IEEE 802.11g
Wireless Broadband Router

Manual

Regulatory notes and statements

Wireless LAN, Health and Authorization for use

Radio frequency electromagnetic energy is emitted from Wireless LAN devices. The energy levels of these emissions however are far much less than the electromagnetic energy emissions from wireless devices like for example mobile phones. Wireless LAN devices are safe for use frequency safety standards and recommendations. The use of Wireless LAN devices may be restricted in some situations or environments for example:

- On board of airplanes, or
- In an explosive environment, or
- In case the interference risk to other devices or services is perceived or identified as harmful

In case the policy regarding the use of Wireless LAN devices in specific organizations or environments (e.g. airports, hospitals, chemical/oil/gas industrial plants, private buildings etc.) is not clear, please ask for authorization to use these devices prior to operating the equipment.

Regulatory Information/disclaimers

Installation and use of this Wireless LAN device must be in strict accordance with the instructions included in the user documentation provided with the product. Any changes or modifications made to this device that are not expressly approved by the manufacturer may void the user's authority to operate the equipment. The Manufacturer is not responsible for any radio or television interference caused by unauthorized modification of this device, of the substitution or attachment. Manufacturer and its authorized resellers or distributors will assume no liability for any damage or violation of government regulations arising from failing to comply with these guidelines.

USA-FCC (Federal Communications Commission) statement

This device complies with Part 15 of FCC Rules.

Operation is subject to the following two conditions:

1. This device may not cause interference, and
2. This device must accept any interference, including interference that may cause undesired operation of this device.

FCC Radio Frequency Exposure statement

This Wireless LAN radio device has been evaluated under FCC Bulletin OET 65 and found compliant to the requirements as set forth in CFR 47 Sections 2.1091, 2.1093, and 15.247 (b) (4) addressing RF Exposure from radio frequency devices. The radiated output power of this Wireless LAN device is far below the FCC radio frequency exposure limits. Nevertheless, this device shall be used in such a manner that the potential for human contact during normal operation is minimized.

When nearby persons has to be kept to ensure RF exposure compliance, in order to comply with RF exposure limits established in the ANSI C95.1 standards, the distance between the antennas and the user should not be less than 20 cm.

FCC Interference Statement

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation.

This equipment generates, uses, and can radiate radio frequency energy. If not installed and used in accordance with the instructions, it 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 and correct the interference by one or more of the following measures:

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

Export restrictions

This product or software contains encryption code that may not be exported or transferred from the US of Canada without an approved US Department of Commerce export license.

Safety Information

Your device contains a low power transmitter. When device is transmitted it sends out radio frequency (RF) signal.

CAUTION: To maintain compliance with FCC's RF exposure guidelines, this equipment should be installed and operated with minimum distance 20cm between the radiator and your body. Use on the supplied antenna. Unauthorized antenna, modification, or attachments could damage the transmitter and may violate FCC regulations.

The antenna(s) used for this transmitter must be installed to provide a separation distance of at least 20 cm from all persons and must not be co-located or operating in conjunction with any other antenna or transmitter.

CE Mark Warning

This is a Class B product. In a domestic environment, this product may cause radio interference, in which case the user may be required to take adequate measures.

Protection requirements for health and safety – Article 3.1a

Testing for electric safety according to EN 60950 has been conducted. These are considered relevant and sufficient.

Protection requirements for electromagnetic compatibility – Article 3.1b

Testing for electromagnetic compatibility according to EN 301 489-1, EN 301 489-17 and EN 55024 has been conducted. These are considered relevant and sufficient.

Effective use of the radio spectrum – Article 3.2

Testing for radio test suites according to EN 300 328-2 has been conducted. These are considered relevant and sufficient.

CE in which Countries where the product may be used freely:

Germany, UK, Italy, Spain, Belgium, Netherlands, Portugal, Greece, Ireland, Denmark, Luxembourg, Austria, Finland, Sweden, Norway and Iceland.

France: except the channel 10 through 13, law prohibits the use of other channels.

TABLE OF CONTENT

ABOUT THIS GUIDE ***1***

Purpose 1

Overview of this User's Guide 1

INTRODUCTION ***2***

Applications 2

Features 3

UNPACKING AND SETUP ***4***

Unpacking 4

Setup 4

HARDWARE INSTALLATION ***5***

Front Panel 5

Rear Panel 6

Hardware connections 6

Connect the Router using LAN 6

4. Connect the Router using Wireless LAN 7

Check the installation 7

PC NETWORK TCP/IP SETTING ***8***

Windows 95/98/ME 8

Windows 2000 9

Windows XP 10

WIRELESS BROADBAND ROUTER CONFIGURATION ***11***

Login to the Wireless Broadband Router through WLAN 11

Login to the Wireless Broadband Router through LAN 11

Using the Web Browser 11

Configuration Menu 12

Setup Wizard 13

WAN Setting 23

DHCP Client or Fixed IP 23

PPPoE with Obtain IP Automatically 24

PPPoE with Specify IP 25

PPTP/L2TP with Obtain IP Automatically 26

PPTP/L2TP with Specify IP 26

BigPond Cable 27

Wireless setting 28

Basic 28

Security 29

Advanced 32

LAN Setting 33

Basic 33
DHCP 33
Access Control Setting 35
Filter 35
Virtual Server 40
Special AP 40
DMZ 41
Firewall Rule 43
System Setting 44
Password 44
Time 45
Device Information 46
Log 47
Log Setting 48
Statistic 49
Restart 49
Configuration 51
UPnP 51
Ping Test 52
Remote Management 53
TECHNICAL SPECIFICATIONS 54

ABOUT THIS GUIDE

Congratulations on your purchase of this IEEE 802.11g Wireless Broadband Router. This integrated access device combines Internet gateway functions with wireless LAN and Fast Ethernet switch. It provides a complete solution for Internet surfing and office resources sharing, and it is easy to configure and operate for every users.

Purpose

This manual discusses how to install the IEEE 802.11g Wireless Broadband Router.

Overview of this User's Guide

Introduction. Describes the Wireless Broadband Router and its features.

Unpacking and Setup. Helps you get started with the basic installation of the Wireless Router.

Identifying External Components. Describes the front panel, rear panel and LED indicators of the Wireless Router.

Connecting the Router. Tells how you can connect the Wireless Router to your xDSL/Cable Modem.

Technical Specifications. Lists the technical (general, physical and environmental, performance and Routers settings) specifications of the Wireless Broadband Router.

INTRODUCTION

With the explosive growth of the Internet, accessing information and services at any time, day or night has become a standard requirement for most people. The era of the standalone PC is waning. Networking technology is moving out of the exclusive domain of corporations and into homes with at least two computers.

This integrated access device combines Internet gateway functions with wireless LAN and Fast Ethernet switch. Designed for the business and home, it saves you the cost of installing a separate modem and ISP line for each computer, while providing ready connection for the users, with or without the network wires.

Broadband network access is also gaining ground. However, allowing more than two computers to access the Internet at the same time means less affordable, higher costs. Thus, there is a need to share one legal IP address over a single Internet connection to link the home with the Internet.

The scarcity of IP addresses and using a shared Internet connection through an Internet sharing device can solve high network access costs. All linked computers can make full use of broadband capabilities over such a device.

This device not only comes equipped with a wide range of features, but also can be installed and configured right out of the box. This device supports a simple local area network and Internet access share, offering great cost savings.

The local area network connects up home computers while also allowing any of the computers to access the Internet, share resources, or play online games—the basis of the family computing lifestyle.

Applications

Broadband Internet access: Several computers can share one high-speed broadband connection through wireless or wired (WLAN, LAN and WAN-Internet).

Resource sharing: Share resources such as printers, scanners and other peripherals.

File sharing: Exchange data, messages, and distribute files thus making good use of hard disk space.

Online gaming: Through the local area network, online gaming and e-commerce services can be easily setup.

Firewall: A built-in firewall function — for security and anti-hack system.

Features

- Compliant with IEEE 802.11g and 802.11b Devices
- Built-in 4 x 10/100Mbps Auto-MDIX LAN Ports
- Built-in 1 x 10/100Mbps Auto-MDIX WAN Port (Internet)
- Supports Cable/DSL Modems with Dynamic IP, Static IP, PPPoE, L2TP, PPTP or BigPond Connection Types
- DHCP Server Feature Allocates up to 253 Client IP Addresses
- Supports 64/128-bit Wired Equivalent Privacy (WEP)
- Supports WPA, WPA2, WPA-PSK and WPA2-PSK Advanced Security
- Supports MAC Address, Protocol Filters and UPnP (Universal Plug & Play)
- Traffic Control with Virtual Server, Virtual PC mapping and DMZ
- Provides Additional Security with SPI / NAT firewall and Attack Alert via emails
- Provides Additional Security of Enable/Disable SSID, Password Protection
- Flash Memory for Firmware Upgrade, Save/Restore Settings, and Traffic Log
- Compliant with Windows 95/98/NT/2000/XP, Linux and Mac OS
- Easy Management and Remote Management via Web Browser (HTTP)
- Range for Indoor of 30 ~ 50 meters (depends on the environment)
- Range for Outdoor of 50 ~ 200 meters (depends on the environment)

UNPACKING AND SETUP

This chapter provides unpacking and setup information for the IEEE 802.11g Wireless Broadband Router.

Unpacking

Open the box of the Wireless Broadband Router and carefully unpack it. The box should contain the following items:

- One IEEE 802.11g Wireless Broadband Router
- One 2dBi dipole antenna
- One CD-ROM with User's Guide
- One AC Power adapter

If any item is found missing or damaged, please contact your local reseller for replacement.

Setup

The setup of the Wireless Broadband Router can be performed properly using the following methods:

- The power outlet should be within 1.82 meters (6 feet) of the Broadband Router.
- Visually inspect the DC power jack and make sure that it is fully secured to the power adapter.
- Make sure that there is proper heat dissipation from and adequate ventilation around the Broadband Router. Do not place heavy objects on the Broadband Router.
- Fix the direction of the antennas. Try to place the Wireless Router in a position that can best cover your wireless network. Normally, the higher you place the antenna, the better the performance will be. The antenna's position enhances the receiving sensitivity.

Front Panel

The figure below shows the front panel of the Wireless Broadband Router.

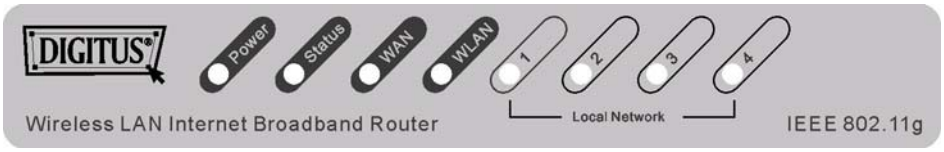


Figure 1. Front panel

POWER

This indicator lights green when the hub is receives power, otherwise it is off.

Status

This indicator blinks green means the Internet Broadband Router is working successful. Otherwise, this indicator always on or off means the function of the Internet Broadband Router is fail.

WAN (Link/ACT)

The indicators light green when the WAN port was connected to an xDSL/Cable modem successfully.

The indicators blink green while the WAN port was transmitting or receiving data on the xDSL/Cable modem.

WLAN (ACT)

This indicator lights green when there are wireless devices connected and transmitting data to the Wireless Router.

LAN (Link/ACT)

These indicators light green when the LAN ports were connected successfully.

These indicators blink green while the LAN ports were transmitting data.

Rear Panel

The figure below shows the rear panel of the Wireless Broadband Router.

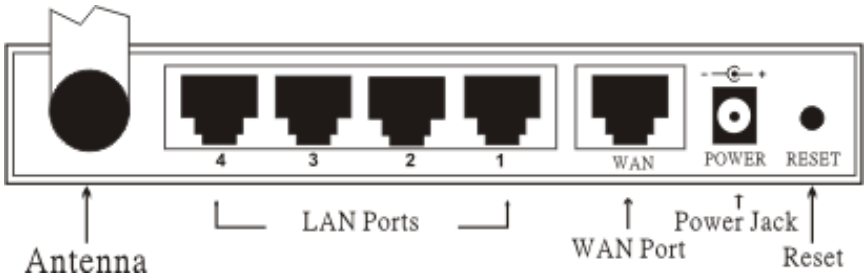


Figure 2. Rear Panel

Antenna

There are one 2 dBi Gain Antenna in the rear panel for wireless connection.

LAN (1-4)

Four RJ-45 10/100Mbps Auto-MDIX ports for connecting to either 10Mbps or 100Mbps Ethernet connections.

WAN

In the four port broadband router, there is an RJ-45 10/100Mbps Auto-MDIX port for the WAN that will fit the xDSL/Cable modem's specification need.

DC IN

Plug the power adapter to this power jack

RESET

Use a pin-shape item to push to reset this device to factory default settings. It will be useful too when the manager forgot the password to login, but the setting will be back to default setting.

Hardware connections

Connect the Router using LAN

1. Plug in one end of the network cable to the WAN port of the Wireless Internet Broadband Router.
2. Plug in the other end of the network cable to the Ethernet port of the xDSL or Cable modem.
3. Use another network cable to connect to the Ethernet card on the computer system; the other end of the cable connects to the LAN port of the Internet Broadband Router. Since the Wireless Broadband Router has four ports, you can connect up to four computers directly to the unit. There you do not have to buy a switch to connect these computers since one Internet Broadband Router functions both as a connection-sharing unit and as a switch.

4. Connect the Router using Wireless LAN

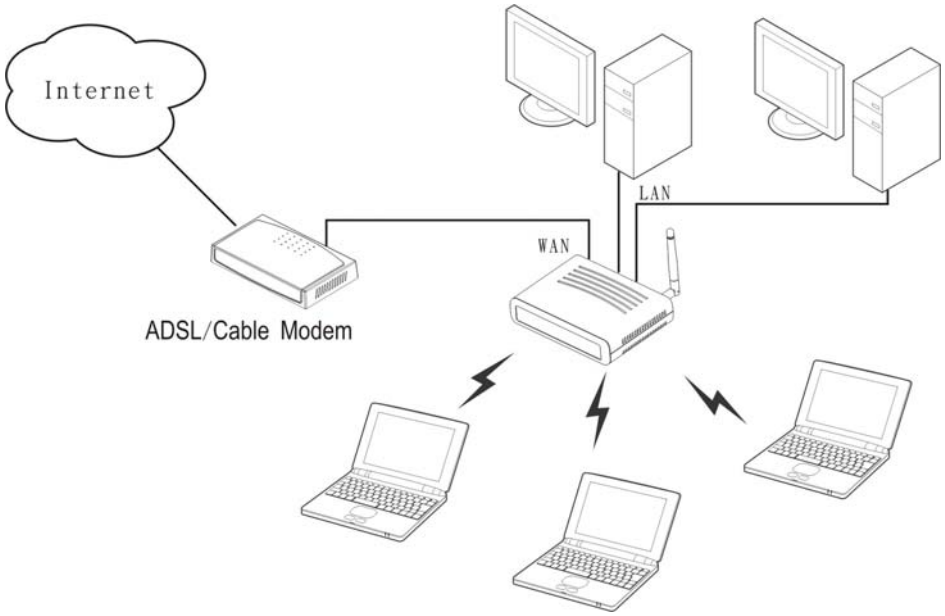


Figure 3. Connecting the WLAN Router

1. Plug in one end of the RJ45 network cable to the xDSL/Cable Modem.
2. Plug in the other end of the RJ45 network cable to the Wireless Internet Broadband Router WAN port.

Check the installation

The control LEDs of the Wireless Internet Broadband Router are clearly visible and the status of the network link can be seen instantly:

1. With the power source on, once the device is connected to the broadband modem, the Power, CPU, LAN, WLAN and WAN port link LEDs of the Internet Broadband Router will light up indicating a normal status.
2. While the WAN is link up to the ADSL/Cable modem, the WAN port's Link/ACT LED will light up.
3. While the LAN is link up to the computer system, the LAN port's Link/ACT LED will light up.

PC NETWORK TCP/IP SETTING

The network TCP/IP settings differ based on the computer's operating system (Win95/98/ME/NT/2000/XP) and are as follows.

Windows 95/98/ME

1. Click on the "**Network neighborhood**" icon found on the desktop.
2. Click the right mouse button and a context menu will be show.
3. Select "**Properties**" to enter the TCP/IP setting screen.
4. Select "**Obtain an IP address automatically**" on the "**IP address**" field.

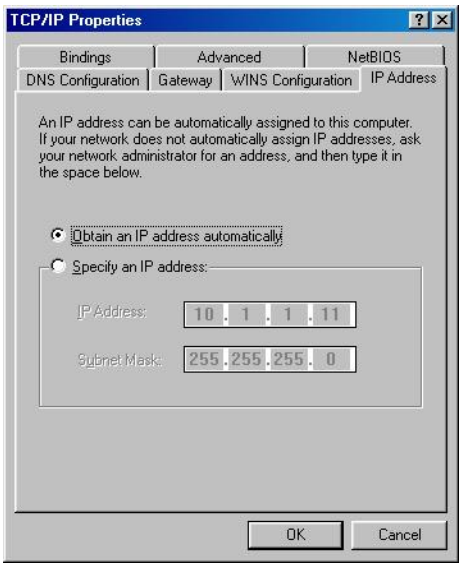


Figure 4. Windows 95/95/Me IP setup

5. Select "**Disable DNS**" in the "**DNS**" field.

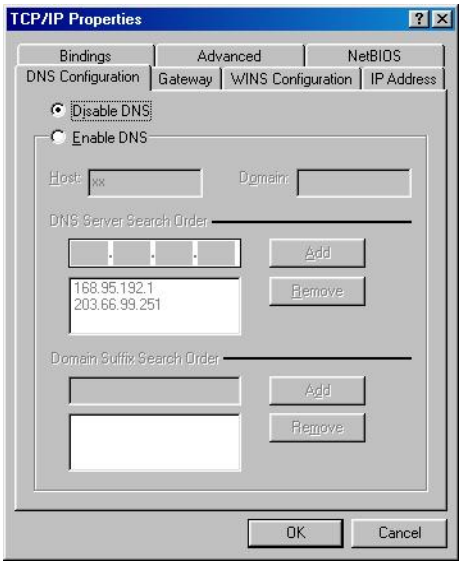


Figure 5. Windows 95/98/Me DNS setup

6. Select “**None**” for the “**Gateway address**” field.

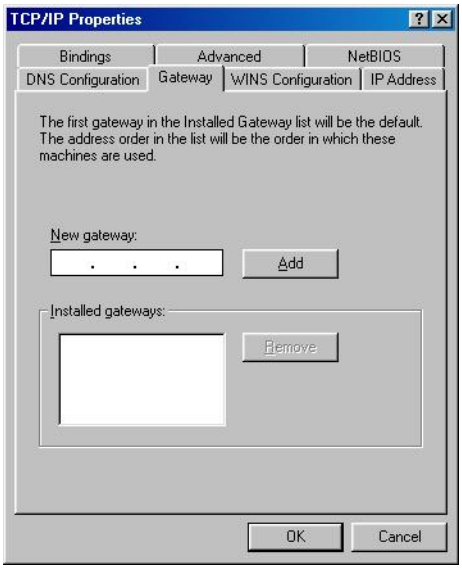


Figure 6. Windows 95/98/Me Gateway setup

Windows 2000

Double click on the “**My computer**” icon on the desktop. When “**My computer**” window opens, open the “**Control panel**” and then open the “**Network dialup connection**” applet. Double click on the “Local area network connection” icon. Select “Properties” to enter the TCP/IP setting window.

1. In the “**Local area network status**” window, click on “**Properties**.”
2. In the “**Local area network connection**” window, first select TCP/IP setting and then select “**Properties**.”
3. Set both “**IP address**” and “**DNS**” to **Automatic configuration**.

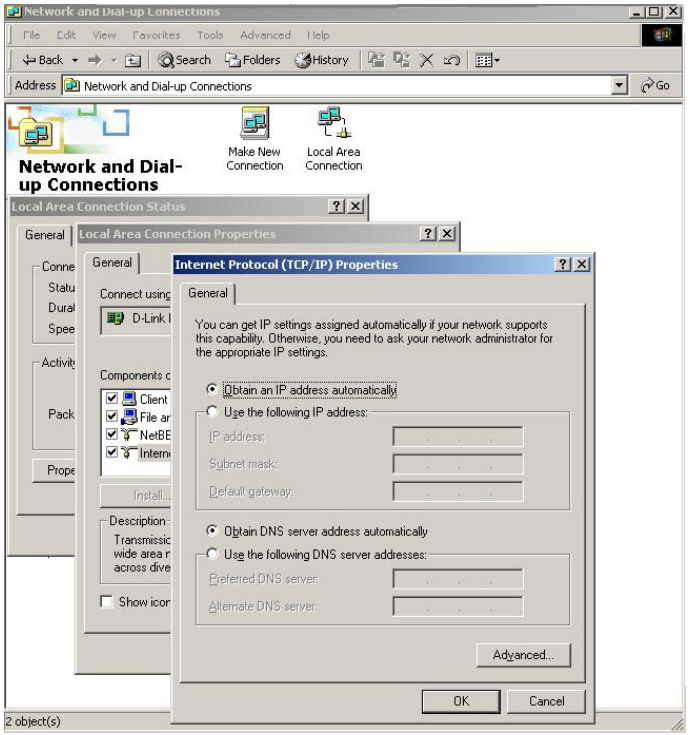


Figure 7. Windows 2000 IP and DNS setup

Windows XP

Point the cursor and click the right button on the “My Network Place” icon.

Select “properties” to enter the TCP/IP setting window.

1. Set “**IP address**” to “**Obtain an IP address automatically**.”
2. Set “**DNS**” to “**Obtain DNS server address automatically**.”

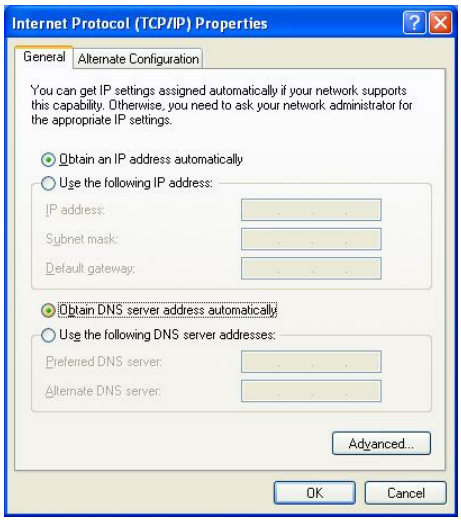


Figure 8. Windows XP IP and DNS setup

WIRELESS BROADBAND ROUTER CONFIGURATION

First make sure that the network connections are functioning normally.

This Wireless Broadband Router can be configured using Internet Explorer 5.0 or newer web browser versions.

Login to the Wireless Broadband Router through WLAN

Before configuring the Wireless Broadband Router through WLAN, make sure that the SSID, Channel and the WEP is set properly.

The default setting of the Wireless Broadband Router that you will use:

- SSID: **default**
- Channel: **6**
- Security: **disable**
- IP Address: **192.168.1.1**

Login to the Wireless Broadband Router through LAN

Before you configure this device, note that when the Wireless Broadband Router is configured through an Ethernet connection, make sure the host PC must be set on the **IP sub-network** that can be accessed by the xDSL/Cable modem. For example, when the default network address of the xDSL/Cable modem Ethernet interface is 192.168.1.x, then the host PC should be set at 192.168.1.xxx (where xxx is a number between 2 and 254), and the default subnet mask is 255.255.255.0.

Using the Web Browser

1. Open Internet Explorer 5.0 or above Internet browser.
2. Enter IP address ***http://192.168.1.1*** (the factory-default IP address setting) to the URL web address location.

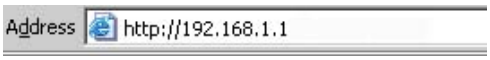


Figure 9. Web address

3. When the following dialog box appears, enter the user name and password to login to the main configuration window, the default username and password is "***admin***".

Figure 10. Login

Note: If needed to set a password, then refer to the **System – Password Setting**.

After entering the password, the main page comes up, the screen will display the device information.

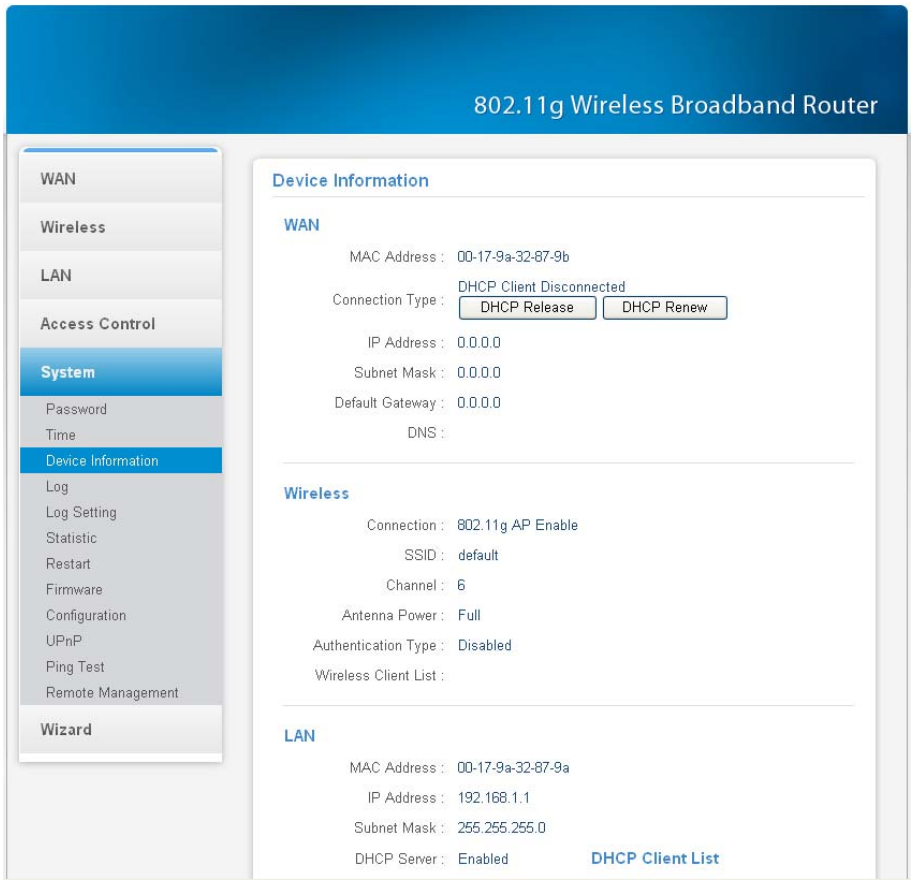


Figure 11. Device information

Configuration Menu

When the main page appears, find the ***Configuration menu*** in the left side of the screen. Click on the setup item that you want to configure. There are six main options: *WAN, Wireless, LAN, Access Control, System and Wizard* as shown in the Configuration Menu screen.

Figure 12. Configuration Menu

Setup Wizard

Setup wizard is provided as the part of the web configuration utility. User can simply follow the step-by-step process to get the wireless router configuration ready to run in 6 easy steps by clicking on the “Wizard” button on the function menu. The following screen will appear. Please click “Next” to continue.

Figure 13. Setup Wizard

Step 1: Set up new Password

User can change the password and then click “Next” to continue.

Figure 14. Setup Wizard – Set Password

Step 2: Choose time zone

Select the time zone from the drop down list. Please click “Next” to continue.

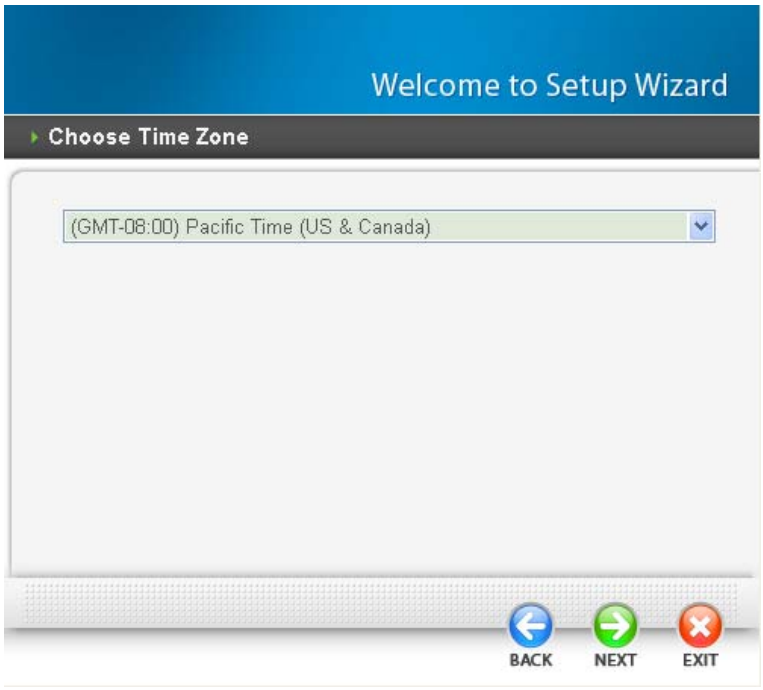


Figure 15. Setup Wizard – Set time zone

Step 3: Set LAN and DHCP Server

Set user’s IP address and mask. The default IP is 192.168.1.1. If user likes to enable DHCP, please click “Enabled”. DHCP enabled is able to automatically assign IP addresses. Please assign the range of IP addresses in the fields of “Range start” and “Range end”. Please click “Next” to continue.

Figure 16. Setup Wizard – Set LAN & DHCP Server

Step 4: Set Internet connection

The WLAN Router will attempt to auto detect your Internet Connection.

Figure 17. Setup Wizard – WAN setup - Auto detect WAN type

If the WLAN Router is unable to auto detect your Internet connection, you will need to manually select the Internet connection type: Obtain IP automatically; Fixed IP, PPPoE, PPTP, L2TP or BigPond.

Obtain IP automatically (DHCP client):

If user has enabled DHCP server, choose "Obtain IP automatically (DHCP client)" to have the router assign IP addresses automatically.

Figure 18.

If your ISP requires you to enter a specific host name or MAC address, please enter it in.

Figure 19.

Fixed IP Address:

Figure 20.

If the Internet Service Providers assign a fixed IP address, choose this option and enter the assigned IP address, subnet mask, gateway IP and DNS IP addresses for your Broadband Router.

Figure 21.

PPPoE:

Figure 22.

Obtain IP Automatically: If connected to the Internet using a PPPoE (Dial-up xDSL) Modem, the ISP will provide a Password and User Name, and then the ISP uses PPPoE. Choose this option and enter the required information.

Figure 23.

Specify IP: If connected to the Internet using a PPPoE (Dial-up xDSL) Modem, the ISP will provide a Password, User Name and a Fixed IP Address, choose this option and enter the required information.

Figure 24.

PPTP:

Figure 25.

If connected to the Internet using a (PPTP) xDSL Modem, enter the your IP Address, Subnet Mask, Gateway, Server IP, PPTP Account and PPTP Password, Your Subnet Mask required by your ISP in the appropriate fields. If your ISP has provided you with a Connection ID, enter it in the Connection ID field, otherwise, leave it zero.

Figure 26.

L2TP:

Figure 27.

If connected to the Internet using a (L2TP) xDSL Modem, enter the your IP Address, Subnet Mask, Gateway, Server IP, L2TP Account and L2TP Password, Your Subnet Mask required by your ISP in the appropriate fields. If your ISP has provided you with a Connection ID, enter it in the Connection ID field, otherwise, leave it zero.

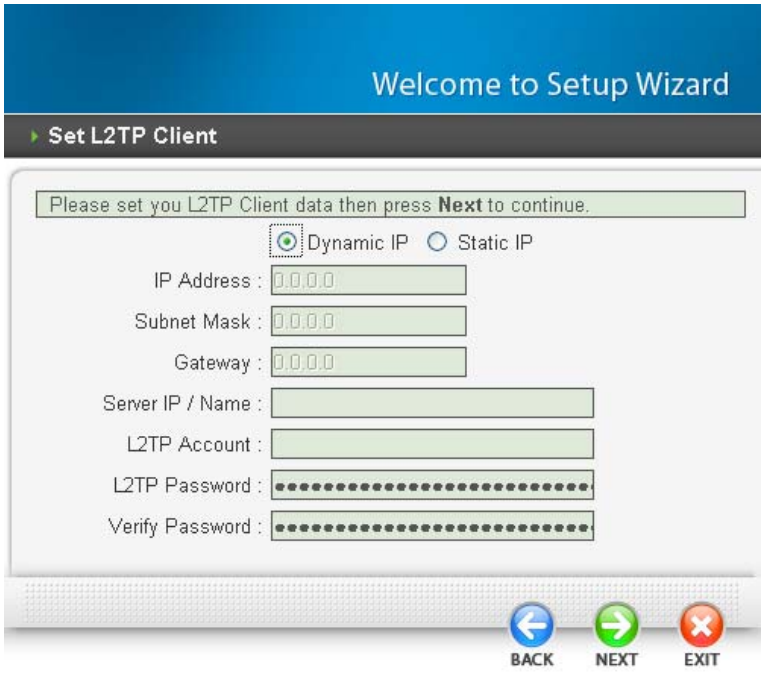


Figure 28.

BigPond:

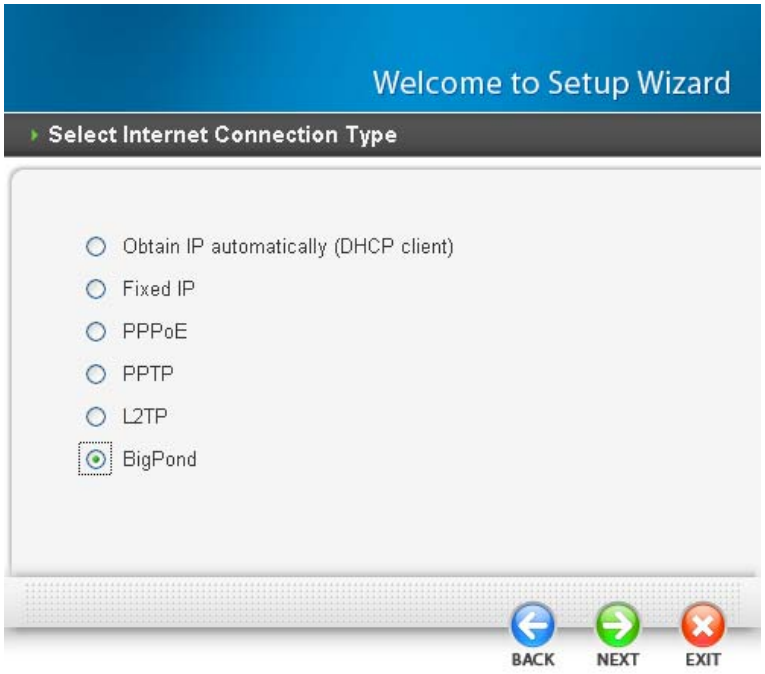


Figure 29.

If your ISP is Big Pond Cable, the ISP will provide a User Name, Password, Authentication Server and Login Server IP (Optional). Choose this option and enter the required information.

Figure 30.

Step 5: Set Wireless LAN connection

Click “Enable” to enable wireless LAN. If user enables the wireless LAN, type the SSID in the text box and select a communications channel. The SSID and channel must be the same as wireless devices attempting communication to the router.

Figure 31.

Step 6: Restart

The Setup wizard is now completed. The new settings will be effective after the Wireless router restarted. Please click “Restart” to reboot the router. If user does not want to make any changes, please click “Exit” to quit without any changes.

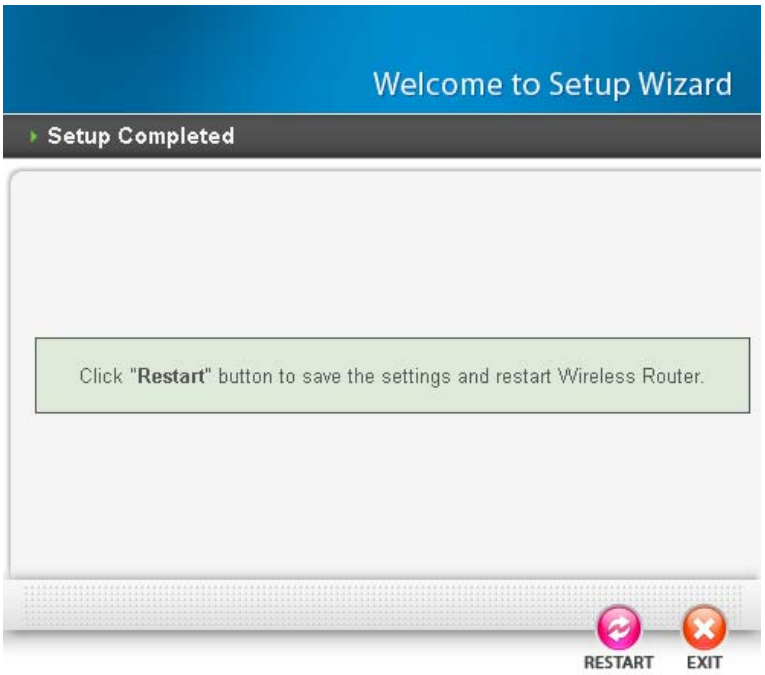


Figure 32.

WAN Setting

This function enables users to set up the WLAN Router WAN connection, specify the IP address for the WAN, add DNS numbers, and enter the MAC address.

Connection Type: Select the connection type, either DHCP client, Fixed IP or PPPoE, PPTP, L2TP or BigPond from the drop-down list.

DHCP Client or Fixed IP

If user has enabled DHCP server, choose "Obtain IP automatically (DHCP client)" to have the router assign IP addresses automatically.

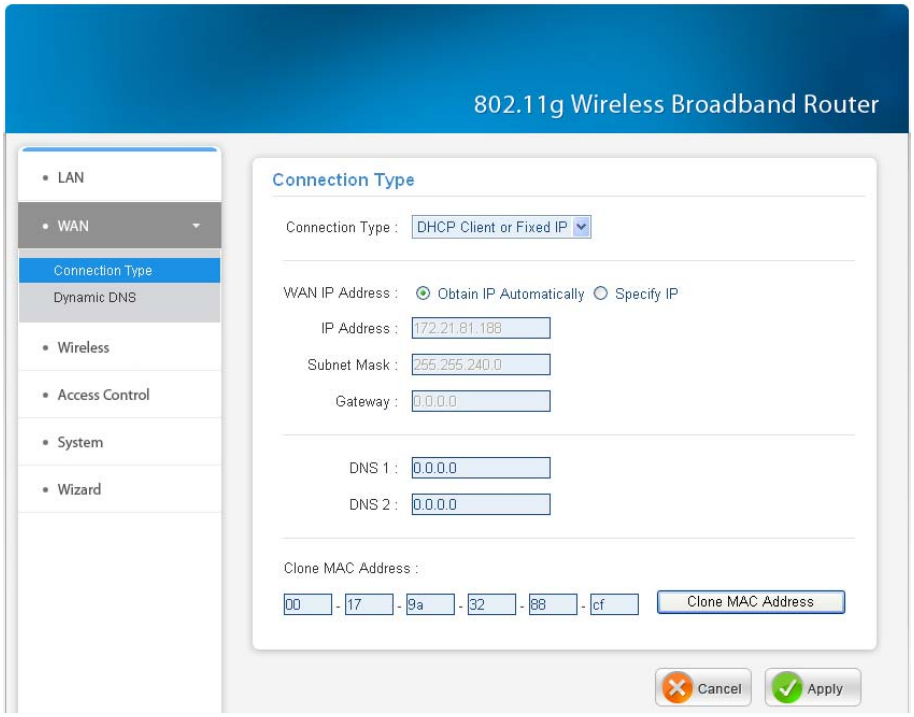


Figure 33.

WAN IP Address: Select whether user wants to specify an IP address manually, or want DHCP to obtain an IP address automatically. When Specify IP is selected, type the IP address, subnet mask, and default gateway in the text boxes. User's ISP will provide with this information.

IP Address: For the Specify mode, enter the specific IP address that provided by your ISP.

Subnet Mask: For the Specify mode, enter the specific subnet mask that provided by your ISP.

Gateway: For the Specify mode, enter the specific gateway IP address that provided by your ISP.

DNS 1/2: Manually specific DNS server IP address. For the Obtain IP Automatically mode, leave 0.0.0.0 hear, the DHCP server will provides DNS server automatically.

Clone MAC Address: If your ISP requires you to enter a specific MAC address, please enter it in. The Clone MAC Address button is used to copy the MAC address of your Ethernet adapter to the Router.

PPPoE with Obtain IP Automatically

If connected to the Internet using a PPPoE (Dial-up xDSL) Modem, the ISP will provide a Password and User Name, and then the ISP uses PPPoE. Choose this option and enter the required information.

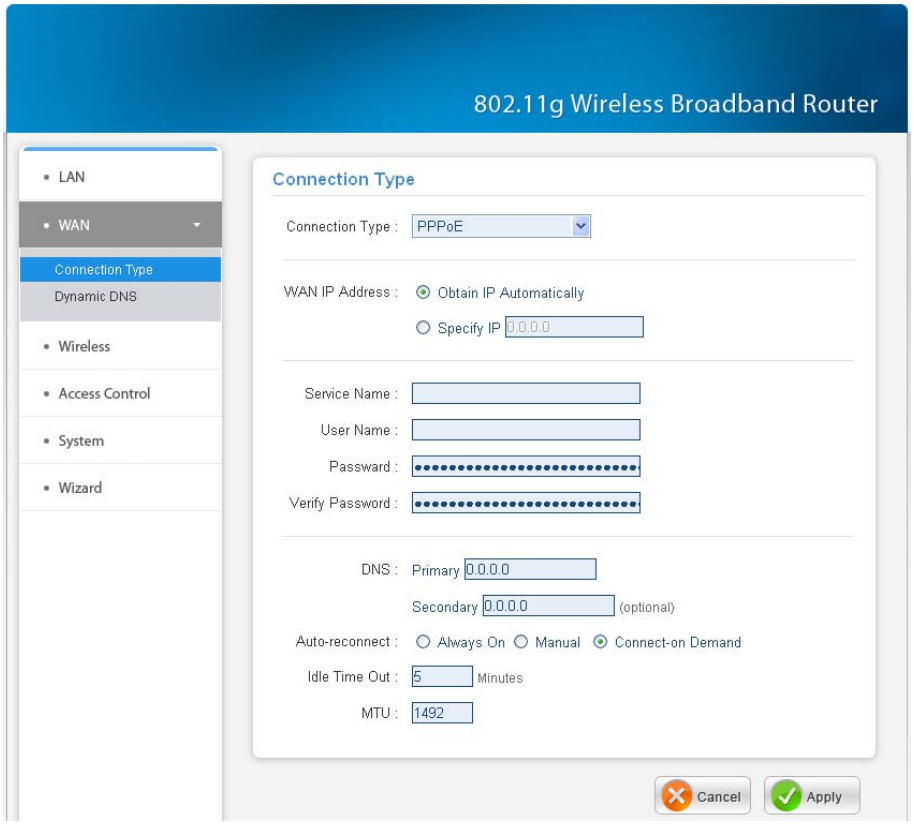


Figure 34.

PPPoE with Specify IP

If connected to the Internet using a PPPoE (Dial-up xDSL) Modem, the ISP will provide a Password, User Name and a Specify IP Address, choose this option and enter the required information.

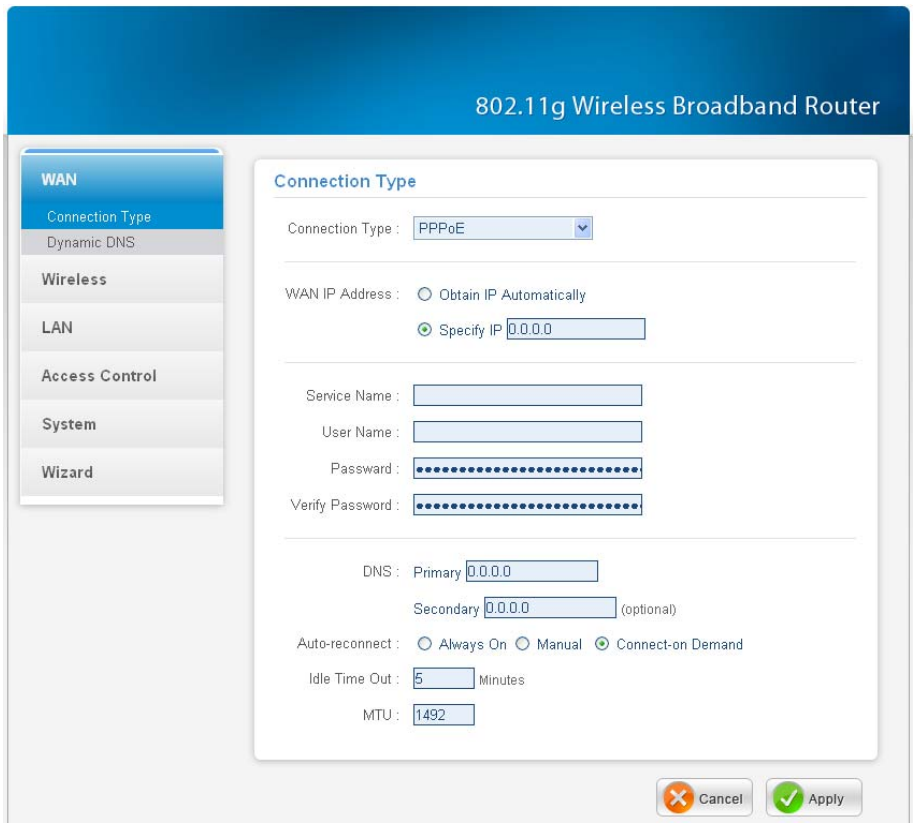


Figure 35.

PPTP/L2TP with Obtain IP Automatically

If connected to the Internet using a PPTP/L2TP (Dial-up xDSL) connection, enter the your Server IP, PPTP/L2TP Account and PPTP/L2TP Password, if your ISP has provided you with a DNS IP address, enter it in the DNS field, otherwise, leave it zero.

Figure 36. PPTP

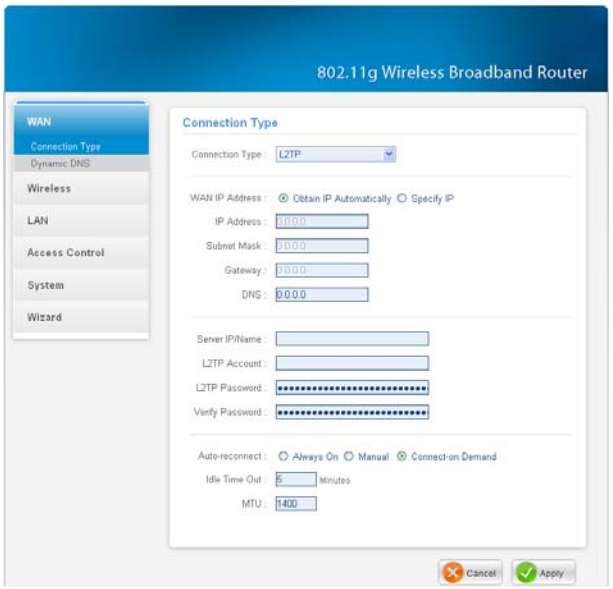


Figure 37. L2TP

PPTP/L2TP with Specify IP

If connected to the Internet using a PPTP/L2TP (Dial-up xDSL) connection, enter the your IP Address, Subnet Mask, Gateway IP address, DNS IP address, Server IP address, PPTP Account and PPTP Password.

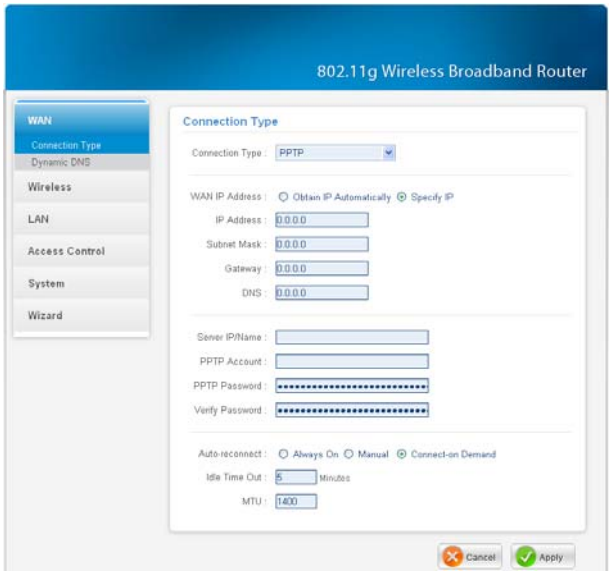


Figure 38. PPTP

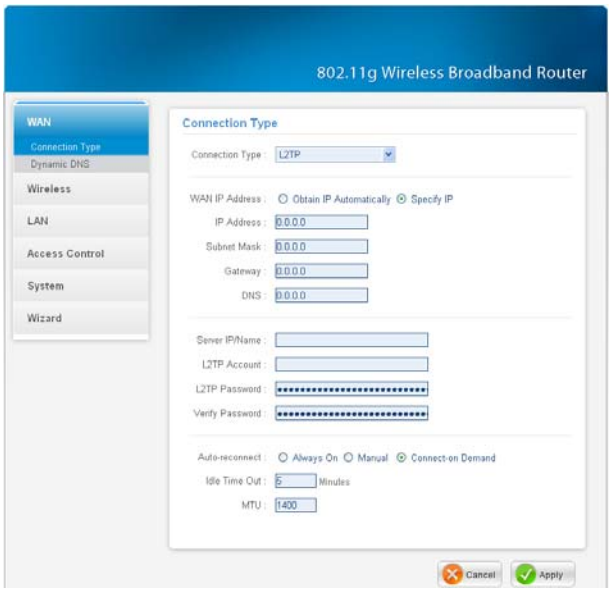
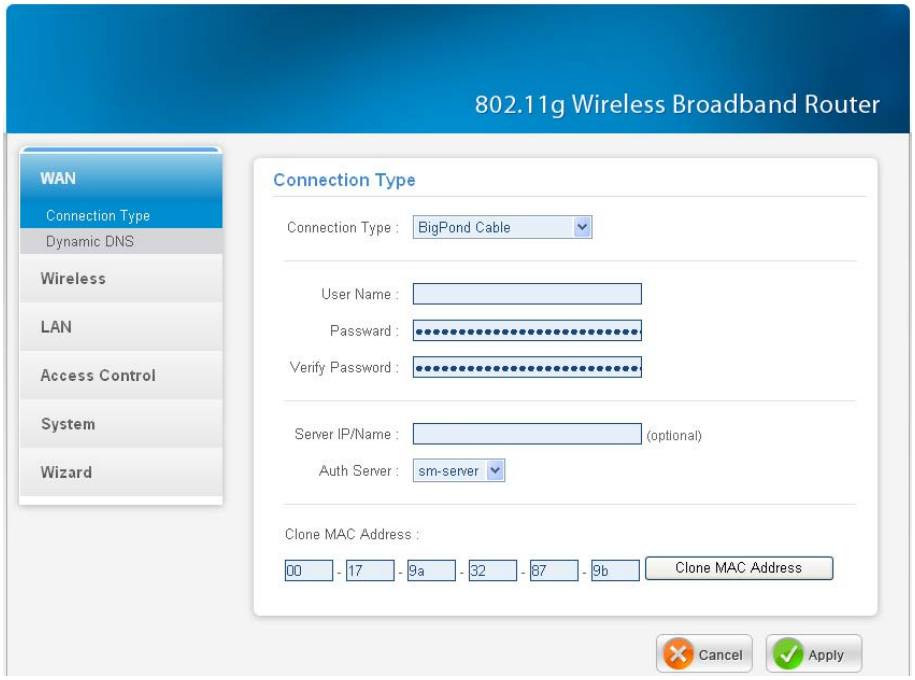


Figure 39. L2TP

BigPond Cable

If your ISP is Big Pond Cable, the ISP will provide a User Name, Password, Authentication Server and Login Server IP (Optional). Choose this option and enter the required information.



Dynamic DNS:

This synchronizes the DDNS server with your current Public IP address when you are online. First, you need to register your preferred DNS with the DDNS provider. Then, please selected one of DDNS server than fill the related information in the below fields: Host Name, User Name and Password.

Figure 40.

Wireless setting

This section enables user to set wireless communications parameters for the router's wireless LAN feature.

Basic

This page allow user to enable and disable the wireless LAN function, create a SSID, and select the channel for wireless communications.

Figure 41.

Wireless: Enables or disables the wireless LAN function of the wireless LAN Router.

SSID: Type an SSID in the text box. The SSID of any wireless device must match the SSID typed here in order for the wireless device to access the LAN and WAN via the router.

Extended Range Mode: Enable and disable the wireless Extended Range enhancement.

SSID Broadcast: While SSID Broadcast is enabled, all wireless clients will be able to view the WLAN Router's SSID. For security purposes, users may want to disable SSID Broadcast to ensure only authorized clients have access.

Channel: Select a transmission channel for wireless communications. The channel of any wireless device must match the channel selected here in order for the wireless device to access the LAN and WAN via the router.

Security

This function enables user to set authentication type for secure wireless communications. Open System allows public access to the router via wireless communications. Shared Key requires the user to set a WEP key to exchange data with other wireless clients that have the same WEP key. This router also supports WPA, WPA2 and WPA-PSK, WPA2-PSK.

Figure 42.

Security: Enable or Disable the wireless LAN security.

WEP

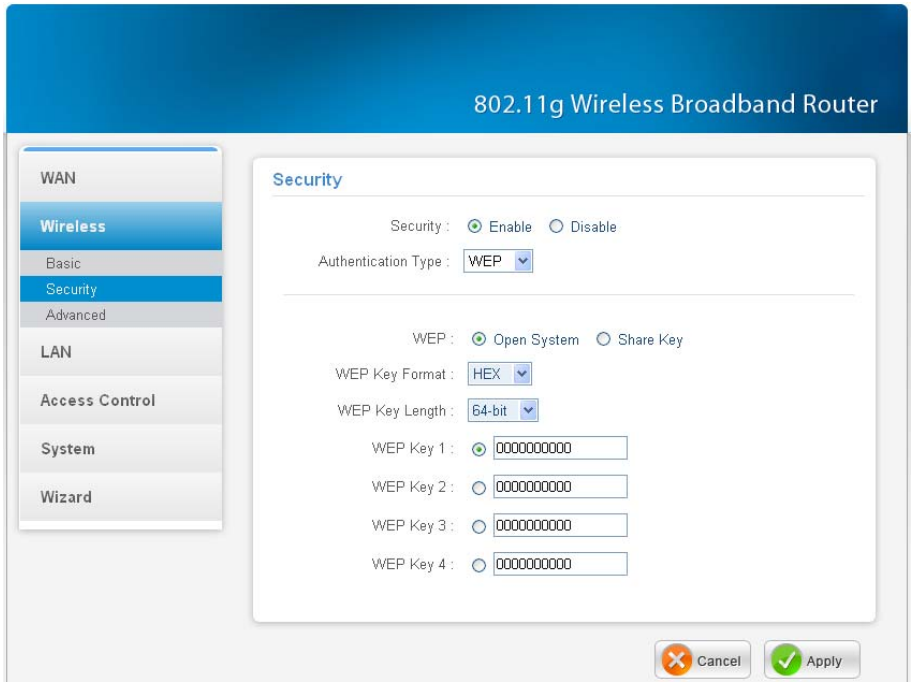


Figure 43.

WEP: Open System and Shared Key requires the user to set a WEP key to exchange data with other wireless clients that have the same WEP key.

WEP Key Format: Select the key format from the drop-down list HEX or ASCII.

WEP Key Length: Select the level of encryption from the drop-down list. The WLAN Router supports, 64 and 128-bit encryption.

WEP Key 1 ~ 4: Enables users to create up to 4 different WEP keys. Manually enter a set of values for each key. Select a key to use by clicking the radio button next to the key. Click “Clear” to erase key values.

WPA-PSK / WPA2-PSK

Figure 44.

Figure 45

If WPA or WPA2 **PSK** is selected, the above screen is shown.

Encryption Type: Select the encryption type for TKIP or AES encryption.

Passphrase: The length should be 8 characters at least.

WPA / WPA2

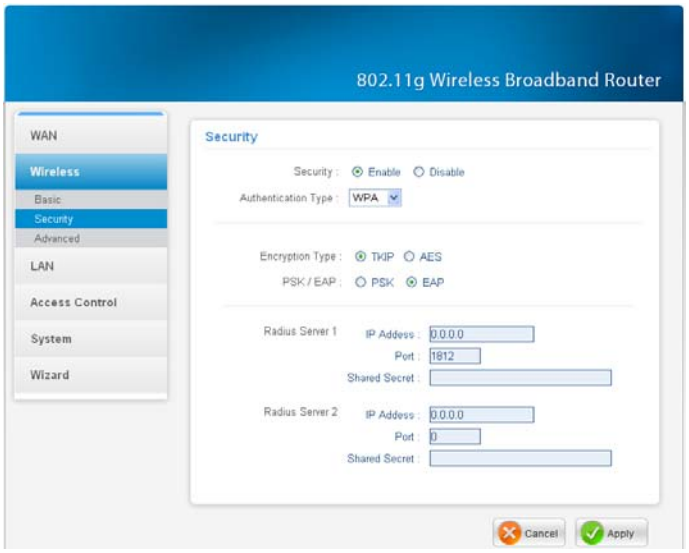


Figure 46.

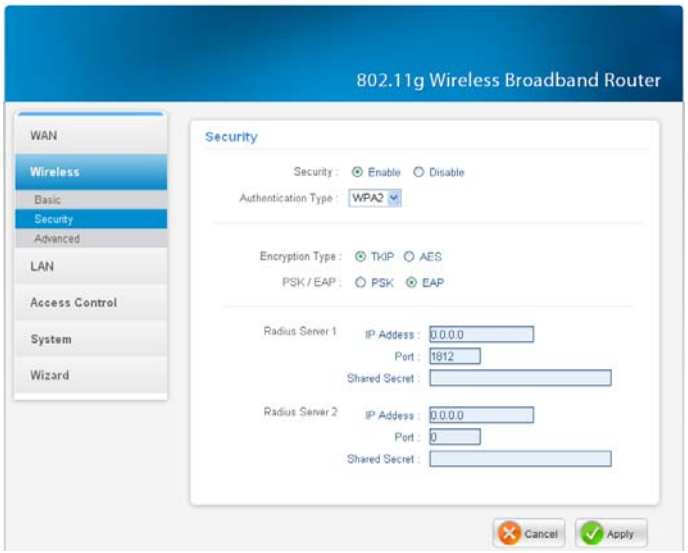


Figure 47

If WPA or WPA2 **EAP** is selected, the above screen is shown. Please set the length of the encryption key and the parameters for the RADIUS server.

Encryption Type: Select the encryption type for TKIP or AES encryption.

RASIUS Server:

1. Enter the IP address, Port used and Shared Secret by the Primary Radius Server.
2. Enter the IP address, Port used and Shared Secret by the Secondary Radius Server. (optional)

Advanced

This function enables user to configure advanced wireless functions.

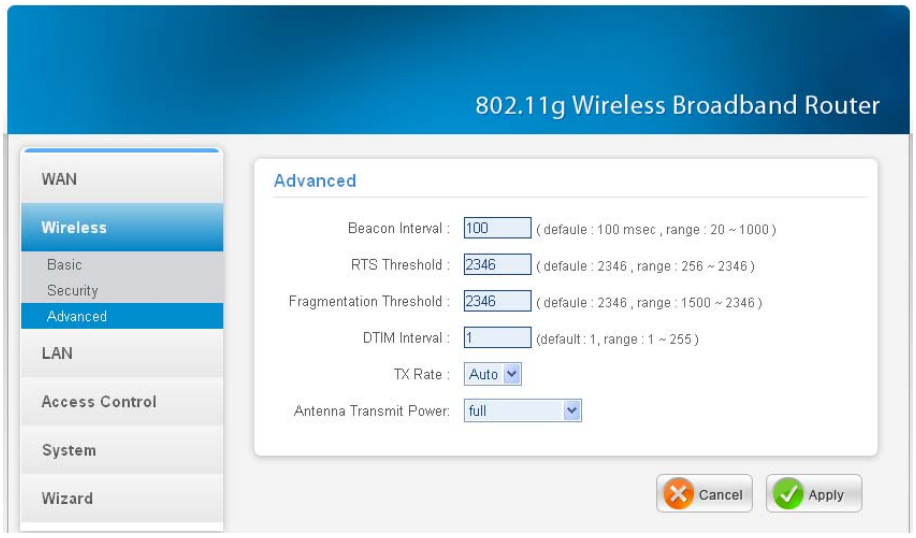


Figure 48.

Beacon Interval: Type the beacon interval in the text box. User can specify a value from 20 to 1000. The default beacon interval is 100.

RTS Threshold: Type the RTS (Request-To-Send) threshold in the text box. This value stabilizes data flow. If data flow is irregular, choose values between 256 and 2346 until data flow is normalized.

Fragmentation Threshold: Type the fragmentation threshold in the text box. If packet transfer error rates are high, choose values between 1500 and 2346 until packet transfer rates are minimized. (NOTE: set this fragmentation threshold value may diminish system performance.)

DTIM Interval: Type a DTIM (Delivery Traffic Indication Message) interval in the text box. User can specify a value between 1 and 255. The default value is 1.

TX Rates: Select one of the wireless communications transfer rates, measured in megabytes per second, based upon the speed of wireless adapters connected to the WLAN.

Antenna Transmit Power: Adjust the power of the antenna transmission by selecting from the drop down list: full, half (-3dB), quarter (-6dB), eighth (-9dB) or min.

LAN Setting

The function enables user to configure the LAN port IP address & DHCP Server.

Basic

This page leads to set LAN port properties, such as the host name, IP address, and subnet mask.

Figure 49.

Host Name: Type the host name in the text box. The host name is required by some ISPs. The default host name is "Wireless Router"

IP Address: This is the IP address of the router. The default IP address is 192.168.1.1.

Subnet Mask: Type the subnet mask for the router in the text box. The default subnet mask is 255.255.255.0.

DHCP

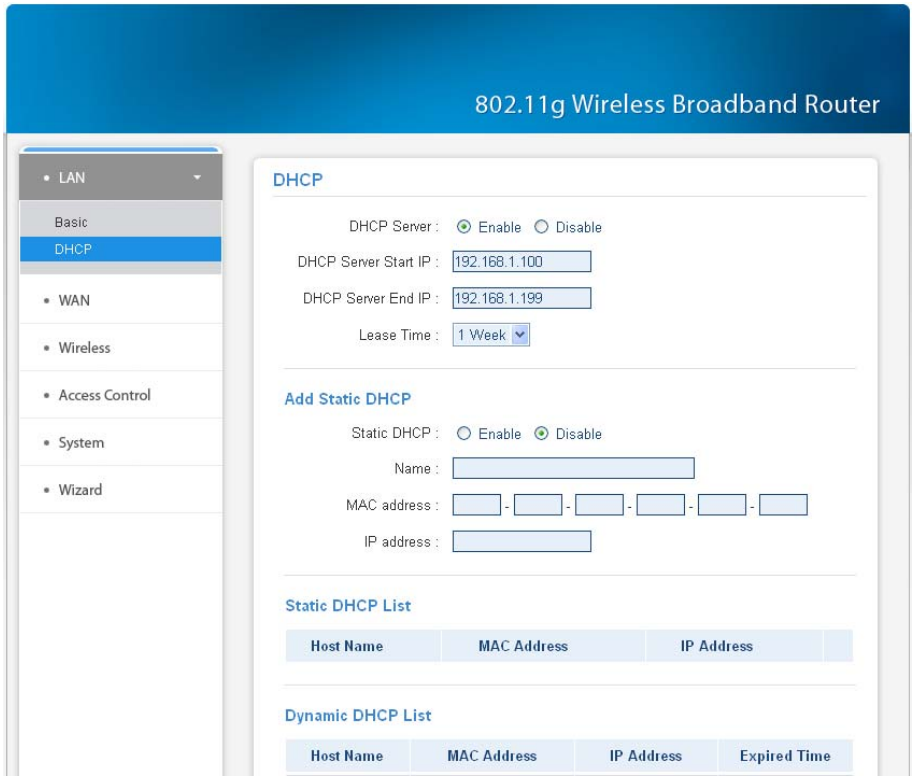


Figure 50.

DHCP Server: Enables the DHCP server to allow the router to automatically assign IP addresses to devices connecting to the LAN. DHCP is enabled by default.

DHCP Server Start IP: Type an IP address to serve as the start of the IP range that DHCP will use to assign IP addresses to all LAN devices connected to the router.

DHCP Server End IP: Type an IP address to serve as the end of the IP range that DHCP will use to assign IP addresses to all LAN devices connected to the router.

Lease Time: The lease time specifies the amount of connection time a network user be allowed with their current dynamic IP address.

Add Static DHCP: Selected Enable the Static DHCP allows you to assign a static IP address to the PC that has the IP address and MAC address mapping set in the Static DHCP List.

Static DHCP List: The static DHCP mapping will list in the table, providing the Host Name, MAC Address and IP Address.

Dynamic DHCP List: All dynamic DHCP client computers are listed in the table and providing the Host name, IP address, and MAC address and Expired Time of the client.

Access Control Setting

This access control enables you to define access restrictions, set up protocol and IP filters, create virtual servers, define access for special applications such as games, and set firewall rules.

Filter

Using filter to deny or allow the users to access. Five types of filters to select: MAC, IP Filter, URL blocking, Domain blocking and Protocol filter.

MAC Filters

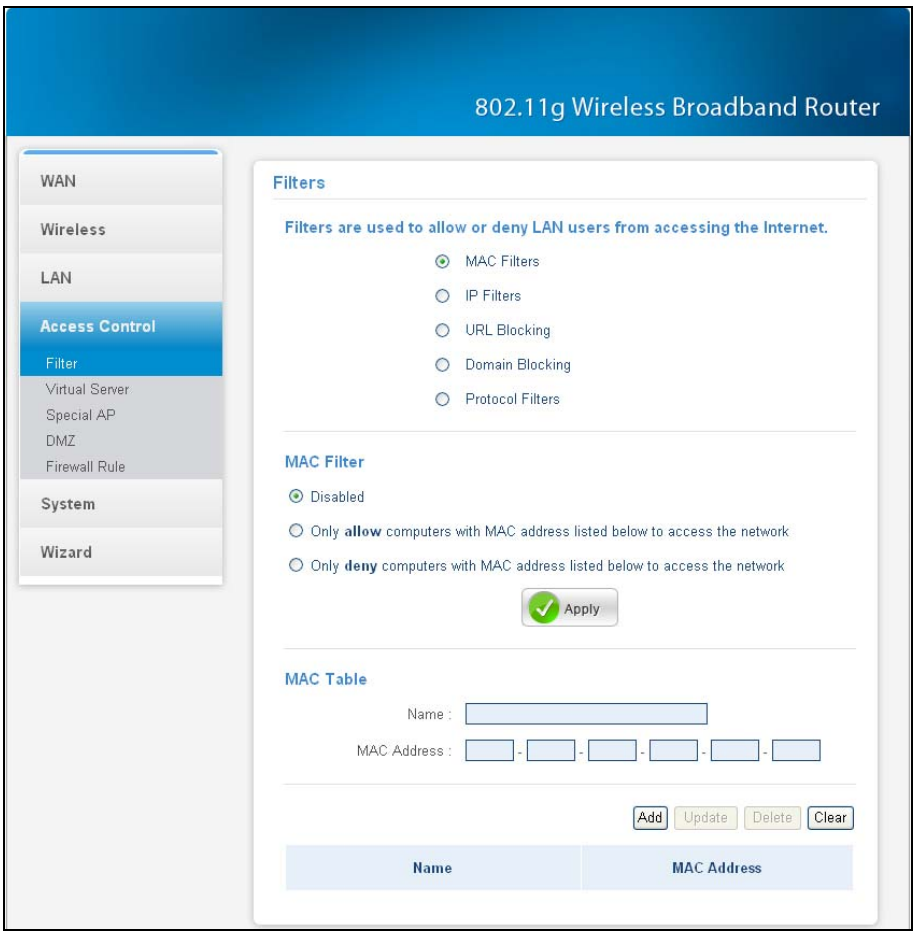


Figure 51.

MAC Filter: Enables you to allow or deny Internet access to users within the LAN based upon the MAC address of their network interface. Click the radio button next to Disabled to disable the MAC filter.

Disable: Disable the MAC filter function.

Allow: Only allow computers with MAC address listed in the MAC Table.

Deny: Computers in the MAC Table are denied Internet access.

MAC Table: Use this section to create a user profile which Internet access is denied or allowed. The user profiles are listed in the table at the bottom of the page. (Note: Click anywhere in the item. Once the line is selected, the fields automatically load the item's parameters, which you can edit.)

Name: Type the name of the user to be permitted/denied access.

MAC Address: Type the MAC address of the user's network interface.

Add: Click to add the user to the list at the bottom of the page.

Update: Click to update information for the user, if you have changed any of the fields.

Delete: Select a user from the table at the bottom of the list and click to remove the user profile.

Clear: Click to erase all fields and enter new information.

IP Filters

The IP filter function enables you to define a minimum and maximum IP address range filter; all IP addresses falling within the range are not allowed Internet access. The IP filter profiles are listed in the table at the bottom of the page. (Note: Click anywhere in the item. Once the line is selected, the fields automatically load the item's parameters, which you can edit.)

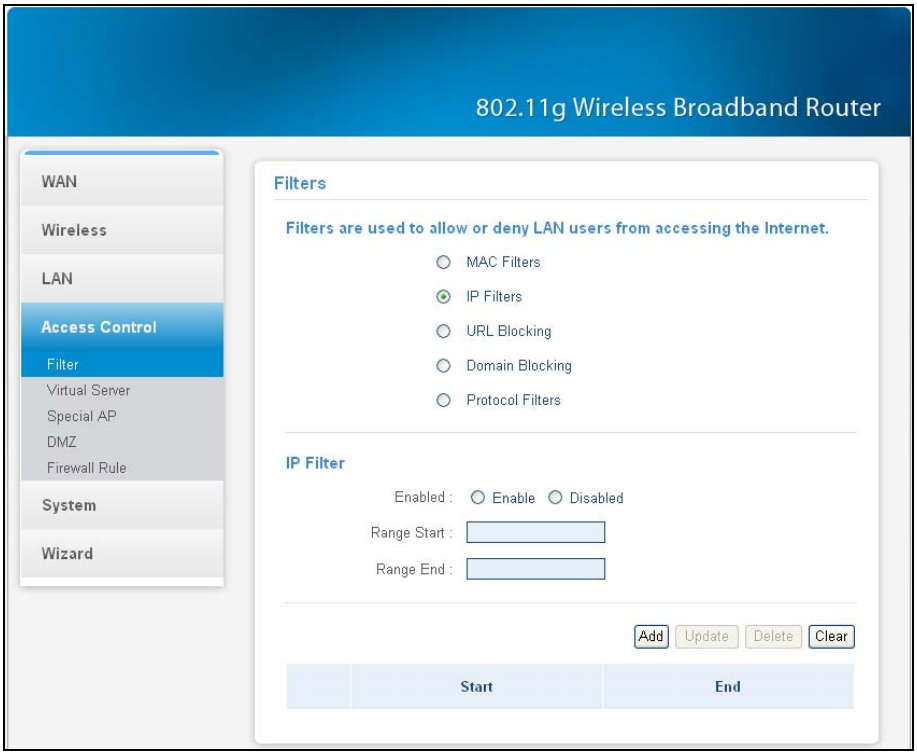


Figure 52.

Enable: Click to enable or disable the IP address filter function.

Range Start: Type the minimum address for the IP range. IP addresses falling between this value and the Range End are not allowed to access the Internet.

Range End: Type the minimum address for the IP range. IP addresses falling between this value and the Range Start are not allowed to access the Internet.

Add: Click to add the IP range to the table at the bottom of the screen.

Update: Click to update information for the range if you have selected a list item and have made changes.

Delete: Select a list item and click Delete to remove the item from the list.

Clear: Click to erase all fields and enter new information.

URL Blocking

You could enable URL blocking to deny the users from accessing the specified URL. Add those specified URL in the text box.

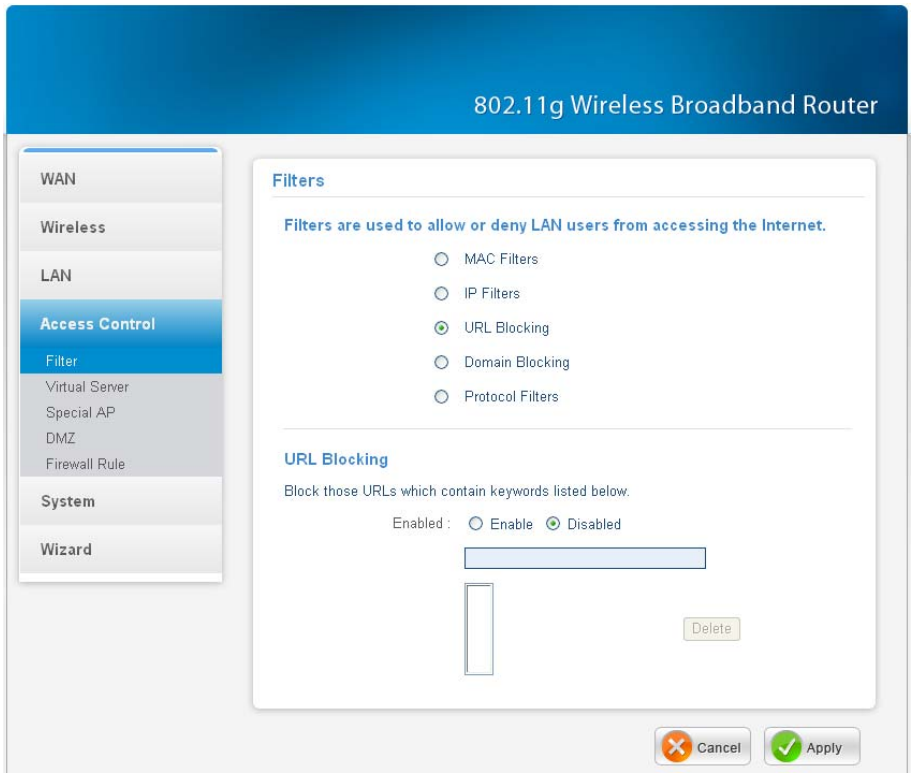


Figure 53

Enable / Disable: Enable or Disable the URL blocking function of the WLAN Router.
Add: Click to add the specific URL to the URL blocking list.

Delete: Selected a URL from the blocking list then click the ***Delete*** button to remove the URL from the URL Blocking list.

Domain Blocking

You could specify the domains that allow users to access or deny by clicking one of the two items. Also, add the specified domains in the text box.

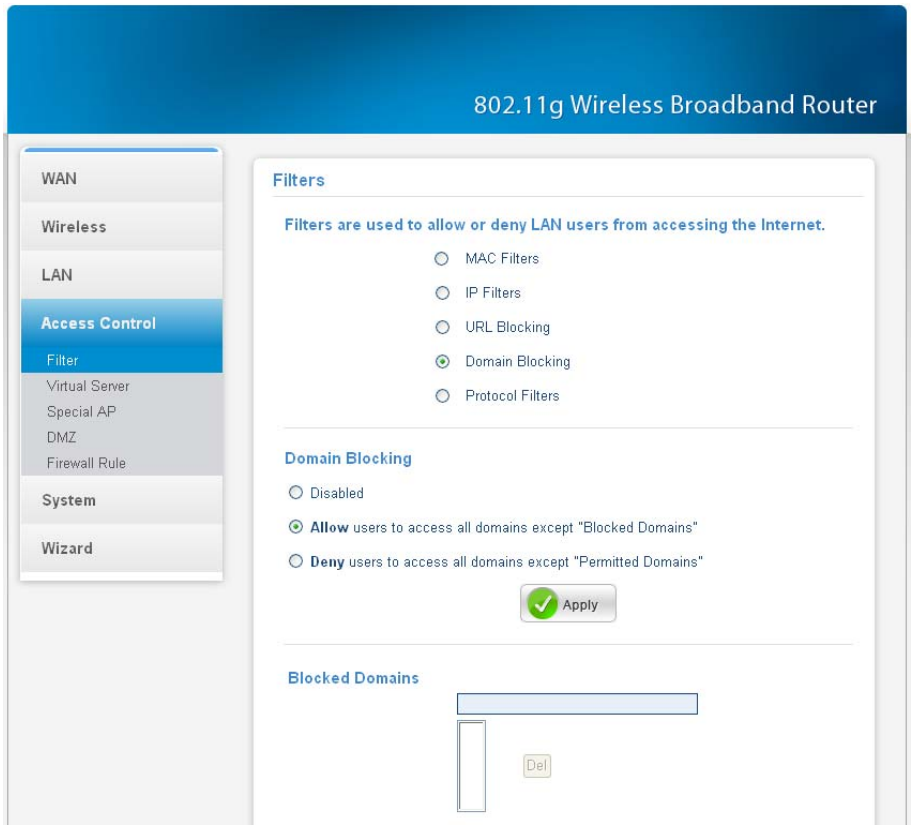


Figure 54.

Disable: Disable the Domain Blocking function.
Allow: Allow users to access all domains except “Blocking Domains”.
Deny: Deny users to access all domains except “Permitted Domains”.
Blocked/Permitted Domains: List domains you will Blocked or Permitted.
Apply: Click to add domain to the Blocked/Permitted Domains list.
Del: Select a user from the table at the bottom of the list and click Del to remove the user profile.

Protocol Filters

This protocol filter enables you to allow and deny access based upon a communications protocol list you create. The protocol filter profiles are listed in the table at the bottom of the page.

Note: When selecting items in the table at the bottom, click anywhere in the item. The line is selected, and the fields automatically load the item's parameters, which you can edit.

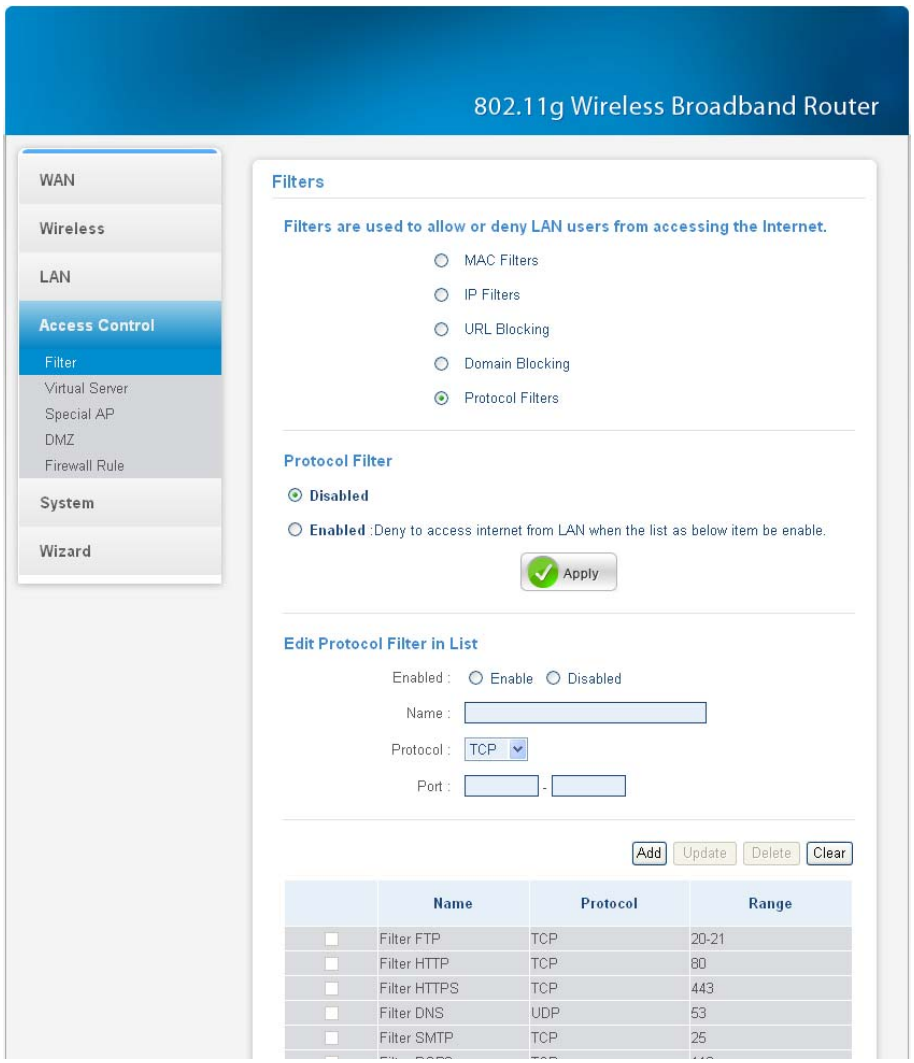


Figure 55.

Enable: Click to enable or disable the Protocol filter.

Name: Type the name of the user to be denied access.

Protocol: Select a protocol (TCP, UDP or ICMP) to use for the virtual server.

Port: Type the port range of the protocol.

Add: Click to add the protocol filter to the table at the bottom of the screen.

Update: Click to update information for the protocol filter if user have selected a list item and have made changes.

Delete: Select a list item and click Delete to remove the item from the list.

Clear: Click to erase all fields and enter new information.

Virtual Server

The virtual server function enables users to create a virtual server via the WLAN Router. If the WLAN Router is set as a virtual server, remote users requesting Web or FTP services through the WAN are directed to local servers in the LAN. The WLAN Router redirects the request via the protocol and port numbers to the correct LAN server. The Virtual Sever profiles are listed in the table at the bottom of the page.

Note: When selecting items in the table at the bottom, click anywhere in the item. The line is selected, and the fields automatically load the item's parameters, which user can edit.

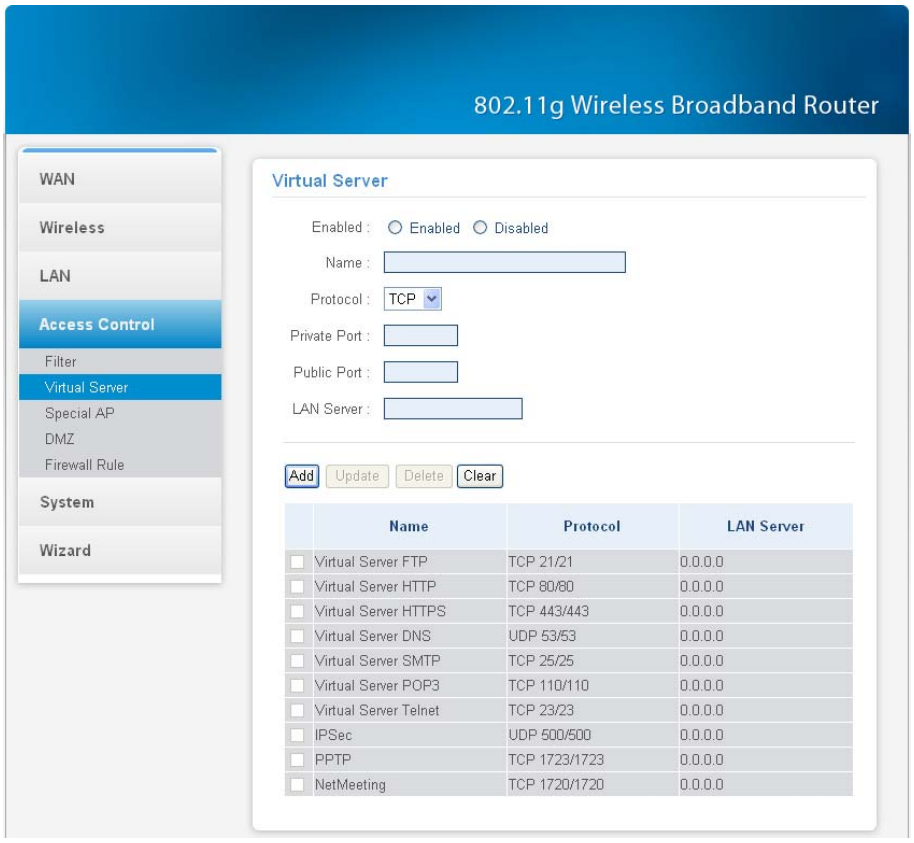


Figure 56

Enable: Click to enable or disable the virtual server.

Name: Type a descriptive name for the virtual server.

Protocol: Select a protocol (TCP or UDP) to use for the virtual server.

Private Port: Type the port number of the computer on the LAN that is being used to act as a virtual server.

Public Port: Type the port number on the WAN that will be used to provide access to the virtual server.

LAN Server: Type the LAN IP address that will be assigned to the virtual server.

Add: Click to add the virtual server to the table at the bottom of the screen.

Update: Click to update information for the virtual server if the user has selected a listed item and has made changes.

Delete: Select a listed item and click “Delete” to remove the item from the list.

Clear: Click to erase all fields and enter new information.

Special AP

The special AP function enables users to specify special applications, such as games which require multiple connections that are blocked by NAT. The special applications profiles are listed in the table at the bottom of the page.

Note: When selecting items in the table at the bottom, click anywhere in the item. The line is selected, and the fields automatically load the item's parameters, which user can edit.

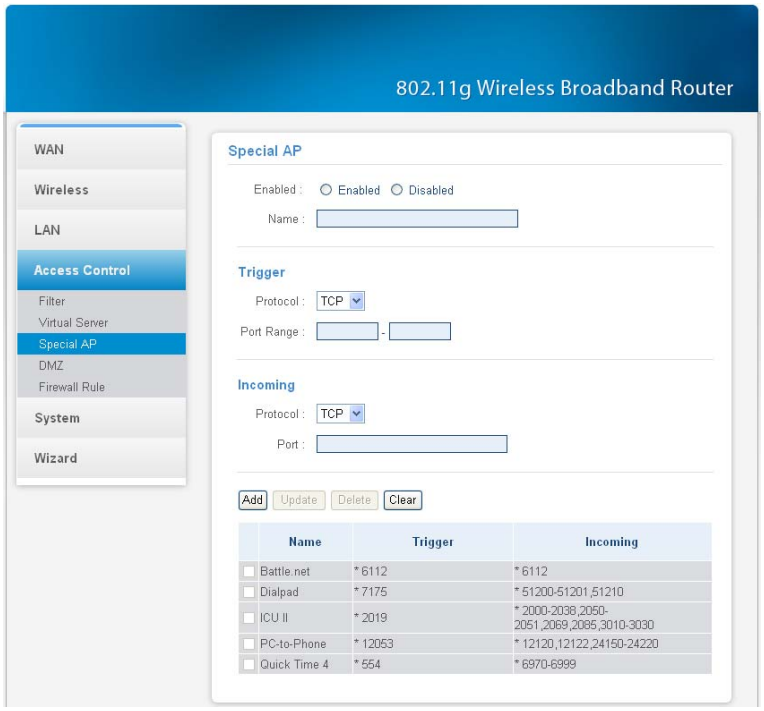


Figure 57.

Enable: Click to enable or disable the application profile. When enabled, users will be able to connect to the application via the WLAN Router's WAN connection. Click "Disabled" on a profile to prevent users from accessing the application on the WAN connection.

Name: Type a descriptive name for the application.

Trigger: Defines the outgoing communication that determines whether the user has legitimate access to the application.

- **Protocol:** Select the protocol TCP or UDP that can be used to access the application, the "*" is meaning to both of TCP and UDP protocols.
- **Port Range:** Type the port range that can be used to access the application in the text boxes.

Incoming: Defines which incoming communications users are permitted to connect with.

- **Protocol:** Select the protocol TCP or UDP that can be used by the incoming communication, the "*" is meaning to both of TCP and UDP protocols.
- **Port:** Type the port number that can be used for the incoming communication.

Add: Click to add the special application profile to the table at the bottom of the screen.

Update: Click to update information for the special application if user have selected a list item and have made changes.

Delete: Select a list item and click Delete to remove the item from the list.

Clear: Click to erase all fields and enter new information.

DMZ

The DMZ function enables users to create a DMZ for those computers that cannot access Internet applications properly through the WLAN Router and associated security settings.

Note: Any clients added to the DMZ exposes the clients to security risks such as viruses and unauthorized access.

Enable: Click to enable or disable the DMZ.

DMZ Host IP: Type a host IP address for the DMZ. The computer with this IP address acts as a DMZ host with unlimited Internet access.

Apply: Click to save the settings.

Firewall Rule

The firewall rule function enables users to set up the firewall. The WLAN Router provides basic firewall functions, by filtering all the packets that enter the WLAN Router using a set of rules. The rules are listed in sequential order--the lower the rule number, the higher the priority the rule has.

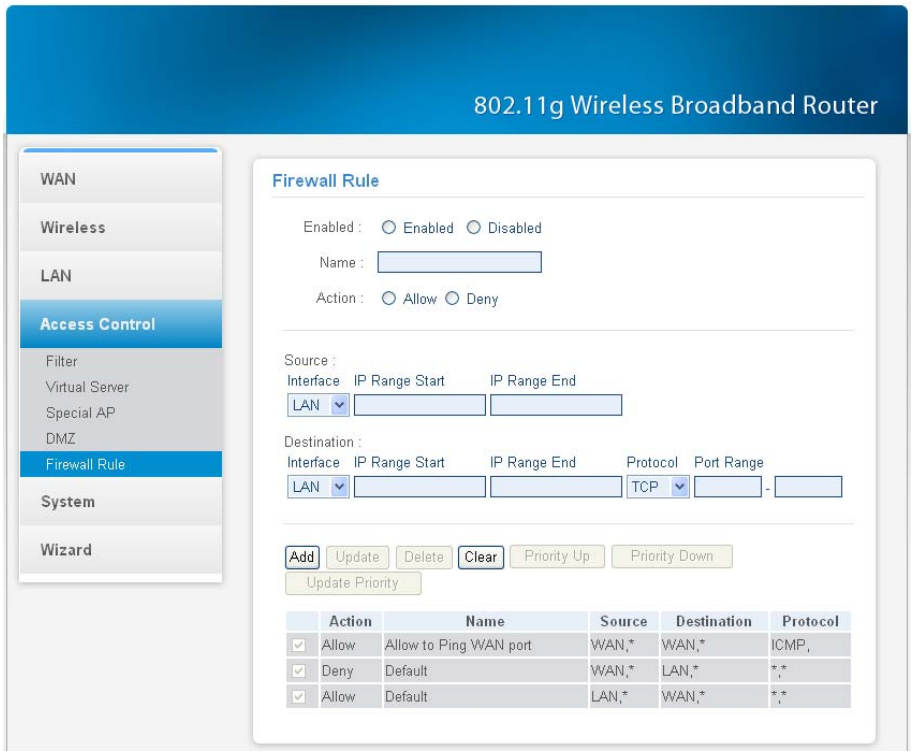


Figure 58.

Enable: Click to enable or disable the firewall rule profile.

Name: Type a descriptive name for the firewall rule profile.

Action: Select whether to allow or deny packets that conform to the rule.

Source: Defines the source of the incoming packet that the rule is applied to.

- **Interface:** Select which interface (WAN or LAN) the rule is applied to.
- **IP Range Start:** Type the start IP address that the rule is applied to.
- **IP Range End:** Type the end IP address that the rule is applied to.

Destination: Defines the destination of the incoming packet that the rule is applied to.

- **Interface:** Select which interface (WAN or LAN) the rule is applied to.
- **IP Range Start:** Type the start IP address that the rule is applied to.
- **IP Range End:** Type the end IP address that the rule is applied to.
- **Protocol:** Select the protocol (TCP, UDP, or ICMP) of the destination.
- **Port Range:** Select the port range.

Add: Click to add the rule profile to the table at the bottom of the screen.

Update: Click to update information for the rule if the user has selected a listed item and has made changes.

Delete: Select a listed item and click **"Delete"** to remove the item from the list.

Clear: Click to erase all fields and enter new information.

Priority Up: Select a rule from the list and click **"Priority Up"** to increase the priority of the rule.

Priority Down: Select a rule from the list and click **"Priority Down"** to decrease the priority of the rule.

Update Priority: After increasing or decreasing the priority of a rule, click **"Update Priority"** to save the changes.

System Setting

This system setting enables users to change password, set the device time, view the device information, restart the system, save and load different settings as profiles, restore factory default settings, upgrade the firmware, and ping remote IP addresses….etc.

Password

This function enables users to set administrative and user passwords. These passwords are used to gain access to the WLAN Router interface.

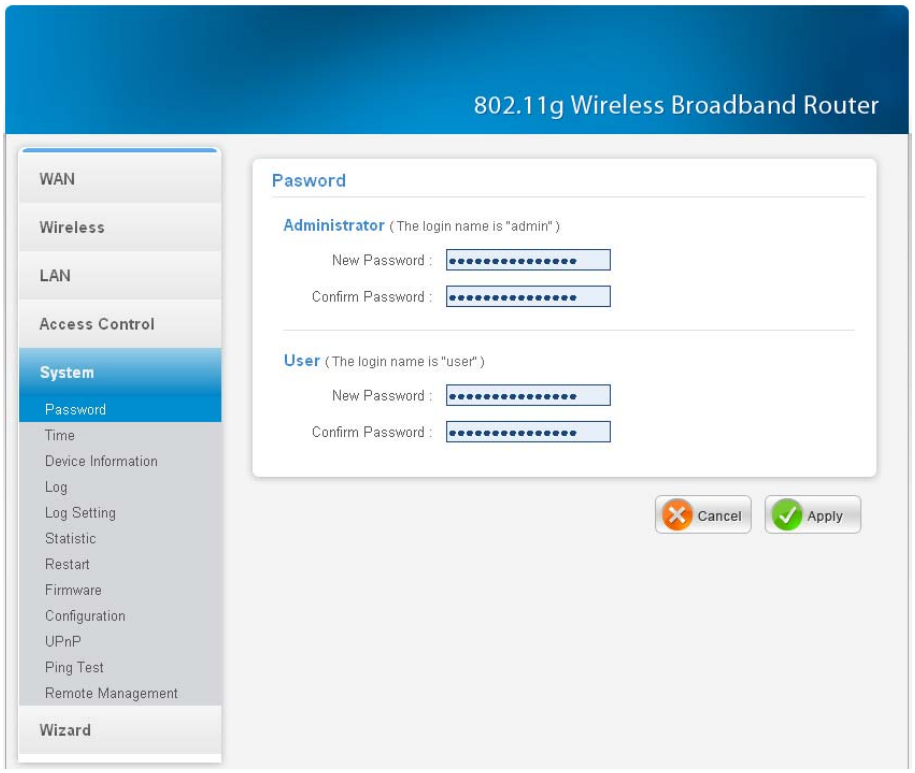


Figure 59

Time

This function enables users to set the time and date for the WLAN Router's real-time clock, select properly time zone, and enable or disable daylight saving.

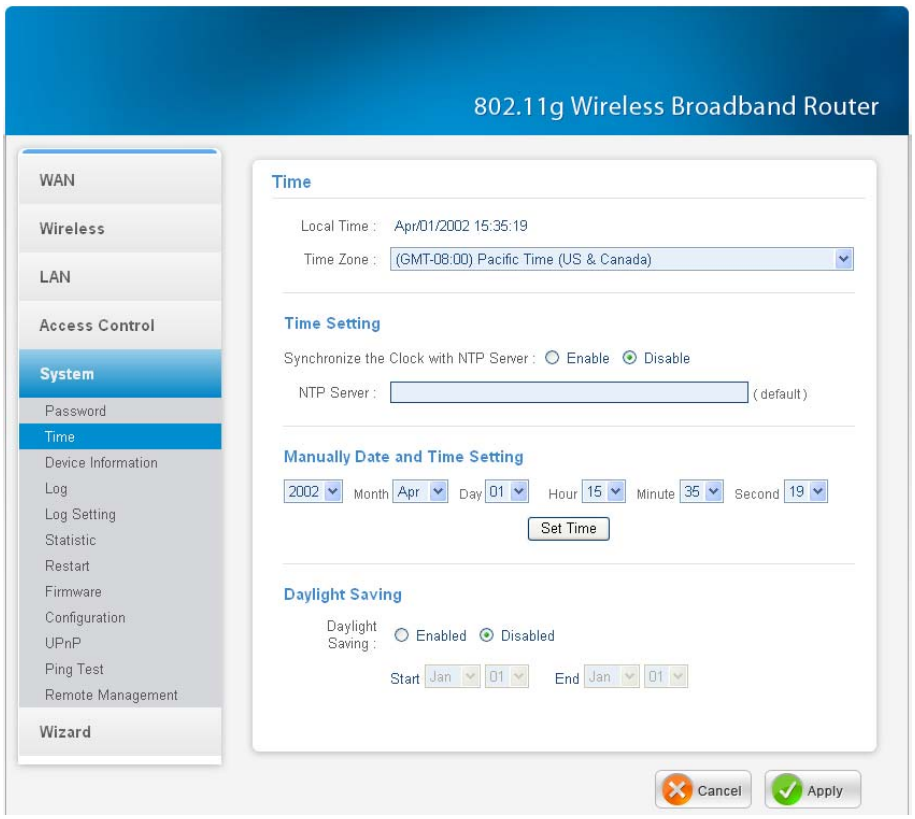


Figure 60

Local Time: Displays the local time and date.

Time Zone: Select the time zone from the drop-down list.

Synchronize the clock with NTP Server: Enable or disable the WLAN Router automatically adjust the system time from NTP Server.

NTP server: The Simple Network Time Protocol (SNTP) server allows the WLAN Router to synchronize the system clock to the global Internet through the SNTP Server. Specify the NTP domain name or IP address in the text box.

Manually Date and Time Setting: Manually setting the WLAN Router system time, press the ***Set Time*** button to update the system time.

Daylight Saving: Enables users to enable or disable daylight saving time. When enabled, select the start and end date for daylight saving time.

Device Information

This function enables users to view the WLAN Router's WAN, Wireless, LAN and System configurations.

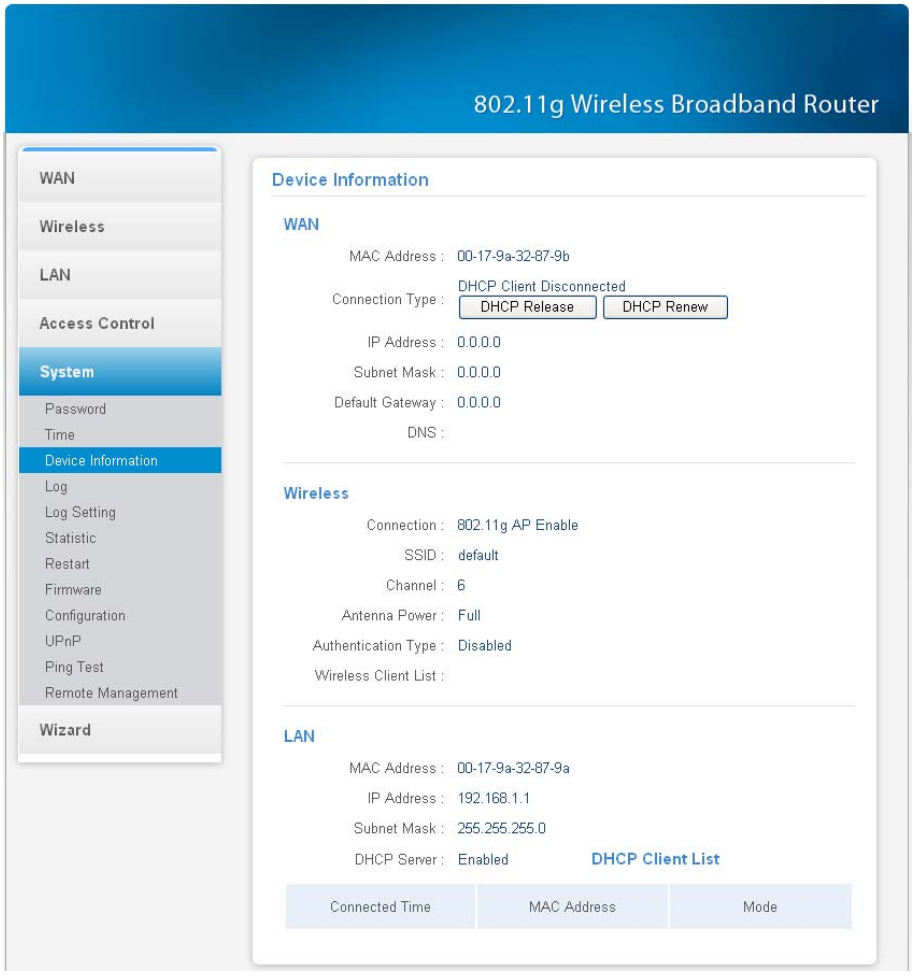


Figure 61

WAN: This section displays the WAN interface configuration including the MAC address, Connection status, DHCP client status, IP address, Subnet mask, Default gateway, and DNS.

Wireless: This section displays the wireless configuration information, including the MAC address, the Connection status, SSID, Channel and Authentication type.

LAN: This section displays the LAN interface configuration including the MAC address, IP Address, Subnet Mask, and DHCP Server Status. Click "DHCP Table" to view a list of client stations currently connected to the WLAN Router LAN interface.

Click ***"DHCP Release"*** to release all IP addresses assigned to client stations connected to the WAN via the WLAN Router. Click ***"DHCP Renew"*** to reassign IP addresses to client stations connected to the WAN.

Log

This function enables users to view a running log of Router system statistics, events, and activities. The log displays up to 200 entries. Older entries are overwritten by new entries.

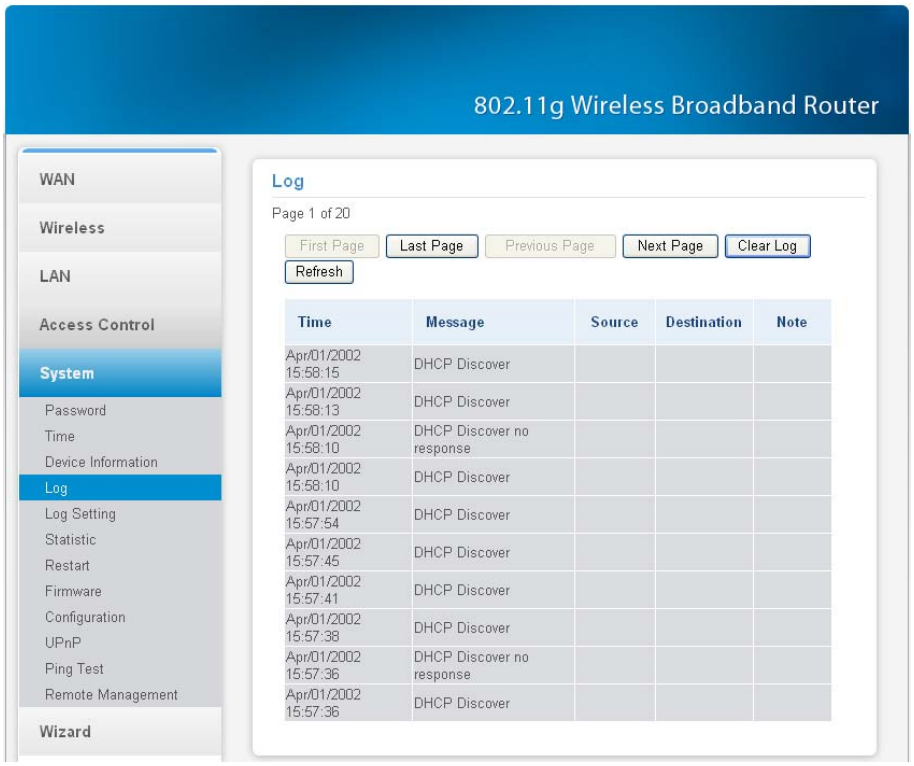


Figure 62.

The Log screen commands are as follows:

Click ***"First Page"*** to view the first page of the log

Click ***"Last Page"*** to view the final page of the log

Click **"*Previous Page*"** to view the page just before the current page

Click **"*Next Page*"** to view the page just after the current page

Click **"*Clear Log*"** to delete the contents of the log and begin a new log

Click **"*Refresh*"** to renew log statistics

Log Setting

This function enables users to set Router Log parameters.

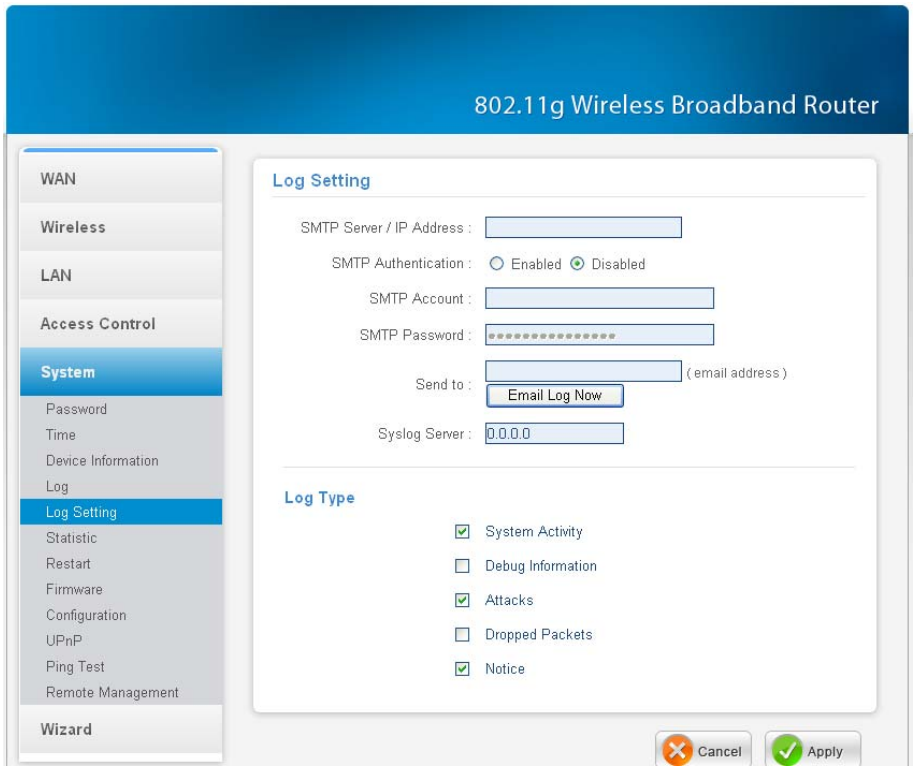


Figure 63.

SMTP Server: Type your SMTP server address here.

Send to: Type an email address for the log to be sent to. Click “Email Log Now” to immediately send the current log.

SMTP Authentication: Selected the Enabled if the SMTP server need for authentication, fill in account name and password in SMTP Account field and SMTP Password field.

SMTP Account: If the SMTP Authentication enabled, fill in the SMTP account name here.

SMTP Password: If the SMTP Authentication enabled, fill in the password of the SMTP account here.

Syslog Server: Type the IP address of the Syslog Server if user wants the WLAN Router to listen and receive incoming Syslog messages.

Log Type: Enables users to select what items will be included in the log:

System Activity: Displays information related to WLAN Router operation.

Debug Information: Displays information related to errors and system malfunctions.

Attacks: Displays information about any malicious activity on the network.

Dropped Packets: Displays information about packets that have not been transferred successfully.

Notice: Displays important notices by the system administrator.

Statistic

This function displays a table that shows the rate of packet transmission via the WLAN Router's LAN, WAN and Wireless ports (in bytes per second).

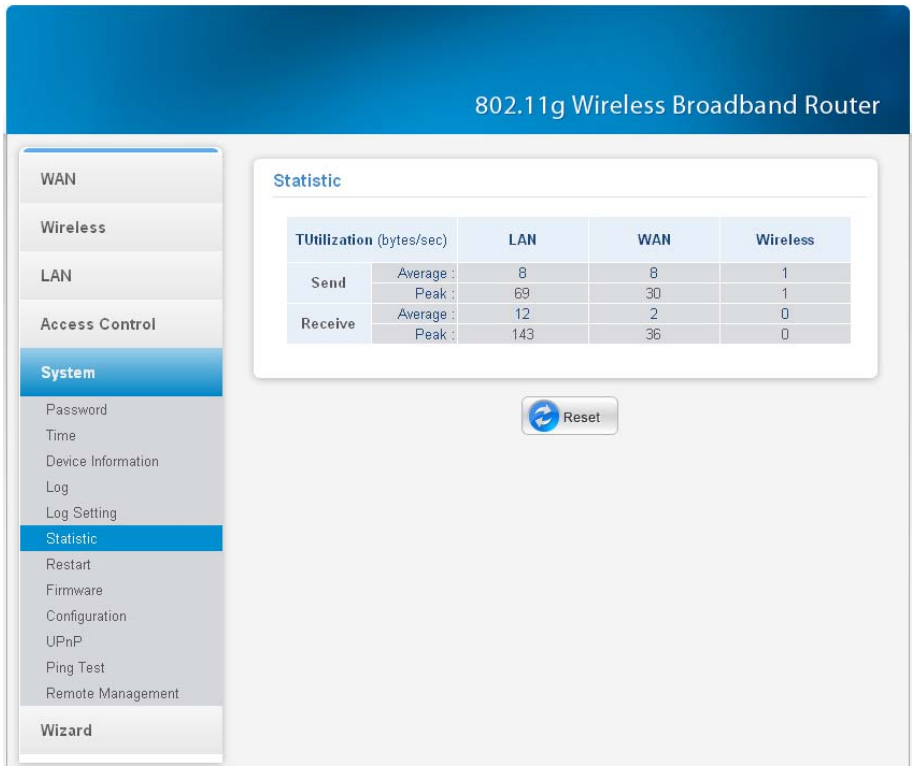


Figure 64.

Click **"Reset"** to erase all statistics and begin logging statistics again.

Restart

Click ***"Restart"*** to restart the system in the event the system is not performing correctly.

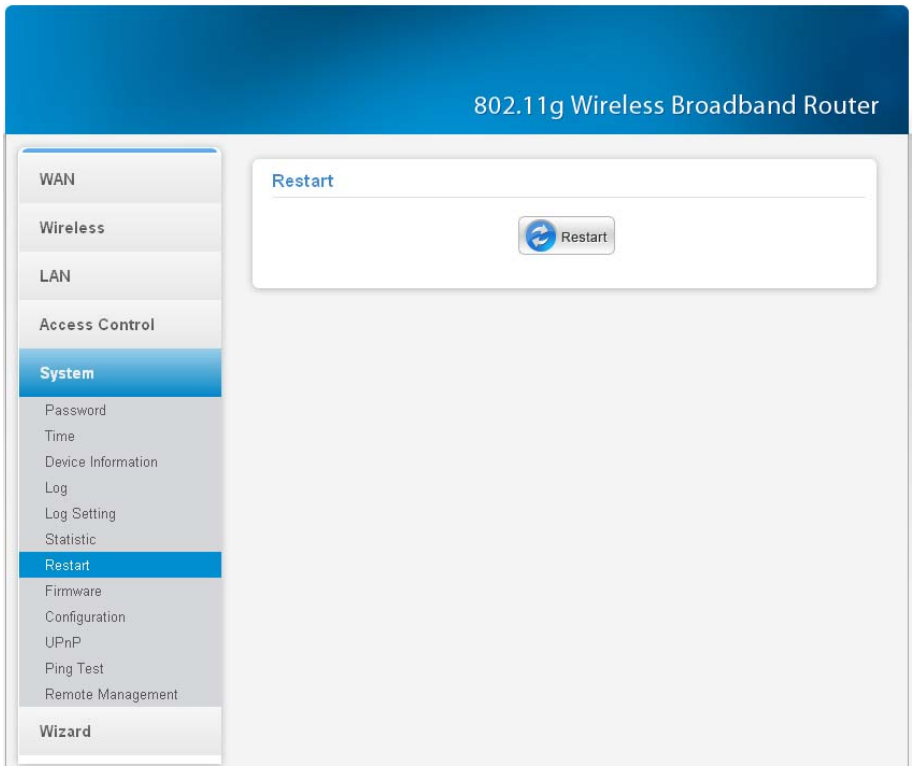


Figure 65.

Firmware

This function enables users to keep the WLAN Router firmware up to date.

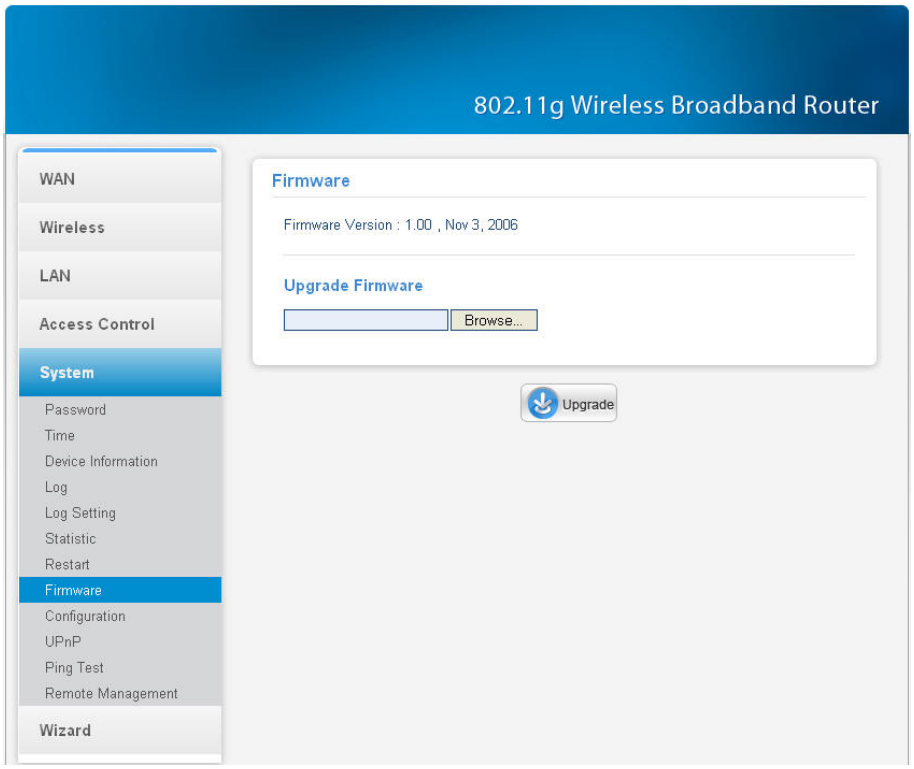


Figure 66.

Please follow the below instructions:

Download the latest firmware from the manufacturer's Web site, and save it to disk.

Click **"Browse"** and go to the location of the downloaded firmware file.

Select the file and click **"Upgrade"** to update the firmware to the latest release.

Configuration

This function enables users to save settings as a profile and load profiles for different circumstances. User can also load the factory default settings, and run a setup wizard to configure the WLAN Router and Router interface.

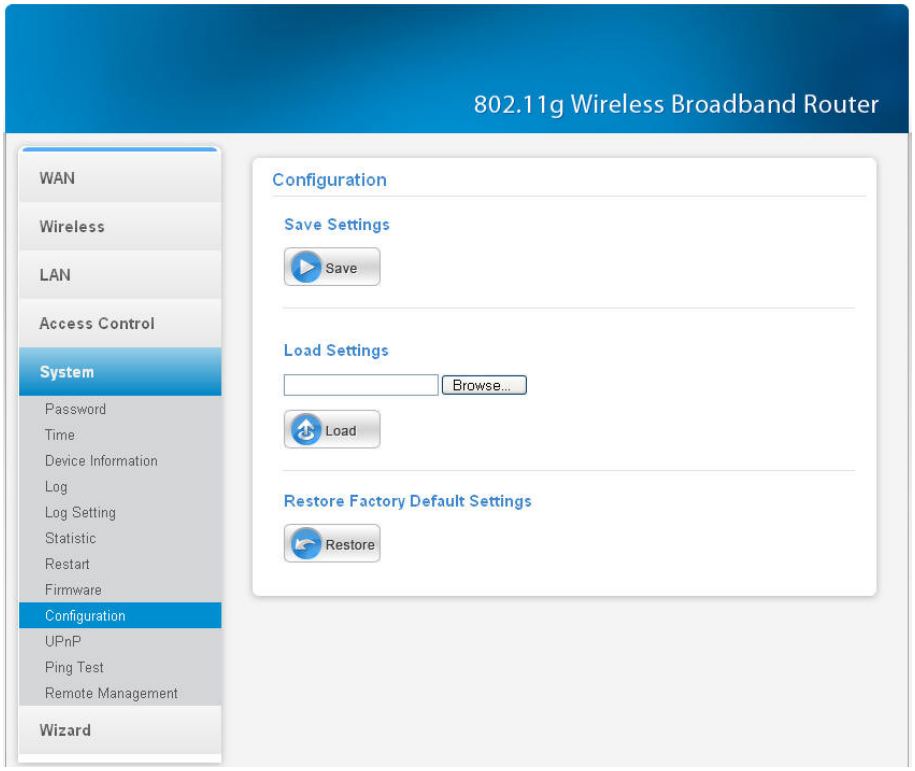


Figure 67.

UPnP

This function enables users to enable or disable the UPnP function on the WLAN Router.

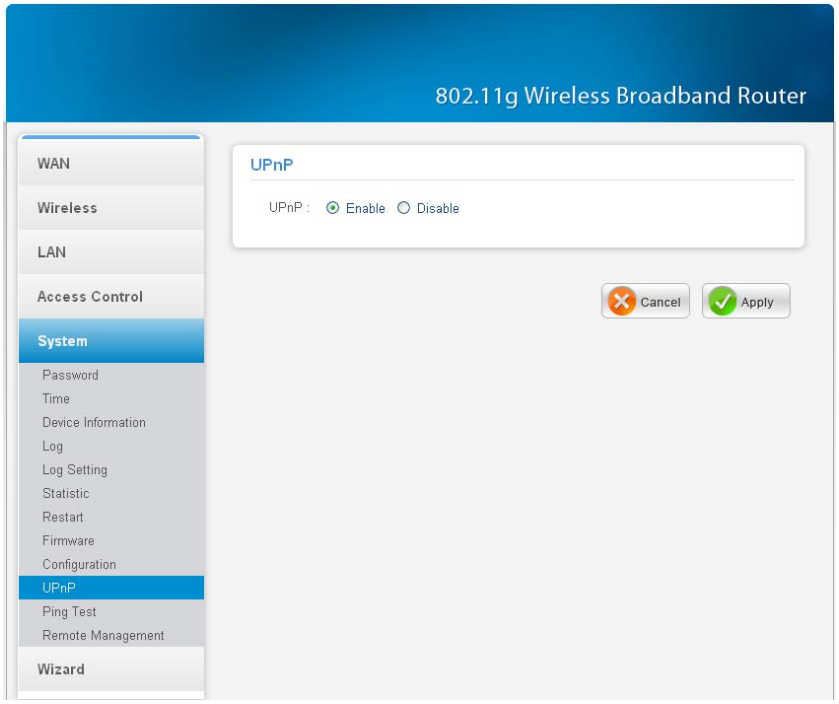


Figure 68.

UPnP: Select to enable or disable the UPnP function on the WLAN Router.

Ping Test

The ping test enables users to determine whether an IP address or host is present on the Internet. Type the host name or IP address in the text box and click Ping button to start the Ping test.

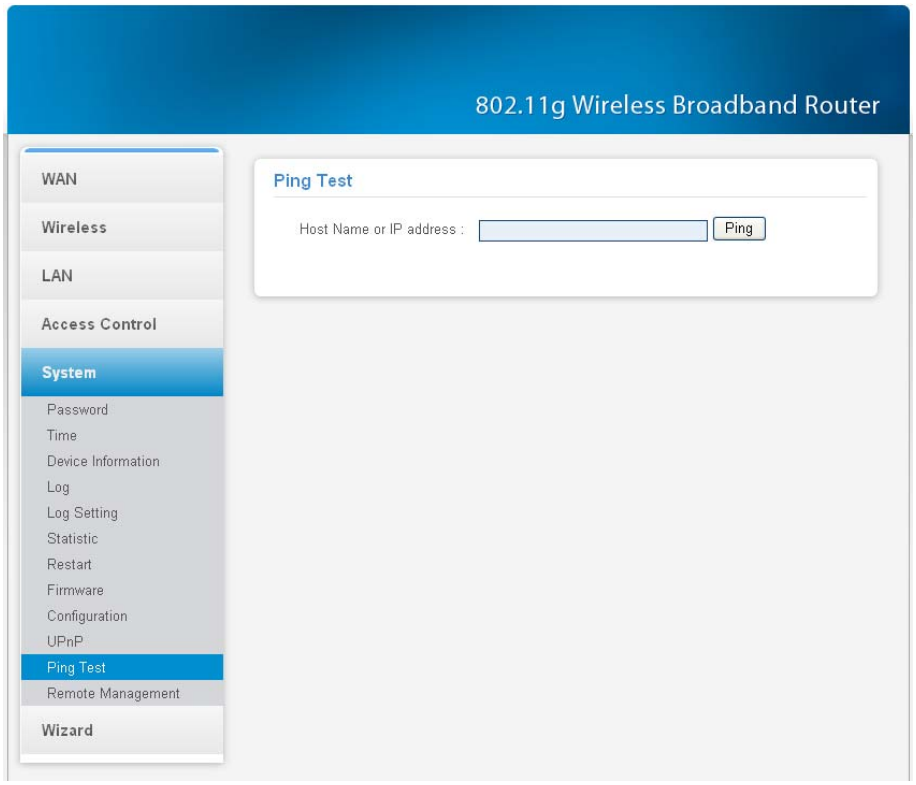


Figure 69.

Remote Management

This function enables users to set up remote management. Using remote management, the WLAN Router can be configured through the WAN via a Web browser. A user name and password are required to perform remote management.

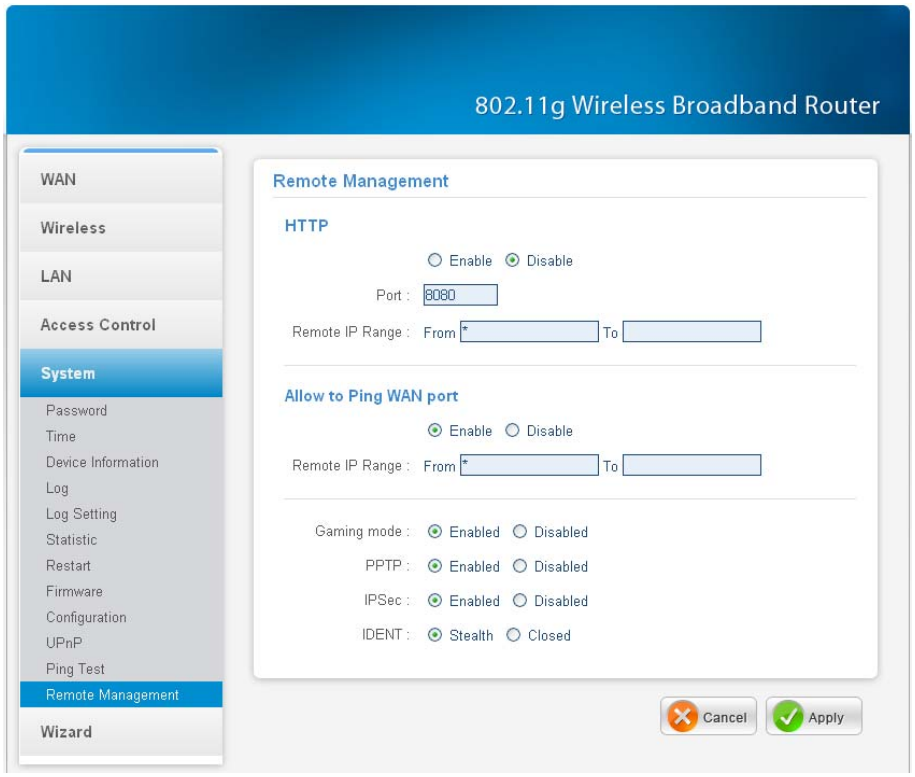


Figure 70.

HTTP: Enables users to set up HTTP access for remote management.

Remote IP Range: Type a range of IP addresses that can be pinged from remote locations

Gaming mode: If user is experiencing difficulties when playing online games or even certain applications that use voice data, user may need to enable Gaming Mode for these applications to work correctly. When not playing games or using these voice applications, it is recommended that Gaming Mode be disabled.

PPTP: Enables users to set up PPTP access for remote management.

IPSec: Enables users to set up IPSec access for remote management.

IDENT: Default is stealth. This enables users to set port 113 stealth.

General	
Standards	IEEE 802.3u 100BASE-TX Fast Ethernet IEEE 802.11g; IEEE 802.11b
Protocol	CSMA/CD
Radio Technology	802.11b: Direct Sequence Spread Spectrum (DSSS) 802.11g: Orthogonal Frequency Division Multiplexing (OFDM)
Data Transfer Rate	802.11b: 1, 2, 5.5, 11Mbps (auto sense) 802.11g: 6, 9, 12, 18, 24, 36, 48, 54Mbps(auto sense) Ethernet: 10Mbps (half duplex), 20Mbps (full-duplex) Fast Ethernet: 100Mbps (half duplex), 200Mbps (full- duplex)
Topology	Star
Receiver Sensitivity	54Mbps: Typical -70dBm @ 10% PER (Packet Error Rate) 11Mbps: Typical -85dBm @ 8% PER (Packet Error Rate)
TX Power	15±2dBm typically @ 802.11g 13±2dBm typically @ 802.11b
Network Cables	10BASE-T: 2-pair UTP Cat. 3,4,5 (100 m), EIA/TIA- 568 100-ohm STP (100 m) 100BASE-TX: 2-pair UTP Cat. 5 (100 m), EIA/TIA-568 100-ohm STP (100 m)
Frequency Range	2412 ~ 2484 MHz ISM band (channels 1 ~ 14)
Modulation Schemes	DBPSK/DQPSK/CCK/OFDM
Security	64/128-bits WEP Encryption; WPA, WPA-PSK, WPA2, WPA2-PSK
Channels	1 ~ 11 channels (FCC); 1 ~ 13 channels (ETSI); 1 ~ 14 channels (MKK)
Number of Ports	LAN: 4 x 10/100Mbps Auto-MDIX Fast Ethernet port WAN: 1 x 10/100Mbps Auto-MDIX Fast Ethernet port
Physical and Environmental	
DC inputs	7.5VDC/1A
Power Consumption	5W (Max)
Temperature	Operating: 0^{O} ~ 40^{O} C, Storage: -10^{O} ~ 70^{O} C
Humidity	Operating: 10% ~ 90%, Storage: 5% ~ 90%
Dimensions	147 x 115 x 35 mm (W x H x D) without Antenna
EMI:	FCC Class B, CE Mark B