11Mbps Wireless Broadband Router

WRT-403

User's Manual

Copyright

Federal Communication Commission Interference Statement

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of 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:

To assure continued compliance.(example-use only shielded interface cables when connecting to computer or peripheral devices). Any changes or modifications not expressly approved by the party responsible for compliance could void the user’s authority to operate the equipment.

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.

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 20 cm(8 inches) during normal operation.

R&TTE Compliance Statement

This equipment complies with all the requirements of DIRECTIVE 1999/5/CE OF THE EUROPEAN PARLIAMENT AND THE COUNCIL OF 9 March 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.

Revision

User's Manual for PLANET 11Mbps Wireless Broadband Router

Model: WRT-403

Rev: 1.0 (October. 2003)

Part No. EM-WRT403

TABLE OF CONTENTS

Chapter 1 Introduction

Thank you for purchasing WRT-403. This device features the latest innovation wireless technology making the wireless networking world happened. This manual guides you on how to install and properly use the WRT-403 in order to take full advantage of its features.

1.1 Package Contents

Make sure that you have the following items:

- One WRT-403
- One AC Power Adapter
- One User's Manual CD
- One Quick Installation Guide
- One External Dipole Antenna

Note:	If any of the above items are missing, contact your supplier as soon as possible.

1.2 System Requirements

Before installation, please check the following requirements with your equipment.

- Pentium Based (And Above) IBM-Compatible PC System
- CD-ROM drive
- Windows 98/ME/NT/2000/XP/Server 2003 Operating System with TCP/IP protocol

1.3 Features

- Allow multiple users to share a single Internet line
- Internet Access via Cable or xDSL modem
- Access Private LAN Servers from the Public Network
- Equipped with four LAN ports (10/100M) and one WAN port (10/100M)
- Provides IEEE 802.11b wireless LAN access point
- Support DHCP Server for easy setup
- Allow you to monitor the router's status such as: Active DHCP Client, Security Log and Device/Connection Status
- Easy to use Web-based GUI for configuration and management purposes
- Remote Management allows configuration and upgrades from a remote site (over the Internet)
- DHCP/PPPOE/PPTP/L2TP/Fixed IP allocation
- MAC/IP filter access control, URL blocking

- SPI firewall + DoS prevention protection
- UPnP function
- Complies with the IEEE 802.11b (DSSS) 2.4GHz specification
- 64/128-bit WEP Encryption to protect the wireless data transmissions

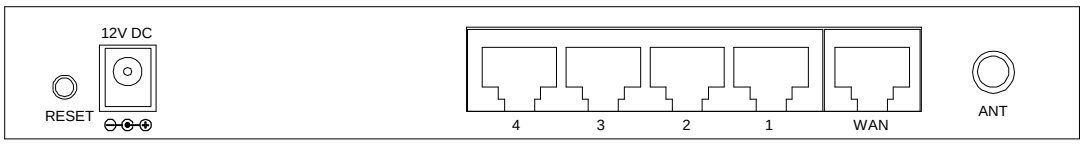
1.4 Specification

Standard	IEEE 802.11b Compliant
Signal Type	DSSS (Direct Sequence Spread Spectrum)
Modulation	QPSK / BPSK / CCK
Port	Five 10/100Base-TX (WAN*1,LAN*4)
Antenna	Dipole Antenna * 1
Data Encryption	64 bit / 128 bit WEP encryption
Frequency	2.4GHz - 2.484GHz
Sensitivity	-78dBm (@PER8%, 11Mbps)
Channel	11 Channels (FCC / US, Canada) 13 Channels (ETSI / Europe) 14 Channels (TELEC / Japan)
Data Rate	Up to 11Mbps (with automatic scale back)
LED Indicators	PWR, WLAN LAN: LNK/ACT * 4, 10/100Mbps * 4 WAN: LNK/ACT * 1, 10/100Mbps * 1
Power Requirement	12V DC, 1A
Power Consumption	TX power consumption: <650mA RX power consumption <350mA
Temperature	Operating :0 ~ 55 degree C Storage: -20 ~ 70 degree C
Humidity	Operating: 0 ~ 90% Storage: 0 ~ 95% Non-Condensing
Dimensions	190 x 98 x 35 mm
Output Power	18dBm

Chapter 2 Hardware Installation

Before you proceed with the installation, it is necessary that you have enough information about the WRT-403.

2.1 Hardware Connection



1. **Locate an optimum location for the WRT-403.** The best place for your WRT-403 is usually at the center of your wireless network, with line of sight to all of your mobile stations.
2. **Adjust the antennas of WRT-403.** Try to adjust them to a position that can best cover your wireless network. The antenna's position will enhance the receiving sensitivity.
3. **Connect RJ-45 cable to WRT-403 LAN port.** Connect one of the LAN ports on WRT-403 to your LAN switch/hub with a RJ-45 cable.
4. **Connect RJ-45 cable to WRT-403 WAN port.** Connect ADSL/Cable Modem to the WAN port on WRT-403. Use the cable supplied with your modem. If no cable was supplied with your modem, please use a RJ-45 Ethernet cable
5. **Plug in power adapter and connect to power source**. After power on, WRT-403 will start to operate.

Note: ONLY use the power adapter supplied with the WRT-403. Otherwise, the product may be damaged.

Note: If you want to reset WRT-403 to default settings, press and hold the Reset button over 5 seconds and release. And then wait for 10 seconds for WRT-403 restart.

WAN port (10/100BaseT)	Connect the xDSL or Cable Modem here. If your modem came with a cable, use the supplied cable. Otherwise, use a standard LAN cable.
Note	If the connection cannot be established (WAN LED is not on), please connect to the *Uplink* port instead, and check if the supplied cable is broken.
10/100BaseT LAN connections	Use standard LAN cables (RJ-45 interface) to connect your PCs to these ports.

Note

If the connection cannot be established (LAN LED is not on), please connect to the *Uplink* port instead, and check if the supplied cable is broken.

Reset Button

This button has two (2) functions:

Reboot. When pressed and released, the router will reboot (restart).

Clear All Data. This button can also be used to clear ALL data and restore ALL settings to the factory default values.

To Reboot machine without Clearing Existing Configurations:

Press the reset button with a pencil tip (for less than 4 seconds), machine will re-boot itself, the existing configurations will be kept.

To Clear All Data and restore the factory default values:

Press the reset button for longer than 4 seconds and the router will reset itself to the factory default settings (warning: your original configurations will be replaced with the factory default settings)

Note

These steps can restore machine factory default IP address: 192.168.0.1, and User name / Password to "admin".

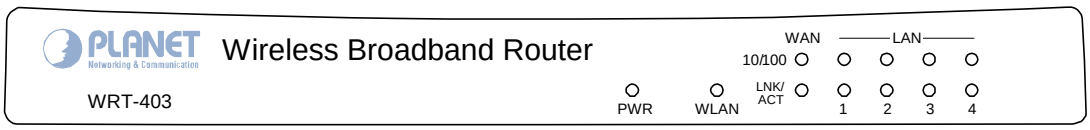
Power port

Connect the supplied power adapter here.

ANT

The reversed-polarity SMA connector for wireless antenna. Please find the omni-antenna from the package.

2.2 LED Indicators



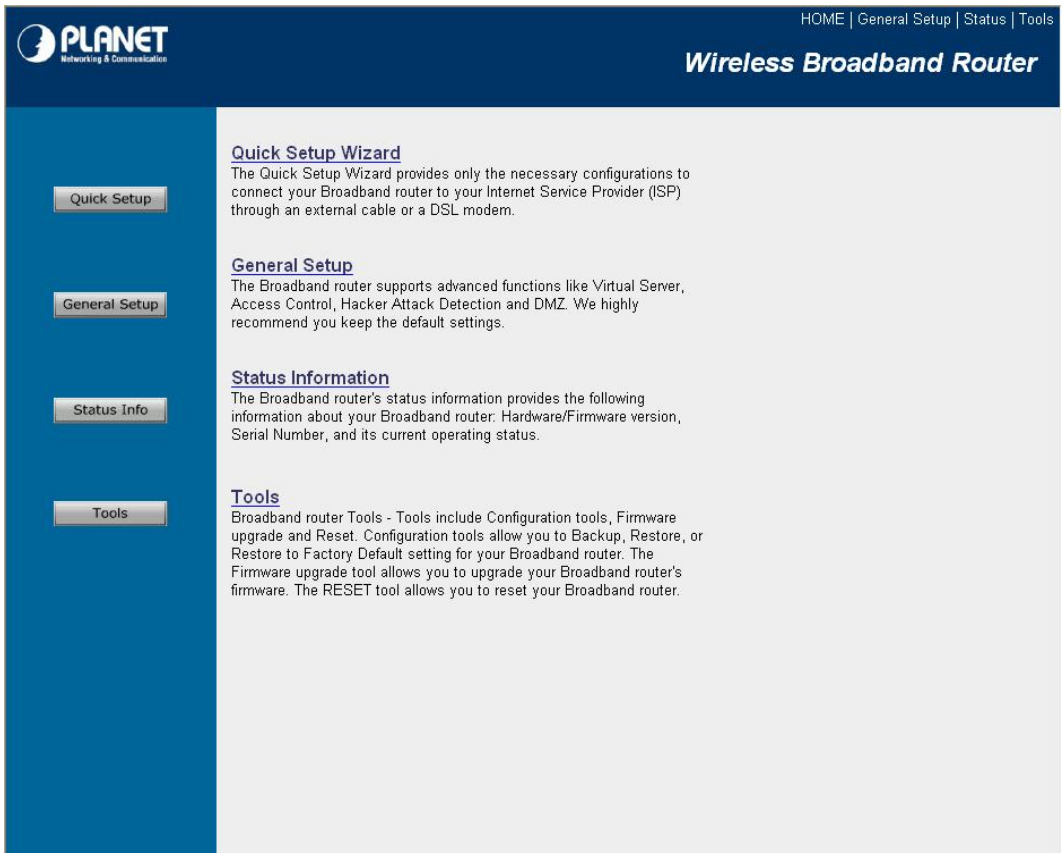
LED	STATE	MEANING
PWR	Green	Device power on
	Off	Device power off
WLAN	Blinking	WLAN activity
	Off	On wireless device connected
10/100	Orange	Port works on 100Mbps
	Off	Port works on 10Mbps
LNK/ACT	Green	Link is established
	Blinking Green	Packets are transmitting or receiving
	Off	Not connected

Chapter 3 Configure through Web Browser

Web configuration provides a user-friendly graphical user interface (web pages) to manage your WRT-403. A WRT-403 with an assigned IP address will allows you to monitor and configure via web browser (e.g., MS Internet Explorer or Netscape).

1. Open your web browser.
2. Enter the IP address of your WRT-403 in the address field (default IP address is http://192.168.0.1).
3. A User Name and Password dialog box will appear. Please enter your User Name and Password here. Default User Name and Password is “admin”. Click OK.

4. Then you will see the WRT-403 web configuration page as below.



In HOME screen. It is divided into four sections, **Quick Setup Wizard**, **General Setup**, **Status Information** and **Tools**. Please refer to the section below to know the details of each option.

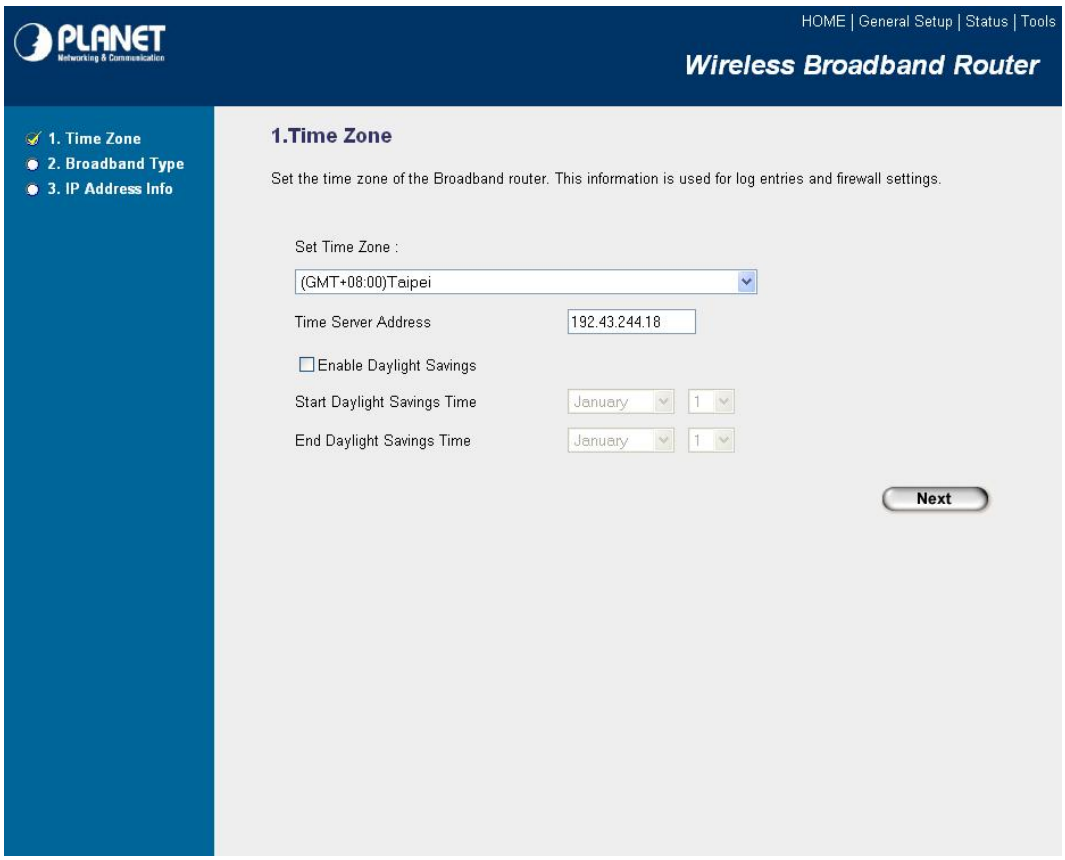
Section	**Description**
Quick Setup Wizard	Select your Internet connection type and then input the configurations needed to connect to your Internet Service Provider (ISP).
General Setup	This section contains configurations for the Broadband router's advance functions such as: Bridge, Address Mapping, Virtual Server, Access Control, Hacker Attack Prevention, DMZ, Special applications and other functions to meet your LAN requirements.
Status Information	In this section you can see the Broadband router's system information, Internet Connection, Device Status, Security Log and DHCP client Log information.
Tools	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 of your Broadband router. The Firmware Upgrade tool allows you to upgrade your Broadband router's firmware. The RESET tool allows you to re-boot your Broadband router.

Chapter4 Quick Setup Wizard

This section will show the basic configuration of the WRT-403 to let you connect to Internet easily. Please follow the steps to setup your WRT-403.

4.1 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.



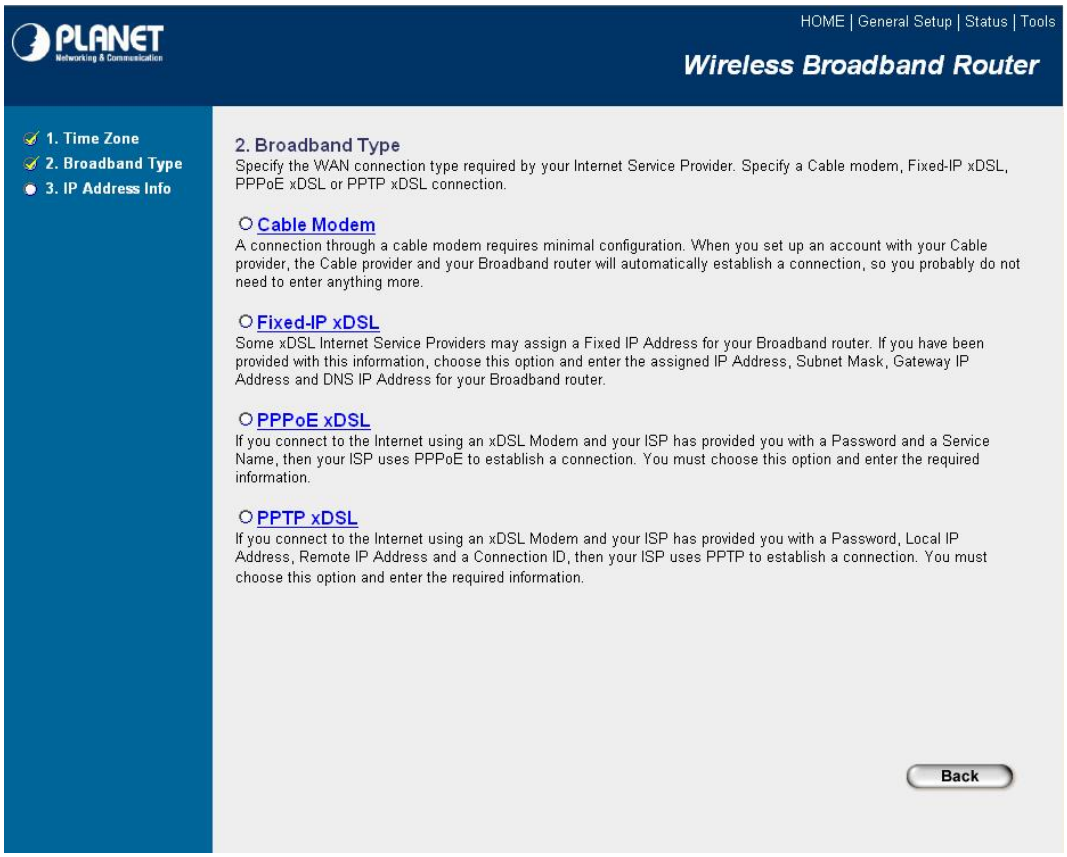
Parameter	Description
Set Time Zone	Select the time zone of the country you are currently in. The router will set its time based on your selection.
Time Server Address	Remain it as default or, you can manually assign an IP address of the Time Server if the default Time Server does not work. The information of Timer Server can be found in the following URL link: http://www.eecis.udel.edu/~mills/ntp/servers.html or http://www.ntp.org.
Enable Daylight Savings	The router can also take Daylight savings into account. If you wish to use this function, you must check/tick the enable box to enable your daylight

	saving configuration (below).
Start Daylight Savings Time	Select the period in which you wish to start daylight Savings Time.
End Daylight Savings Time	Select the period in which you wish to end daylight Savings Time.

Click “NEXT” button to proceed to the next step.

4.2 Broadband Type

Before establishing the Internet connection, please be sure to check the demands from your ISP, and then choose a proper Internet access method supported.



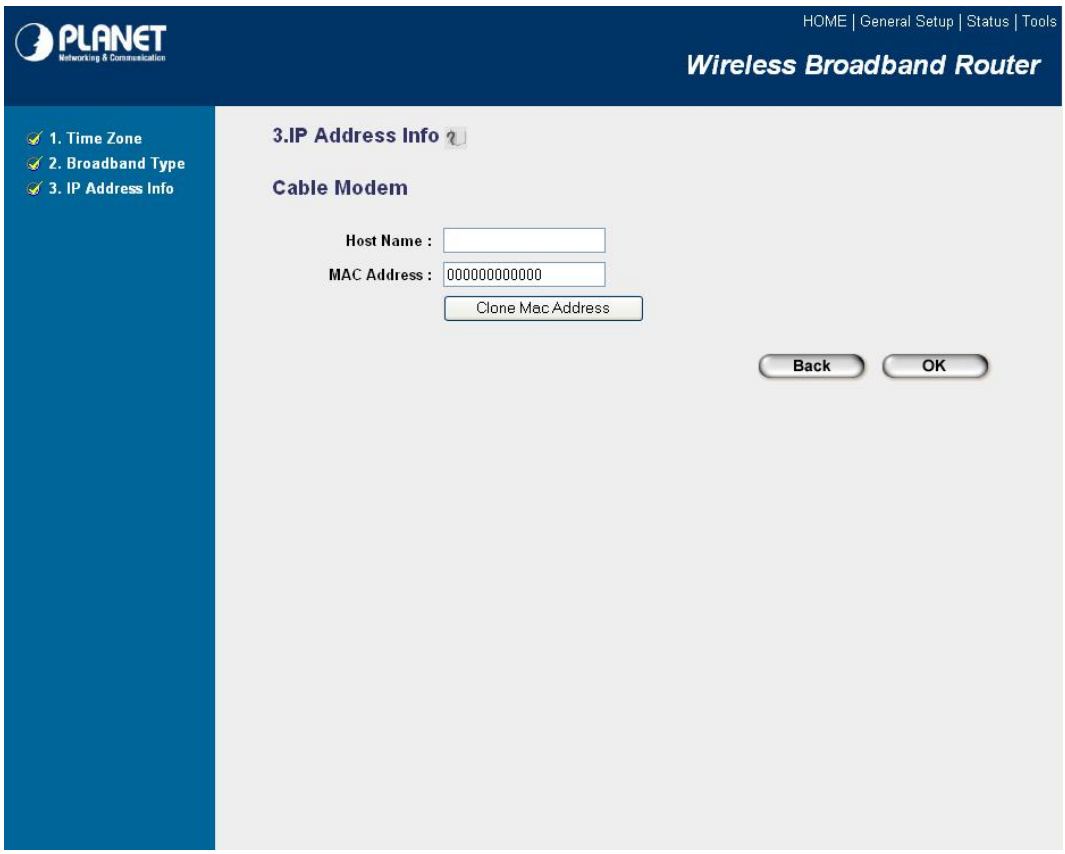
Broadband	Description
Cable Modem	ISP will automatically give you an IP address. Please refer to section 4.2.1 for details.
Fixed-IP xDSL	ISP has given you a fixed IP address already. Please refer to section 4.2.2 for details.
PPPoE xDSL	ISP requires you to use a Point-to-Point Protocol over Ethernet (PPPoE) connection. Please refer to section 4.2.3 for details.
PPTP xDSL	ISP requires you to use a Point-to-Point Tunneling Protocol (PPTP)

	connection. Please refer to section 4.2.4 for details.

4.2.1 Cable Modem

Choose Cable Modem if the ISP will automatically give you an IP address. Some ISP may also require you to fill in additional information such as Host Name and MAC address (see screen below).

Note: The Host Name and MAC address section is **optional** and you can skip this section if your ISP does not require these settings for you to connect to the Internet.

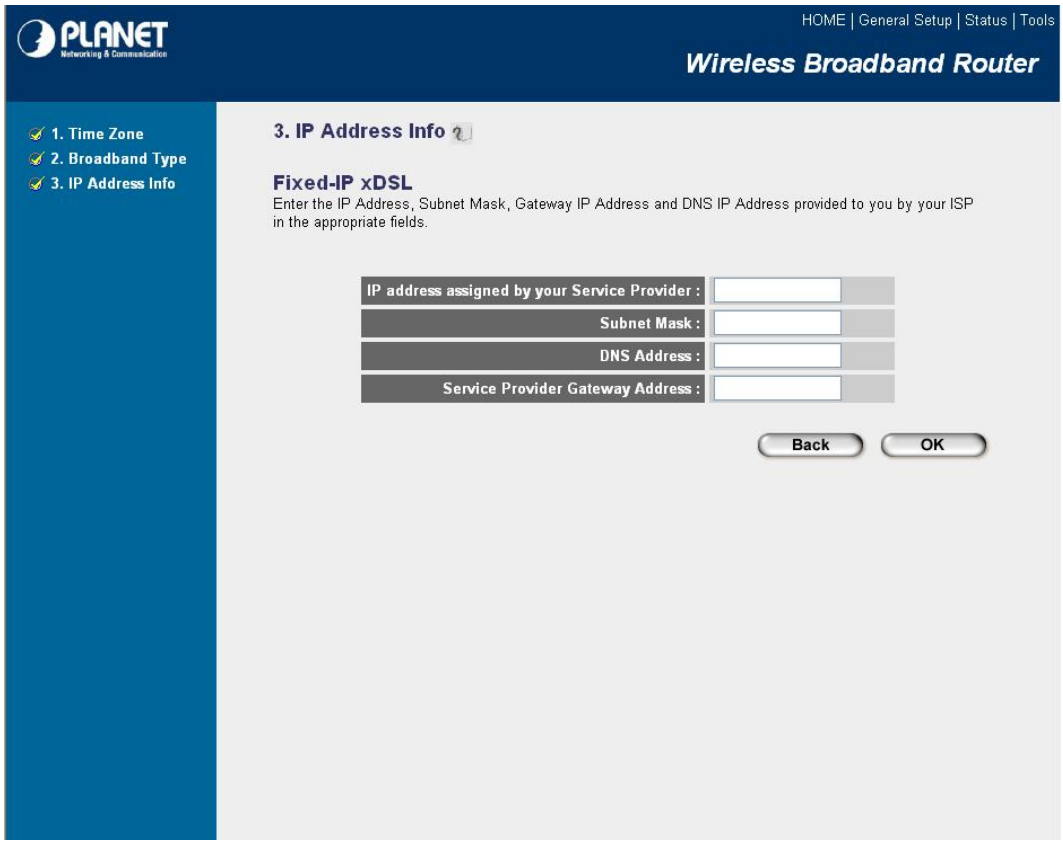


Parameters	Description
Host Name	If your ISP requires a Host Name, type in the host name provided by your ISP, otherwise leave it blank if your ISP does not require a Host Name.
MAC Address	To connect to the Internet, your ISP will require a MAC address from your PC or installed in your PC that used to connect to the Internet previously.. Type in this MAC address in this section or use the “Clone MAC Address” button to replace the WAN MAC address with the MAC address of that PC (you have to be using that PC for the Clone MAC Address button to work). To find out the PC’s MAC address see Appendix A. (see Glossary for an explanation on MAC address.

When the configuration finished please click “OK” to next step or click “Back” to previous step.

4.2.2 Fixed-IP xDSL

Select Fixed-IP xDSL if your ISP has given you a specified IP address for you. Your ISP should provide all the information required in this section.



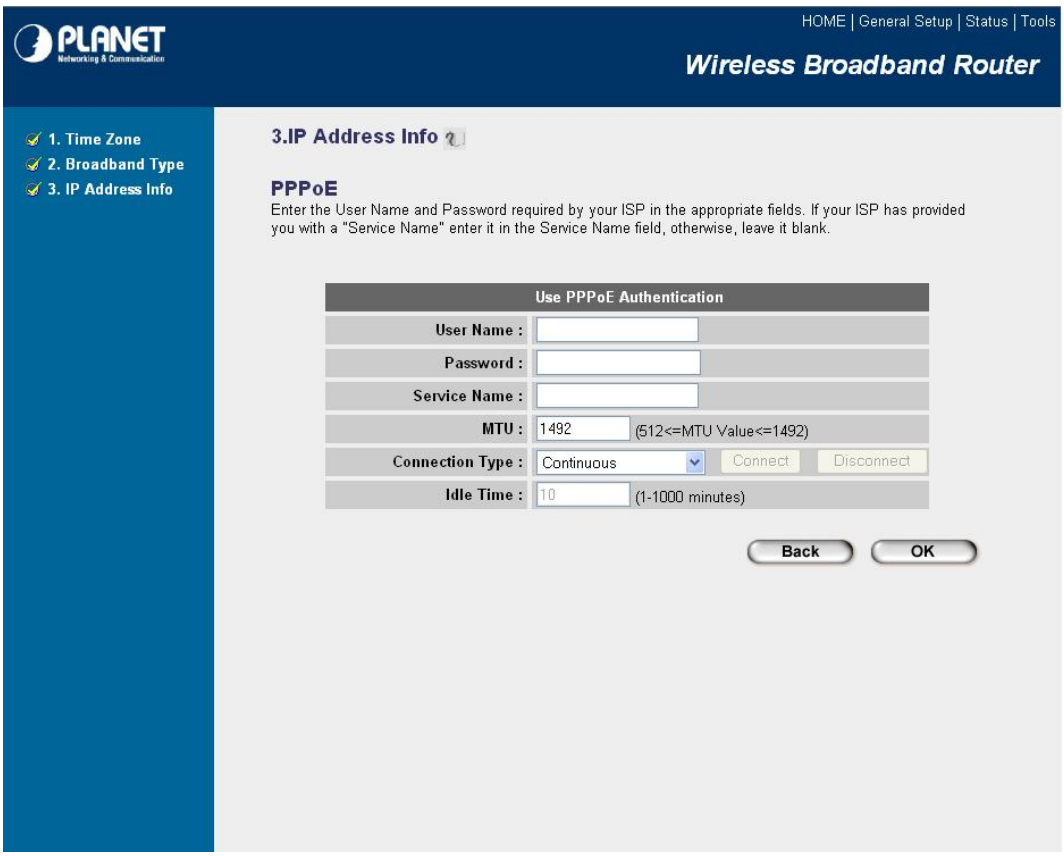
Parameters	Description
IP address assigned by your Service Provider	The IP address that your ISP should provide you.
Subnet Mask	Enter the Subnet Mask provided by your ISP (e.g. 255.255.255.0).
DNS Address	The IP address of ISP's DNS (Domain Name Service) Server.
Service Provide Gateway Address	The ISP's IP address gateway.

Please consult your local ISP about the information above.

When the configuration finished, Please click "OK" for next step or click "Back" to previous step.

4.2.3 PPPoE xDSL

Select PPPoE if your ISP requires the PPPoE protocol for Internet connectivity. Your ISP should provide all the information like user name, password required in this section.



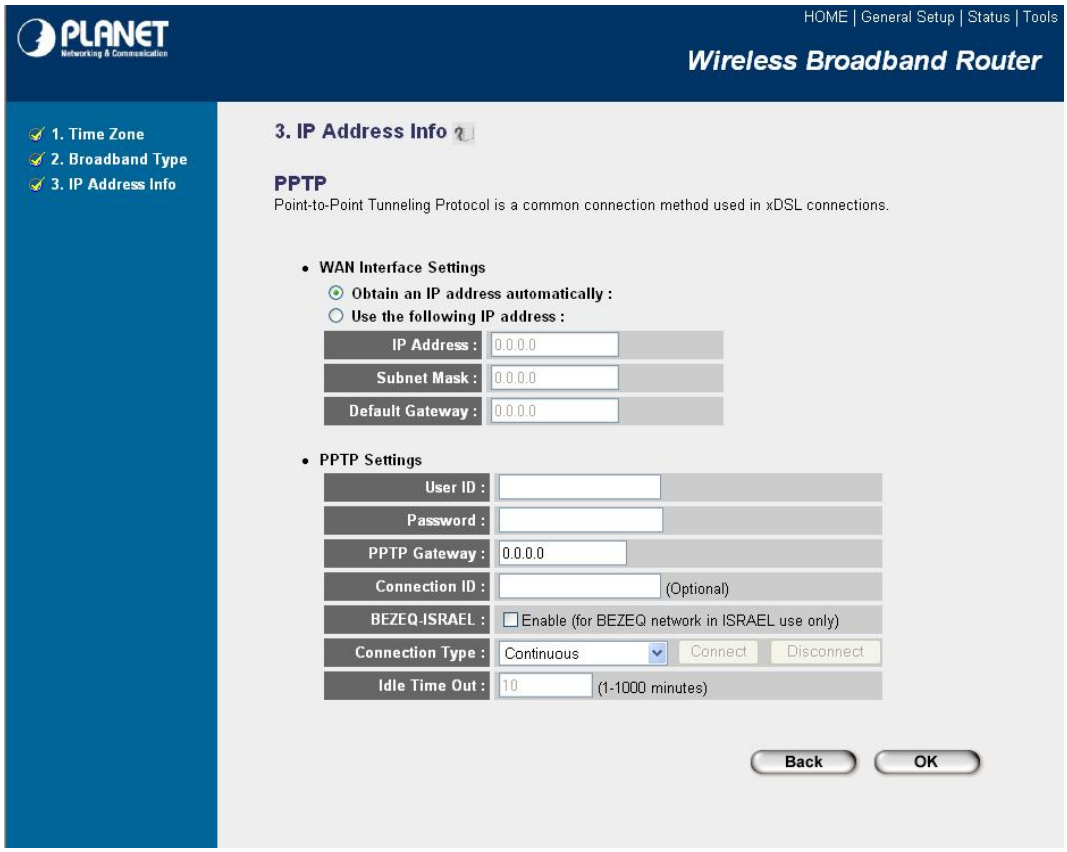
Parameters	Description
User Name	Enter the User Name provided by your ISP for the PPPoE connection.
Password	Enter the Password provided by your ISP for the PPPoE connection.
Service Name	This is an optional parameter. Leave it blank unless your ISP requires it.
MTU	This is an optional parameter. You can specify the maximum size of transmission packet to the Internet. The range of the MTU will be from 1492 to 512. You can also consult you ISP for the optimal MTU as well. Default: 1492
Connection Type	If you select "**Continuous**", the router will always connect to the ISP. If the WAN line breaks down and links again, the router will auto-reconnect to the ISP. If you select "**Connect On Demand**", the router will auto-connect to the ISP when someone want to use the Internet and keep connected until the WAN idle timeout. The router will close the WAN connection if the time period that no one is using the Internet exceeds the "**Idle Time**". If you select "**Manual**", the router will connect to ISP only when you click "Connect" manually from the Web user interface. The WAN connection will not disconnected

	due to the idle timeout. If the WAN line breaks down and latter links again, the router will not auto-connect to the ISP. Default: **Continuous**.
Idle Time	You can specify an idle time threshold (minutes) for the WAN port. This means if no packets have been sent (no one using the Internet) during this specified period, the router will automatically disconnect the connection from your ISP.
➘ **Note**	This "idle timeout" 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.

When the configuration finished, please click "OK" to next step or click "Back" to previous step.

4.2.4 PPTP xDSL

Select PPTP if your ISP requires the PPTP protocol to connect to the Internet. Your ISP should provide all the information required in this section. When configuration finished, please click "OK" to next step or click "Back" to previous step.

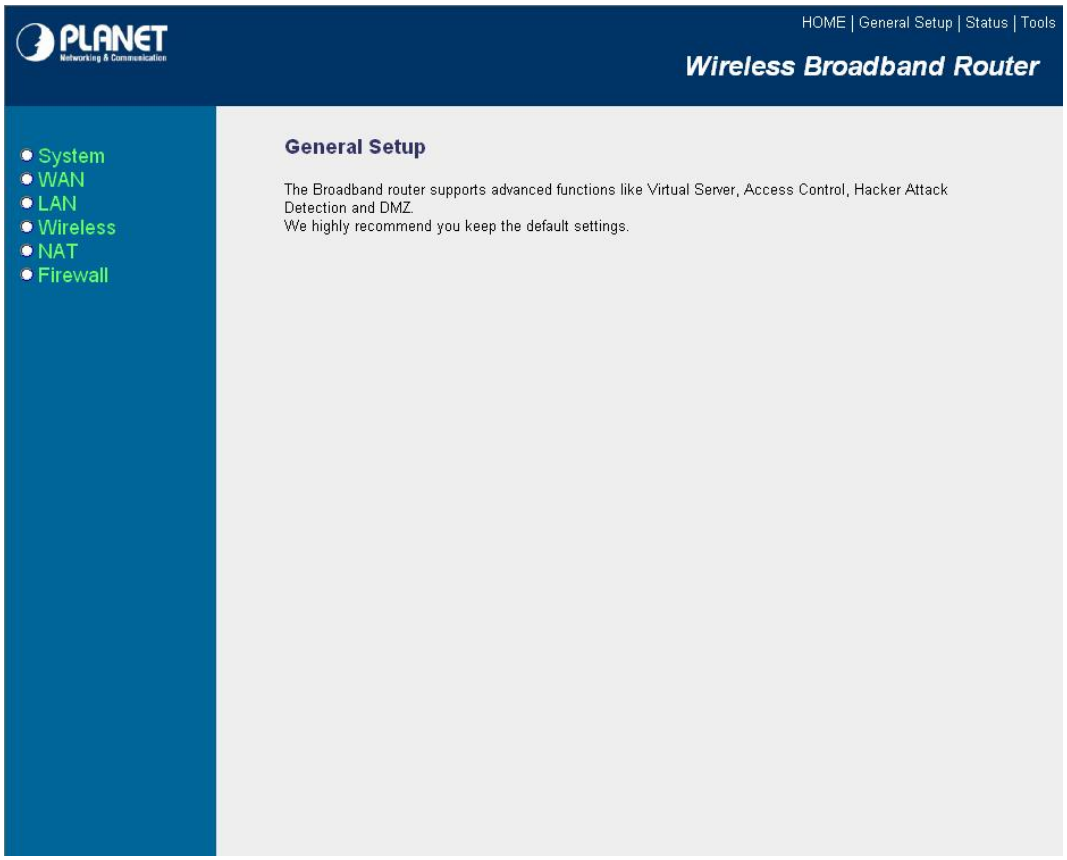


Parameter	Description
Obtain an IP address	The ISP requires you to obtain an IP address by DHCP automatically before connecting to the PPTP server.
Use the following IP address	The ISP provides you a static IP to connect to the PPTP server.
IP Address	This is the IP address that your ISP has given you to establish a PPTP connection.
Subnet Mask	Enter the Subnet Mask provided by your ISP (e.g. 255.255.255.0)
Gateway	Enter the IP address of the ISP's Gateway.
User ID	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
PPTP Gateway	If your LAN has a PPTP gateway, then enter that PPTP gateway's IP address here. If you do not have a PPTP gateway then enter the ISP's Gateway IP address above.
Connection ID	This is the ID given by ISP. This is an optional parameter.
BEZEQ-ISRAEL	Select this item if you are using the service provided by BEZEQ in Israel.
Connection Type	If you select "**Continuous**", the router will always connect to the ISP. If the WAN

	line breaks down and links again, the router shall auto- reconnect to the ISP. If you select "**Connect On Demand**", the router will auto-connect to the ISP when someone want to use the Internet and keep connected until the WAN idle timeout. The router will close the WAN connection if the time period that no one is using the Internet exceeds the "Idle Time". If you select "**Manual**", the router will connect to ISP only when you click "Connect" manually from the Web user interface. The WAN connection will not disconnected due to the idle timeout. If the WAN line breaks down and latter links again, the router will not auto-connect to the ISP. Default: **Continuous.**
Idle Time	You can specify an idle time threshold (minutes) for the WAN port. This means if no packets have been sent (no one using the Internet) throughout this specified period, then the router will automatically disconnect the connection with your ISP.
Note	This "idle timeout" 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.

Chapter 5 General Setup

After click on the “General Setup” button at the HOME Page, you should see the screen below.

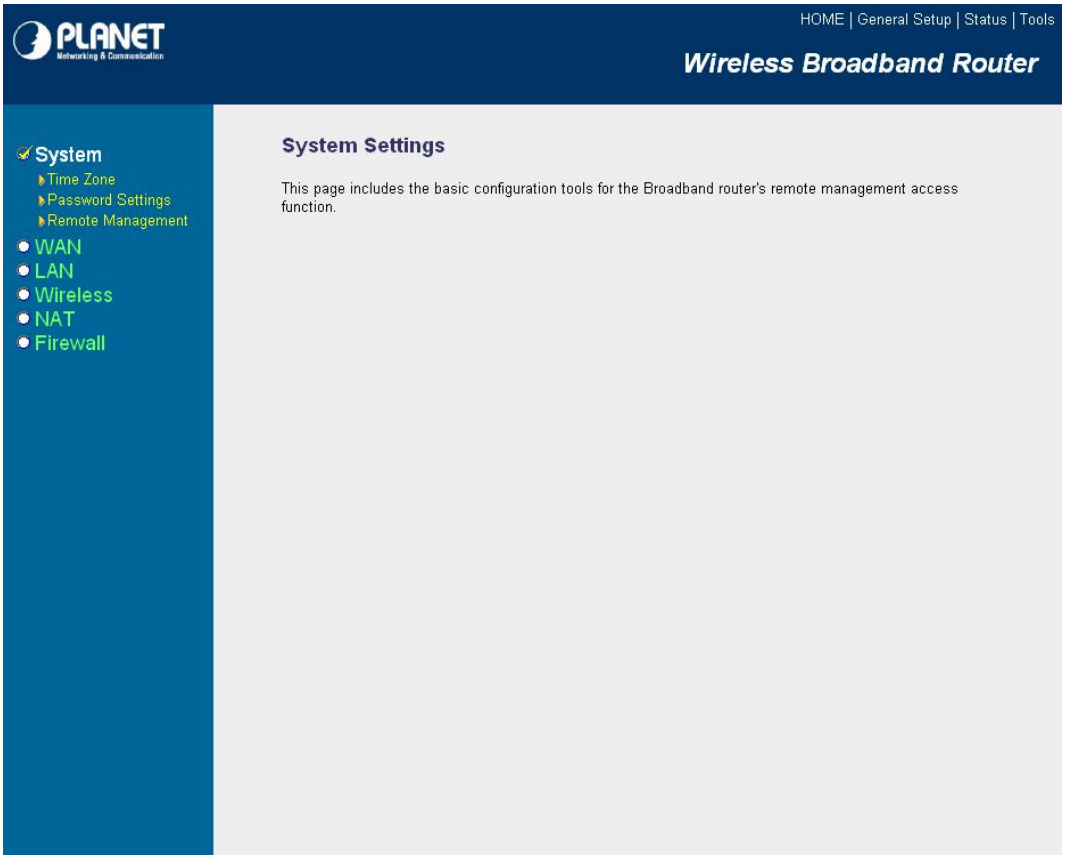


If you have done the configuration from “Quick Setup Wizard”, you do NOT need to configure anything in the General Setup screen for the first time Internet connection.

The General Setup contain advanced features that allow you to configure the router to meet the network’s needs such as: Wireless, Port Forwarding, Virtual Server, Access Control, URL Blocking, Special Applications, DMZ and other functions.

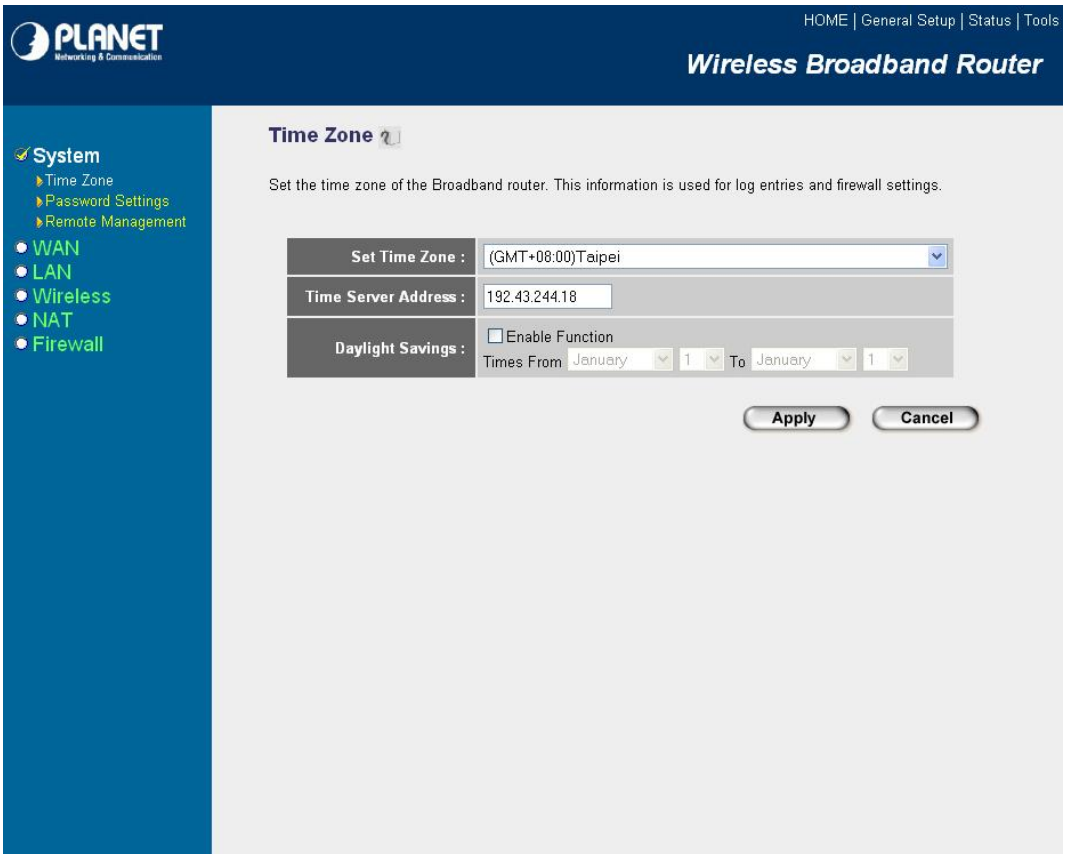
5.1 System

This section shows how to setup the Broadband router’s system Time Zone, Password and Remote Management Administrator.


PLANET
Networking & Communication
HOME | General Setup | Status | Tools
Wireless Broadband Router
System
Time Zone
Password Settings
Remote Management
WAN
LAN
Wireless
NAT
Firewall
System Settings
This page includes the basic configuration tools for the Broadband router's remote management access function.

5.1.1 Time Zone

The Time Zone allows WRT-403 to allocate its time on the settings configured here, it will affect log display functions such as Security Log and Firewall settings.

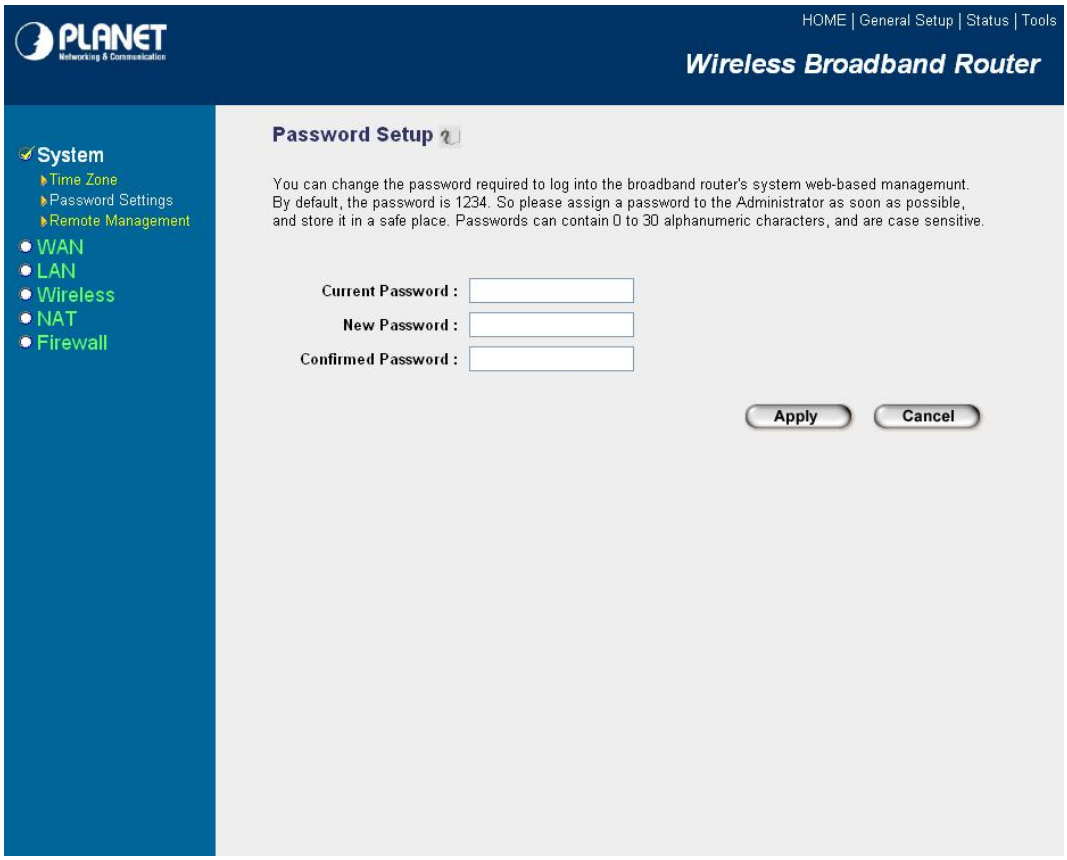


Parameter	Description
Set Time Zone	Select the time zone of the country you are currently in. The router will set its time based on your selection.
Time Server Address	You can keep the default IP address or enter a new Time Server Address for this device to update its time. You can also refer to the web site http://www.ntp.org to find a time server near you.
Daylight Savings	The router can also take Daylight savings into account. If you wish to use this function, you must check/tick the enable box to enable your daylight saving configuration. You can set the days that you wish to start and stop daylight Savings Time.

After the setup completed, please click “Apply” to save the settings.

5.1.2 Password Setup

Allows you to select a password in order to access the web-based management website.



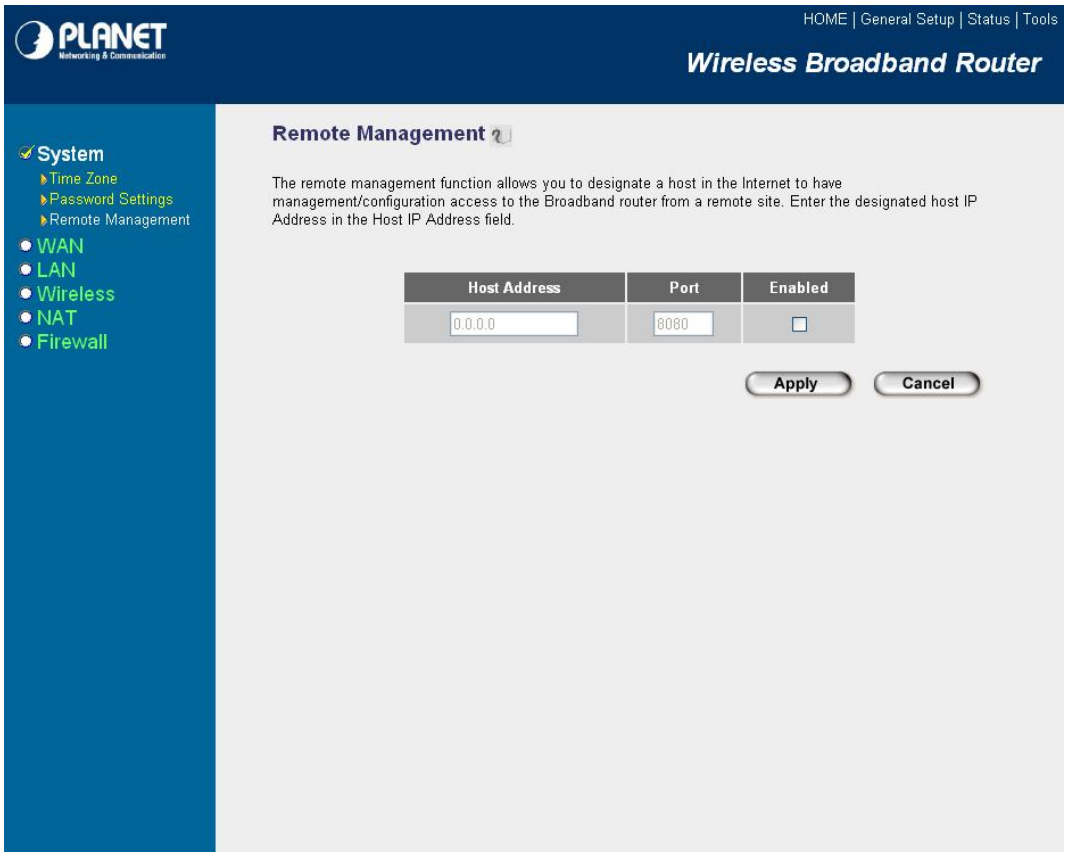
Parameters	Description
Current Password	Enter your current password for the remote management administrator to login to your Broadband router.
New Password	Enter your new password.
Confirmed Password	Enter your new password again for verification purposes.

Click “Apply” button of the screen to save the above configurations. You can now configure other advance sections or start using the router.

Note: If you forget the password, please reset the WRT-403 to the factory default from the reset button (see router’s back panel).

5.1.3 Remote Management

You can specify a Host IP address that can perform remote management from Internet.

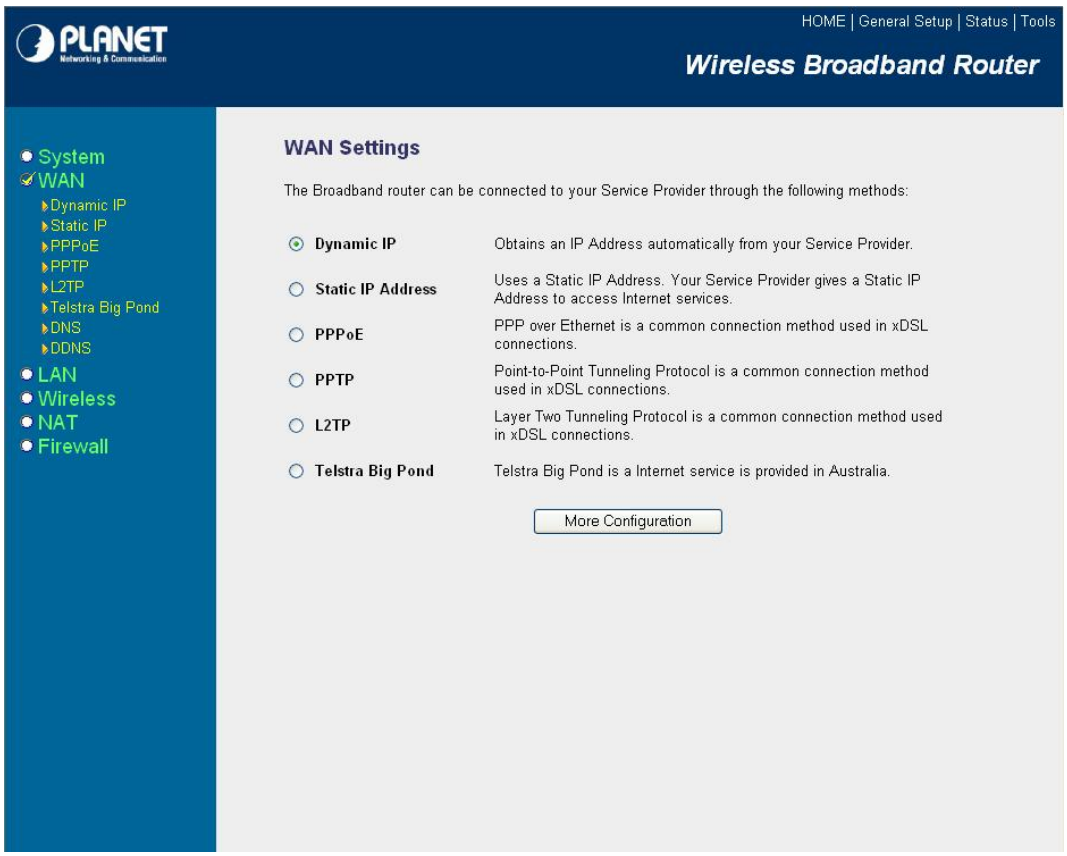


Parameters	Description
Host Address	The IP address of the host in the Internet that will have management / configuration access to the Broadband router from a remote site. This means if you are at home and your home IP address has been designated the Remote Management host IP address for this router (ex. located in your office), then you are able to configure this router from your home. Left it to **0.0.0.0** means anyone can access the router's web-based configuration from any remote location. Click the **Enabled** box to enable the Remote Management function.
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 (see below). You'll also need to know the password set in the Password Setting screen in order to access the router's web-based management.

Click "Apply" button of the screen to save the above configurations. You can now configure other advance sections or start using the router.

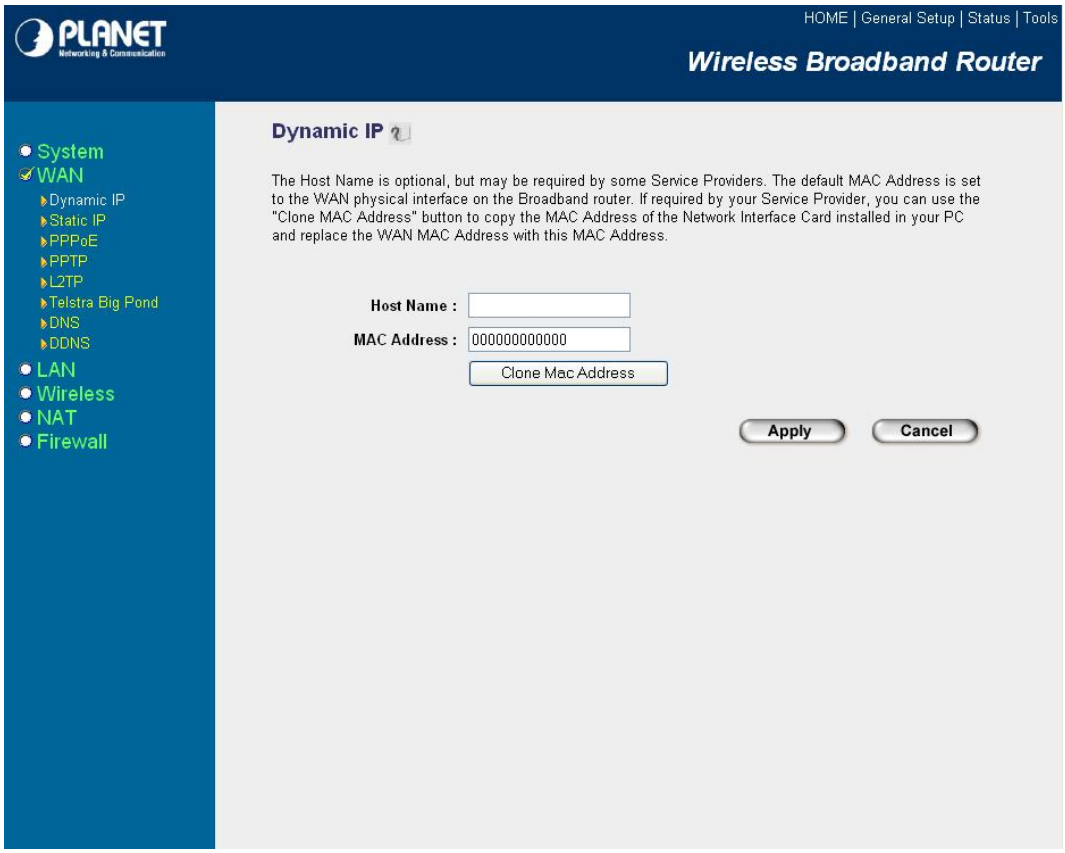
5.2 WAN

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 you to specify the type of WAN port connect you want to establish with your ISP. In the WAN Settings screen you can also specify the router to act as a Bridge. The WAN settings offer the following selections for the router's WAN port, **Dynamic IP**, **Static IP**, **PPPoE**, **PPTP**, **L2TP**, **Telstra Big Pond**, **DNS** and **DDNS**.



5.2.1 Dynamic IP

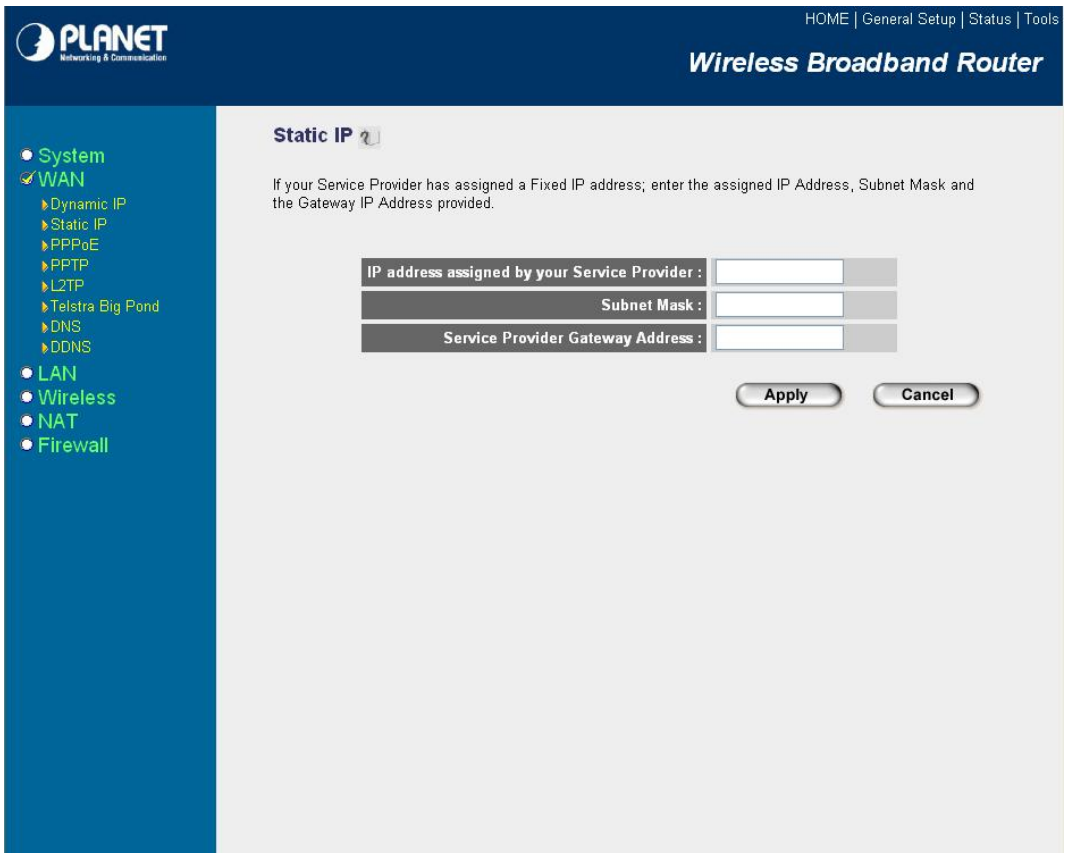
Choose the Dynamic IP selection if your ISP will automatically give you an IP address. Some ISP's may also require that you fill in additional information such as Host Name, Domain Name and MAC address.



Please refer to the section 4.2.1 for more settings of this option.

5.2.2 Static IP

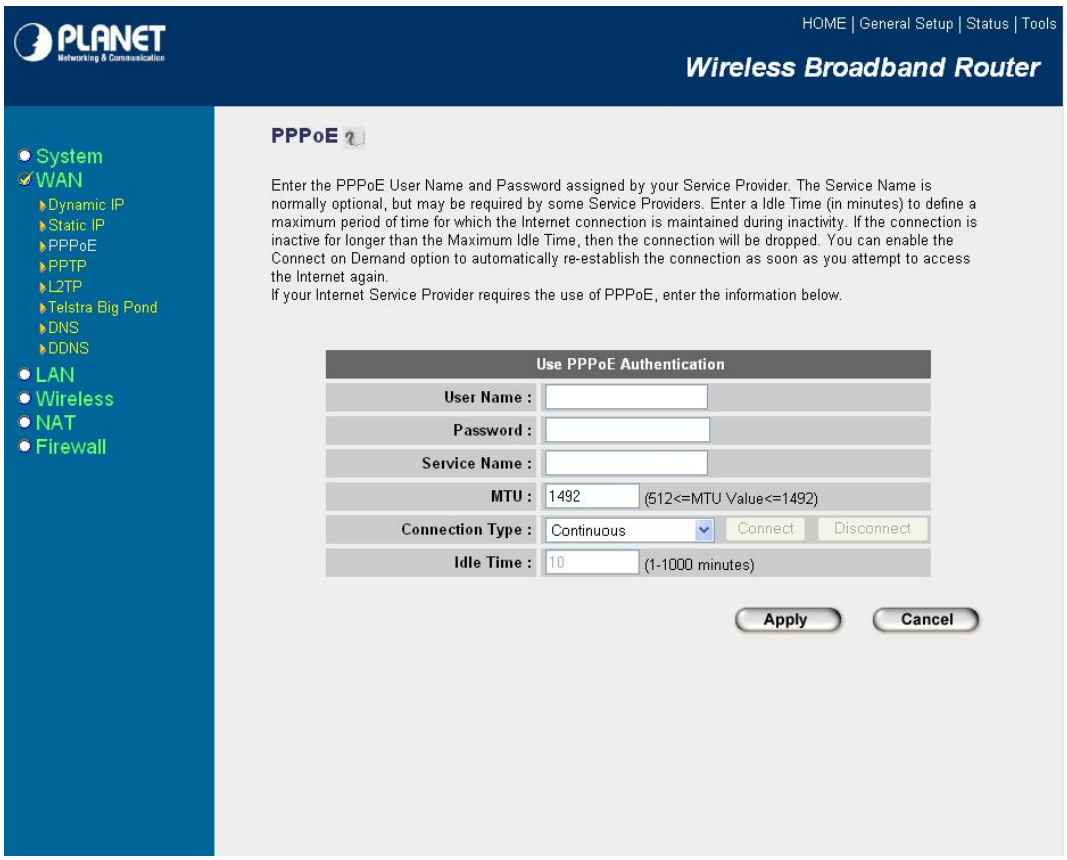
Select Static IP address if your ISP provide a specific IP address Internet connectivity. Your ISP should provide all the information required in this section.



Please refer to the section 4.2.2 for more settings of this option.

5.2.3 PPPoE

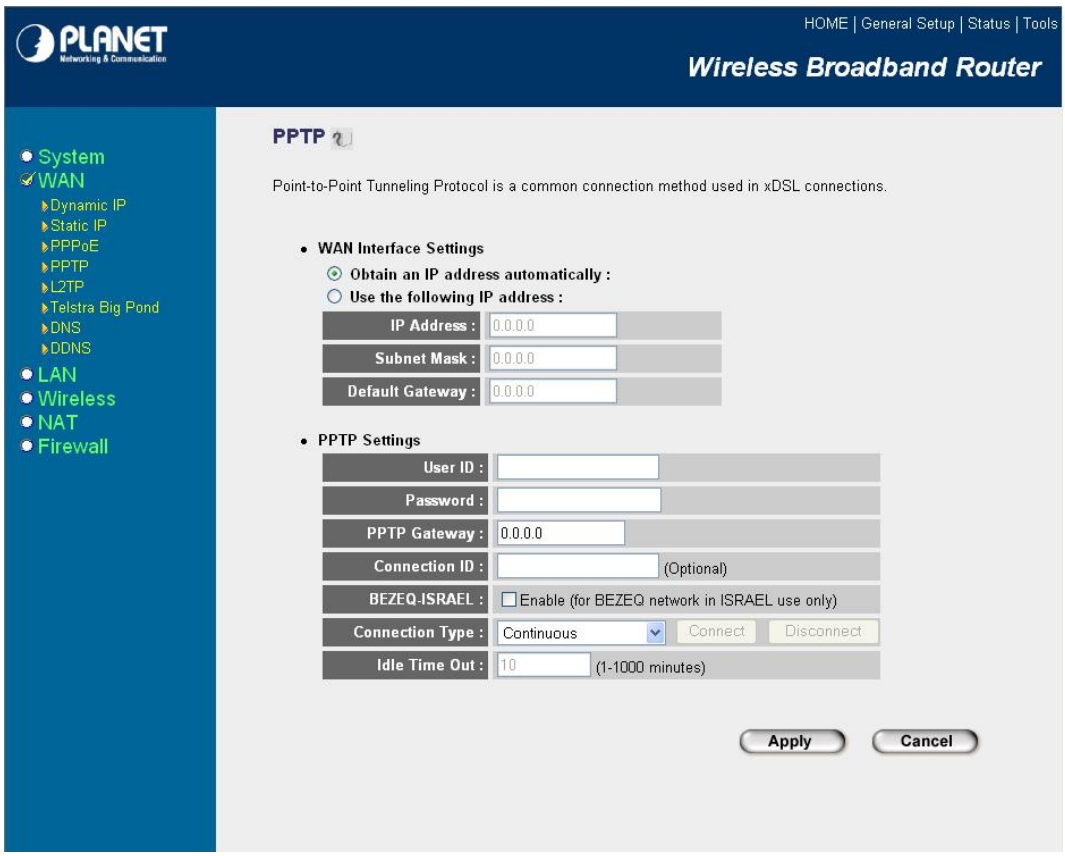
Select PPPoE if your ISP requires PPPoE protocol to connect to the Internet. Your ISP should provide all the information required in this section.



Please refer to the section 4.2.3 to know the detail settings of this option.

5.2.4 PPTP

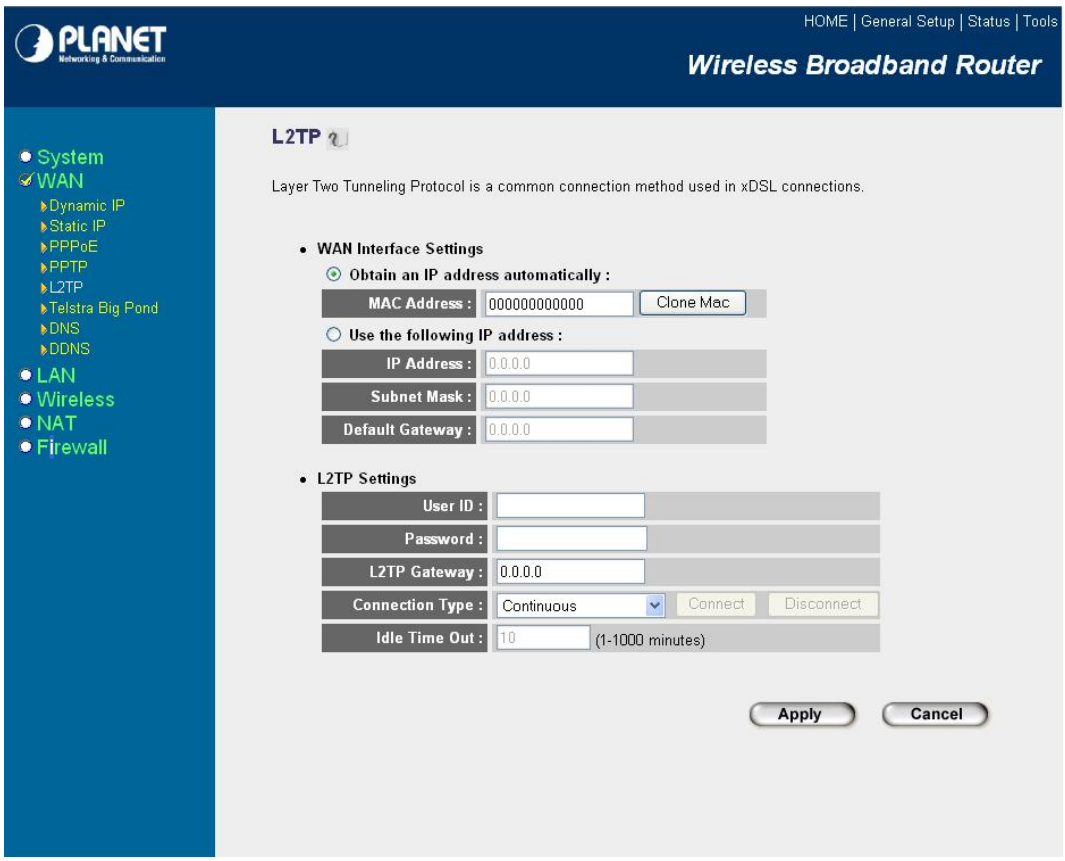
Select PPTP if your ISP requires the PPTP protocol to connect to the Internet. Your ISP should provide all the information required in this section.



Please refer to section 4.2.4 for more settings of this option.

5.2.5 L2TP

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



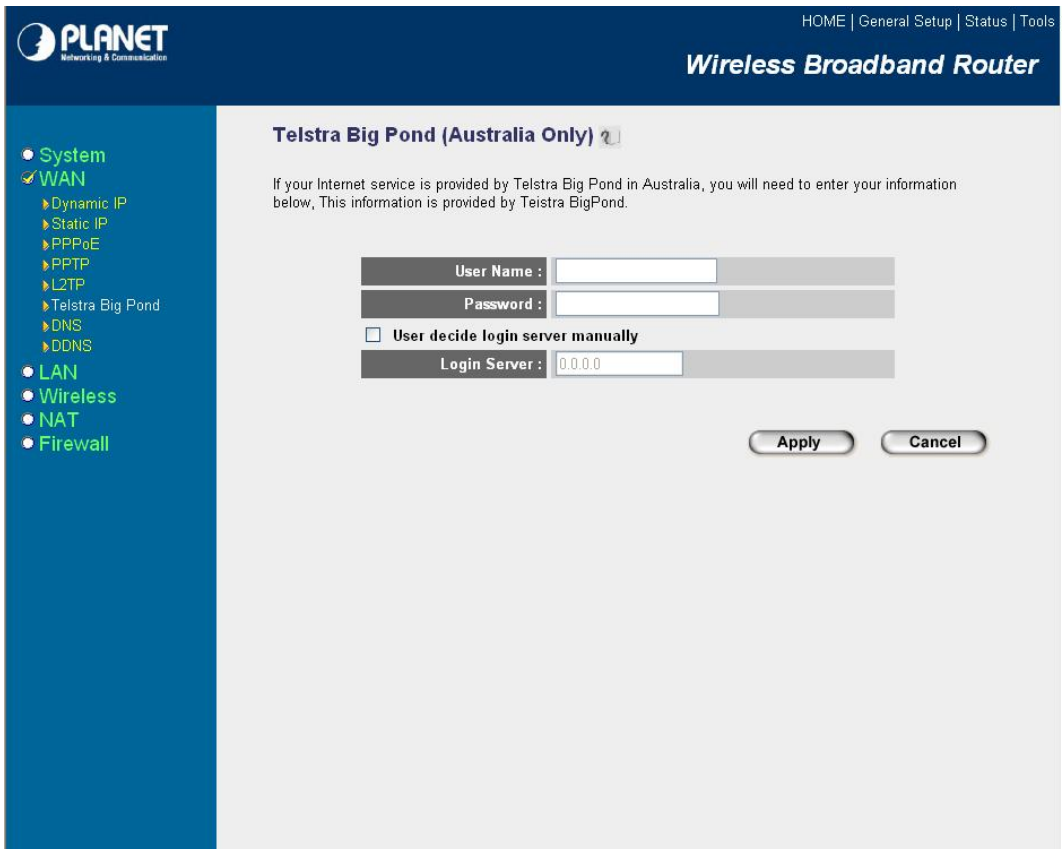
Parameters	Description
Obtain an IP address automatically	The ISP requires you to obtain an IP address by DHCP before connecting to the L2TP server.
Use the following IP address	The ISP gives you a static IP to connect to the L2TP server.
IP Address	This is the IP address that ISP has given to establish a L2TP connection.
Subnet Mask	Enter the Subnet Mask provided by your ISP (e.g. 255.255.255.0)
Gateway	Enter the IP address of the ISP Gateway.
User ID	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.
L2TP Gateway	If your LAN has a L2TP gateway, then enter that L2TP gateway IP address here. If you do not have a L2TP gateway then enter the ISP's Gateway IP address above.
Connection Type	If you select "**Continuous**", the router will always connect to the ISP. If the WAN

	line breaks down and links again, the router will auto-reconnect to the ISP. If you select "**Connect On Demand**", the router will auto-connect to the ISP when someone want to use the Internet and keep connected until the WAN idle timeout. The router will close the WAN connection if the time period that no one is using the Internet exceeds the "Idle Time". If you select "**Manual**", the router will connect to ISP only when you click "Connect" manually from the Web user interface. The WAN connection will not disconnected due to the idle timeout. If the WAN line breaks down and latter links again, the router will not auto-connect to the ISP.
Idle Time Out	You can specify an idle time threshold (minutes) for the WAN port. This means if no packets have been sent (no one using the Internet) throughout this specified period, then the router will automatically disconnect the connection with your ISP.
. **Note**	This "idle timeout" 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.

Click "Apply" when you have finished the configuration above. Congratulations! You have completed the configuration for the L2TP connection. You can start using the router now, if you wish to use some of the advance features supported by this router see chapter below.

5.2.6 Telstra Big Pond

Select Telstra Big Pond if your ISP requires the Telstra Big Pond protocol to connect you to the Internet. Your ISP should provide all the information required in this section. Telstra Big Pond protocol is used by the ISP in Australia.

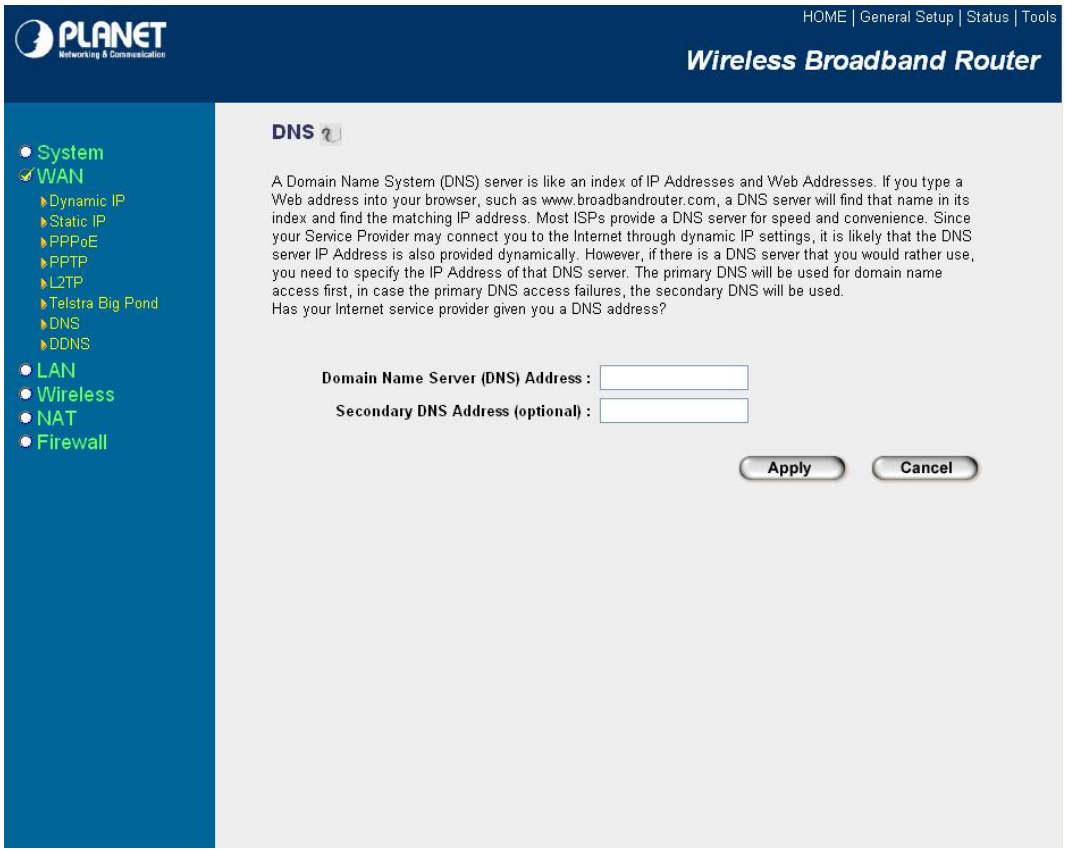


Parameters	Description
User Name	Enter the User Name provided by your ISP for the Telstra Big Pond connection.
Password	Enter the Password provided by your ISP for the Telstra Big Pond connection.
User decide login server manually	Select if you want to assign the IP of Telstra Big Pond's login server manually.
Login Server	The IP of the Login Server.

Click "Apply" button of the screen to save the above configurations. You can now configure other advance sections or start using the router.

5.2.7 DNS

A Domain Name System (DNS) server is like an index of IP addresses and Web addresses. If you type a Web address into your browser, such as www.router.com, a DNS server will find that name in its index and the matching IP address. Most ISPs provide a DNS server for speed and convenience. If your Service Provider connects you to the Internet with dynamic IP settings, it is likely that the DNS server IP address is provided automatically. However, if there is a DNS server that you would rather to use, please specify the IP address of that DNS server here.

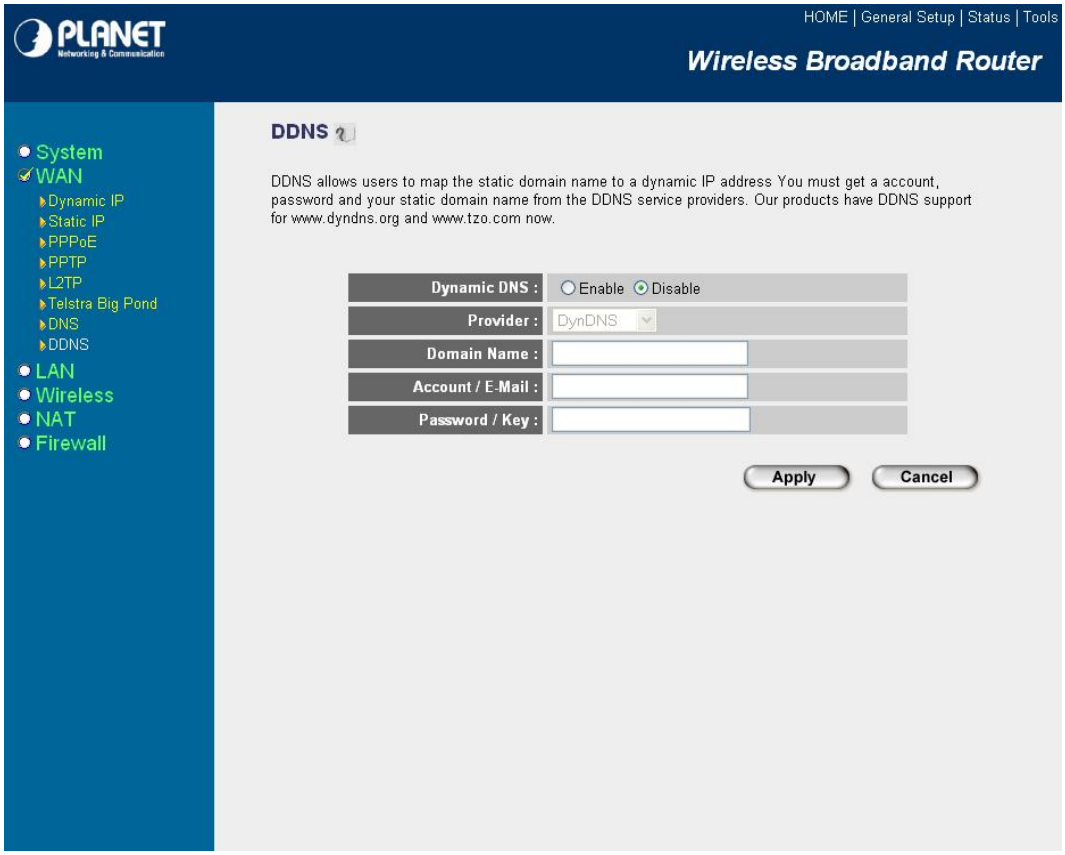


Parameters	Description
Domain Name Server (DNS) Server	This is the ISP's DNS server IP address that they gave you; or you can specify your own preferred DNS server IP address.
Secondary DNS Address (optional)	This is optional. You can enter another DNS server's IP address as a backup. The secondary DNS will be used should the above DNS fail.

Click "Apply" button of the screen to save the above configurations. You can now configure other advance sections or start using the router.

5.2.8 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.

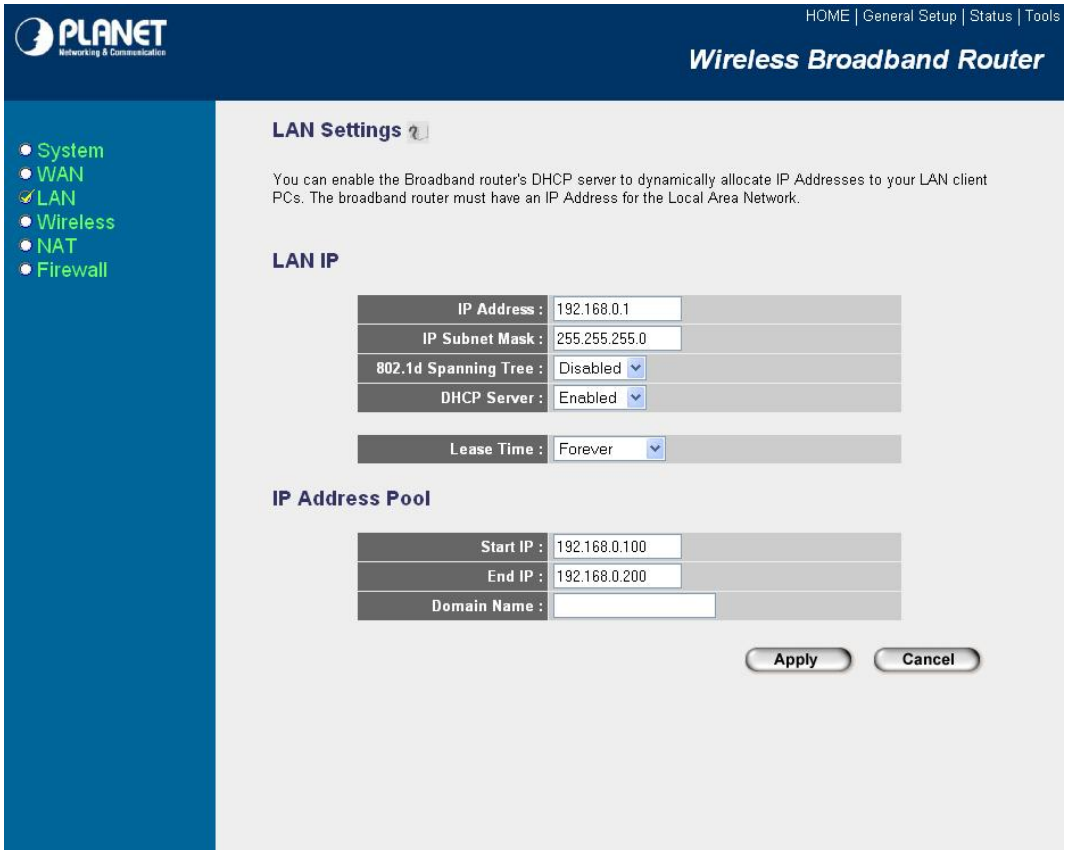


Parameters	Description
Dynamic DNS	Enable/Disable the DDNS function of this router.
Provider	Select a DDNS service provider, the default setting is “DynDNS”.
Domain name	Your static domain name that use DDNS.
Account / E-mail	The account that your DDNS service provider assigned to you.
Password / Key	The password you set for the DDNS service account above.

Click “Apply” button of the screen to save the above configurations. You can now configure other advance sections or start using the router.

5.3 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 of your LAN segment.



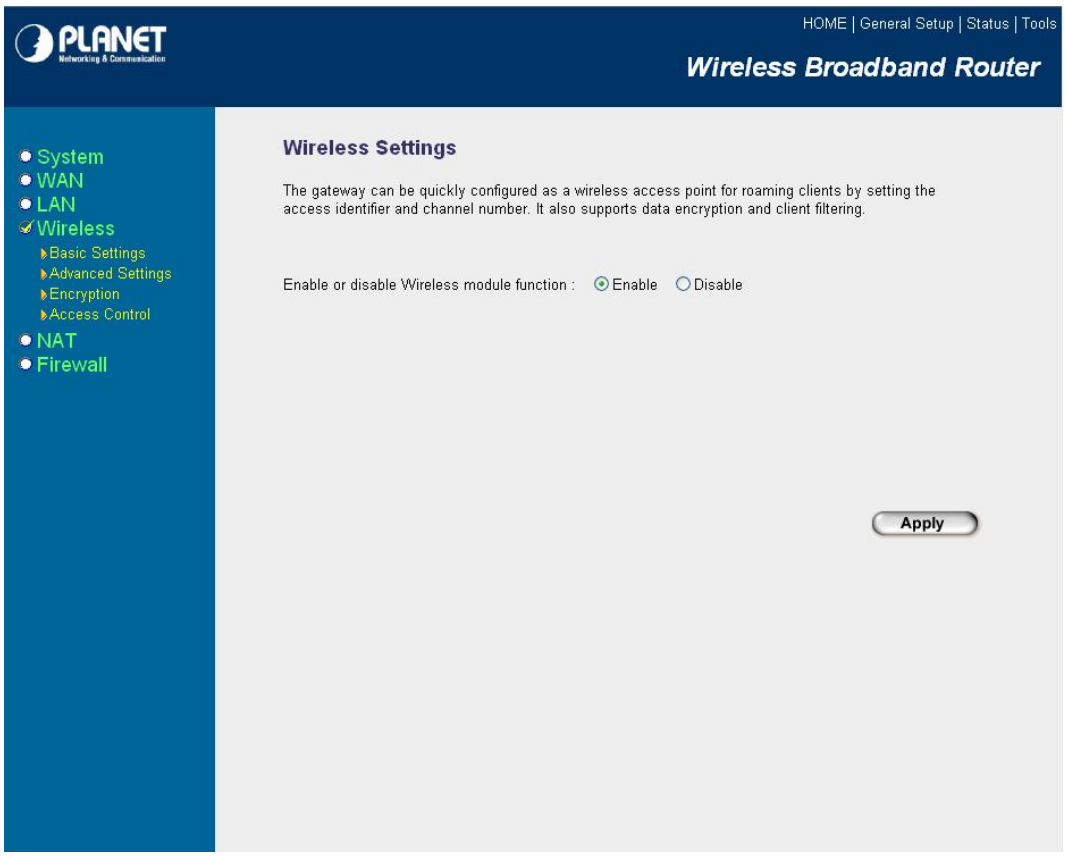
Parameters	Description
LAN IP	
IP Address	Designate the Access Point's IP Address. This IP Address should be unique in your network. The default IP Address is **192.168.0.1**.
Subnet Mask	Specify a Subnet Mask for your LAN segment. The Subnet Mask of the Access Point is fixed and the value is **255.255.255.0**.
802.1d Spanning Tree	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.
DHCP Server	Enable or disable the DHCP Server.
Lease Time	The DHCP Server when enabled will temporarily give your LAN client an IP address. In the Lease Time setting you can specify the time period that the DHCP Server lends an IP address to your LAN clients. The DHCP Server will change your LAN client's IP address when this time threshold period is reached.

IP Address Pool	
Start IP/End IP	You can designate a particular IP address range for your DHCP server to issue IP addresses to your LAN Clients. By default the IP range is from: Start IP **192.168.0.100** to End IP **192.168.0.200**.
Domain Name	You can specify the Domain Name for your Access Point.

Click “Apply” button of the screen to save the above configurations. You can now configure other advance sections or start using the router.

5.4 Wireless

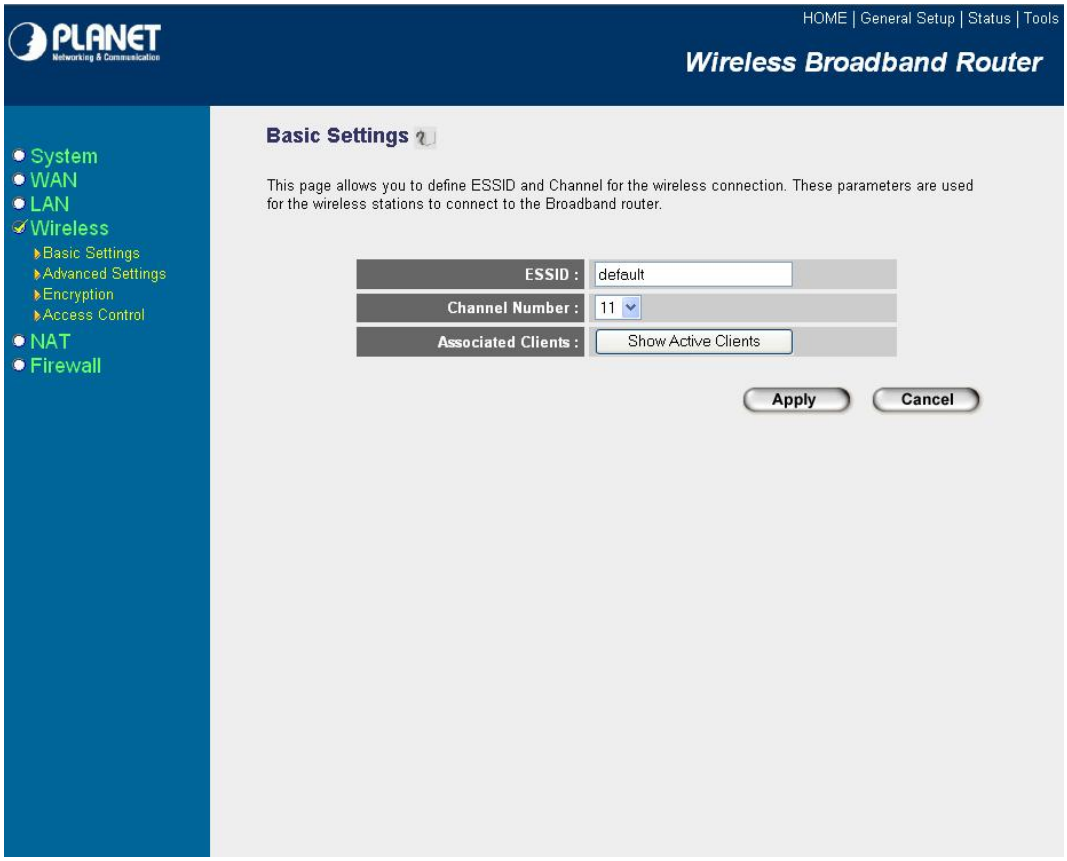
This screen allows you to Enable/Disable WRT-403 wireless function.



Parameters	Description
Enable/Disable	You can select to “**Enable**” or “**Disable**” the Wireless interface. After selected, please click “Apply” to make the settings effect.

5.4.1 Basic Settings

Please assign this WRT-403 an ESSID and Channel Number for your wireless network.



Parameters	Description
ESSID	The ESSID (up to 31 printable ASCII characters) is the unique name identified in a WLAN. The ID prevents the unintentional merging of two co-located WLANs. Please make sure that the ESSID of all stations in the same WLAN network are the same. The default ESSID is "**default**".
Channel Number	Select the appropriate channel from the list provided to correspond with your network settings. Channels differ from country to country. Channel 1-11 (North America) Channel 1-14 (Japan) Channel 1-13 (Europe)
Associated Clients	Click "**Show Active Clients**" button, then a "Active Wireless Client Table" will pop up as below. You can see the status of all active wireless stations that are connecting to the access point.

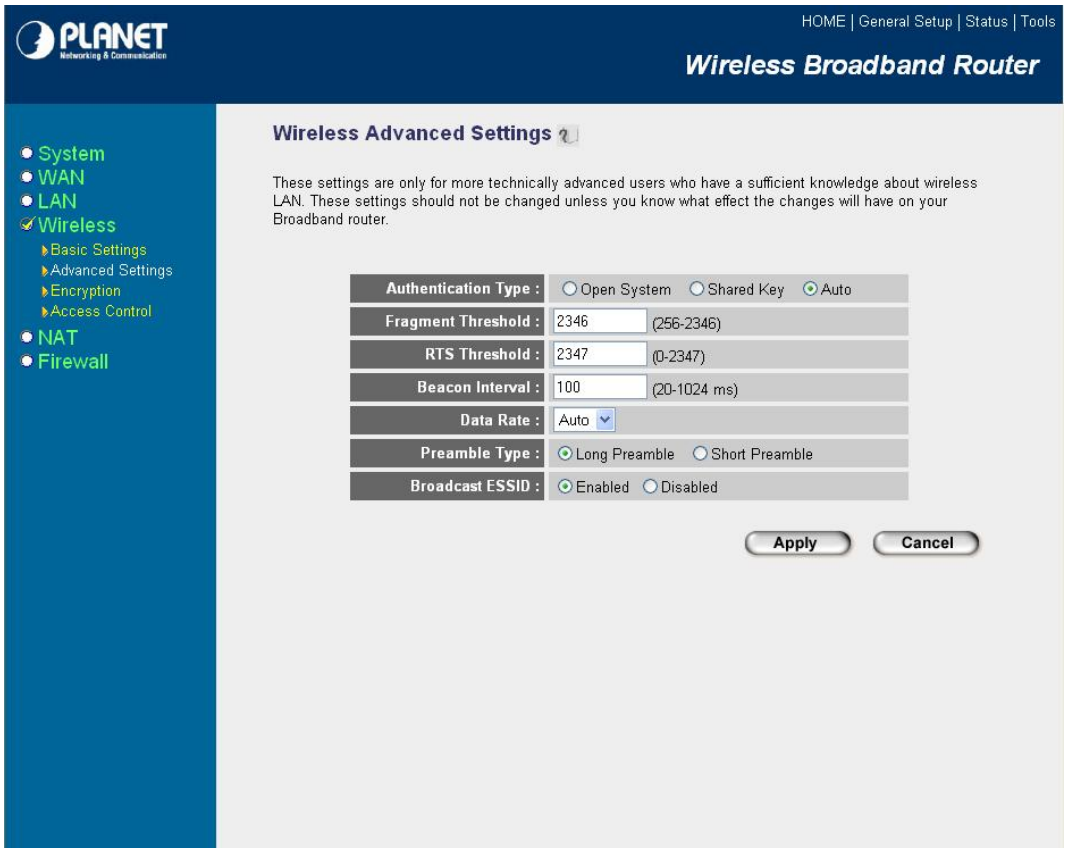
Click "Apply" button to save the above configurations. You can now configure other advance sections or start using the router.

"Active Wireless Client Table" records the status of all active wireless stations that are connecting to the access point. You can lookup the MAC Address, Number of Transmitted Packets, Number of Received Packets and Encryption Status of each active wireless client in this table.

Parameters	**Description**
MAC Address	MAC address of this active wireless station.
Tx Packet	The number of transmitted packets that are sent out from this active wireless station.
Rx Packet	The number of received packets that are received by this active wireless station.
TX Rate	The transmission rate in Mbps.
Power Saving	Shows if the wireless client is in Power Saving mode.
Expired Time	The time in second before dissociation. If the wireless keeps idle long than the expired time, this access point will dissociate it. The wireless client station has to associate again when it become active.
Refresh	Refresh the "Active Wireless Client Table".
Close	Close "Active Wireless Client Table" window.

5.4.2 Advance Settings

You can set advanced parameters of this WRT-403. The parameters include Authentication Type, Fragment Threshold, RTS Threshold, Beacon Interval, Data Rate, Preamble Type, and Broadcast ESSID. You should not change these parameters unless you know what effect the changes will have on WRT-403. When configuration finished, please click “Apply” to save the settings.

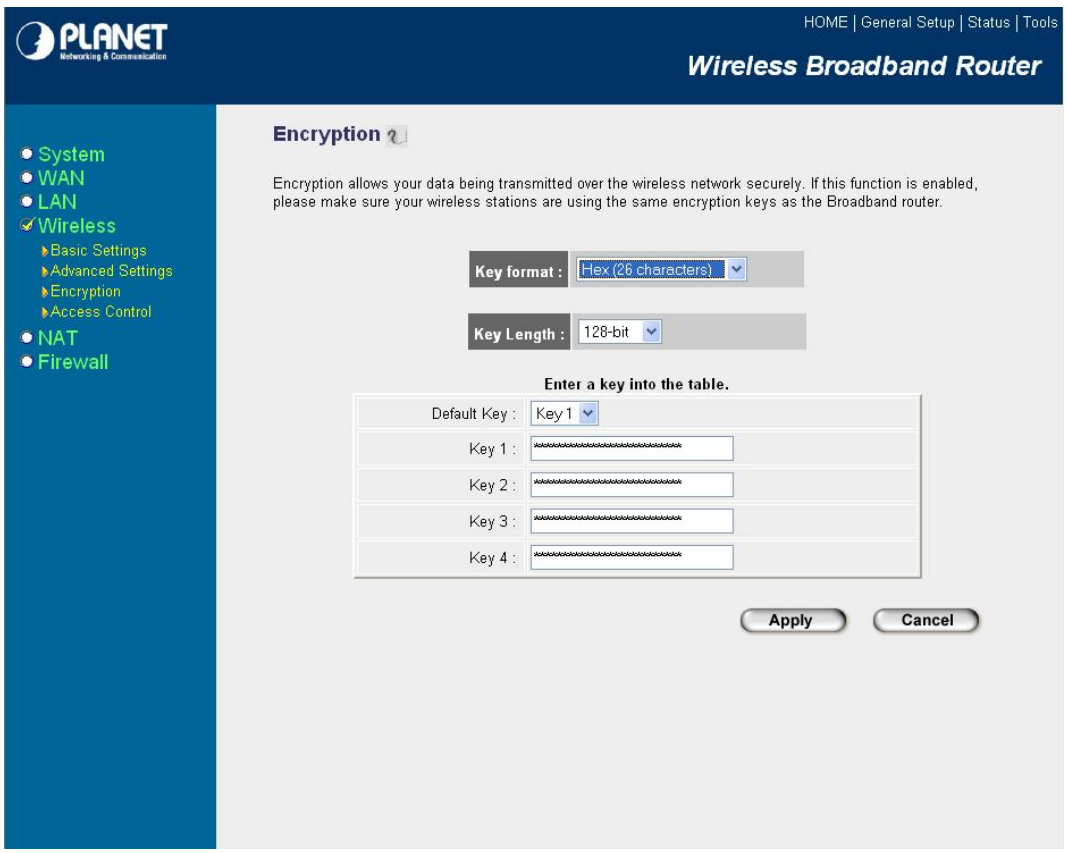


Parameters	Description
Authentication Type	There are two authentication types: “**Open System**” and “**Shared Key**”. When you select “**Open System**”, wireless stations can associate with this access point without WEP encryption. When you select “**Shared Key**”, you should also setup WEP key in the “Encryption” page and wireless stations should use WEP encryption in the authentication phase to associate with this access point. If you select “**Auto**”, the wireless client can associate with this WRT-403 by using any one of these two authentication types.
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 the RTS threshold, the access point will not use the RTS/CTS mechanism to send this packet.

Beacon Interval	The interval of time that this access point broadcast a beacon. Beacon is used to synchronize the wireless network.
Data Rate	The Data Rate is the rate of data transmission. The WRT-403 will use the highest possible selected transmission rate to transmit the data packets.
Preamble Type	Preamble type defines the length of CRC block in the frames during the wireless communication. "**Short Preamble**" is suitable for high traffic wireless network. "**Long Preamble**" can provide more reliable communication.
Broadcast ESSID	If you enable "Broadcast ESSID", every wireless station located within the coverage of this access point can discover this WRT-403 easily. If you are building a public wireless network, enabling this feature is recommended. In private network, disabling "Broadcast ESSID" can provide better security.

5.4.3 Encryption

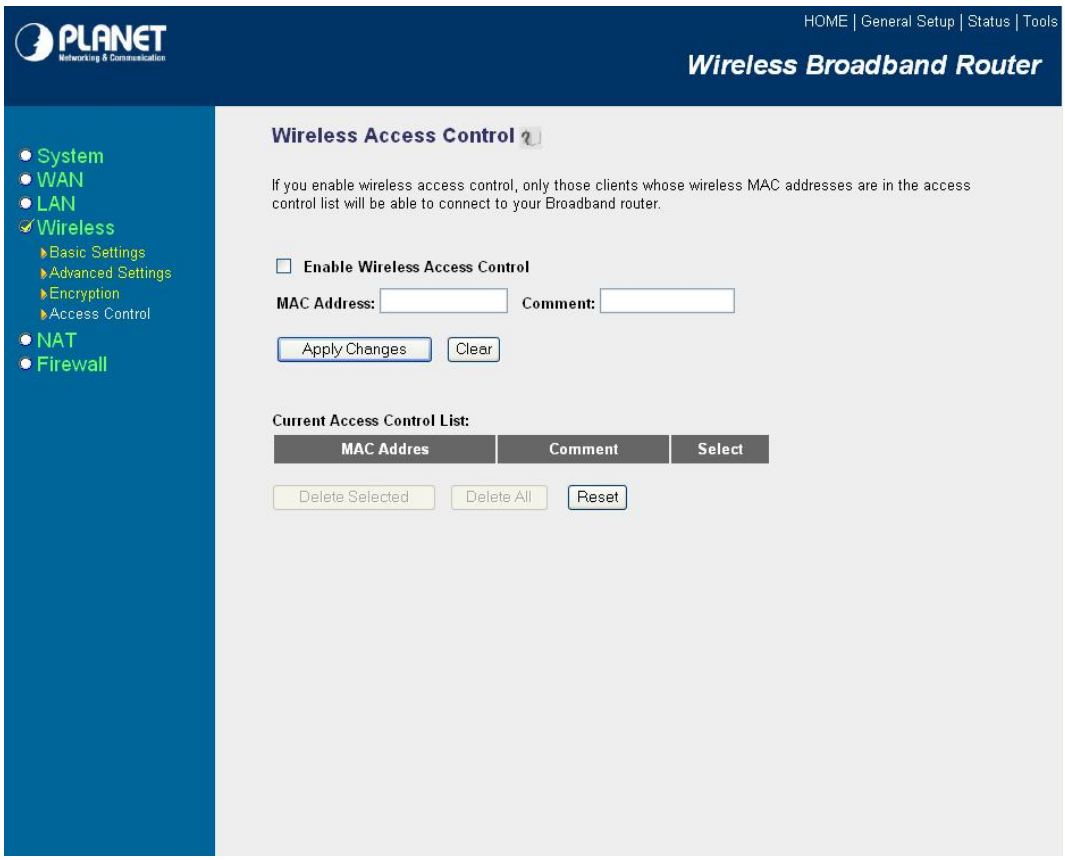
WEP is an authentication algorithm, which protects authorized Wireless LAN users against eavesdropping. The Authentication type and WEP key of wireless stations must be the same with the WRT-403. It has support 64/128-bit WEP Encryption function. With those functions, your data will be transmitted over the wireless network securely. In default, this function is "Disable". When configuration finished, please click "Apply" to save the settings.



Parameters	Description
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 Length	The selections in this setting are use to enable or disable the WEP function and select the key format to 64bit or 128bit. Default is “Disable”.
Default Key	Select one of the four WEP keys to encrypt your data. Only the key you selected in the “Default Key” will take effect.
Key 1 - Key 4	The WEP keys 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 10-digit ASCII characters as the encryption keys.

5.4.4 Access Control

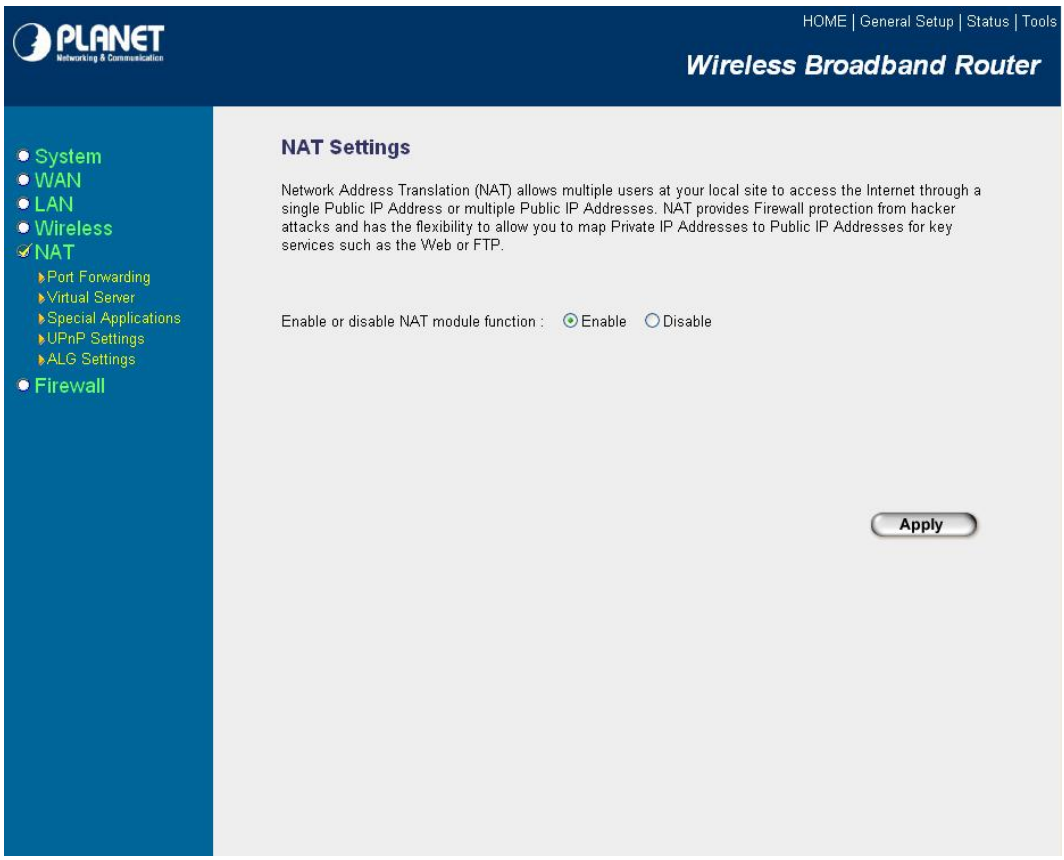
WRT-403 provides MAC Address Filtering, which prevents the unauthorized MAC Addresses to access your wireless network.



Parameters	Description
Enable Wireless Access Control	Please click “Enable Wireless Access Control” first. Fill in the “MAC Address” and “Comment” of the wireless station will be added and then click “Apply Changes”. Then this wireless station will be added into the “Current Access Control List”. If you find any typo before adding it and want to retype again. Just click “Clear” and both “MAC Address” and “Comment” fields will be cleared.
Current Access Control List	This list records the MAC addresses of wireless stations you want to allow to access your network. The “Comment” field is the description of the wireless station associated with the “MAC Address” and is helpful for you to recognize the wireless station.
Delete Selected	If you want to remove some MAC address from the “Current Access Control List”, select the MAC addresses you want to remove in the list and then click “Delete Selected”.
Delete All	If you want remove all MAC addresses from the list, just click this button.
Reset	Click “Reset” will clear your current selections.

5.5 NAT

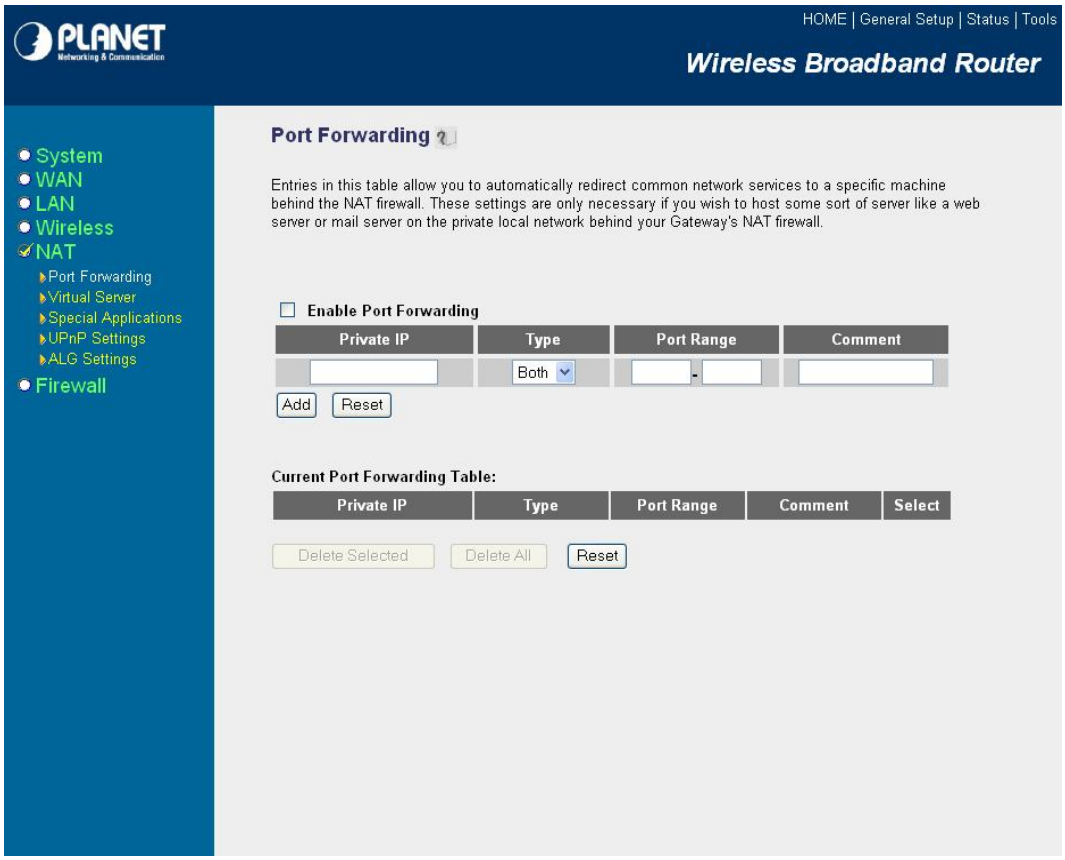
Network Address Translation (NAT) allows multiple users at your local site to access the Internet via a single legal IP Address. NAT provides Firewall protection from hacker attacks and has the flexibility to allow you to map Private IP Addresses to Public IP Addresses for key services such as Websites and FTP. To meet various field applications, WRT-403 NAT function can be disabled to work as a regular router. If NAT is disabled, all LAN side workstations must have legal IP addresses for Internet access. If the router is used for routing application, not for Internet access, then the NAT function can be disabled.



Parameters	Description
Enable/Disable	You can select to enable or disable the NAT function. After selected, please click “Apply” to make the settings effect.

5.5.1 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.

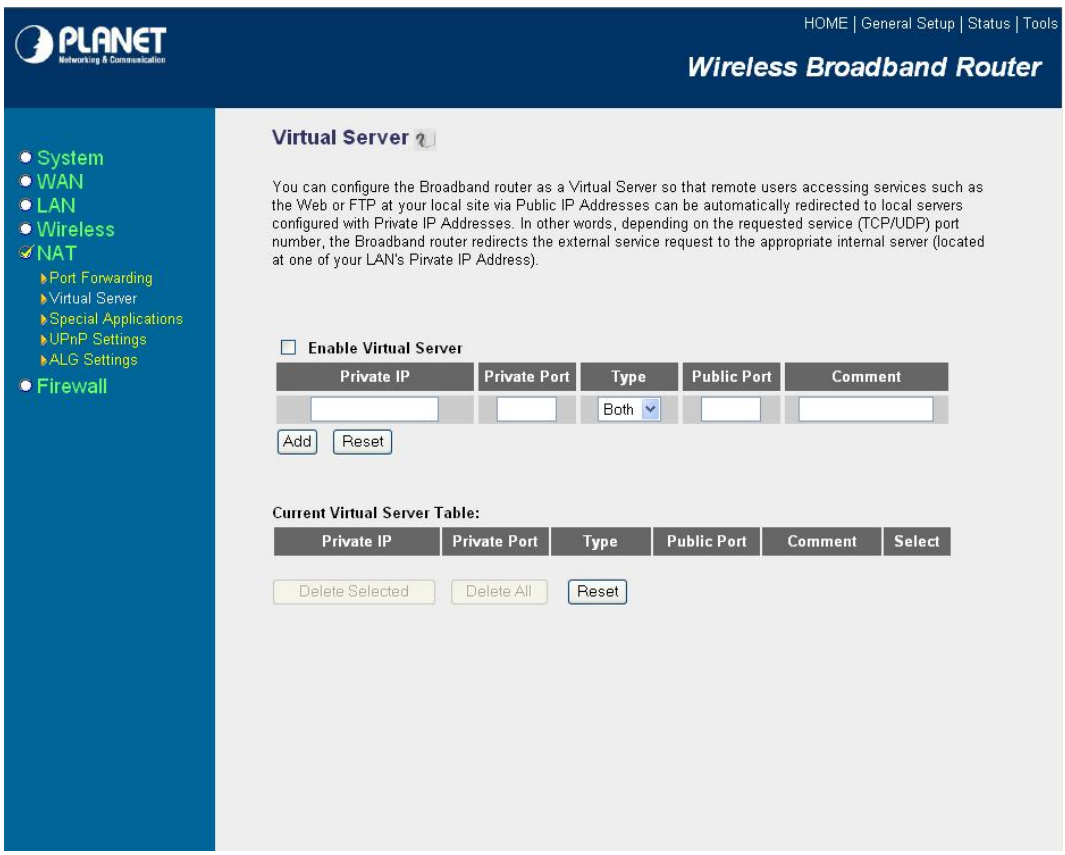


Parameters	Description
Enable Port Forwarding	Enable Port Forwarding.
Private IP	This is the private IP of the server behind the NAT firewall. Note: You need to give your LAN PC clients a fixed/static IP address for Port Forwarding to work properly.
Type	This is the protocol type to be forwarded. You 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.
Add	Fill in the "Private IP", “Type”, “Port Range” and "Comment" of the setting to be added and then click "Add". Then this Port Forwarding setting will be added into the "Current Port Forwarding Table" below. If you find any typo before adding it and want to retype again, just click "Clear" and the fields will

	be cleared.
Reset	Click “Reset” will clear your current settings to allows you to enter again.
Current Port Forwarding Table	
Delete Selected	If you want to remove some MAC address from the “Current Access Control List”, select the MAC addresses you want to remove in the table and then click “Delete Selected”.
Delete All	If you want remove all MAC addresses from the table, just click this button.
Reset	Click “Reset” will clear your current selections.

5.5.2 Virtual Server

Use the Virtual Server function when you need to have different servers in your LAN to handle many services and Internet applications (e.g. Email, FTP, Web server etc.) to the Internet. Computers use numbers called port numbers to recognize a particular service/Internet application type. The Virtual Server allows you to re-direct a particular service port number (from the WAN Port) to a particular LAN private IP address as its service port number. (See Glossary for an explanation on Port number).

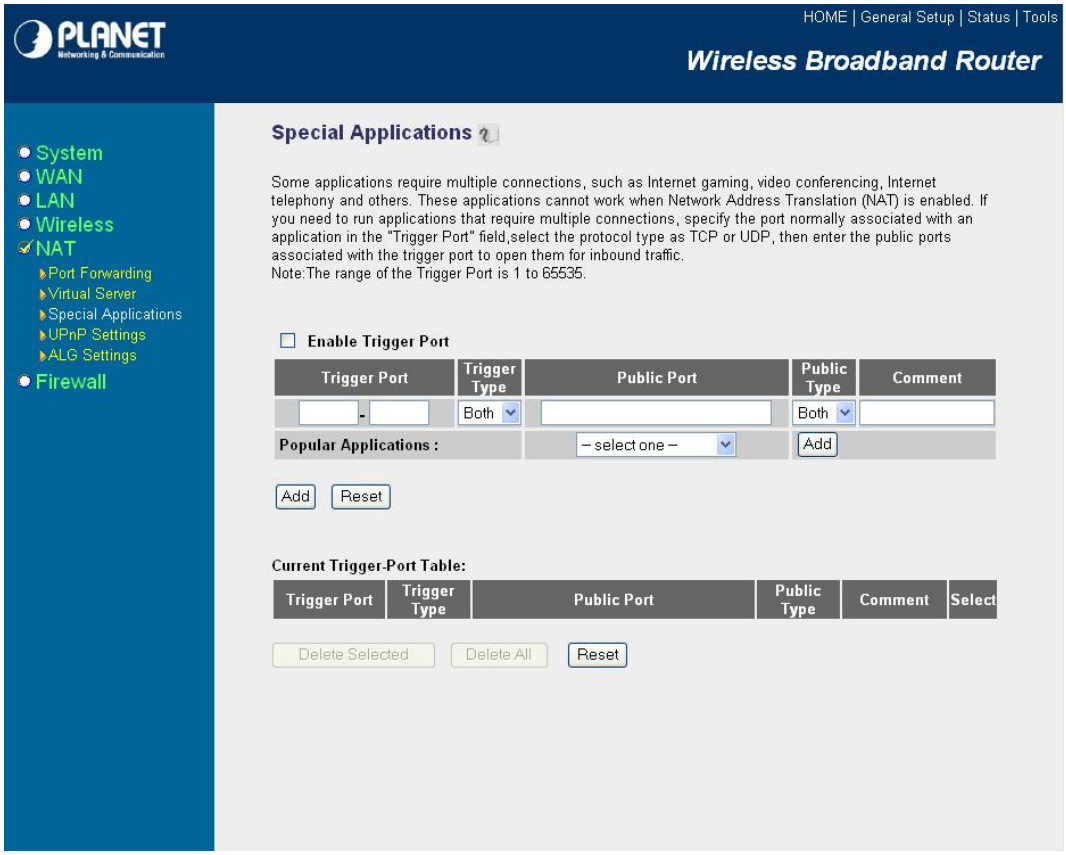


Parameters	Description
Enable Virtual Server	Enable Virtual Server.
Private IP	This is the LAN client/host IP address that the Public Port number packet will be sent to.
Note	---------- You need to give your LAN PC clients a fixed/static IP address for Virtual Server to work properly. ----------
Private Port	This is the port number (of the above Private IP host) that the below Public Port number will be changed to when the packet enters your LAN (to the LAN Server/Client IP).
Type	Select the port number protocol type (**TCP**, **UDP** or **Both**). If you are unsure, then leave it to the default both protocols.
Public Port	Enter the service (service/Internet application) port number from the Internet that will be re-directed to the above Private IP address host in your LAN.
Note	---------- Virtual Server function will have priority over the DMZ function if there is a conflict between the Virtual Server and the DMZ settings. ----------
Add	Fill in the "Private IP", "Private Port", "Type", “Public Port” and "Comment" of the setting to be added and then click "Add". Then this Virtual Server setting will be added into the "Current Virtual Server Table" below. If you find any typo before adding it and want to retype again, just click "Clear" and the fields will be cleared.
Reset	Click “Reset” will clear your current settings to allows you to enter again.
Current Virtual Server Table	
Delete Selected	If you want to remove some items from the “Current Virtual Server Table”, select the MAC addresses you want to remove in the table and then click “Delete Selected”.
Delete All	If you want remove all items of the table, just click this button.
Reset	Click “Reset” will clear your current selections.

Click “Apply” button to save the above configurations. You can now configure other advance sections or start using the router.

5.5.3 Special Applications

Some applications require multiple connections, such as Internet games, video conferencing, Internet telephony and others. In this section you can configure the router to support multiple connections for these types of applications.



Parameters	Description
Enable Trigger Port	Enable the Special Application function.
Trigger Port	This is the out going (Outbound) range of port numbers for this particular application.
Trigger Type	Select whether the outbound port protocol are "**TCP**", "**UDP**" or "**Both**".
Public Port	Enter the In-coming (Inbound) port or port range for this type of application (e.g. 2300-2400, 47624).
Note	Individual port numbers are separated by a comma (e.g. 47624, 5775, 6541 etc.). To input a port range use a "dash" to separate the two port number range (e.g. 2300-2400).
Public Type	Select the Inbound port protocol type: "TCP", "UDP" or both.
Comment	The description of this setting.
Popular applications	This section lists the more popular applications that require multiple

	connections. Select an application from the Popular Applications selection. Once you have selected an application, click the “Add” button in right side of this setting. This will automatically copy the Port Trigger information required for this popular application in into the input fields.
Add	Add the settings into the “Current Trigger Port Table”.
Reset	Click “Reset” will clear your current settings to allows you to enter again.
Current Trigger Port Table	
Delete Selected	If you want to remove some items from the “Current Trigger Port Table”, select the MAC addresses you want to remove in the table and then click “Delete Selected”.
Delete All	If you want to remove all items from the table, just click this button.
Reset	Click “Reset” will clear your current selections.

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.

Example: Special Applications

If you need to run applications that require multiple connections, then specify the port (outbound) normally associated with that application in the "Trigger Port" field. Then select the protocol type (TCP or UDP) and enter the public ports associated with the trigger port to open them up for inbound traffic.

Example:

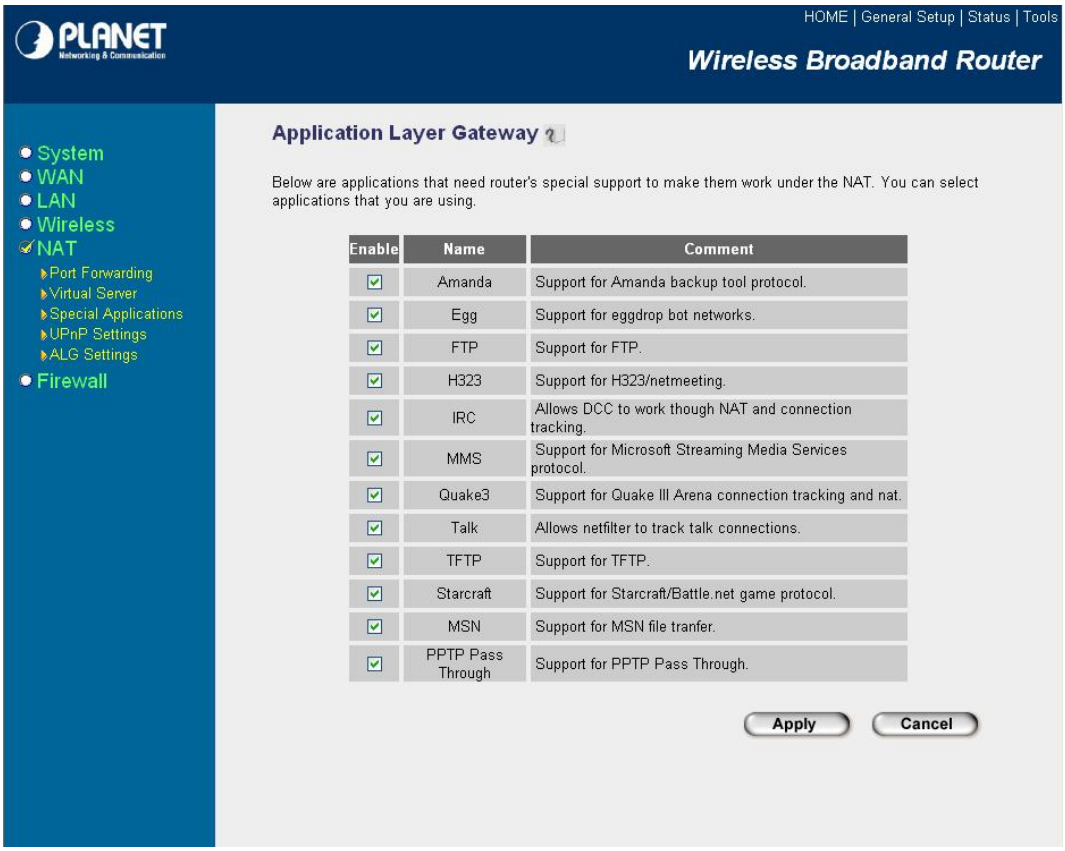
ID	Trigger Port	Trigger Type	Public Port	Public Type	Comment
1	28800	UDP	2300-2400, 47624	TCP	MSN Game Zone
2	6112	UDP	6112	UDP	Battle.net

In the example above, when a user trigger’s port 28800 (outbound) for MSN Game Zone then the router will allow incoming packets for ports 2300-2400 and 47624 to be directed to that user.

Note: Only one LAN client can use a particular special application at a time.

5.5.4 ALG Settings

You can select applications that need “Application Layer Gateway” to support.

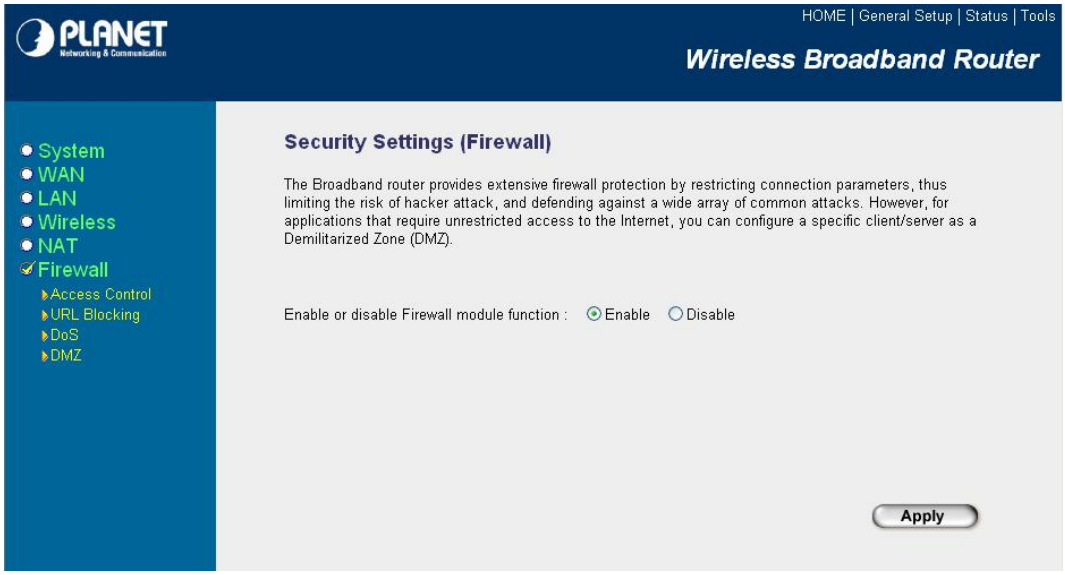


Parameters	Description
Enable	You can select to enable “Application Layer Gateway” of an application and then the router will let that application correctly pass though the NAT gateway.

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.

5.6 Firewall

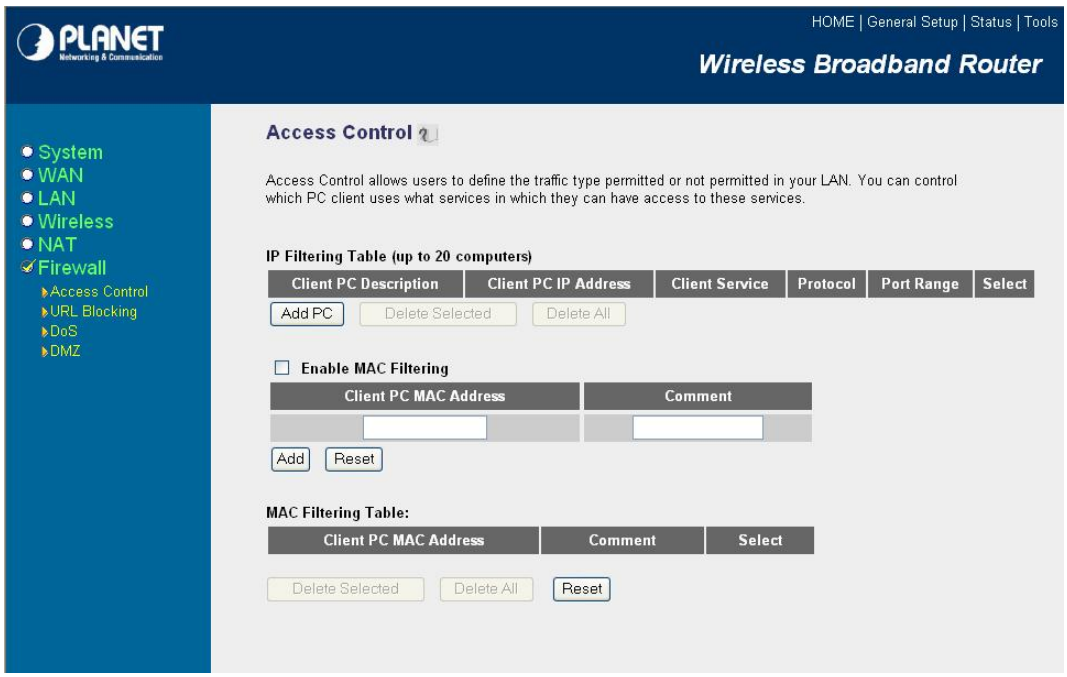
WRT-403 provides extensive firewall protection by restricting connection parameters, thus limiting the risk of hacker attack, and defending against a wide array of common Internet attacks. However, for applications that require unrestricted access to the Internet, you can configure a specific client/server as a Demilitarized Zone (DMZ).



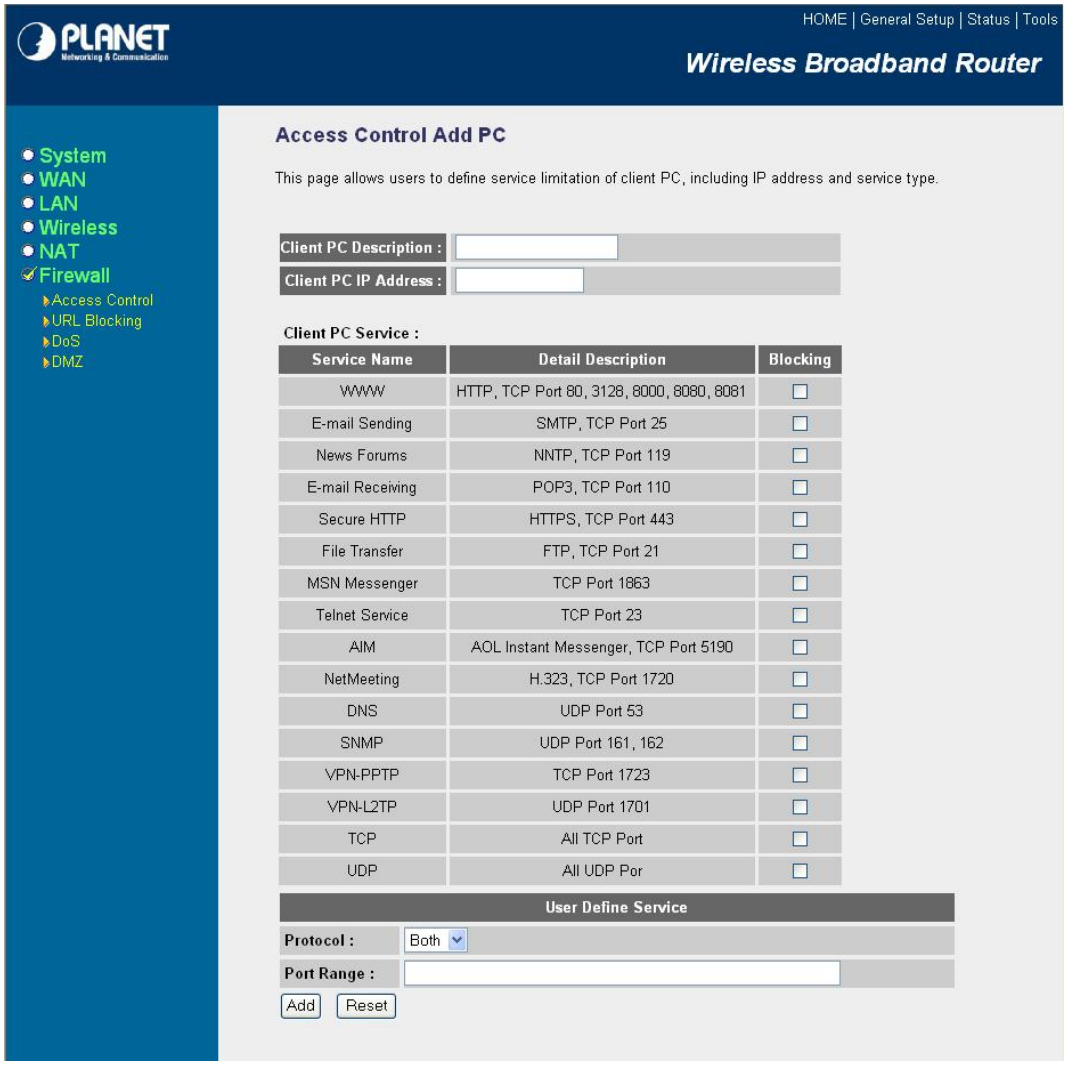
Parameters	Description
Enable/Disable	You can select to enable or disable the firewall function. After selected, please click “Apply” to make the settings effect.

5.6.1 Access Control

If you want to restrict users from accessing certain Internet applications/services (e.g. Internet websites, email, FTP etc.), this is the place to set that configuration. Access Control allows network administrator to define the traffic type permitted in your LAN. You can control which PC client can have access to these services.



Parameters	Description
IP Filtering Table	Fill “IP Filtering Table” to filter PC clients by IP.
Add PC	You can click “Add PC” to add an access control rule for users by IP addresses. After click this button, you will see the screen as below.
Remove PC	If you want to remove some PCs from the "IP Filtering Table", select the PC you want to remove in the table and then click "Delete Selected".
Delete All	If you want to delete all PCs. Please click this button.
Filter client PC by MAC address	Check “Enable MAC Filtering” to enable MAC Filtering.
Add PC	Fill in “Client PC MAC Address” and “Comment” of the PC that is allowed to access the Internet, and then click “Add”. If you find any typo before adding it and want to retype again, just click "Reset" and the fields will be cleared.
Remove PC	If you want to remove some PC from the "MAC Filtering Table", select the PC you want to remove in the table and then click "Delete Selected". If you want remove all PCs from the table, just click "Delete All" button. If you want to clear the selection and re-select again, just click “Reset”.



Parameters	Description
Client PC Description	The description for this client PC rule.
Client PC IP Addresses	Enter the IP address range that you wish to apply this Access Control rule. This is the user's IP address that you wish to setup an Access Control rule. You can select a range of users simply by inputting the starting users' IP address and the last user's IP address in the appropriate boxes. If you want to select only one user then input the user's IP address in both boxes.
Note	You need to give your LAN PC clients a fixed/static IP address for the Access Control rule to work properly
Client PC Service	You can block the clients from accessing some Internet services by checking the services you want to block.
Protocol	This allows you to select **UDP**, **TCP** or **Both** protocol type you want to block.
Port Range	You can assign up to five port ranges. The router will block clients from

	accessing Internet services that use these ports.
Add	Click “Add” to save the settings.
Reset	Click “Reset” to clear all fields.

5.6.2 URL Blocking

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

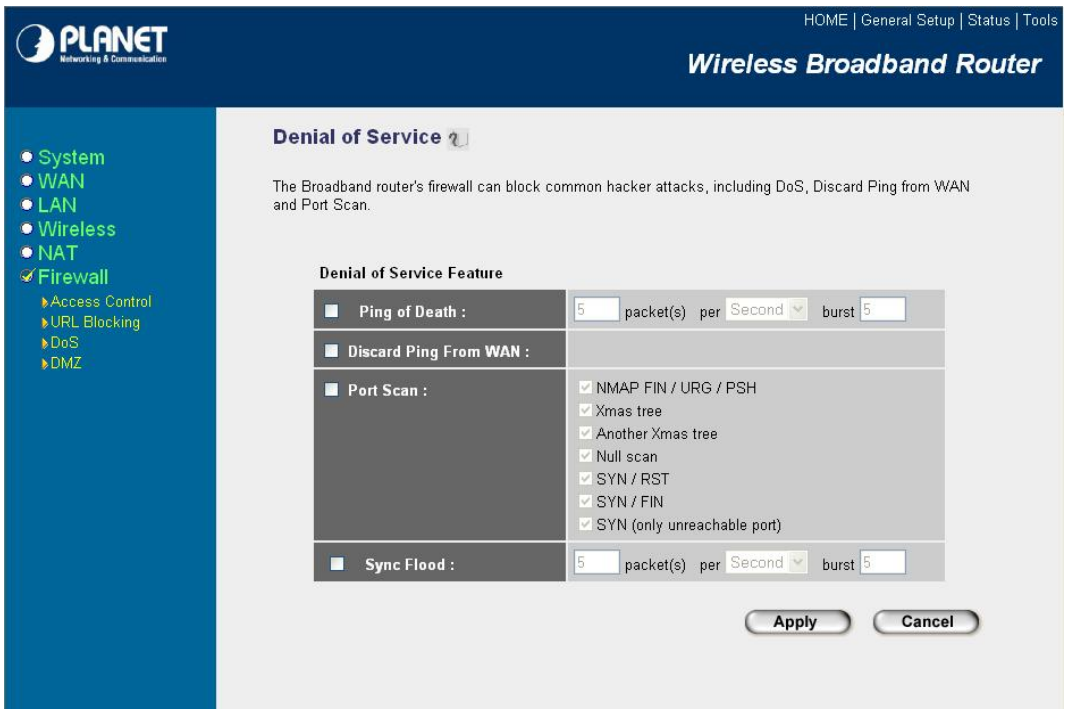
Parameters	Description
Enable URL Blocking	Enable/disable URL Blocking.
Add URL / Keyword	Fill in “URL / Keyword” and then click “Add”. You can enter the full URL address or the keyword of the web site you want to block. If you find any typo before adding it and want to retype again, just click "Reset" and the field will be cleared.
Remove URL / Keyword	If you want to remove some URL keyword from the "Current URL Blocking Table", select the URL keyword you want to remove in the table and then click "Delete Selected". If you want remove all URL keyword from the table, just click "Delete All" button. If you want to clear the selection and re-select again, just click “Reset”.

5.6.3 DoS

WRT-403's firewall can block common hacker attacks, including Denial of Service, Ping of Death, Port Scan and Sync Flood. If Internet attacks occur the router can log the events.

Parameters	Description
Ping of Death	Protections from Ping of Death attack.
Discard Ping From WAN	The router's WAN port will not respond to any Ping requests.
Port Scan	Protection the router from Port Scan.
Sync Flood	Protection the router from Sync Flood attack.
Advance Settings	If you want to configure the details of each setting above. Please click this button, then you will see the detail configure screen as below. Please make sure what the effect of the settings will affect before your adjustment.

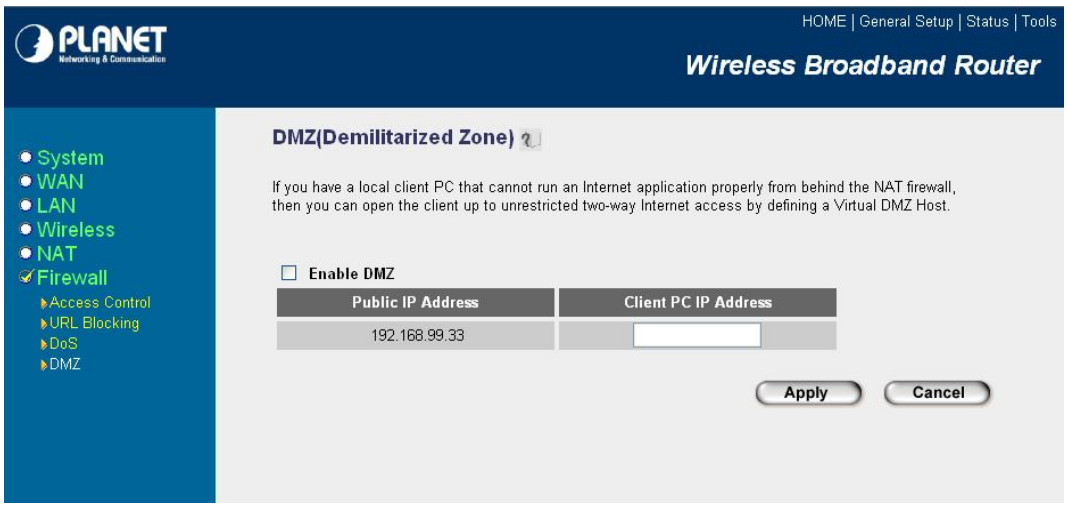
Click "Apply" to save the above configurations. You can now configure other advance sections or start using the router.



5.6.4 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 from your WAN port IP address to a particular IP address in your LAN. The difference between the virtual server and the DMZ function is

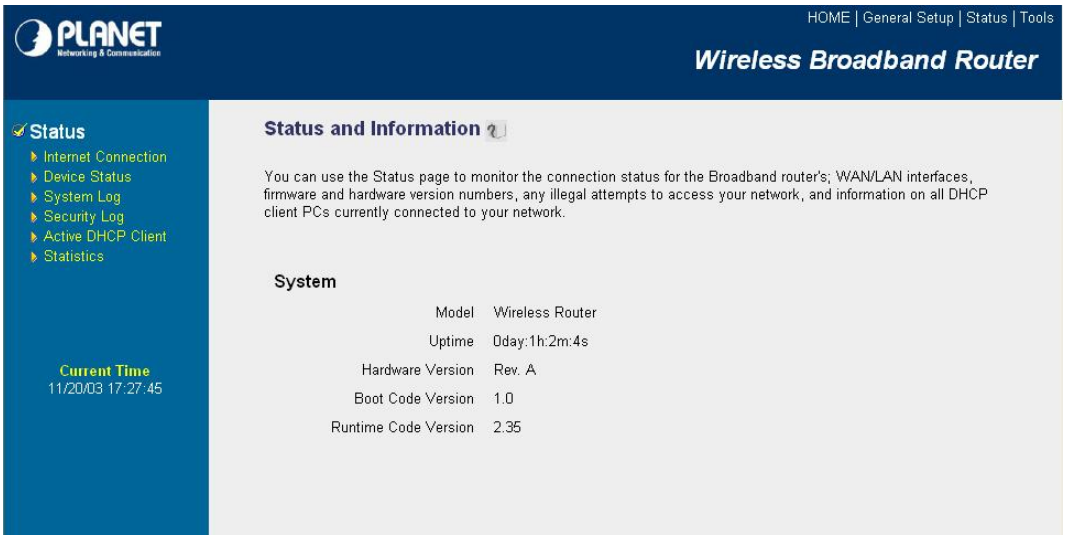
that the virtual server re-directs a particular service/Internet application (e.g. FTP, websites) to a particular LAN client/server, whereas DMZ re-directs all packets (regardless of services) to one particular LAN client/server.



Parameters	Description
Enable DMZ	Enable/disable DMZ.
Note	If there is a conflict between the Virtual Server and the DMZ setting, then Virtual Server function will have priority over the DMZ function.
Public IP Address	The IP address of the WAN port or any other Public IP addresses given to you by your ISP.
Client PC 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.

5.7 Status

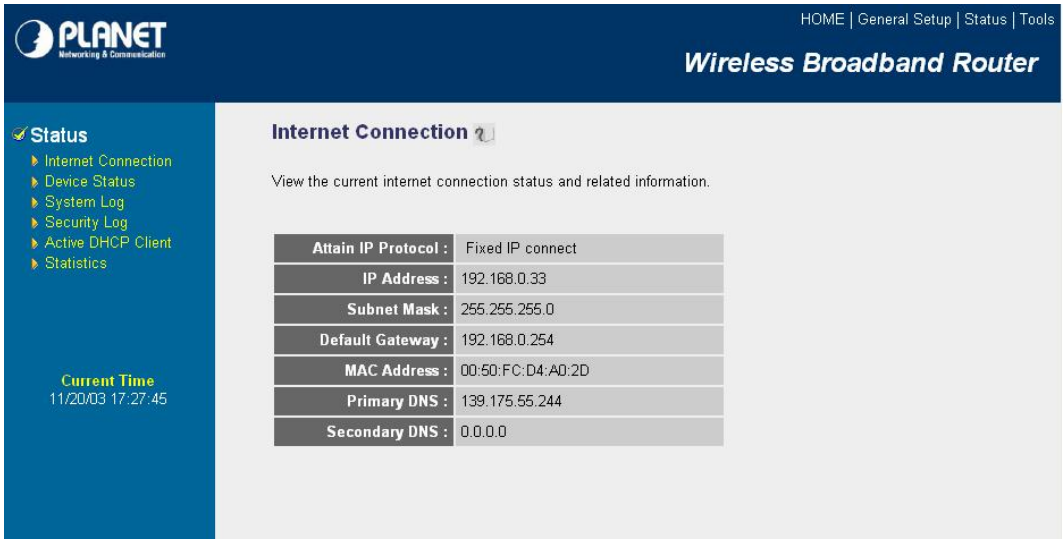
The Status section allows you to monitor the current status of your router. You can use the Status page to monitor the connection status of WRT-403's WAN/LAN interfaces, the current firmware and hardware version numbers, any illegal attempts to access your network, and information on all DHCP client PCs currently connected to your network.



Select one of the six status selections and proceed to the manual's relevant sub-section.

5.7.1 Internet Connection

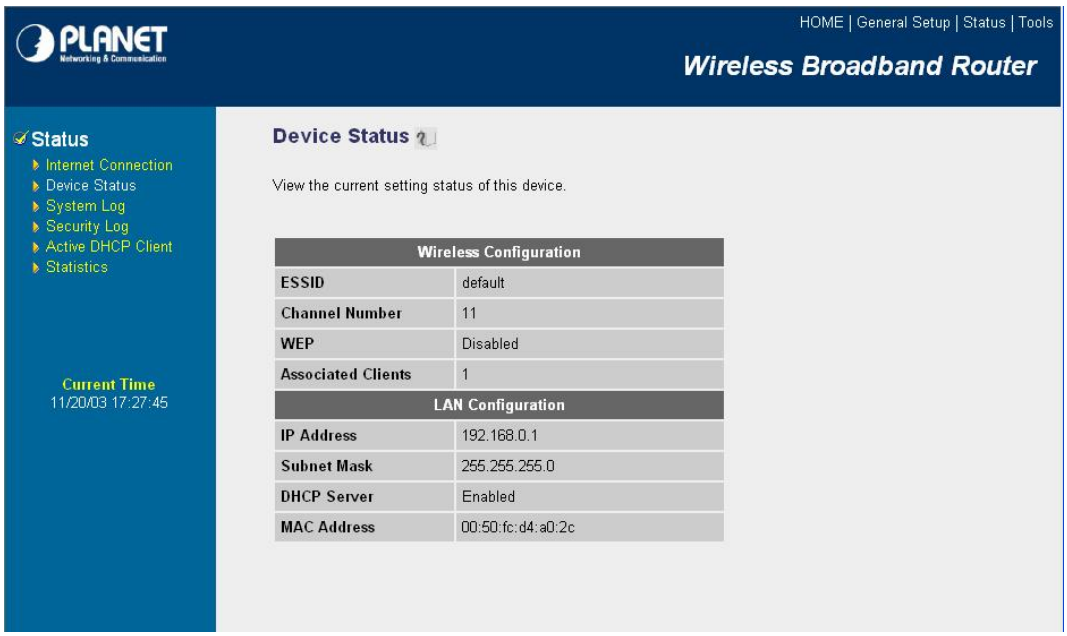
View WRT-403's current Internet connection status and other related information.



Parameters	Description
Internet Connection	This page displays whether the WAN port connection type. It also displays the router's WAN port: WAN IP address, Subnet Mask, and ISP Gateway as well as the Primary DNS and Secondary DNS being used.

5.7.2 Device Status

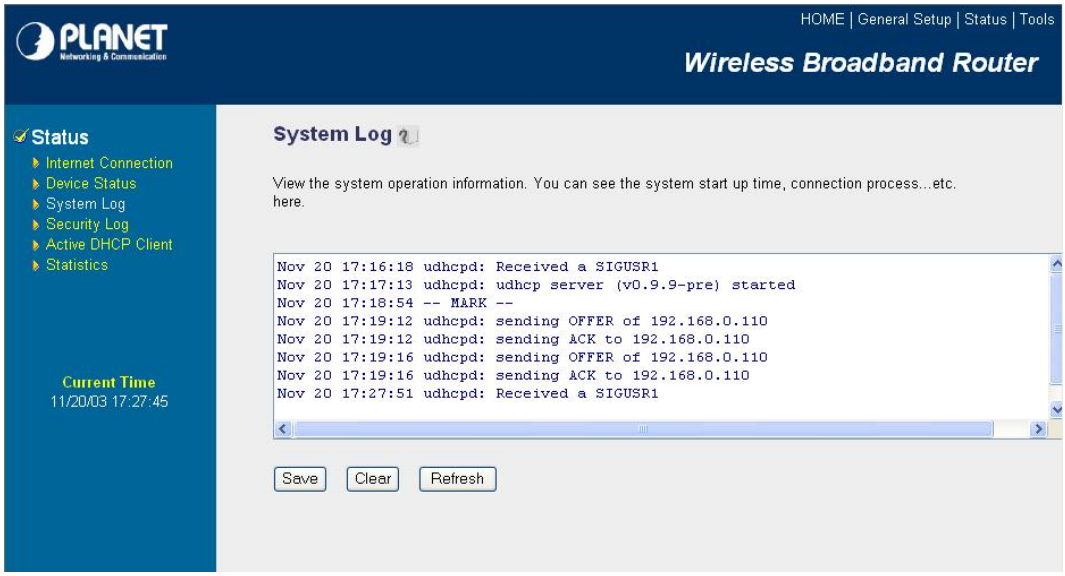
View WRT-403's current configuration settings. The Device Status displays the configuration settings of Wireless LAN and LAN.



Parameters	Description
Device Status	This page shows WRT-403's current device settings. This page displays WRT-403 LAN port's and Wireless current settings.

5.7.3 System Log

This screen will show you the real-time information of WRT-403.



Parameters	Description
System Log	This page shows the current system log of WRT-403. It displays the working information about WRT-403. About the bottoms of the page, the system log can be saved to a local file by press “Save” button. If there is too much message in this screen, please press “Clear” button to clear the system log . It can be refreshed to get the most updated situation by press “Refresh” button. When the system is powered down, the system log will be cleared.

5.7.4 Security Log

View any attempts that have been made to illegally gain access to your network.

Parameters	Description
Security Log	This page shows the current security log of WRT-403. It displays any illegal attempts to access your network. About the bottoms of the page, the security log can be saved to a local file by press “Save” button. If there is too much message in this screen, please press “Clear” button to clear the system log . It can be refreshed to get the most updated situation by press “Refresh” button. When the system is powered down, the security log will be cleared.

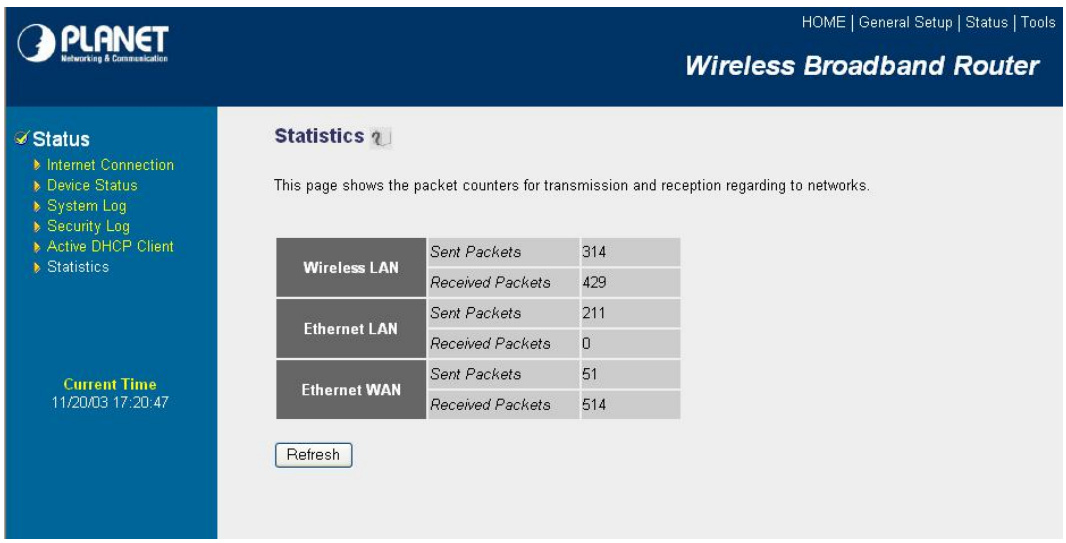
5.7.5 Active DHCP Client

View your client's information that is currently linked to WRT-403's DHCP server.

Parameters	Description
DHCP Client Table	This page shows all the DHCP clients currently connected to your network. The “Active DHCP Client Table” displays the IP address and the MAC address and Time Expired of each Client. Use the Refresh button to get the most updated situation.

5.7.6 Statistics

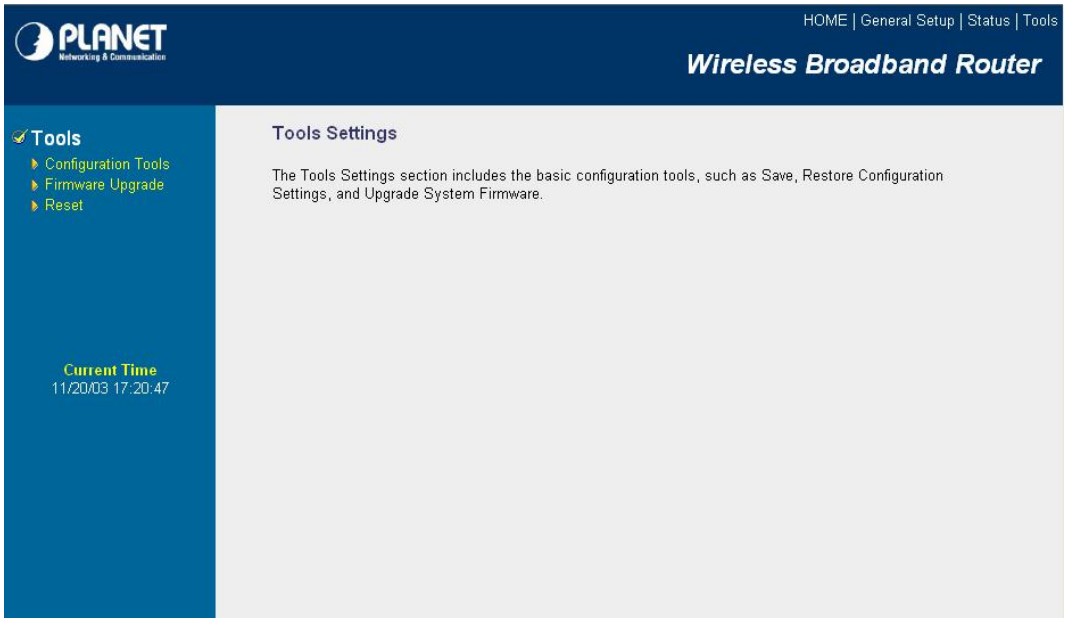
View the statistics of packets sent and received on WLAN, LAN and WAN.



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

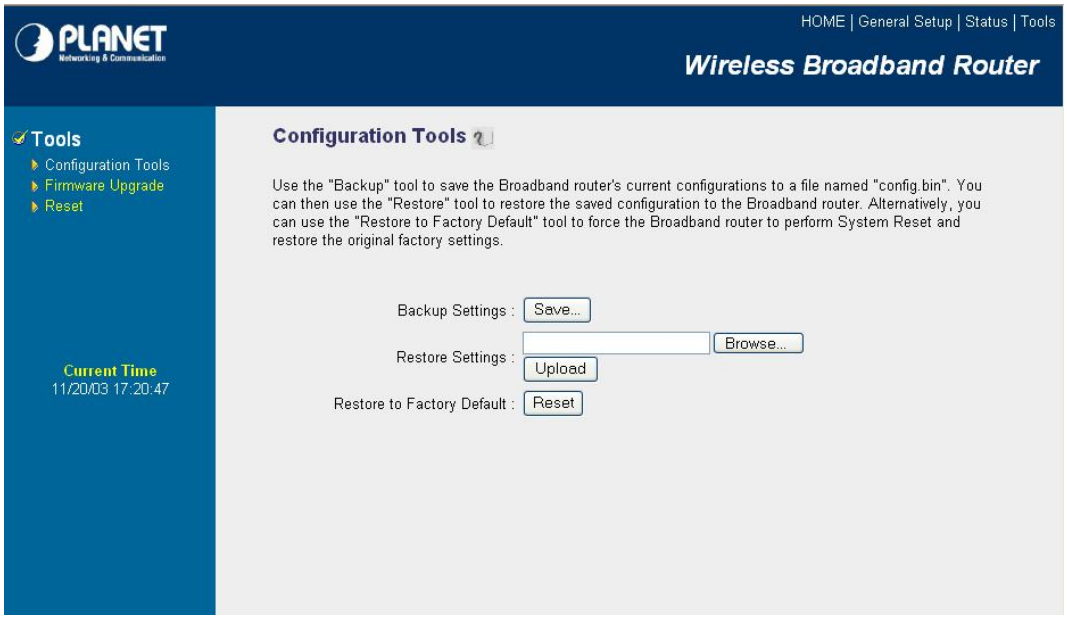
5.8 Tools

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



5.8.1 Configuration Tools

The Configuration Tools screen allows you to “Backup” the router’s current configuration setting. Saving the configuration settings provides an added protection and convenience when problems occur and you have to reset to factory default. With the saved file, you can re-load the saved configuration into the router through the “Restore” function. If extreme problems occur you can use the “Restore to Factory Defaults” selection, this will set all configurations to its original default settings.



Parameters	Description
Configuration Tools	Use the "**Backup**" tool to save WRT-403 current configuration to a file named "config.bin" in your PC. You can then use the "**Restore**" tool to restore the saved configuration to WRT-403. The "**Restore to Factory Defaults**" tool can force WRT-403 to perform a power reset for restore it to original factory settings.

5.8.2 Firmware Upgrade

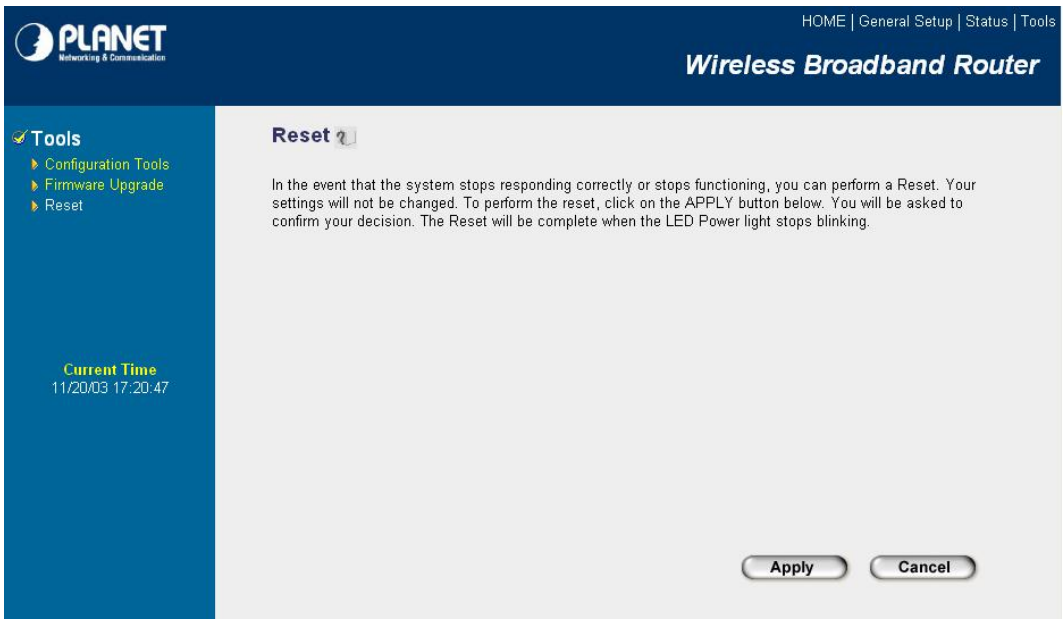
This page allows you to upgrade the router's firmware.

Parameters	Description
Firmware Upgrade	This tool allows you to upgrade WRT-403'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 press the "Browse…" button to find out the firmware file on your PC.

Once you've selected the new firmware file, click "Apply" bottom to start the upgrade process. (You may have to wait a few minutes for the upgrade to complete and WRT-403 restart). After the WRT-403 restart, you can start using the router.

5.8.3 Reset

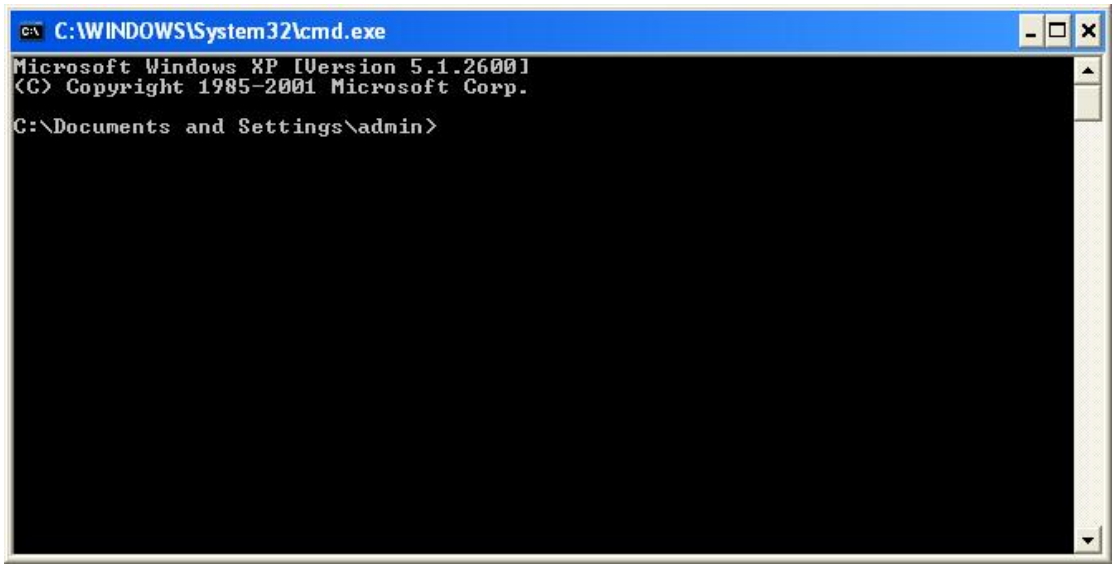
You can reset the router's system should any problem exist. The reset function is essentially Re-boot your router.



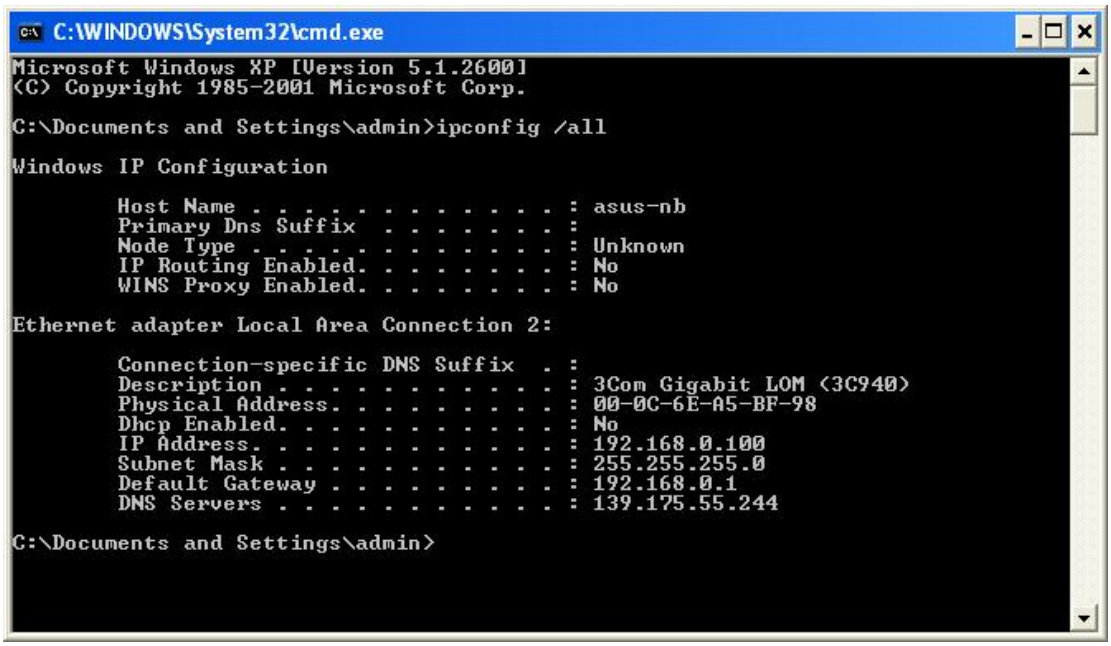
Parameters	Description
Reset	In the event that the system stops responding correctly or in some way stops functioning, you can perform a reset. **Your settings will not be changed**. To perform the reset, click on the "Apply" button. You will be asked to confirm your decision. The reset will be complete when the power light stops blinking. Once the reset process is complete you may start using the router again.

Appendix A Network Adapter Information

1. In Window's open the Command Prompt program.



2. Type "ipconfig /all" and press "Enter" key.



Then you can see the informations of your network adapter.

Your PC's IP address is the one entitled **IP address** (192.168.0.100).

The router's IP address is the one entitled **Default Gateway** (192.168.0.1).

Your PC's MAC Address is the one entitled **Physical Address** (00-0C-6E-A5-BF-98).

Appendix B FAQ

Can I run an application from a remote computer over the wireless network?

This will depend on whether or not the application is designed to be used over a network. Consult the application's user guide to determine if it supports operation over a network.

Can I play games with other members of the wireless network?

Yes, as long as the game supports multiple plays over a LAN (local area network). Refer to the game's user guide for more information.

What is the IEEE 802.11b standard?

The IEEE 802.11b Wireless LAN standards subcommittee, which is formulating a standard for the industry. The objective is to enable wireless LAN hardware from different manufactures to communicate.

What IEEE 802.11 features are supported?

The product supports the following IEEE 802.11 functions:

- CSMA/CA plus Acknowledge protocol
- Multi-Channel Roaming
- Automatic Rate Selection
- RTS/CTS feature
- Fragmentation
- Power Management

What is Roaming?

Roaming is the ability of a portable computer user to communicate continuously while moving freely throughout an area greater than that covered by a single Wireless Network Access Point. Before using the roaming function, the workstation must make sure that it is the same channel number with the Wireless Network Access Point of dedicated coverage area.

Appendix C Glossary

Access Point

Access points are way stations in a wireless LAN that are connected to an Ethernet hub or server. Users can roam within the range of access points and their wireless device connections are passed from one access point to the next.

Authentication

Authentication refers to the verification of a transmitted message's integrity.

DMZ

DMZ (DeMilitarized Zone) is a part of an network that is located between a secure LAN and an insecure WAN. DMZ provides a way for some clients to have unrestricted access to the Internet.

Beacon Interval

Refers to the interval between packets sent by access points for the purposes of synchronizing wireless LANs.

DHCP

DHCP (Dynamic Host Configuration Protocol) software automatically assigns IP addresses to client stations logging onto a TCP/IP network, which eliminates the need to manually assign permanent IP addresses.

DNS

DNS stands for Domain Name System. DNS converts machine names to the IP addresses that all machines on the net have. It translates from name to address and from address to name.

Domain Name

The domain name typically refers to an Internet site address.

Filter

Filters are schemes which only allow specified data to be transmitted. For example, the router can filter specific IP addresses so that users cannot connect to those addresses.

Firewall

Firewalls are methods used to keep networks secure from malicious intruders and unauthorized access. Firewalls use filters to prevent unwanted packets from being transmitted. Firewalls are typically used to provide secure access to the Internet while keeping an organization's public Web server separate from the internal LAN.

Firmware

Firmware refers to memory chips that retain their content without electrical power (for example, BIOS ROM). The router firmware stores settings made in the interface.

Fragmentation

Refers to the breaking up of data packets during transmission.

FTP

FTP (File Transfer Protocol) is used to transfer files over a TCP/IP network, and is typically used for transferring large files or uploading the HTML pages for a Web site to the Web server.

Gateway

Gateways are computers that convert protocols enabling different networks, applications, and operating systems to exchange information.

Host Name

The name given to a computer or client station that acts as a source for information on the network.

HTTP

HTTP (HyperText Transport Protocol) is the communications protocol used to connect to servers on the World Wide Web. HTTP establishes a connection with a Web server and transmits HTML pages to client browser (for example Windows IE). HTTP addresses all begin with the prefix 'http://' prefix (for example, *http://www.yahoo.com*).

ICMP

ICMP (Internet Control Message Protocol) is a TCP/IP protocol used to send error and control messages over the LAN (for example, it is used by the router to notify a message sender that the destination node is not available).

IP

IP (Internet Protocol) is the protocol in the TCP/IP communications protocol suite that contains a network address and allows messages to be routed to a different network or subnet. However, IP does not ensure delivery of a complete message—TCP provides the function of ensuring delivery.

IP Address

The IP (Internet Protocol) address refers to the address of a computer attached to a TCP/IP network. Every client and server station must have a unique IP address. Clients are assigned either a permanent address or have one dynamically assigned to them via DHCP. IP addresses are written as four sets of numbers separated by periods (for example, 211.23.181.189).

ISP

An ISP is an organization providing Internet access service via modems, ISDN (Integrated Services Digital Network), and private lines.

LAN

LANs (Local Area Networks) are networks that serve users within specific geographical areas, such as in a company building. LANs are comprised of servers, workstations, a network operating system, and

communications links such as the router.

MAC Address

A MAC address is a unique serial number burned into hardware adapters, giving the adapter a unique identification.

Metric

A number that indicates how long a packet takes to get to its destination.

MTU

MTU (Maximum Transmission/Transfer Unit) is the largest packet size that can be sent over a network. Messages larger than the MTU are divided into smaller packets.

NAT

NAT (Network Address Translation - also known as IP masquerading) enables an organization to present itself to the Internet with one address. NAT converts the address of each LAN node into one IP address for the Internet (and vice versa). NAT also provides a certain amount of security by acting as a firewall by keeping individual IP addresses hidden from the WAN.

(Network) Administrator

The network administrator is the person who manages the LAN within an organization. The administrator's job includes ensuring network security, keeping software, hardware, and firmware up-to-date, and keeping track of network activity.

NTP

NTP (Network Time Protocol) is used to synchronize the real-time clock in a computer. Internet primary and secondary servers synchronize to Coordinated Universal Time (UTC).

Packet

A packet is a portion of data that is transmitted in network communications. Packets are also sometimes called frames and datagrams. Packets contain not only data, but also the destination IP address.

Ping

Ping (Packet Internet Groper) is a utility used to find out if a particular IP address is present online, and is usually used by networks for debugging.

Port

Ports are the communications pathways in and out of computers and network devices (routers and switches). Most PCs have serial and parallel ports, which are external sockets for connecting devices such as printers, modems, and mice. All network adapters use ports to connect to the LAN. Ports are typically numbered.

PPPoE

PPPoE (Point-to-Point Protocol Over Ethernet) is used for running PPP protocol (normally used for dial-up Internet connections) over an Ethernet.

Preamble

Preamble refers to the length of a CRC (Cyclic Redundancy Check) block that monitors communications between roaming wireless enabled devices and access points.

Protocol

A protocol is a rule that governs the communication of data.

RIP

RIP (Routing Information Protocol) is a routing protocol that is integrated in the TCP/IP protocol. RIP finds a route that is based on the smallest number of hops between the source of a packet and its destination.

RTS

RTS (Request To Send) is a signal sent from the transmitting station to the receiving station requesting permission to transmit data.

Server

Servers are typically powerful and fast machines that store programs and data. The programs and data are shared by client machines (workstations) on the network.

SMTP

SMTP (Simple Mail Transfer Protocol) is the standard Internet e-mail protocol. SMTP is a TCP/IP protocol defining message format and includes a message transfer agent that stores and forwards mail.

SNMP

SNMP (Simple Network Management Protocol) is a widely used network monitoring and control protocol. SNMP hardware or software components transmit network device activity data to the workstation used to oversee the network.

SSID

SSID (Service Set Identifier) is a security measure used in WLANs. The SSID is a unique identifier attached to packets sent over WLANs. This identifier emulates a password when a wireless device attempts communication on the WLAN. Because an SSID distinguishes WLANS from each other, access points and wireless devices trying to connect to a WLAN must use the same SSID.

Subnet Mask

Subnet Masks are used by IP protocol to direct messages into a specified network segment (i.e., subnet). A subnet mask is stored in the client machine, server or router and is compared with an

incoming IP address to determine whether to accept or reject the packet.

SysLog Server

A SysLog server monitors incoming Syslog messages and decodes the messages for logging purposes.

TCP

(Transmission Control Protocol) is the transport protocol in TCP/IP that ensures messages over the network are transmitted accurately and completely.

TCP/IP

TCP/IP (Transmission Control Protocol/Internet Protocol) is the main Internet communications protocol. The TCP part ensures that data is completely sent and received at the other end. Another part of the TCP/IP protocol set is UDP, which is used to send data when accuracy and guaranteed packet delivery are not as important (for example, in realtime video and audio transmission).

The IP component of TCP/IP provides data routability, meaning that data packets contain the destination station and network addresses, enabling TCP/IP messages to be sent to multiple networks within the LAN or in the WAN.

Telnet

Telnet is a terminal emulation protocol commonly used on the Internet and TCP- or IP-based networks.

Telnet is used for connecting to remote devices and running programs. Telnet is an integral component of the TCP/IP communications protocol.

UDP

(User Datagram Protocol) is a protocol within TCP/IP that is used to transport information when accurate delivery isn't necessary (for example, real-time video and audio where packets can be dumped as there is no time for retransmitting the data).

Virtual Servers

Virtual servers are client servers (such as Web servers) that share resources with other virtual servers (i.e., it is not a dedicated server).

WEP

WEP (Wired Equivalent Privacy) is the de facto security protocol for wireless LANs, providing the "equivalent" security available in hardwired networks.

Wireless LAN

Wireless LANs (WLANs) are local area networks that use wireless communications for transmitting data. Transmissions are usually in the 2.4 GHz band. WLAN devices do not need to be lined up for communications like infrared devices. WLAN devices use access points which are connected to the

wired LAN and provide connectivity to the LAN. The radio frequency of WLAN devices is strong enough to be transmitted through non-metal walls and objects, and can cover an area up to a thousand feet. Laptops and notebooks use wireless LAN PCMCIA cards while PCs use plug-in cards to access the WLAN.

WLAN

WLANs (Wireless LANs) are local area networks that use wireless communications for transmitting data. Transmissions are usually in the 2.4 GHz band. WLAN devices do not need to be lined up for communications like infrared devices. WLAN devices use access points which are connected to the wired LAN and provide connectivity to the LAN. The radio frequency of WLAN devices is strong enough to be transmitted through non-metal walls and objects, and can cover an area up to a thousand feet. Laptops and notebooks use wireless LAN PCMCIA cards while PCs use plug-in cards to access the WLAN.

WAN

WAN (Wide Area Network) is a communications network that covers a wide geographic area such as a country (contrasted with a LAN, which covers a small area such as a company building).