Aztech
www.aztech.com

# WL830RT4 Wireless G Broadband Router

## User Manual

VERSION 1.0

# Contents

# About the Manual

This manual provides a description of the components, basic operation, and advanced configuration options of the device.

## Target Audience

This manual is designed for users who are required to install and maintain the router. It assumes the user of this manual has basic knowledge and experience in configuring routers, computer networks, and computer systems.

## Document Structure

The manual is divided into the following sections:

| Chapter | Contents |
|---|---|
| 1 | About the Manual |
| 2 | About the Router |
| 3 | About the Web Manager |
| 4 | Getting Started |
| 5 | Advanced Settings |
| 6 | Maintenance |
| 7 | FAQ |
| 8 | Glossary |
| 9 | Regulatory Compliance Notices |

# About the Router

Congratulations on your purchase of WL830RT4 Wireless G Broadband Router. This product allows you to converge your computer and other network appliances into a unified network through wired or wireless links. It also enables you to share Internet connection among the different network components simultaneously.

WL830RT4 has a browser-based configuration tool called Web Manager. From the Web Manager, you can easily setup, configure, and modify router settings. The Web Manager's right pane is dedicated to display help topics to guide your tasks.

WL830RT4 is designed to suit the needs of homes and small offices. There are four ports for wired connection and an access point for wireless connection. Up to 54 Mbps transmission rate can be achieved through the access point. WL830RT4 also features the eXtended Range™ WLAN transmission technology which effectively extends the transmission range 4 to 9 times more than other traditional wireless routers.

WL830RT4 provides easy to setup security options. It has an access control mechanism to establish access and device restrictions. For wireless security, it utilizes WEP, WPA, and WPA2 authentication standards with up to 152-bit encryption. These standards are used to dissuade unauthorized connection into your network. The router also supports VPN pass-through for secure data transmission.

NAT and DHCP server functions are built-in. The router also supports Virtual Server and DMZ host for Port Triggering. Through remote management, you can manage and monitor the network activities in real time.

# Specifications

| General | |
|---|---|
| Standards | IEEE 802.3, 802.3u, 802.11b and 802.11g |
| Protocols | TCP/IP, PPPoE, DHCP, ICMP, NAT, SNTP |
| Ports | One 10/100M Auto-Negotiation WAN RJ45 port, Four 10/100M Auto-Negotiation LAN RJ45 ports supporting Auto MDI/MDIX |
| Cabling Type | 10BASE-T<br>▪ UTP category 3, 4, 5 cable (maximum 100m)<br>▪ EIA/TIA-568 100. STP (maximum 100m)<br>100BASE-TX<br>▪ UTP category 5, 5e cable (maximum 100m)<br>▪ EIA/TIA-568 100. STP (maximum 100m) |
| Radio Data Rate | 54/48/36/24/18/12/9/6Mbps or 11/5.5/3/2/1Mbp |
| Power Supply | 9V~ 0.8A |
| LEDs | Power, SYS, WLAN, WAN, 1-4 |
| Safety & Emissions | FCC, CE |

| Environmental and Physical | |
|---|---|
| Operating Temp. | 0 °C~40 °C (32 °F~104 °F ) |
| Operating Humidity | 10% - 95% RH, Non-condensing |
| Dimensions (W×D×H) | 7.3×5.7×1.7 in. (186×146×44 mm) (without antenna) |

# Requirements

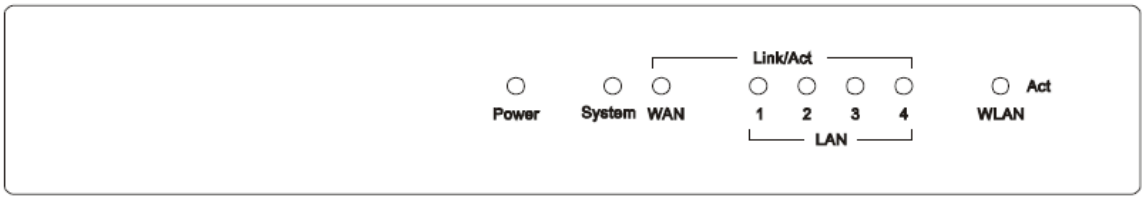
Here are the minimum requirements:

- Broadband Internet Access Account (DSL/Cable/Ethernet)
- One DSL/Cable modem with Ethernet connectors
- Each computer needs an Ethernet Adapter with an Ethernet cable with TCP/IP protocol installed
- Web browser (At least Microsoft Internet Explorer 5.0 or Netscape Navigator 6.0)

# Device Design

## Front Panel

The router's front panel consists of LED's that indicate connection status.

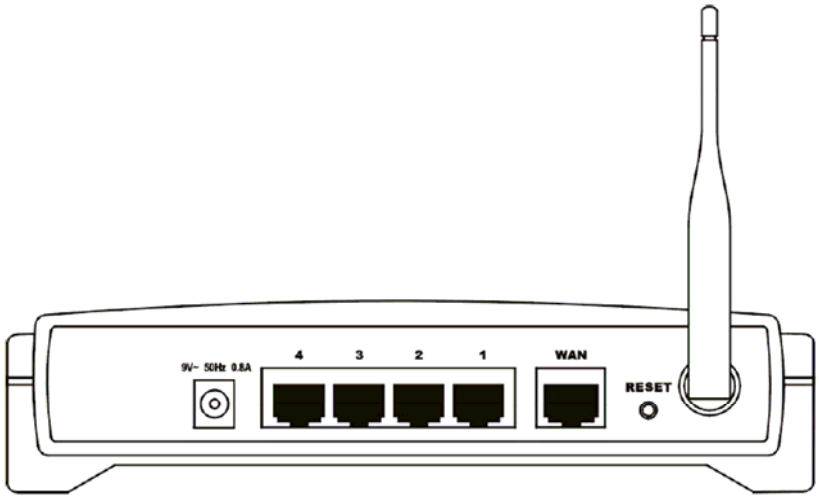



**Front Panel**

| Label | Status | Description/Function |
|---|---|---|
| POWER | Off | No power connection. |
| | On | Power is on. |
| System | Off | Hardware/System error |
| | On | The router is initializing |
| | Flashing | The router is working properly |
| WAN | Off | No wired device is connected to the corresponding port |
| | On | An inactive device is connected to the corresponding port |

| | | |
|---|---|---|
| | Flashing | The device connected to the corresponding port is active. |
| LAN 1-4 | Off | No wired device is connected to the corresponding port |
| | On | An inactive device is connected to the corresponding port |
| | Flashing | The device connected to the corresponding port is active. |
| WLAN | Off | No wireless device connected to the router |
| | Flashing | Access point is enabled |

# Rear Panel

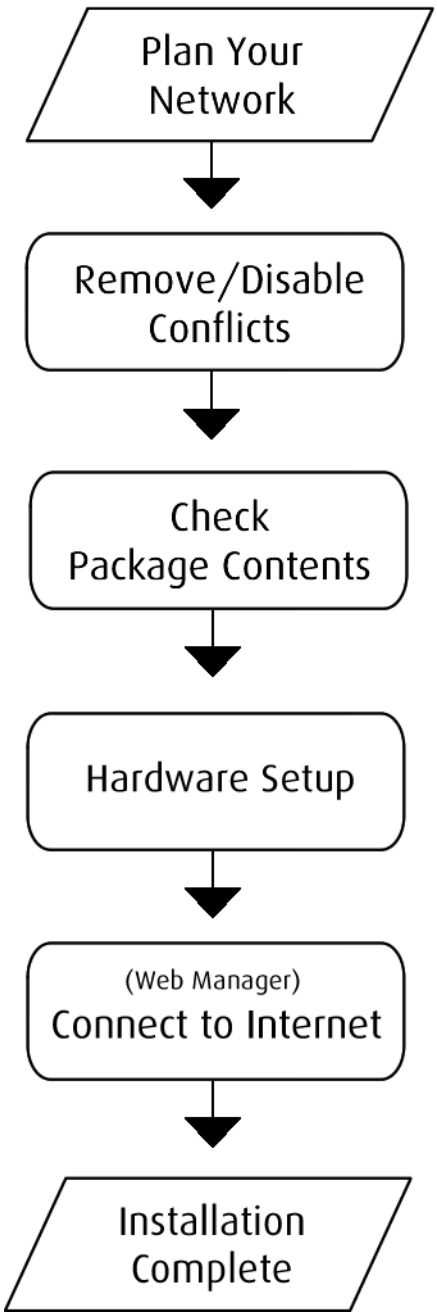



**Rear Panel**

| Label | Description/Function |
|---|---|
| 9V 50Hz .8A | AC power socket |
| 4-1 | Ethernet port |
| WAN | Port for connecting to a cable or DSL modem |
| RESET | To manually reset the router, unplug the power first. Press RESET then plug the power cord without releasing RESET for 3-4 seconds. When the SYS LED lights up, release RESET and then wait for the router to restart. |
| Antenna | Access point |

# Getting Started

Setting up the device is easy. The flowchart below provides an outline of the steps you need to go through. There are brief descriptions beside each step to help you along. Detailed instructions are provided in the subsequent pages.




Draw a simple map of how you want to connect your computers and other network devices.

Check the TCP/IP settings and Internet Properties. You may need to disable some applications and delete temporary Internet files before installation.

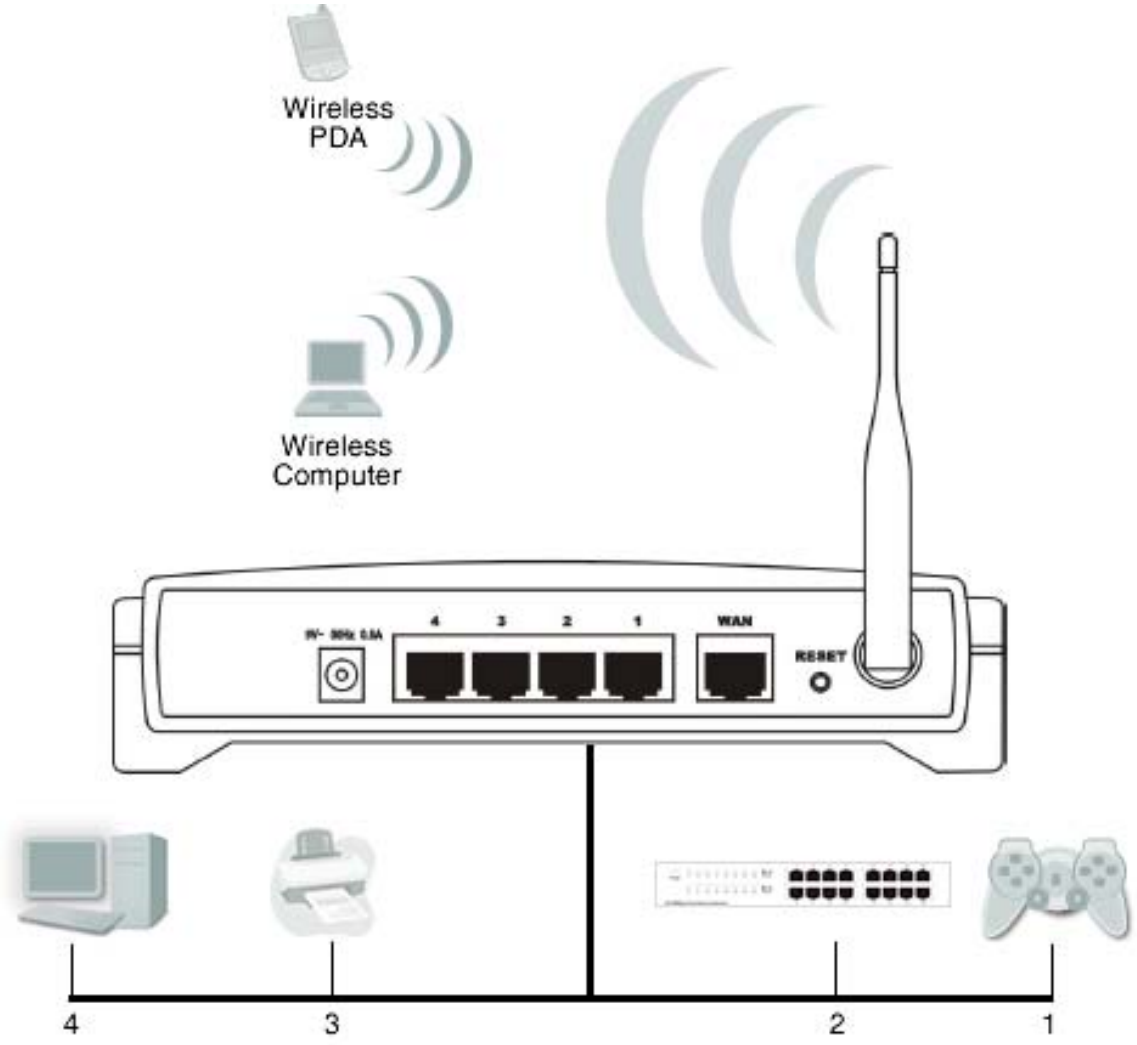
The product package includes the router, power adaptor, network cable, Resource CD, and a printed Easy Start Guide.

Use Ethernet cables to connect to the WAN and LAN links. Connect the Power Adapter and then plug to an electrical source. This switches on the Power LED light.

To establish an Internet connection, use Quick Setup from the Web Manager. The Web Manager is used to configure the connection settings and other advanced options.

# Planning Your Network

Decide what devices you want to include in your local network. Draw a simple diagram to visualize the network connections. For Ethernet devices like a computer, network printer, gaming console, or another router, use a network cable to connect them into the router. Identify the port number that you want to use for each device. In the diagram below, the Ethernet device is placed on the port it will use. The access point, on the other hand, will allow you to connect devices with wireless capability.




Sample network diagram

# Remove or Disable Conflicts

To make sure the router installation moves on smoothly, you need to remove or disable conflicts that may interfere the installation. Probable conflicts may include:

- Internet sharing applications
- Proxy software
- Security software
- TCP/IP settings
- Internet properties
- Temporary Internet files

## Internet Sharing, Proxy, and Security Applications

Internet sharing, proxy software, and firewall applications may interfere with the router installation. These should be removed or disabled before you install and configure the router.

If you have any of the following or similar applications installed on your computer, remove or disable them according to the manufacturer's instructions.

| Internet Sharing Applications | Proxy Software | Security Software |
|---|---|---|
| Microsoft Internet Sharing | WinGate | Symantec |
| | WinProxy | Zone Alarm |

# Configuring TCP/IP Settings

Use the default TCP/IP settings to allow the router to provide a network address to the computer,

**To set the TCP/IP properties:**

1. Select **Start** > **Run**. This opens the **Run** dialog box.
2. Enter **control ncpa.cpl** and then click **OK**. This opens the **Network Connections** in your computer.
3. Right-click **LAN** and then select **Properties**. This opens the **Local Area Connection Properties** dialog box.
4. Select **Internet Protocol (TCP/IP)** and then click **Properties**. This opens the **Internet Protocol (TCP/IP)** dialog box.
5. Select **Obtain an IP address automatically**.
6. Click **OK** to close the **Internet Protocol (TCP/IP)** dialog box.
7. Click **OK** to close the **Local Area Connection Properties** dialog box.

# Configuring Internet Properties

**To set the Internet Properties:**

1. Select **Start** > **Run**. This opens the **Run** dialog box.
2. Enter **control inetcpl.cpl** and then click **OK**. This opens the **Internet Properties** dialog box.
3. Click **Connections** tab.
4. In the **Dial-up and Virtual Private Network settings** pane, select **Never dial a connection**.
5. Click **OK** to close the **Internet Properties** dialog box.

## Removing Temporary Internet Files

Temporary Internet files are files from Web sites that are stored in your computer. Delete these filed to purge the Internet cache and remove footprints left by the Web pages you visited.

**To remove temporary Internet files:**

1. Select **Start** > **Run**. This opens the **Run** dialog box.
2. Enter **control** and then click **OK**. This opens the **Control Panel**.
3. Double-click **Internet Options**. This opens the Internet Options dialog box.
4. In the **Temporary Internet Files** pane, click **Delete Cookies**.
5. Click **Delete Files**.
6. Click **OK** to close the **Internet Properties** dialog box.

# Check Package Contents

The following items are included in the package:

- 1 Wireless Router
- 1 AC Power Adaptor
- 1 network cable
- 1 Easy Start Guide
- 1 Utility CD containing the User Manual

**Note:** If any of the contents are damaged or missing, please contact the retailer.

# Hardware Setup

Before you install the router, you should connect your PC to the Internet through your broadband service successfully. If there is any problem, please contact your ISP. After that, please install the router according to the following steps. Don't forget to pull out the power plug and keep your hands dry.

**To setup the hardware:**

1. Use Ethernet cables to connect the computers in your network into the **LAN** ports.
2. Use an Ethernet cable to connect the cable/DSL Modem into the **WAN** port.
3. Connect the AC power adaptor to the **AC power socket** on the router, and the other end into an electrical outlet. The router will start to work automatically.
4. Check the LED's. Power stays on. System, WAN, and LAN 1-4 should remain flashing. The LED for the LAN port with no connection remains off.

# Connecting to the Internet

To connect to the Internet, use Quick Setup from the Web Manager.

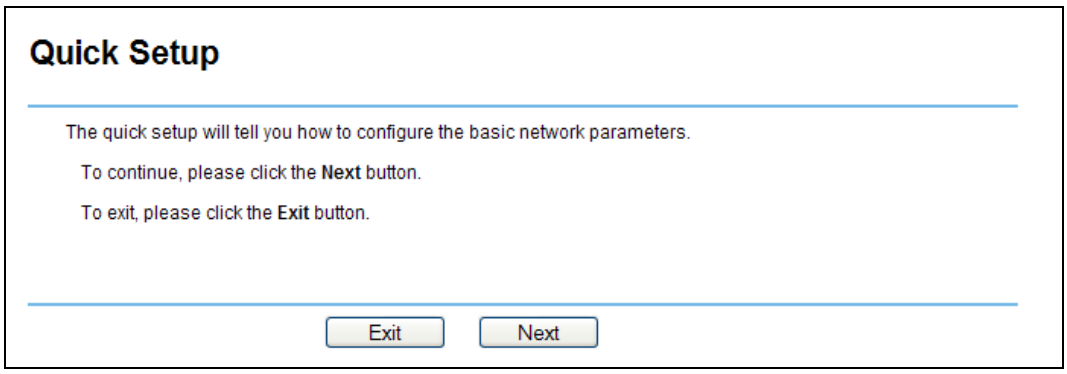
**To connect to the Internet using Quick Setup:**

1. Open a browser.
2. Enter 192.168.1.1 and then press Enter. This opens the login window.
3. Enter the User Name and Password and then press **Enter**. The default User Name and Password is **admin**. This opens the Web Manager.


**Note:** If the Login window does not open, it means that your browser has been set to a proxy. Go to **Tools** Menu and then select **Internet Options**. Click **Connections > LAN Settings**. This opens **Local Area Network (LAN) Settings** and then cancels **Proxy server** settings.

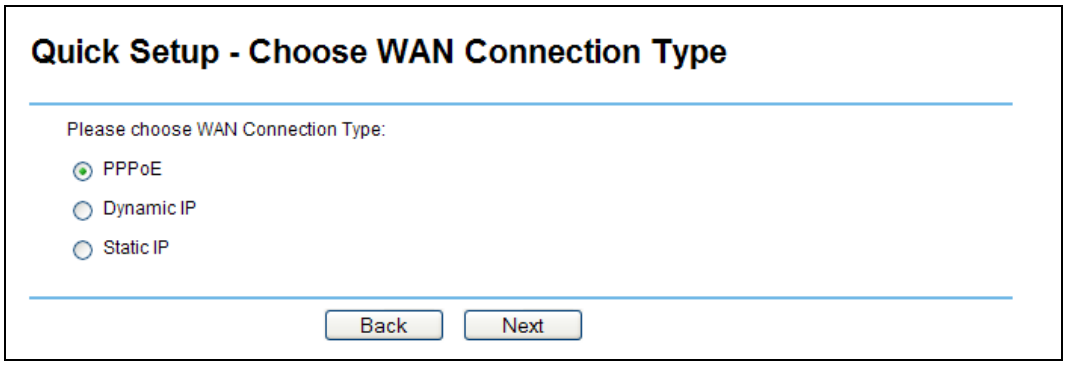
4. From the left pane, select **Quick Setup**.

5. Click **Next**.




**Quick Setup**

6. Select the WAN Connection Type used by your Internet service provider.




**Quick Setup – Choose WAN Connection Type**

a. **PPPoE** When you select PPPoE, you will be asked to enter the User Name and Password. These fields are case sensitive. Your ISP provides these parameters.

b. **Dynamic IP** When you select Dynamic IP, the router will automatically receive the IP parameters from your ISP without needing to enter any parameter.

c. **Static IP** When you select Static IP, you will need to manually enter connection parameters in the Static IP settings page. Your ISP provides these parameters.

7. After selecting a connection type, click **Next**. This opens Quick Setup –Wireless.

8. Edit the wireless settings:

    a. Edit the **SSID**. This field is case sensitive. It can accept up to 32 characters.

    b. Select **Region**.

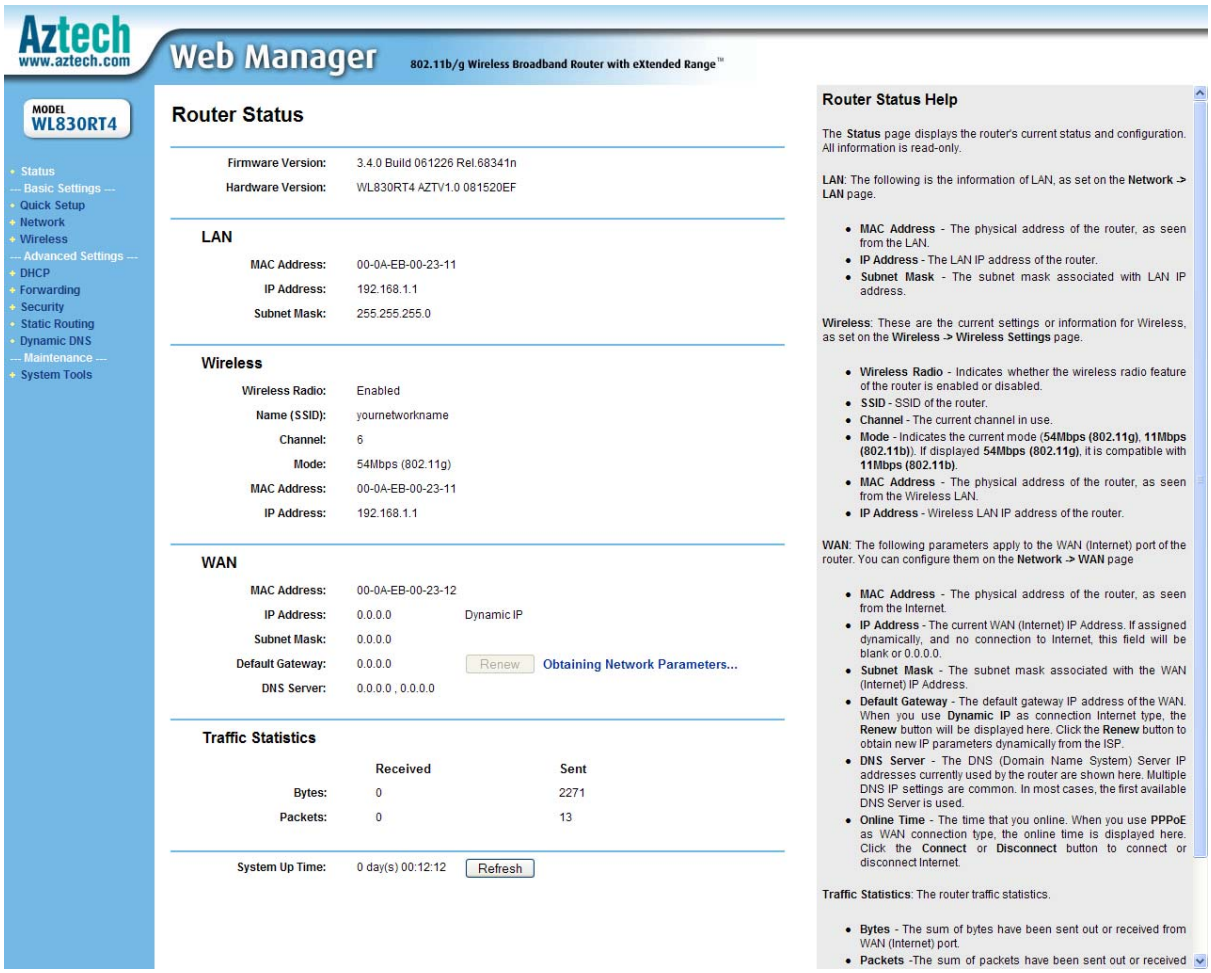
> **Note:** After you finish **Quick Setup**, you can enable the wireless security options by clicking **Wireless** under **Basic Settings**.

9. Click **Next**. This opens Quick Setup – Finish.

10. Click **Finish**.

# About the Web Manager

Web Manager is a browser-based utility that can be used on a computer using any operating system. It allows you to configure the basic and advanced router features.




Web Manager

# Accessing the Web Manager

**To connect to the Internet using Quick Setup:**

1. Open a browser.
2. Enter **192.168.1.1** and then press **Enter**. This opens the login window.
3. Enter the User Name and Password and then press **Enter**. The default User Name and Password is **admin**. This opens the Web Manager.


**Note:** If the Login window does not open, it means that your browser has been set to a proxy. Go to **Tools** Menu and then select **Internet Options**. Click **Connections > LAN Settings**. This opens **Local Area Network (LAN) Settings** and then cancels **Proxy server** settings.

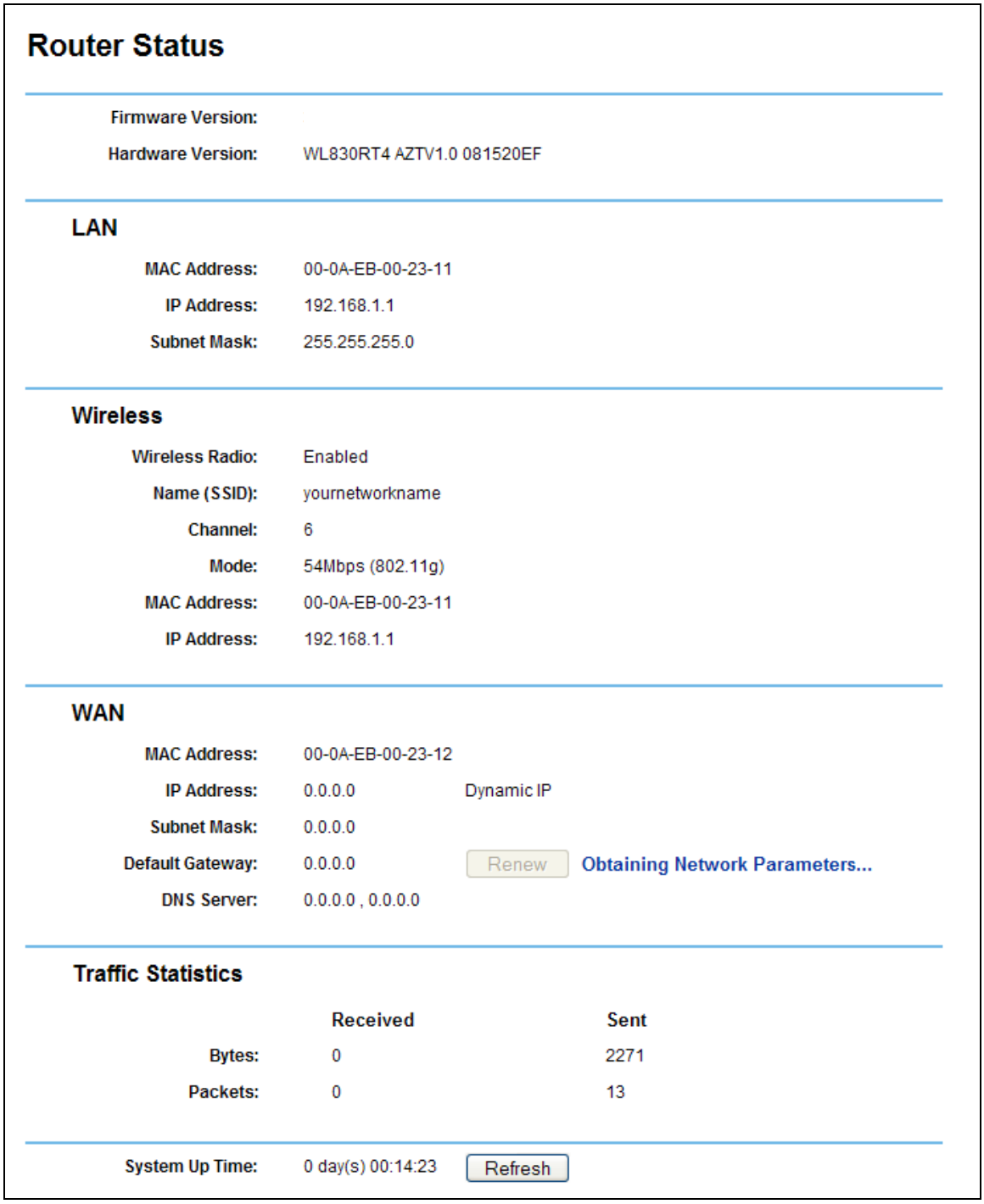
# Menu Structure

Web Manager includes several menus and submenus. The outline below displays the menu structure.

1. Status
2. Quick Setup
3. Network
    a. LAN
    b. WAN
    c. MAC Clone
4. Wireless
    a. Wireless Settings
    b. MAC Filtering
    c. Wireless Statistics
5. DHCP
    a. DHCP Settings
    b. DHCP Clients List
    c. Address Reservation
6. Forwarding
    a. Virtual Servers
    b. Port Triggering
    c. DMZ
    d. UPnP
7. Security
    a. Firewall
    b. IP Address Filtering
    c. Domain Filtering
    d. MAC Filtering
    e. Remote Management
    f. Advanced Security
8. Static Routing
9. Dynamic DNS
10. System Tools
    a. Time
    b. Firmware
    c. Factory Defaults
    d. Backup and Restore
    e. Reboot
    f. Password
    g. Log
    h. Statistics

# Status

The Status page displays the router's current status and configuration.




Router Status

**LAN** (Local Area Network) This field displays the current settings or information for the LAN, including the MAC address, IP address and Subnet Mask.

**Wireless** This field displays basic information or status for wireless function, including Wireless Radio, SSID, Channel, Mode, Wireless MAC address and IP address.

**WAN** (Wide Area Network) These parameters apply to the WAN port of the router, including MAC address, IP address, Subnet Mask, Default Gateway, DNS server and WAN connection type. If PPPoE is chosen as the WAN connection type, Disconnect will be shown here while you are accessing the Internet. Click Disconnect to cut the connection. If you have not connected to the Internet, just click Connect to establish the connection.

**Traffic Statistics** This field displays the router's traffic statistics.

**System Up Time** The amount of time from when the router was switched on or reset.

# Basic Settings

The Basic Settings Menu includes the links for Quick Setup, Network, and Wireless.

# Quick Setup

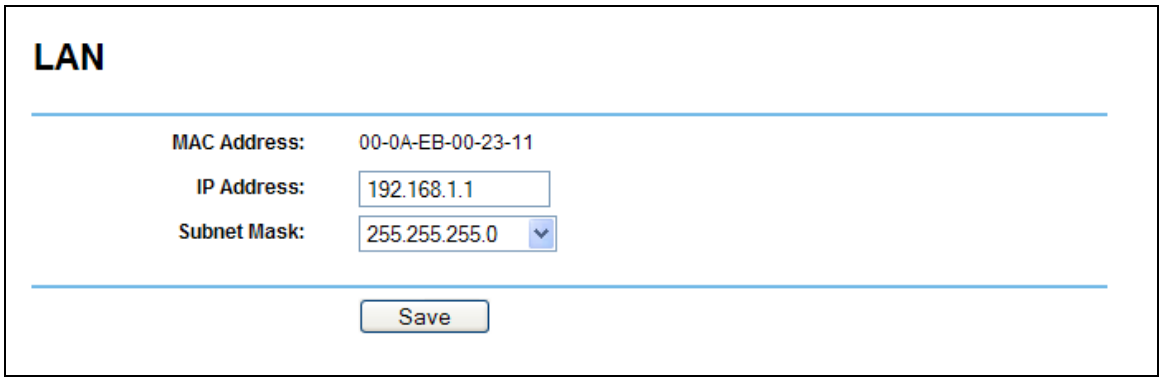
Please refer to Using Quick Setup.

# Network

There are three submenus under the Network menu: LAN, WAN and MAC Clone. Click any of them and you will be able to configure the corresponding function.

## LAN (Local Area Network)

You can configure the IP parameters of LAN on this page.




LAN (Local Area Network)

**MAC Address** The physical address of the router, as seen from the LAN. The value cannot be changed.

**IP Address** Enter the IP address of your router in dotted-decimal notation (factory default: 192.168.1.1).

**Subnet Mask** An address code that determines the size of the network. Normally use 255.255.255.0 as the subnet mask.

**Note:**

A. If the new LAN IP Address you set is not in the same subnet, the IP Address pool of the DHCP server will not take effect, until they are reconfigured.

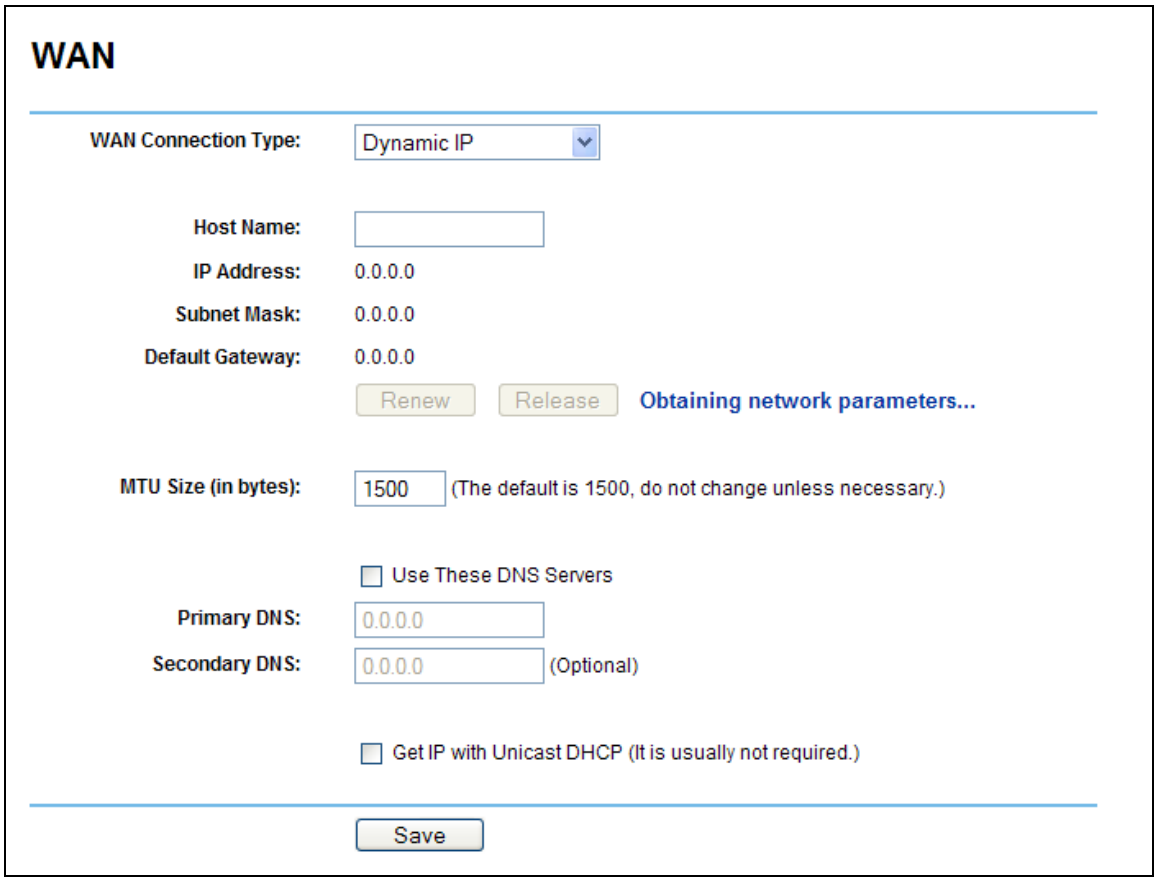
B. If the new LAN IP Address you set is not in the same subnet, the Virtual Server and DMZ Host will change accordingly at the same time.

# WAN (Wide Area Network)

You can configure the WAN connection parameters on this page. Ask your ISP for the correct connection type. There are several connection types:

- Dynamic IP (default)
- Static IP
- PPPoE
- 802.1X + Dynamic IP
- 802.1X + Static IP
- BigPond Cable
- L2TP
- PPTP

# Dynamic IP




Dynamic IP connection

In Dynamic IP, the router will automatically get IP parameters from your ISP, including IP address, Subnet Mask, and Default Gateway. Click **Renew** to renew the IP parameters from your ISP. Click **Release** to release the IP parameters.

**MTU Size** The normal MTU (Maximum Transmission Unit) value for most Ethernet networks is 1500 Bytes. In rare instances, some ISPs require to reduce the MTU. Otherwise, this is not changed.

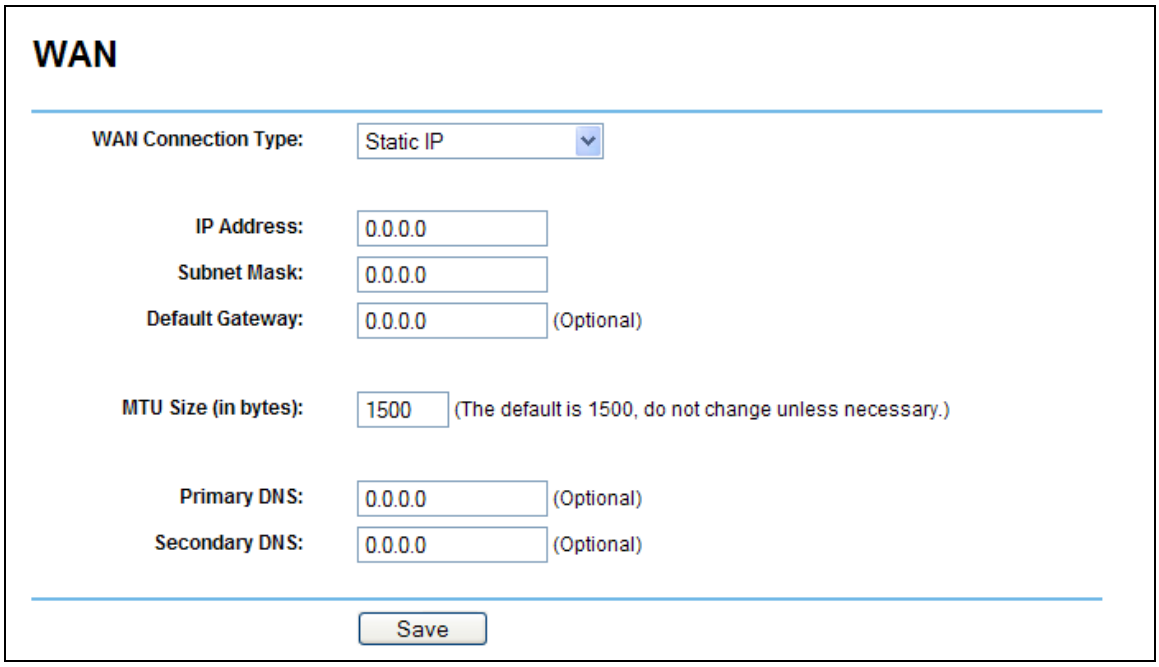
If your ISP gives you one or two DNS addresses, select **Use These DNS Servers** and enter the primary and secondary addresses. Otherwise, the DNS servers will be assigned dynamically from your ISP.

**Note:** If you find an error when you go to a Web site, it is likely that your DNS servers are set up improperly. Ask your ISP for the correct DNS server addresses.

**Get IP with Unicast DHCP** Some ISPs' do not support the broadcast applications. If you cannot get the IP Address normally, you can choose this option. (This is rarely required.)

## Static IP

If you choose Static IP, you should have fixed IP Parameters specified by your ISP.




**Static IP Connection**

You should type the following parameters into the spaces provided:

**IP Address** Enter the IP address in dotted-decimal notation provided by your ISP.

**Subnet Mask** Enter the subnet Mask in dotted-decimal notation provided by your ISP. For example, 255.255.255.0.

**Default Gateway** (Optional) Enter the gateway IP address in dotted-decimal notation provided by your ISP.

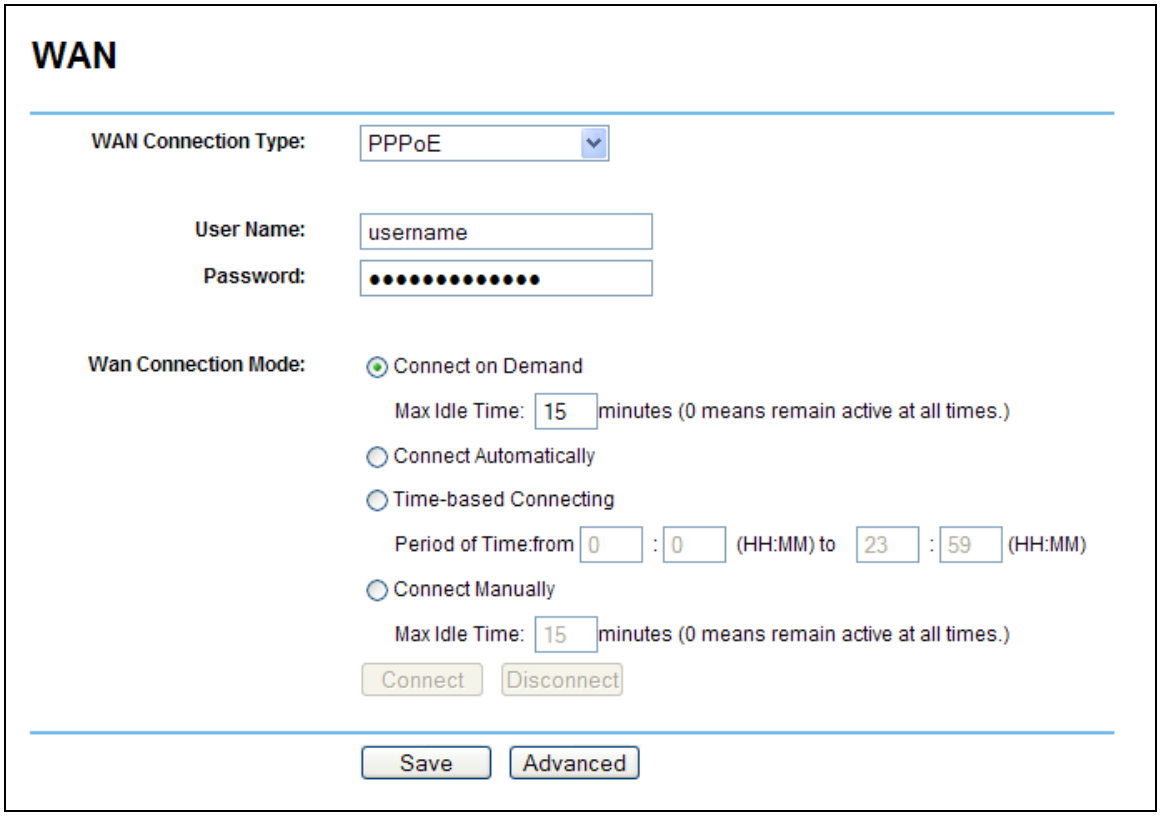
**MTU Size** The normal MTU (Maximum Transmission Unit) value for most Ethernet networks is 1500 Bytes. In rare instances, some ISPs require to reduce the MTU. Otherwise, this is not changed.

**Primary DNS** (Optional) Enter the DNS address in dotted-decimal notation provided by your ISP.

**Secondary DNS** (Optional) Type another DNS address in dotted-decimal notation provided by your ISP if provided.

# PPPoE

PPPoE means Point-to-Point Protocol over Ethernet.




**PPPoE Connection**

If you choose PPPoE, you should enter the following parameters:

**User Name/Password** Enter the User Name and Password provided by your ISP. These fields are case-sensitive.

**Connect on Demand** You can configure the router to disconnect your Internet connection after a specified period of inactivity (Max Idle Time). If your Internet connection has been terminated due to inactivity, Connect on Demand enables the router to automatically re-establish your connection as soon as you attempt to access the Internet again. Select **Connect on Demand** to activate it. If you want your Internet connection to remain active at all times, enter 0 in the Max Idle Time field. Otherwise, enter the number of minutes you want to have elapsed before your Internet connection terminates.

**Caution:** Sometimes the connection cannot be disconnected although you specify a time to Max Idle Time, since some applications is visiting the Internet continually in the background.

**Connect Automatically** Connect automatically after the router is disconnected. Select to use this option.

**Time-based Connecting** You can configure the router to connect or disconnect based on time. Enter the start time in HH:MM format for connecting and end time in HH:MM format for disconnecting in the Period of Time fields.

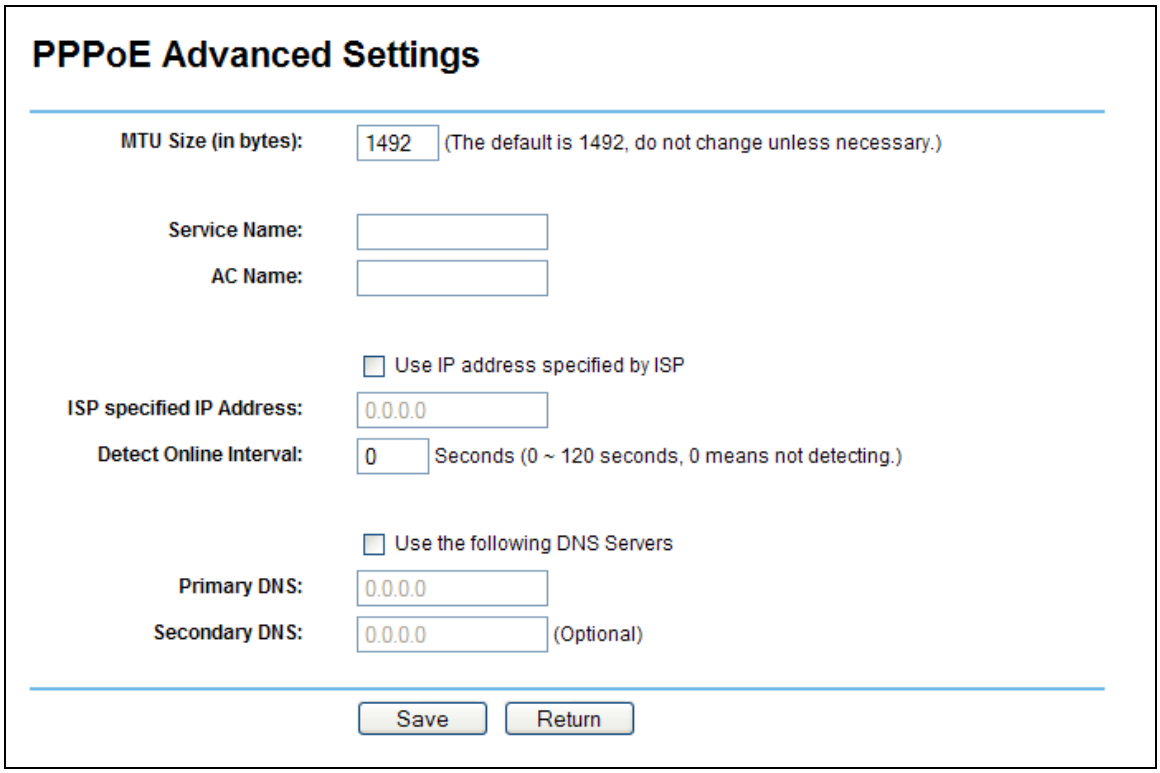
**Note:** Only when you have configured the system time on System Tools -> Time page, will the Time-based Connecting function can take effect.

**Connect Manually** You can configure the router to make it connect or disconnect manually. After a specified period of inactivity (Max Idle Time), the router will disconnect from the Internet connection, and you will not be able to re-establish your connection automatically as soon as you attempt to access the Internet again. Select to use this option. If you want your Internet connection to remain active at all times, enter **0** in the Max Idle Time field. Otherwise, enter the number time in minutes that you wish to have the Internet connecting last unless a new link is requested.

**Caution:** Sometimes the connection cannot be disconnected although you specify a time to Max Idle Time, since some applications are visiting the Internet continually in the background.

## *Advanced PPPoE Settings*

Click **Advanced Settings** to set up the advanced options.




PPPoE Advanced Settings

**Packet MTU** The default MTU size is 1492 bytes, which value is usually fine. For some ISPs, you need modify the MTU. This should not be done unless you are sure it is necessary for your ISP.

**Service Name/AC Name** The service name and AC (Access Concentrator) name, these should not be configured unless you are sure it is necessary for your ISP.

I

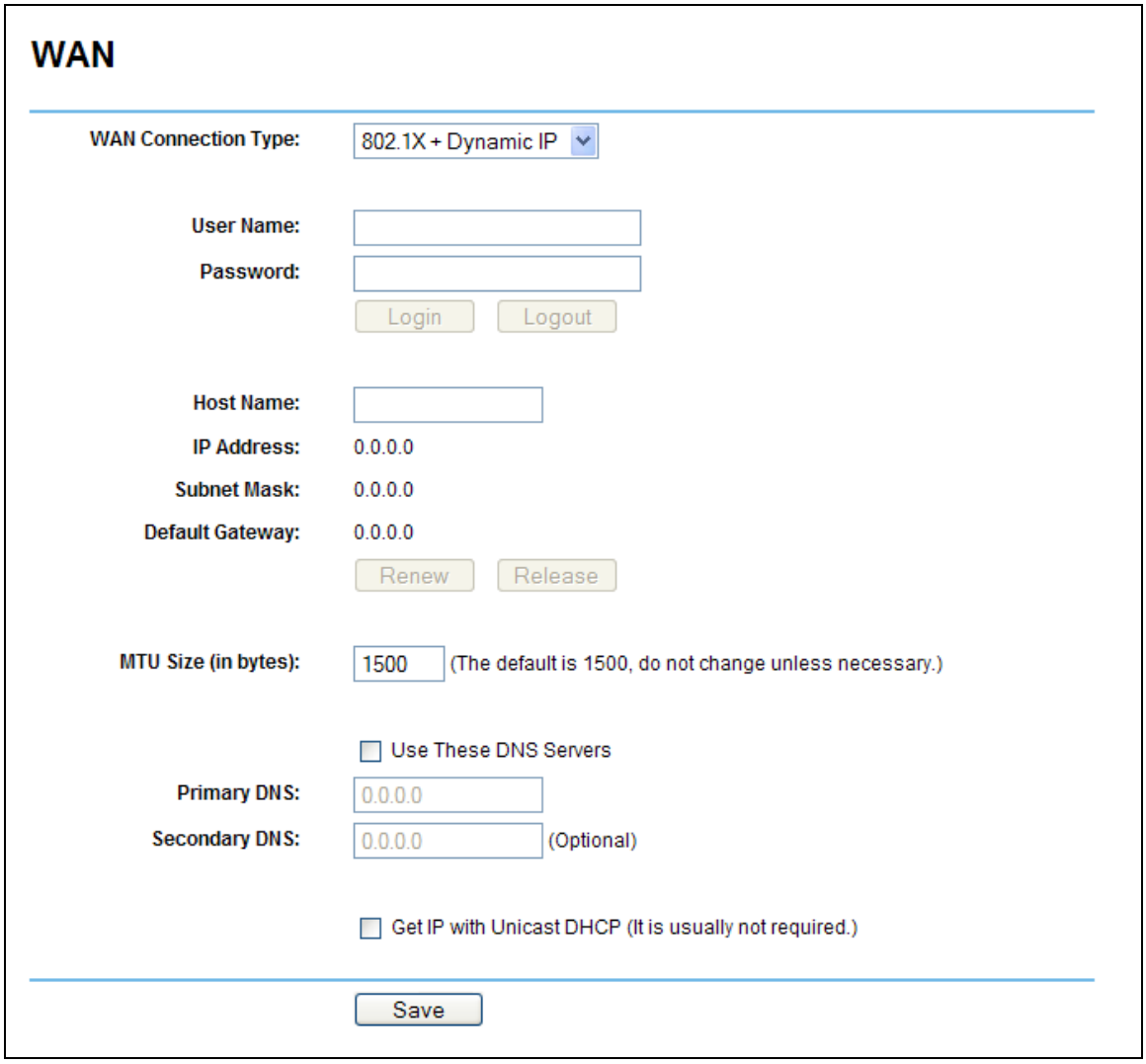
**SP Specified IP Address** If you know that your ISP does not automatically transmit your IP address to the router during login, click **Use the IP Address specified by ISP** check box and enter the IP Address in dotted-decimal notation, which your ISP provided.

**Detect Online Interval** The default value is 0, you can input the value between 0 and 120. The router will detect Access Concentrator online at every interval between seconds. If the value is 0, it means, do not detect.

**DNS IP address** If you know that your ISP does not automatically transmit DNS addresses to the router during login, click **Use the following DNS servers** checkbox and enter the IP address in dotted-decimal notation of your ISP's primary DNS server. If a secondary DNS server address is available, enter it as well. Click Save.

## 802.1X + Dynamic IP

If you choose 802.1X + Dynamic IP, you should enter the follow parameters:




802.1X + Dynamic IP Connection

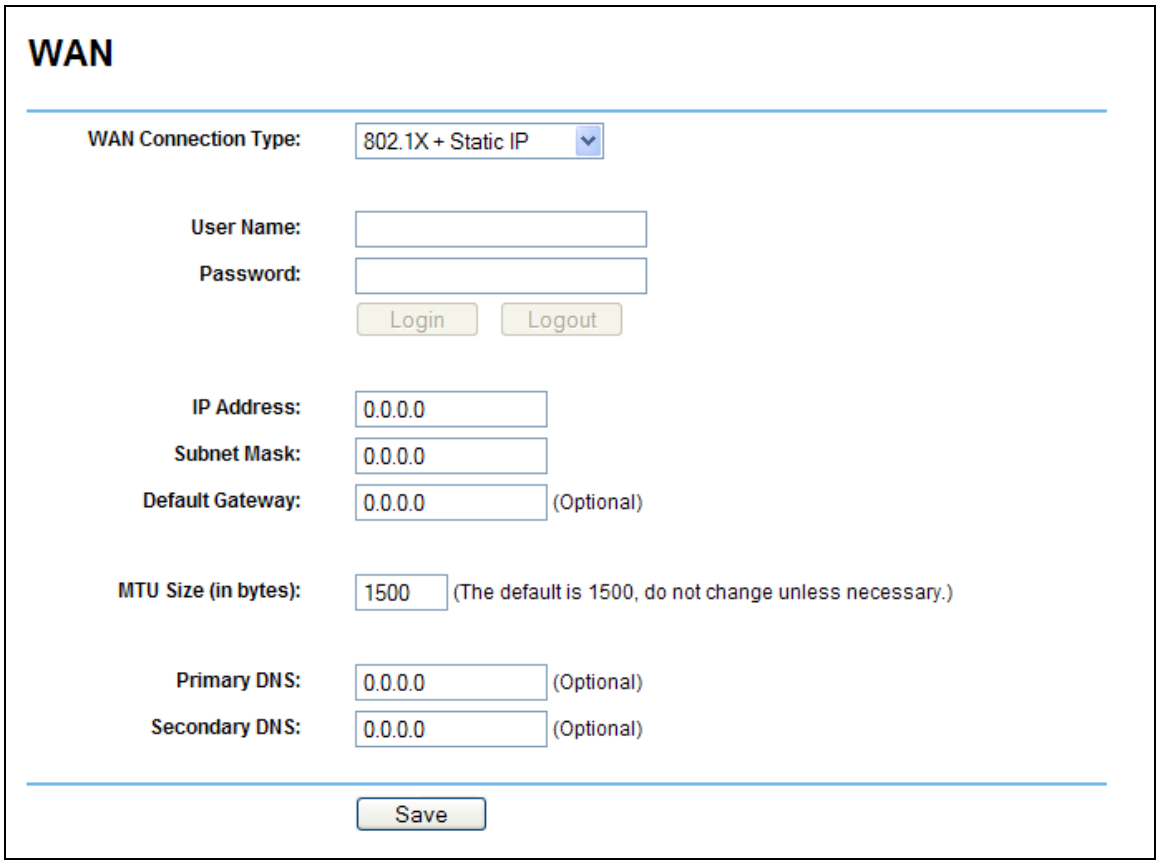
**User Name** Enter the user name for 802.1X authentication provided by your ISP

**Password** Enter the password for 802.1X authentication provided by your ISP. Click **Login** to start 802.1X authentication.

Click **Logout** to end 802.1X authentication.

**Host Name** This field is required to be filled by some service provider.

# 802.1X + Static IP




802.11X + Static IP

If you choose 802.1X + Static IP, you should enter the follow parameters:

**User Name** Enter the user name for 802.1X authentication provided by your ISP

**Password** Enter the password for 802.1X authentication provided by your ISP. Click Login to start 802.1X authentication.

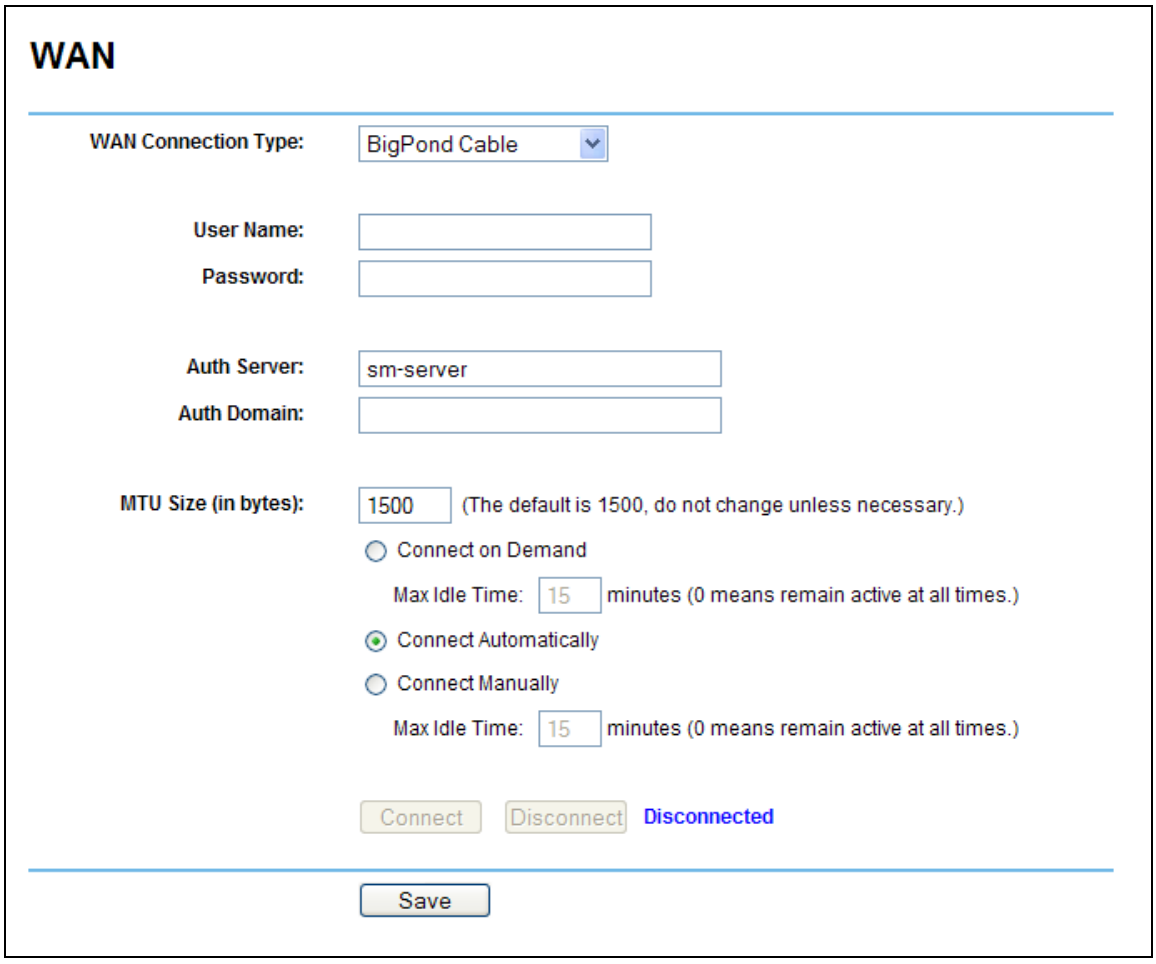
Click Logout to end 802.1X authentication.

**IP Address** Enter the IP address in dotted-decimal notation provided by your ISP.

**Subnet Mask** Enter the subnet Mask in dotted-decimal notation from your ISP.

**Default Gateway** (Optional) Enter the default gateway IP address in dotted-decimal notation provided by your ISP.

# BigPond Cable




**BigPond Cable**

If you choose BigPond Cable, you should enter the following parameters:

**User Name/Password** Enter the User Name and Password provided by your ISP. These fields are case-sensitive.

**Auth Server** Enter the authenticating server IP address or host name.

**Auth Domain** Type in the domain suffix server name based on your location. For example, NSW / ACT - nsw.bigpond.net.au VIC / TAS / WA / SA / NT - vic.bigpond.net.au QLD - qld.bigpond.net.au

**Connect on Demand** You can configure the router to disconnect from your Internet connection after a specified period of inactivity (Max Idle Time). If your Internet connection has been terminated due to inactivity, Connect on Demand enables

the router to automatically re-establish your connection as soon as you attempt to access the Internet again. Select Connect on Demand to activate it. If you want your Internet connection to remain active at all times, enter 0 in the Max Idle Time field. Otherwise, enter the number of minutes you want to have elapsed before your Internet connection terminates.

**Caution:** Sometimes the connection cannot be disconnected although you specify a time to Max Idle Time, since some applications are visiting the Internet continually in the background.

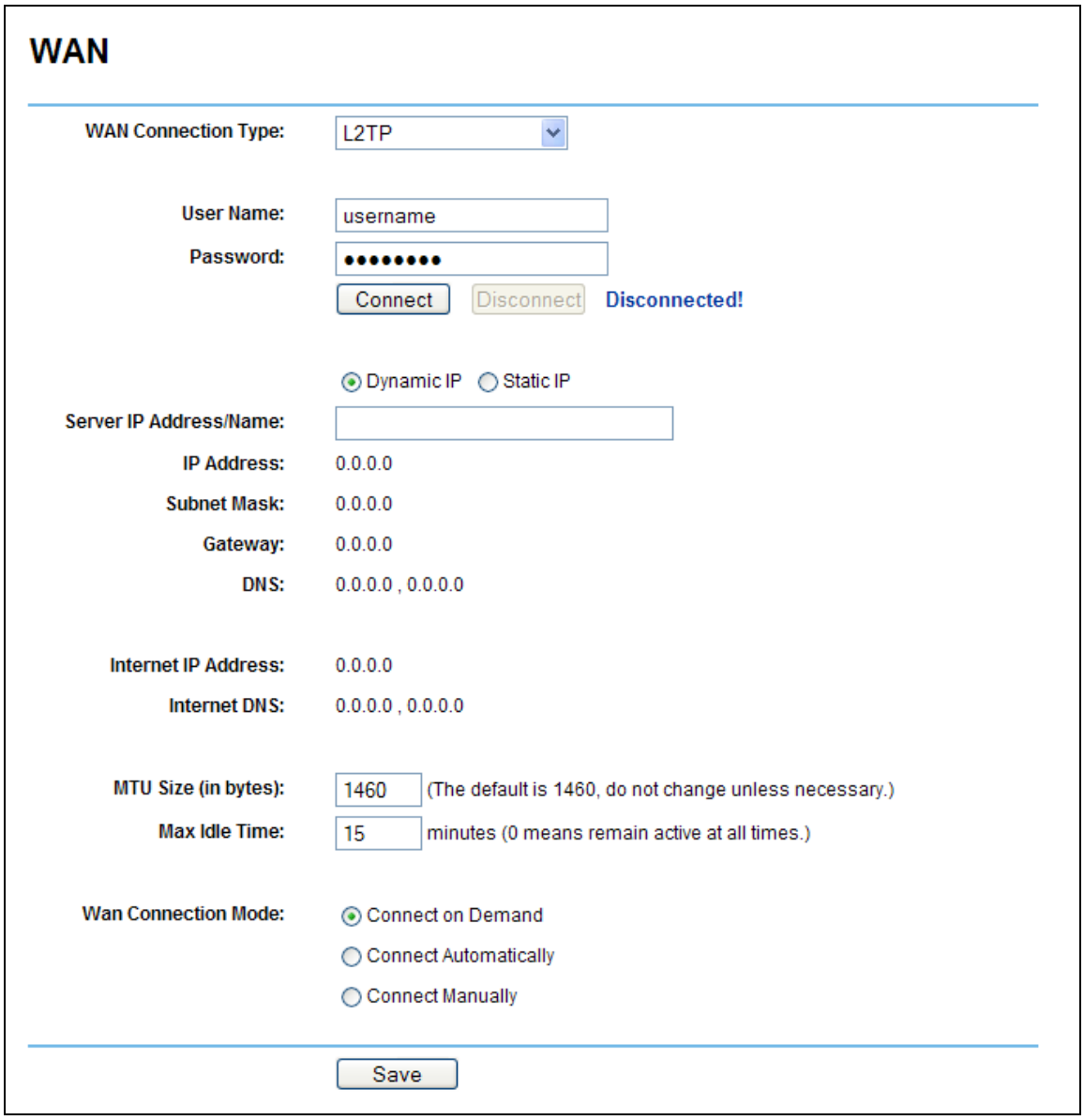
**Connect Automatically** Connect automatically after the router is disconnected. Select to use this option.

**Connect Manually** You can configure the router to make it connect or disconnect manually. After a specified period of inactivity (Max Idle Time), the router will disconnect from your Internet connection, and you will not be able to re-establish your connection automatically as soon as you attempt to access the Internet again. Select to use this option. If you want your Internet connection to remain active at all times, enter **0** in the Max Idle Time field. Otherwise, enter the number in minutes that you wish to have the Internet connecting last unless a new link is requested.

**Caution:** Sometimes the connection cannot be disconnected although you specify a time to Max Idle Time, since some applications are visiting the Internet continually in the background.

Click **Connect** to connect immediately. Click **Disconnect** to disconnect immediately.

# L2TP




L2TP Connection

If you choose L2TP, you should enter the following parameters:

**User Name/Password** Enter the User Name and Password provided by your ISP. These fields are case-sensitive.

**Dynamic IP/ Static IP** Contact your ISP for the correct WAN IP address. Click **Connect** to connect immediately or click **Disconnect** to disconnect immediately.

**Connect on Demand** You can configure the router to disconnect from your Internet connection after a specified period of inactivity (Max Idle Time). If your Internet connection has been terminated due to inactivity, Connect on Demand enables the router to automatically re-establish your connection as soon as you attempt to access the Internet again. Select to activate Connect on Demand. If you want your Internet connection to remain active at all times, enter 0 in the Max Idle Time field. Otherwise, enter the number of minutes you want to have elapsed before your Internet connection terminates.

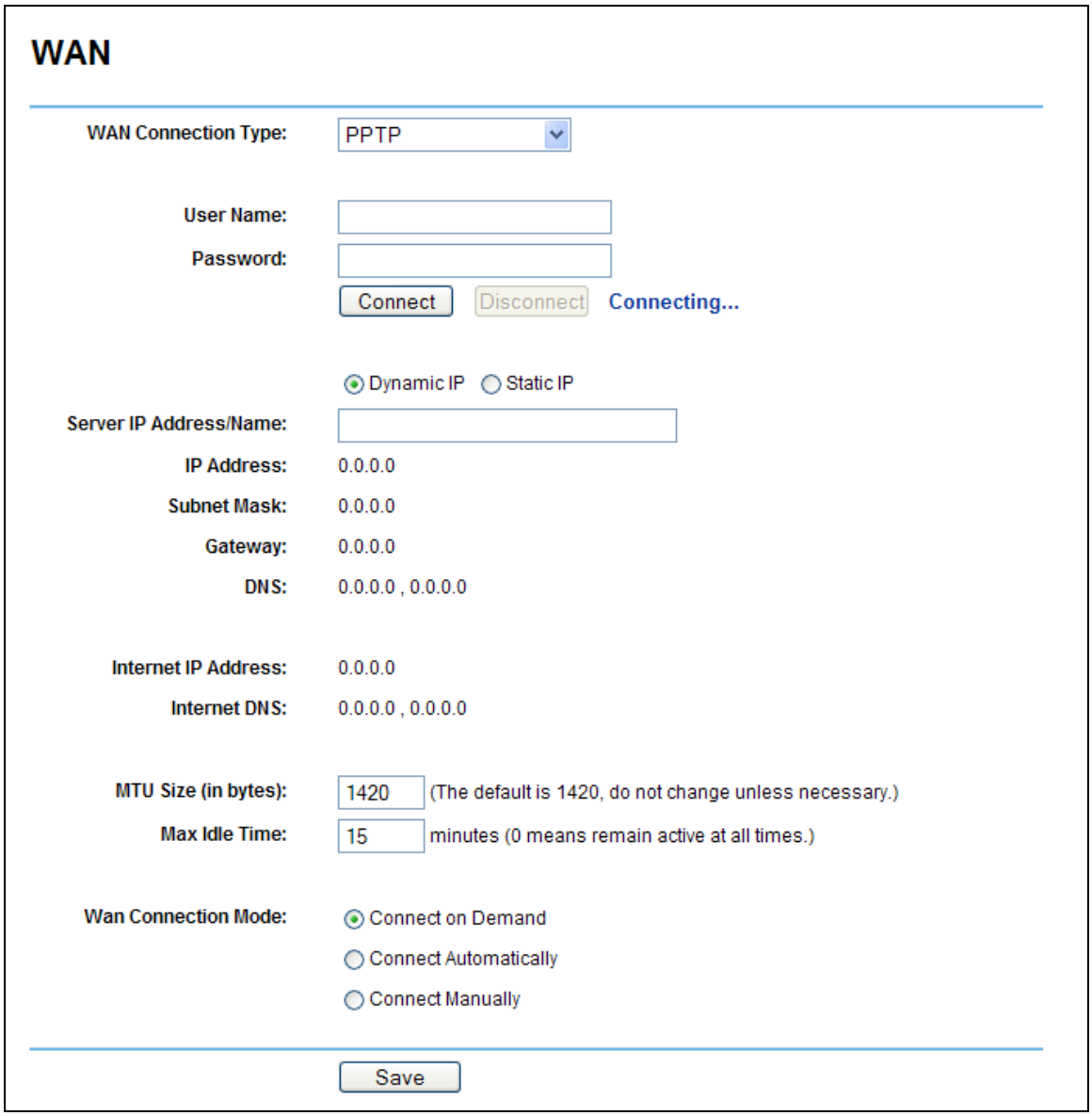
**Caution:** Sometimes the connection cannot be disconnected although you specify a time to Max Idle Time, since some applications is visiting the Internet continually in the background.

**Connect Automatically** Connect automatically after the router is disconnected. Select to use this option.

**Connect Manually** You can configure the router to make it connect or disconnect manually. After a specified period of inactivity (Max Idle Time), the router will disconnect from your Internet connection, and you will not be able to re-establish your connection automatically as soon as you attempt to access the Internet again. Select to use this option. If you want your Internet connection to remain active at all times, enter **0** in the Max Idle Time field. Otherwise, enter the number in minutes that you wish to have the Internet connecting last unless a new link is requested.

**Caution:** Sometimes the connection cannot be disconnected although you specify a time to Max Idle Time, since some applications is visiting the Internet continually in the background.

# PPTP




PPTP Connection

If you choose PPTP, you should enter the following parameters:

**User Name/Password** Enter the User Name and Password provided by your ISP. These fields are case-sensitive.

**Dynamic IP/ Static IP** Contact your ISP for the correct WAN IP address.

If you choose static IP and enter the domain name, you should also enter the DNS assigned by your ISP. Click **Save**.

Click Connect to connect immediately. Click Disconnect to disconnect immediately.

**Connect on Demand** You can configure the router to disconnect from your Internet connection after a specified period of inactivity (Max Idle Time). If your Internet connection has been terminated due to inactivity, Connect on Demand enables the router to automatically re-establish your connection as soon as you attempt to access the Internet again. Select to activate Connect on Demand. If you want your Internet connection to remain active at all times, enter 0 in the Max Idle Time field. Otherwise, enter the number of minutes you want to have elapsed before your Internet connection terminates.

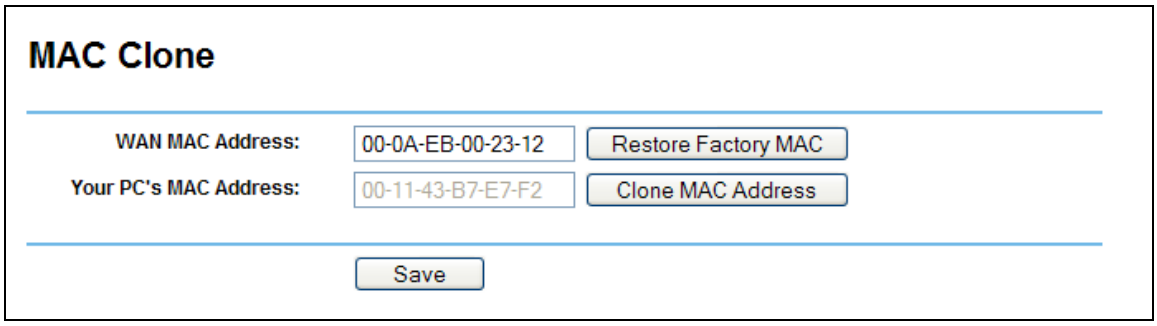
**Caution:** Sometimes the connection cannot be disconnected although you specify a time to Max Idle Time, since some applications are visiting the Internet continually in the background.

**Connect Automatically** Connect automatically after the router is disconnected. Select to use this option.

**Connect Manually** You can configure the router to make it connect or disconnect manually. After a specified period of inactivity (Max Idle Time), the router will disconnect from your Internet connection, and you will not be able to re-establish your connection automatically as soon as you attempt to access the Internet again. Select to use this option. If you want your Internet connection to remain active at all times, enter **0** in the Max Idle Time field. Otherwise, enter the number in minutes that you wish to have the Internet connecting last unless a new link is requested.

**Caution:** Sometimes the connection cannot be disconnected although you specify a time to Max Idle Time, since some applications are visiting the Internet continually in the background.

# MAC Clone




**MAC Clone**

You can configure the MAC address of the WAN port on this page:

Some ISPs require that you register the MAC Address of your adapter, which is connected to your cable, DSL modem or Ethernet during installation. Changes are rarely needed here.

**WAN MAC Address** This field displays the current MAC address of the WAN port, which is used for the WAN port. If your ISP requires that you register the MAC address, please enter the correct MAC address into this field. The format for the MAC Address is XX-XX-XX-XX-XX-XX (X is any hexadecimal digit).

**Your PC's MAC Address** This field displays the MAC address of the PC that is managing the router. If the MAC address is required, click **Clone MAC Address**.

Click **Restore Factory MAC** to restore the MAC address of WAN port to the factory default value.

Click **Save** to save your settings.

**Note:**

1. Only the PC on your LAN can use the MAC Address Clone feature.

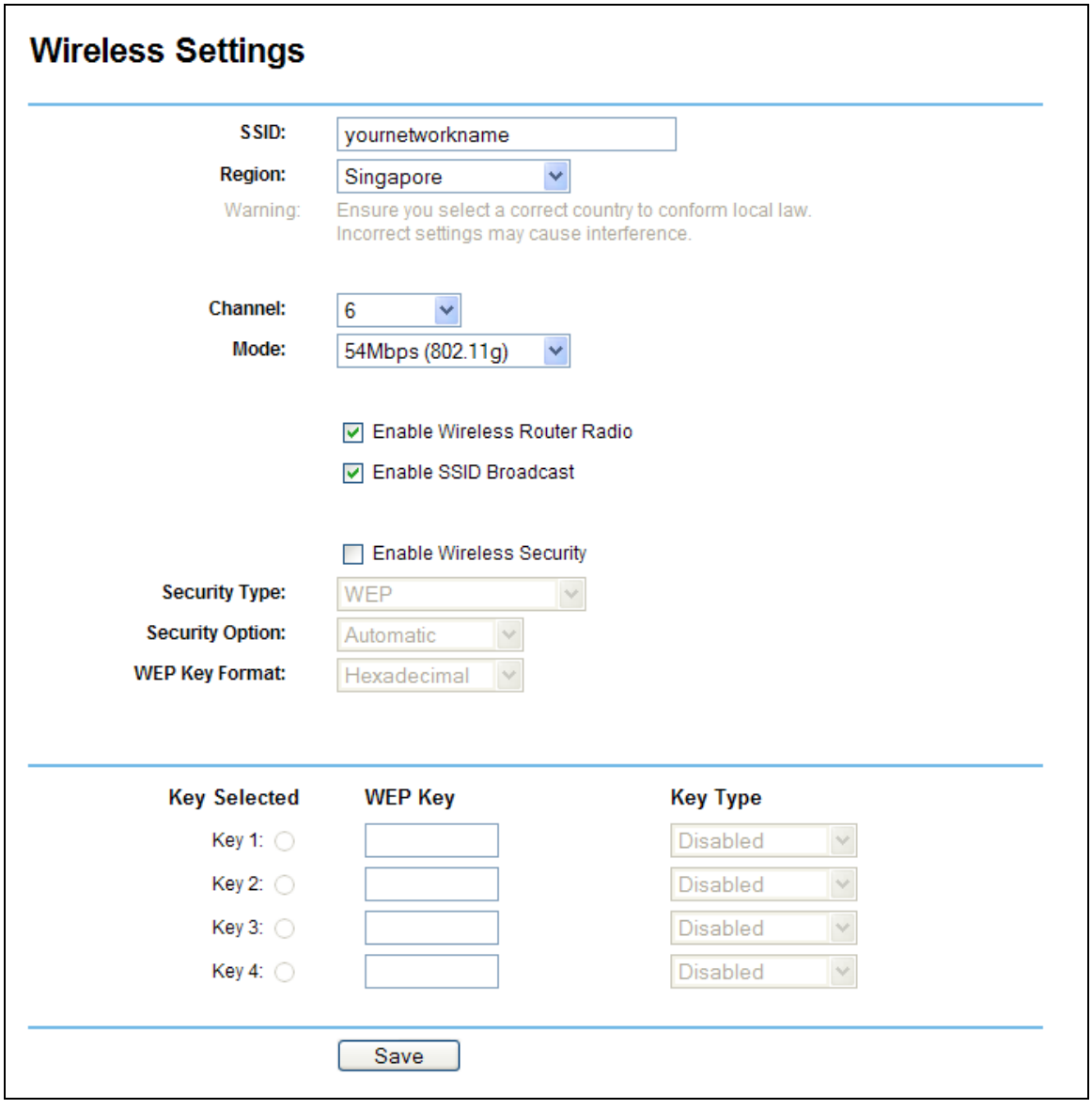
2. If you click Save, the router will prompt you to reboot.

# Wireless

There are three submenus under the Wireless menu: Wireless Settings, MAC Filtering and Wireless Statistics. Click any of them, and you will be able to configure the corresponding function. The detailed explanations for each submenu are provided below.

## Wireless Settings

**Note:** The router will restart after you change the Wireless Settings. This will disconnect the Internet connection of wireless devices connected into the router. The wireless devices, however, will still be connected to the local network.




Wireless Settings

The basic settings for the wireless network are set on this page:

**SSID** (Service Set Identifier) Enter a value of up to 32 characters. The same SSID must be assigned to all wireless devices in your network. The default SSID is yournetworkname, but it is recommended strongly that you change your networks name (SSID) to a different value. This value is case-sensitive.

**Region** Select your region from the pull-down list. This field specifies the region where the wireless function of the router can be used. It may be illegal to use the wireless function of the router in a region other than one of those specified in this field. If your country or region is not listed, please contact your local government agency for assistance. The default region is United States. When you select your local region from the pull-down list, Click Save, then the Note Dialog appears. Click OK.

**Note:** Limited by local law regulations, version for North America does not have region selection option.

**Channel** This field determines which operating frequency will be used. It is not necessary to change the wireless channel unless you notice interference problems with another nearby access point.

**Mode** Select the desired wireless mode. The options are:

- 54Mbps (802.11g) Both 802.11g and 802.11b wireless stations can connect to the router.
- 11Mbps (802.11b) Only 802.11b wireless stations can connect to the router.

**Note:** The default is 54Mbps (802.11g), which allows both 802.11g and 802.11b wireless stations to connect to the router.

**Enable Wireless Router Radio** The wireless radio of this Router can be enabled or disabled to allow wireless stations access. If enabled, wireless stations will be able to access the router, otherwise, wireless stations will not be able to access.

**Enable SSID Broadcast** If you select the Enable SSID Broadcast checkbox, the Wireless Router SSID will broadcast its name (SSID) on the air.

**Enable Wireless Security** The wireless security function can be enabled or disabled. If disabled, the wireless stations will be able to connect the router without encryption. It is strongly recommended that you choose this option to encrypt your wireless network. The encryption settings are described below.

**Authentication Type** You can select one of the following authentication types:

- WEP - Select WEP authentication type based on 802.11 authentications.
- WPA-PSK/WPA2-PSK - Select WPA/WPA2 authentication type based on pre-shared passphrase.
- WPA/WPA2 - Select WPA/WPA2 authentication type based on Radius Server.

**Authentication Options** You can select one of the following authentication options:

When you select WEP for authentication type you can select the following authentication options:

**Automatic** Select Shared Key or Open System authentication type automatically based on the wireless station request.

**Shared Key** Select 802.11 Shared Key authentication.

**Open System** Select 802.11 Open System authentication.

When you select WPA-PSK/WPA2-PSK for authentication type you can select Automatic, WPA –PSK or WPA2-PSK as authentication options.

When you select WPA/WPA2 as an authentication type you can select Automatic WPA or WPA2 as authentication option.

**WEP Key Format** You can select ASCII or Hexadecimal format. ASCII Code Format stands for any combination of keyboard characters in the specified length. Hexadecimal format stands for any combination of hexadecimal digits (0-9, a-f, A-F) in the specified length.

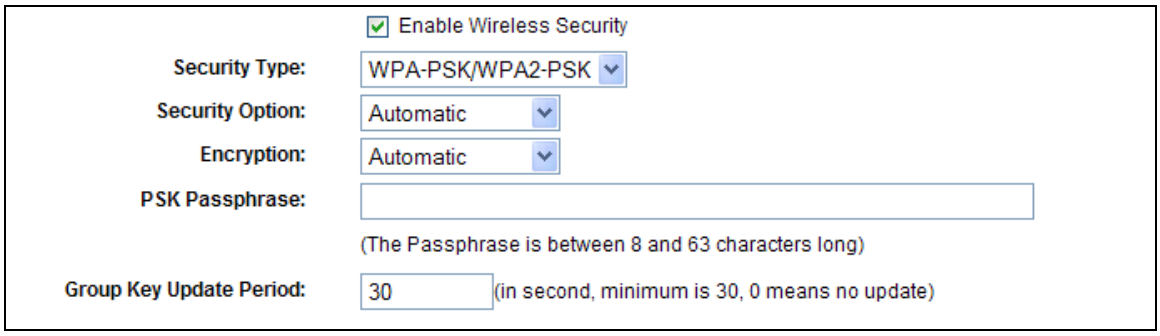
**WEP Key settings** Select which of the four keys will be used and enter the matching WEP key information for your network. These values must be identical on all wireless stations in your network.

**Key Type** You can select the WEP key length (64-bit, or 128-bit, or 152-bit) for encryption. **Disabled** means the WEP key entry is invalid.

- For 64-bit encryption - You can enter 10 hexadecimal digits (any combination of 0-9, a-f, A-F, zero key is not permitted) or 5 ASCII characters.
- For 128-bit encryption - You can enter 26 hexadecimal digits (any combination of 0-9, a-f, A-F, zero key is not permitted) or 13 ASCII characters.
- For 152-bit encryption - You can enter 32 hexadecimal digits (any combination of 0-9, a-f, A-F, zero key is not permitted) or 16 ASCII characters.

**Encryption** When you select WPA-PSK/WPA2-PSK or WPA/WPA2 for Authentication Type you can select Automatic, TKIP or AES as Encryptions.

## WPA-PSK/WPA2-PSK

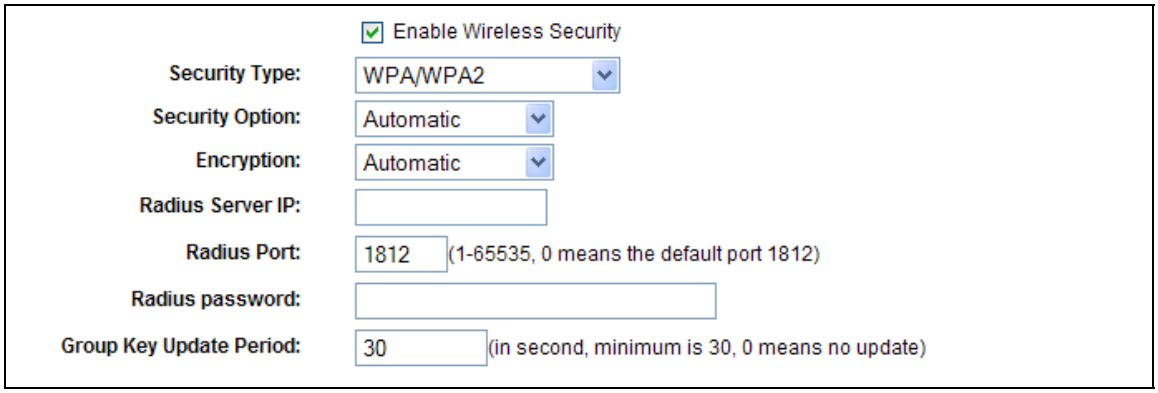



**WPA-PSK/WPA2-PSK**

**WPA-PSK/WPA2-PSK Passphrase** You can enter a WPA or WPA2 Passphrase between 8 and 63 characters long composed of letter, numbers or a combination of both.

**Group Key Update Period** Specify the group key update interval in seconds. The value can be either 0 seconds or from 30 seconds and up, 1-29 seconds are not usable figures. Enter 0 to disable the update.

## WPA/WPA2




**WPA/WPA2**

**Radius Server IP** Enter the IP address of the Radius Server

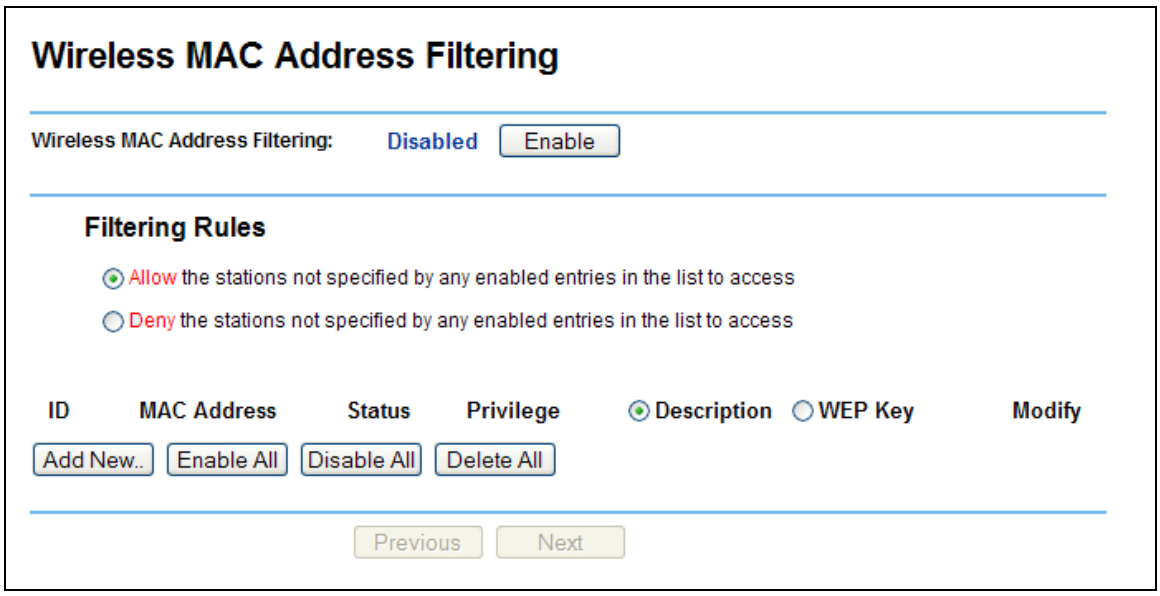
**Radius Port** Enter the port number that the radius service used.

**Radius Password** Enter the password for the Radius Server.

Be sure to click **Save** to save your settings. The router will reboot automatically after you click save.

# MAC Filtering

The Wireless MAC Filtering for wireless networks are set on this page:




**Wireless MAC Address Filtering**

The Wireless MAC Address Filtering feature allows you to control wireless stations accessing the router, which depend on the station's MAC addresses.

**MAC Address** The wireless station's MAC address that you want to access.

**Status** The status of this entry either Enabled or Disabled.

**Privilege** Select the privileges for this entry. You may select one of the following Allow / Deny / 64-bit / 128-bit / 152-bit.

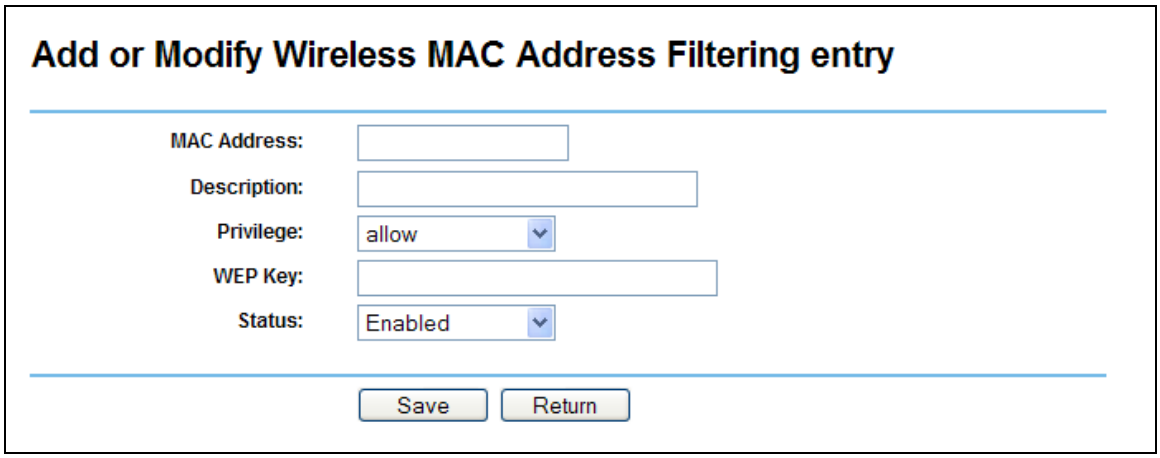
**Description** A simple description of the wireless station.

**WEP Key** Specify a unique WEP key (in Hexadecimal format) to access the router.

**To set up an entry, follow these instructions:**

First, you must decide whether the unspecified wireless stations can access the router or not. If you desire that the unspecified wireless stations can access the router, please select Allow the stations not specified by any enabled entries in the list to access, otherwise, select to Deny the stations not specified by any enabled entries in the list to access.

# Wireless MAC Address Filter List

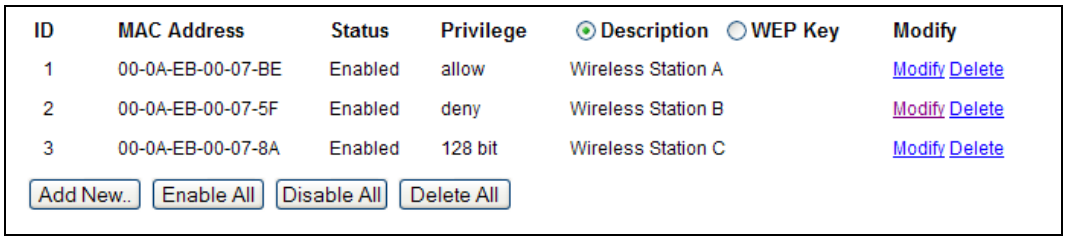



Add or Modify Wireless MAC Address Filtering Entry

### To add a Wireless MAC Address filtering entry

1. Click **Add New**. This opens Add or Modify Wireless MAC Address Filtering entry
2. Enter the MAC Address of the wireless device. The MAC Address format is XX-XX-XX-XX-XX-XX where X is any hexadecimal character. For example, 00-0A-EB-B0-00-0B.
3. Enter a simple description of the wireless station in the Description field. For example, Wireless station A.
4. Select the type of Privilege
   - Allow
   - Deny
   - 64-bit
   - 128-bit
   - 152-bit
5. If you selected 64-bit, 128-bit, or 152-bit in the Privilege field, enter any combination of hexadecimal digits (0-9, a-f, A-F) in the specified length. For example: 2F34D20BE2.

6. Select a status
   - Enabled
   - Disabled
7. Click **Save**.




**To modify or delete an existing entry:**

1. Click **Modify** to modify the entry or click **Delete** to delete the entry.
2. Modify the information.
3. Click **Save**.

Click **Enable All** to enable all entries.

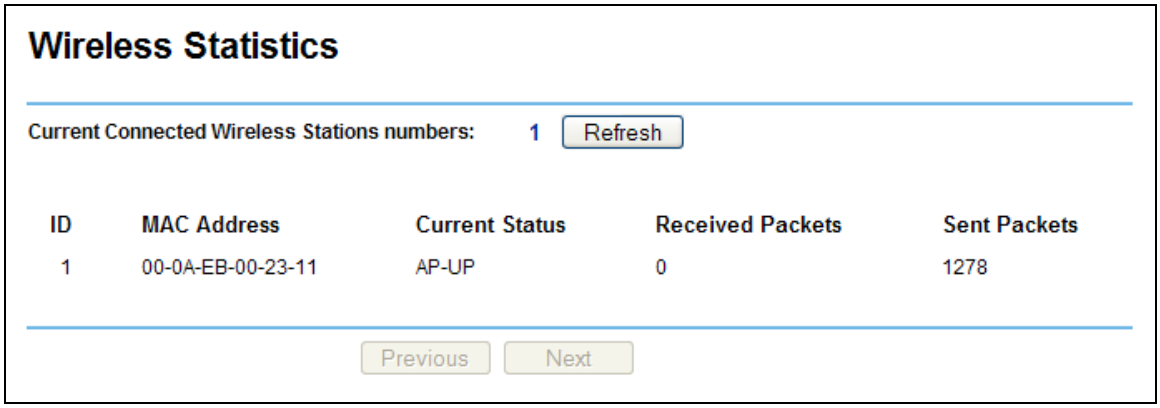
Click **Disabled All** to disable all entries.

Click **Delete All** to delete all entries.

Click **Next** to go to the next page and click **Previous** to return to the previous page.

# Wireless Statistics

This page shows MAC Address, Current Status, Received Packets and Sent Packets for each connected wireless station.




Wireless Statistics

**MAC Address** The connected wireless station's MAC address

**Current Status** The connected wireless station's running status, one of STA-AUTH / STA-ASSOC / AP-UP / WPA / WPA-PSK /WPA2/WPA2-PSK/None

**Received Packets** Packets received by the station

**Sent Packets** Packets sent by the station

You cannot change any of the values on this page. To update this page and to show the current connected wireless stations, click **Refresh**.

If the numbers of connected wireless stations go beyond one page, click **Next** to go to the next page or click **Previous** to return the previous page.

**Note:** This page will be refreshed automatically every 5 seconds.

# Advanced Settings

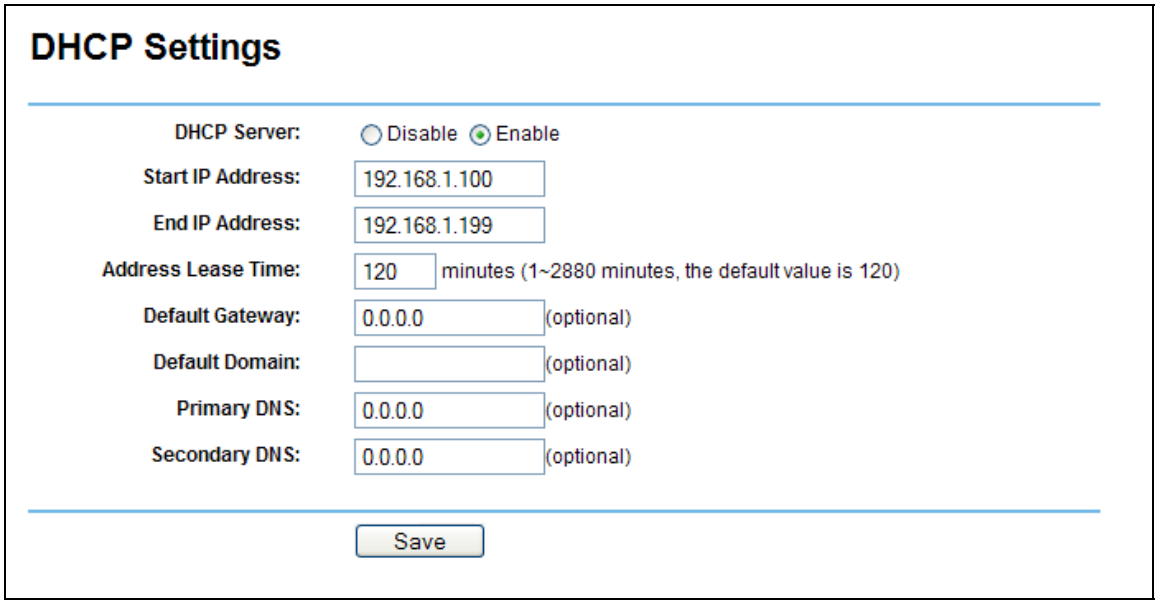
Advanced settings include DHCP, Forwarding, Security, Static Routing, and Dynamic DNS.

# DHCP (Dynamic Host Configuration Protocol)

There are three submenus under the DHCP menu: DHCP Settings, DHCP Clients List and Address Reservation. Click any of them, and you will be able to configure the corresponding function.

## DHCP Settings

The router is set up by default as a DHCP (Dynamic Host Configuration Protocol) server, which provides the TCP/IP configuration for all the PCs that are connected to the router on the LAN.




DHCP Settings

**DHCP Server** Enable or Disable the DHCP server. If you disable the Server, you must have another DHCP server within your network or else you must manually configure the computer.

**Start IP Address** This field specifies the first of the addresses in the IP address pool. 192.168.1.100 is the default start address.

**End IP Address** This field specifies the last of the addresses in the IP address pool. 192.168.1.199 is the default end address.

**Address Lease Time** The Address Lease Time is the amount of time in which a network user will be allowed connection to the router with their current dynamic IP Address. Enter the amount of time, in minutes. The user will be leased this dynamic IP Address. The range of the time is 1 ~ 2880 minutes. The default value is 120 minutes.

**Default Gateway** (Optional) Suggest to input the IP address of the LAN port of the router, default value is 192.168.1.1

**Default Domain** (Optional.) Input the domain name of your network.

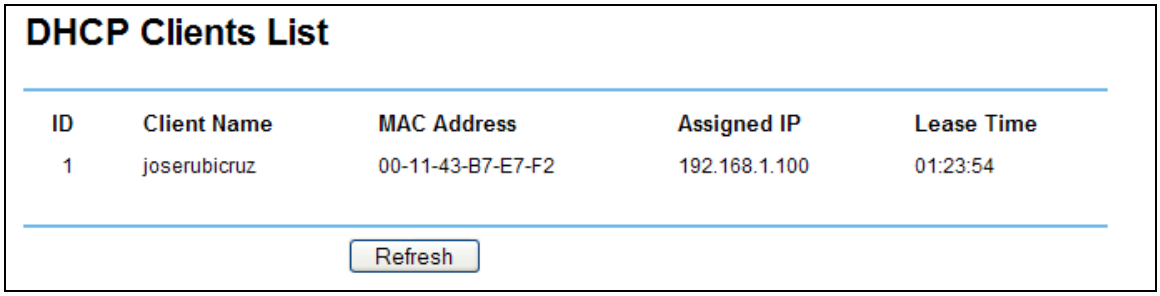
**Primary DNS** (Optional.) Input the DNS IP address provided by your ISP. Or consult your ISP.

**Secondary DNS** (Optional.) Input the IP address of another DNS server if your ISP provides two DNS servers.

**Note:** To use the DHCP server function of the router, you must configure all computers on the LAN as **Obtain an IP Address automatically** mode. This function will take effect until the router reboots.

# DHCP Clients List

This page shows Client Name, MAC Address, Assigned IP and Lease Time for each DHCP Client attached to the router:




**DHCP Clients List**

**Index** The index of the DHCP Client

**Client Name** The name of the DHCP client

**MAC Address** The MAC address of the DHCP client

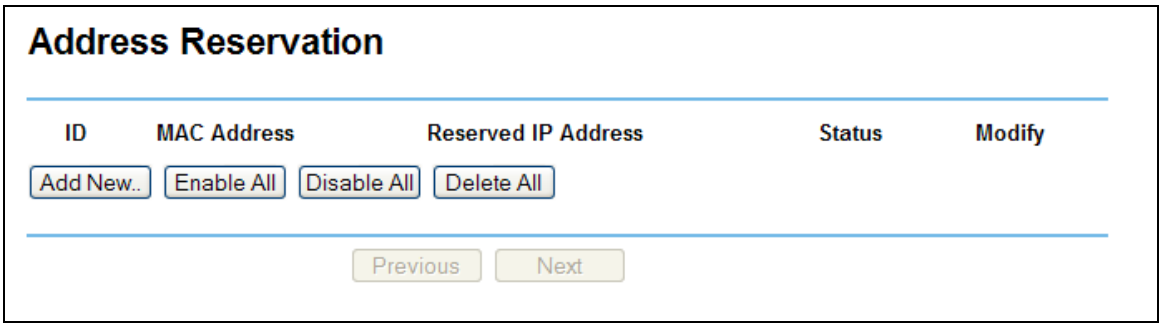
**Assigned IP** The IP address that the router has allocated to the DHCP client.

**Lease Time** The time of the DHCP client leased. Before the time is up, DHCP client will request to renew the lease automatically.

You cannot change any of the values on this page. To update this page and to show the current attached devices, click **Refresh**.

# Address Reservation

When you specify a reserved IP address for a PC on the LAN, that PC will always receive the same IP address each time when it accesses the DHCP server. Reserved IP addresses should be assigned to servers that require permanent IP settings. This page is used for address reservation.




Address Reservation

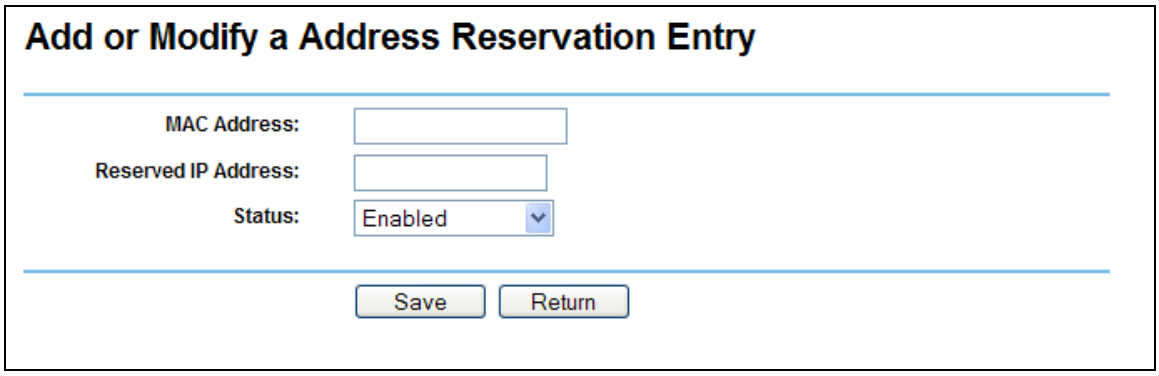
**MAC Address** The MAC address of the PC of which you want to reserve IP address.

**Assigned IP Address** The IP address of the router reserved.

**Status** The status of this entry either Enabled or Disabled.

**To Reserve IP addresses:**

1. Click **Add New**.
2. Enter the **MAC address** (The format for the MAC Address is XX-XX-XX-XX-XX-XX.) and IP address in dotted-decimal notation of the computer you wish to add.
3. Click **Save**.




Add or Modify an Address Reservation Entry

**To modify or delete an existing entry:**

1. Click **Modify** in the entry you want to modify. If you want to delete the entry, click the **Delete**.
2. Modify the information.
3. Click **Save**.

Click **Enable All** to make all entries enabled

Click **Disabled All** to make all entries disabled.

Click **Delete All** to delete all entries

Click **Next** to go to the next page or click **Previous** to return the previous page.

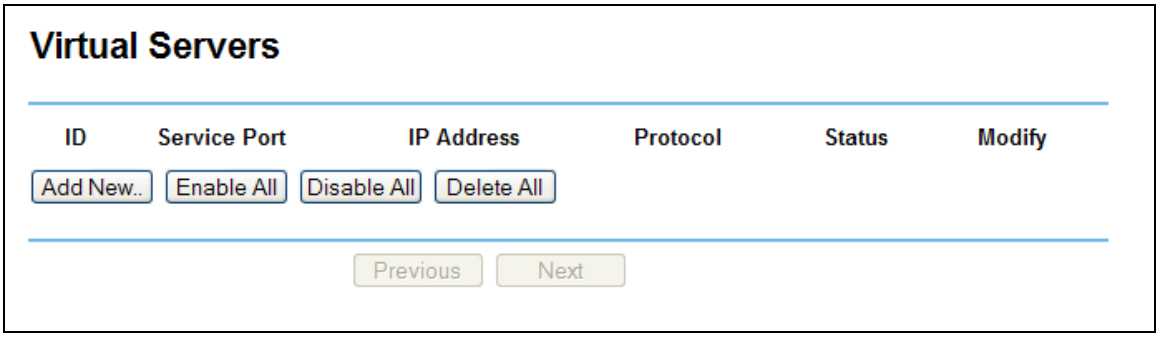
> **Note:** The function won't take effect until the router reboots.

# Forwarding

There are four submenus under the Forwarding menu: Virtual Servers, Port Triggering, DMZ and UPnP. Click any of them, and you will be able to configure the corresponding function. The detailed explanations for each submenu are provided below.

## Virtual Servers

Virtual servers can be used for setting up public services on your LAN, such as DNS, Email and FTP. A virtual server is defined as a service port, and all requests from the Internet to this service port will be redirected to the computer specified by the server IP. Any PC that was used for a virtual server must have a static or reserved IP Address because its IP Address may change when using the DHCP function. You can set up virtual servers on this page:




Virtual Servers

**Service Port** The numbers of External Ports. You can type a service port or a range of service ports (the format is XXX – YYY, XXX is Start port, YYY is End port).

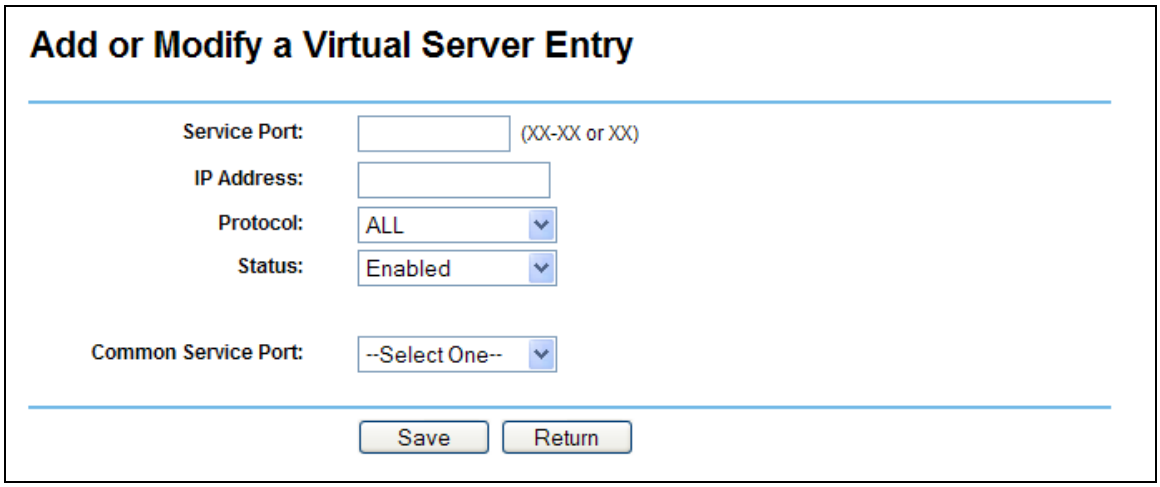
**IP Address** The IP Address of the PC providing the service application.

**Protocol** The protocol used for this application, either TCP, UDP, or All (all protocols supported by the router).

**Status** The status of this entry either Enabled or Disabled.

**To setup a virtual server entry:**

1. Click **Add New**.
2. Select the service you want to use from the Common Service Port list. If the Common Service Port list does not have the service that you want to use, type the number of the service port or service port range in the Service Port box.
3. Type the IP Address of the computer in **Server IP Address**.
4. Select the protocol used for this application:
   - TCP
   - UDP
   - All
5. Select a Status.
6. Click **Save**.




Add or Modify a Virtual Server Entry

> **Note:** It is possible that you have a computer or server that has more than one type of available service. If so, select another service, and enter the same IP Address for that computer or server.

**To modify or delete an existing entry:**

1. Click **Modify** in the entry you want to modify. If you want to delete the entry, click **Delete**.
2. Modify the information.
3. Click **Save**.

Click **Enable All** to make all entries enabled

Click **Disabled All** to make all entries disabled.

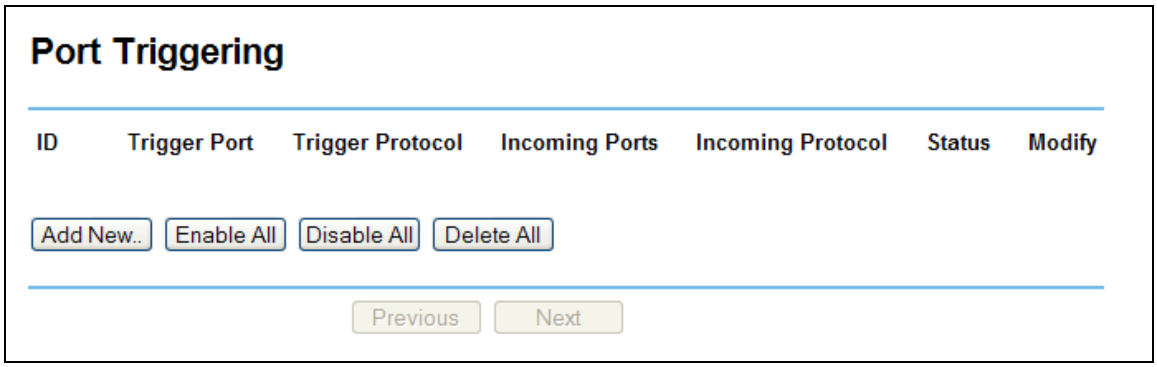
Click **Delete All** to delete all entries

Click **Next** to go to the next page or click **Previous** to return the previous page.

> **Note:** If you set the virtual server of service port as 80, you must set the web management port on Security –> Remote Management page to be any value except 80 such as 8080. Or else there will be a conflict to disable the virtual server.

# Port Triggering

Some applications require multiple connections, like Internet games, video conferencing, Internet calling and so on. These applications cannot work with a pure NAT router. Port Triggering is used for some of these applications that can work with an NAT router. You can set up Port Triggering on this page:




Port Triggering

**Port triggering process:**

1. A local host makes an outgoing connection using a destination port number defined in the Trigger Port field.

2. The router records this connection, opens the incoming port or ports associated with this entry in the Port Triggering table, and associates them with the local host.

3. When necessary the external host will be able to connect to the local host using one of the ports defined in the Incoming Ports field.

   **Trigger Port** The port for outgoing traffic. An outgoing connection using this port will *Trigger* this rule.

   **Trigger Protocol** The protocol used for Trigger Ports, either TCP, UDP, or All (all protocols supported by the router).

   **Incoming Ports Range** The port or port range used by the remote system when it responds to the outgoing request. A response using one of these ports will be forwarded to the PC that triggered this rule. You can input at most 5 groups of

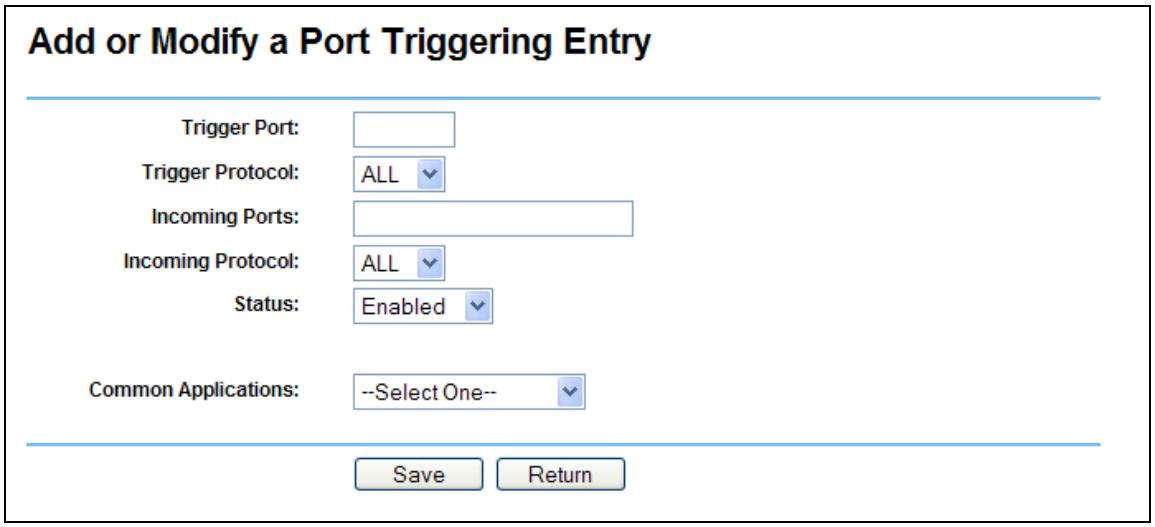
ports (or port section). Every group of ports must be set apart with a comma (,). For example, 2000-2038, 2050-2051, 2085, 3010-3030.

**Incoming Protocol** The protocol used for Incoming Ports Range, either TCP or UDP, or ALL (all protocols supported by the router).

**Status** The status of this entry either Enabled or Disabled.

**To add a new rule:**

1. Click **Add New**.
2. Enter a port number used by the application when it generates an outgoing request.
3. Select the protocol used for Trigger Port:
   - TCP
   - UDP
   - All
4. Enter the range of port numbers used by the remote system when it responds to the PC's request.
5. Select a protocol used for Incoming Ports Range:
   - TCP
   - UDP
   - All
6. Select the Status:
7. Click **Save**.




Add or Modify a Port Triggering Entry

There are many popular applications in the Popular Application list. You can select it, and the application will fill in the Trigger Port, incoming Ports Range boxes and select **Enable**. It has the same effect as adding a new rule.

**To modify or delete an existing entry:**

1. Click Modify in the entry you want to modify. If you want to delete the entry, click the **Delete**.
2. Modify the information.
3. Click **Save**.

Click **Enable All** to make all entries enabled

Click **Disabled All** to make all entries disabled.

Click **Delete All** to delete all entries

**Note:**

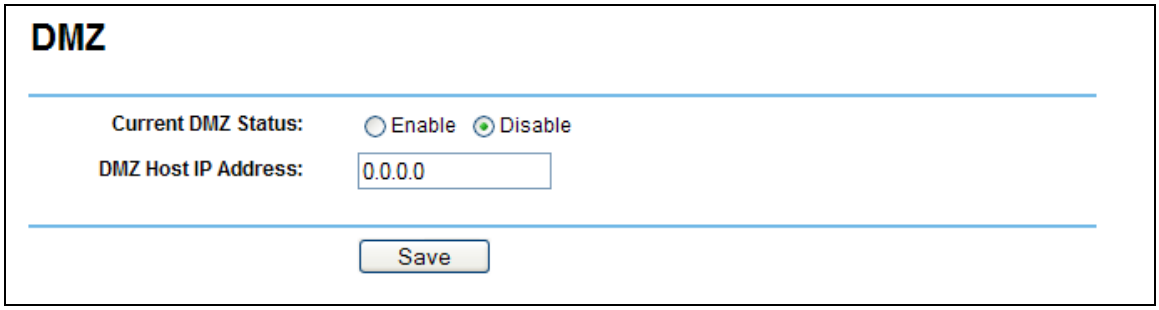
1. When the trigger connection is released, the according opening ports will be closed.

2. Each rule allowed to be used only by one host on LAN synchronously. The trigger connection of other hosts on LAN will be refused.

3. Incoming Port Range cannot overlap each other.

# DMZ (Demilitarized Zone)

The DMZ host feature allows one local host to be exposed to the Internet for a special-purpose service such as Internet gaming or videoconferencing. DMZ host forwards all the ports at the same time. Any PC whose port is being forwarded must have its DHCP client function disabled and should have a new static IP Address assigned to it because its IP Address may change when using the DHCP function. You can set up DMZ host on this page:




**DMZ**

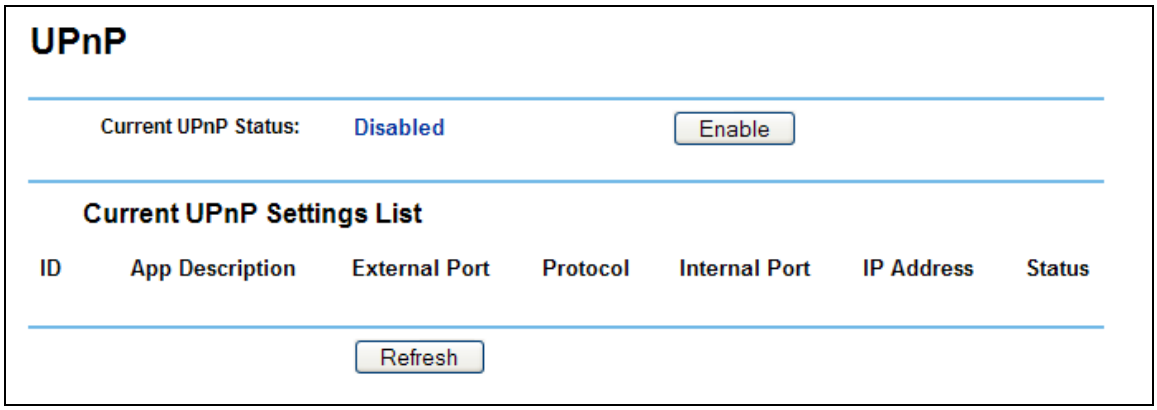
**To assign a computer or server to be a DMZ server:**

1. Select **Enable**.
2. Enter the local host IP Address in the DMZ Host IP Address field.
3. Click **Save**.

**Note:** After you set the DMZ host, the firewall related to the host will not work.

# UPnP (Universal Plug and Play)

The Universal Plug and Play (UPnP) feature allows the devices, such as Internet computers, to access the local host resources or devices as needed. UPnP devices can be automatically discovered by the UPnP service application on the LAN. You can configure UPnP on this page:




UPnP

**Current UPnP Status** UPnP can be enabled or disabled by selecting Enable or Disable. As allowing this may present a risk to security, this feature is disabled by default.

**Current UPnP Settings List** This table displays the current UPnP information.

- App Description – The description provided by the application in the UPnP request
- External Port - External port, which the router opened for the application.
- Protocol - Which type of protocol is opened.
- Internal Port - Internal port, which the router opened for local host.
- IP Address - The UPnP device that is currently accessing the router.
- Status - Enabled means that port is still active, otherwise, the port is inactive.

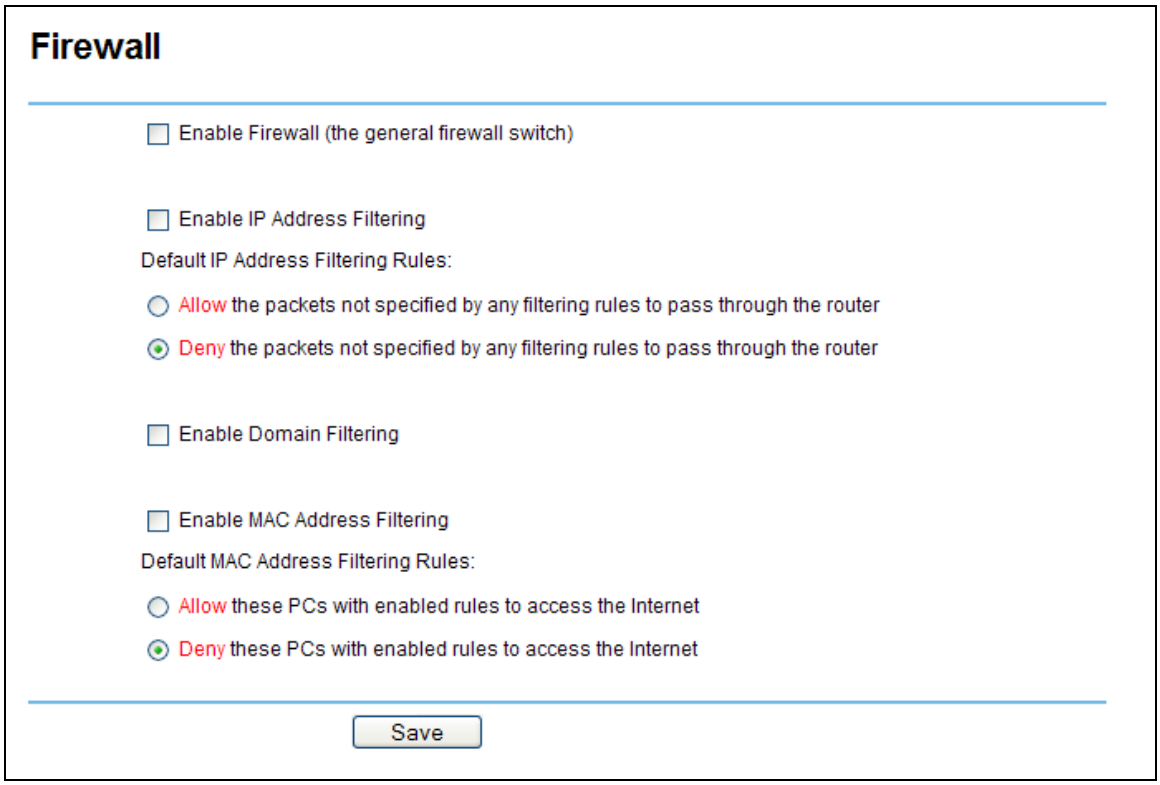
Click **Refresh** to update the Current UPnP Settings List.

# Security

There are six submenus under the Security menu: Firewall, IP Address Filtering, Domain Filtering, MAC Filtering, Remote Management and Advanced Security. Click any of them, and you will be able to configure the corresponding function.

## Firewall

Using the Firewall page you can turn the general firewall switch on or off. The default setting for the switch is off. If the general firewall switch is off, even if IP Address Filtering, DNS Filtering and MAC Filtering are enabled, their settings are ineffective.




**Firewall**

**Enable Firewall** the general firewall switch is on or off.

**Enable IP Address Filtering** set IP Address Filtering is enabled or disabled. There are two default filtering rules of IP Address Filtering, either Allow or Deny passing through the router.

**Enable Domain Filtering** set Domain Filtering is enabled or disabled.

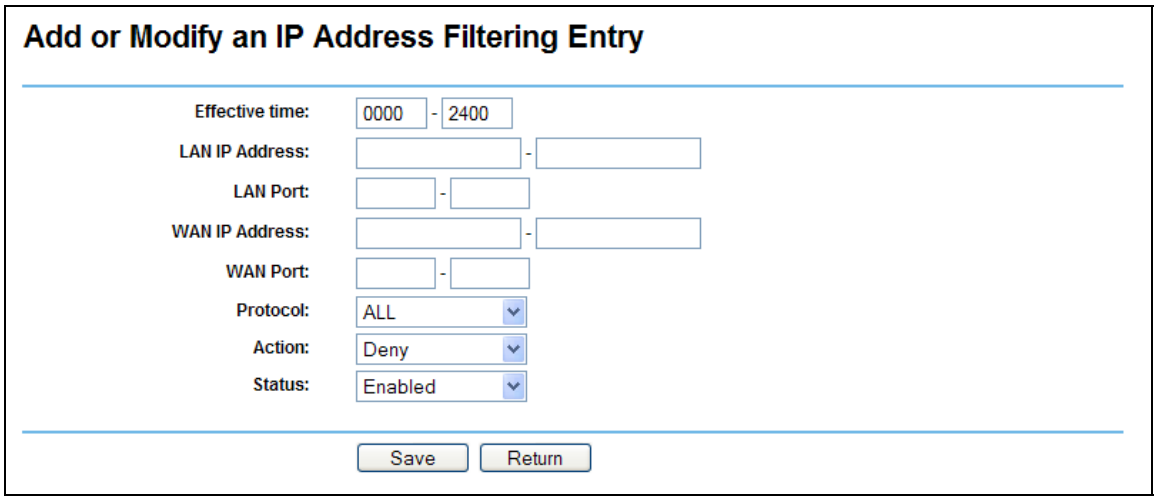
**Enable MAC Filtering** set MAC Address Filtering is enabled or disabled. You can select the default filtering rules of MAC Address Filtering, either Allow or Deny accessing the router.

# IP Address Filtering

The IP address Filtering feature allows you to control Internet Access by specific users on your LAN based on their IP addresses. The IP address filtering is set on this page:


**IP Address Filtering**

To disable the IP Address Filtering feature, keep the default setting, Disabled. To set up an IP Address Filtering entry, click Enable Firewall and Enable IP Address Filtering on the Firewall page, and click **Add New**. The page **Add or Modify an IP Address Filtering entry** will appear:




Add or Modify an IP Address Filtering Entry

**To create or modify an IP Address Filtering entry:**

1. Enter the effective range of time when the filter will be applied. For example, enter 0803 and 1705 to make the filter take effect from 08:03 to 17:05.

2. Enter a LAN IP Address or a range of LAN IP addresses in the field, in dotted-decimal notation format. For example, 192.168.1.20 - 192.168.1.30. Keep the field open, which means all LAN IP Addresses have been put into the field.

3. Enter a LAN Port or a range of LAN ports in the field. For example, 1030 - 2000. Keeping the field blank means all LAN ports have been put into the field.

4. Enter a WAN IP Address or a range of WAN IP Addresses in the field, in dotted-decimal notation format. For example, 61.145.238.6 – 61.145.238.47. Keeping the field blank means all WAN IP Addresses have been put into the field.

5. Enter a WAN Port or a range of WAN Ports in the field. For example, 25 – 110. Keeping the field blank means all WAN Ports have been put into the field.

6. Select a protocol

   - TCP
   - UDP
   - All

7. Select an action
   - Allow
   - Deny
8. Select a status
   - Enabled
   - Disabled
9. Click **Save**.

**To modify or delete an existing entry:**

1. Click **Modify** in the entry you want to modify. If you want to delete the entry, click the **Delete**.
2. Modify the information.
3. Click **Save**.

Click **Enable All** to make all entries enabled

Click **Disabled All** to make all entries disabled.

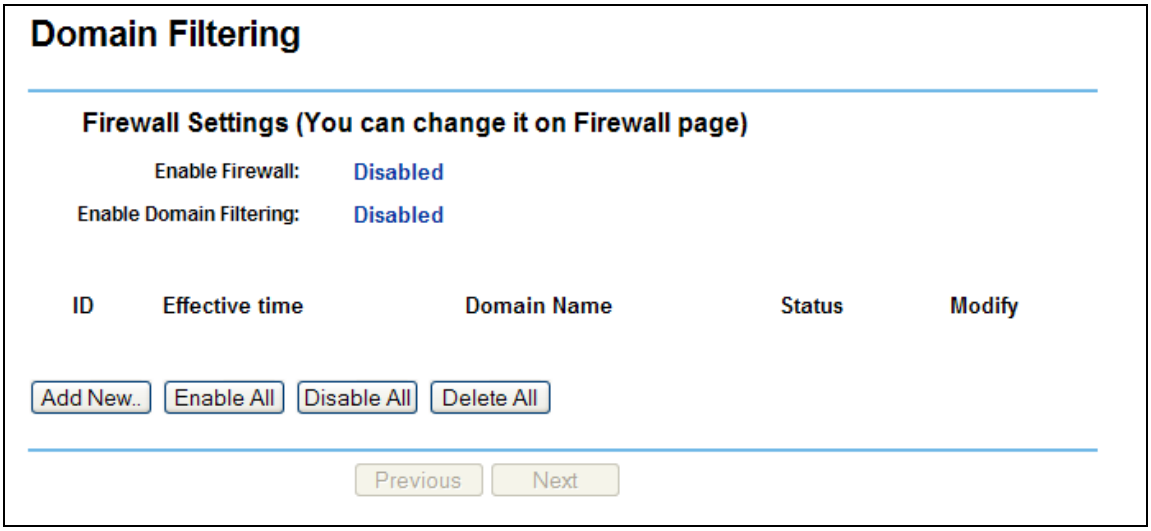
Click **Delete All** to delete all entries

Click **Next** to go the next page or click **Previous** to return to the previous page.

For example: If you desire to block E-mail received and sent by the IP Address 192.168.1.7 on your local network, and to make the PC with IP Address 192.168.1.8 unable to visit the website of IP Address 202.96.134.12, while other PCs have no limit you should specify the following IP address filtering list:

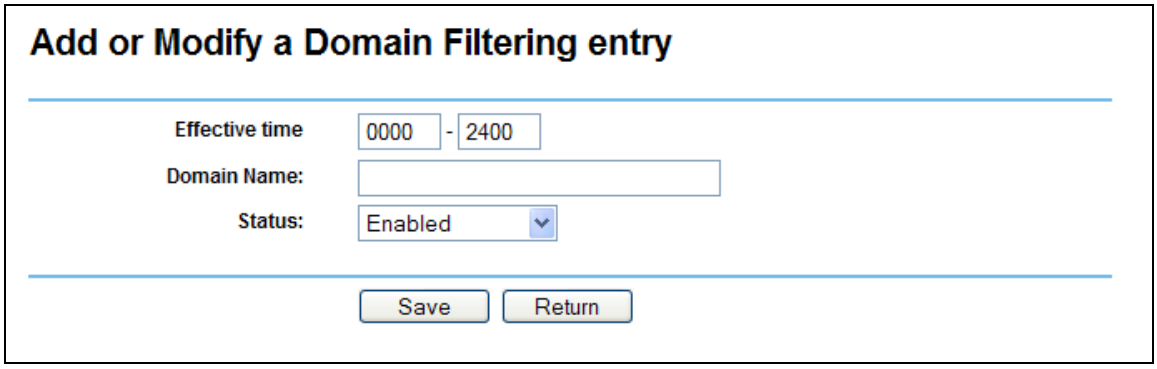
# Domain Filtering

The Domain Filtering page allows you to control access to certain websites on the Internet by specifying their domains or key words.




Domain Filtering

Before adding a Domain Filtering entry, you must ensure that Enable Firewall and Enable Domain Filtering have been selected on the Firewall page. To Add a Domain filtering entry, click **Add New**. The page **Add or Modify a Domain Filtering entry** will appear:




Add or Modify a Domain Filtering Entry

**To add or modify a Domain Filtering entry, follow these instructions:**

1. Effective Time - Enter a range of time in HHMM format specifying the time for the entry to take effect. For example, if you enter: 0803 - 1705, than the entry will take effect from 08:03 to 17:05.

2. Domain Name - Type the domain or key word as desired in the field. A blank in the domain field means all websites on the Internet. For example: www.xxyy.com.cn, .net.
3. Status - Select Enabled or Disabled for this entry on the Status pull-down list.
4. Click **Save**.

**To modify or delete an existing entry:**

1. Click the Modify in the entry you want to modify. If you want to delete the entry, click the Delete.
2. Modify the information.
3. Click **Save**.

Click **Enabled All** to make all entries enabled.

Click **Disabled All** to make all entries disabled.

Click **Delete All** to delete all entries

Click **Next** to go to the next page or **Previous** to return to the previous page.

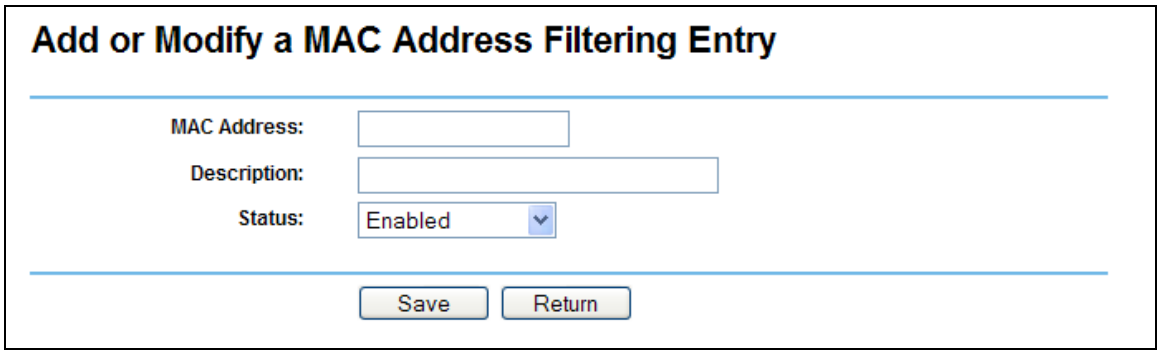
For example, if you want to block the PCs on your LAN to access websites www.xxyy.com.cn, www.aabbcc.com and websites with .net in the end on the Internet while no limit for other websites, you should specify the following Domain filtering list:

# MAC Filtering

Like the IP Address Filtering page, the MAC Address Filtering page allows you to control access to the Internet by users on your local network based on their MAC Address.


MAC Address Filtering

Before setting up MAC Filtering entries, you must ensure that Enable Firewall and Enable MAC Filtering have been selected on the Firewall page. To Add a MAC Address filtering entry, click Add New. The page **Add or Modify a MAC Address Filtering entry** will appear:




Add or Modify a MAC Address Filtering Entry

**To add or modify a MAC Address Filtering entry, follow these instructions:**

1. Enter the appropriate MAC Address into the MAC Address field. The format of the MAC Address is XX-XX-XX-XX-XX-XX (X is any hexadecimal digit). For example: 00-0E-AE-B0-00-0B.

2. Type the description of the PC in the Description field. Fox example: John's PC.
3. Status - Select Enabled or Disabled for this entry on the Status pull-down list.
4. Click **Save**.
5. When finished, click **Return** to return to the MAC Address Filtering page.

**To modify or delete an existing entry:**

1. Click the **Modify** in the entry you want to modify. If you want to delete the entry, click the **Delete**.
2. Modify the information.
3. Click **Save**.

Click **Enable All** to make all entries enabled.

Click **Disabled All** to make all entries disabled.

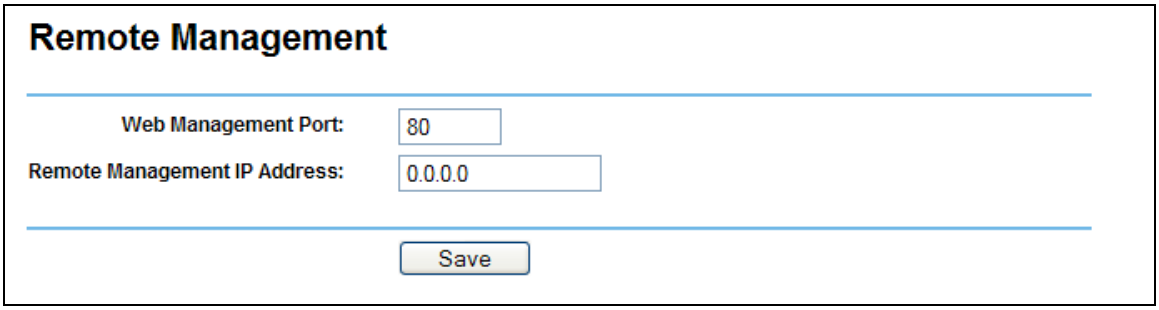
Click **Delete All** to delete all entries

Click **Next** to go to the next page or click **Previous** to return to the previous page.

Fox example: If you want to block the PC with MAC addresses 00-0A-EB-00-07-BE and 00-0A-EB-00-07-5F to access the Internet, first, enable the Firewall and MAC Address Filtering on the Firewall page, then, you should specify the Default MAC Address Filtering Rule **Deny these PCs with effective rules to access the Internet** on the Firewall page and the following MAC address filtering list.

# Remote Management

Remote Management allows you to manage your Router from a remote location, via the Internet.




Remote Management

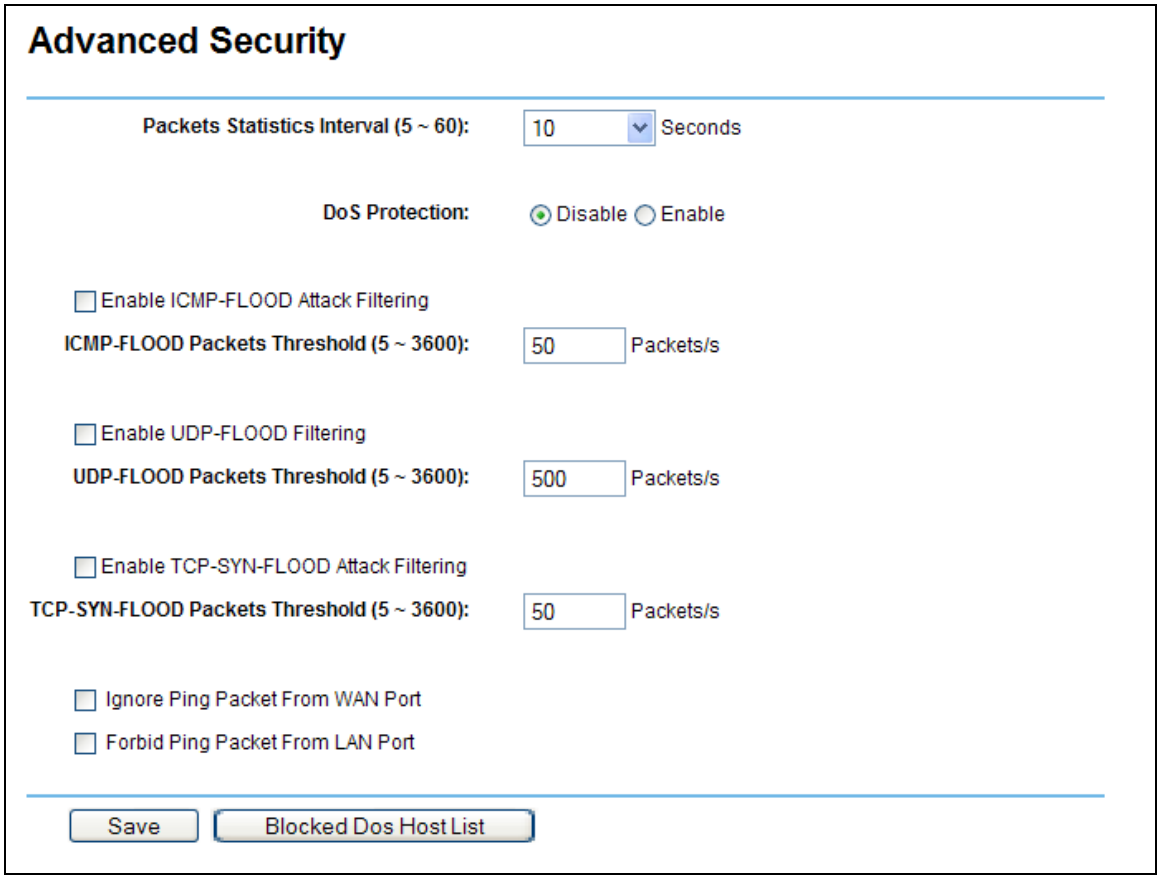
**Web Management Port** Web browser access normally uses the standard HTTP service port 80. This router's default remote management web port number is 80. For greater security, you can change the remote management web interface to a custom port by entering that number in this box provided. Choose a number between 1024 and 65534, but do not use the number of any common service port.

**Remote Management IP Address** This is the current address you will use when accessing your router from the Internet. The default IP Address is 0.0.0.0. It means this function is disabled. To enable this function, change the default IP Address to another IP Address as desired. To access the router, you will type your router's WAN IP Address into your browser's Address (in IE) or Location (in Navigator) box, followed by a colon and the custom port number. For example, if your Router's WAN address is 202.96.12.8 and you use port number 8080, enter in your browser: http://202.96.12.8:8080. You will be asked for password. After successfully entering the password, you will be able to access the router's web-based utility.

**Note:** Be sure to change the router's default password to a very secure password.

# Advanced Security

Using Advanced Security page, you can protect the router from being attacked by TCP-SYN Flood, UDP Flood and ICMP-Flood from LAN.




Advanced Security

**Packets Statistic interval (5 ~ 60)** The default value is 10. Select a value between 5 and 60 seconds in the pull-down list. The Packets Statistic interval value indicates the time section of the packets statistic. The result of the statistic used for analysis by SYN Flood, UDP Flood and ICMP-Flood.

**DoS protection** Enable or Disable the DoS protection function. Only when it is enabled, will the flood filters be effective.

**Enable ICMP-FLOOD Attack Filtering** Enable or Disable the ICMP-FLOOD Attack Filtering.

**ICMP-FLOOD Packets threshold: (5 ~ 3600)** The default value is 50. Enter a value between 5 ~ 3600 packets. When the current ICMP-FLOOD Packets number sis beyond the set value, the router will start up the blocking function immediately.

**Enable UDP-FLOOD Filtering** Enable or Disable the UDP-FLOOD Filtering.

**UDP-FLOOD Packets threshold: (5 ~ 3600)** The default value is 50. Enter a value between 5 ~ 3600 packets. When the current UPD-FLOOD Packets numbers is beyond the set value, the router will start up the blocking function immediately.

**Enable TCP-SYN-FLOOD Attack Filtering** Enable or Disable the TCP-SYN- FLOOD Attack Filtering.

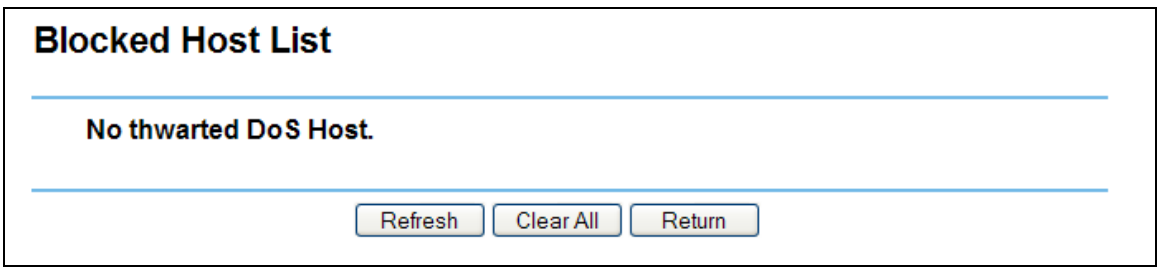
**TCP-SYN-FLOOD Packets threshold: (5 ~ 3600)** The default value is 50. Enter a value between 5 ~ 3600 packets. When the current TCP-SYN-FLOOD Packets numbers is beyond the set value, the router will start up the blocking function immediately.

**Ignore Ping Packet from WAN Port** Enable or Disable ignore ping packet from WAN port. The default is disabled. If enabled, the ping packet from the Internet cannot access the router.

**Forbid Ping Packet from LAN Port** Enable or Disable forbidding Ping Packet to access the router from the LAN port. The default value is disabled. If enabled, the ping packet from the LAN port cannot access the router. (Defends against some viruses)

Click **Save** to save the settings.

Click **Blocked DoS Host Table** to display the DoS host table by blocking.




Blocked Host List

This page shows Host IP Address and Host MAC Address for each host blocked by the router.

**Host IP Address** The IP address that blocked by DoS are displayed here.

**Host MAC Address** The MAC address that blocked by DoS are displayed here.

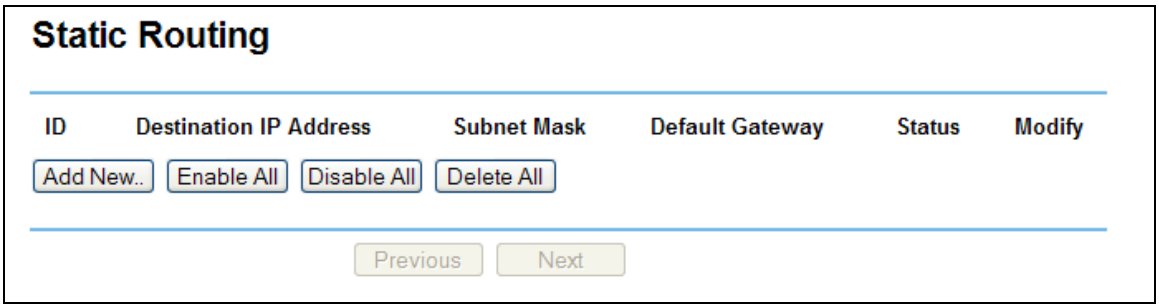
To update this page and to show the current blocked host, click **Refresh**.

Click **Clear All** to clear all displayed entries. After the table is empty the blocked host will regain the capability to access Internet.

Click **Return** to return to the Advanced Security page

# Static Routing

A static route is a pre-determined path that network information must travel to reach a specific host or network. To add or delete a route, work in the area under the Static Routing page (shown in figure 5-42).



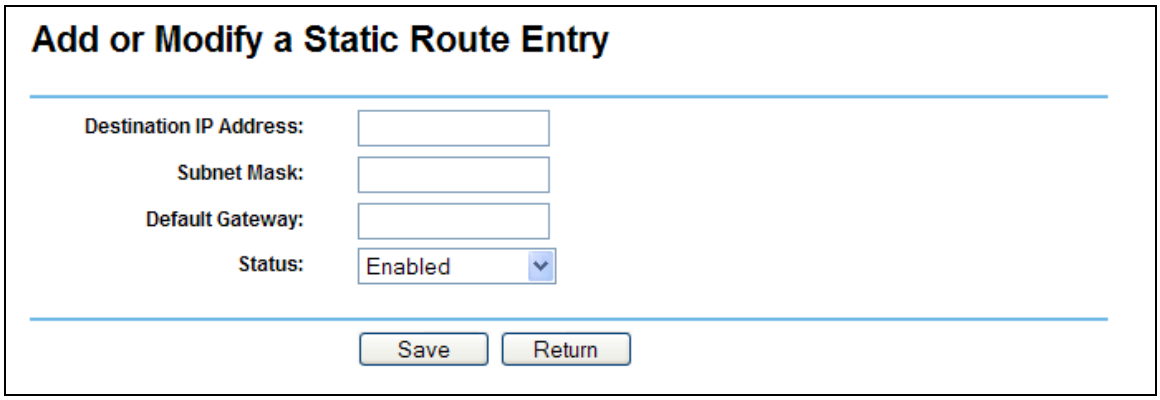

Static Routing

**Destination IP Address** The Destination IP Address is the address of the network or host that you want to assign to a static route.

**Subnet Mask** The Subnet Mask determines which portion of an IP Address is the network portion, and which portion is the host portion.

**Gateway** This is the IP Address of the gateway device that allows for contact between the router and the network or host.

# Add/Edit/Delete a Static Route Entry




Add or Modify a Static Route Entry

### To add static routing entries:

1. Click **Add New**.
2. Enter the following data:
   - Destination IP Address
   - Subnet Mask
   - Gateway
3. Select a status
   - Enabled
   - Disable
4. Click **Save**.

**To modify or delete an existing entry:**

1. Click Modify in the entry you want to modify. If you want to delete the entry, click the **Delete**.
2. Modify the information.
3. Click **Save**.

Click **Enable All** to make all entries enabled.

Click **Disabled All** to make all entries disabled.

Click **Delete All** to delete all entries

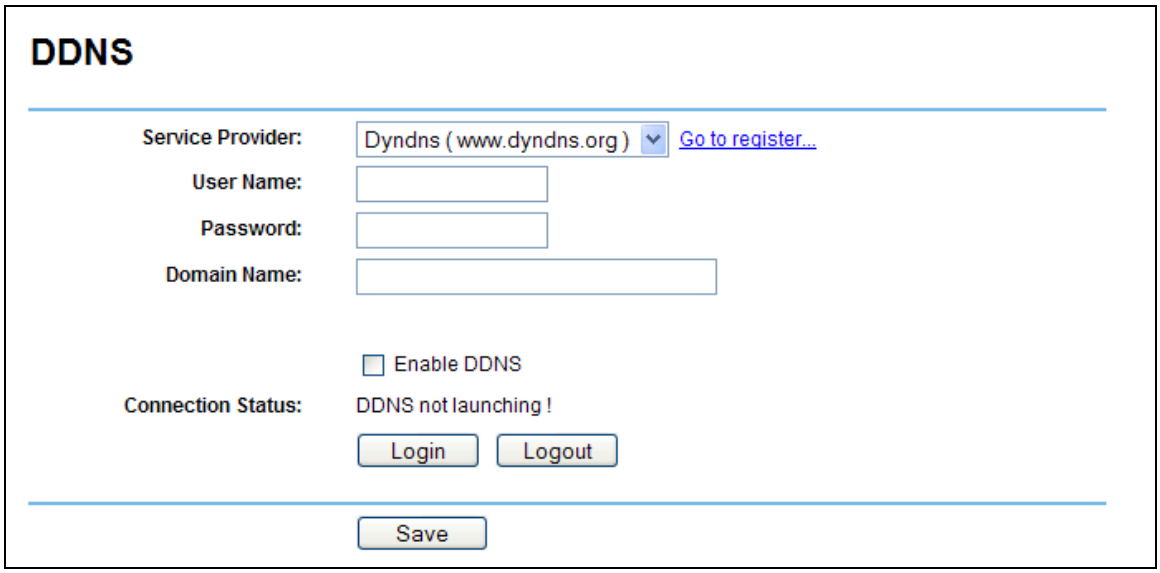
# Dynamic DNS

The router offers a Dynamic Domain Name System (DDNS) feature. DDNS lets you assign a fixed host and domain name to a dynamic Internet IP Address. It is useful when you are hosting your own website, FTP server, or other server behind the router.

Before using this feature, you need to sign up for DDNS service providers. The router supports three popular Dynamic DNS service providers that include:

- www.dyndns.org
- www.oray.net
- www.comexe.cn

# Using Dyndns (Dyndns.org)

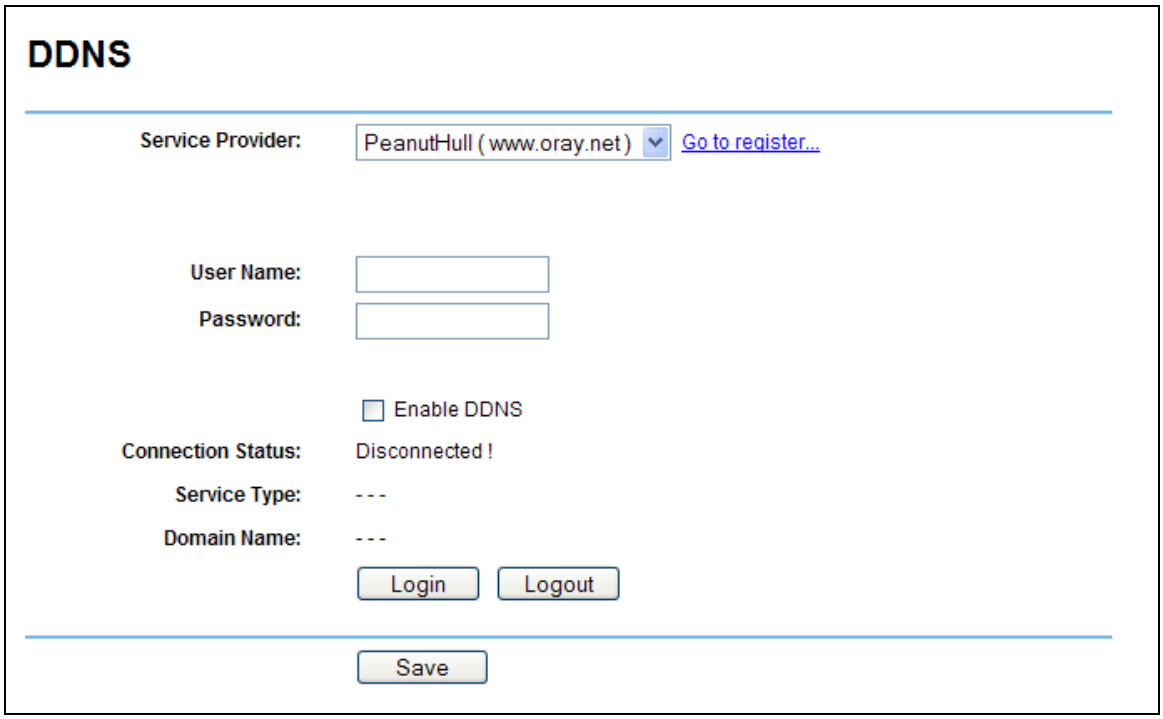



DDNS - Dyndns

**To set up DDNS:**

1. Select Dyndns (www.dyndns.org)
2. Enter **User Name** for your DDNS account.
3. Enter **Password** for your DDNS account.
4. Enter the **Domain name** from your dynamic DNS service provider.
5. Click **Login**. Check the **Connection Status**.
6. When you are connected to the dynamic DNS service provider, click **Save**.

# Using PeanutHull (www.oray.net)




DDNS - PeanutHull

**To set up for DDNS:**

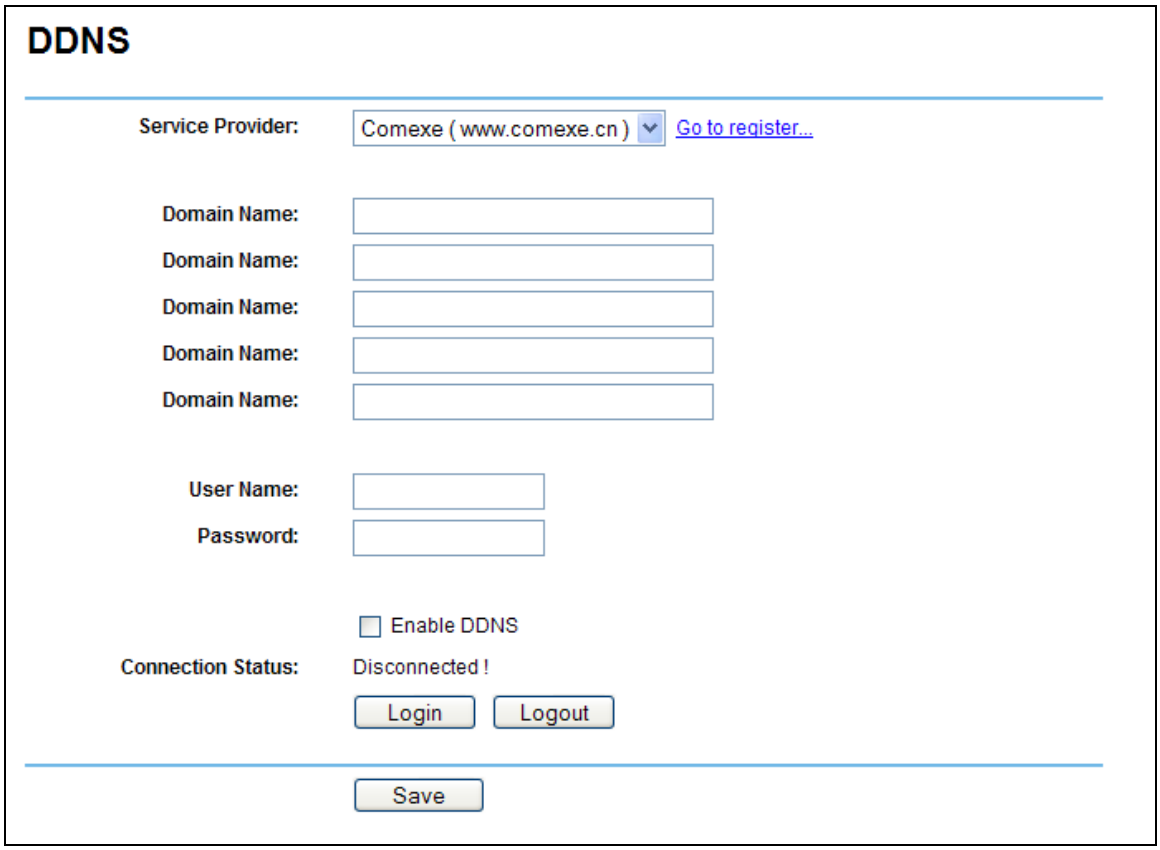
1. Type the User Name for your DDNS account.
2. Type the Password for your DDNS account.
3. Click Login to login the DDNS service.

**Connection Status** The status of the DDNS service connection is displayed here.

**Domain Name** The domain names are displayed here.

Click **Logout** to logout the DDNS service.

# Using Comexe (Comexe.cn)




DDNS - Comexe

**To set up DDNS:**

1. Enter the domain names your dynamic DNS service provider gave.
2. Type the User Name for your DDNS account.
3. Type the Password for your DDNS account.
4. Click Login to login to the DDNS service.

**Connection Status** The status of the DDNS service connection is displayed here.

Click **Logout** to logout of the DDNS service.

# Maintenance

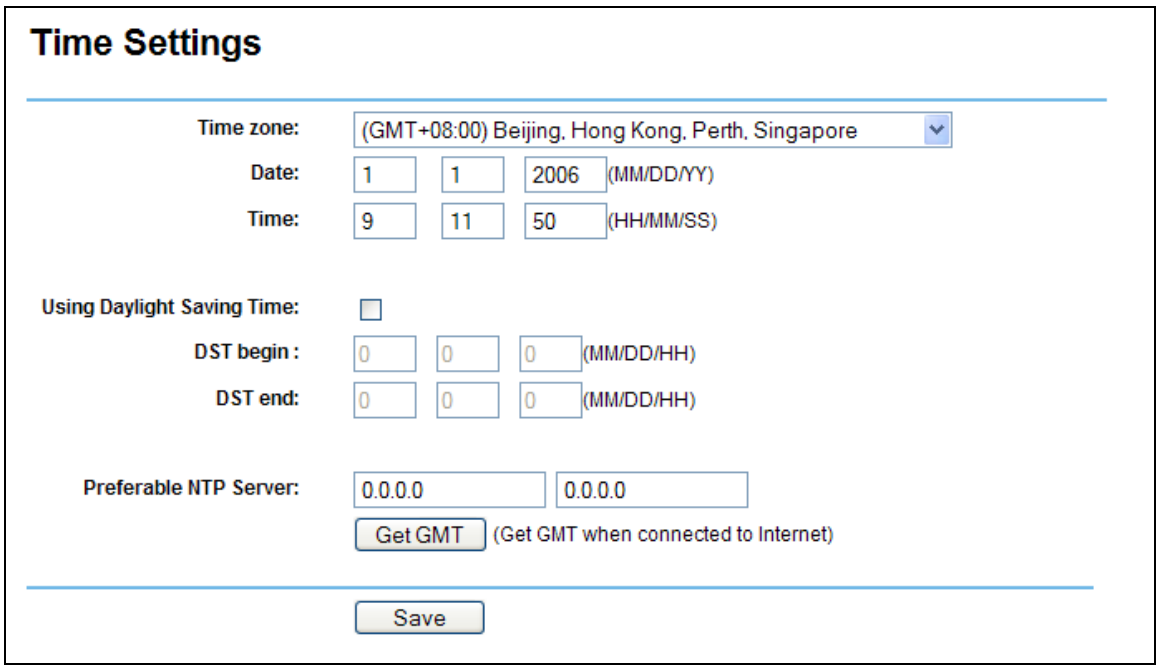
WL830RT4 provides several maintenance tools to help keep your router up to date.

# System Tools

The System Tools menu includes Time, Firmware, Factory Defaults, Backup and Restore, Reboot, Password, Log, and Statistics.

## Time

You can set time manually or get GMT from the Internet.




Time Settings

### To set time manually:

1. Select your local **Time zone**.
2. Enter **Date** and **Time**.
3. Click **Save**.

**To use NTP Server time:**

1. Enter Preferable NTP Server IP Address.
2. Click Get GMT.
3. Click Save.

**To enable daylight saving time:**

1. Select Using daylight saving time.
2. Enter DST begin and DST end.
3. Click Save.

**Note:**

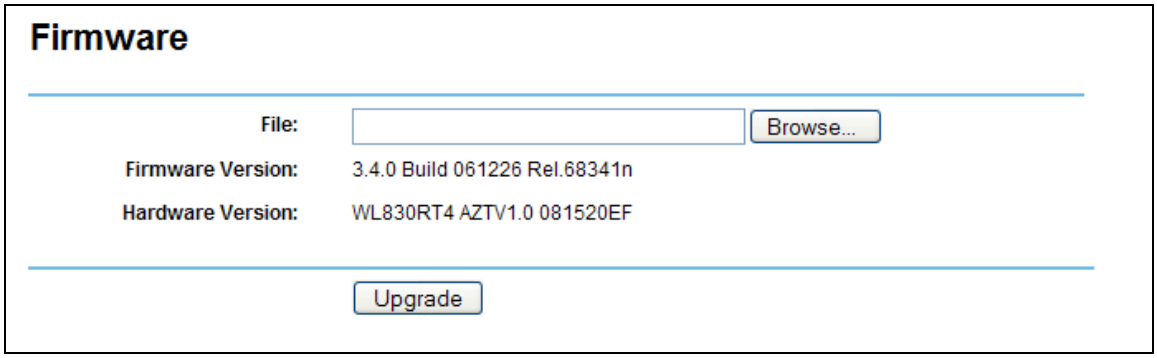
1. This setting will be used for some time-based functions such as firewall. You must specify your time zone once you login to the router successfully, if not, the time limited on these functions will not take effect.

2. The time will be lost if the router is turned off.

3. The router will obtain GMT automatically from Internet if it has already connected to Internet.

# Firmware

New firmware is posted at www.aztech.com and can be downloaded for free. If the router is not experiencing difficulties, there is no need to upgrade firmware, unless the new firmware supports a new feature you need.




Firmware

**Firmware Version** Displays the current firmware version.

**Hardware Version** Displays the current hardware version. The hardware version of the upgrade file must accord with the current hardware version.

**To upgrade the firmware:**

1. Download the latest firmware upgrade file from www.aztech.com.
2. Click **Browse** to select the downloaded file.
3. Click **Upgrade**.

**Note:**

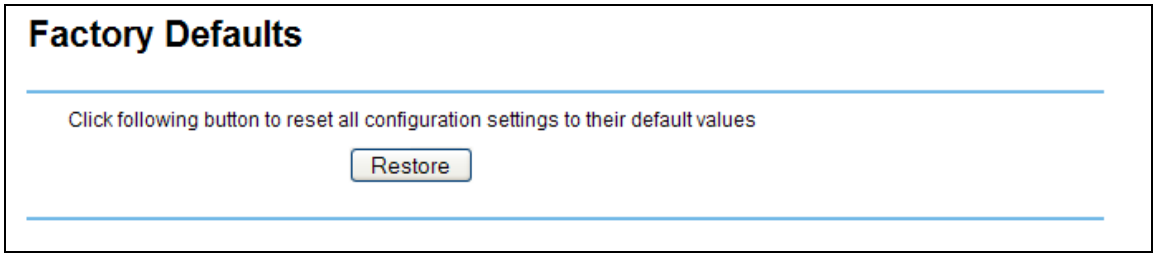
1. Do not unplug the router or press Reset while the firmware is being upgraded.

2. The router will reboot after the Upgrading has been finished.

3. When you upgrade the router's firmware, you will lose current configuration settings, so make sure you backup the router's settings before you upgrade its firmware.

# Factory Defaults

This page allows you to restore the factory default settings. Click **Restore** to reset all configuration settings to their default values.




**Factory Defaults**

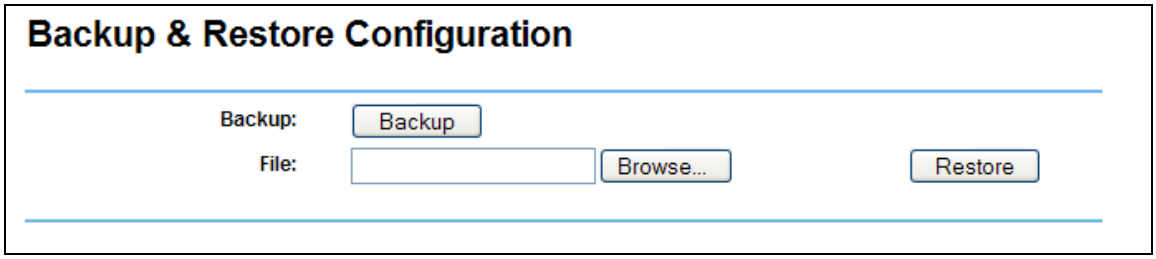
The default values are:

- User Name: admin
- Password: admin
- IP Address: 192.168.1.1
- Subnet Mask: 255.255.255.0

**Note:** Any settings you have saved will be lost when the default settings are restored.

# Backup and Restore

This page allows you to save current configuration of router as backup or restore the configuration file you saved before. Click **Backup** to save all configuration settings as a backup file in your local computer.




Backup & Restore Configuration

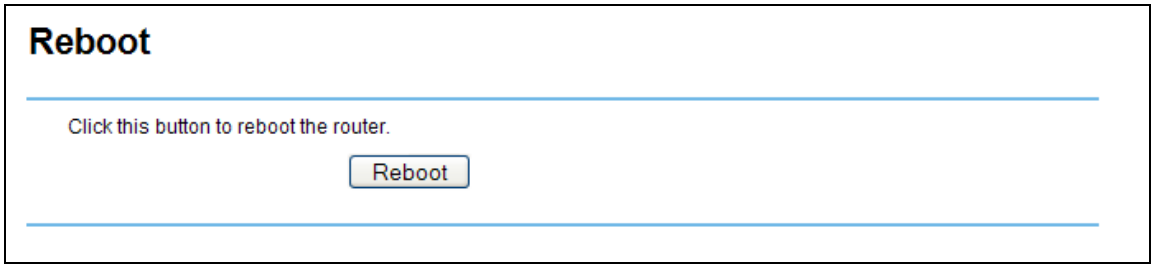
**To restore the router's configuration:**

1. Click **Browse** to select the backup file.
2. Click **Restore**.

> **Note:** The current configuration will be covered with the uploading configuration file. The restoration process lasts for 20 seconds and the router will restart automatically. Keep the router on during the restoring process to prevent any damage.

# Reboot

This page allows you to reboot the router. Click **Reboot** to reboot the router.




**Reboot**

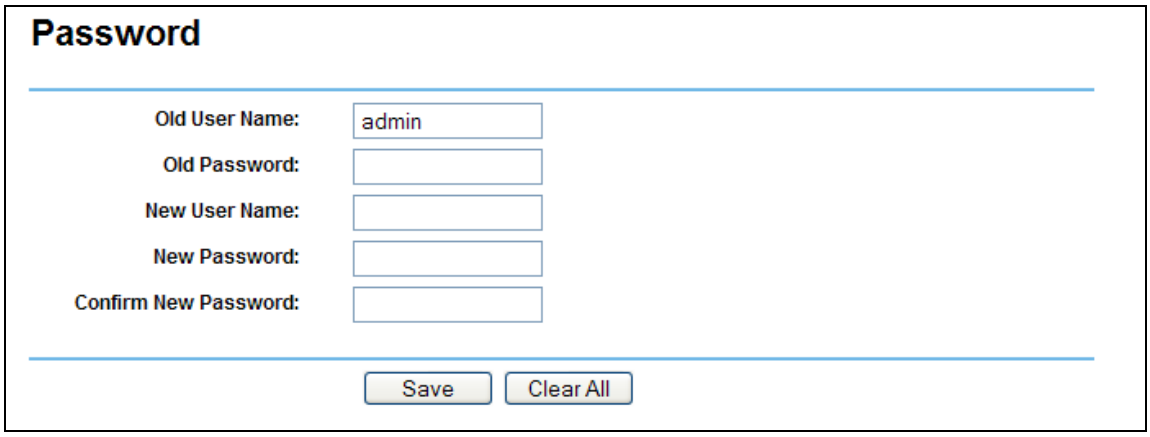
Some router settings will take effect only after rebooting. These include:

- Change LAN IP Address (automatic reboot)
- MAC Clone (automatic reboot)
- DHCP service function
- Static address assignment of DHCP server
- Web Service Port of the router
- Firmware upgrade (automatic reboot)
- Restore to factory default (automatic reboot)

# Password

It is strongly recommended that you change the default user name and password for the Web Manager.

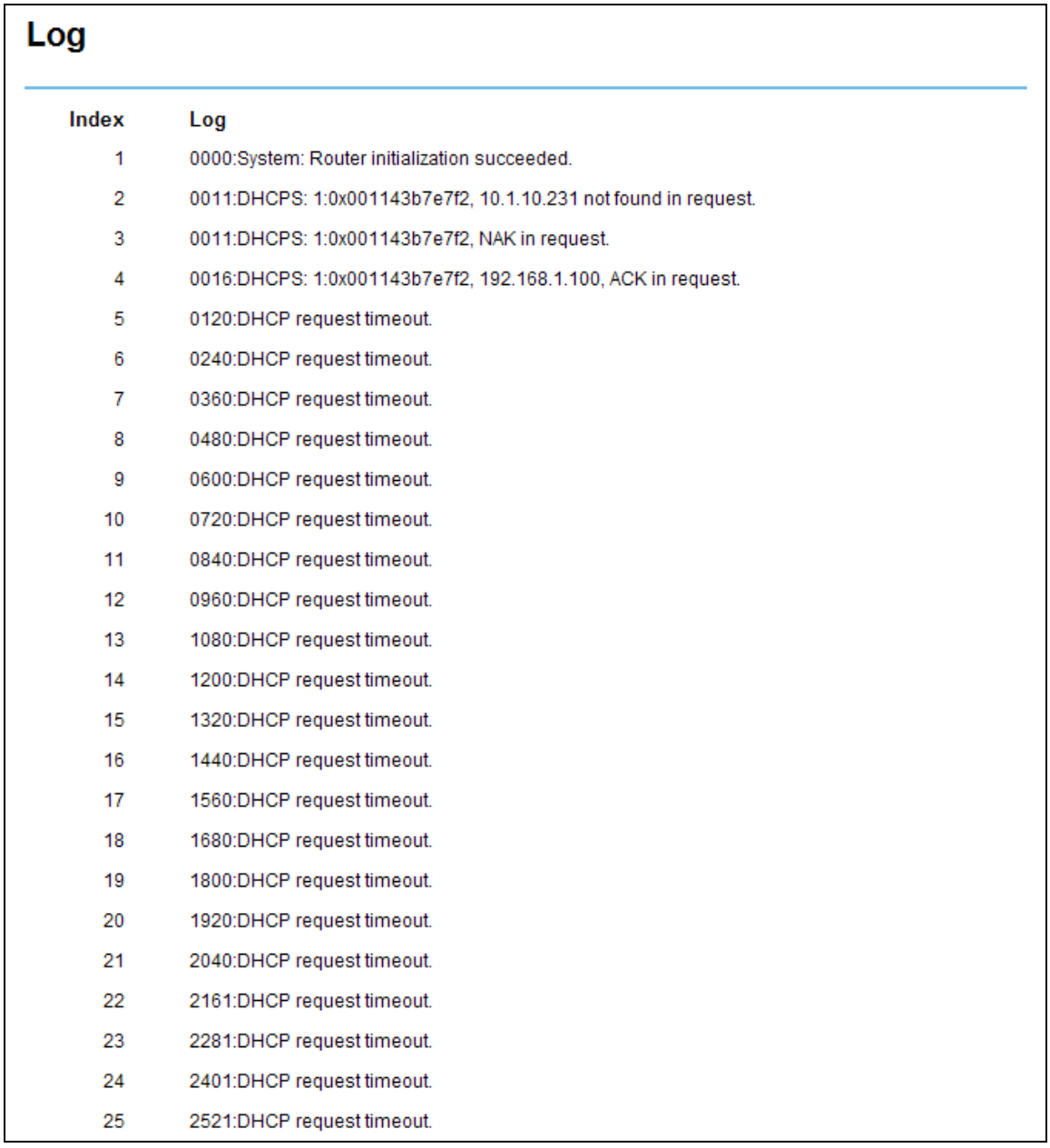
> **Note:** The new user name and password must not exceed 14 characters in length and must not include any spaces. Enter the new Password twice to confirm it.




**Password**

# Log

The router can keep logs of all traffic. You can query the logs to find what happened to the router. Click **Refresh** to refresh the logs. Click **Clear Log** to clear all the logs.



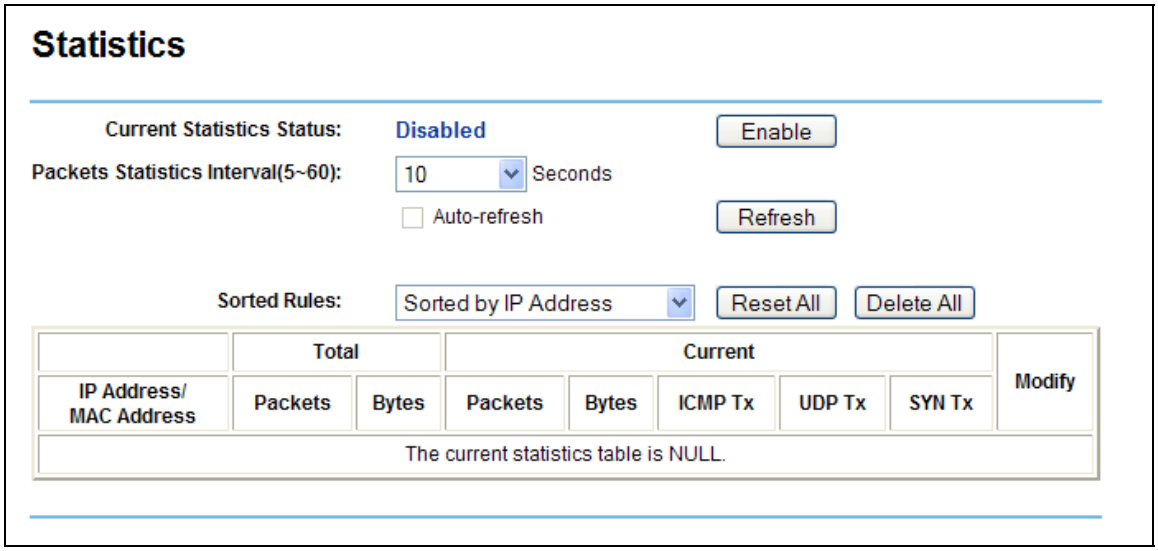
## Log

| Index | Log |
|---|---|
| 1 | 0000:System: Router initialization succeeded. |
| 2 | 0011:DHCPS: 1:0x001143b7e7f2, 10.1.10.231 not found in request. |
| 3 | 0011:DHCPS: 1:0x001143b7e7f2, NAK in request. |
| 4 | 0016:DHCPS: 1:0x001143b7e7f2, 192.168.1.100, ACK in request. |
| 5 | 0120:DHCP request timeout. |
| 6 | 0240:DHCP request timeout. |
| 7 | 0360:DHCP request timeout. |
| 8 | 0480:DHCP request timeout. |
| 9 | 0600:DHCP request timeout. |
| 10 | 0720:DHCP request timeout. |
| 11 | 0840:DHCP request timeout. |
| 12 | 0960:DHCP request timeout. |
| 13 | 1080:DHCP request timeout. |
| 14 | 1200:DHCP request timeout. |
| 15 | 1320:DHCP request timeout. |
| 16 | 1440:DHCP request timeout. |
| 17 | 1560:DHCP request timeout. |
| 18 | 1680:DHCP request timeout. |
| 19 | 1800:DHCP request timeout. |
| 20 | 1920:DHCP request timeout. |
| 21 | 2040:DHCP request timeout. |
| 22 | 2161:DHCP request timeout. |
| 23 | 2281:DHCP request timeout. |
| 24 | 2401:DHCP request timeout. |
| 25 | 2521:DHCP request timeout. |

**Log**

# Statistics

The Statistics page displays the network traffic of each computer in the LAN, including total traffic and traffic of the last Packets Statistic interval seconds.




Statistics

**Current Statistics Status** The default value is disabled. To enable, click Enable. If disabled, the function of DoS protection in Security settings will be ineffective.

**Packets Statistics Interval** The default value is 10. Select a value between 5 and 60 seconds in the pull-down list. The Packets Statistic interval indicates the time section of the packets statistic.

**Sorted Rules** Here displays sort as desired

### Statistics Table

**IP Address** The IP Address displayed with statistics

**Total** Overall total of packets sent/received

**Packets** The total amount of packets received and transmitted by the router.

**Bytes** The total amount of bytes received and transmitted by the router.

**Current** Current total of packets sent/received

**Packets** The total amount of packets received and transmitted in the last Packets Statistic interval seconds.

**Bytes** The total amount of bytes received and transmitted in the last Packets Statistic interval seconds.

**ICMP Tx** The total amount of the ICMP packets transmitted to WAN in the last Packets Statistic interval seconds.

**UDP Tx** The total amount of the UDP packets transmitted to WAN in the last Packets Statistic interval seconds.

**TCP SYN Tx** The total amount of the TCP SYN packets transmitted to WAN in the last Packets Statistic interval seconds.

Click **Save** to save the Packets Statistic interval value. Select **Auto-refresh** to refresh automatically. Click **Refresh** to refresh immediately.

# FAQ

**1. How do I configure the router to access Internet by ADSL users?**

- First, configure the ADSL modem configured in RFC1483 bridge model.
- Connect the Ethernet cable from your ADSL modem to the WAN port on the router. The telephone cord plugs into the Line port of the ADSL modem.
- Login to the router, click the **Network** menu on the left of your browser, and click WAN submenu. On the WAN page, select **PPPoE** for WAN Connection Type. Type user name in the User Name field and password in the Password field, finish by clicking **Connect**.
- If your ADSL lease is in **pay-according-time** mode, select **Connect on Demand** or **Connect Manually** for Internet connection mode. Type an appropriate number for **Max Idle Time** to avoid wasting paid time. Otherwise, you can select **Auto-connecting** for Internet connection mode.

**2. How do I configure the router to access Internet by Ethernet users?**

- Login to the router, click the **Network** menu on the left of your browser, and click **WAN** submenu. On the WAN page, select Dynamic IP for WAN Connection Type, finish by clicking **Save**.
- Some ISPs require that you register the MAC Address of your adapter, which is connected to your cable or DSL modem during installation. If your ISP requires MAC register, login to the router and click the **Network** menu link on the left of your browser, and then click **MAC Clone** submenu link. On the MAC Clone page, if your PC's MAC address is proper MAC address, click Clone MAC Address and your PC's MAC address will fill in the **WAN MAC Address** field. Or else, type the MAC Address into the WAN MAC Address field. The format for the MAC Address is XX-XX-XX-XX-XX-XX. Click **Save**. Changes take effect after rebooting.

**3. I want to use NetMeeting, what do I need to do?**

- If you start NetMeeting as a sponsor, you don't need to do anything with the router.
- If you start as a responsor, you need to configure Virtual Server or DMZ Host.
- How to configure Virtual Server: Login to the router, click the **Forwarding** menu on the left of your browser, and click **Virtual Servers** submenu. On the **Virtual Server** page, click Add New, then on the **Add or Modify a Virtual Server** page, enter **1720** into the blank behind the **Service Port**, and your IP address behind the IP Address, assuming 192.168.1.169 for an example, remember to **Enable** and **Save**.

> **Note:** Your opposite side should call your WAN IP, displayed on the Status page.

- How to enable DMZ Host: Login to the router, click the **Forwarding** menu on the left of your browser, and click **DMZ** submenu. On the DMZ page, click Enable radio and type your IP address into the DMZ Host IP Address field, using 192.168.1.169 as an example, remember to click **Save**.

**4. I want to build a WEB Server on the LAN, what should I do?**

- Because the WEB Server port 80 will interfere with the WEB management port 80 on the router, you must change the WEB management port number to avoid interference.
- To change the WEB management port number: Login to the router, click the **Security** menu on the left of your browser, and click **Remote Management** submenu. On the **Remote Management** page, type a port number except 80, such as 88, into the Web Management Port field. Click **Save** and reboot the router.

> **Note:** If the above configuration takes effect, to configure to the router by typing http://192.168.1.1:88 (the router's LAN IP address: Web Management Port) in the address field of the web browser.

- 3) Login to the router, click the **Forwarding** menu on the left of your browser, and click the **Virtual Servers** submenu. On the **Virtual Server** page, click Add New, then on the **Add or Modify a Virtual Server** page, enter **80** into the blank behind the **Service Port**, and your IP address behind the IP Address, assuming 192.168.1.188 for an example, remember to Enable and Save.

**5. The wireless clients cannot connect to the router.**

- Make sure the Wireless Router Radio is enabled.
- Verify the SSID.
- Verify the wireless security key.
- If the wireless connection is ready, but you cannot access the router, check the IP Address of your wireless stations.

# Glossary

## 2x to 3x eXtended Range™ WLAN Transmission Technology

The WLAN device with 2x to 3x eXtended Range™ WLAN transmission technology make its sensitivity up to 105 dB, which gives users the ability to have robust, longer-range wireless connections. With this range-enhancing technology, a 2x to 3x eXtended Range™ based client and access point can maintain a connection at as much as three times the transmission distance of traditional 802.11b and 802.11g products, for a coverage area that is up to nine times greater. A traditional 802.11b and 802.11g product transmission distance is about 300m, a 2x to 3x eXtended Range™ based client and access point can maintain a connection transmission distance may be up to 830m.

## 802.11b

The 802.11b standard specifies a wireless networking at 11 Mbps using direct-sequence spread-spectrum (DSSS) technology and operating in the unlicensed radio spectrum at 2.4GHz, and WEP encryption for security. 802.11b networks are also referred to as Wi-Fi networks.

## 802.11g

The technical specification for wireless networking at 54 Mbps using direct-sequence spread-spectrum (DSSS) technology, using OFDM modulation and operating in the unlicensed radio spectrum at 2.4GHz, and backward compatibility with IEEE 802.11b devices, and WEP encryption for security.

## DDNS (Dynamic Domain Name System)

The capability of assigning a fixed host and domain name to a dynamic Internet IP Address.

## DHCP (Dynamic Host Configuration Protocol)

A protocol that automatically configures the TCP/IP parameters of all the computers connected to a DHCP server.

## DMZ (Demilitarized Zone)

A Demilitarized Zone allows one local host to be exposed to the Internet for a special-purpose service such as Internet gaming or videoconferencing.

## DNS (Domain Name System)

An Internet Service that translates the names of websites into IP addresses.

## Domain Name

A descriptive name for an address or group of addresses on the Internet.

## DoS (Denial of Service)

A hacker attack designed to prevent your computer or network from operating or communicating.

## DSL (Digital Subscriber Line)

A technology that allows data to be sent or received over existing traditional phone lines.

## ISP (Internet Service Provider)

A company that provides access to the Internet.

## MTU (Maximum Transmission Unit)

The size in bytes of the largest packet that can be transmitted.

## NAT (Network Address Translation)

NAT technology translates IP addresses of a local area network to a different IP address for the Internet.

## PPPoE (Point to Point Protocol over Ethernet)

PPPoE is a protocol for connecting remote hosts to the Internet over an always-on connection by simulating a dial-up connection.

## SSID (Service Set Identifier)

A Service Set Identification is a thirty-two character (maximum) alphanumeric key identifying a wireless local area network. For the wireless devices in a network to communicate with each other, all devices must be configured with the same SSID. This is typically the configuration parameter for a wireless PC card. It corresponds to the ESSID in the wireless Access Point and to the wireless network name.

## WEP (Wired Equivalent Privacy)

A data privacy mechanism based on a 64-bit or 128-bit or 152-bit shared key algorithm, as described in the IEEE 802.11 standard.

## Wi-Fi

A trade name for the 802.11b wireless networking standard, given by the Wireless Ethernet Compatibility Alliance (WECA, see http://www.wi-fi.net), an industry standards group promoting interoperability among 802.11b devices.

## WLAN (Wireless Local Area Network)

A group of computers and associated devices communicate with each other wirelessly, which network serving users are limited in a local area.

# Regulatory Compliance Notices

## FCC STATEMENT

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

This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

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

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

1. This device may not cause harmful interference.
2. This device must accept any interference received, including interference that may cause undesired operation.

Changes or modifications to this unit not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

# FCC RF Radiation Exposure Statement

This equipment complies with FCC RF radiation exposure limits set forth for an uncontrolled environment. This device and its antenna must not be co-located or operating in conjunction with any other antenna or transmitter.

"To comply with FCC RF exposure compliance requirements, the antenna 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 Declaration of Conformity

This equipment is herewith confirmed to comply with the requirements set out in the Council Directive on the Approximation of the Laws of the Member States relating to Electromagnetic Compatibility (89/336/EEC), Low-voltage Directive (73/23/EEC) and the Amendment Directive (93/68/EEC), the procedures given in European Council Directive 99/5/EC and 89/3360EEC.

The equipment was passed. The test was performed according to the following European standards:

- EN 300 328 V.1.4.1 (2003)
- EN 301 489-1 V.1.4.1 (2002) / EN 301 489-17 V.1.2.1 (2002)
- EN 60950-1: 2001

European standards dictate maximum radiated transmit power of 100mW EIRP and frequency range 2.400-2.4835GHz; In France, the equipment must be restricted to the 2.4465-2.4835GHz frequency range and must be restricted to indoor use.

# ⚠ Safety Warnings

For your safety, be sure to read and follow all warning notices and instructions.

- Do not open the device. Opening or removing the device cover can expose you to dangerous high voltage points or other risks. Only qualified service personnel can service the device. Please contact your vendor for further information.
- Do not use your device during a thunderstorm. There may be a risk of electric shock brought about by lightning.
- Do not expose your device to dust or corrosive liquids.
- Do not use this product near water sources.
- Make sure to connect the cables to the correct ports.
- Do not obstruct the ventilation slots on the device.