TP-LINK®

User Guide

TL-WR841N

TL-WR841ND

Wireless N Router

Rev: 1.0.0

COPYRIGHT & TRADEMARKS

Specifications are subject to change without notice. TP-LINK® is a registered trademark of TP-LINK TECHNOLOGIES CO., LTD. Other brands and product names are trademarks or registered trademarks of their respective holders.

http://www.tp-link.com

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.

Any changes or modifications 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, this grant is applicable to only Mobile Configurations. The antennas used for this transmitter must be installed to provide a separation distance of at least 20 cm from all persons and must not be co-located or operating in conjunction with any other antenna or transmitter.”

CE Mark Warning

CE 1588 ①

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

National restrictions

This device is intended for home and office use in all EU countries (and other countries following the EU directive 1999/5/EC) without any limitation except for the countries mentioned below:

Country	Restriction	Reason/remark
Bulgaria	None	General authorization required for outdoor use and public service
France	Outdoor use limited to 10 mW e.i.r.p. within the band 2454-2483.5 MHz	Military Radiolocation use. Refarming of the 2.4 GHz band has been ongoing in recent years to allow current relaxed regulation. Full implementation planned 2012
Italy	None	If used outside of own premises, general authorization is required
Luxembourg	None	General authorization required for network and service supply(not for spectrum)
Norway	Implemented	This subsection does not apply for the geographical area within a radius of 20 km from the centre of Ny-Ålesund
Russian Federation	None	Only for indoor applications

CONTENTS

Package Contents **1**

Chapter 1. Introduction **2**

1.1 Overview of the Router 2

1.2 Conventions 3

1.3 Main Features 3

1.4 Panel Layout 4

1.4.1 The Front Panel 4

1.4.2 The Rear Panel 4

Chapter 2. Connecting the Router **6**

2.1 System Requirements 6

2.2 Installation Environment Requirements 6

2.3 Connecting the Router 6

Chapter 3. Quick Installation Guide **8**

3.1 TCP/IP configuration 8

3.2 Quick Installation Guide 10

Chapter 4. Configuring the Router **14**

4.1 Login 14

4.2 Status 14

4.3 Quick Setup 16

4.4 QSS 16

4.5 Network 21

4.5.1 LAN 21

4.5.2 WAN 22

4.5.3 MAC Clone 26

4.6 Wireless 26

4.6.1 Wireless Settings 27

4.6.2 Wireless Security 28

4.6.3 Wireless MAC Filtering 31

4.6.4 Wireless Advanced 33

4.6.5 Wireless Statistics 34
4.7 DHCP 35
4.7.1 DHCP Settings 35
4.7.2 DHCP Clients List 36
4.7.3 Address Reservation 37
4.8 Forwarding 38
4.8.1 Virtual Servers 38
4.8.2 Port Triggering 40
4.8.3 DMZ 42
4.8.4 UPnP 42
4.9 Security 43
4.9.1 Firewall 43
4.9.2 IP Filtering 44
4.9.3 Domain Filtering 47
4.9.4 MAC Filtering 49
4.10 Static Routing 50
4.11 Dynamic DNS 52
4.12 System Tools 53
4.12.1 Time Setting 53
4.12.2 Firmware 54
4.12.3 Factory Defaults 55
4.12.4 Backup & Restore 55
4.12.5 Reboot 56
4.12.6 Password 56
4.12.7 System log 57
4.12.8 Remote Management 58
4.12.9 Statistics 58
Appendix A: FAQ 60
Appendix B: Configuring the PCs 65
Appendix C: Specifications 69
Appendix D: Glossary 70

Package Contents

The following items should be found in your package:

- TL-WR841N/TL-WR841ND Wireless N Router
- DC Power Adapter
- Quick Installation Guide
- Resource CD, including:
  - This Guide
  - Other Helpful Information

☞ **Note:**

Make sure that the package contains the above items. If any of the listed items are damaged or missing, please contact with your distributor.

Chapter 1. Introduction

1.1 Overview of the Router

Thank you for choosing the TL-WR841N/TL-WR841ND Wireless N Router.

The TL-WR841N/TL-WR841ND Wireless N Router integrates 4-port Switch, Firewall, NAT-router and Wireless AP. Powered by 2x2 MIMO technology, the Wireless N Router delivers exceptional range and speed, which can fully meet the need of Small Office/Home Office (SOHO) networks and the users demanding higher networking performance.

Incredible Speed

The TL-WR841N/TL-WR841ND Wireless N Router provides up to 300Mbps wireless connection with other 802.11n wireless clients. The incredible speed makes it ideal for handling multiple data streams at the same time, which ensures your network stable and smooth. The performance of this 802.11n wireless router will give you the unexpected networking experience at speed 650% faster than 802.11g. It is also compatible with all IEEE 802.11g and IEEE 802.11b products.

Multiple Security Protections

With multiple protection measures, including SSID broadcast control and wireless LAN 64/128/152-bit WEP encryption, WiFi Protected Access (WPA2- PSK, WPA- PSK), as well as advanced Firewall protections, the TL-WR841N/841ND Wireless N Router provides complete data privacy.

Flexible Access Control

The TL-WR841N/TL-WR841ND Wireless N Router provides flexible access control, so that parents or network administrators can establish restricted access policies for children or staff. It also supports Virtual Server and DMZ host for Port Triggering, and then the network administrators can manage and monitor the network in real time with the remote management function.

Simple Installation

Since the router is compatible with virtually all the major operating systems, it is very easy to manage. Quick Setup Wizard is supported and detailed instructions are provided step by step in this user guide. Before installing the router, please look through this guide to know all the router's functions.

1.2 Conventions

The router or TL-WR841N/TL-WR841ND mentioned in this guide stands for TL-WR841N/TL-WR841ND Wireless N Router without any explanation.

☞ **Note:**

The two devices of TL-WR841N and TL-WR841ND are sharing this User Guide. For simplicity, we will take TL-WR841ND for example throughout this Guide,

The differences between them are:

- TL-WR841N router with 2 fixed antennas.
- TL-WR841ND router with 2 detachable antennas.

1.3 Main Features

- Complies with IEEE 802.11n draft version 2.0 to provide a wireless data rate of up to 300Mbps.
- One 10/100M Auto-Negotiation RJ45 WAN port, four 10/100M Auto-Negotiation RJ45 LAN ports, supporting Auto MDI/MDIX.
- Provides WPA/WPA2, WPA-PSK/WPA2-PSK authentication, TKIP/AES encryption security.
- Shares data and Internet access for users, supporting Dynamic IP/Static IP/PPPoE Internet access.
- Supports Virtual Server, Special Application and DMZ host.
- Supports UPnP, Dynamic DNS, Static Routing.
- Provide Automatic-connection and Scheduled Connection on certain time to the Internet
- Built-in NAT and DHCP server supporting static IP address distributing.
- Built-in firewall supporting IP address filtering, Domain Name filtering, and MAC address filtering.
- Connecting Internet on demand and disconnecting from the Internet when idle for PPPoE.
- Provides 64/128/152-bit WEP encryption security and wireless LAN ACL (Access Control List).
- Supports Flow Statistics.
- Supports firmware upgrade and Web management.

1.4 Panel Layout

1.4.1 The Front Panel

Figure 1-1 Front Panel sketch

The Router's LEDs and the QSS button are located on the front panel (View from left to right).

Name	Status	Indication
Power	Off	Power off
	On	Power on
System	On	The router is initializing or maybe has a system error
	Flashing	The router is working properly
	Off	The router has a system error
WLAN	Off	The Wireless function is disabled
	Flashing	The Wireless function is enabled
WAN, LAN 1-4	Off	There is no device linked to the corresponding port
	On	There is a device linked to the corresponding port but no activity
	Flashing	There is an active device linked to the corresponding port
QSS	Flash(green)	There is a wireless device connecting to the network by QSS function.
	On(green)	There is a wireless device successfully added to the network by QSS function.
	Flash(red)	There is a wireless device failed to add to the network by QSS function.

Table 2-1 The LEDs description

1.4.2 The Rear Panel

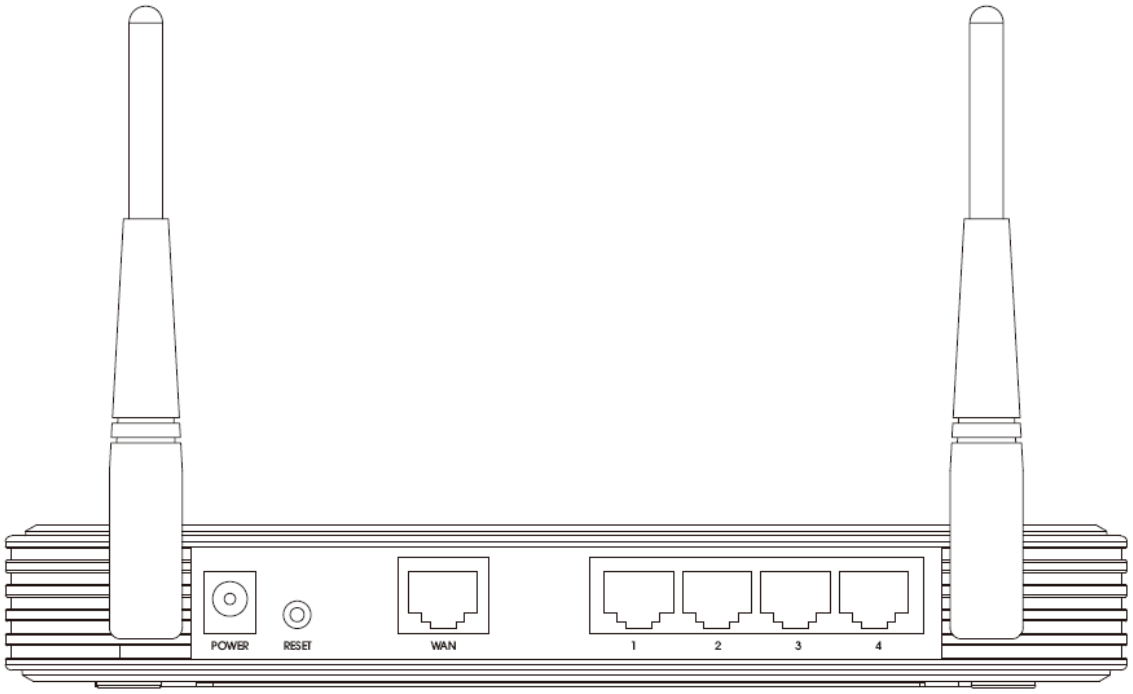


Figure 1-2 Rear Panel sketch

The following parts are located on the rear panel (View from left to right).

- **Power socket:** The Power socket is where you will connect the power adapter. Please use the power adapter provided with this TL-WR841N/TL-WR841ND Wireless N Router.
- **LAN 1,2,3,4:** These ports (1, 2, 3, 4) connect the router to the local PC(s)
- **WAN:** This WAN port is where you will connect the DSL/cable Modem, or Ethernet
- **Reset button**

  There are two ways to reset to the router's factory defaults:

  1) Use the **Factory Defaults** function on **System Tools** -> **Factory Defaults** page in the router's Web-based Utility.
  2) Use the Factory Default Reset button: Press the Reset button for five seconds and then wait for the router to reboot.
- **Wireless antenna:** To receive and transmit the wireless data.

Chapter 2. Connecting the Router

2.1 System Requirements

- Broadband Internet Access Service (DSL/Cable/Ethernet)
- One DSL/Cable Modem that has an RJ45 connector (which is not necessary if the router is connected directly to the Ethernet.)
- PCs with a working Ethernet Adapter and an Ethernet cable with RJ45 connectors
- TCP/IP protocol on each PC
- Web browser, such as Microsoft Internet Explorer 5.0 , Netscape Navigator 6.0 or above

2.2 Installation Environment Requirements

- Place the router in a well ventilated place far from any heater or heating vent
- Avoid direct irradiation of any strong light (such as sunlight)
- Keep at least 2 inches (5 cm) of clear space around the router
- Operating Temperature: 0℃~40℃ (32℉~104℉)
- Operating Humidity: 10%~90%RH, Non-condensing

2.3 Connecting the Router

Before installing the router, make sure your PC is connected to the Internet through the 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.

1. Power off your PC, Cable/DSL Modem, and the router.
2. Locate an optimum location for the router. The best place is usually at the center of your wireless network. The place must accord with the Installation Environment Requirements.
3. Adjust the direction of the antenna. Normally, upright is a good direction.
4. Connect the PC(s) and each Switch/Hub in your LAN to the LAN Ports on the router, shown in Figure 2-1. (If you have the wireless NIC and want to use the wireless function, you can skip this step.)

5. Connect the DSL/Cable Modem to the WAN port on the router, shown in Figure 2-1.

6. Connect the DC power adapter to the DC power socket on the router, and the other end into an electrical outlet. The router will start to work automatically.

7. Power on your PC and Cable/DSL Modem.

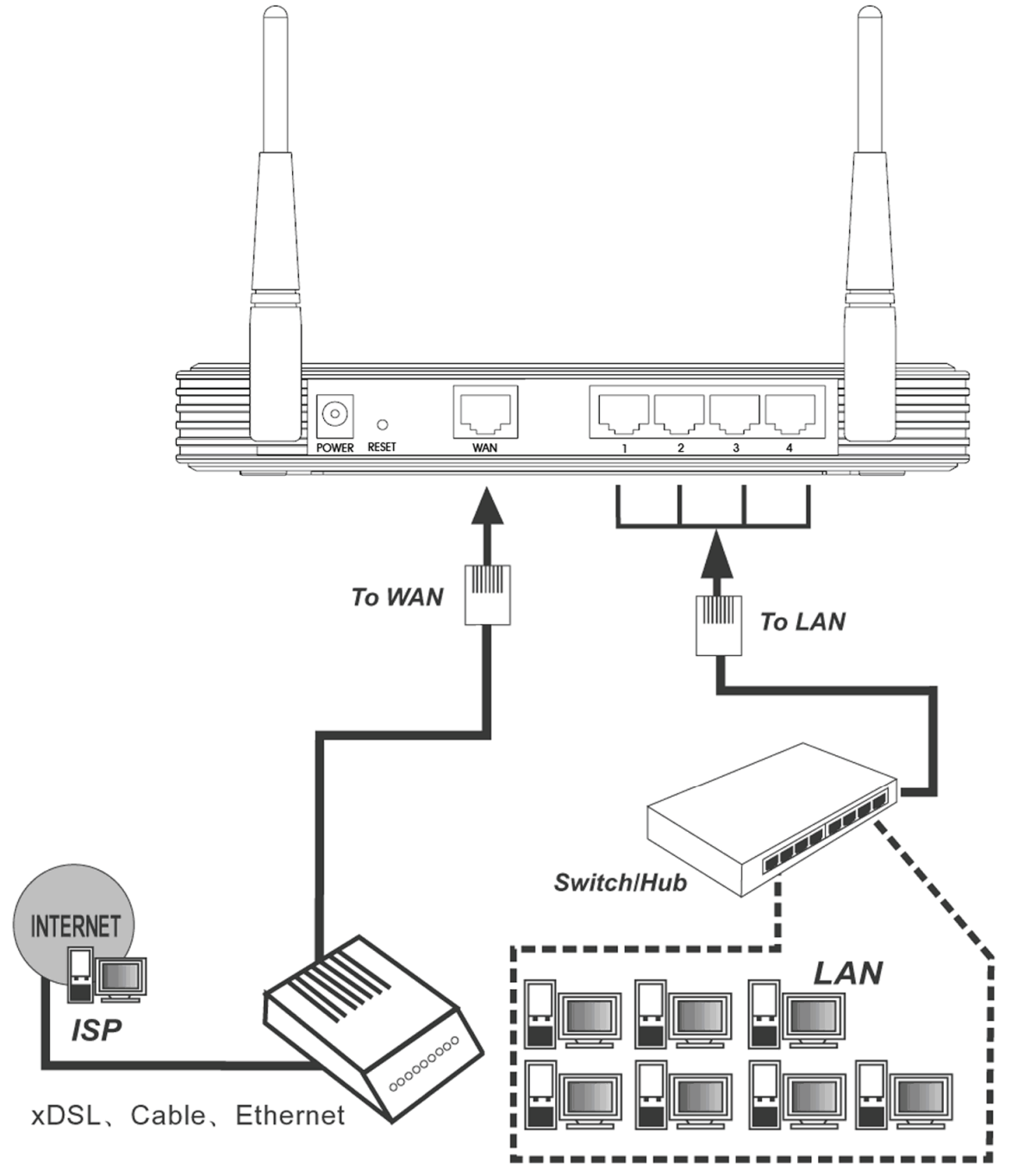


Figure 2-1 Hardware Installation of the TL-WR841ND Wireless N Router

Chapter 3. Quick Installation Guide

This chapter will show you how to configure the basic functions of your TL-WR841ND Wireless N Router using **Quick Setup Wizard** within minutes.

3.1 TCP/IP configuration

The default IP address of the TL-WR841ND Wireless N Router is 192.168.1.1. And the default Subnet Mask is 255.255.255.0. These values can be changed as you desire. In this guide, we use all the default values for description.

Connect the local PC to the LAN ports of the router. And then you can configure the IP address for your PC in the following two ways.

- Configure the IP address manually

  1) Set up the TCP/IP Protocol for your PC. If you need instructions as to how to do this, please refer to Appendix B: "Configuring the PC."

  2) Configure the network parameters. The IP address is 192.168.1.xxx ("xxx" is any number from 2 to 254), Subnet Mask is 255.255.255.0, and Gateway is 192.168.1.1 (The router's default IP address)

- Obtain an IP address automatically

  1) Set up the TCP/IP Protocol in "**Obtain an IP address automatically**" mode on your PC. If you need instructions as to how to do this, please refer to Appendix B: "Configuring the PC."

  2) Reboot the PC and the router. Then the built-in DHCP server will assign IP address for the PC.

Now, you can run the Ping command in the **command prompt** to verify the network connection between your PC and the router. The following example is in Windows 2000 OS.

Open a command prompt, and type *ping 192.168.1.1*, and then press **Enter**.

- If the result displayed is similar to the Figure 3-1, it means the connection between your PC and the router has been established well.

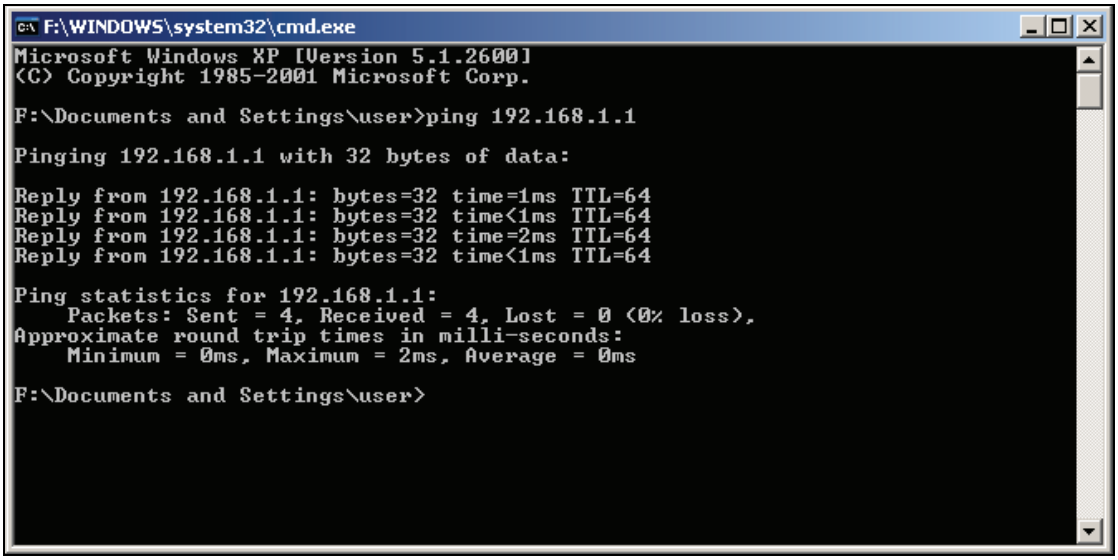


Figure 3-1 Success result of Ping command

- If the result displayed is similar to the Figure 3-2, it means the connection between your PC and the router is failed.

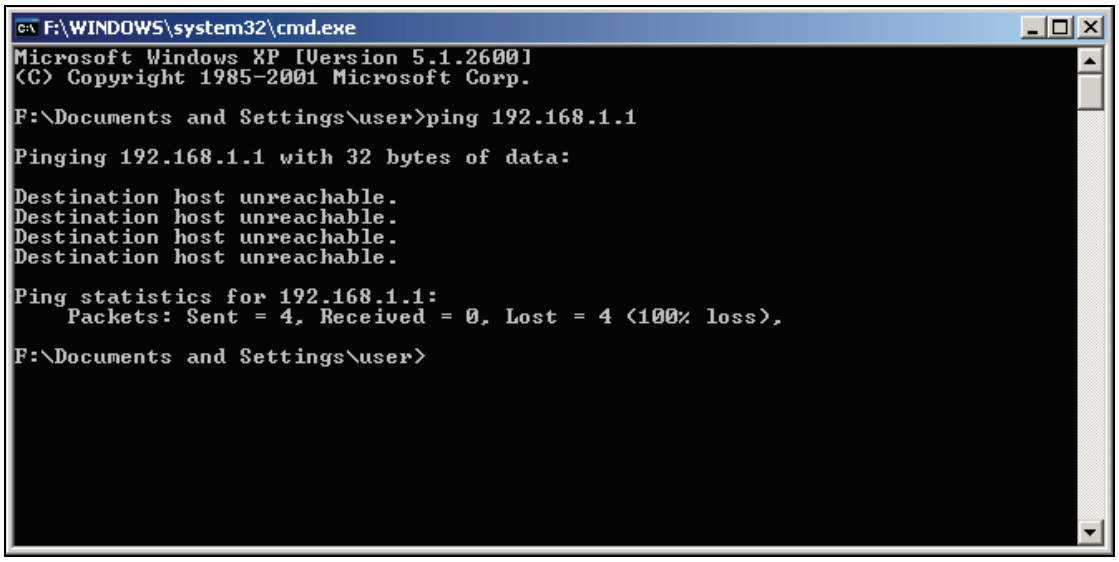


Figure 3-2 Failure result of Ping command

Please check the connection following these steps:

1. Is the connection between your PC and the router correct?

Note:

The 1/2/3/4 LEDs of LAN ports which you link to on the router and LEDs on your PC's adapter should be lit.

2. Is the TCP/IP configuration for your PC correct?

Note:

If the router's IP address is 192.168.1.1, your PC's IP address must be within the range of 192.168.1.2 ~ 192.168.1.254.

3.2 Quick Installation Guide

With a Web-based (Internet Explorer or Netscape® Navigator) utility, it is easy to configure and manage the TL-WR841ND Wireless N Router. The Web-based utility can be used on any Windows, Macintosh or UNIX OS with a Web browser.

1. To access the configuration utility, open a web-browser and type in the default address http://192.168.1.1 in the address field of the browser.

Figure 3-3 Login the router

After a moment, a login window will appear, similar to the Figure 3-4. Enter **admin** for the User Name and Password, both in lower case letters. Then click the **OK** button or press the **Enter** key.

Figure 3-4 Login Windows

☞ **Note:**

If the above screen does not pop-up, it means that your Web-browser has been set to a proxy. Go to Tools menu>Internet Options>Connections>LAN Settings, in the screen that appears, cancel the Using Proxy checkbox, and click OK to finish it.

2. After successfully login, you can click the **Quick Setup** to quickly configure your router.

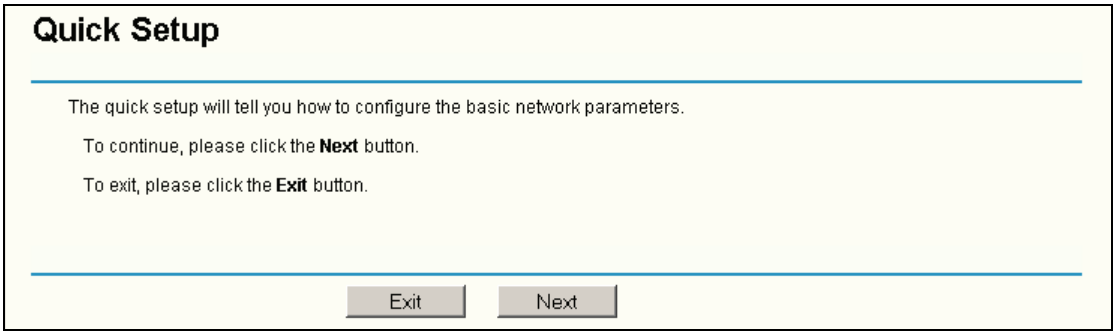


Figure 3-5 Quick Setup

3. Click **Next**, and then **Choose WAN Connection Type** page will appear, shown in Figure 3-6.

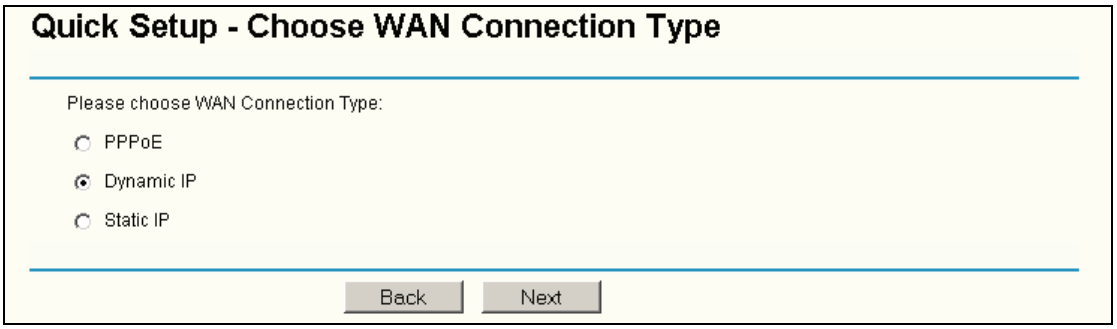


Figure 3-6 Choose WAN Connection Type

The router supports three popular ways to connect to Internet. Please select one compatible with your ISP. Click **Next** to enter the necessary network parameters.

a) If you are provided the ADSL Dial-up service, please choose "**PPPoE**"(Point-to-Point Protocol over Ethernet), and you will see this page shown in Figure 3-7:

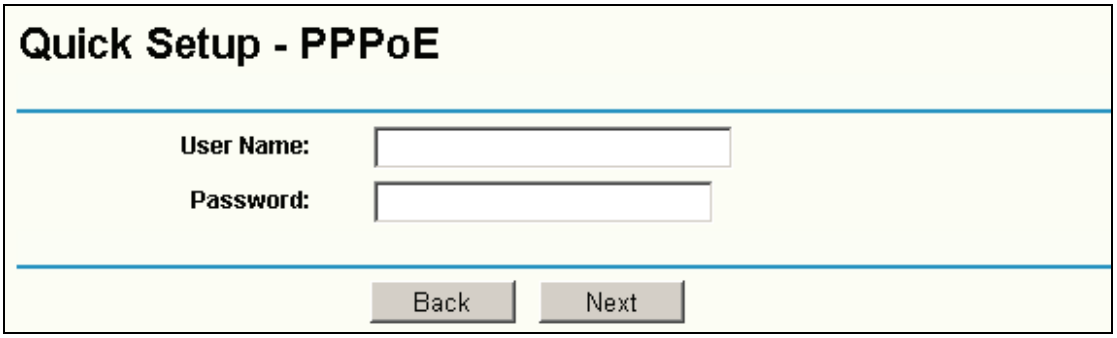


Figure 3-7 Quick Setup - PPPoE

- **User Name and Password -** Enter the **User Name** and **Password** provided by your ISP. These fields are case sensitive. If you have difficulty with this process, please contact your ISP.

b) If the Router connects to a DHCP server, or the ISP supplies you with DHCP connection, please choose "Dynamic IP", the router will automatically receive the IP parameters from your ISP with no need to enter any parameters.

c) If the IP parameters have been provided by your ISP, please choose "Static IP", and then the Static IP settings page will appear, shown in Figure 3-8

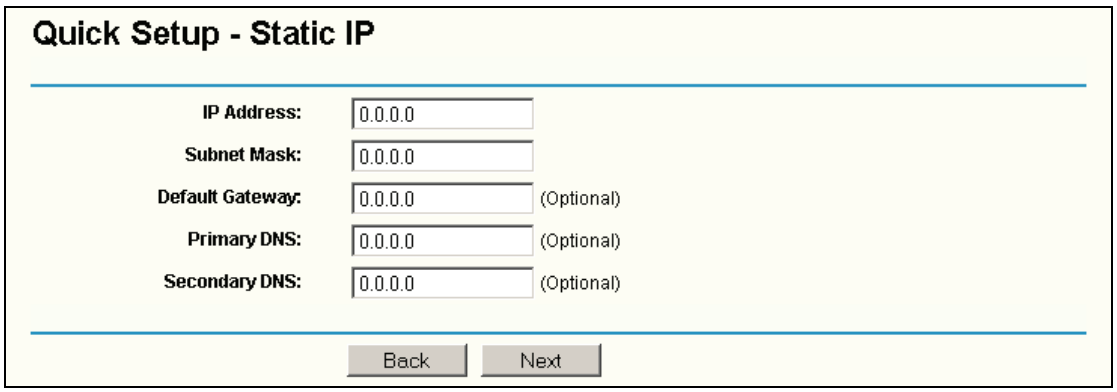


Figure 3-8 Quick Setup - Static IP

- **IP Address -** This is the WAN IP address as seen by external users on the Internet (including your ISP). Enter the IP address into the field.
- **Subnet Mask -** The Subnet Mask is used for the WAN IP address, it is usually 255.255.255.0
- **Default Gateway -** Enter the gateway IP address into the box if required.
- **Primary DNS -** Enter the DNS Server IP address into the box if required.
- **Secondary DNS -** If your ISP provides another DNS server, enter it into this field.

4. Click **Next** to continue, the Wireless settings page will appear, shown in Figure 3-9.

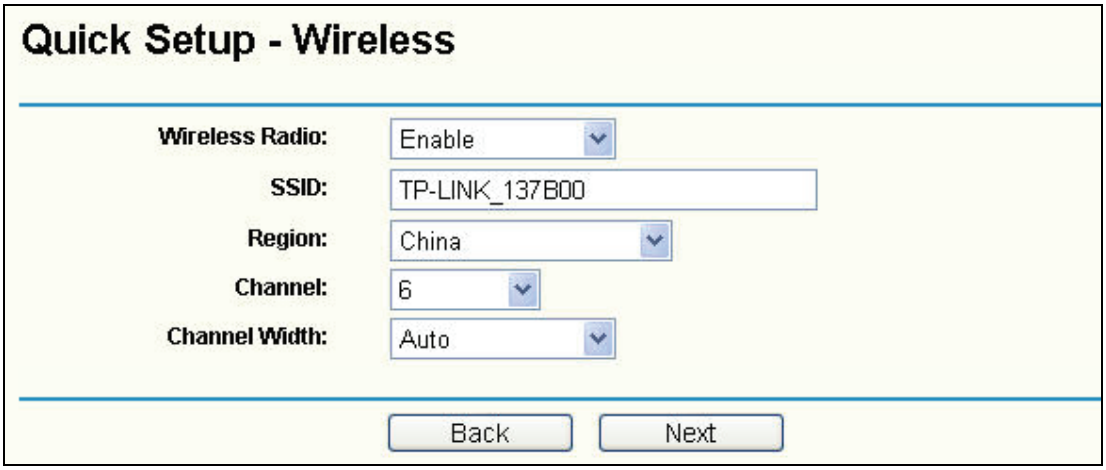


Figure 3-9 Quick Setup – Wireless

- **Wireless Radio -** Enable or disable the wireless radio choosing from the pull-down list.
- **SSID -** Enter a value of up to 32 characters. The same name of SSID (Service Set Identification) must be assigned to all wireless devices in your network. Considering your wireless network security, the default SSID is set to be TP-LINK_xxxxxx (xxxxxx indicates the last unique six numbers of each Router's MAC address). This value is case-sensitive. For example, *TP-LINK* is NOT the same as *tp-link*.

- **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.
- **Channel -** This field determines which operating frequency will be used. The default channel is set to 6. It is not necessary to change the wireless channel unless you notice interference problems with another nearby access point
- **Channel width -** Select any channel width from the pull-down list. The default setting is automatic, which can adjust the channel width for your clients automatically.

These settings are only for basic wireless parameters. For advanced settings, please refer to Section 4.5: "Wireless."

5. Click the **Next** button. You will then see the Finish page:

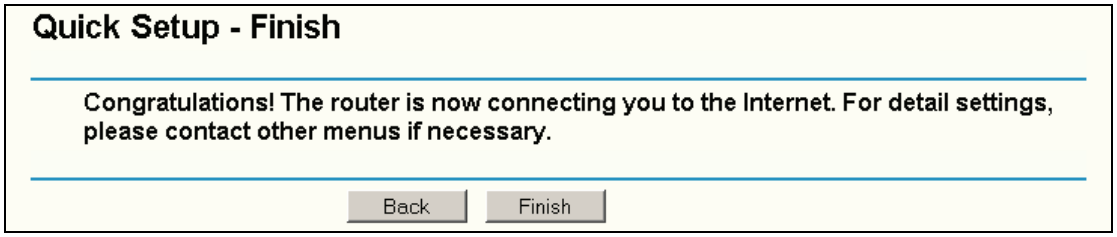


Figure 3-10 Quick Setup - Finish

After finishing all configurations of basic network parameters, please click **Finish** button to exit this **Quick Setup**.

Chapter 4. Configuring the Router

This chapter will show each Web page's key functions and the configuration way.

4.1 Login

After your successful login, you will see the eleven main menus on the left of the Web-based utility. On the right, there are the corresponding explanations and instructions.

The detailed explanations for each Web page's key function are listed below.

4.2 Status

The Status page provides the current status information about the router. All information is read-only.

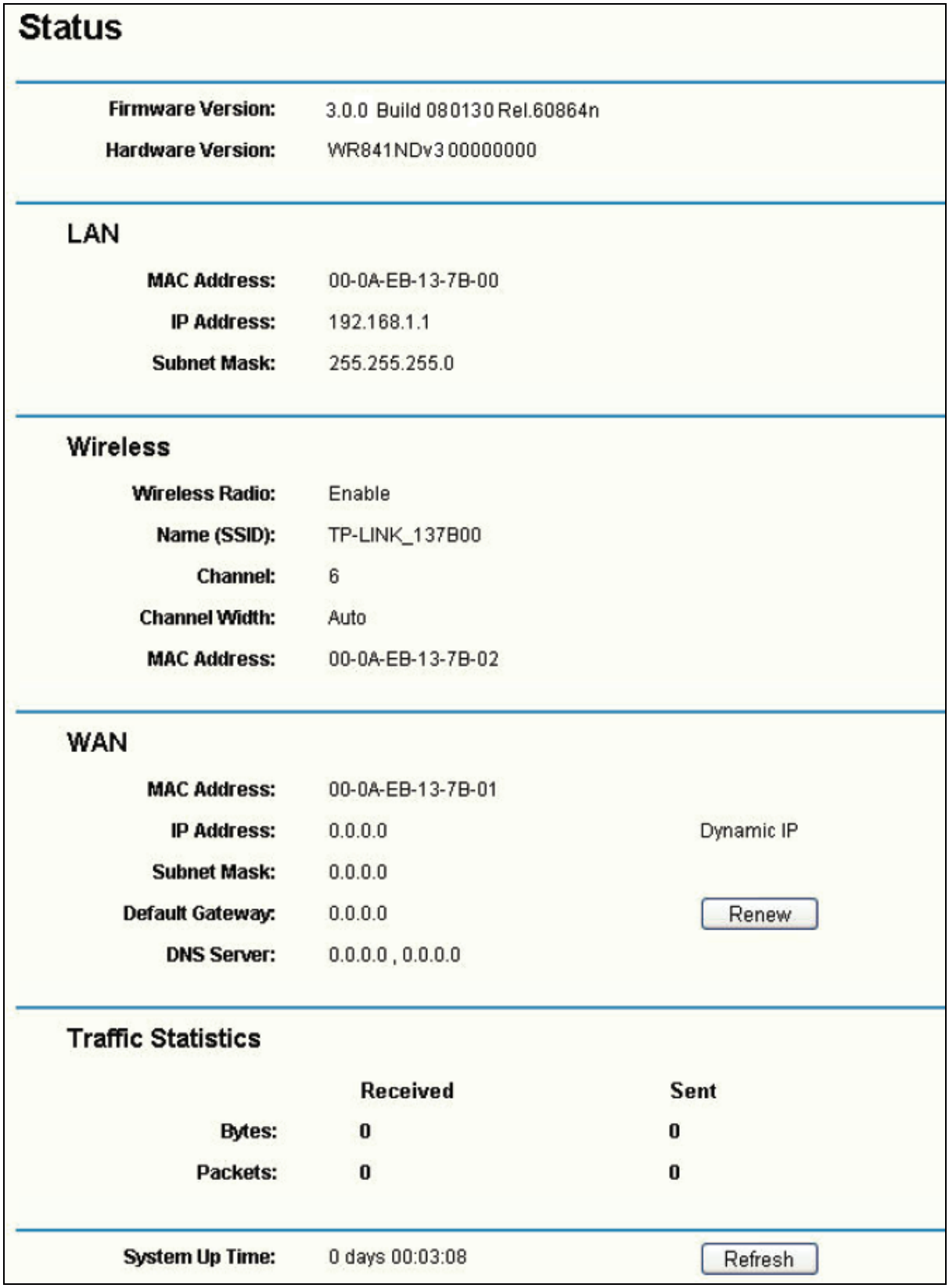


Figure 4-1 Router Status

4.3 Quick Setup

Please refer to Section 3.2: "Quick Installation Guide."

4.4 QSS

This section will guide you add a new wireless device to an existing network quickly by **QSS (Quick Secure Setup)** function.

a). Choose menu "**QSS**", you will see the next screen (shown in Figure 4-2).

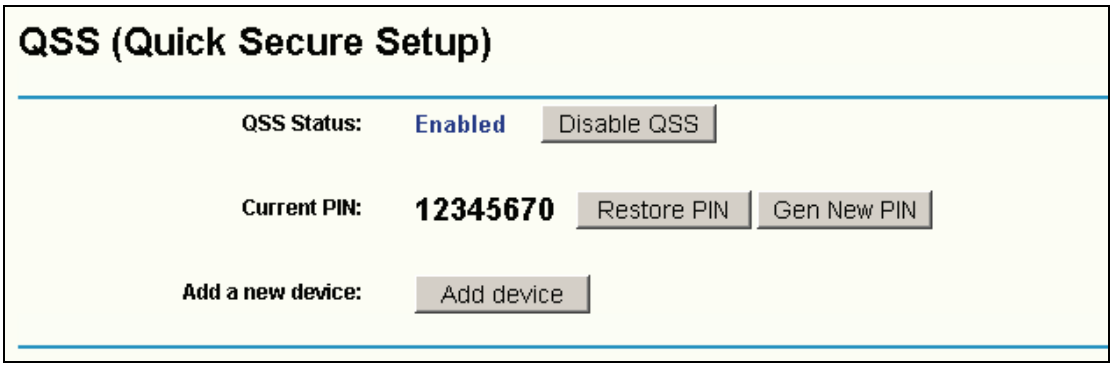


Figure 4-2 QSS

- **QSS Status -** Enable or disable the QSS function here.
- **Current PIN -** The current value of the router's PIN displayed here. The default PIN of the router can be found in the label or User Guide.
- **Restore PIN -** Restore the PIN of the router to its default.
- **Gen New PIN -** Click this button, and then you can get a new random value for the router's PIN. You can ensure the network security by generating a new PIN.
- **Add device -** You can add the new device to the existing network manually by clicking this button.

b). To add a new device:

If the wireless adapter supports Wi-Fi Protected Setup (WPS), you can establish a wireless connection between wireless adapter and router using either Push Button Configuration (PBC) method or PIN method.

☞ **Note:**

To build a successful connection by QSS, you should also do the corresponding configuration of the new device for QSS function meanwhile.

For the configuration of the new device, here takes the Wireless Adapter of our company for example.

I. By PBC

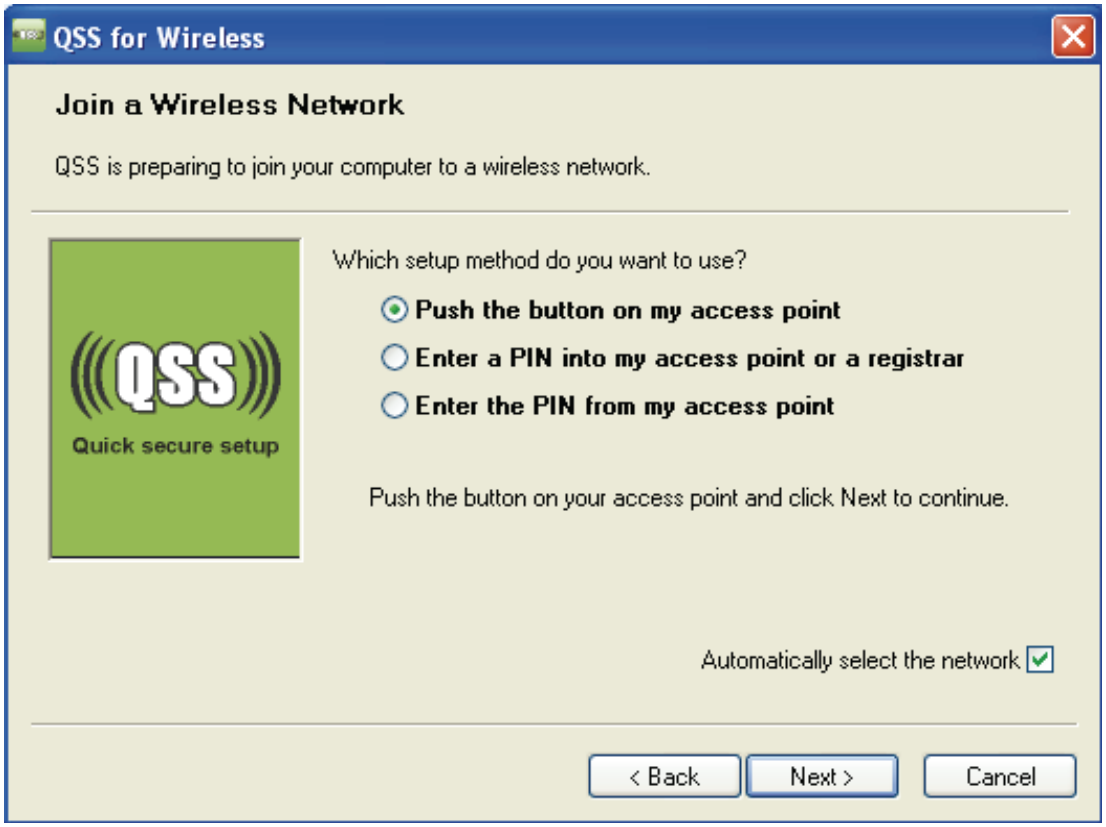
If the wireless adapter supports Wi-Fi Protected Setup and the Push Button Configuration (PBC)

method, you can add it to the network by PBC with the following two methods.

Method One:

Step 1: Press the QSS button on the front panel of the router.

Step 2: For the configuration of the wireless adapter, please choose **Push the button on my access point** in the configuration utility of the QSS as below, and click **Next**.



The QSS Configuration Screen of Wireless Adapter

Method Two:

Step 1: Keep the default QSS Status as **Enabled** and click the **Add device** button in Figure 4-2, then the following screen will appear.

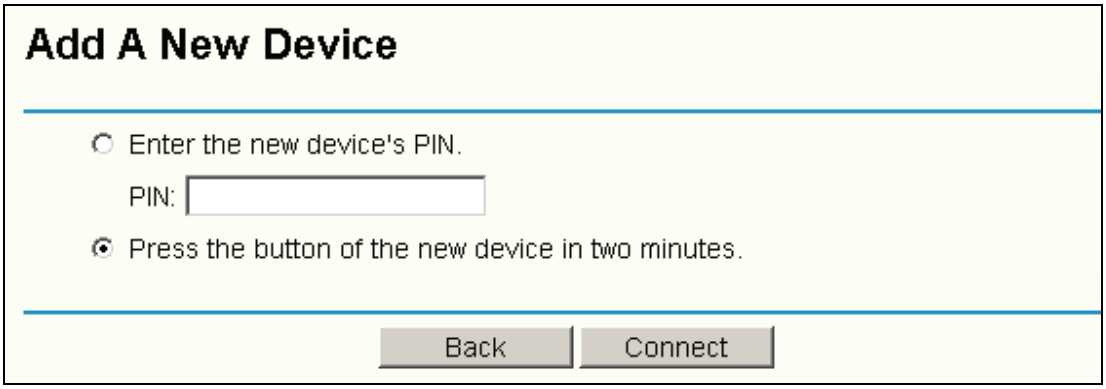
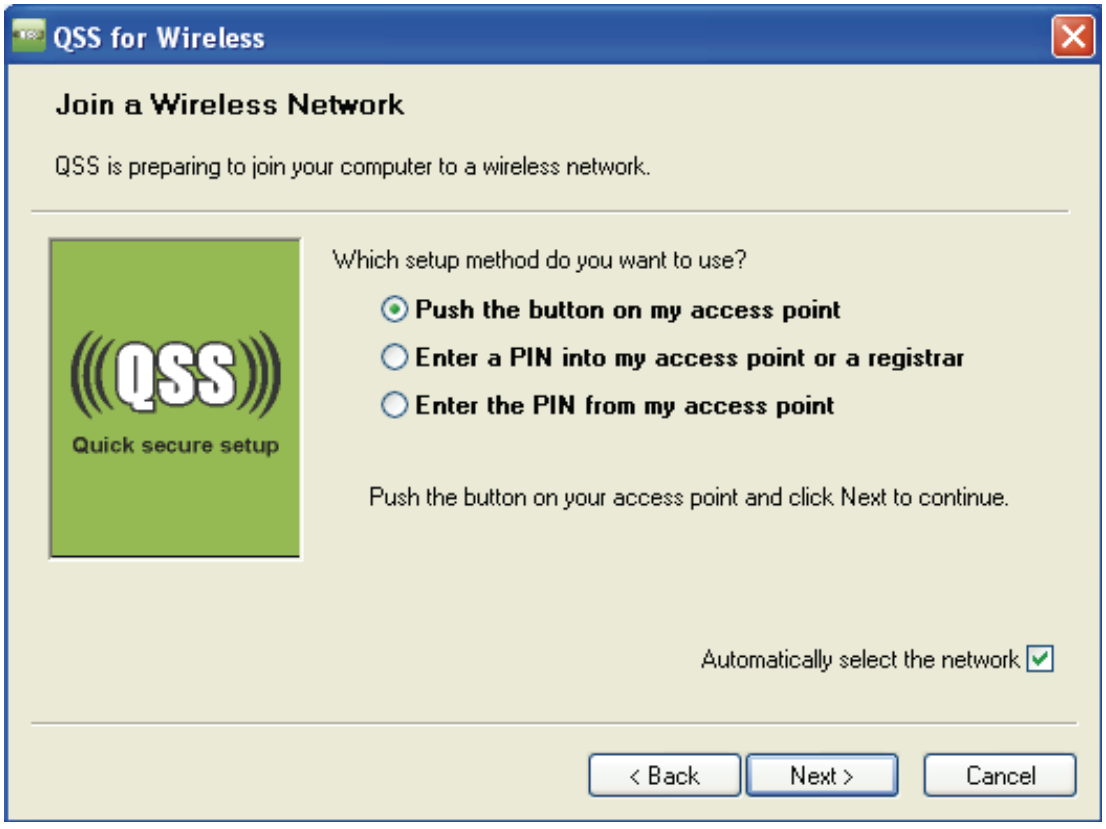


Figure 4-3 Add A New Device

Step 2: Choose **Press the button of the new device in two minutes** and click **Connect**..

Step 3: For the configuration of the wireless adapter, please choose **Push the button on my access point** in the configuration utility of the QSS as below, and click **Next**.



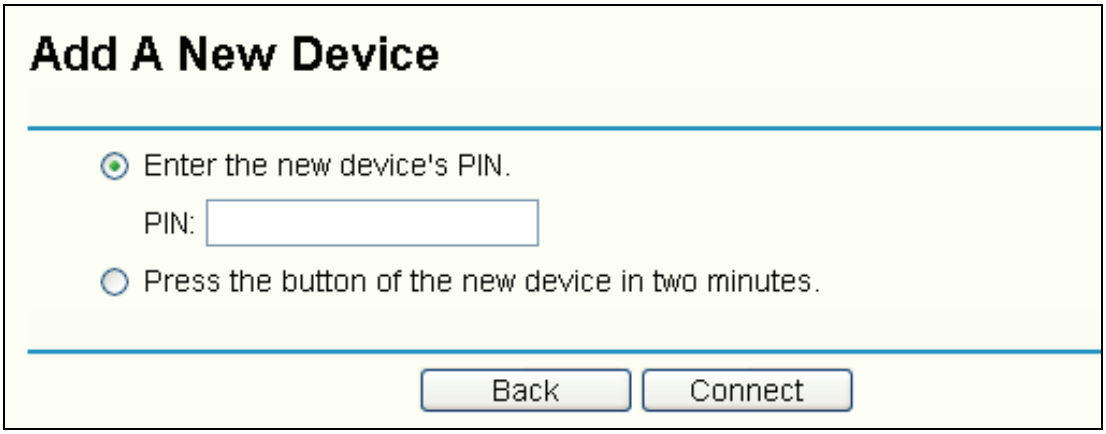
The QSS Configuration Screen of Wireless Adapter

II. By PIN

If the new device supports Wi-Fi Protected Setup and the PIN method, you can add it to the network by PIN with the following two methods.

Method One: Enter the PIN into my Router

Step 1: Keep the default QSS Status as **Enabled** and click the **Add device** button in Figure 4-2, then the following screen will appear.

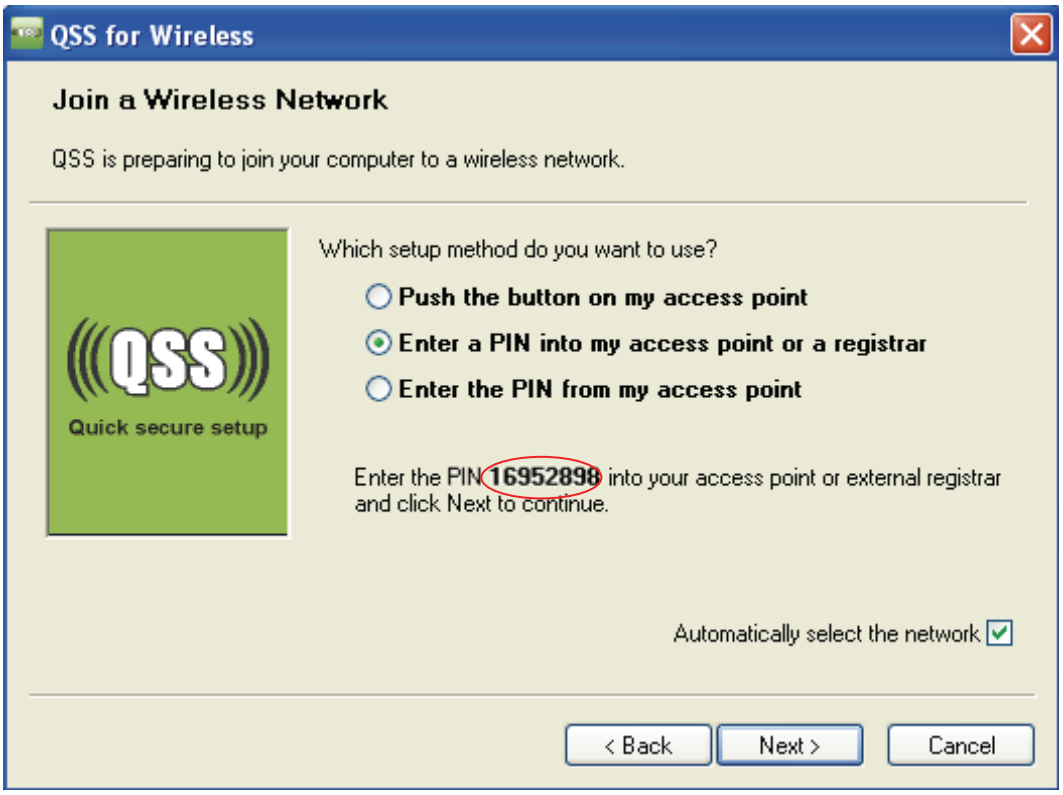


Step 2: Choose **Enter the new device's PIN** and enter the PIN code of the wireless adapter in the field behind **PIN** in the above figure. Then click **Connect.**

☞ **Note:**

The PIN code of the adapter is always displayed on the QSS configuration screen

Step 3: For the configuration of the wireless adapter, please choose **Enter a PIN into my access point or a registrar** in the configuration utility of the QSS as below, and click **Next.**



The QSS Configuration Screen of Wireless Adapter

☞ **Note:**

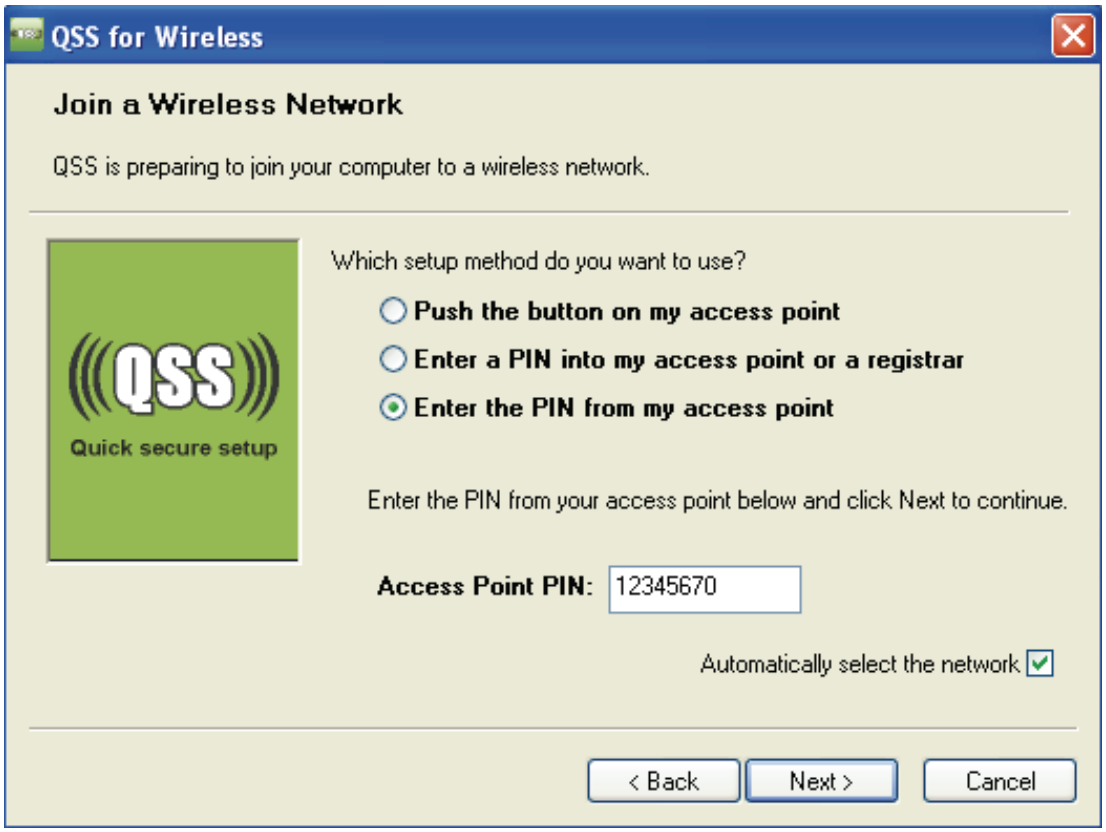
In this example, the default PIN code of this adapter is 16952898 as the above figure shown.

Method Two: Enter the PIN from my Router

Step 1: Get the Current PIN code of the Router in Figure 4-2 (each router has its unique PIN

code. Here takes the PIN code 12345670 of this router for example).

Step 2: For the configuration of the wireless adapter, please choose **Enter a PIN from my access point** in the configuration utility of the QSS as below, and enter the PIN code of the Router into the field behind **Access Point PIN**. Then click **Next.**

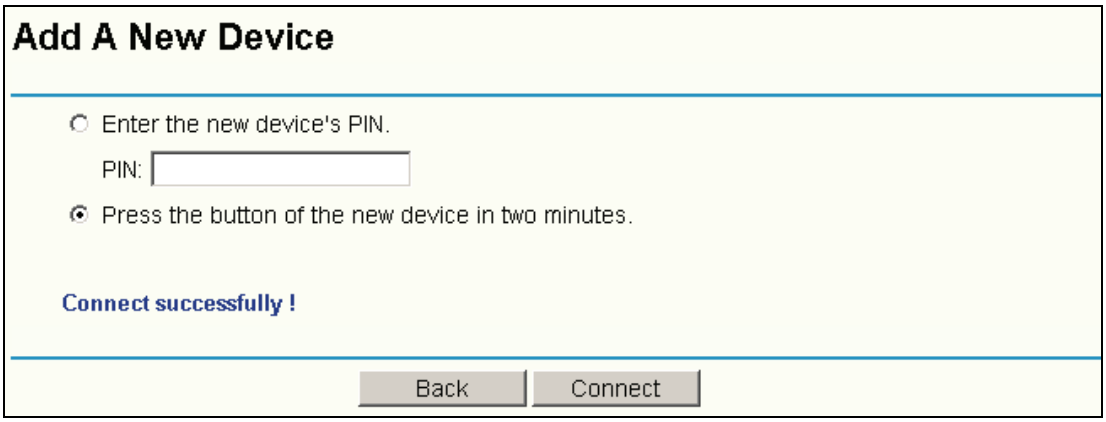


The QSS Configuration Screen of Wireless Adapter

Note:

The default PIN code of the Router can be found in its label or the QSS configuration screen as Figure 4-2.

c). You will see the following screen when the new device successfully connected to the network.



Note:

a. The status LED on the router will light green all the time if the device has been successfully added to the network.

b. The QSS function cannot be configured if the Wireless Function of the router is disabled. Please make sure the Wireless Function is enabled before configuring the QSS.

4.5 Network

Figure 4-4 the Network menu

There are three submenus under the Network menu (shown in Figure 4-4): **LAN**, **WAN** and **MAC Clone.** Click any of them, and you will be able to configure the corresponding function.

4.5.1 LAN

Choose menu "**Network→LAN**", you can configure the IP parameters of the LAN on the screen as below.

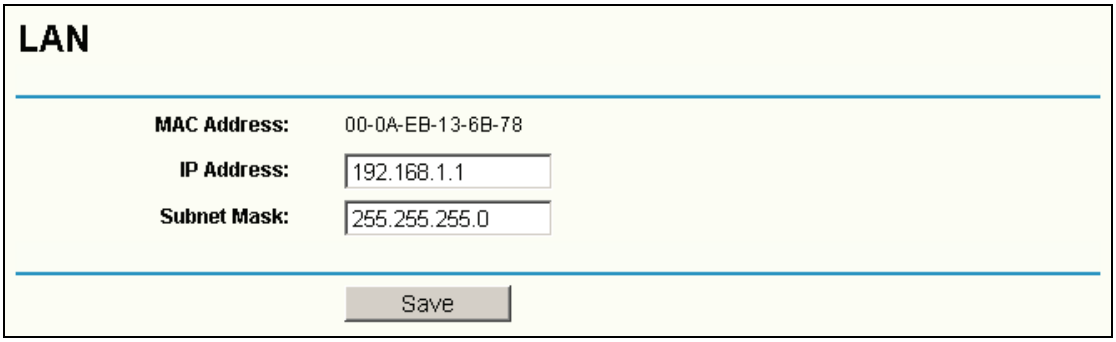


Figure 4-5 LAN

- **MAC Address -** The physical address of the router, as seen from the LAN. The value can't be changed.
- **IP Address -** Enter the IP address of your router or reset it 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 you change the IP Address of LAN, you must use the new IP Address to login the router.

b. If the new LAN IP Address you set is not in the same subnet, the IP Address pool of the

DHCP server will change accordingly at the same time，while the Virtual Server and DMZ Host will not take effect until they are re-configured.

4.5.2 WAN

Choose menu "**Network→WAN**", you can configure the IP parameters of the WAN on the screen below.

1. If your ISP provides the DHCP service, please choose **Dynamic IP** type, and the router will automatically get IP parameters from your ISP. You can see the page as follows (Figure 4-6):

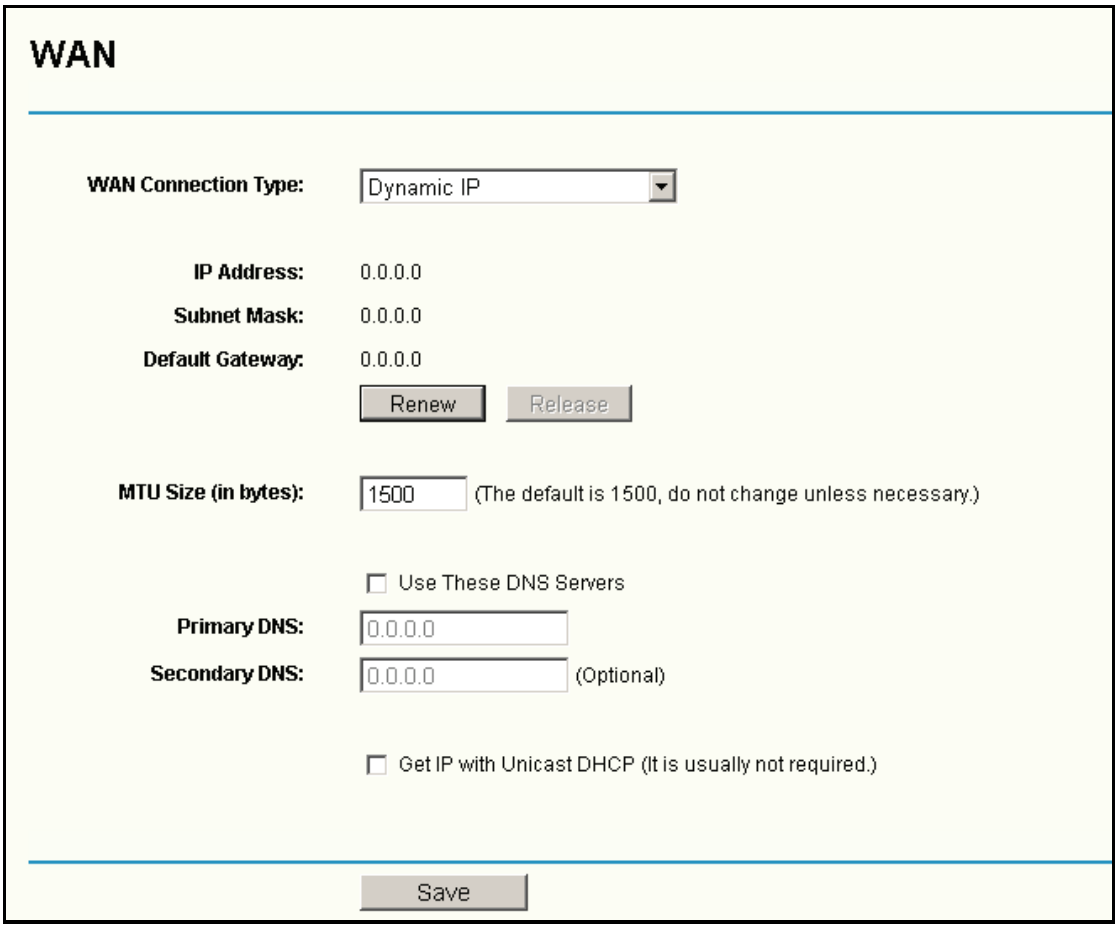


Figure 4-6 WAN – Dynamic IP

This page displays the WAN IP parameters assigned dynamically by your ISP, including IP address, Subnet Mask, Default Gateway, etc. Click the **Renew** button to renew the IP parameters from your ISP. Click the **Release** button to release the IP parameters.

- **MTU Size** - The normal **MTU** (Maximum Transmission Unit) value for most Ethernet networks is 1500 Bytes. It is not recommended that you change the default **MTU Size** unless required by your ISP.
- **Use These DNS Servers -** If your ISP gives you one or two DNS addresses, select **Use These DNS Servers** and enter the primary and secondary addresses into the correct fields. Otherwise, the DNS servers will be assigned dynamically from your ISP.

Note:

If you find error when you go to a Web site after entering the DNS addresses, it is likely that your DNS servers are set up improperly. You should contact your ISP to get DNS server addresses.

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

2. If you choose **Static IP,** you should have the fixed IP Parameters given by your ISP. The Static IP settings page will appear, shown in Figure 4-7.

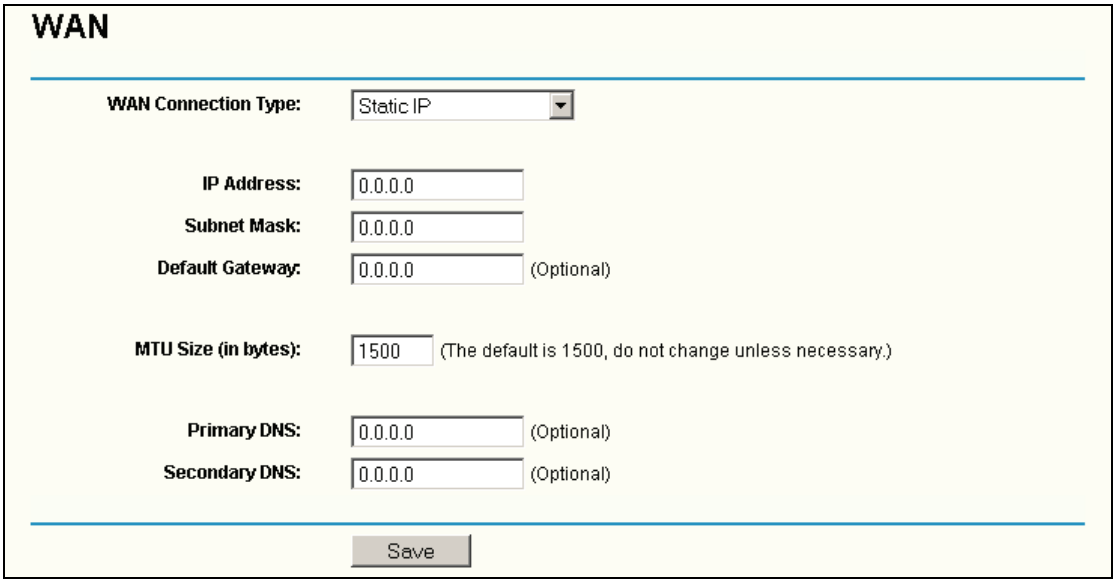


Figure 4-7 WAN - Static IP

- **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, usually is 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. It is not recommended that you change the default **MTU Size** unless required by your ISP.
- **Primary/Secondary DNS -** (Optional) Enter one or two DNS addresses in dotted-decimal notation provided by your ISP.

3. If you choose **PPPoE,** you should enter the following parameters (Figure 4-8):

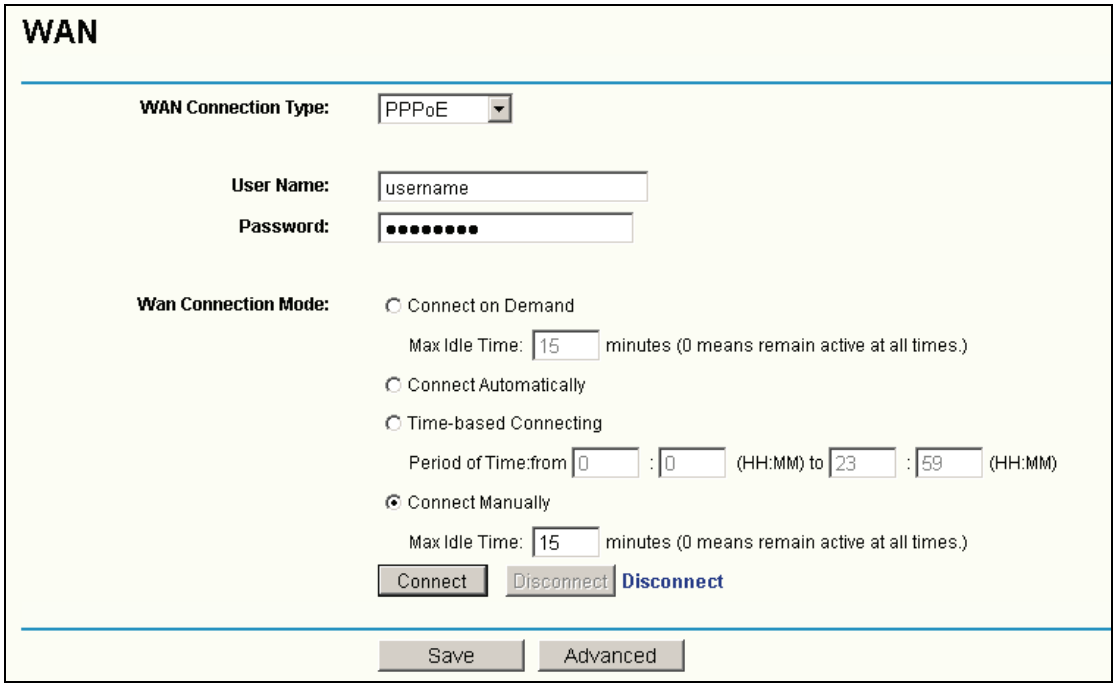


Figure 4-8 WAN - PPPoE

- **User Name/Password -** Enter the User Name and Password provided by your ISP. These fields are case-sensitive.
- **Connect on Demand -** In this mode, the Internet connection can be terminated automatically after a specified inactivity period (**Max Idle Time**) and **be** re-established when you attempt to access the Internet again. If you want your Internet connection keeps active all the time, please enter "0" in the **Max Idle Time** field. Otherwise, enter the number of minutes you want to have elapsed before your Internet access disconnects.
- **Connect Automatically -** The connection can be re-established automatically when it was down..
- **Time-based Connecting -** The connection will only be established in the period from the start time to the end time (both are in HH:MM format).

☞ **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 click the **Connect**/ **Disconnect** button to connect/disconnect immediately. This mode also supports the **Max Idle Time** function as **Connect on Demand** mode. The Internet connection can be disconnected automatically after a specified inactivity period and re-established when you attempt to access the Internet again.

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

If you want to do some advanced configurations, please click the **Advanced** button, and the page shown in Figure 4-9 will then appear:

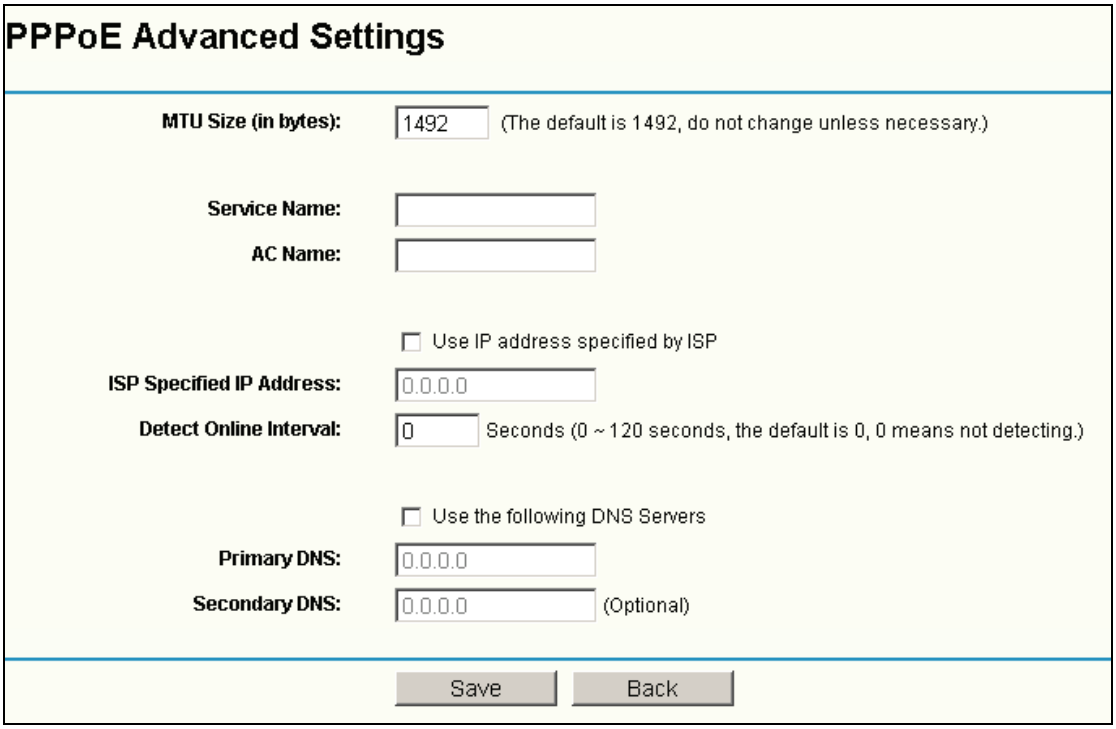


Figure 4-9 PPPoE Advanced Settings

- **MTU Size -** The default MTU size is "1492" bytes, which is usually fine. It is not recommended that you change the default **MTU Size** unless required by your ISP.
- **Service Name/AC Name -** The service name and AC (Access Concentrator) name, which should not be configured unless you are sure it is necessary for your ISP. In most cases, leaving these fields blank will work.
- **ISP Specified IP Address -** If your ISP does not automatically assign IP addresses to the router during login, please click "**Use IP address specified by ISP**" check box and enter the IP address provided by your ISP in dotted-decimal notation.
- **Detect Online Interval -** The router will detect Access Concentrator online at every interval. The default value is "0". You can input the value between "0"and "120". The value "0" means no detect.
- **DNS IP address -** If your ISP does not automatically assign DNS addresses to the router during login, please click "**Use the following DNS servers**" check box 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 the **Save** button to save your settings.

4.5.3 MAC Clone

Choose menu "**Network→MAC Clone**", you can configure the MAC address of the WAN on the screen below, Figure 4-10:

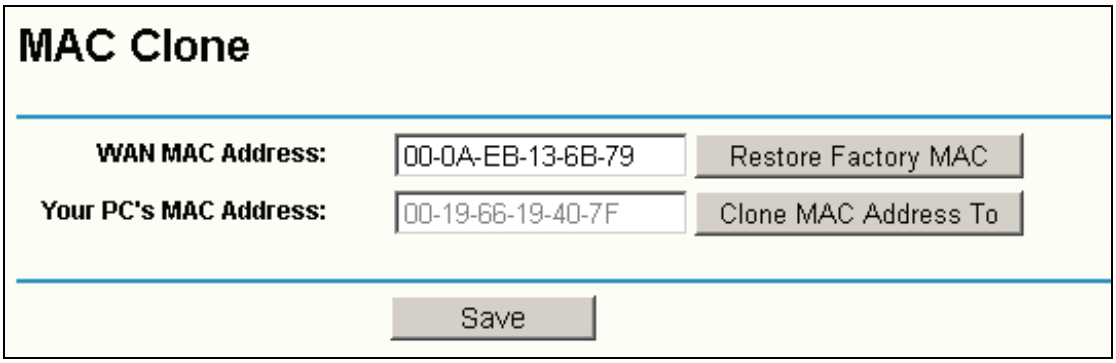


Figure 4-10 MAC Address Clone

Some ISPs require that you register the MAC Address of your adapter. Changes are rarely needed here.

- **WAN MAC Address -** This field displays the current MAC address of the WAN port. If your ISP requires you to register the MAC address, please enter the correct MAC address into this field in XX-XX-XX-XX-XX-XX format(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, you can click the **Clone MAC Address To** button and this MAC address will fill in the **WAN MAC Address** field.

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

Click the **Save** button to save your settings.

☞ **Note:**

Only the PC on your LAN can use the **MAC Address Clone** function.

4.6 Wireless

Figure 4-11 Wireless menu

There are four submenus under the Wireless menu (shown in Figure 4-11): **Wireless Settings**, **Wireless Security, Wireless MAC Filtering, Wireless Advanced** and **Wireless Statistics.** Click

any of them, you will be able to configure the corresponding function.

4.6.1 Wireless Settings

Choose menu "**Wireless→Wireless Setting**", you can configure the basic settings for the wireless network on this page.

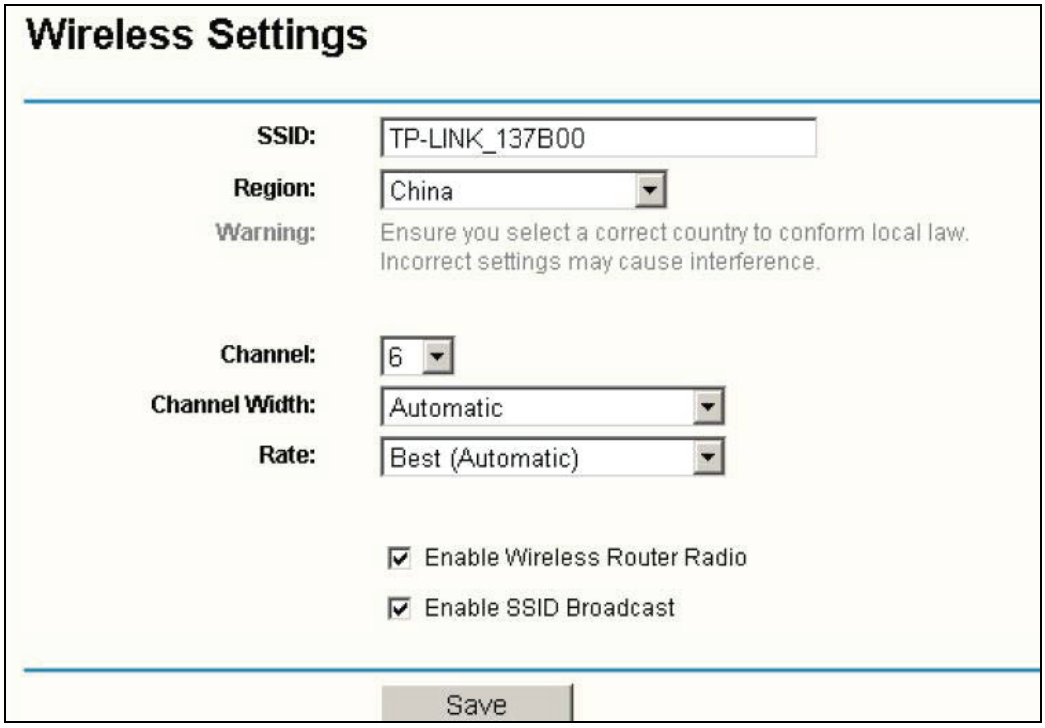
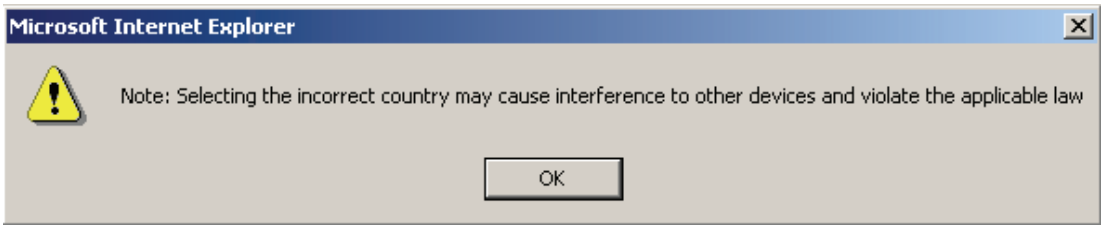


Figure 4-12 Wireless Settings

- **SSID -** Enter a value of up to 32 characters. The same name of SSID (Service Set Identification) must be assigned to all wireless devices in your network. Considering your wireless network security, the default SSID is set to be TP-LINK_xxxxxx (xxxxxx indicates the last unique six numbers of each Router's MAC address). This value is case-sensitive. For example, *TP-LINK* is NOT the same as *tp-link*.

- **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.

  When you select your local region from the pull-down list, Click the **Save** button**,** then the Note Dialog appears. Click OK.



Note Dialog

☞ **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. The default channel is set to 6. It is not necessary to change the wireless channel unless you notice interference problems with another nearby access point
- **Channel width -** Select any channel width from the pull-down list. The default setting is automatic, which can adjust the channel width for your clients automatically.
- **Rate-** Select the appropriate wireless network rate from the pull-down list.
- **Enable Wireless Router Radio -** The wireless radio of this Router can be enabled or disabled to allow wireless stations access.
- **Enable SSID Broadcast -** When wireless clients survey the local area for wireless networks to associate with, they will detect the SSID broadcast by the Router. If you select the **Enable SSID Broadcast** checkbox, the Wireless Router will broadcast its name (SSID) on the air.

4.6.2 Wireless Security

Choose menu "**Wireless→Wireless Security**", you can configure the security settings of your wireless network.

There are five wireless security modes supported by the Router: WEP (Wired Equivalent Privacy), WPA (Wi-Fi Protected Access), WPA2 (Wi-Fi Protected Access 2), WPA2-PSK (Pre-Shared Key), WPA-PSK (Pre-Shared Key).

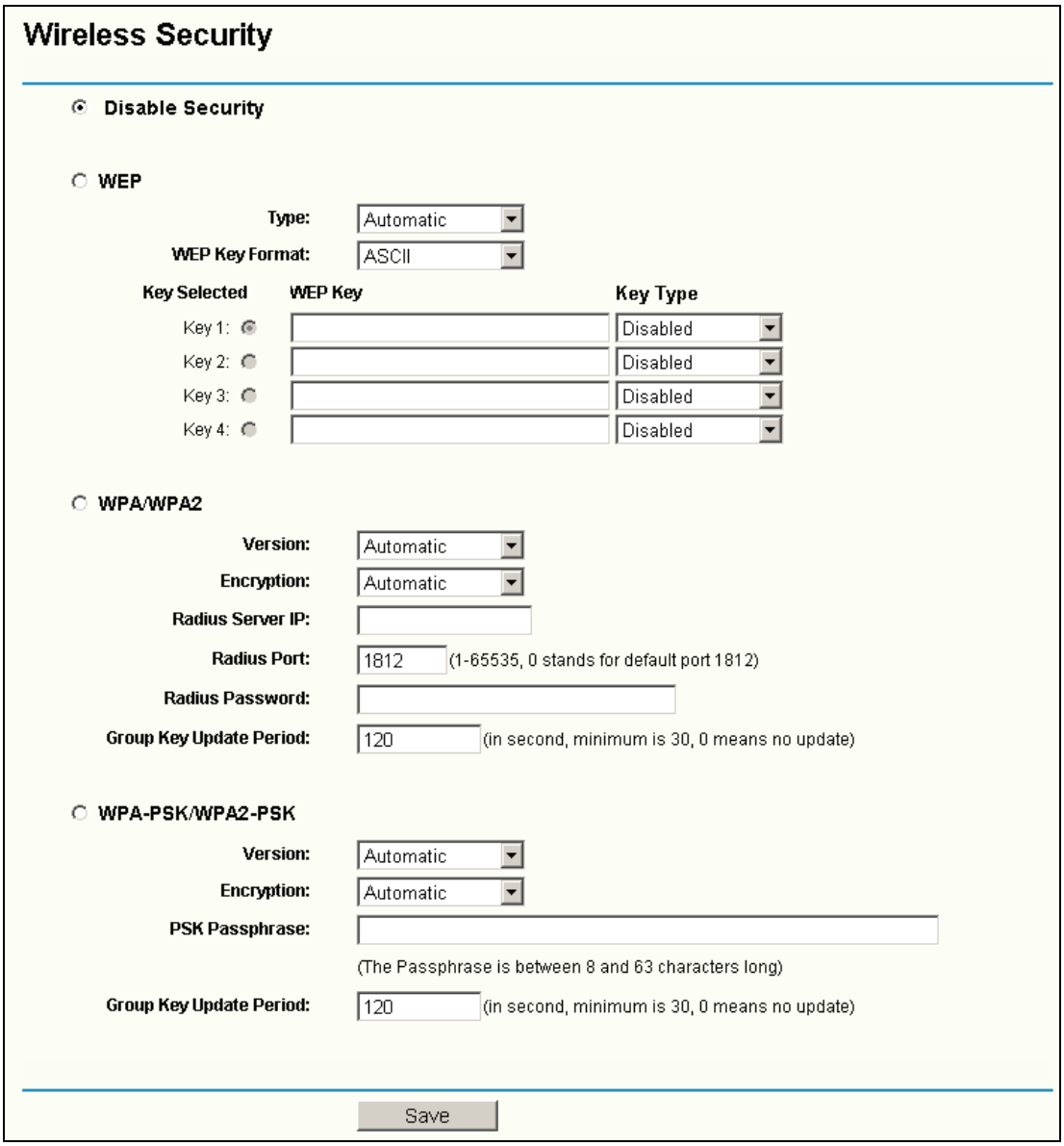


Figure 4-13

- **Disable Security** - If you do not want to use wireless security, select this check box, but it's recommended strongly to choose one of the following modes to enable security.
- **WEP -** It is based on the IEEE 802.11 standard.
  - **Type** - you can choose the type for the WEP security on the pull-down list. The default setting is **Automatic**, which can select **Shared Key** or **Open System** authentication type automatically based on the wireless station's capability and request.
  - **WEP Key Format** – **ASCII** and **Hexadecimal** formats are provided. **ASCII** 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 that you create. Make sure these values are 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 this WEP key entry is invalid.

64-bit - You can enter 10 hexadecimal digits (any combination of 0-9, a-f, A-F, zero key is not promoted) or 5 ASCII characters.

128-bit - You can enter 26 hexadecimal digits (any combination of 0-9, a-f, A-F, zero key is not promoted) or 13 ASCII characters.

152-bit - You can enter 32 hexadecimal digits (any combination of 0-9, a-f, A-F, zero key is not promoted) or 16 ASCII characters.

☞ **Note:**

If you do not set the key, the wireless security function is still disabled even if you have selected Shared Key as Authentication Type.

➢ **WPA /WPA2** - It's based on Radius Server.

- **Version -** you can choose the version of the WPA security on the pull-down list. The default setting is **Automatic**, which can select **WPA (**Wi-Fi Protected Access) or **WPA2 (**WPA version 2) automatically based on the wireless station's capability and request.
- **Encryption -** You can select either **Automatic**, or **TKIP** or **AES.**
- **Radius Server IP -** Enter the IP address of the Radius Server.
- **Radius Port -** Enter the port that radius service used.
- **Radius Password -** Enter the password for the Radius Server.
- **Group Key Update Period -** Specify the group key update interval in seconds. The value should be 30 or above. Enter 0 to disable the update.

➢ **WPA-PSK/WPA2-PSK**-It's the WPA/WPA2 authentication type based on pre-shared passphrase.

- **Version -** you can choose the version of the WPA-PSK security on the dropl-down list. The default setting is **Automatic**, which can select **WPA-PSK (**Pre-shared key of WPA) or **WPA2-PSK** (Pre-shared key of WPA) automatically based on the wireless station's capability and request.
- **Encryption -** When **WPA-PSK** or **WPA** is set as the Authentication Type, you can select either **Automatic**, or **TKIP** or **AES** as Encryption.

- **PSK Passphrase -** You can enter a Passphrase between 8 and 63 characters.
- **Group Key Update Period -** Specify the group key update interval in seconds. The value should be 30 or above. Enter 0 to disable the update.

Be sure to click the **Save** button to save your settings on this page.

4.6.3 Wireless MAC Filtering

Choose menu "**Wireless→MAC Filtering**", you can control the wireless access by configuring the MAC addresses Filtering function, shown in Figure 4-14.

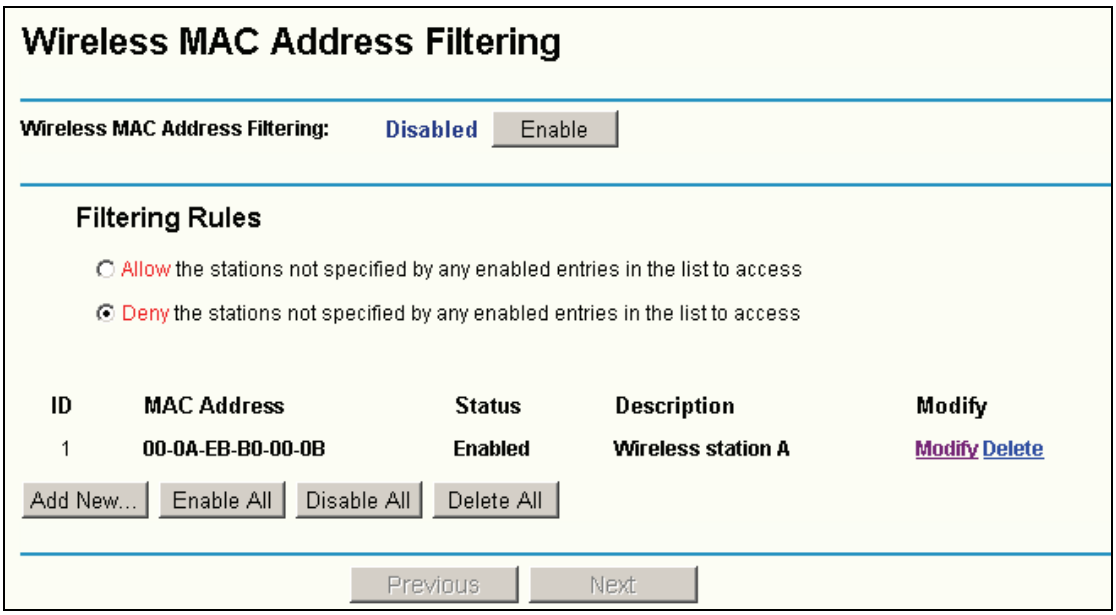


Figure 4-14 Wireless MAC address Filtering

To filter wireless users by MAC Address, click **Enable**. If you do not wish to filter users by MAC Address, select **Disable**.

- **MAC Address -** The wireless station's MAC address that you want to filter.
- **Status -** The status of this entry either **Enabled** or **Disabled**.
- **Description -** A simple description of the wireless station.

To Add a Wireless MAC Address filtering entry, click the **Add New…** button. The "**Add or Modify Wireless MAC Address Filtering entry"** page will appear, shown in Figure 4-15:

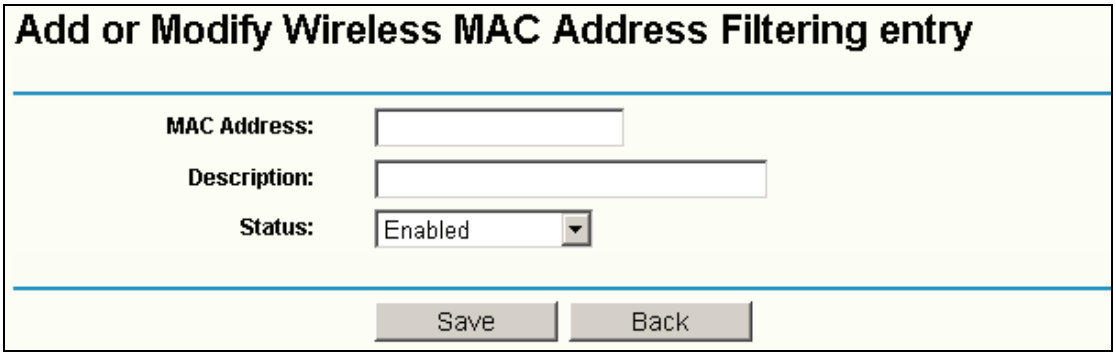


Figure 4-15 Add or Modify Wireless MAC Address Filtering entry

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: 00-0A-EB-B0-00-0B.
2. Enter a simple description of the wireless station in the **Description** field. For example: Wireless station A.
3. **Status** - Select **Enabled** or **Disabled** for this entry on the **Status** pull-down list.
4. Click the **Save** button to save this entry.

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 the **Save** button.

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

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

Click the **Delete All** button to delete all entries

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

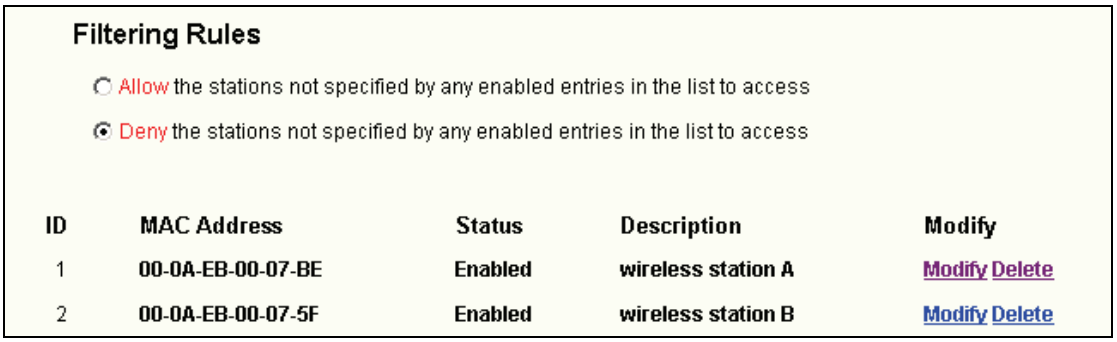
For example: If you desire that the wireless station A with MAC address 00-0A-EB-00- 07-BE and the wireless station B with MAC address 00-0A-EB- 00-07-5F are able to access the router, but all the other wireless stations cannot access the router, you can configure the **Wireless MAC Address Filtering** list by following these steps:

1. Click the **Enable** button to enable this function.
2. Select the radio button: **Deny the stations not specified by any enabled entries in the list**

to access for **Filtering Rules.**

3. Delete all or disable all entries if there are any entries already.
4. Click the **Add New...** button and enter the MAC address 00-0A-EB-00-07-BE/00-0A-EB-00-07-5F in the **MAC Address** field, then enter wireless station A/B in the **Description** field, while select **Enabled** in the **Status** pull-down list. Finally, click the **Save** and the **Back** button.

   The filtering rules that configured should be similar to the following list:



4.6.4 Wireless Advanced

Choose menu "**Wireless→Wireless Advanced**", you can configure the advanced settings of your wireless network.

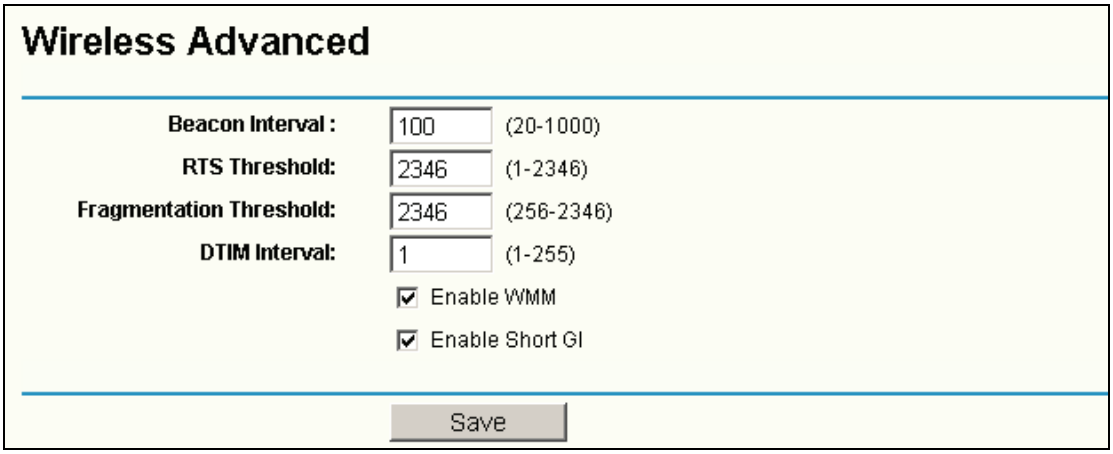


Figure 4-16 Wireless Advanced

- **Beacon Interval -** Enter a value between 20-1000 milliseconds for Beacon Interval here. The beacons are the packets sent by the router to synchronize a wireless network. Beacon Interval value determines the time interval of the beacons. The default value is 100.
- **RTS Threshold -** Here you can specify the RTS (Request to Send) Threshold. If the packet is larger than the specified RTS Threshold size, the router will send RTS frames to a particular receiving station and negotiate the sending of a data frame. The default value is 2346.

- **Fragmentation Threshold -** This value is the maximum size determining whether packets will be fragmented. Setting the Fragmentation Threshold too low may result in poor network performance since excessive packets. 2346 is the default setting and is recommended.
- **DTIM Interval -** This value determines the interval of the Delivery Traffic Indication Message (DTIM). A DTIM field is a countdown field informing clients of the next window for listening to broadcast and multicast messages. When the Router has buffered broadcast or multicast messages for associated clients, it sends the next DTIM with a DTIM Interval value. You can specify the value between 1-255 Beacon Intervals. The default value is 1, which indicates the DTIM Interval is the same as Beacon Interval.
- **Enable WMM - WMM** function can guarantee the packets with high- priority messages being transmitted preferentially. It is strongly recommended enabled.
- **Enable Short GI -** This function is recommended for it will increase the data capacity by reducing the guard interval time.

☞ **Note:**

If you are not familiar with the setting items in this page, it's strongly recommended to keep the provided default values, otherwise may result in lower wireless network performance.

4.6.5 Wireless Statistics

Choose menu "**Wireless→Wireless Statistics**", you can see the MAC Address, Current Status, Received Packets and Sent Packets for each connected wireless station.

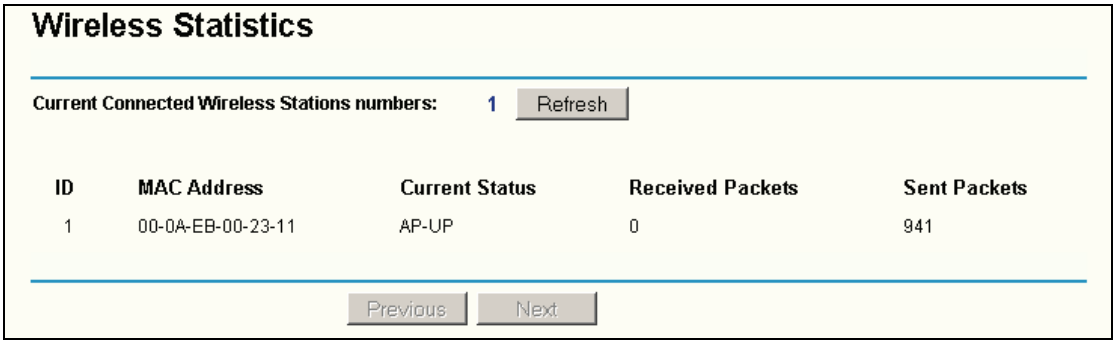


Figure 4-17 The router attached wireless stations

- **MAC Address -** The connected wireless station's MAC address
- **Current Status -** The connected wireless station's running status, one of **STA-AUTH / STA-ASSOC / STA-JOINED / WPA / WPA-PSK / WPA2 / WPA2-PSK / AP-UP / AP-DOWN / Disconnected**
- **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 on the **Refresh** button.

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

Note:

This page will be refreshed automatically every 5 seconds.

4.7 DHCP

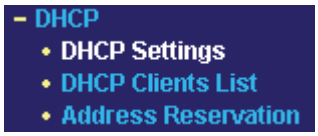


Figure 4-18 The DHCP menu

There are three submenus under the DHCP menu (shown in Figure 4-18): **DHCP Settings**, **DHCP Clients List** and **Address Reservation.** Click any of them, and you will be able to configure the corresponding function.

4.7.1 DHCP Settings

Choose menu "**DHCP→DHCP Settings**", you can configure the DHCP Server on the page (shown in Figure 4-19).The router is set up by default as a DHCP (Dynamic Host Configuration Protocol) server, which provides the TCP/IP configuration for all the PC(s) that are connected to the router on the LAN.

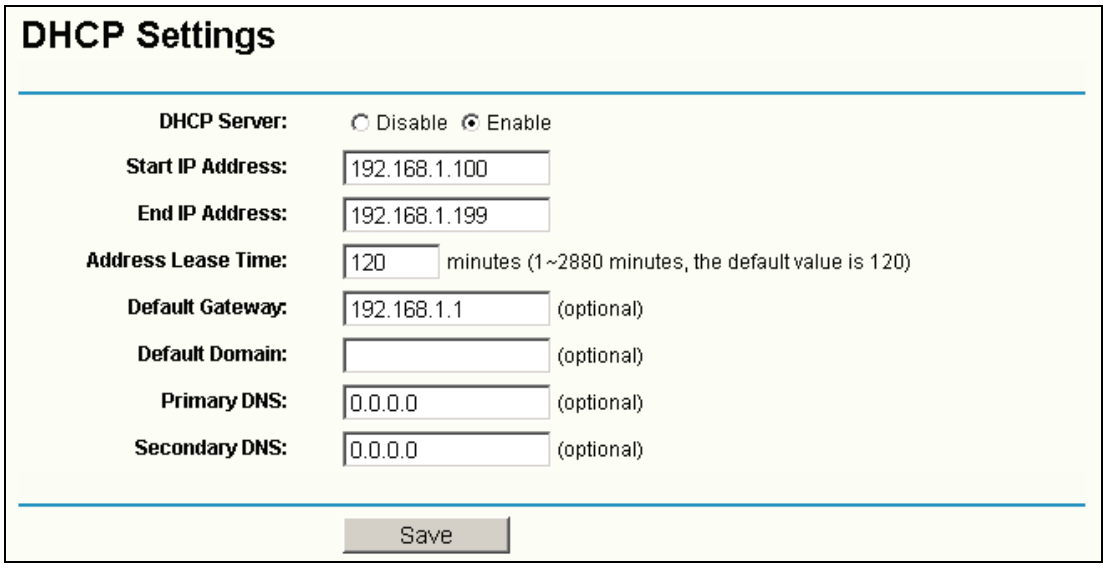


Figure 4-19 DHCP Settings

- **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.

4.7.2 DHCP Clients List

Choose menu "**DHCP→DHCP Clients List**", you can view the information about the clients attached to the router in the next screen (shown in Figure 4-20).

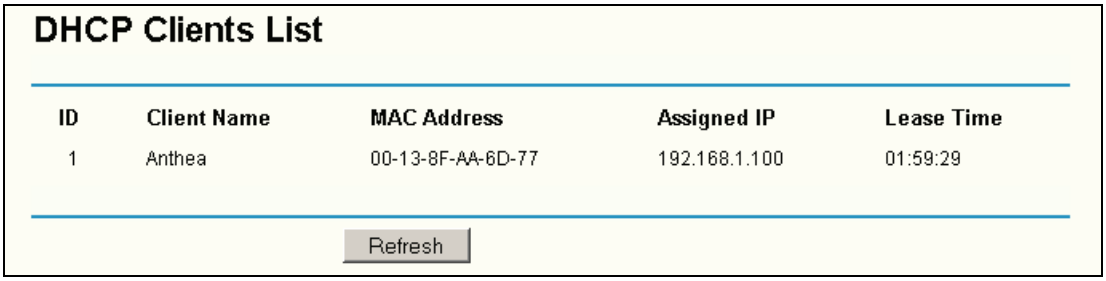


Figure 4-20 DHCP Clients List

- **ID -** 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. After the dynamic IP address has expired, the user will be automatically assigned a new dynamic IP address.

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

4.7.3 Address Reservation

Choose menu "**DHCP→Address Reservation**", you can view and add a reserved addresses for clients via the next screen (shown in Figure 4-21).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 the servers that require permanent IP settings.

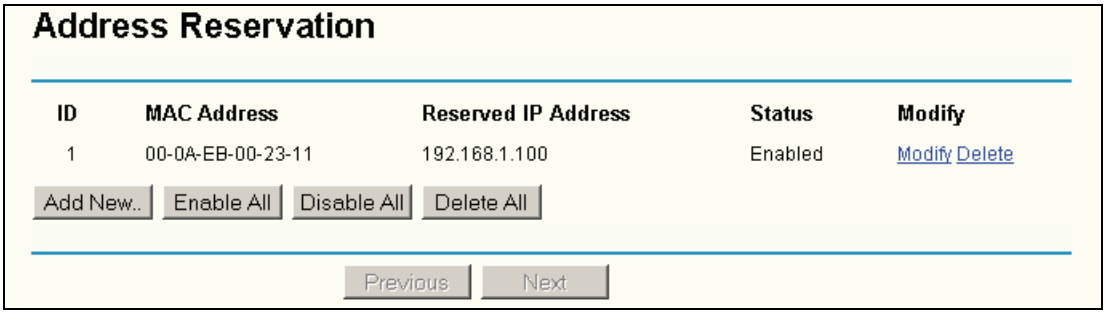


Figure 4-21 Address Reservation

- **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 the **Add New button**. (Pop-up Figure 4-22)
2. Enter the MAC address (in XX-XX-XX-XX-XX-XX format.) and IP address in dotted-decimal notation of the computer you wish to add.
3. Click the **Save** button when finished.

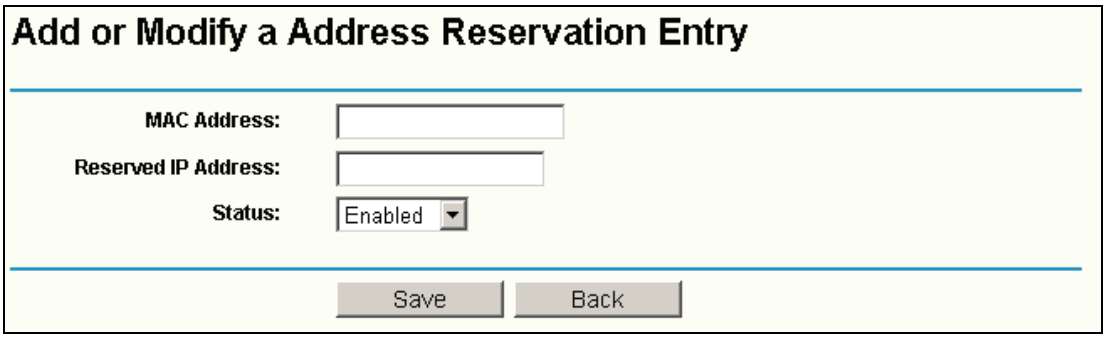


Figure 4-22 Add or Modify an Address Reservation Entry

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 the **Save** button.

Click the **Enable/ Disabled All** button to make all entries enabled/disabled

Click the **Delete All** button to delete all entries

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

4.8 Forwarding

Figure 4-23 The Forwarding menu

There are four submenus under the Forwarding menu (shown in Figure 4-23): **Virtual Servers**, **Port Triggering**, **DMZ** and **UPnP**. Click any of them, and you will be able to configure the corresponding function.

4.8.1 Virtual Servers

Choose menu "**Forwarding→Virtual Servers**", you can view and add virtual servers in the next screen (shown in Figure 4-24). 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.

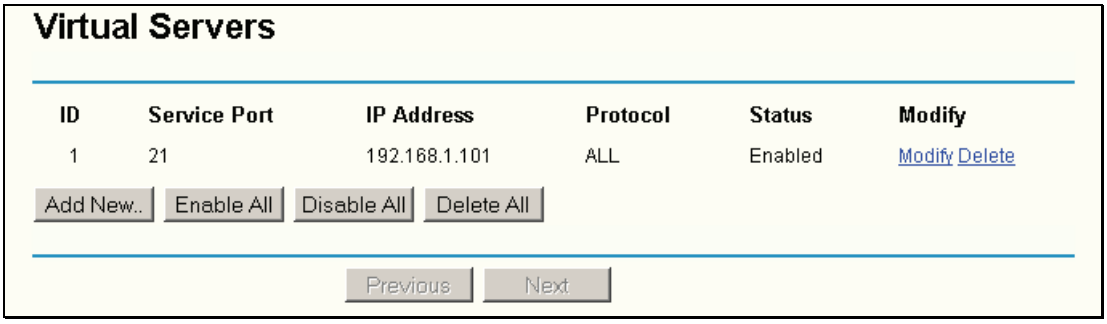


Figure 4-24 Virtual Servers

- **Service Port -** The numbers of External Ports. You can type a service port or a range of service ports (in XXX – YYY format, XXX is the start port number, YYY is the end port number).

- **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 the **Add New button**. (pop-up Figure 4-25)
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 the **Server IP Address** box.
4. Select the protocol used for this application, either **TCP** or **UDP**, or **All**.
5. Select the **Enable** check box to enable the virtual server.
6. Click the **Save** button.

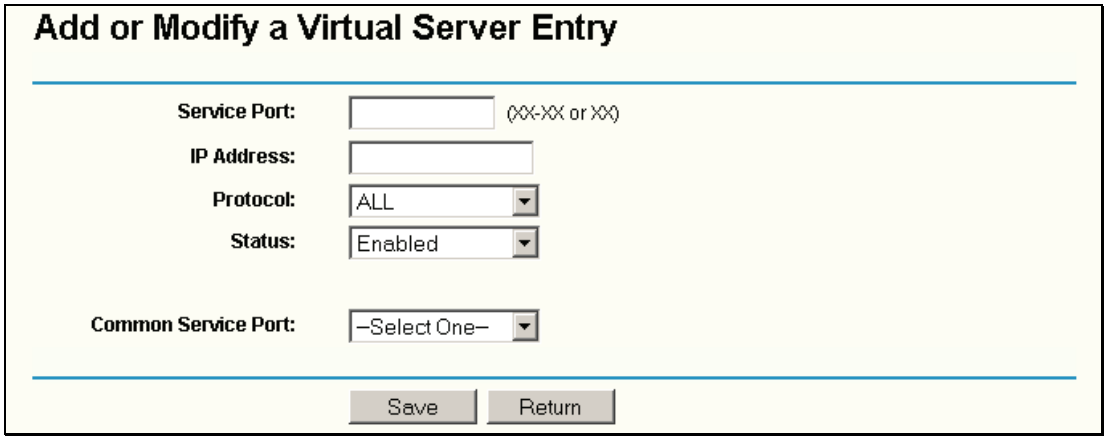


Figure 4-25 Add or Modify a Virtual Server Entry

Note:

If your computer or server has more than one type of available service, please select another service, and enter the same IP Address for that computer or server.

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 the **Save** button.

Click the **Enable/ Disabled All** button to make all entries enabled/ disabled.
Click the **Delete All** button to delete all entries.

Click the **Next** button to go to the next page and click the **Previous** button 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 **System Tools –> Remote Management** page to be any other value except 80 such as 8080. Otherwise there will be a conflict to disable the virtual server.

4.8.2 Port Triggering

Choose menu "**Forwarding→Port Triggering**", you can view and add port triggering in the next screen (shown in Figure 4-26). 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.

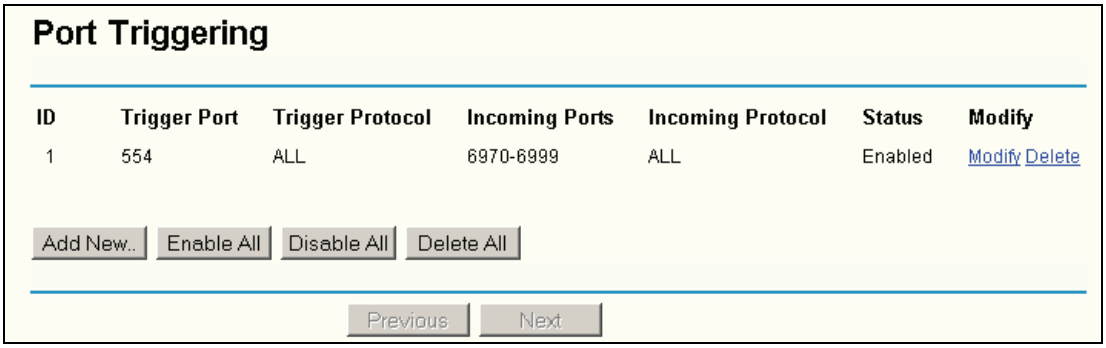


Figure 4-26 Port Triggering

Once configured, operation is as follows: Figure 4-26

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 ",". 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, enter the following data on the **Port Triggering** screen.

1. Click the **Add New button** (pop-up Figure 4-27).
2. Enter a port number used by the application when it generates an outgoing request.
3. Select the protocol used for **Trigger Port** from the pull-down list, either **TCP**, **UDP**, or **All.**
4. Enter the range of port numbers used by the remote system when it responds to the PC's request.
5. Select the protocol used for **Incoming Ports Range** from the pull-down list, either **TCP** or **UDP**, or **All.**
6. Select the **Enable** checkbox to enable.
7. Click the **Save** button to save the new rule.

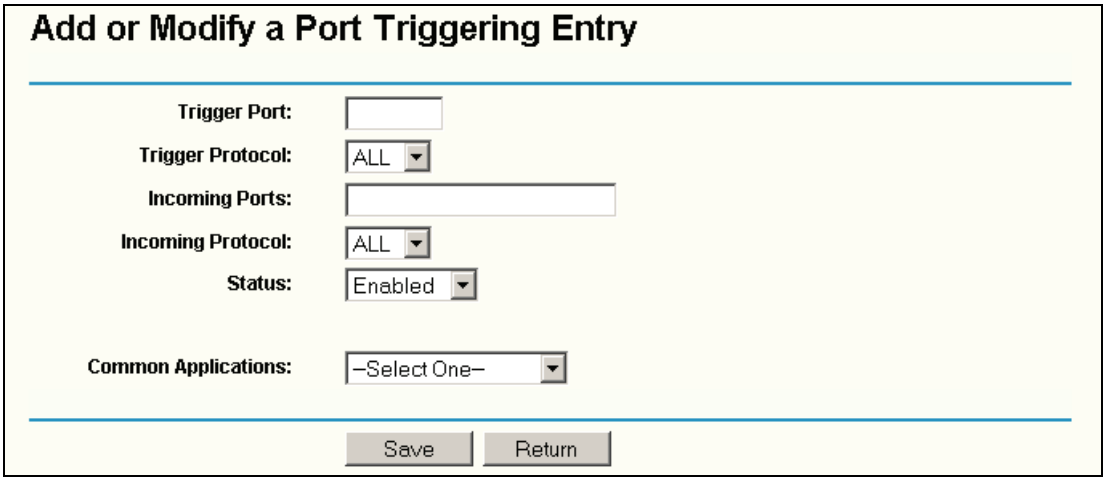


Figure 4-27 Add or Modify a Triggering Entry

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 the **Enable** checkbox. It has the same effect as adding a new rule.

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 the **Save** button.

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

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

Click the **Delete All** button 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.

4.8.3 DMZ

Choose menu "**Forwarding→DMZ**", you can view and configure DMZ host in the screen (shown in Figure 4-28).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.

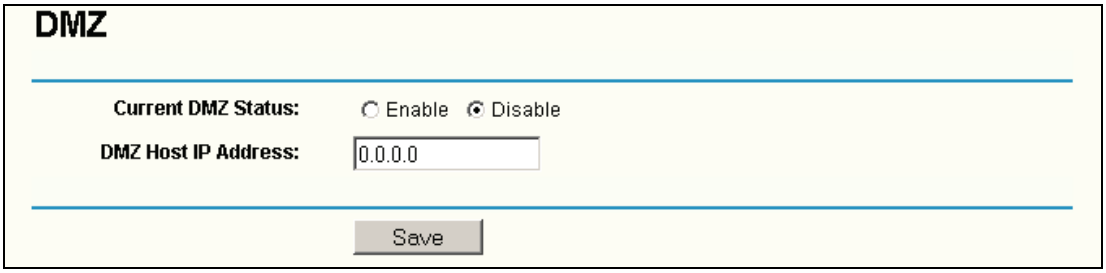


Figure 4-28 DMZ

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

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

Note:

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

4.8.4 UPnP

Choose menu "**Forwarding→UPnP**", you can view the information about **UPnP**(Universal Plug and Play) in the screen (shown in Figure 4-29).The 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.

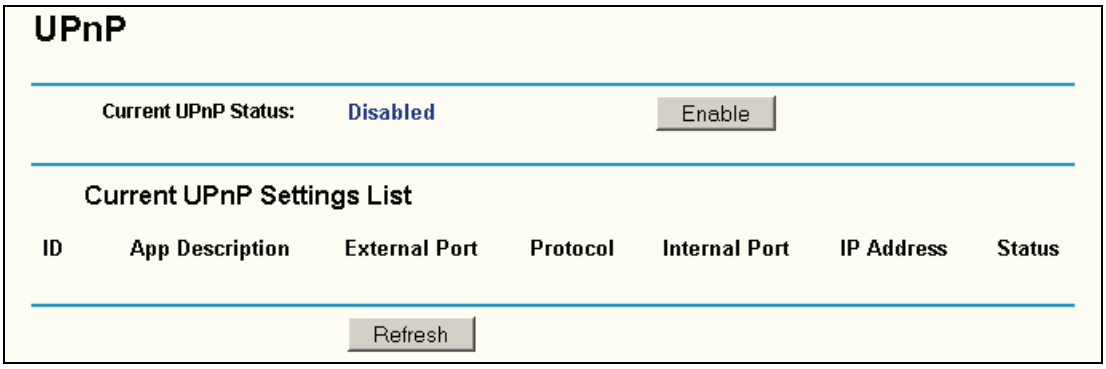


Figure 4-29 UPnP Setting

- **Current UPnP Status -** UPnP can be enabled or disabled by clicking the **Enable** or **Disable** button. 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 -** Shows 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 -** The port's status displayed here. "Enabled" means that port is still active. Otherwise, the port is inactive.

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

4.9 Security

Figure 4-30 The Security menu

There are four submenus under the Security menu (shown in Figure 4-30): **Firewall**, **IP Filtering, Domain Filtering** and **MAC Filtering.** Click any of them, and you will be able to configure the corresponding function.

4.9.1 Firewall

Choose menu "**Security→Firewall**", you can control the general firewall switch in the firewall page (shown in Figure 4-31). The default setting for the switch is off. When the general firewall switch is off, even if IP Address Filtering, DNS Filtering and MAC Filtering are enabled, their settings are ineffective.

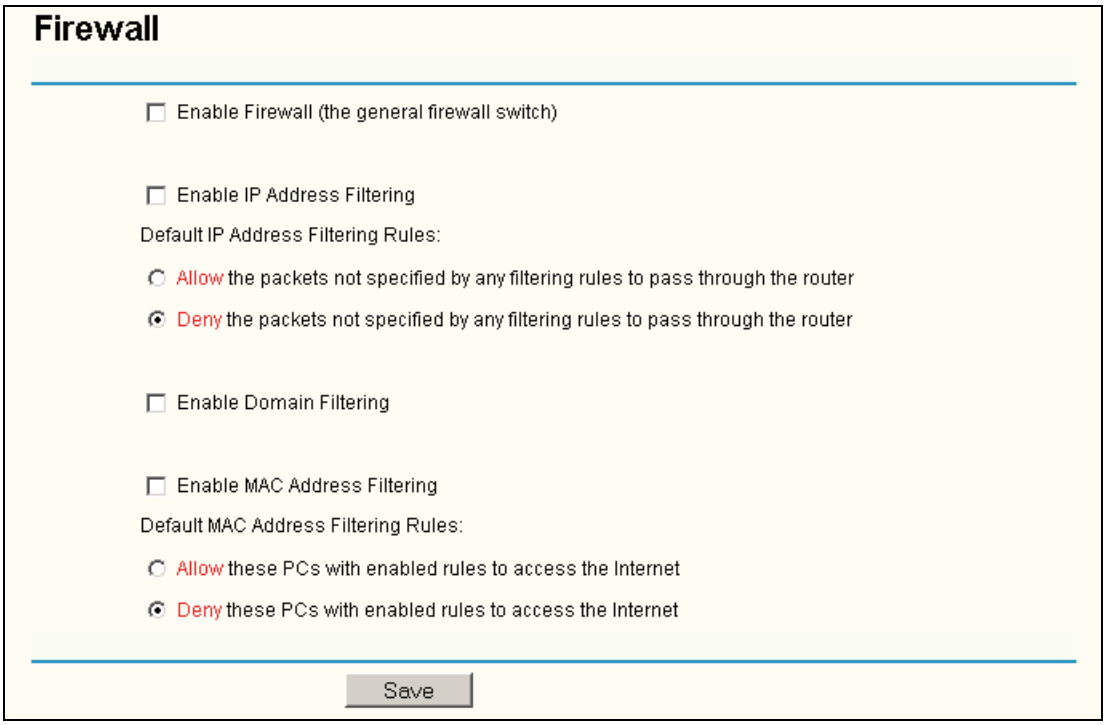


Figure 4-31 Firewall

- **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.

4.9.2 IP Filtering

Choose menu "**Security→IP Filtering**", you can configure the IP Address filtering rule in the screen (shown in Figure 4-32). The IP Address Filtering feature allows you to control the Internet Access of some specific users based on their IP addresses.

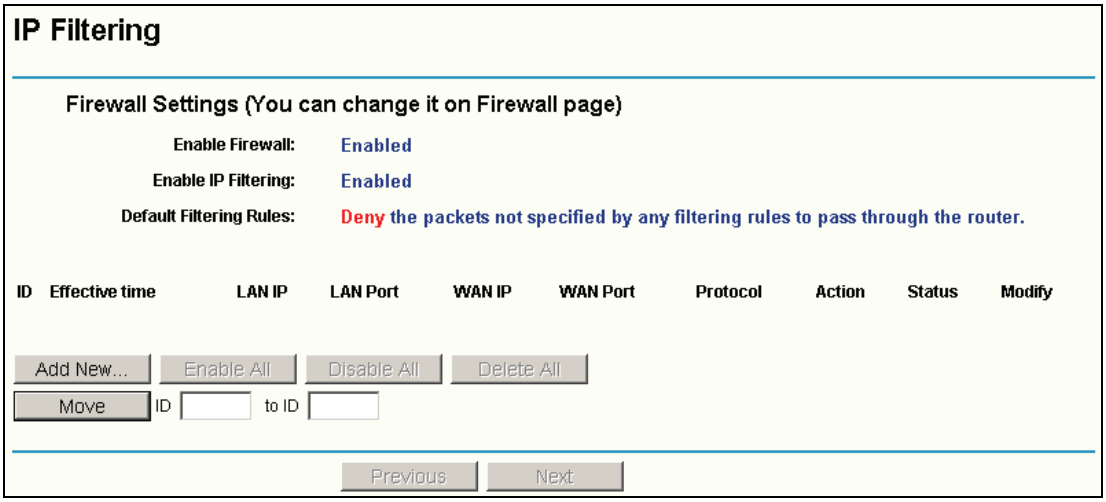


Figure 4-32 IP address Filtering

- **Effective Time -** This is the time or the range of time for the entry to take effect. For example, 1800 - 2200, it means that the entry will take effect from 18:00 to 22:00.
- **LAN IP -** This is the LAN IP address or the range of LAN IP addresses in dotted-decimal notation format. For example, 192.168.1.20 - 192.168.1.30. Keep the field blank, which means all LAN IP addresses are controlled by the rule.
- **LAN Port -** This is the LAN Port or the range of LAN ports in the field. For example, 1030 - 2000. Keep the field blank, which means all LAN ports are controlled by the rule.
- **WAN IP -** This is the WAN IP address or the range of WAN IP addresses in dotted-decimal notation format. For example, 202.96.134.210 – 202.96.134.230. Keep the field blank, which means all WAN IP addresses are controlled by the rule.
- **WAN Port -** This is the WAN Port or the range of WAN Ports. For example, 25 – 110. Keep the field blank, which means all WAN Ports are controlled by the rule.
- **Protocol -** This indicates which protocol is used, either **TCP**, **UDP**, or **All** (all protocols supported by the router).
- **Action -** This field displays the action that the Router takes to deal with the traffic. **Allow** means that the Router allows the traffic through the Router, **Deny** means that the Router rejects the traffic through the router.
- **Status -** This field displays the status of the rule. **Enabled** means the rule will take effect, **Disabled** means the rule will not take effect.

Note:

Before adding an IP Address Filtering entry, you should enable the Firewall and the IP Address Filtering function first (shown in Figure 4-31).

To add/modify an IP Address filtering entry:

For example: If you desire to block E-mail received and sent by the IP address 192.168.1.7 on

your local network during the time of 1800 to 2200; And wish to make the PCs with IP addresses 192.168.1.8 to 192.168.1.12 unable to visit the website of IP address 202.96.134.12 all the day, while other PCs have no limit. You can configure the rules as follows.

1. Enable the “Firewall” and “IP Address Filtering” on the Firewall screen (show in Figure 4-31), and then, you should select the Default IP Address Filtering Rule "Allow the packets not specified by any filtering rules to pass through the router".

2. Click **Add New…/Modify** shown in Figure 4-32, you will see a new screen shown in Figure 4-33. Enter the “Effective time” for the rule to take effect.

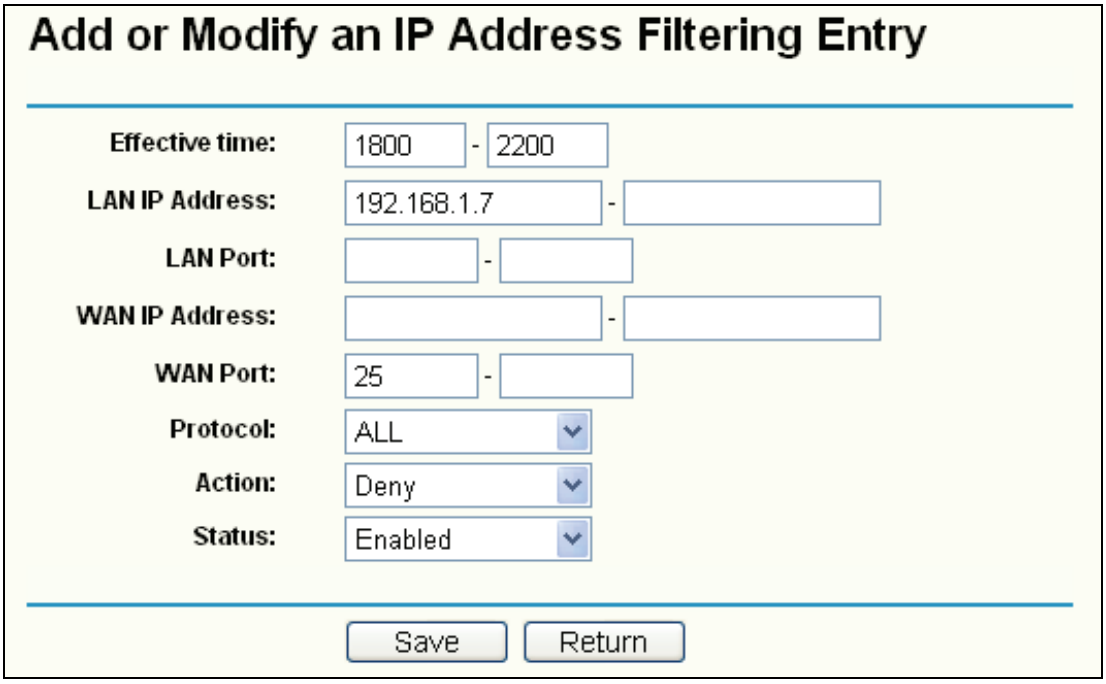


Figure 4-33

3. Enter the “LAN IP Address”, “LAN Port”, “WAN IP Address” and “WAN Port” in the corresponding field.

4. Select the “Protocol”, “Action” and “Status” for the rule as shown in the Figure 4-33

5. Click the **Save** button to save this entry.

6. Go to **Step 2** to complete the other rules continually.

After you finish the configurations, you will see the rules in the table below:

ID	Effective time	LAN IP	LAN Port	WAN IP	WAN Port	Protocol	Action	Status	Modify
1	1800-2200	192.168.1.7	-	-	25	ALL	Deny	Enabled	Modify Delete
2	1800-2200	192.168.1.7	-	-	110	ALL	Deny	Enabled	Modify Delete
3	0000-2400	192.168.1.8-192.168.1.12	-	202.96.134.12	-	ALL	Deny	Enabled	Modify Delete

Other configurations for the entries:

Click the **Delete** button to delete the entry.

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

Click the **Disable All** button to disable all the entries.

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

Click the **Move** button to change the entry's order after entering the ID number in the first box and another ID number in second box

Click the **Previous** button to view the information in the previous screen, click the **Next** button to view the information in the next screen.

4.9.3 Domain Filtering

Choose menu "**Security→Domain Filtering**", you can configure the Domain filtering rule in the screen (shown in Figure 4-34). The Domain Filtering feature allows you to control access to certain websites on the Internet by specifying their domains or key words.

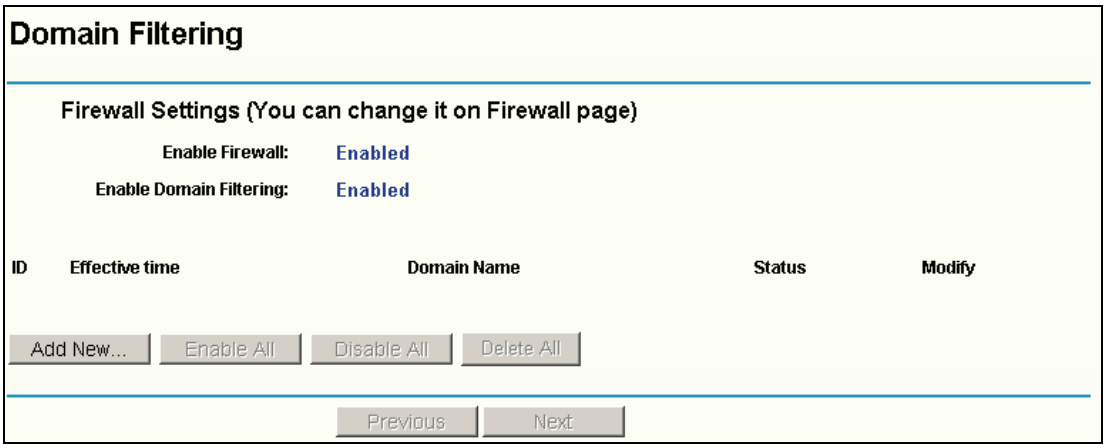


Figure 4-34 Domain Filtering

- **Effective Time -** Enter a time in HHMM format to specify the period when the filtering will take effect. For example, if the period is 0803 - 1705 then filtering will be active from 08:03 to 17:05.
- **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.
- **Status -** Select **Enabled** or **Disabled** for this entry on the **Status** pull-down list. **Enabled** means the rule is effective, **Disabled** means the rule is ineffective.

Note:

Before adding an IP Address Filtering entry, you should enable the Firewall and the IP Address Filtering function first (shown in Figure 4-31).

To Add a Domain filtering entry:

For example: if you want to block the PCs on your LAN from accessing websites www.xxyy.com.cn, www.aabbcc.com and websites with end of .net on the Internet, while no limit for other websites, you can configure as follows.

1. Click **Add New…/Modify** shown in Figure 4-34, you will see following screen.

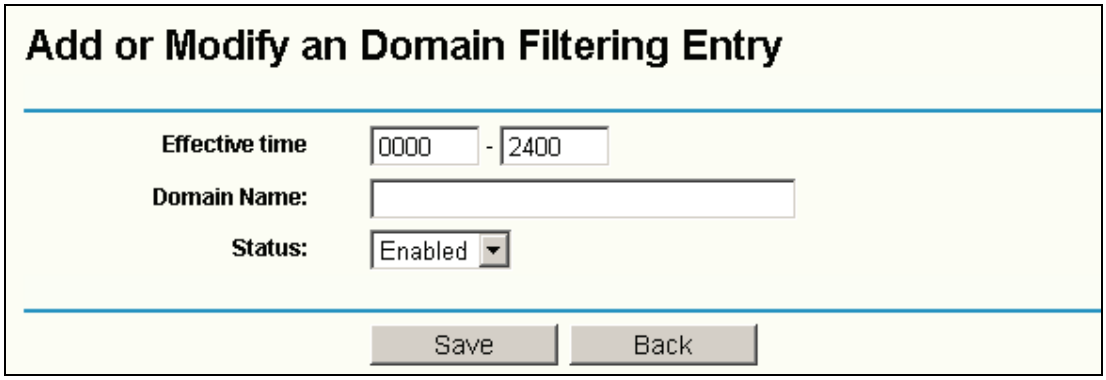


Figure 4-35 Add or Modify a Domain Filtering entry

2. Enter the “Effective time” and “Domain Name” in the screen shown in Figure 4-35.
3. Select the “Status” for the rule as shown in the screen.
4. Finally, click **Save** to make the rule take effect.

To add additional entries, repeat steps 1-4.

After you finish the configurations, you will see the rules in the table below:

ID	Effective time	Domain Name	Status	Modify
1	0000-2400	www.xxyy.com	Enabled	Modify Delete
2	0800-2000	www.aabbcc.com	Enabled	Modify Delete
3	0000-2400	.net	Enabled	Modify Delete

Other configurations for the entries:

Click the **Delete** button to delete the entry.

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

Click the **Disable All** button to disable all the entries.

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

Click the **Previous** button to view the information in the previous screen, click the **Next** button to view the information in the next screen.

4.9.4 MAC Filtering

Choose menu "**Security→MAC Address Filtering**", you can configure the MAC Address filtering rule in the next screen (shown in Figure 4-36). The MAC Address Filtering feature allows you to control access to the Internet by users on your local network based on their MAC addresses.

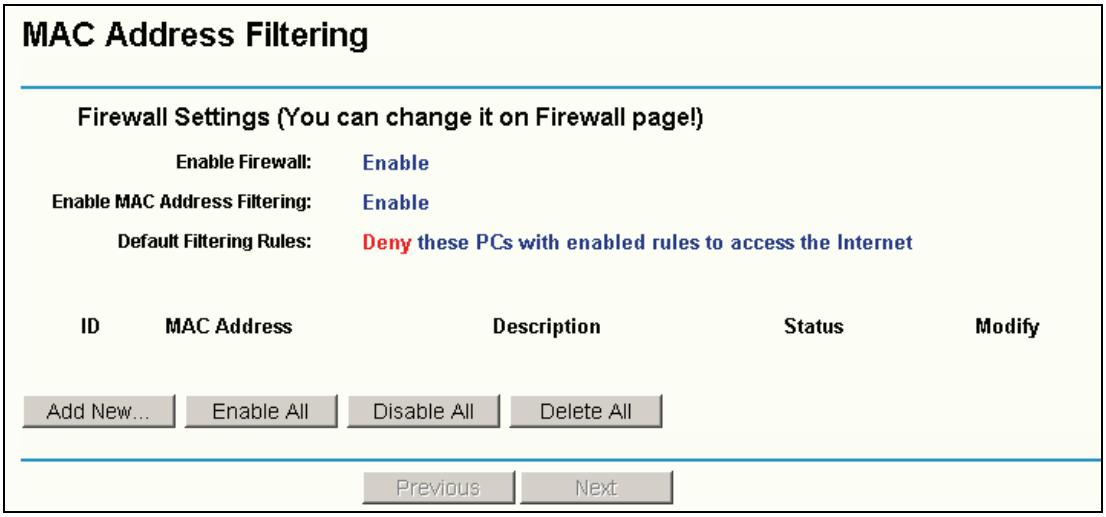


Figure 4-36 MAC Address Filtering

- **MAC Address -** .This is the PC'S MAC address which is controlled by the rule. Its format is XX-XX-XX-XX-XX-XX (X is any hexadecimal digit). For example: 00-0E-AE-B0-00-0B.
- **Description -** This is the description about the PC, Fox example: John's PC.
- **Status -** This field displays the status, **Enabled** means the rule is effective, **Disabled** means the rule is ineffective.

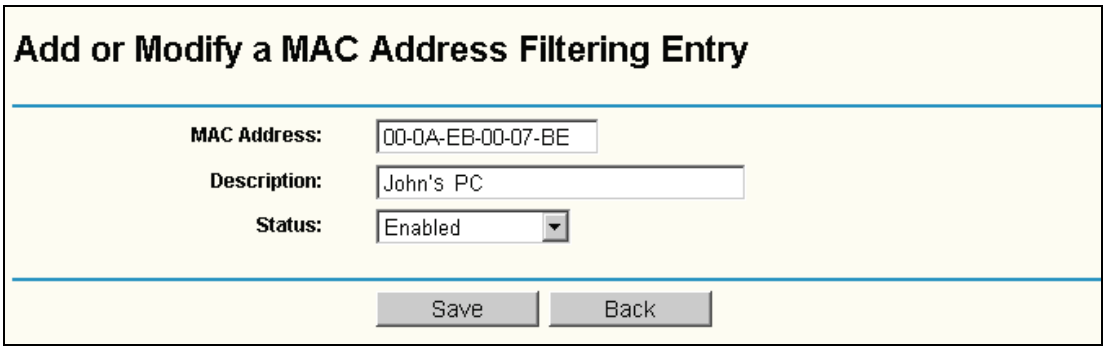
Note:

Before adding a MAC Address Filtering entry, you should enable the Firewall and the MAC Address Filtering function first (shown in Figure 4-31).

To add or modify a Domain Filtering entry:

Fox example: If you want to block the PCs with MAC addresses 00-0A-EB-00-07-BE and 00-0A-EB-00-07-5F to access the Internet, you can configure as follows.

1. Enable the "Firewall" and "MAC Address Filtering" on the Firewall screen (show in Figure 4-31). And then specify the Default MAC Address Filtering Rule as "Deny these PCs with enabled rules to access the Internet".
2. Click Add New…/Modify shown in Figure 4-36, you will see the following screen.



3. Enter the appropriate MAC address and descriptions, and then choose the enabled status.

4. Finally, click **Save** to make the rule take effect.

To add additional entries, repeat steps 1-4.

After you finish the configurations, you will see the rules in the table below:

ID	MAC Address	Description	Status	Modify
1	00-0A-EB-00-07-BE	John's computer	Enabled	Modify Delete
2	00-0A-EB-00-07-5F	Alice's computer	Enabled	Modify Delete

Figure 4-37

Other configurations for the entries:

Click the **Delete** button to delete the entry.

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

Click the **Disable All** button to disable all the entries.

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

Click the **Previous** button to view the information in the previous screen, click the **Next** button to view the information in the next screen.

4.10 Static Routing

Choose menu "**static routing**", you can configure the static route in the next screen (shown in Figure 4-38). A static route is a pre-determined path that network information must travel to reach a specific host or network.

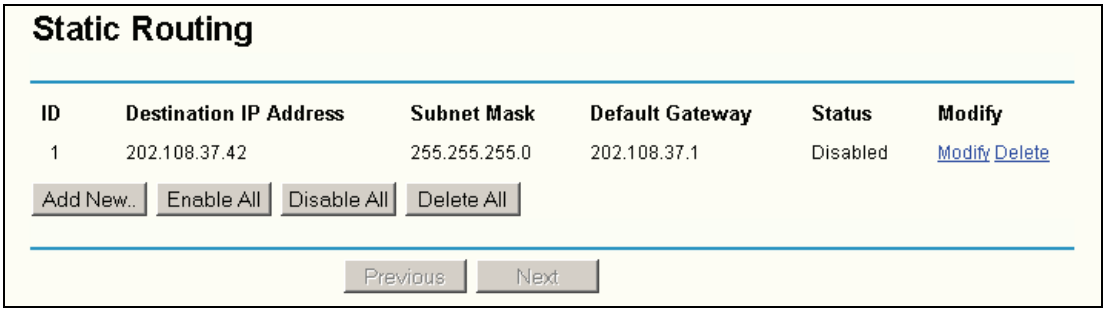


Figure 4-38 Static Routing

To add static routing entries:

1. Click **Add New…** shown in Figure 4-38, you will see the following screen.

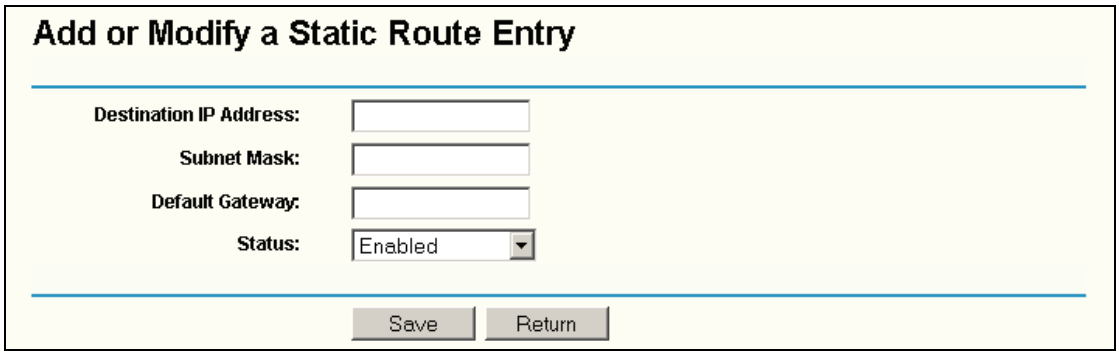


Figure 4-39 Add or Modify a Static Route Entry

2. Enter the following data:

   - **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.

3. Select **Enabled** or **Disabled** for this entry on the **Status** pull-down list.

4. Click the **Save** button to make the entry take effect.

Other configurations for the entries:

Click the **Delete** button to delete the entry.

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

Click the **Disable All** button to disable all the entries.

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

Click the **Previous** button to view the information in the previous screen, click the **Next** button to view the information in the next screen.

4.11 Dynamic DNS

Choose menu "**Dynamic DNS**", you can configure the Dynamic DNS function in the next screen (shown in Figure 4-40).

The router offers the **DDNS** (Dynamic Domain Name System) feature, which allows the hosting of a website, FTP server, or e-mail server with a fixed domain name (named by yourself) and a dynamic IP address, and then your friends can connect to your server by entering your domain name no matter what your IP address is.

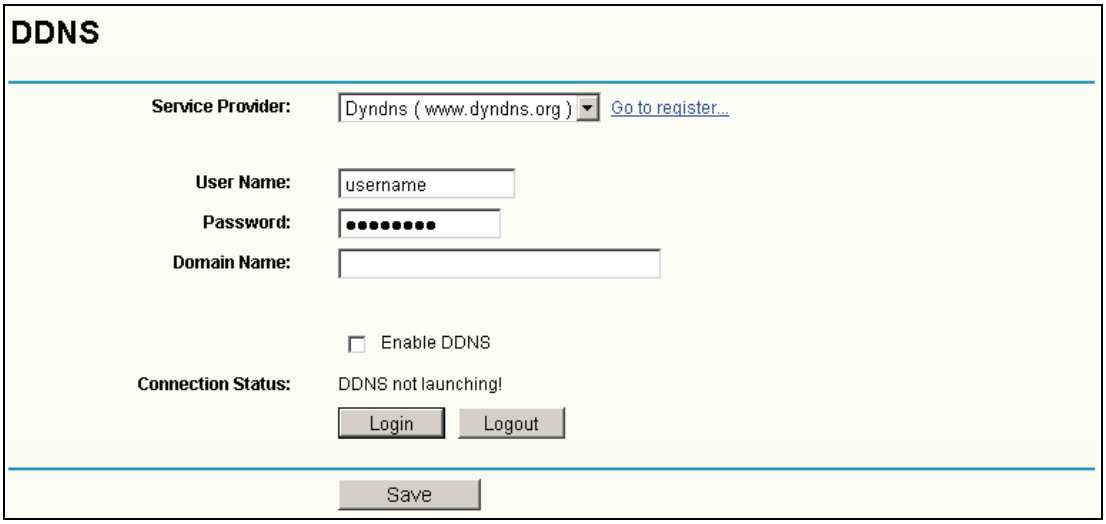


Figure 4-40 Dyndns.org DDNS Settings

Before using this feature, you need to sign up for DDNS service providers www.dyndns.org,

To set up for DDNS, follow these instructions:

1. Type the **domain names** that you registered with your DDNS service provider..
2. Type the **User Name** for your DDNS account.
3. Type the **Password** for your DDNS account.
4. Click the **Login** button 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.

4.12 System Tools

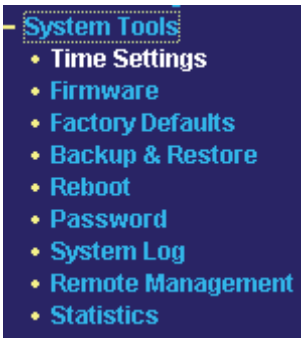


Figure 4-41 The System Tools menu

Choose menu "**System Tools**", you can see the submenus under the main menu: **Time Settings**, **Firmware**, **Factory Defaults, Backup & Restore, Reboot, Password, System Log, Remote Management** and **Statistics.** Click any of them, and you will be able to configure the corresponding function. The detailed explanations for each submenu are provided below.

4.12.1 Time Setting

Choose menu "**System Tools→Time Setting**", you can configure the time on the following screen.

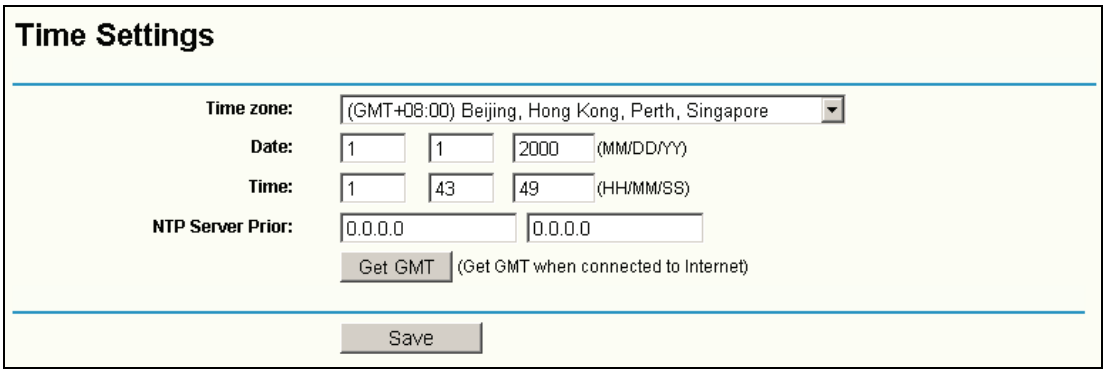


Figure 4-42 Time settings

- **Time Zone -** Select your local time zone from this pull down list.
- **Date -** Enter your local date in MM/DD/YY into the right blanks.
- **Time -** Enter your local time in HH/MM/SS into the right blanks.
- **NTP Server Prior -** Enter the address for the NTP Server, then the Router will get the time from the NTP Server preferentially. In addition, the Router built-in some common NTP Servers, so it can get time automatically once it connects the Internet.

To configure the system manually:

1. Select your local time zone.
2. Enter date and time in the right blanks.

3. Click **Save** to save the configuration.

To configure the system automatically:

1. Select your local time zone.
2. Enter the IP address for **NTP Server Prior**.
3. Click the **Get GMT** button to get system time from Internet if you have connected to the Internet.

☞ **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, otherwise, 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.

4.12.2 Firmware

Choose menu "**System Tools→Firmware**", you can update the latest version of firmware for the Router on the following screen.

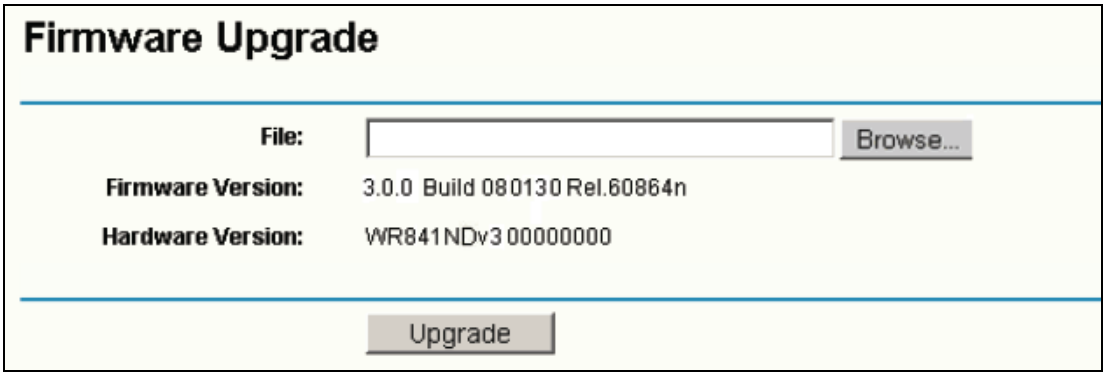


Figure 4-43 Firmware Upgrade

- **Firmware Version -** This displays the current firmware version.
- **Hardware Version -** This displays the current hardware version. The hardware version of the upgrade file must accord with the Router's current hardware version.

To upgrade the router's firmware, follow these instructions below:

1. Download a more recent firmware upgrade file from the TP-LINK website (www.tp-link.com).
2. Type the path and file name of the update file into the "File" field. Or click the **Browse** button to locate the update file.
3. Click the **Upgrade** button.

☞ **Note:**

1) New firmware versions are posted at www.tp-link.com and can be downloaded for free. If your router experiences no difficulties, it is unnecessary to download a recent firmware version

unless the new version has a special feature that you want.

2) When you upgrade the router's firmware, you may lose its current configurations, so please back up the router's current settings before you upgrade its firmware.

3) Do not turn off the router or press the Reset button while the firmware is being upgraded, otherwise, the router may be damaged.

4) The router will reboot after the upgrading has been finished.

4.12.3 Factory Defaults

Choose menu "**System Tools→Factory Defaults**", and you can restore the configurations of the Router to factory defaults on the following screen

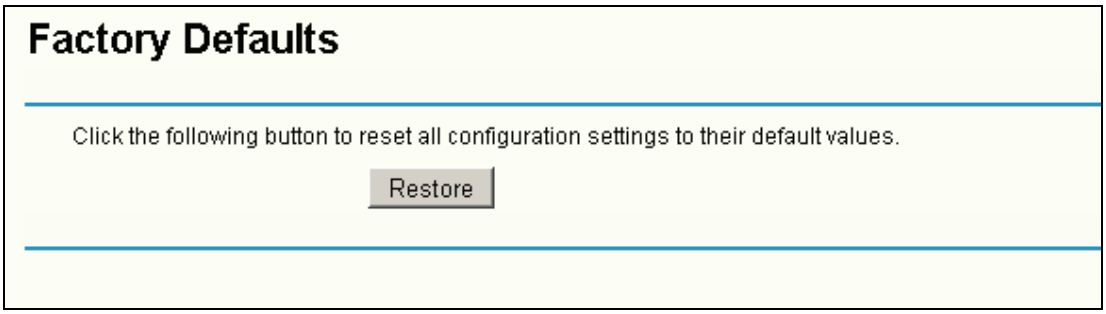


Figure 4-44 Restore Factory Default

Click the **Restore** button to reset all configuration settings to their default values.

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

☞ **Note:**

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

4.12.4 Backup & Restore

Choose menu "**System Tools→Backup and Restore**", you can save the current configuration of the Router as a backup file and restore the configuration via a backup file(shown in Figure 4-45).

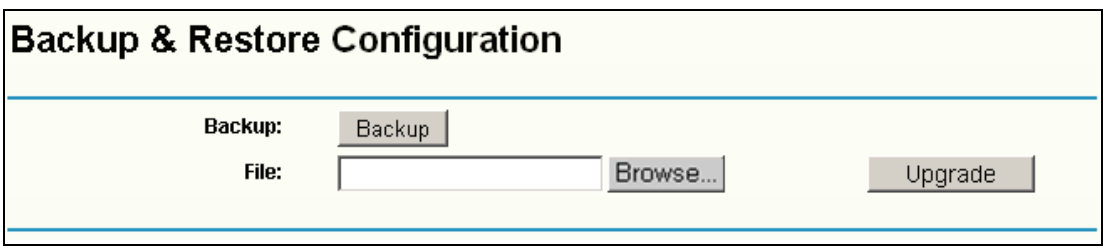


Figure 4-45 Backup & Restore Configuration

- Click the **Backup** button to save all configuration settings as a backup file in your local computer.
- To upgrade the router's configuration, follow these instructions:
  - Click the **Browse** button to locate the update file for the device, or enter the exact path to the Setting file in the text box.
  - Click the **Upgrade** button.

Note:

The current configuration will be covered by the uploading configuration file. The upgrade process lasts for 20 seconds and the router will restart automatically. Keep the router on during the upgrading process, to prevent any damage.

4.12.5 Reboot

Choose menu "**System Tools→Reboot**", click the **Reboot** button to reboot the router via the next screen.

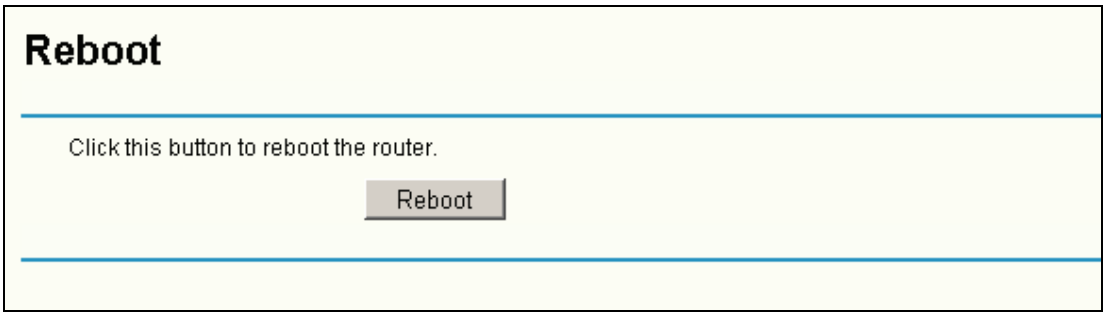


Figure 4-46 Reboot the router

Some settings of the router will take effect only after rebooting, which include:

- Change Web Service Port of the router.
- Upgrade the firmware of the router (system will reboot automatically).
- Restore the router's settings to factory default (system will reboot automatically).

4.12.6 Password

Choose menu "**System Tools→Password**", you can change the factory default user name and password of the router in the next screen (shown in Figure 4-47).

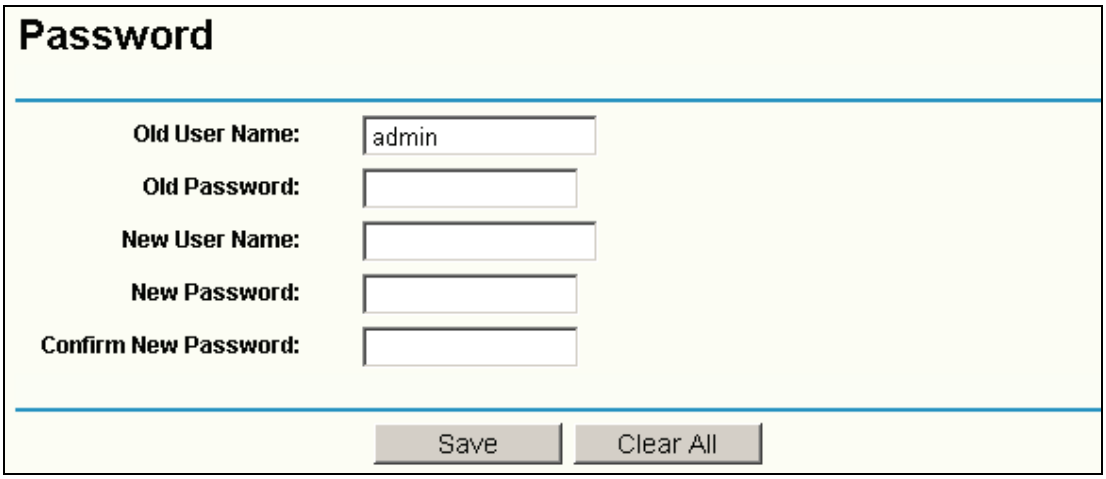


Figure 4-47 Password

It is recommended strongly that you should change the factory default user name and password of the router, because all users who try to access the router's Web-based utility or Quick Setup will be prompted for the router's default user name and password.

☞ **Note:**

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

Click the **Save** button when finished.

Click the **Clear All** button to clear all.

4.12.7 System log

Choose menu "**System Tools→System Log**", you can view the logs of the Router.

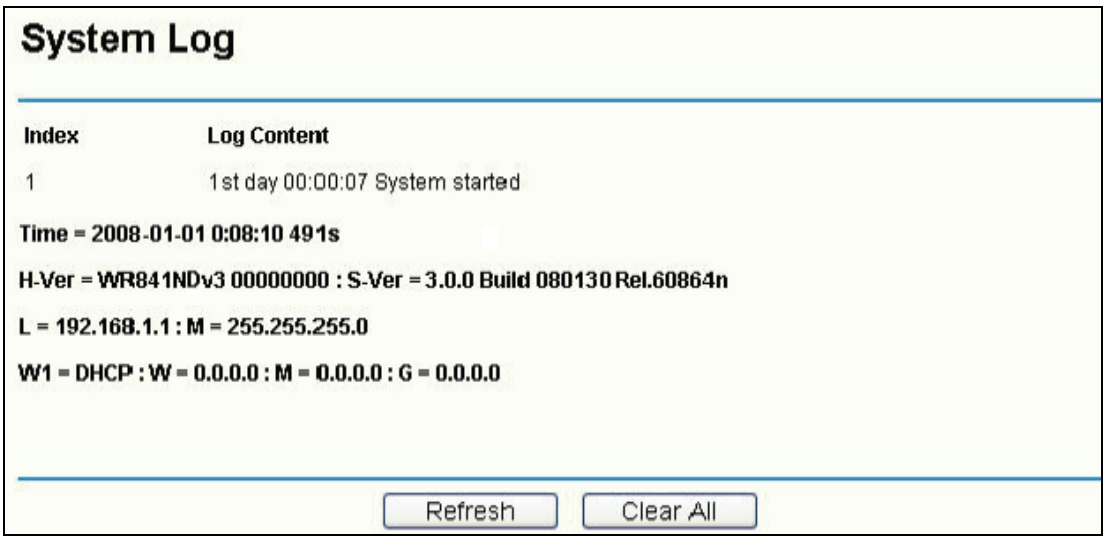


Figure 4-48 System Log

The router can keep logs of all traffic. You can query the logs to find what happened to the router.

Click the **Refresh** button to refresh the logs.

Click the **Clear All** button to clear all the logs.

4.12.8 Remote Management

Choose menu "**System Tools → Remote Management**", you can configure the Remote Management function on this screen (shown in Figure 4-49). This feature allows you to manage your Router from a remote location via the Internet.

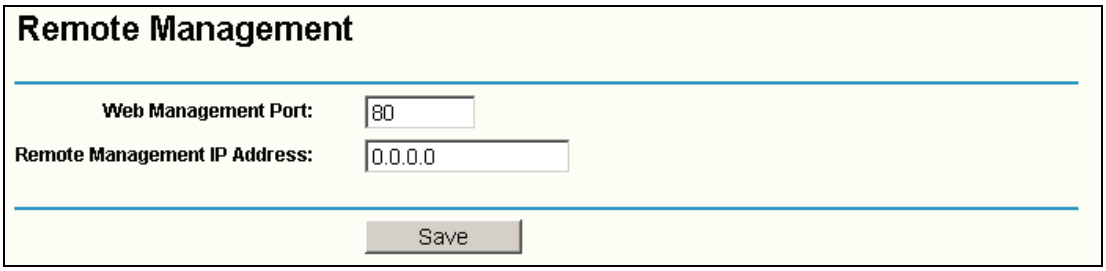


Figure 4-49 Remote Management

- **Web Management Port -** The port number used to access the router. This router's default remote management web port number is 80. For greater security, you'd better change the remote management web interface to a custom port by entering that number in the 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.

Note:

1) 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 the port number you use is 8080, please enter http://202.96.12.8:8080 in your browser. Later, you may be asked for the router's password. After successfully entering the username and password, you will be able to access the router's web-based utility.
2) Be sure to change the router's default password to a very secure password.

4.12.9 Statistics

Choose menu "**System Tools→Statistics**", you can view the statistics of the Router, including total traffic and current traffic of the last "Packets Statistic interval" seconds.

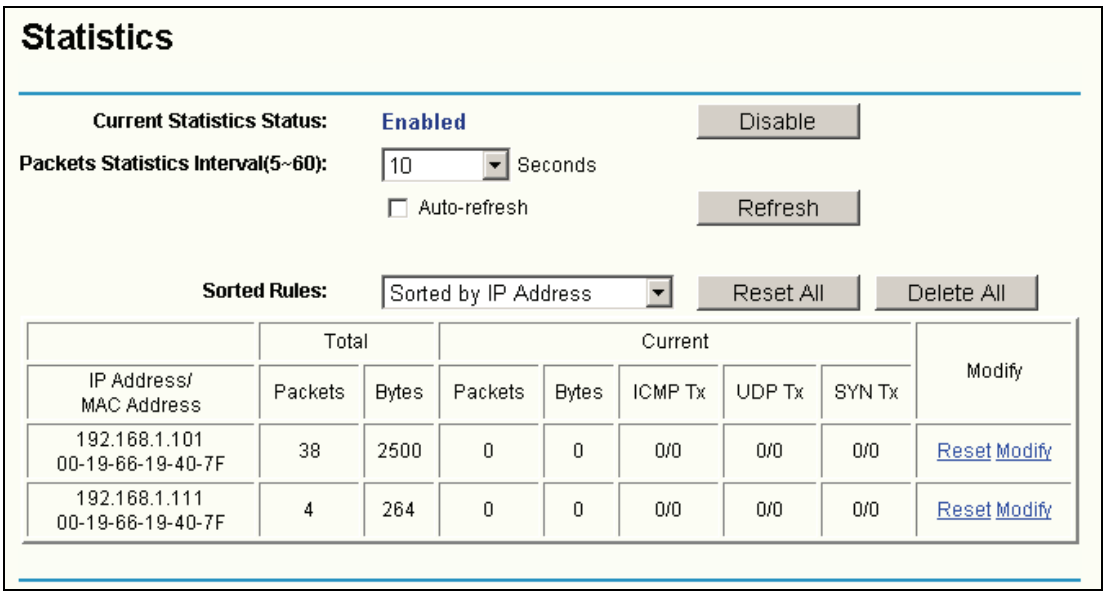


Figure 4-50 Statistics

- **Current Statistics Status -** Enable or Disable. The default value is disabled. To enable, click the **Enable** button.
- **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/MAC Address		The IP/MAC Address displayed with statistics
Total	**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	**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 the **Save** button to save the **Packets Statistic interval** value.

Click the **Auto-refresh** checkbox to refresh automatically.

Click the **Refresh** button to refresh immediately.

Appendix A: FAQ

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

1) First, configure the ADSL Modem configured in RFC1483 bridge model.

2) 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.

3) 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”.

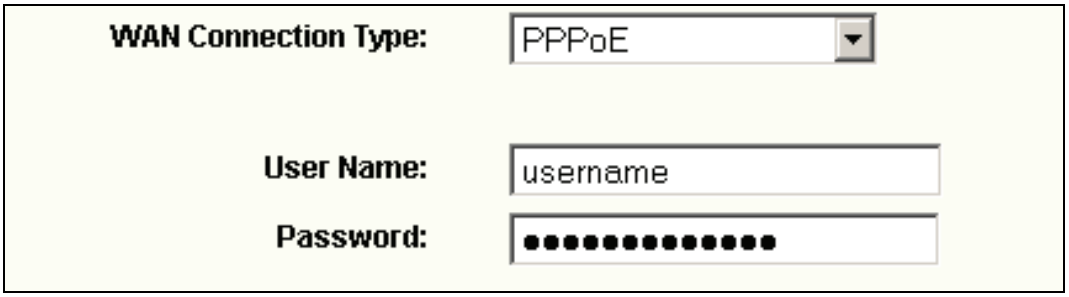


Figure A-1 PPPoE Connection Type

4) 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.

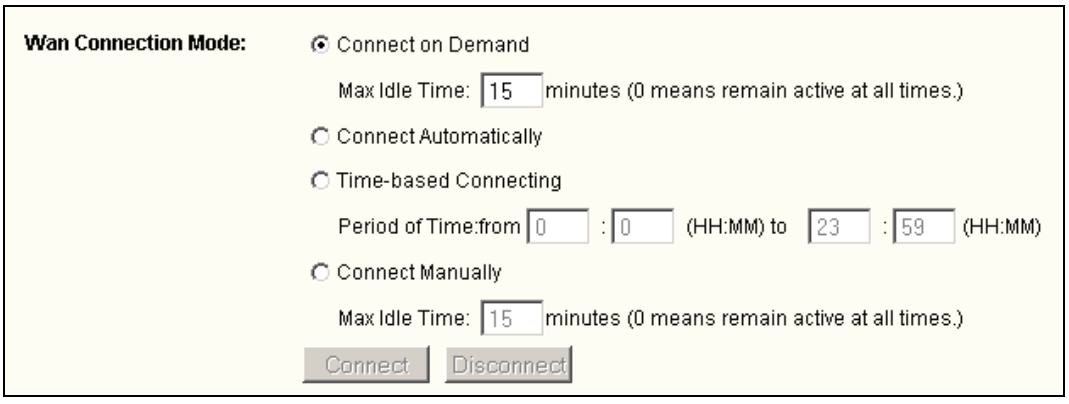


Figure A-2 PPPoE Connection Mode

☞ **Note:**

i. 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.

ii. If you are a Cable user, please configure the router following the above steps.

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

1) 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”.

2) Some ISPs require that you register the MAC Address of your adapter, which is connected to your cable/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 the "Clone MAC Address" button 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. Then click the "Save" button. It will take effect after rebooting.

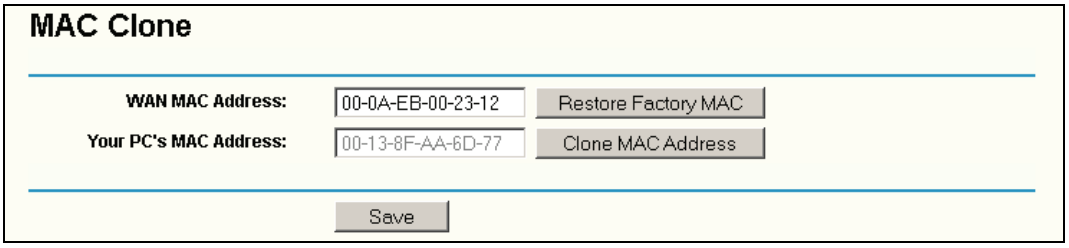


Figure A-3 MAC Clone

3. I want to use Netmeeting, what do I need to do?

1) If you start Netmeeting as a sponsor, you don’t need to do anything with the router.

2) If you start as a response, you need to configure Virtual Server or DMZ Host.

3) 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” for the “Service Port” blank, and your IP address for the “IP Address” blank, taking 192.168.1.169 for an example, remember to “Enable” and “Save”.

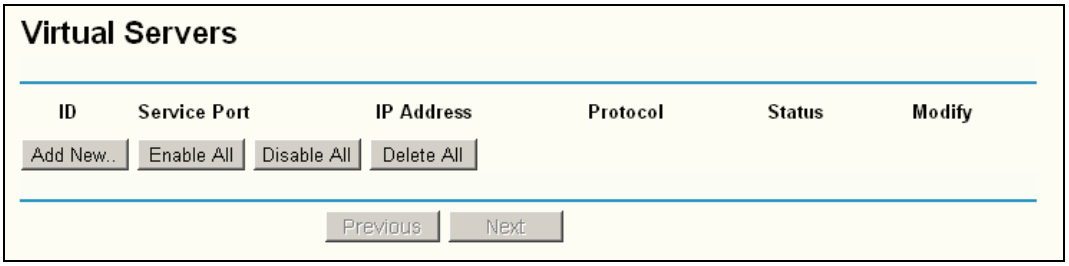


Figure A-4 Virtual Servers

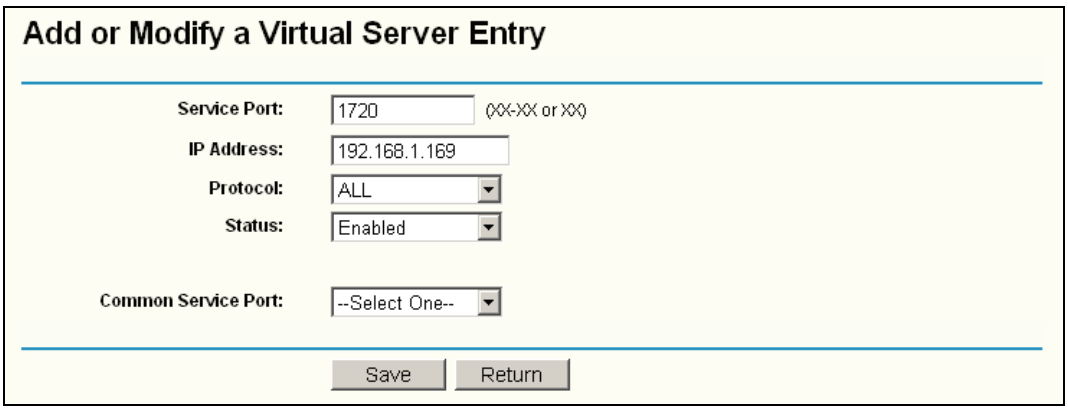


Figure A-5 Add or Modify a Virtual server Entry

Note:

Your opposite side should call your WAN IP, which is displayed on the “Status” page.

4) 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 the "Save” button.

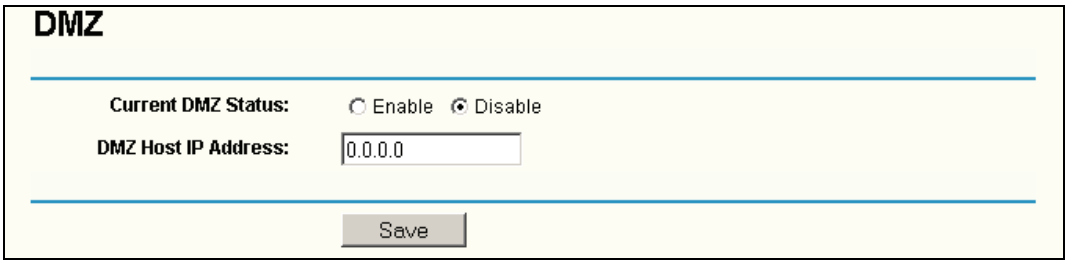


Figure A-6 DMZ

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

1) 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.

2) 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.

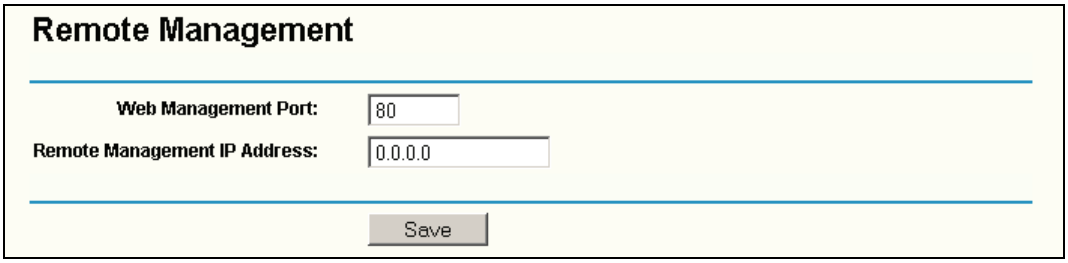


Figure A-7 Remote Management

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".

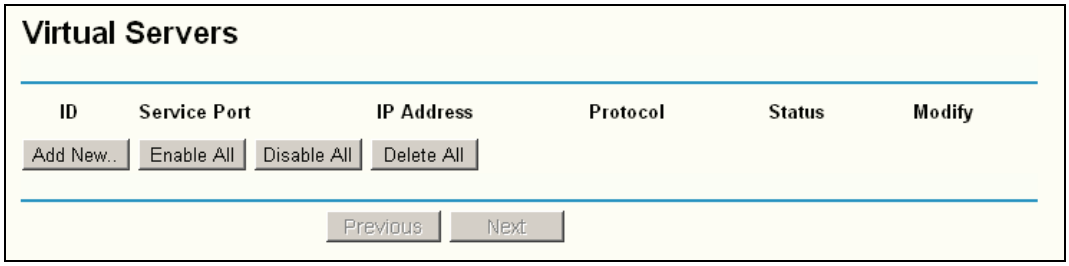


Figure A-8 Virtual Servers

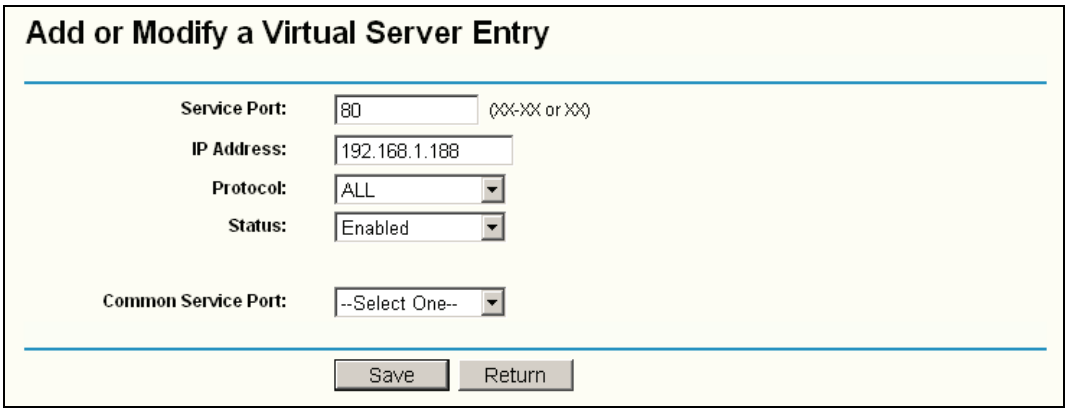


Figure A-9 Add or Modify a Virtual server Entry

5. The wireless stations cannot connect to the router.

1) Make sure the "Wireless Router Radio" is enabled.

2) Make sure that the wireless stations' SSID accord with the router's SSID.

3) Make sure the wireless stations have right KEY for encryption when the router is encrypted.

4) If the wireless connection is ready, but you can't access the router, check the IP Address of your wireless stations.

Appendix B: Configuring the PCs

In this section, we'll introduce how to install and configure the TCP/IP correctly in Windows XP. First make sure your Ethernet Adapter is working, refer to the adapter's manual if needed.

1. Install TCP/IP component

1) On the Windows taskbar, click the **Start** button, point to **Settings**, and then click **Control Panel**.

2) Click the **Network and Internet Connections** icon, and then click on the **Network Connections** tab in the appearing window.

3) Right click the icon that showed below, select Properties on the prompt page.

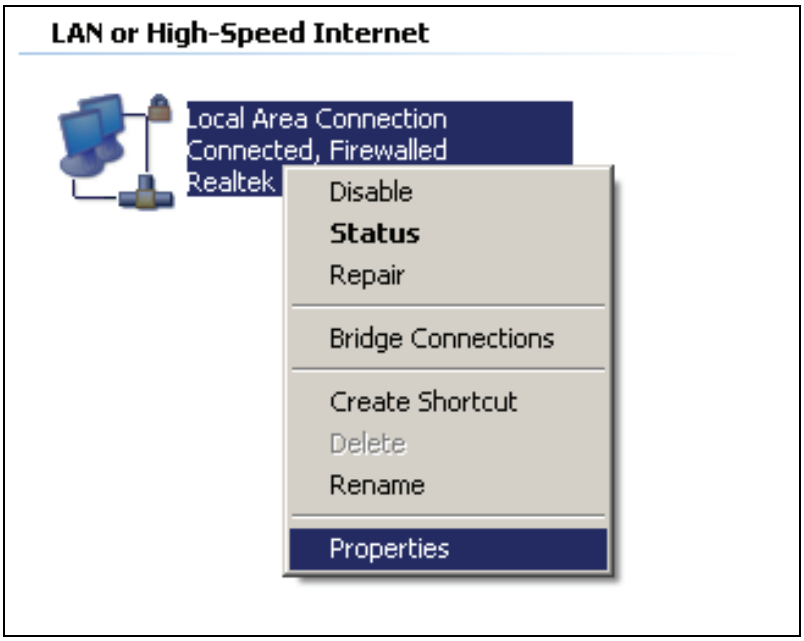


Figure B-1

4) In the prompt page that showed below, double click on the **Internet Protocol (TCP/IP)**.

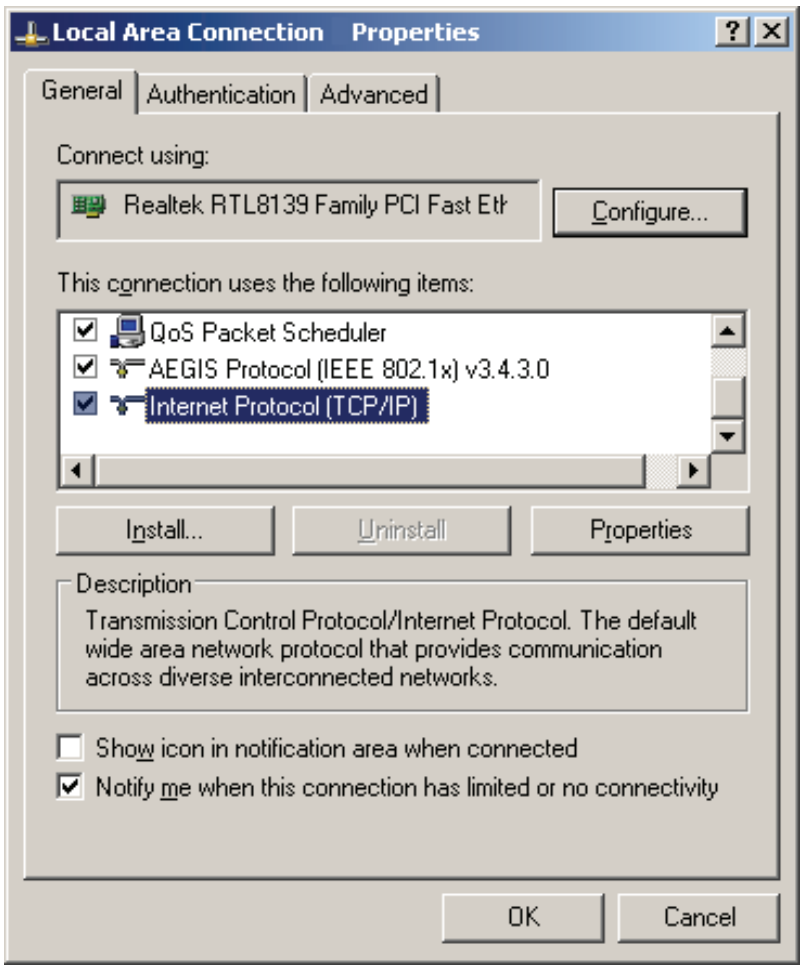


Figure B-2

5) The following **TCP/IP Properties** window will display and the **IP Address** tab is open on this window by default.

Now you have two ways to configure the **TCP/IP** protocol below:

- **Setting IP address automatically**

Select **Obtain an IP address automatically**, Choose **Obtain DNS server automatically**, as shown in the Figure below:

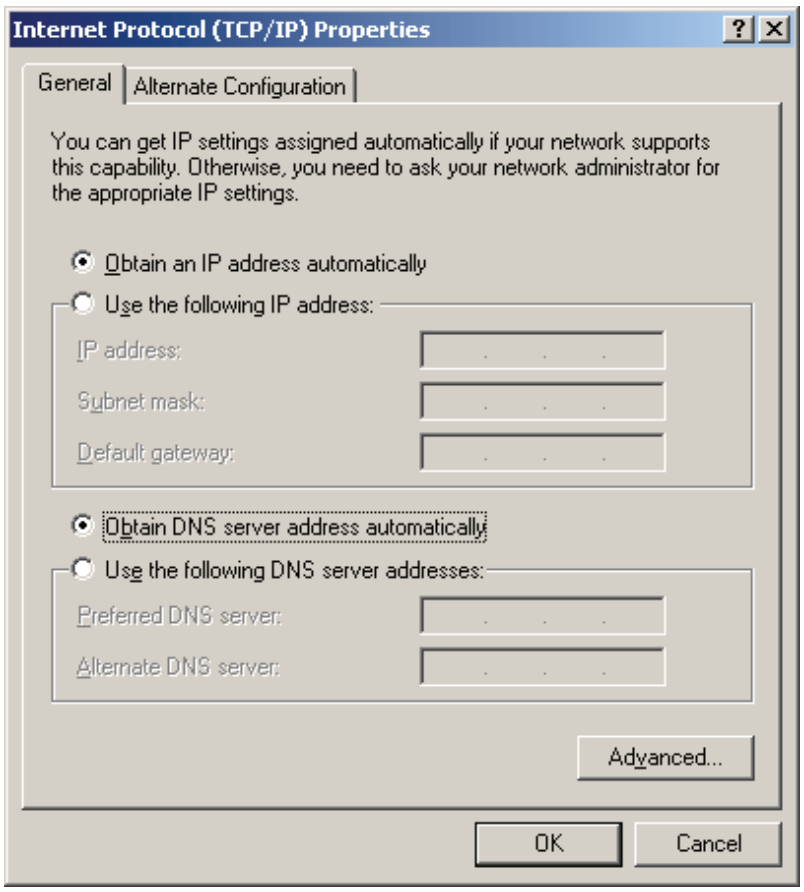


Figure B-3

➢ **Setting IP address manually**

1 Select **Use the following IP address** radio button. And the following items available

2 If the router's LAN IP address is 192.168.1.1, type IP address is 192.168.1.x (x is from 2 to 254), and **Subnet mask** is 255.255.255.0.

3 Type the router's LAN IP address (the default IP is 192.168.1.1) into the **Default gateway** field.

4 Select **Use the following DNS server addresses** radio button. In the **Preferred DNS Server** field you can type the DNS server IP address, which has been provided by your ISP

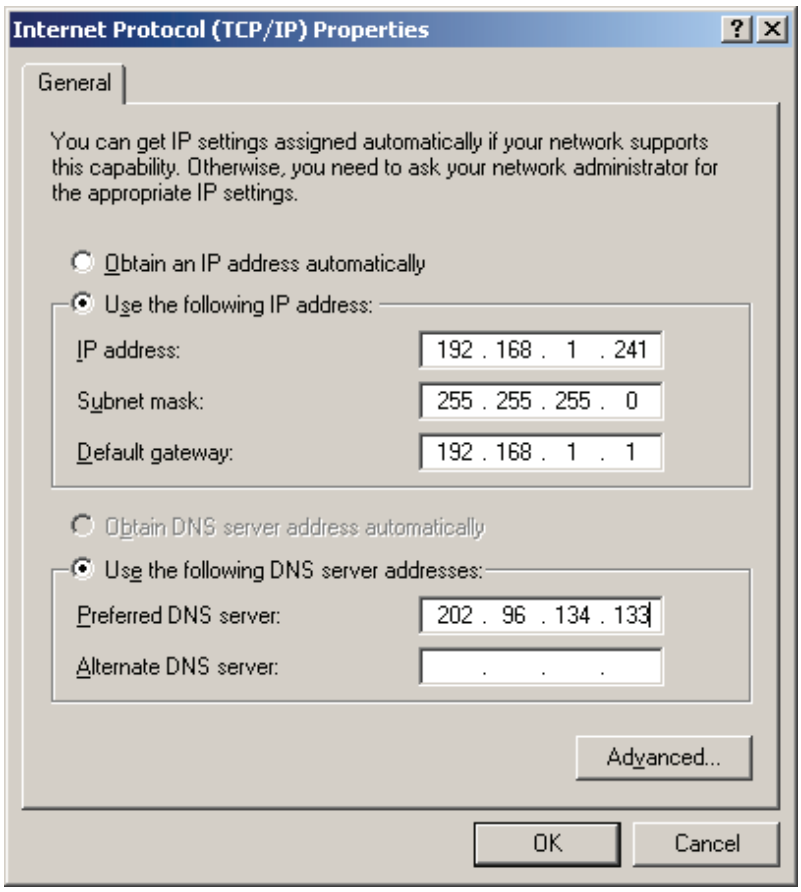

Internet Protocol (TCP/IP) Properties
General
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.
Obtain an IP address automatically
Use the following IP address:
IP address: 192 . 168 . 1 . 241
Subnet mask: 255 . 255 . 255 . 0
Default gateway: 192 . 168 . 1 . 1
Obtain DNS server address automatically
Use the following DNS server addresses:
Preferred DNS server: 202 . 96 . 134 . 133
Alternate DNS server:
Advanced...
OK
Cancel

Figure B-4

Appendix C: Specifications

General	
Standards	IEEE 802.3, 802.3u, 802.11b, 802.11g and 802.11n (draft 2.0)
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: UTP category 3, 4, 5 cable (maximum 100m) EIA/TIA-568 100Ω STP (maximum 100m)
	100BASE-TX: UTP category 5, 5e cable (maximum 100m) EIA/TIA-568 100Ω STP (maximum 100m)
LEDs	Power, System, WLAN, WAN, LAN (1-4), QSS
Safety & Emissions	FCC, CE
Wireless	
Frequency Band	2.4~2.4835GHz
Radio Data Rate	11n：up to 300Mbps（Automatic） 11g：54/48/36/24/18/12/9/6M（Automatic） 11b：11/5.5/2/1M（Automatic）
Channels	13
Frequency Expansion	DSSS(Direct Sequence Spread Spectrum)
Modulation	DBPSK, DQPSK, CCK, OFDM, 16-QAM, 64-QAM
Security	WEP/WPA/WPA2/WPA2-PSK/WPA-PSK
Sensitivity @PER	270M: -68dBm@10% PER; 130M: -68dBm@10% PER 108M: -68dBm@10% PER; 54M: -68dBm@10% PER 11M: -85dBm@8% PER; 6M: -88dBm@10% PER 1M: -90dBm@8% PER
RF Power	20dBm(max)
Antenna Gain	2dBi * 2
Environmental and Physical	
Temperature.	Operating : 0℃~40℃ (32℉~104℉)
	Storage: -40℃~70℃(-40℉~158℉)
Humidity	Operating: 10% - 90% RH, Non-condensing
	Storage: 5% - 90% RH, Non-condensing

Appendix D: Glossary

- **802.11n -** 802.11n builds upon previous 802.11 standards by adding MIMO (multiple-input multiple-output). MIMO uses multiple transmitter and receiver antennas to allow for increased data throughput via spatial multiplexing and increased range by exploiting the spatial diversity, perhaps through coding schemes like Alamouti coding. The Enhanced Wireless Consortium (EWC) [3] was formed to help accelerate the IEEE 802.11n development process and promote a technology specification for interoperability of next-generation wireless local area networking (WLAN) products.
- **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 -** 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** (**D**ynamic **D**omain **N**ame **S**ystem) **-** The capability of assigning a fixed host and domain name to a dynamic Internet IP Address.
- **DHCP** (**D**ynamic **H**ost **C**onfiguration **P**rotocol) **-** A protocol that automatically configure the TCP/IP parameters for the all the PC(s) that are connected to a DHCP server.
- **DMZ** (**D**e**m**ilitarized **Z**one) **-** 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** (**D**omain **N**ame **S**ystem) **–** 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.
- **DSL** (**D**igital **S**ubscriber **L**ine) **-** A technology that allows data to be sent or received over existing traditional phone lines.
- **ISP** (**I**nternet **S**ervice **P**rovider) **-** 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** (**N**etwork **A**ddress **T**ranslation) **-** NAT technology translates IP addresses of a local area network to a different IP address for the Internet.

- **PPPoE** (**P**oint to **P**oint **P**rotocol **o**ver **E**thernet) **-** PPPoE is a protocol for connecting remote hosts to the Internet over an always-on connection by simulating a dial-up connection.
- **SSID -** A **S**ervice **S**et **Id**entification 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** (**W**ired **E**quivalent **P**rivacy) **-** 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** (**W**ireless **L**ocal **A**rea **N**etwork) **-** A group of computers and associated devices communicate with each other wirelessly, which network serving users are limited in a local area.