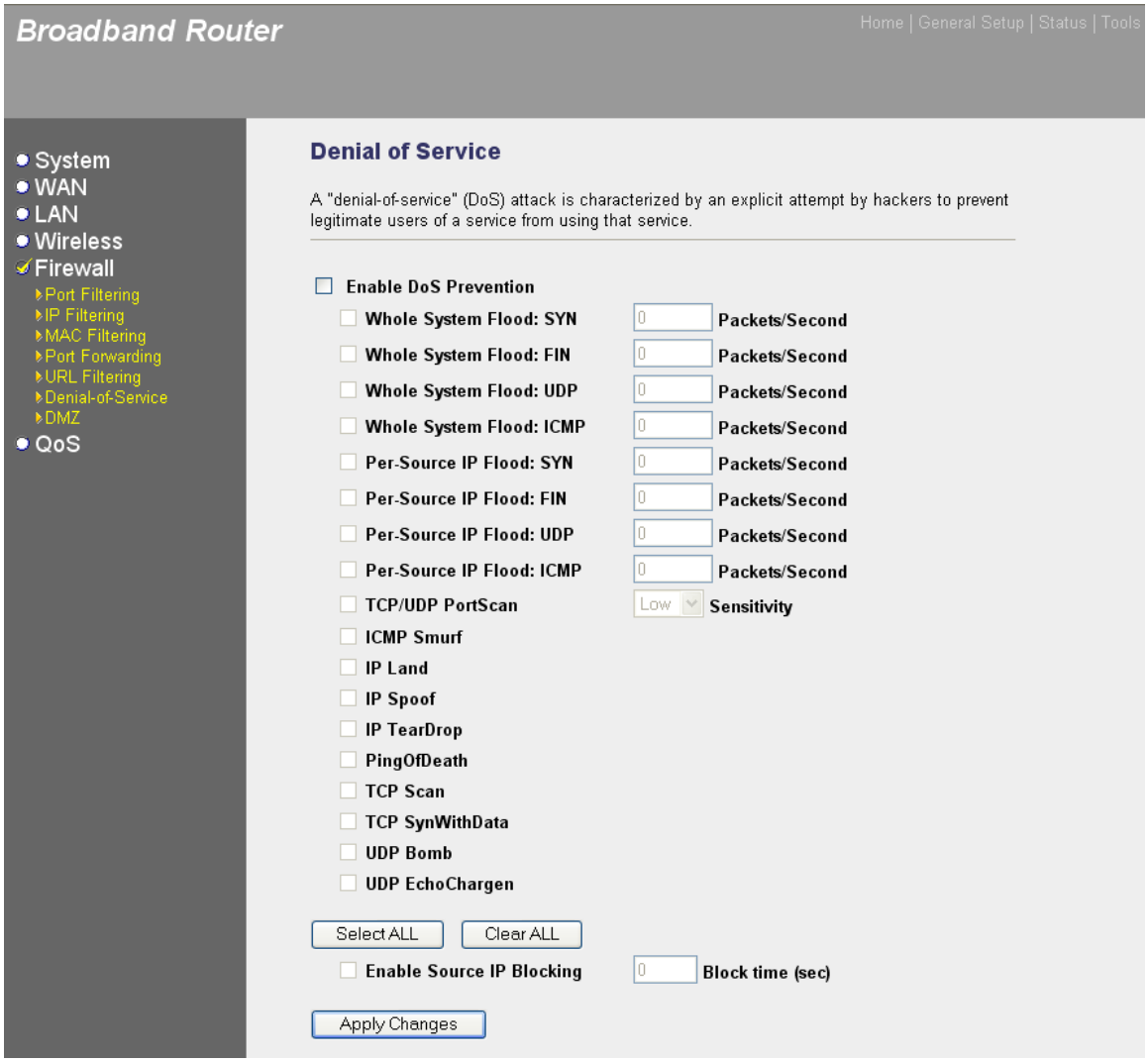
URL Address	You can enter the full URL address or the keyword of the web site you want to block.
Current Filter Table	From the table, you can check each URL filter setting.
Delete Selected	If you want to delete a setting, check the 'select' box of the setting you want to delete, then click 'Delete Selected' button. (You can select more than one setting).
Delete All	If you want to delete all settings listed here, please click 'Delete All' button.
Reset	You can also click 'Reset' button to unselect all.

Click <**Apply Changes**> at the bottom of the screen to save the above configurations. You can now configure other advance sections or start using the router (with the advance settings in place)

3.5.6 Denial-of-Service

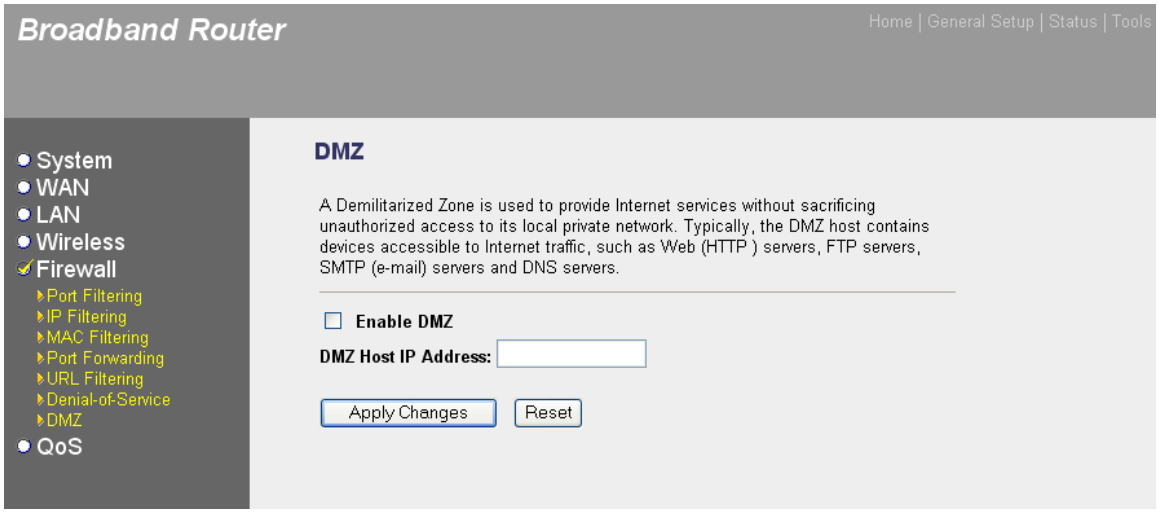
Denial of Service (DoS) is a common attack measure, by transmitting a great amount of data or request to your Internet IP address and server, the Internet connection will become very slow, and server may stop responding because it is not capable to handle too much traffics.

This router has a built-in DoS attack prevention mechanism; when you activate it, the router will stop the DoS attack for you.


Broadband Router
Home | General Setup | Status | Tools
System
WAN
LAN
Wireless
Firewall
Port Filtering
IP Filtering
MAC Filtering
Port Forwarding
URL Filtering
Denial-of-Service
DMZ
QoS
Denial of Service
A "denial-of-service" (DoS) attack is characterized by an explicit attempt by hackers to prevent legitimate users of a service from using that service.
Enable DoS Prevention
Whole System Flood: SYN 0 Packets/Second
Whole System Flood: FIN 0 Packets/Second
Whole System Flood: UDP 0 Packets/Second
Whole System Flood: ICMP 0 Packets/Second
Per-Source IP Flood: SYN 0 Packets/Second
Per-Source IP Flood: FIN 0 Packets/Second
Per-Source IP Flood: UDP 0 Packets/Second
Per-Source IP Flood: ICMP 0 Packets/Second
TCP/UDP PortScan Low Sensitivity
ICMP Smurf
IP Land
IP Spoof
IP TearDrop
PingOfDeath
TCP Scan
TCP SynWithData
UDP Bomb
UDP EchoChargen
Select ALL
Clear ALL
Enable Source IP Blocking 0 Block time (sec)
Apply Changes

3.5.7 DMZ

If you have a local client PC that cannot run an Internet application (e.g. Games) properly from behind the NAT firewall, then you can open the client up to unrestricted two-way Internet access by defining a DMZ Host. The DMZ function allows you to re-direct all packets going to your WAN port IP address to a particular IP address in your LAN.

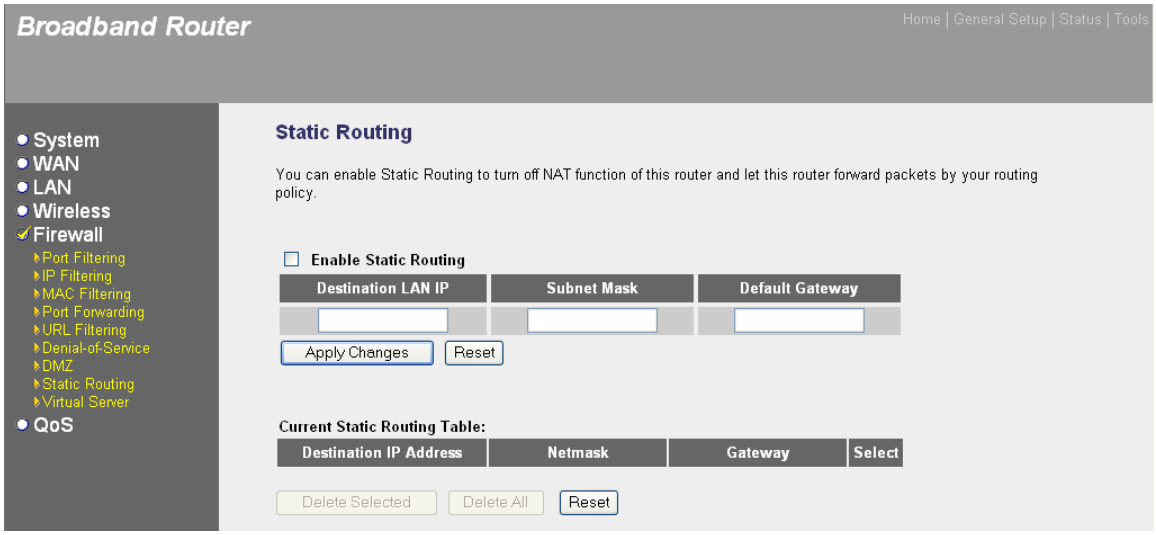


Parameters	Description
Enable DMZ	Enable/disable DMZ.
DMZ Host IP Address	Input the IP address of a particular host in your LAN that will receive all the packets originally going to the WAN port/Public IP address above **Note:** You need to give your LAN PC clients a fixed/static IP address for DMZ to work properly.

Click <**Apply Changes**> at the bottom of the screen to save the above configurations. You can now configure other advance sections or start using the router (with the advance settings in place)

3.5.8 Static Routing

You can enable Static Routing to turn off NAT function of your router and let the router forward packets by your routing policy.

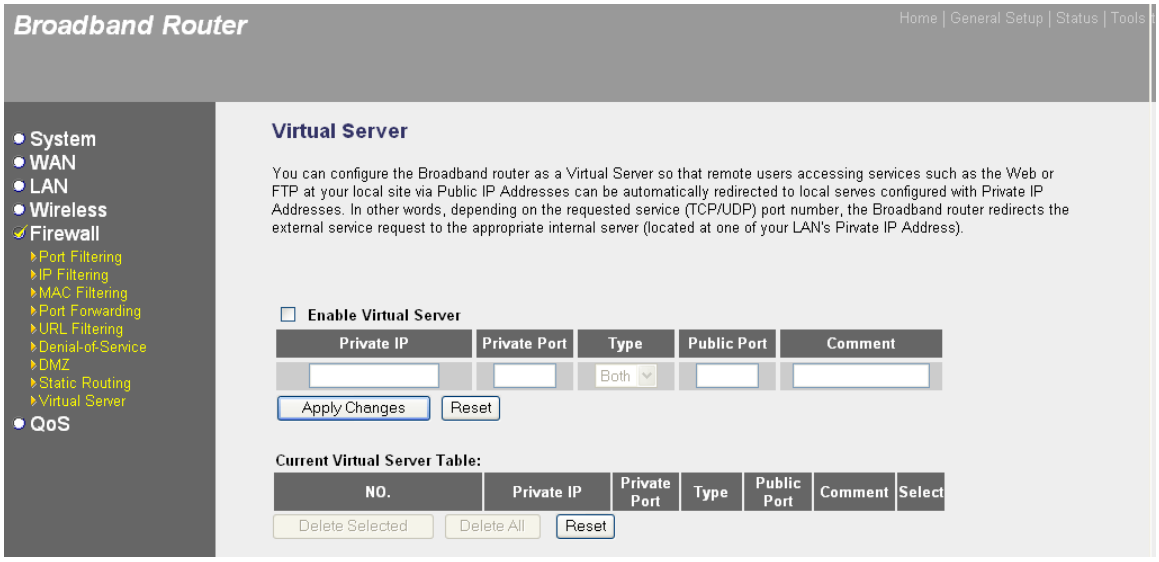


Parameter	Description
Enable Static Routing	Enter the IP Address of the destination LAN.
Destination LAN IP	Enter the Subnet Mask of the destination LAN.
Default Gateway	This is the gateway IP Address where packets are sent. Input the gateway IP Address.
Current Static Routing Table	From the table, you can check each Static Routing setting.
Delete Selected	If you want to delete a setting, check the 'select' box of the setting you want to delete, then click 'Delete Selected' button. (You can select more than one setting).
Delete All	If you want to delete all settings listed here, please click 'Delete All' button.
Reset	You can also click 'Reset' button to unselect all.

Click <**Apply Changes**> at the bottom of the screen to save the above configurations. You can now configure other advance sections or start using the router (with the advance settings in place)

3.5.9 Virtual Server

This function allows you to redirect a port on Internet IP address (on WAN port) to a specified port of an IP address on local network, so you can setup an Internet service on the computer on local network, without exposing it on Internet directly. You can also build many sets of port redirection, to provide many different Internet services on different local computers via a single Internet IP address.



Parameter	Description
Enable Virtual Server	Check this box to enable virtual server, and uncheck this box to disable virtual server.
Private IP	Input the IP address of the computer which provides Internet service.
Private Port	Input the port number of the IP address which provides Internet service.

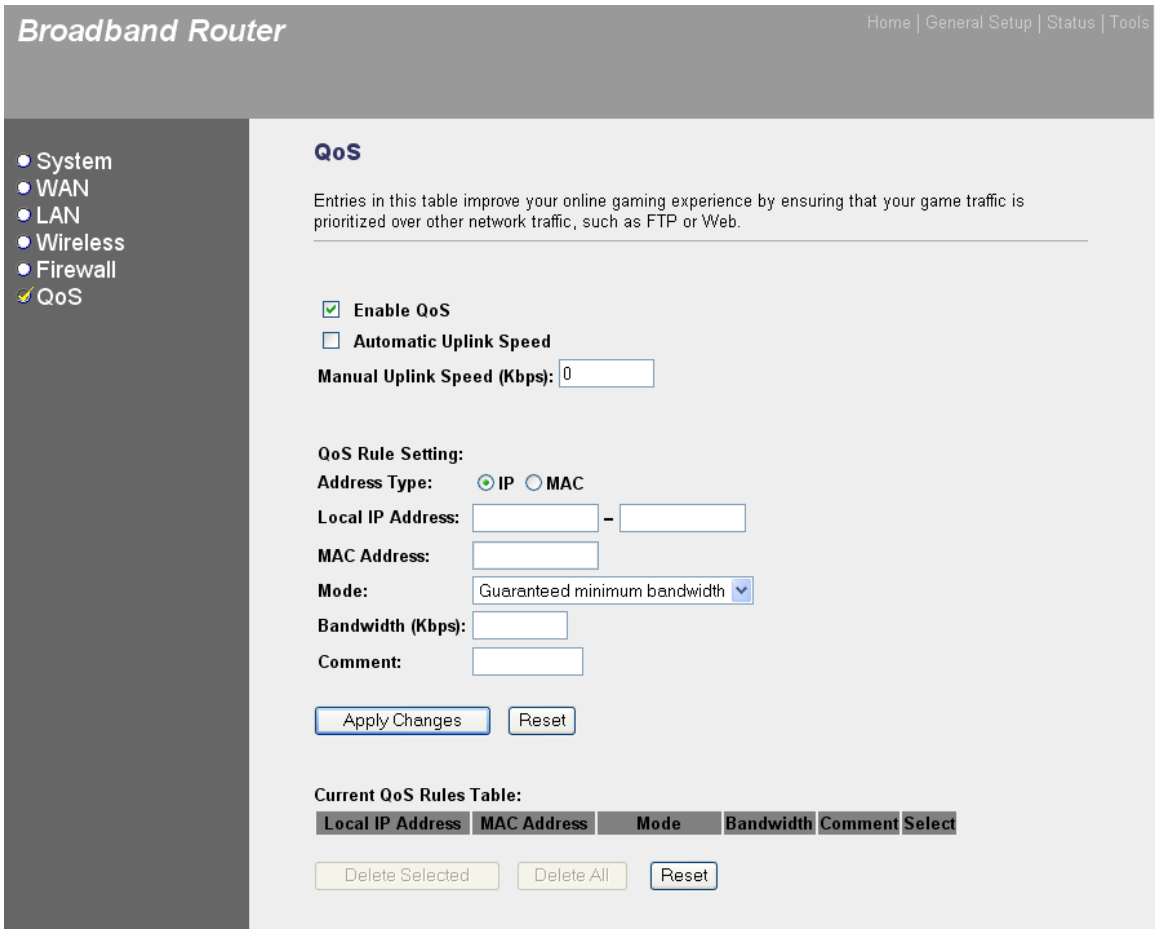
Type	Select the type of connection, TCP or UDP. If you're not sure, please select 'Both'.
Public Port	Please select the port number of Internet IP address which will be redirected to the port number of local IP address defined above.
Comment	Please input any text to describe this mapping.
Current Virtual Server Table	From the table, you can check each virtual server setting.
Delete Selected	If you want to delete a setting, check the 'select' box of the setting you want to delete, then click 'Delete Selected' button. (You can select more than one setting).
Delete All	If you want to delete all settings listed here, please click 'Delete All' button.
Reset	You can also click 'Reset' button to unselect all.

Click <**Apply Changes**> at the bottom of the screen to save the above configurations. You can now configure other advance sections or start using the router (with the advance settings in place)

3.6 QoS

Quality of service provides an efficient way for computers on the network to share the internet bandwidth with a promised quality of internet service. Without QoS, all computers and devices on the network will compete with each other to get internet bandwidth, and some applications which require guaranteed bandwidth (like video streaming and network telephone) will be affected, therefore an unpleasing result will occur, like the interruption of video / audio transfer.

With this function, you can limit the maximum bandwidth or give a guaranteed bandwidth for a specific computer, to avoid said unpleasing result from happening.



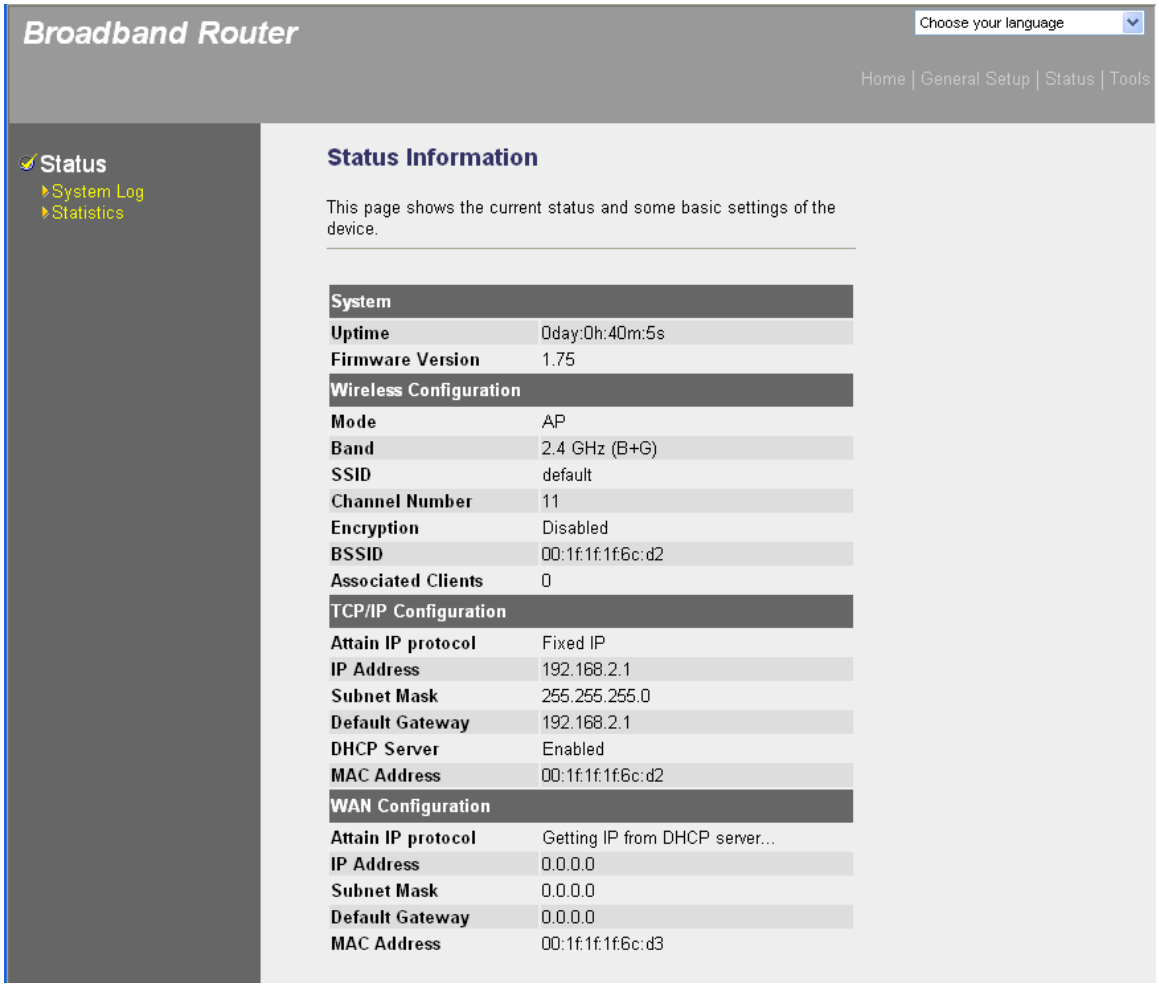
Parameter	Description
Enable QoS	Check this box to enable QoS, and uncheck this box to disable QoS.

Automatic Uplink Speed	Check this box to enable automatic uplink speed.
Manual Uplink Speed (Kbps)	You can set the limit of uplink speed in kbits. To disable uplink bandwidth limitation, input '0' here.
Local IP Address	Input the IP Address of your computer for configure the QoS rule.
Mode	Select to guarantee a minimum or maximum bandwidth to the IP Address you designate.
Bandwidth (Kbps)	Input the bandwidth in kbits.
Comment	Please input any text to describe this QoS rule.
Current QoS Rules Table	From the table, you can check each QoS rule setting.
Delete Selected	If you want to delete a setting, check the 'select' box of the setting you want to delete, then click 'Delete Selected' button. (You can select more than one setting).
Delete All	If you want to delete all settings listed here, please click 'Delete All' button.
Reset	You can also click 'Reset' button to unselect all.

Click <**Apply Changes**> at the bottom of the screen to save the above configurations. You can now configure other advance sections or start using the router (with the advance settings in place)

Chapter 4 Status

The Status section allows you to monitor the current status of your router. You can use the Status page to monitor: the connection status of the Broadband router's WAN/LAN interfaces, the current firmware version numbers, and any illegal attempts to access your network.

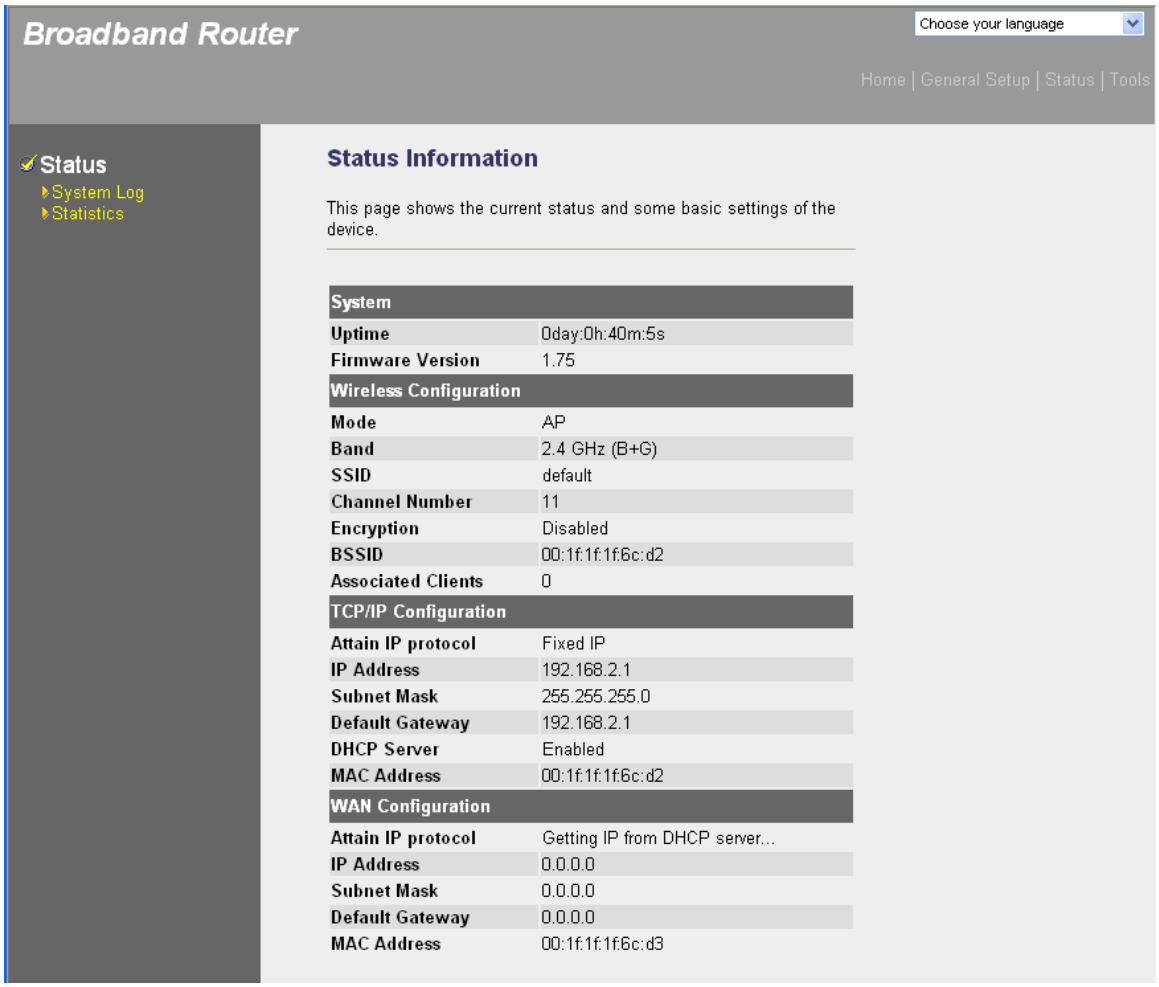


Parameters	Description
5.1 Status	Shows the router's system information.
5.2 System Log	View the Broadband router's system log.
5.3 Statistics	Shows the statistics.

Select one of the above five Status selections and proceed to the manual's relevant sub-section.

4.1 Status

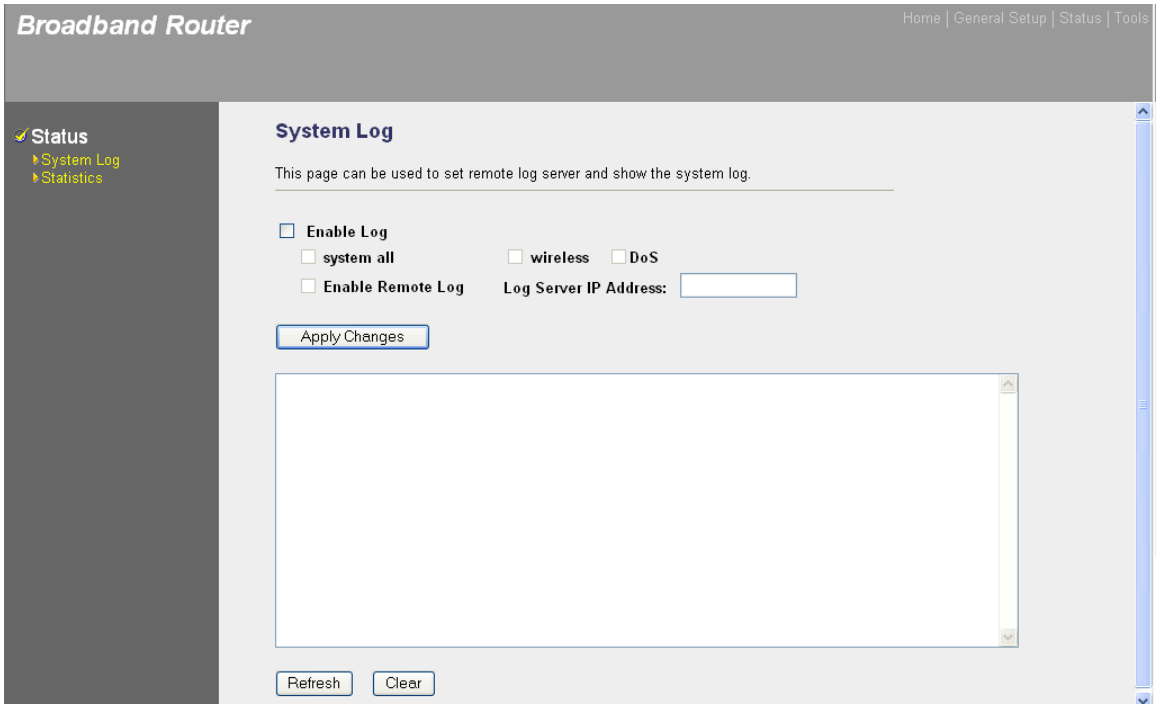
The Status section allows you to view the router's system information.



Parameters	Description
Information	You can see the router's system information such as the router's: Uptime, Firmware version, Wireless Configuration, LAN Address information, WAN Configuration information.

4.2 System Log

View the operation log of the system.



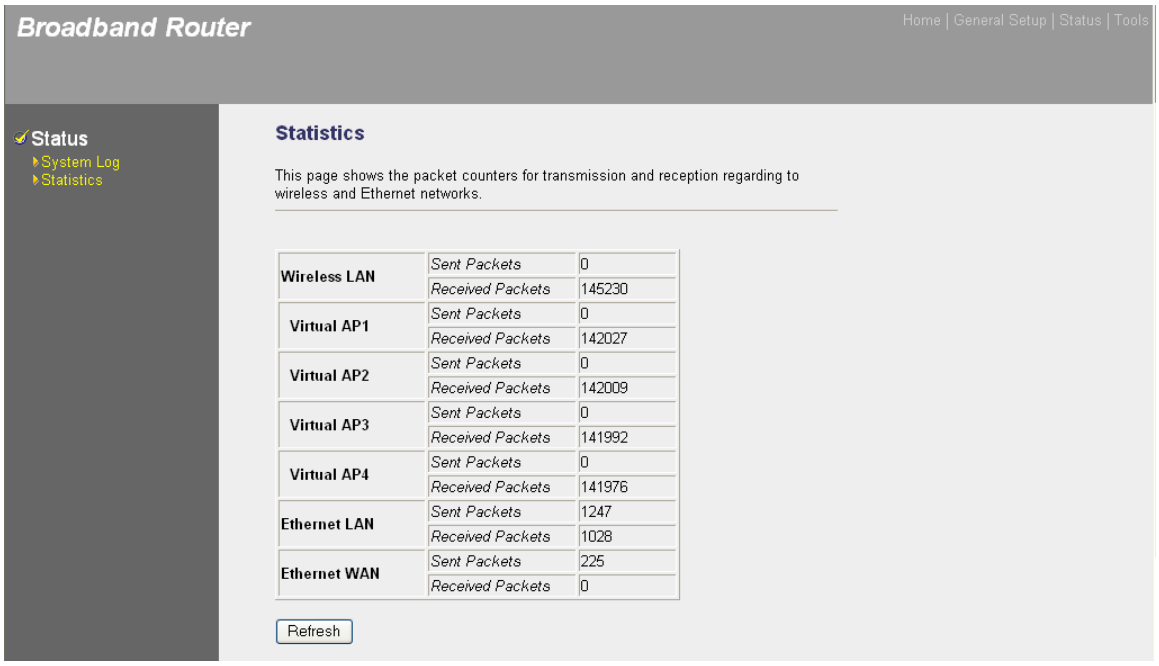
Parameters	Description
Enable Log	Check this box to enable the logging system.
System all	This page shows the current system log of the Broadband router. It displays any event occurred after system start up. At the bottom of the page, the system log can be cleared <**Clear**> or it can be refreshed <**Refresh**> to get the most updated situation. When the system is powered down, the system log will disappear if not saved to a local file.
Wireless	By select this options, you can check wireless log.
DoS	By select this options, you can check DoS log.
Enable Remote Log	If you want to send all log information to remote server, please check this box to enable this function and fill the server IP Address in the “Log Server IP Address” field.

Log Server IP Address	Input the server IP address where you want to save the logs.

Click <**Apply Changes**> at the bottom of the screen to save the above configurations. You can now configure other advance sections or start using the router (with the advance settings in place)

4.3 Statistics

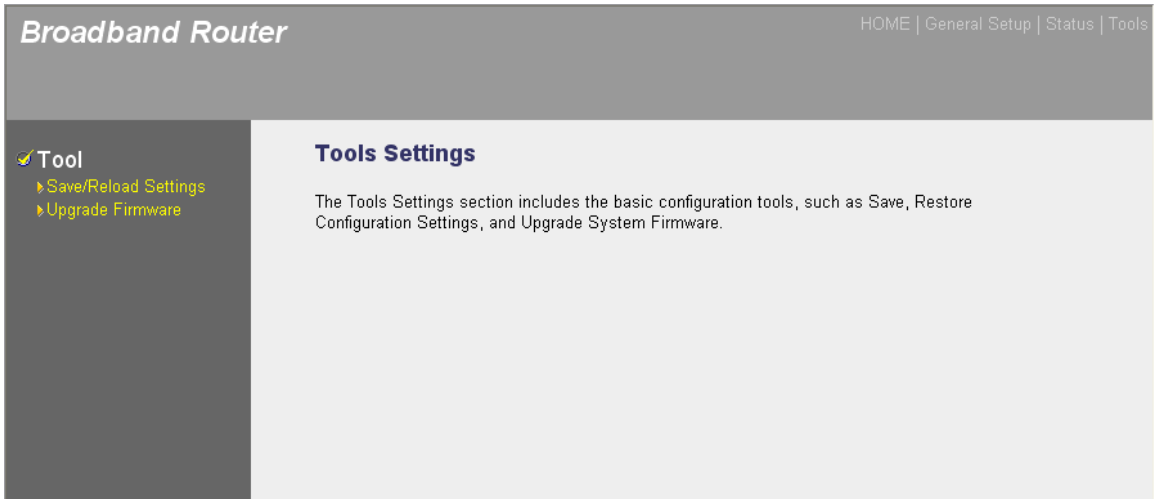
View the statistics of packets sent and received on WAN, LAN and Wireless LAN.



Parameters	Description
Statistics	Shows the counters of packets sent and received on WAN, LAN and Wireless LAN.

Chapter 5 Tool

This page includes the basic configuration tools, such as Configuration Tools (save or restore configuration settings), Firmware Upgrade (upgrade system firmware) and Reset.

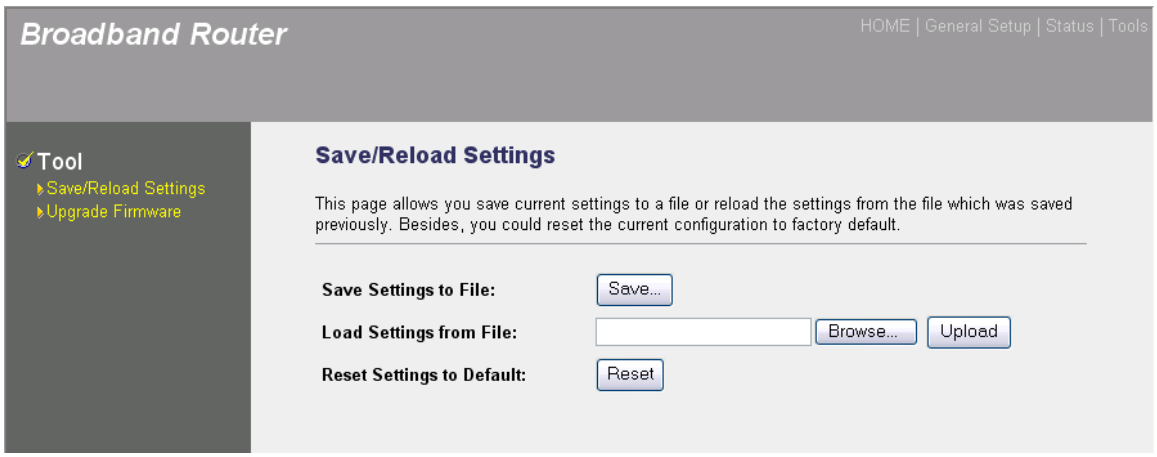


Parameters	Description
5.1 Save/Reload Settings	You can save the router's current configuration, restore the router's saved configuration files and restore the router's factory default settings.
5.2 Upgrade Firmware	This page allows you to upgrade the router's firmware.

Select one of the above three **Tools Settings** selection and proceed to the manual's relevant sub-section

5.1 Save/Reload Settings

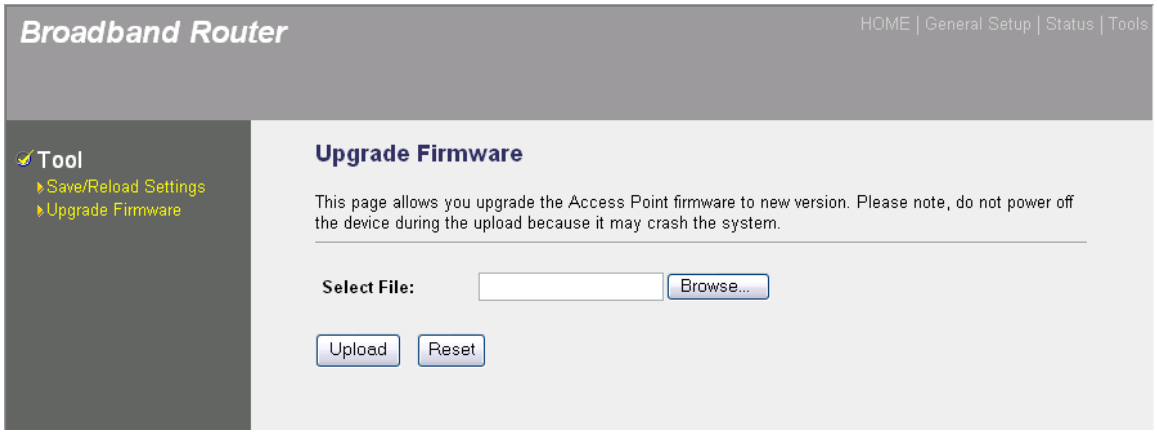
The Save/Reload Settings screen allows you to save (**Backup**) the router's current configuration setting. Saving the configuration settings provides an added protection and convenience should problems occur with the router and you have to reset to factory default. When you save the configuration setting (Backup) you can re-load the saved configuration into the router through the **Restore** selection. If extreme problems occur you can use the **Restore Settings to Defaults** selection, this will set all configurations to its original default settings (e.g. when you first purchased the router).



Parameters	Description
Configuration Tools	**Save Settings to File** : Click Save button to save the Broadband router current configuration to a file named "config.bin" on your PC. **Load Settings from File** : Click Browse button to search the file you have saved before and click Upload button to restore the saved configuration to the Broadband router. **Restore Settings to Default** : Click Reset button if you want to force the Broadband router to perform a power reset and restore the original factory settings.

5.2 Firmware Upgrade

This page allows you to upgrade the router's firmware



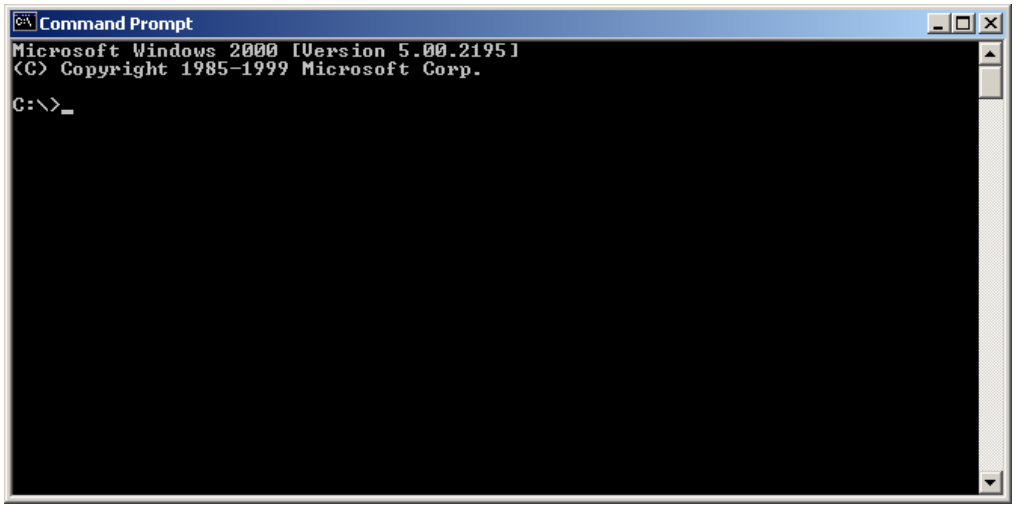
Parameters	Description
Upgrade Firmware	This tool allows you to upgrade the Broadband router's system firmware. To upgrade the firmware of your Broadband router, you need to download the firmware file to your local hard disk, and enter that file name and path in the appropriate field on this page. You can also use the Browse button to find the firmware file on your PC.

Once you've selected the new firmware file, click <**Upload**> at the bottom of the screen to start the upgrade process. (You may have to wait a few minutes for the upgrade to complete). Once the upgrade is complete you can start using the router.

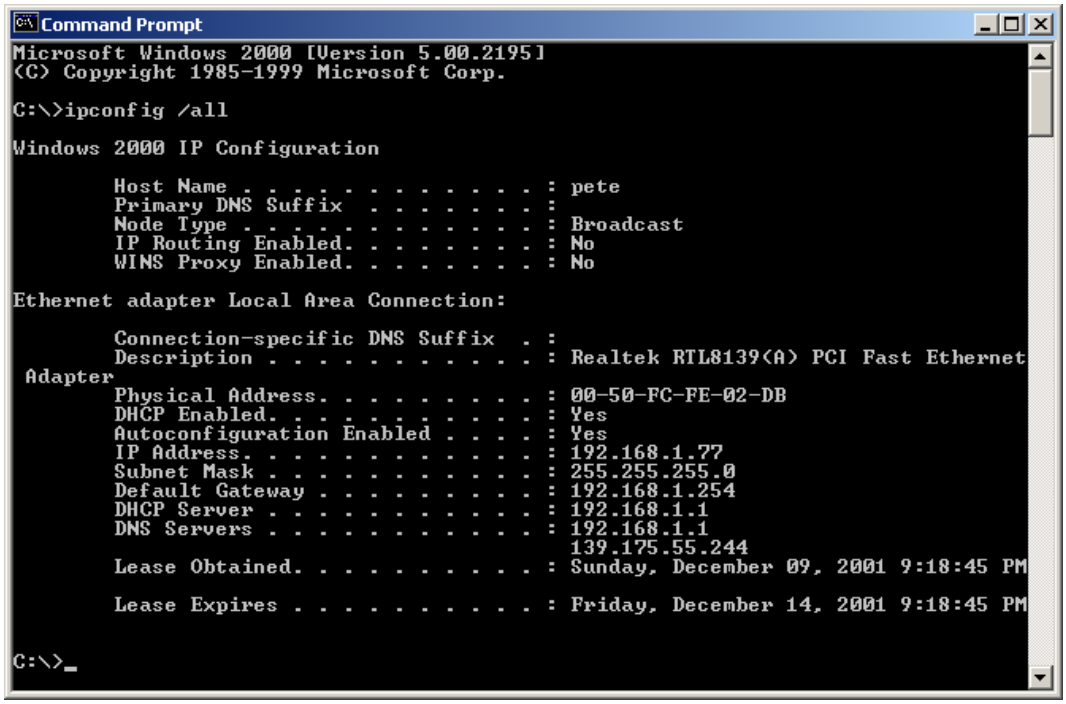
Appendix A

How to manually find your PC's IP and MAC address?

1) In Window's open the Command Prompt program



2) Type **Ipconfig /all** and <enter>



- Your PC's IP address is the one entitled **IP address** (192.168.1.77)
- The router's IP address is the one entitled **Default Gateway** (192.168.1.254)
- Your PC's MAC Address is the one entitled **Physical Address** (00-50-FC-FE-02-DB)

Glossary

Default Gateway (Router): Every **non-router IP d**evice needs to configure a default gateway's IP address. W**hen the device s**ends out an IP packet, if the destination is not on the same network, the device has to send the packet to its default gateway, which will then send it out towards the destination.
DHCP: Dynamic Host Configuration Protocol. This protocol automatically gives every computer on your home network an IP address.
DNS Server IP Address: DNS stands for Domain Name System, which allows Internet servers to have a domain name (such as www.Broadbandrouter.com) and one or more IP addresses (such as 192.34.45.8). A DNS server keeps a database of Internet servers and their respective domain names and IP addresses, so that when a domain name is requested (as in typing "Broadbandrouter.com" into your Internet browser), the user is sent to the proper IP address. The DNS server IP address used by the computers on your home network is the location of the DNS server your ISP has assigned to you.
DSL Modem: DSL stands for Digital Subscriber Line. A DSL modem uses your existing phone lines to transmit data at high speeds.
Ethernet: A standard for computer networks. Ethernet networks are connected by special cables and hubs, and move data around at up to 10/100 million bits per second (Mbps).
Idle Timeout: **Idle Timeout is designed so that after there is no traffic to the Internet for a pre-configured amount of time, the connection will automatically be disconnected.**

IP Address and Network (Subnet) Mask: IP stands for Internet Protocol. An IP address consists of a series of four numbers separated by periods, that identifies a single, unique Internet computer host in an IP network. Example: 192.168.2.1. It consists of 2 portions: the IP network address, and the host identifier.

The IP address is a 32-bit binary pattern, which can be represented as four cascaded decimal numbers separated by ".": aaa.aaa.aaa.aaa, where each "aaa" can be anything from 000 to 255, or as four cascaded binary numbers separated by ".": bbbbbbbb.bbbbbbbb.bbbbbbbb.bbbbbbbb, where each "b" can either be 0 or 1.
A network mask is also a 32-bit binary pattern, and consists of consecutive leading 1's followed by consecutive trailing 0's, such as 11111111.11111111.11111111.00000000. Therefore sometimes a network mask can also be described simply as "x" number of leading 1's.
When both are represented side by side in their binary forms, all bits in the IP address that correspond to 1's in the network mask become part of the IP network address, and the remaining bits correspond to the host ID.

For example, if the IP address for a device is, in its binary form,
11011001.10110000.10010000.00000111, and if its network mask is,
11111111.11111111.11110000.00000000
It means the device's network address is
11011001.10110000.10010000.00000000, and its host ID is,

00000000.00000000.0000<u>0000.00000111</u>. This is a convenient and efficient method for routers to route IP packets to their destination.

ISP Gateway Address: (see ISP for definition). The ISP Gateway Address is an IP address for the Internet router located at the ISP's office.

ISP: Internet Service Provider. An ISP is a business that provides connectivity to the Internet for individuals and other businesses or organizations.

LAN: Local Area Network. A LAN is a group of computers and devices connected together in a relatively small area (such as a house or an office). Your home network is considered a LAN.

MAC Address: MAC stands for Media Access Control. A MAC address is the hardware address of a device connected to a network. The MAC address is a unique identifier for a device with an Ethernet interface. It is comprised of two parts: 3 bytes of data that corresponds to the Manufacturer ID (unique for each manufacturer), plus 3 bytes that are often used as the product's serial number.

NAT: Network Address Translation. This process allows all of the computers on your home network to use one IP address. Using the broadband router's NAT capability, you can access the Internet from any computer on your home network without having to purchase more IP addresses from your ISP.

Port: Network Clients (LAN PC) uses port numbers to distinguish one network application/protocol over another. Below is a list of common applications and protocol/port numbers:

Application	Protocol	Port Number
Telnet	TCP	23
FTP	TCP	21
SMTP	TCP	25
POP3	TCP	110
H.323	TCP	1720
SNMP	UCP	161
SNMP Trap	UDP	162
HTTP	TCP	80
PPTP	TCP	1723
PC Anywhere	TCP	5631
PC Anywhere	UDP	5632

PPPoE: Point-to-Point Protocol over Ethernet. Point-to-Point Protocol is a secure data transmission method originally created for dial-up connections; PPPoE is for Ethernet connections. PPPoE relies on two widely accepted standards, Ethernet and the Point-to-Point Protocol. It is a communications protocol for transmitting information over Ethernet between different manufacturers

Protocol: A protocol is a set of rules for interaction agreed upon between multiple parties so that when they interface with each other based on such a protocol, the interpretation of their behavior is well defined and can be made objectively, without confusion or misunderstanding.

Router: A router is an intelligent network device that forwards packets between different networks based on network layer address information such as IP addresses.
Subnet Mask: A subnet mask, which may be a part of the TCP/IP information provided by your ISP, is a set of four numbers (e.g. 255.255.255.0) configured like an IP address. It is used to create IP address numbers used only within a particular network (as opposed to valid IP address numbers recognized by the Internet, which must be assigned by InterNIC).
TCP/IP, UDP: Transmission Control Protocol/Internet Protocol (TCP/IP) and Unreliable Datagram Protocol (UDP). TCP/IP is the standard protocol for data transmission over the Internet. Both TCP and UDP are transport layer protocol. TCP performs proper error detection and error recovery, and thus is reliable. UDP on the other hand is not reliable. They both run on top of the IP (Internet Protocol), a network layer protocol.

WAN: Wide Area Network. A network that connects computers located in geographically separate areas (e.g. different buildings, cities, countries). The Internet is a wide area network.

Web-based management Graphical User Interface (GUI): Many devices support a graphical user interface that is based on the web browser. This means the user can use the familiar Netscape or Microsoft Internet Explorer to Control/configure or monitor the device being managed.