User Guide

TL-WR543G

54M Wireless AP Client Router

- 2x to 3x eXtended Range™
- 2.4GHz • 802.11g/b

Rev: 1.0.1

COPYRIGHT & TRADEMARKS

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.”

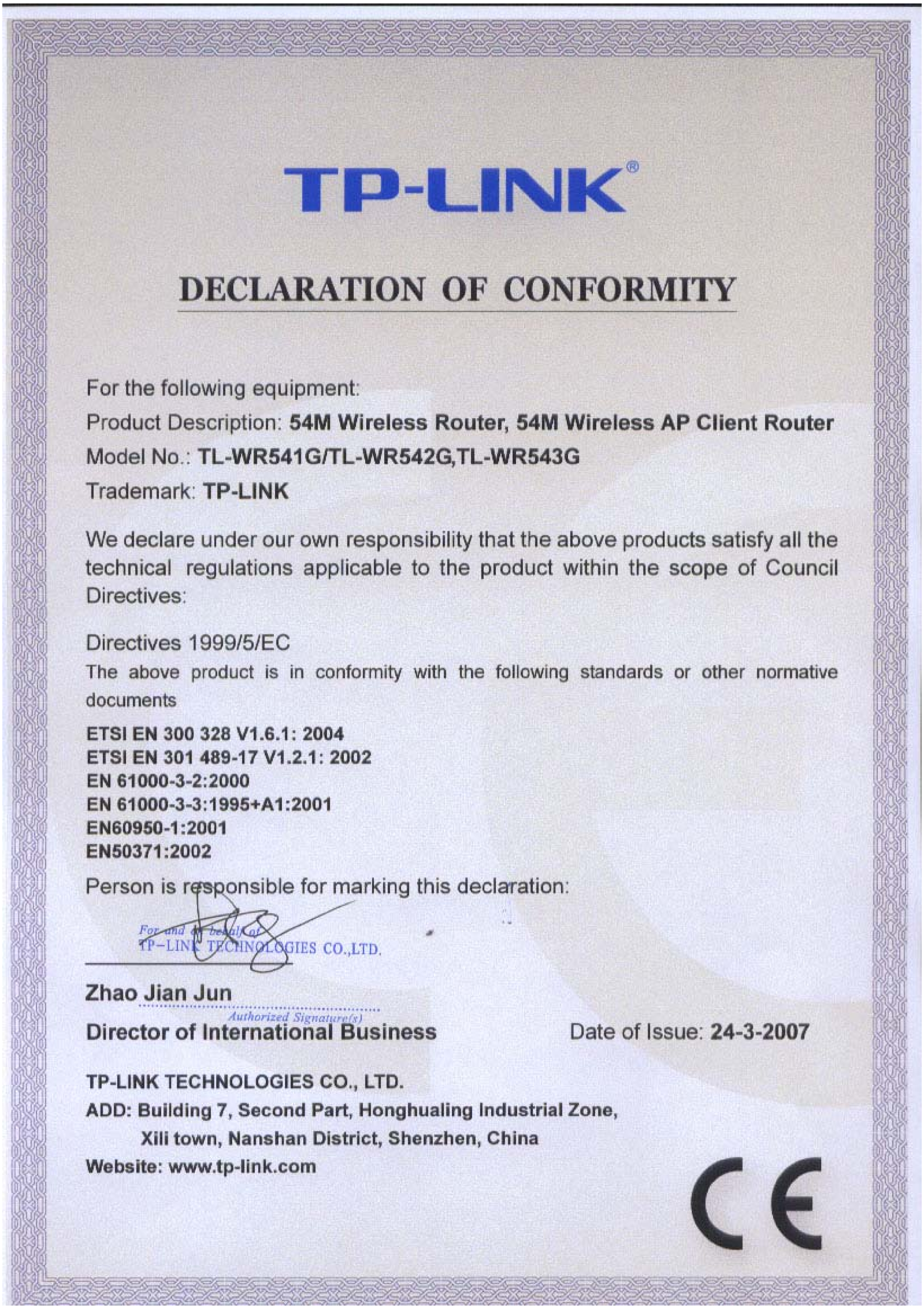
CE Mark Warning

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

2400.0-2483.5 MHz

Country	**Restriction**	**Reason/remark**
Bulgaria		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		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		Only for indoor applications



TP-LINK®

DECLARATION OF CONFORMITY

For the following equipment:

Product Description: **54M Wireless Router, 54M Wireless AP Client Router**

Model No.: **TL-WR541G/TL-WR542G,TL-WR543G**

Trademark: **TP-LINK**

We declare under our own responsibility that the above products satisfy all the technical regulations applicable to the product within the scope of Council Directives:

Directives 1999/5/EC

The above product is in conformity with the following standards or other normative documents

ETSI EN 300 328 V1.6.1: 2004
ETSI EN 301 489-17 V1.2.1: 2002
EN 61000-3-2:2000
EN 61000-3-3:1995+A1:2001
EN60950-1:2001
EN50371:2002

Person is responsible for marking this declaration:

For and on behalf of
TP-LINK TECHNOLOGIES CO.,LTD.

Zhao Jian Jun

Authorized Signature(s)

Director of International Business Date of Issue: **24-3-2007**

TP-LINK TECHNOLOGIES CO., LTD.
ADD: Building 7, Second Part, Honghualing Industrial Zone,
Xili town, Nanshan District, Shenzhen, China
Website: www.tp-link.com

CE

Package contents

The following contents should be found in your box:

- One TL-WR543G 54M Wireless AP Client Router
- One AC power Adapter for TL-WR543G 54M Wireless AP Client Router
- One Quick Installation Guide
- One Resource CD for TL-WR543G 54M Wireless AP Client Router, including:
  - This Guide
  - Other Helpful Information

☞ **Note:**

If any of the listed contents are damaged or missing, please contact the retailer from whom you purchased the product for assistance.

COMMENT

Chapter 1 About this Guide

Thank you for choosing the TL-WR543G 54M Wireless AP Client Router. This router provides dedicated solution for Small Office/Home Office (SOHO) networks. With your network all connected, your local wired or wireless network can share the Internet access, files and fun for multiple PC(s) through one ISP account. And if the device works in the AP Client mode, you can access the Internet wirelessly by your WISP's support.

It adopts **2x to 3x eXtended Range™ WLAN transmission technology** so that the transmission distance is 2-3 times of traditional IEEE 802.11g and IEEE 802.11b solutions, up to 855.36m tested in China. The transmission range is extended to 4-9 times.

It is an easy Web-based setup for installation and management. Even though you may not be familiar with the router, this guide will make configuring the router easy. Before installing the router, please look through this guide to know all the router's functions.

1.1 Purposes

This Guide tells you how to use the TL-WR543G 54M Wireless AP Client Router.

1.2 Conventions

The router mentioned in this guide stands for TL-WR543G 54M Wireless AP Client Router.

1.3 Overview of this User Guide

Chapter 1: About this Guide

Chapter 2: Introduction

Chapter 3: Connecting the Router

Chapter 4: Quick Installation Guide

Chapter 5: Configuring the Router

Appendix A: FAQ

Appendix B: Configuring the PC

Appendix C: Specifications

Appendix D: Glossary

Chapter 2 Introduction

2.1 Overview of the Router

The TL-WR543G 54M Wireless AP Client Router integrates 4-port Switch, Firewall, NAT-router and Wireless AP. Its design is dedicated to Small Office/Home Office (SOHO) wireless network solutions. The TL-WR543G 54M Wireless AP Client Router will allow you to connect your network wirelessly better than ever, sharing the Internet Access, files and fun, easily and securely.

The TL-WR543G 54M Wireless AP Client Router provides 2 operation modes for multi-user to access the Internet: AP client router and AP router. In AP client router mode, it can access the Internet wirelessly by your WISP's support. In AP router mode, it can access the Internet via ADSL/Cable Modem.

In the most attentive wireless security, the TL-WR543G 54M Wireless AP Client Router provides multiple protection measures. In AP router mode, it can be set to turn off wireless network name (SSID) broadcast so that only stations that have the SSID can be connected. The router provides wireless LAN 64/128/152-bit WEP encryption security, and WPA/WPA2 and WPA-PSK/WPA2-PSK authentication, as well as TKIP/AES encryption security. It also supports VPN pass-through for sensitive data secure transmission.

The TL-WR543G 54M Wireless AP Client Router complies with the IEEE 802.11g and IEEE 802.11b standards so that the data transmission rate is up to 54Mbps. It adopts **2x to 3x eXtended Range™ WLAN transmission technology** so that the transmission distance is 2-3 times of traditional IEEE 802.11g and IEEE 802.11b solutions, up to a distance of 855.36m tested in China. The transmission range is extended to 4-9 times. It is compatible with all IEEE 802.11g and IEEE 802.11b products.

The TL-WR543G 54M Wireless AP Client Router provides flexible access control in AP router mode so that parents or network administrators can establish restricted access policies for children or staff. It has built-in NAT and DHCP server supporting static IP address distributing. It also supports Virtual Server and DMZ host for Port Triggering needs, and remote management and log so that network administrators can manage and monitor the network in real time. These device supports Bridge mode which can make two APs communicate with each other wirelessly. In addition, it supports Port QoS function which can help you to use the network resource sensible.

The TL-WR543G 54M Wireless AP Client Router is easy-to-manage. Quick Setup is supported and friendly help messages are provided for every step. So you can configure it quickly and share the Internet access, files and fun.

2.2 Features

- Complies with IEEE 802.11g, IEEE 802.11b, IEEE 802.3, IEEE 802.3u standards.
- 1 10/100M Auto-Negotiation RJ45 WAN port, 4 10/100M Auto-Negotiation RJ45 LAN ports, supporting Auto MDI/MDIX.
- Supports AP Client Router and AP Router operation mode.
- Supports WIFI Internet Access (WISP).
- Supports Wireless Distribution System (WDS).
- Adopts 2x to 3x eXtended Range™.
- Wireless Data transfer rates up to 54Mbps.
- Supports Port-based QoS.
- Output transmit power adjustable.
- Supports enabling/disabling the function of eXtended Range™ manually.

- Provides WPA/WPA2 and 64/128/152-bit WEP encryption security.
- Supports PPPoE, Dynamic IP, Static IP, L2TP, PPTP and Big Pond Cable Internet Access. (AP Router mode only)
- Built-in NAT and DHCP server supporting static IP address distributing.
- Supports UPnP, Dynamic DNS, Static Routing, VPN Pass-through.
- Support Port QoS.
- Supports Parental Control, Virtual Server, Special Application and DMZ host.
- Built-in firewall supporting IP address filtering, Domain Name filtering, and MAC address filtering.
- Provides WLAN ACL (Access Control List) (AP Router mode only).
- Supports configuration backup/restore and firmware upgrade.
- Supports Web management.
- Detachable Antenna (reverse SMA connector).

2.3 Panel Layout

2.3.1 The Front Panel

The front panel of the TL-WR543G consists of several LED indicators, which is designed to indicate connections. View from left to right. Table 2-1 describes the LEDs on the front panel of the router.

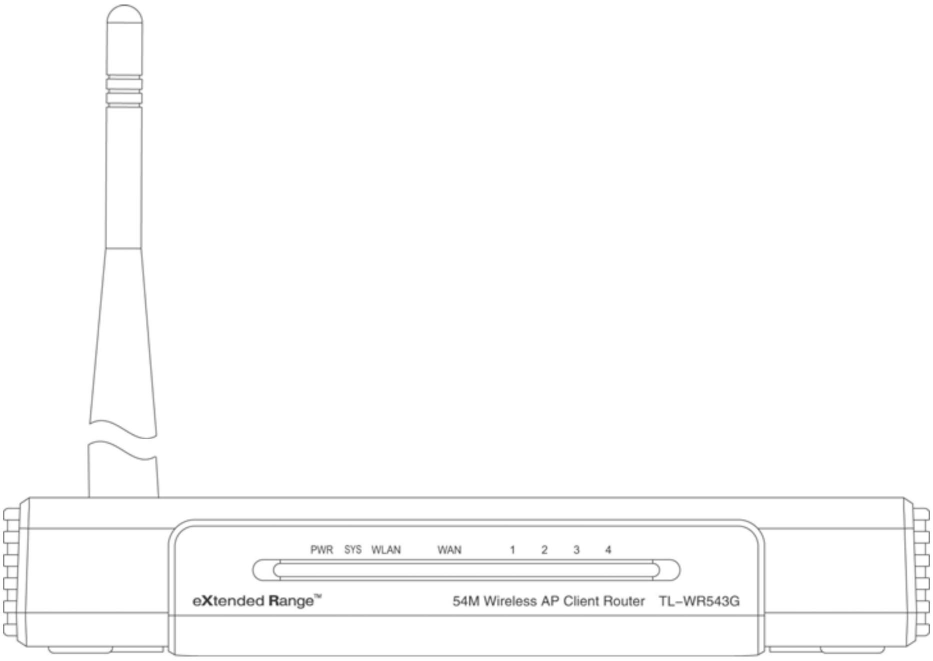


Figure 2-1 Front Panel sketch

2.3.2 LED Explanation

Name	Status	description
PWR	Off	Power off
	On	Power on
SYS	On	The router is initializing
	Flashing	The router is working properly
	Off	The router has a hardware error
WLAN	Off	There is no wireless device linked to the router
	Flashing	The Wireless function is enabled
WAN,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

2.3.3 The Rear Panel

The rear panel contains the following features. (View from left to right)

- AC power socket: Please use the power adapter which is supplied with the TL-WR543G 54M Wireless AP Client Router only, the use of a different adapter may result in product damage.
- Four 10/100Mbps RJ45 LAN ports for connecting the router to the local PC(s)
- RJ45 WAN port for connecting the router to a cable/DSL Modem, or Ethernet
- Factory Default Reset button

  There are two ways to reset 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: First, turn off the router's power. Second, press and hold the default reset button then turn on the router's power, until the SYS LED lights up (about 3 seconds). Last, release the reset button and wait for the router to reboot.

☞ **Note:**

Ensure the router is powered on before it restarts completely.

- Wireless antenna

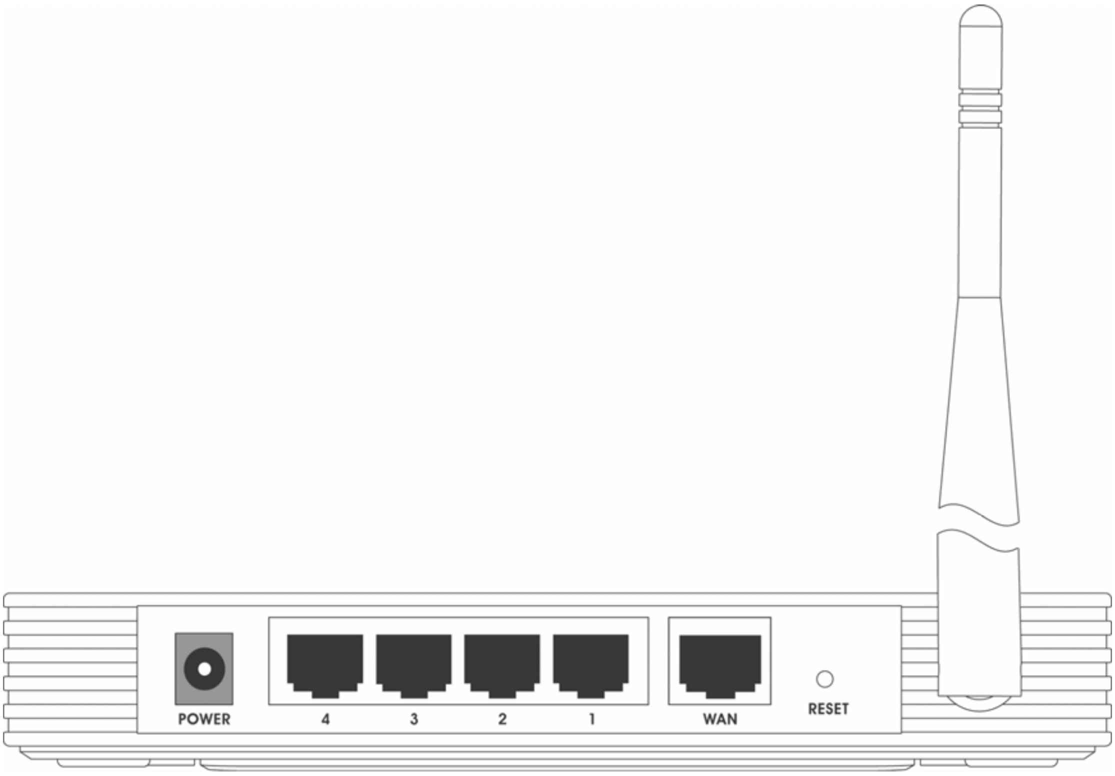


Figure 2-2 Rear Panel sketch

Chapter 3 Connecting the Router

3.1 System Requirements

- Each PC in the LAN needs a working Ethernet Adapter and an Ethernet cable with RJ45 connectors
- TCP/IP protocol must be installed on each PC
- Web browser, such as Microsoft Internet Explorer 5.0 or later, Netscape Navigator 6.0 or later
- If the device is configured to AP client router mode, you also need:
- Wireless Internet Access Service (WISP).
- If the device is configured to AP router mode, you also need:
- Broadband Internet Access Service (DSL/Cable/Ethernet)
- One DSL/Cable Modem that has an RJ45 connector (you do not need it if you connect the router to the Ethernet)

3.2 Installation Environment Requirements

- Do not place in direct sunlight or near a heater or heating vent
- Do not cluttered or crowded. There should be at least 2 inches (5 cm) of clear space on all sides of the router
- Well ventilated (especially if it is in a closet)
- Operating temperature: 0℃~40℃ (32℉~104℉)
- Operating Humidity: 10%~90% RH, Non-condensing

3.3 Connecting the Router

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

1. Power off your PC, Cable/DSL Modem, and the router.
2. Locate an optimum location for the router. The best place is usually near the center of the area in which your PC will connect wirelessly. 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 3-1. (If you have the wireless NIC and want to use wireless function, you can skip this step.)
5. Connect the DSL/Cable Modem to the WAN port on the router, shown in Figure 3-1(If you want your device works in AP Client router mode, you can skip this step).
6. Connect the AC power adapter to the AC 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.

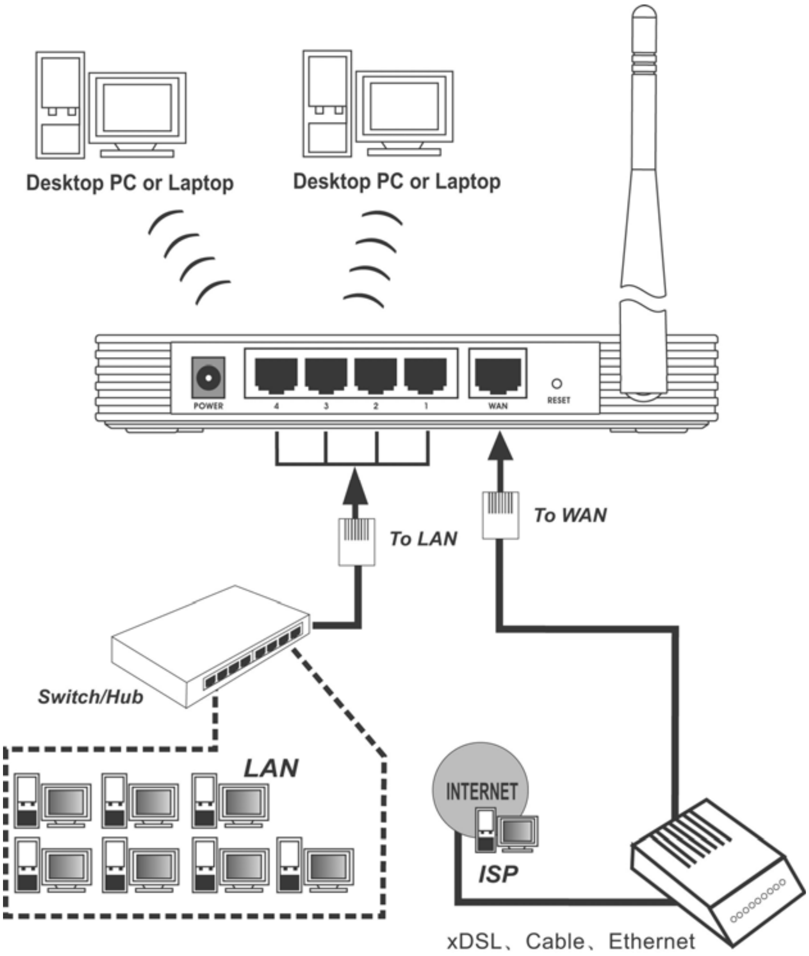


Figure 3-1 Hardware Installation of the TL-WR543G 54M Wireless AP Client Router

Chapter 4 Quick Installation Guide

After connecting the TL-WR543G Router into your network, you should configure it. This chapter describes how to configure the basic functions of your TL-WR543G Wireless AP Client Router. These procedures only take you a few minutes. You can access the Internet via the router immediately after successfully configuring.

4.1 TCP/IP configuration

The default IP address of the TL-WR543G 54M Wireless AP Client Router is 192.168.1.1. And the default Subnet Mask is 255.255.255.0. These values can be seen from the LAN. They can be changed as you desire, as an example we use the default values for description in this guide.

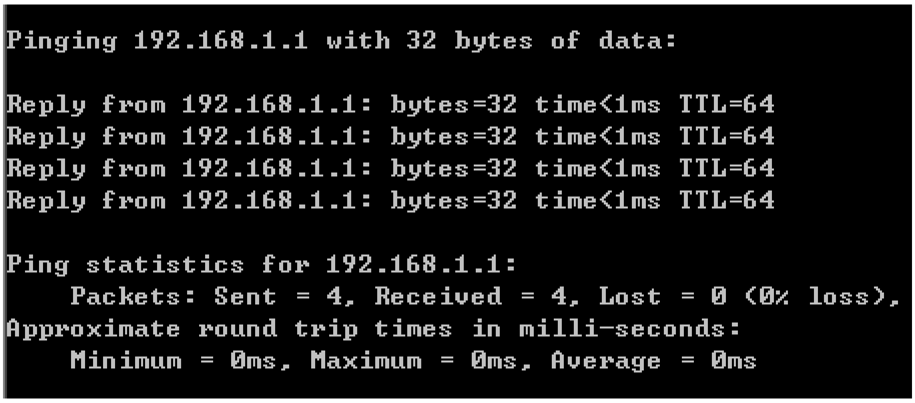
Connect the local PC to the LAN ports of the router. There are then two ways to configure the IP address for your PC.

- 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 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) Power off the router and PC. Then turn on the router and restart the PC. 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 that shown in Figure 4-1, the connection between your PC and the router has been established.



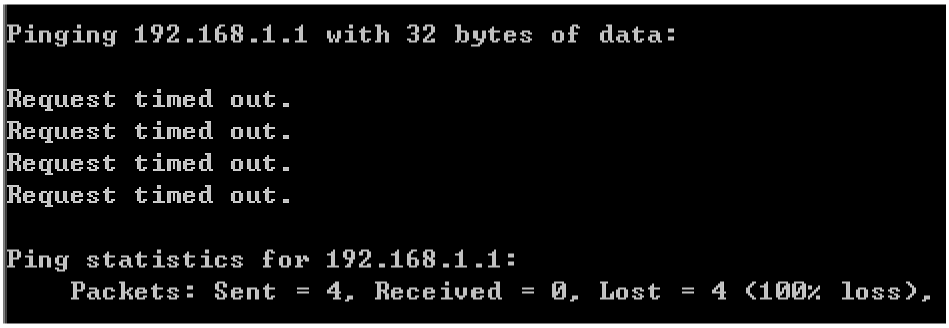
```
Pinging 192.168.1.1 with 32 bytes of data:

Reply from 192.168.1.1: bytes=32 time<1ms TTL=64
Reply from 192.168.1.1: bytes=32 time<1ms TTL=64
Reply from 192.168.1.1: bytes=32 time<1ms TTL=64
Reply from 192.168.1.1: bytes=32 time<1ms TTL=64

Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

Figure 4-1 Success result of Ping command

If the result displayed is similar to that shown in Figure 4-2, it means that your PC has not connected to the router.



```
Pinging 192.168.1.1 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

Figure 4-2 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 port 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, the gateway must be 192.168.1.1

4.2 Quick Installation Guide

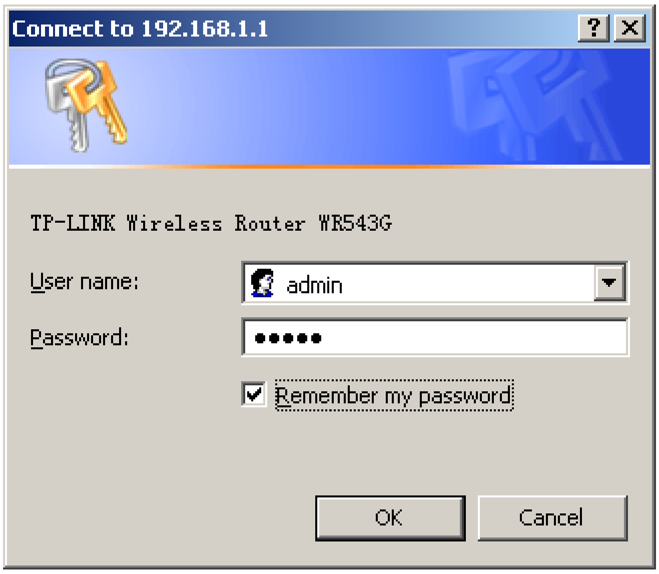
With a Web-based (Internet Explorer or Netscape® Navigator) utility, it is easy to configure and manage the TL-WR543G 54M Wireless AP Client Router. The Web-based utility can be used on any Windows, Macintosh or UNIX OS with a Web browser.

Connect to the router by typing *http://192.168.1.1* in the address field of Web browser.

Address http://192.168.1.1

Figure 4-3 Login the router

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



Connect to 192.168.1.1

TP-LINK Wireless Router WR543G

User name: admin

Password: •••••

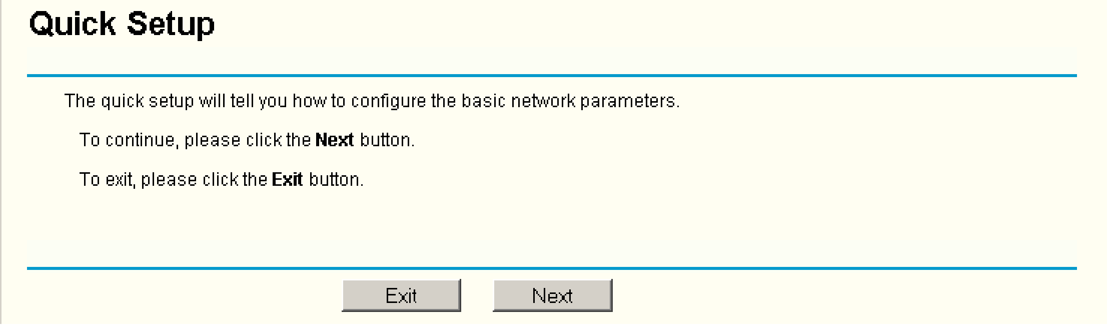
☑ Remember my password

Figure 4-4 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.

If the User Name and Password are correct, you can configure the router using the Web browser. Please click the **Quick Setup** link on the left of the main menu and the Quick Setup screen will appear.



Quick Setup

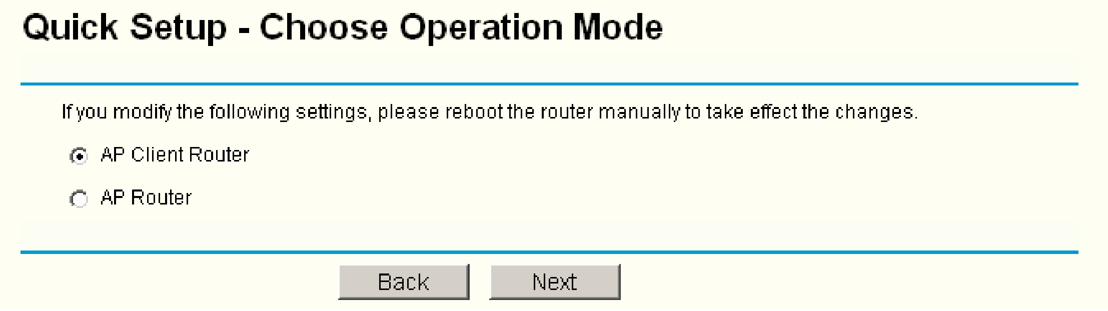
The quick setup will tell you how to configure the basic network parameters.

To continue, please click the **Next** button.

To exit, please click the **Exit** button.

Figure 4-5 Quick Setup

Click Next, and then **Choose Operation mode** page will appear, shown in Figure 4-6:



Quick Setup - Choose Operation Mode

If you modify the following settings, please reboot the router manually to take effect the changes.

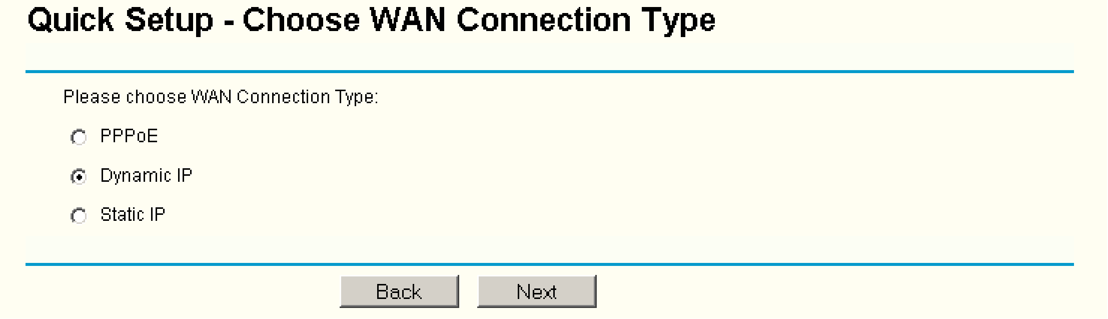
● AP Client Router

○ AP Router

Figure 4-6 Choose Operation mode

The router supports two mode2 operation modes for multi-user to access the Internet: AP client router and AP router. In AP client router mode, it can access the Internet wirelessly by your WISP's support. In AP router mode, it can access the Internet via ADSL/Cable Modem.

Click **Next**, and then **Choose WAN Connection Type** page will appear, shown in Figure 4-7:



Quick Setup - Choose WAN Connection Type

Please choose WAN Connection Type:

○ PPPoE

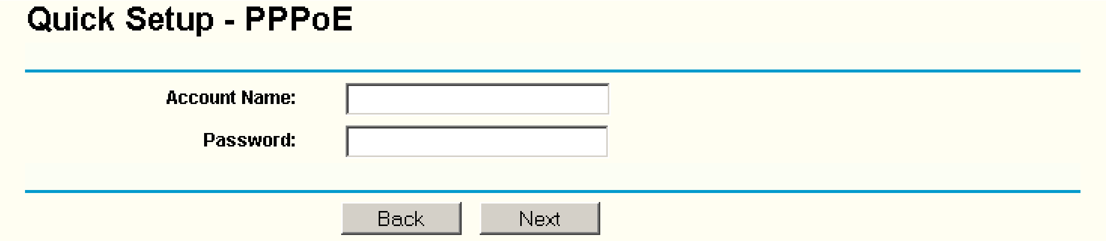
● Dynamic IP

○ Static IP

Figure 4-7 Choose WAN Connection Type

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

If you choose "**PPPoE**", you will see this page shown in Figure 4-8:



Quick Setup - PPPoE

Account Name:

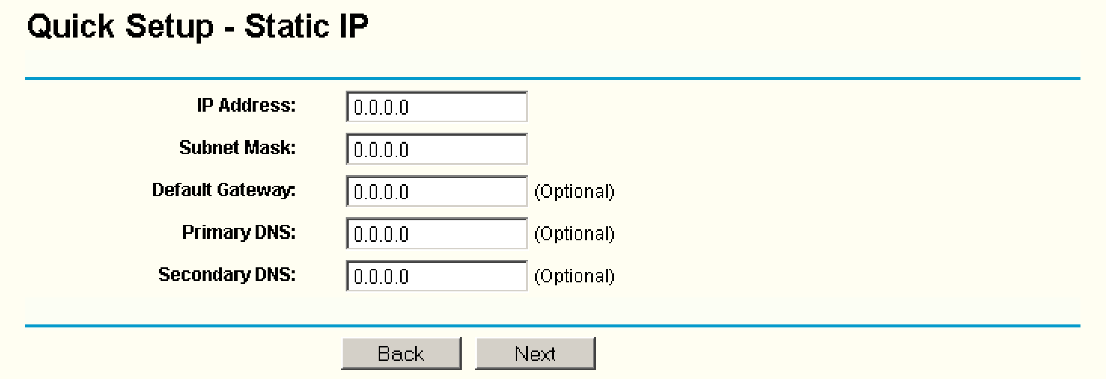
Password:

Figure 4-8 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.

If you choose "**Dynamic IP**", the router will automatically receive the IP parameters from your ISP without needing to enter any parameters.

If you Choose "**Static IP**", the Static IP settings page will appear, shown in Figure 4-9:



Quick Setup - Static IP

IP Address: 0.0.0.0

Subnet Mask: 0.0.0.0

Default Gateway: 0.0.0.0 (Optional)

Primary DNS: 0.0.0.0 (Optional)

Secondary DNS: 0.0.0.0 (Optional)

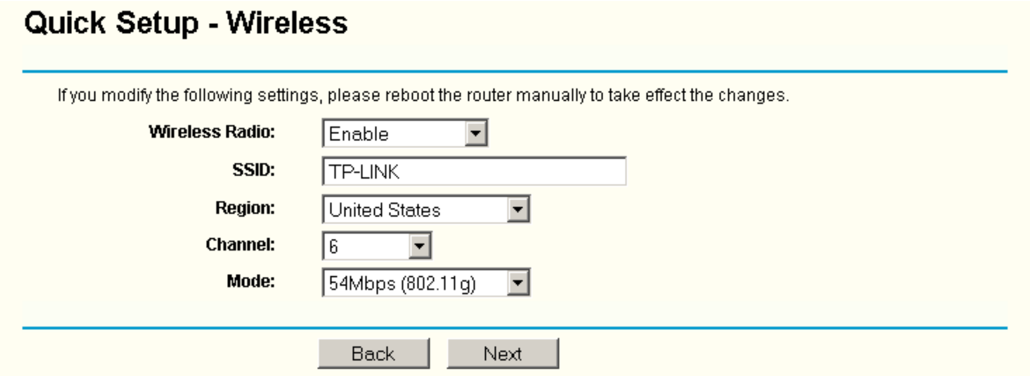
Figure 4-9 Quick Setup - Static IP

☞ **Note:**

The IP parameters should have been provided by your ISP.

- **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 boxes if required.
- **Secondary DNS -** If your ISP provides another DNS server, enter it into this field.

After you complete the above, click **Next**, the Wireless settings page will appear below.



Quick Setup - Wireless

If you modify the following settings, please reboot the router manually to take effect the changes.

Wireless Radio: Enable

SSID: TP-LINK

Region: United States

Channel: 6

Mode: 54Mbps (802.11g)

Figure 4-10 Quick Setup - Wireless settings

In this page, you can configure the following wireless parameters:

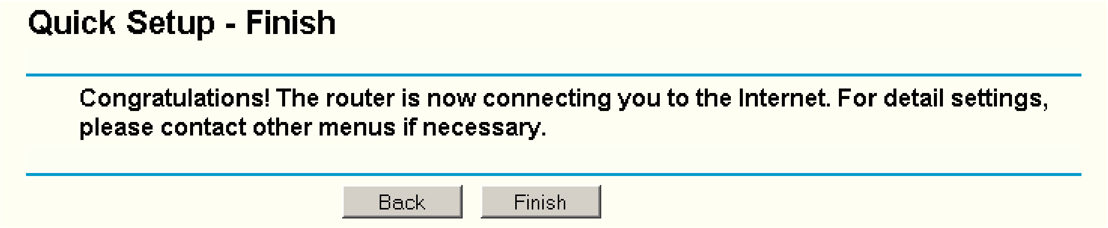
- **Wireless Radio -** Indicates whether the Access Point feature of the router is enabled or disabled. If disabled, the WLAN LED on the front panel will not be lit and the wireless stations will not be able to access the router. If enabled, the WLAN LED will be lit up and wireless stations will be able to access the router.
- **SSID -** Enter a value of up to 32 characters. The same SSID must be assigned to all wireless devices on your network. The default SSID is TP-LINK. 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.
- **Channel -** The current channel in use. This field determines which operating frequency will be used.
- **Mode -** Indicates the current mode **54Mbps (802.11g)**, **11Mbps (802.11b)**. If you select **54Mbps (802.11g)**, it is compatible with **11Mbps (802.11b)**.

These settings are only for basic wireless parameters, for advanced settings, please refer to Section 5.5: "Wireless."

☞ **Note:**

The change of wireless settings won't take effect until the router reboots! You can reboot it manually. If you need instructions as to how to do this, please refer to Section 5.11.5: "Rebooting the Router"

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



Quick Setup - Finish

Congratulations! The router is now connecting you to the Internet. For detail settings, please contact other menus if necessary.

Figure 4-11 Quick Setup - Finish

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

Chapter 5 Configuring the Router

This chapter describes each Web page's key functions.

5.1 Login

After your successful login, you can configure and manage the router. There are eleven main menus on the left of the Web-based utility. Submenus will be available after you click one of the main menus. The eleven main menus are: **Status, Quick Setup, Operation Mode, Network, Wireless, DHCP, Forwarding, Security, Static Routing, DDNS and System Tools.** On the right of the Web-based utility, there are the detailed explanations and instructions for the corresponding page. To apply any settings you have altered on the page, please click the **Save** button.

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

5.2 Status

The Status page displays the router's current status and configuration. All information is read-only.

1. **LAN**

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

2. **Wireless**

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

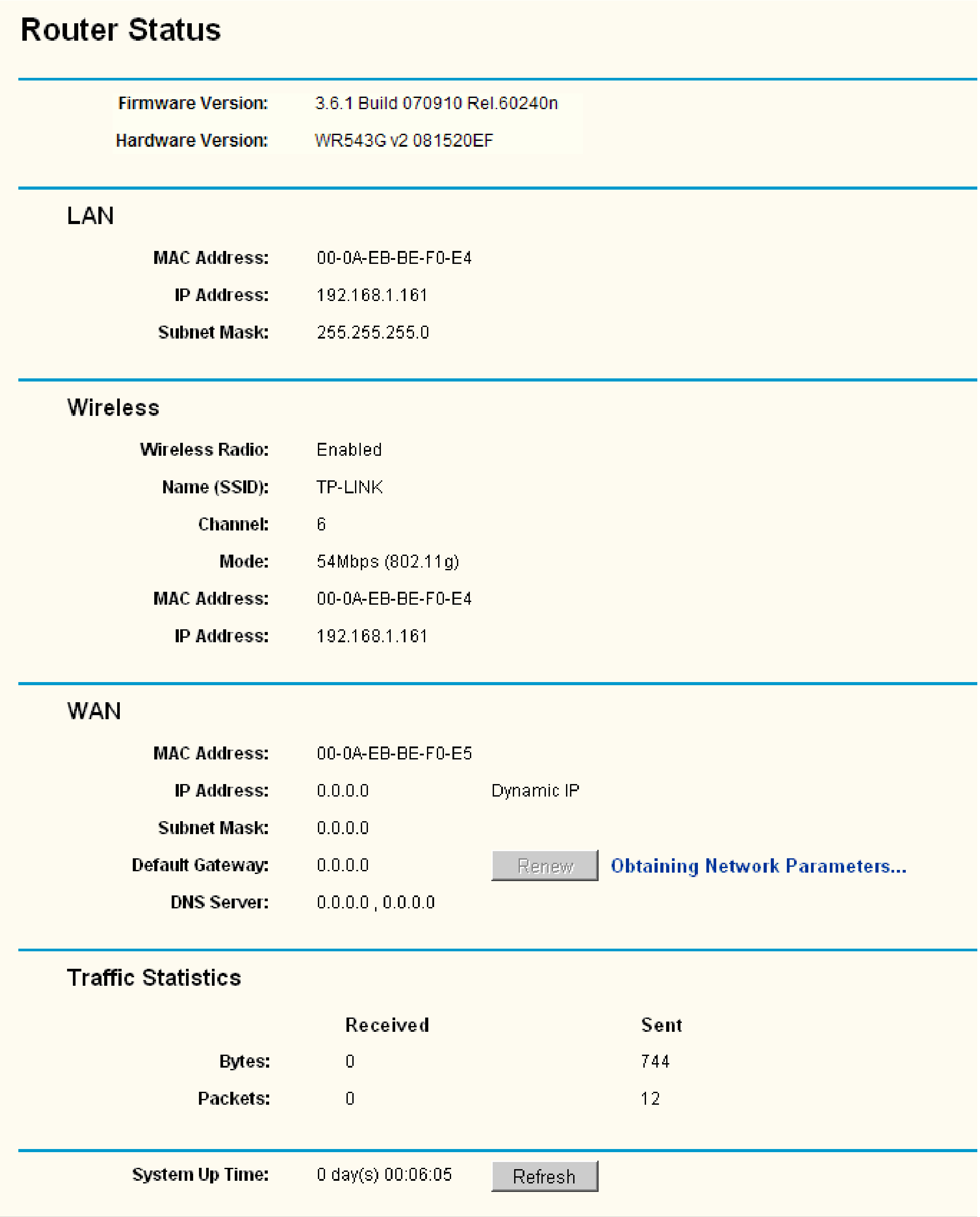
3. **WAN**

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

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

4. **System Up Time**

   The total up time of the router from when it was switched on or reset.



Router Status

Firmware Version:	3.6.1 Build 070910 Rel.60240n	
Hardware Version:	WR543G v2 081520EF	

LAN

MAC Address:	00-0A-EB-BE-F0-E4
IP Address:	192.168.1.161
Subnet Mask:	255.255.255.0

Wireless

Wireless Radio:	Enabled
Name (SSID):	TP-LINK
Channel:	6
Mode:	54Mbps (802.11g)
MAC Address:	00-0A-EB-BE-F0-E4
IP Address:	192.168.1.161

WAN

MAC Address:	00-0A-EB-BE-F0-E5	
IP Address:	0.0.0.0	Dynamic IP
Subnet Mask:	0.0.0.0	
Default Gateway:	0.0.0.0	Renew Obtaining Network Parameters...
DNS Server:	0.0.0.0 , 0.0.0.0	

Traffic Statistics

	Received	Sent
Bytes:	0	744
Packets:	0	12

System Up Time: 0 day(s) 00:06:05

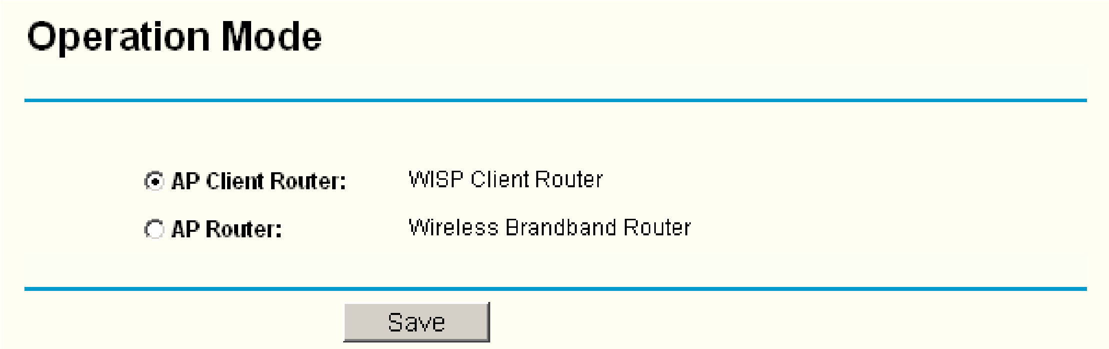
Figure 5-1 Router Status

5.3 Quick Setup

Please refer to Section 4.2: "Quick Installation Guide."

5.4 Operation Mode

The router supports two operation modes, **AP Client Router** and **AP Router**. Please select one your want. Click **Save** to save your choice. (The default mode is **AP Client Router**). Figure 5-2:



Operation Mode

● AP Client Router: WISP Client Router

○ AP Router: Wireless Brandband Router

Figure 5-2 Operation Mode

- **AP Client Router:** In this mode, the device enables multi-user to share the Internet from WISP. All LAN ports share the same IP from WISP through Wireless port. While connecting to WISP, the Wireless port works as a WAN port in AP Client mode. The Ethernet WAN port is automatically disabled. The WAN Connection Type can be setup in **WAN** page by using Dynamic IP, Static IP, PPPoE, L2TP, and PPTP.

- **AP Router:** In this mode, the device enables multi-user to share the Internet via ADSL/Cable Modem. All LAN ports and the wireless port share the same IP to ISP through Ethernet WAN port. The Wireless port acts same as a LAN port while in AP mode. The WAN Connection Type can be setup in **WAN** page by using Dynamic IP, Static IP, PPPoE, 802.1X + Dynamic IP, 802.1X + Static IP, Big Pond Cable, L2TP, PPTP.

5.5 Network

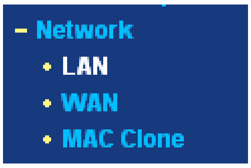
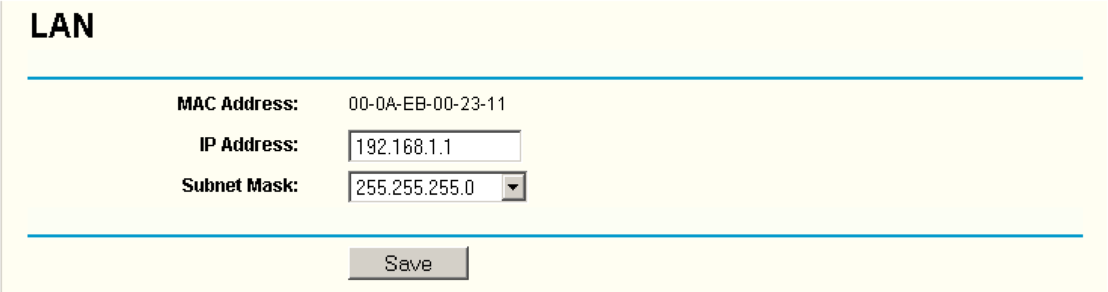


Figure 5-3 the Network menu

There are three submenus under the Network menu (shown in Figure 5-3): **LAN**, **WAN** and **MAC Clone.** Click any of them, and you will be able to configure the corresponding function. The detailed explanations for each submenu are provided below.

5.5.1 LAN

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



LAN

MAC Address: 00-0A-EB-00-23-11

IP Address: 192.168.1.1

Subnet Mask: 255.255.255.0

Figure 5-4 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 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 not take effect, until they are re-configured.

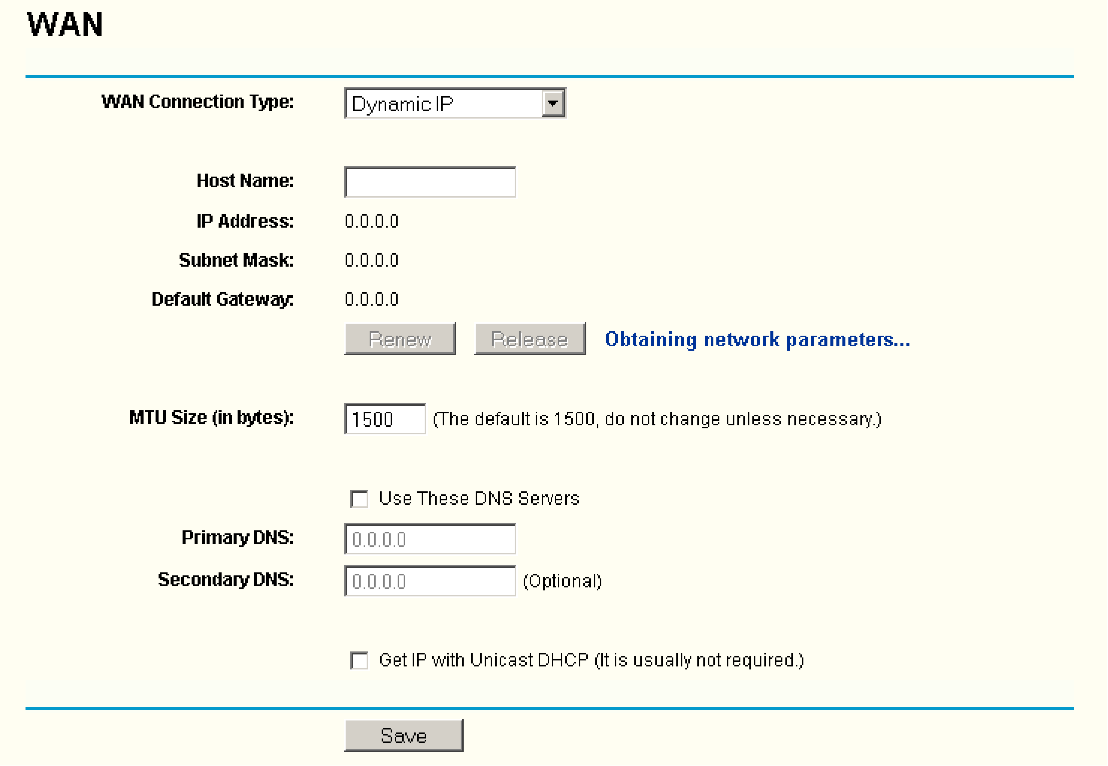
c. If the new LAN IP Address you set is not in the same subnet, the Virtual Server and DMZ Host will change accordingly at the same time.

5.5.2 WAN

You can configure the WAN port parameters on this page.

First, please choose the WAN Connection Type (Dynamic IP/Static IP/PPPoE/802.1X + Dynamic IP/802.1X + Static IP/Big Pond Cable/L2TP/PPTP) for the Internet. If the device works in the AP Client mode, it only provides five kinds of connection type, "Dynamic IP", "Static IP", "PPPoE", "L2TP", and "PPTP". The default type is **Dynamic IP**. If you aren't given any login parameters (fixed IP Address, logging ID, etc), please select **Dynsamic IP**. If you are given a fixed IP (static IP), please select **Static IP**. If you are given a user name and a password, please select the type of your ISP provided (PPPoE/BigPond/L2TP/PPTP). If you are not sure which connection type you use currently, please contact your ISP to obtain the correct information.

1. If you choose **Dynamic IP,** the router will automatically get IP parameters from your ISP. You can see the page as follows (Figure 5-5):



WAN

WAN Connection Type: Dynamic IP

Host Name:

IP Address: 0.0.0.0

Subnet Mask: 0.0.0.0

Default Gateway: 0.0.0.0

Renew Release **Obtaining network parameters...**

MTU Size (in bytes): 1500 (The default is 1500, do not change unless necessary.)

□ Use These DNS Servers

Primary DNS: 0.0.0.0

Secondary DNS: 0.0.0.0 (Optional)

□ Get IP with Unicast DHCP (It is usually not required.)

Save

Figure 5-5 WAN – Dynamic IP

This page displays the WAN IP parameters assigned dynamically by your ISP, including IP address, Subnet Mask, Default Gateway, etc. Clicks 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. For some ISPs you need to reduce the MTU. But this is rarely required, and should not be done unless you are sure it is necessary for your ISP connection.

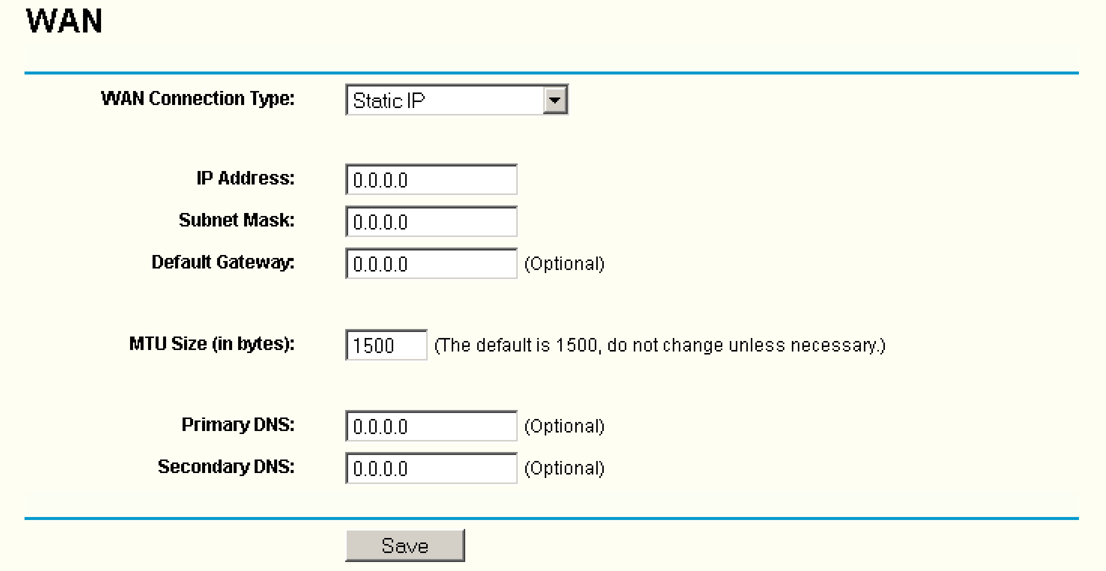
If your ISP gives you one or two DNS addresses, select **Use These DNS Servers** and enter the primary and secondary addresses into the correct fields. Otherwise, the DNS servers will be assigned dynamically from your ISP.

☞ **Note:**

If you get address and find error when you go to a Web site, 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. (This is rarely required.)

2. If you choose **Static IP,** you should have fixed IP Parameters specified by your ISP. The Static IP settings page will appear, shown in Figure 5-6:



WAN

WAN Connection Type: Static IP

IP Address: 0.0.0.0

Subnet Mask: 0.0.0.0

Default Gateway: 0.0.0.0 (Optional)

MTU Size (in bytes): 1500 (The default is 1500, do not change unless necessary.)

Primary DNS: 0.0.0.0 (Optional)

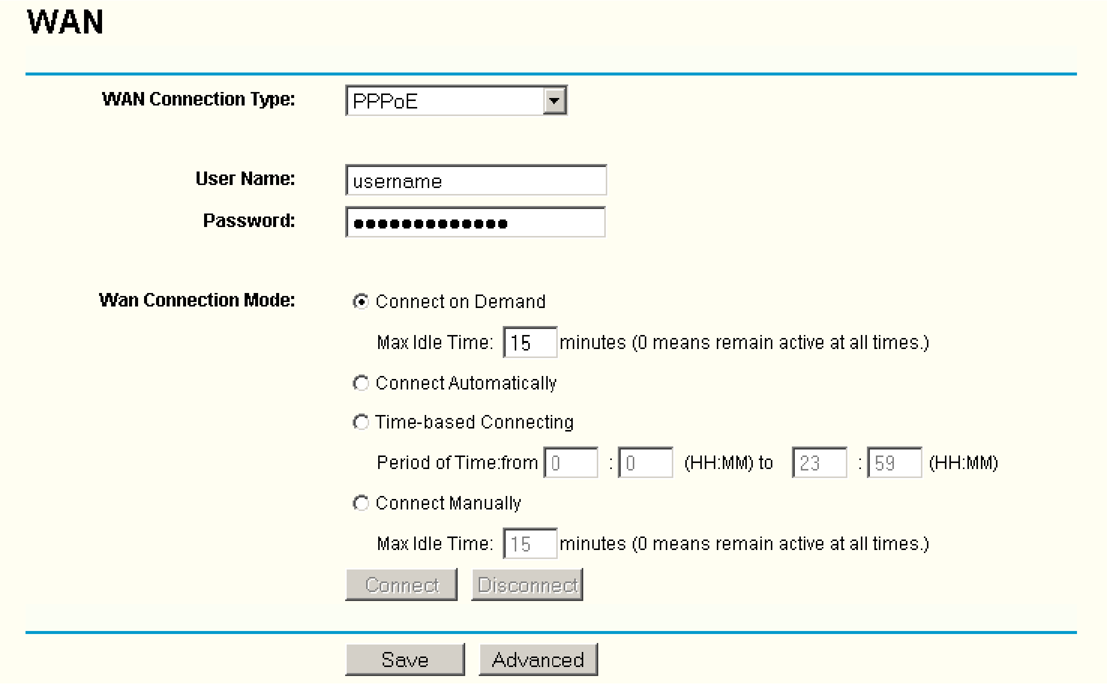
Secondary DNS: 0.0.0.0 (Optional)

Figure 5-6 WAN - Static IP

You should type the following parameters into the spaces provided:

- **IP Address -** Enter the IP address in dotted-decimal notation provided by your ISP.
- **Subnet Mask -** Enter the subnet Mask in dotted-decimal notation provided by your ISP, 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. For some ISPs you may need to modify the MTU. But this is rarely required, and should not be done unless you are sure it is necessary for your ISP connection.
- **Primary DNS -** (Optional) Enter the DNS address in dotted-decimal notation provided by your ISP.
- **Secondary DNS -** (Optional) Type another DNS address in dotted-decimal notation provided by your ISP if provided.

3. If you choose **PPPoE,** you should enter the following parameters (Figure 5-7):



WAN

WAN Connection Type: PPPoE

User Name: username

Password: ●●●●●●●●●●●●●

Wan Connection Mode:
● Connect on Demand
Max Idle Time: 15 minutes (0 means remain active at all times.)
○ Connect Automatically
○ Time-based Connecting
Period of Time:from 0 : 0 (HH:MM) to 23 : 59 (HH:MM)
○ Connect Manually
Max Idle Time: 15 minutes (0 means remain active at all times.)

Figure 5-7 WAN - PPPoE

- **User Name/Password -** Enter the User Name and Password provided by your ISP. These fields are case-sensitive.
- **Connect on Demand -** You can configure the router to disconnect your Internet connection after a specified period of inactivity (**Max Idle Time**). If your Internet connection has been terminated due to inactivity, **Connect on Demand** enables the router to automatically re-establish your connection as soon as you attempt to access the Internet again. If you wish to activate **Connect on Demand**, click the radio button. If you want your Internet connection to remain active at all times, enter 0 in the **Max Idle Time** field. Otherwise, enter the number of minutes you want to have elapsed before your Internet connection terminates.

  Caution: Sometimes the connection cannot be disconnected although you specify a time to Max Idle Time, since some applications is visiting the Internet continually in the background.
- **Connect Automatically -** Connect automatically after the router is disconnected. To use this option, click the radio button.
- **Time-based Connecting -** You can configure the router to make it connect or disconnect based on time. Enter the start time in HH:MM format for connecting and end time in HH:MM format for disconnecting in the **Period of Time** fields.

☞ **Note:**

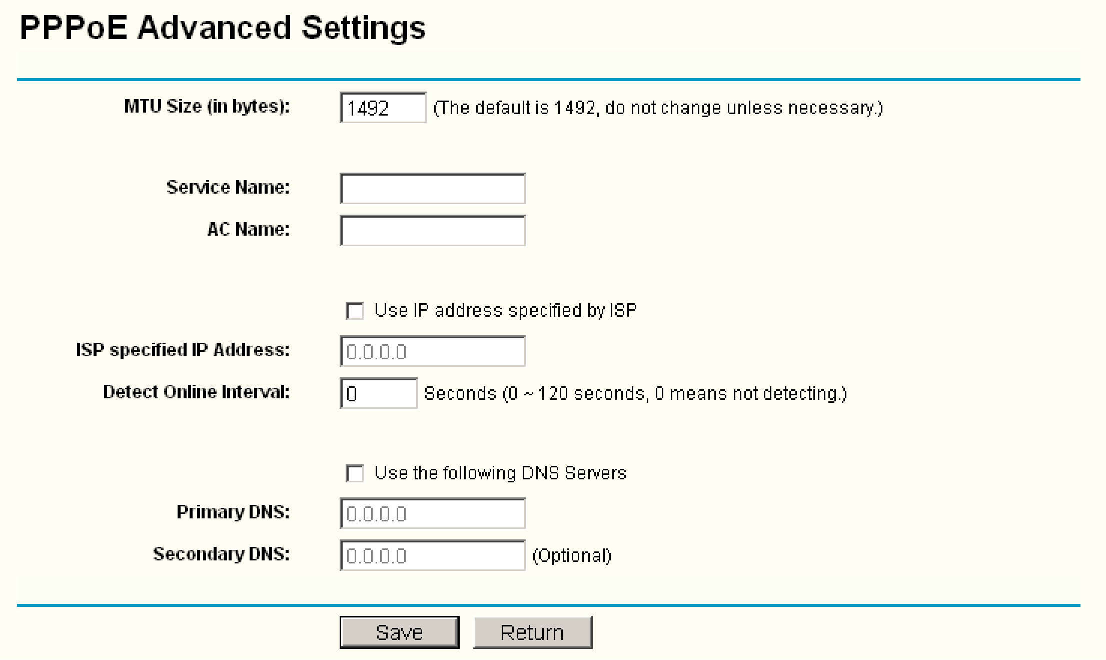
Only when you have configured the system time on **System Tools -> Time** page, will the **Time-based Connecting** function can take effect.

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

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

Click the **Connect** button to connect immediately, Click the **Disconnect** button to disconnect immediately.

Click the **Advanced Settings** button to set up the advanced option, the page shown in Figure 5-8 will then appear:



PPPoE Advanced Settings

MTU Size (in bytes): 1492 (The default is 1492, do not change unless necessary.)

Service Name:

AC Name:

□ Use IP address specified by ISP

ISP specified IP Address: 0.0.0.0

Detect Online Interval: 0 Seconds (0 ~ 120 seconds, 0 means not detecting.)

□ Use the following DNS Servers

Primary DNS: 0.0.0.0

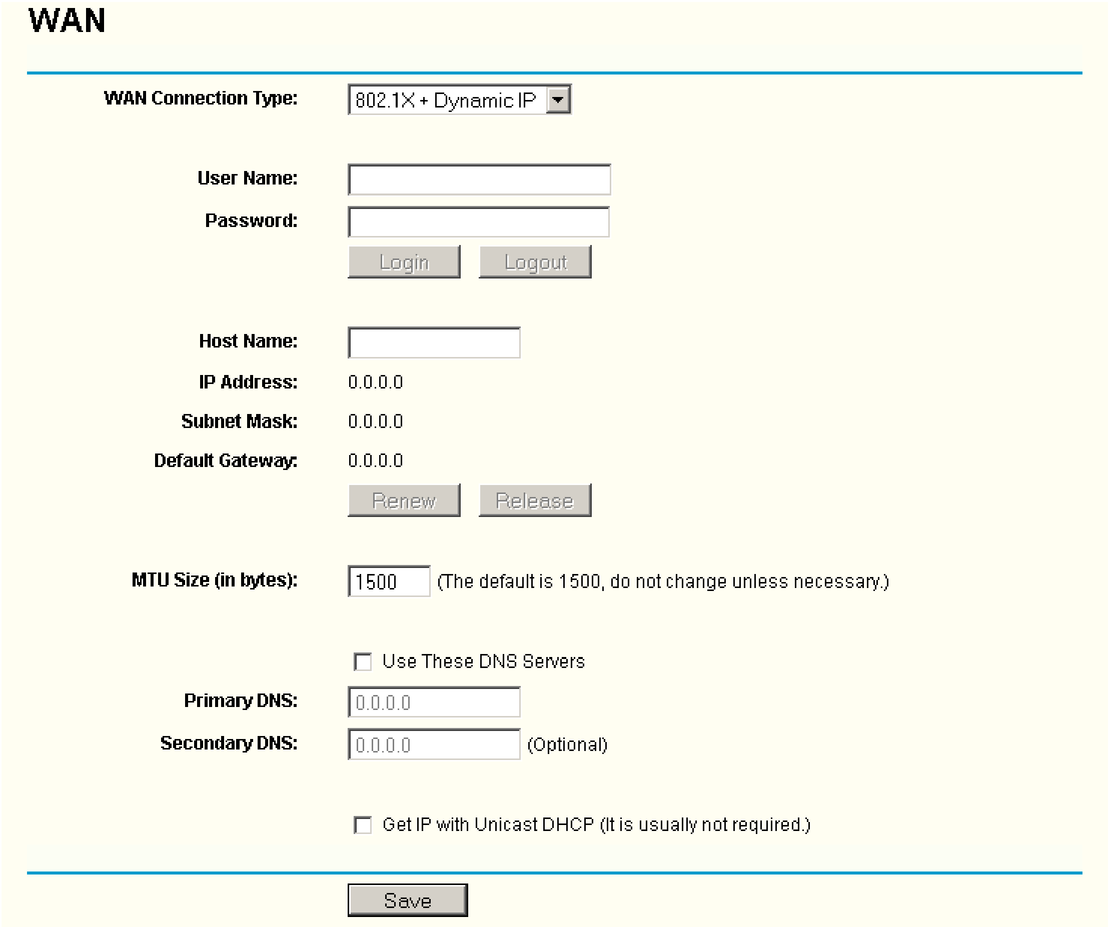
Secondary DNS: 0.0.0.0 (Optional)

Figure 5-8 PPPoE Advanced Settings

- **Packet MTU -** The default MTU size is 1492 bytes, which value is usually fine. For some ISPs, you need modify the MTU. This should not be done unless you are sure it is necessary for your ISP.
- **Service Name/AC Name -** The service name and AC (Access Concentrator) name, these should not be configured unless you are sure it is necessary for your ISP.
- **ISP Specified IP Address -** If you know that your ISP does not automatically transmit your IP address to the router during login, click "**Use the IP Address specified by ISP**" check box and enter the IP Address in dotted-decimal notation, which your ISP provided.
- **Detect Online Interval -** The default value is 0, you can input the value between 0 and 120. The router will detect Access Concentrator online at every interval between seconds. If the value is 0, it means, do not detect.
- **DNS IP address -** If you know that your ISP does not automatically transmit DNS addresses to the router during login, click "**Use the following DNS servers**" checkbox and enter the IP address in dotted-decimal notation of your ISP's primary DNS server. If a secondary DNS server address is available, enter it as well.

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

4. If you choose **802.1X + Dynamic IP,** you should enter the follow parameters(Figure 5-9) :



WAN

WAN Connection Type: 802.1X + Dynamic IP

User Name:

Password:

Host Name:

IP Address: 0.0.0.0

Subnet Mask: 0.0.0.0

Default Gateway: 0.0.0.0

MTU Size (in bytes): 1500 (The default is 1500, do not change unless necessary.)

□ Use These DNS Servers

Primary DNS: 0.0.0.0

Secondary DNS: 0.0.0.0 (Optional)

□ Get IP with Unicast DHCP (It is usually not required.)

Figure 5-9 802.1X + Dynamic IP Settings

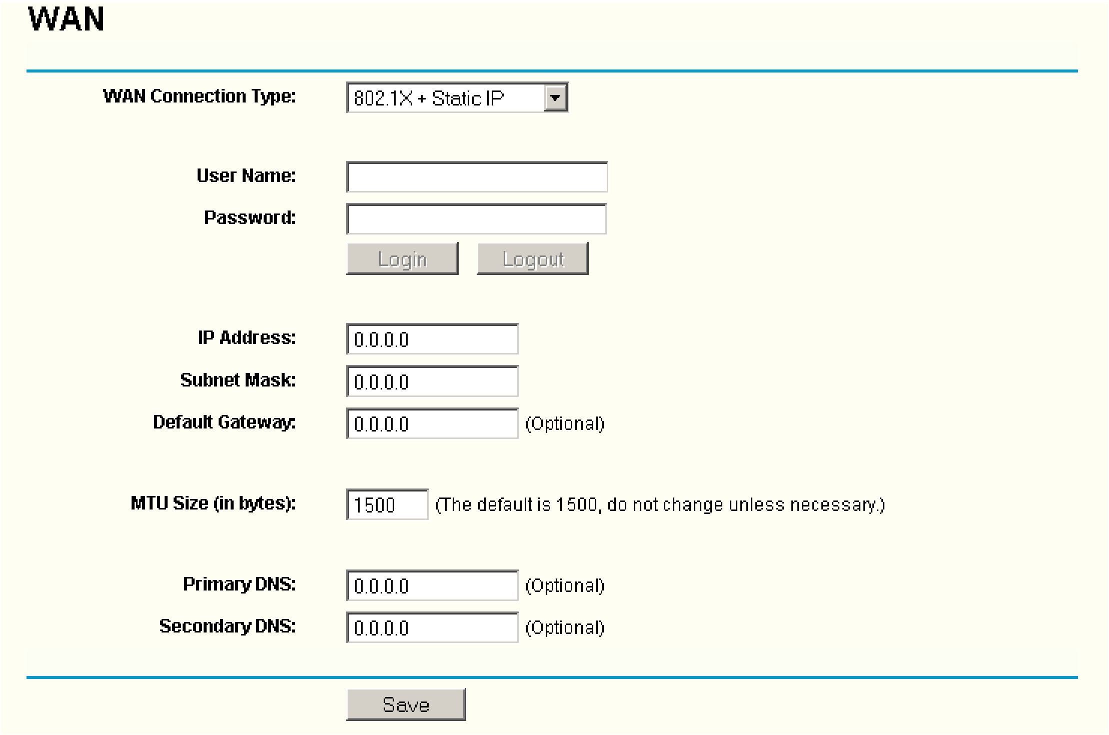
- **User Name -** Enter the user name for 802.1X authentication provided by your ISP
- **Password -** Enter the password for 802.1X authentication provided by your ISP.

Click **Login** to start 802.1X authentication.

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

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

5. If you choose **802.1X + Static IP,** you should enter the follow parameters (Figure 5-10) :



WAN

WAN Connection Type: 802.1X + Static IP

User Name:

Password:

IP Address: 0.0.0.0

Subnet Mask: 0.0.0.0

Default Gateway: 0.0.0.0 (Optional)

MTU Size (in bytes): 1500 (The default is 1500, do not change unless necessary.)

Primary DNS: 0.0.0.0 (Optional)

Secondary DNS: 0.0.0.0 (Optional)

Figure 5-10 802.1X + Static IP Settings

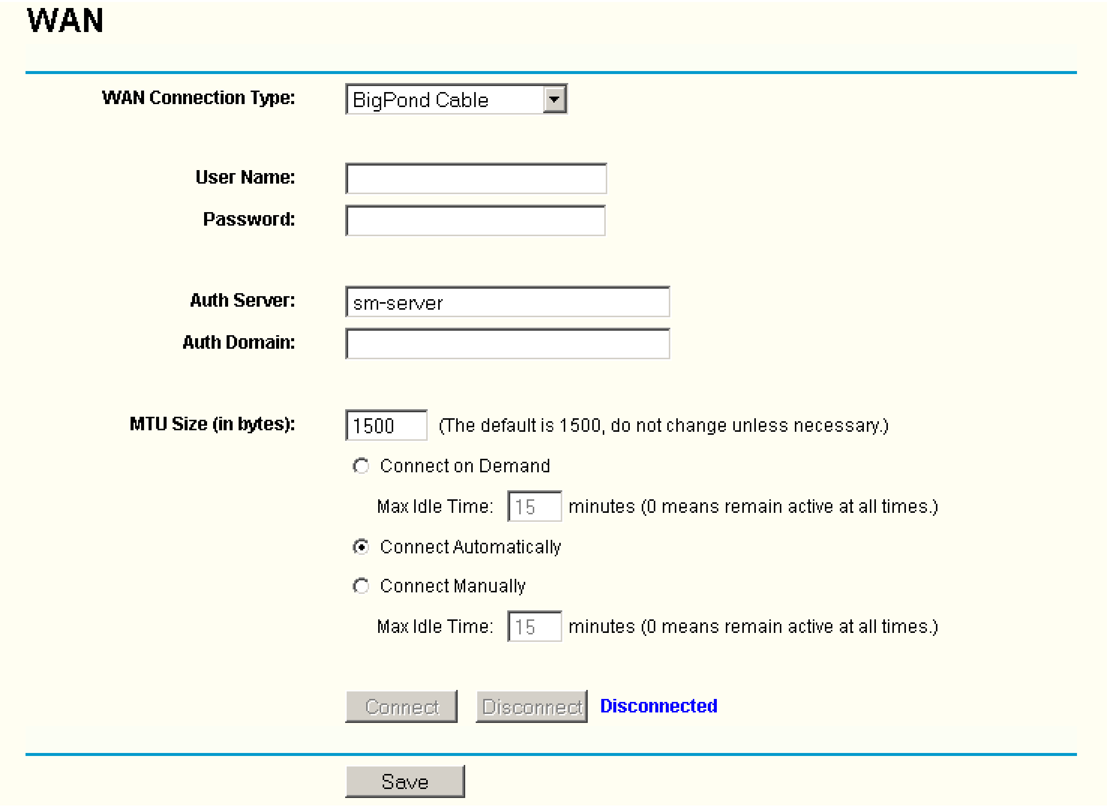
- **User Name -** Enter the user name for 802.1X authentication provided by your ISP
- **Password -** Enter the password for 802.1X authentication provided by your ISP.

Click **Login** to start 802.1X authentication.

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

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

6. If you choose **Big Pond Cable,** you should enter the following parameters (Figure 5-11):



WAN

WAN Connection Type: BigPond Cable

User Name:

Password:

Auth Server: sm-server

Auth Domain:

MTU Size (in bytes): 1500 (The default is 1500, do not change unless necessary.)

○ Connect on Demand

Max Idle Time: 15 minutes (0 means remain active at all times.)

● Connect Automatically

○ Connect Manually

Max Idle Time: 15 minutes (0 means remain active at all times.)

Figure 5-11 Big Pond Settings

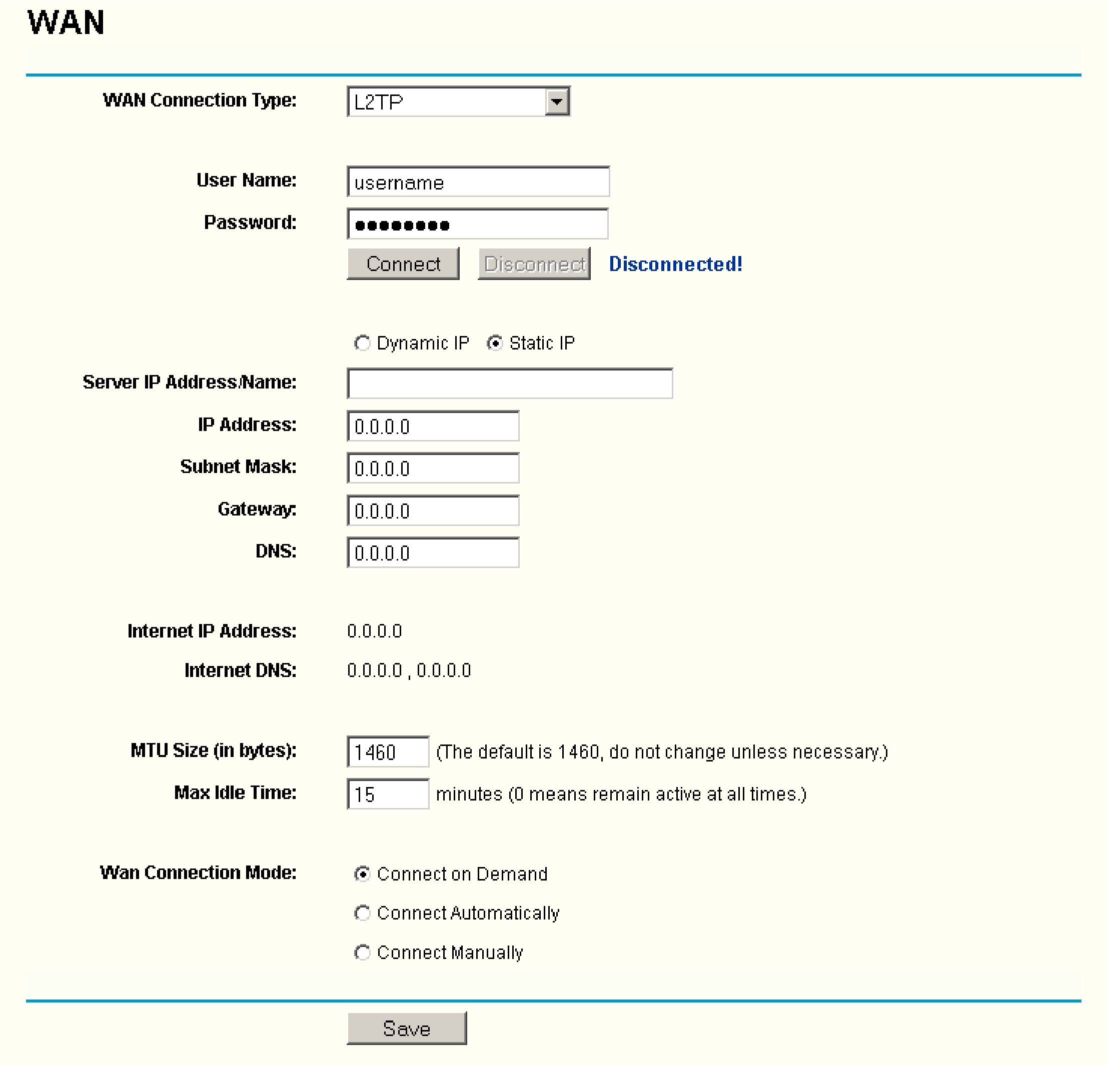
- **User Name/Password -** Enter the User Name and Password provided by your ISP. These fields are case-sensitive.
- **Auth Server -** Enter the authenticating server IP address or host name.
- **Auth Domain** - Type in the domain suffix server name based on your location. E.g.,
  NSW / ACT - **nsw.bigpond.net.au**
  VIC / TAS / WA / SA / NT - **vic.bigpond.net.au**
  QLD - **qld.bigpond.net.au**
- **Connect on Demand -** You can configure the router to disconnect from your Internet connection after a specified period of inactivity (**Max Idle Time**). If your Internet connection has been terminated due to inactivity, **Connect on Demand** enables the router to automatically re-establish your connection as soon as you attempt to access the Internet again. If you wish to activate **Connect on Demand**, click the radio button. If you want your Internet connection to remain active at all times, enter 0 in the **Max Idle Time** field. Otherwise, enter the number of minutes you want to have elapsed before your Internet connection terminates.

  Caution: Sometimes the connection cannot be disconnected although you specify a time to Max Idle Time, since some applications are visiting the Internet continually in the background.
- **Connect Automatically -** Connect automatically after the router is disconnected. To use this option, click the radio button.
- **Connect Manually -** You can configure the router to make it connect or disconnect manually. After a specified period of inactivity (**Max Idle Time**), the router will disconnect from your Internet connection, and you will not be able to re-establish your connection automatically as soon as you attempt to access the Internet again. To use this option, click the radio button. If you want your Internet connection to remain active at all times, enter "0" in the **Max Idle Time** field. Otherwise, enter the number in minutes that you wish to have the Internet connecting last unless a new link is requested.

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

Click the **Connect** button to connect immediately, Click the **Disconnect** button to disconnect immediately.

7. If you choose **L2TP**, you should enter the following parameters (Figure 5-12):



WAN

WAN Connection Type: L2TP

User Name: username

Password: ●●●●●●●●

Disconnected!

○ Dynamic IP ● Static IP

Server IP Address/Name:

IP Address: 0.0.0.0

Subnet Mask: 0.0.0.0

Gateway: 0.0.0.0

DNS: 0.0.0.0

Internet IP Address: 0.0.0.0

Internet DNS: 0.0.0.0 , 0.0.0.0

MTU Size (in bytes): 1460 (The default is 1460, do not change unless necessary.)

Max Idle Time: 15 minutes (0 means remain active at all times.)

Wan Connection Mode:
● Connect on Demand
○ Connect Automatically
○ Connect Manually

Figure 5-12 L2TP Settings

- **User Name/Password -** Enter the User Name and Password provided by your ISP. These fields are case-sensitive.
- **Dynamic IP/ Static IP –** Choose either as you are given by your ISP.

Click the **Connect** button to connect immediately, Click the **Disconnect** button to disconnect immediately.

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

☞ **Note:**

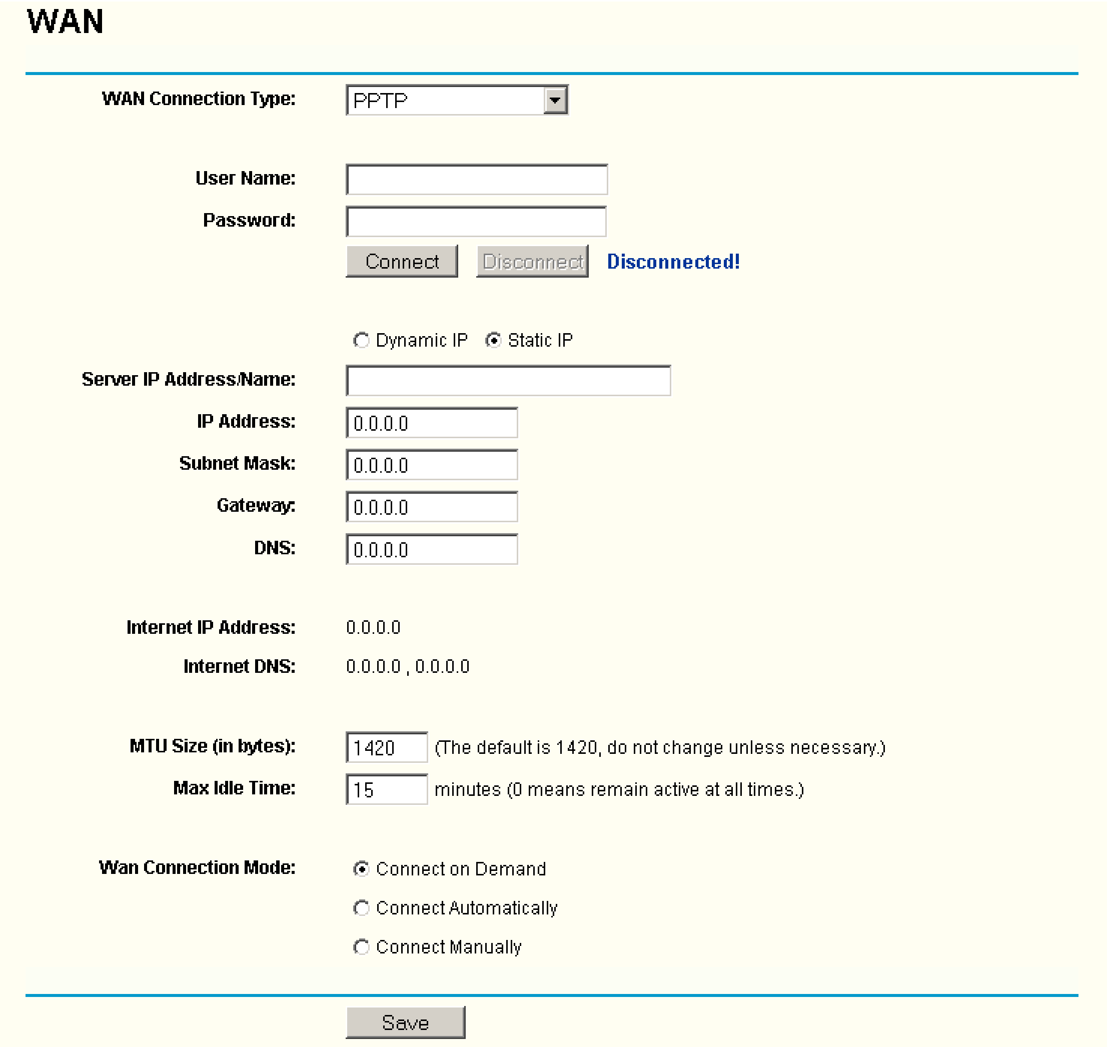
Sometimes the connection cannot be disconnected although you specify a time to Max Idle Time, since some applications is visiting the Internet continually in the background.

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

☞ **Note:**

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.

8. If you choose **PPTP**, you should enter the following parameters (Figure 5-13):



WAN

WAN Connection Type: PPTP

User Name:

Password:

Disconnected!

○ Dynamic IP ● Static IP

Server IP Address/Name:

IP Address: 0.0.0.0

Subnet Mask: 0.0.0.0

Gateway: 0.0.0.0

DNS: 0.0.0.0

Internet IP Address: 0.0.0.0

Internet DNS: 0.0.0.0 , 0.0.0.0

MTU Size (in bytes): 1420 (The default is 1420, do not change unless necessary.)

Max Idle Time: 15 minutes (0 means remain active at all times.)

Wan Connection Mode:

● Connect on Demand

○ Connect Automatically

○ Connect Manually

Figure 5-13 PPTP Settings

- **User Name/Password -** Enter the User Name and Password provided by your ISP. These fields are case-sensitive.
- **Dynamic IP/ Static IP –** Choose either as you are given by your ISP and enter the ISP's IP

address or the domain name.

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

Click the **Connect** button to connect immediately, Click the **Disconnect** button to disconnect immediately.

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

☞ **Note:**

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

- **Connect Automatically -** Connect automatically after the router is disconnected. To use this option, click the radio button.

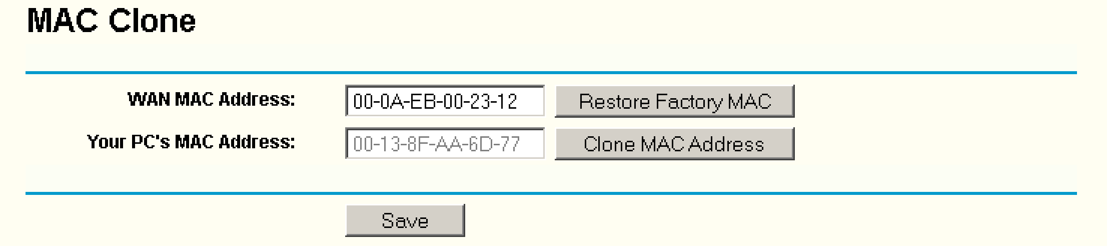
- **Connect Manually -** You can configure the router to make it connect or disconnect manually. After a specified period of inactivity (**Max Idle Time**), the router will disconnect from your Internet connection, and you will not be able to re-establish your connection automatically as soon as you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

☞ **Note:**

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

5.5.3 MAC Clone

You can configure the MAC address of the WAN port on this page, Figure 5-14:



MAC Clone

WAN MAC Address: 00-0A-EB-00-23-12

Your PC's MAC Address: 00-13-8F-AA-6D-77

Figure 5-14 MAC Address Clone

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

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

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

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

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

5.6 Wireless

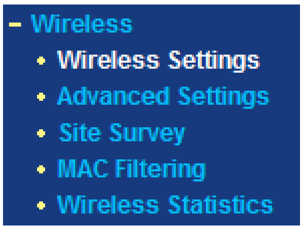


Figure 5-15 Wireless menu

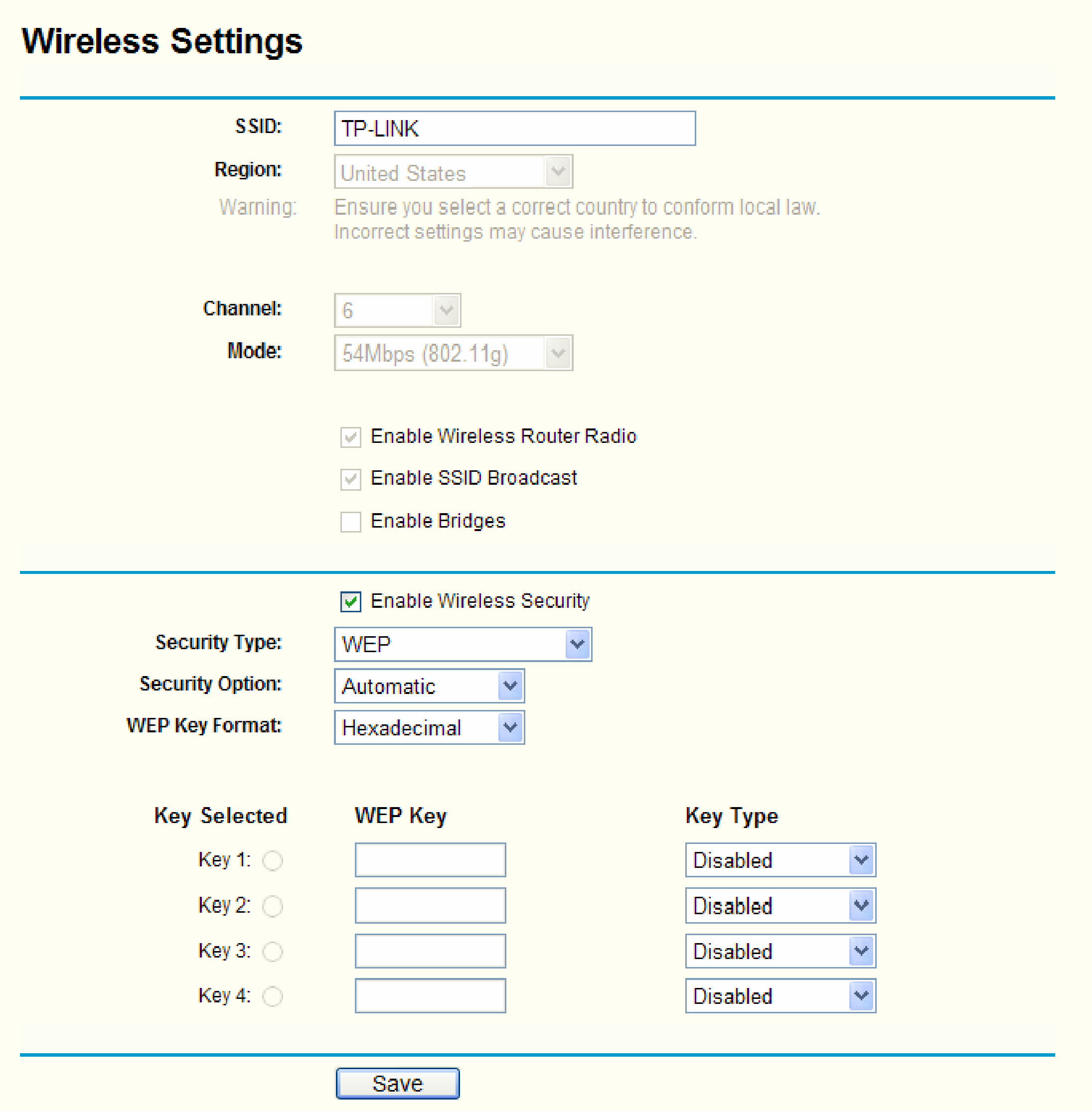
There are four submenus under the Wireless menu (shown in Figure 5-15): **Wireless Settings**, **Advanced Settings**, **Site Survey, MAC Filtering** and **Wireless Statistics.** Click any of them, and you will be able to configure the corresponding function. The detailed explanations for each submenu are provided below.

☞ **Note:**

The **MAC Filtering** is only available in the AP mode.

5.6.1 Wireless Settings

The basic settings for the wireless network in AP Client mode are set on this page. In AP Client mode**,** some options (**Region, Channel Mode, Enable Wireless Router Radio, Enable Bridges and Enable SSID Broadcast)** are not available and could not be modified. Figure 5-16:



Wireless Settings

SSID: TP-LINK

Region: United States

Warning: Ensure you select a correct country to conform local law.
Incorrect settings may cause interference.

Channel: 6

Mode: 54Mbps (802.11g)

☑ Enable Wireless Router Radio

☑ Enable SSID Broadcast

□ Enable Bridges

☑ Enable Wireless Security

Security Type: WEP

Security Option: Automatic

WEP Key Format: Hexadecimal

Key Selected	WEP Key	Key Type
Key 1: ○		Disabled
Key 2: ○		Disabled
Key 3: ○		Disabled
Key 4: ○		Disabled

Figure 5-16 Wireless Settings in AP Client Router mode

- **SSID -** Enter a value of up to 32 characters. The same name (SSID) must be assigned to all wireless devices in your network. The default SSID is TP-LINK, but it is recommended strongly that you change your networks name (SSID) to a different value. This value is case-sensitive. For example, *TP-LINK* is NOT the same as *tp-link*.
- **Enable Wireless Security -** The wireless security function can be enabled or disabled. If disabled, the wireless stations will be able to connect the router without encryption. It is strongly recommended that you choose this option to encrypt your wireless network. The encryption settings are described below.
- **Security Type -** You can select one of the following authentication types:
  - **WEP -** Select WEP authentication type based on 802.11 authentications.
  - **WPA-PSK/WPA2-PSK -** Select WPA/WPA2 authentication type based on pre-shared passphrase.
  - **WPA /WPA2 -** Select WPA/WPA2 authentication type based on Radius Server.
- **Security Options -** You can select one of the following authentication options:
  - When you select **WEP** for authentication type you can select the following authentication options:

- **Automatic -** Select Shared Key or Open System authentication type automatically based on the wireless station request.
- **Shared Key -** Select 802.11 Shared Key authentication.
- **Open System -** Select 802.11 Open System authentication.
- When you select **WPA-PSK/WPA2-PSK** for authentication type you can select **Automatic**, **WPA –PSK** or **WPA2-PSK** as authentication options.
- When you select **WPA/WPA2** as an authentication type you can select **Automatic WPA** or **WPA2** as authentication option.

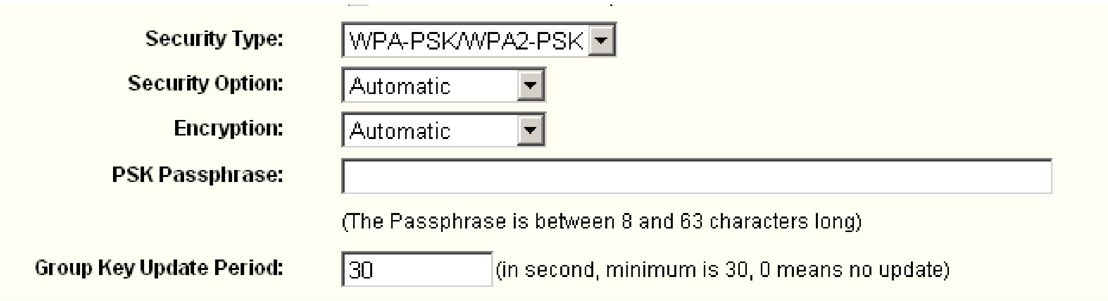
➢ **WEP Key Format -** You can select **ASCII** or **Hexadecimal** format. ASCII Code Format stands for any combination of keyboard characters in the specified length. Hexadecimal format stands for any combination of hexadecimal digits (0-9, a-f, A-F) in the specified length.

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

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

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

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



Security Type: WPA-PSK/WPA2-PSK

Security Option: Automatic

Encryption: Automatic

PSK Passphrase:

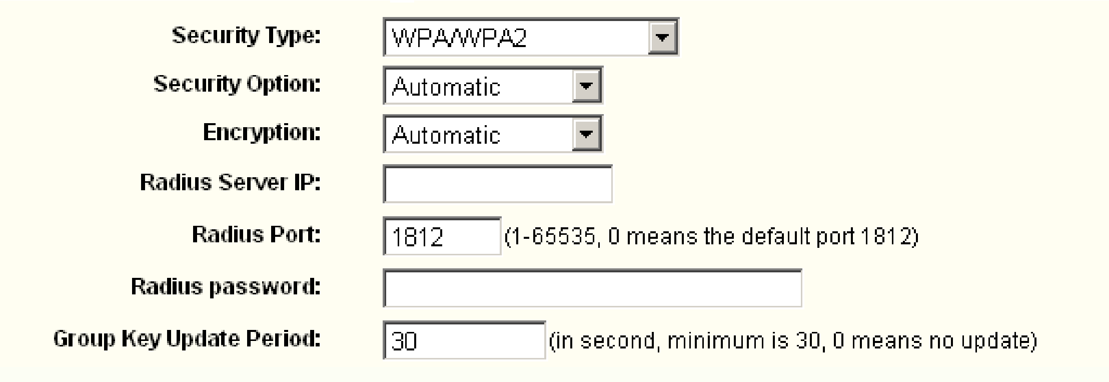
(The Passphrase is between 8 and 63 characters long)

Group Key Update Period: 30 (in second, minimum is 30, 0 means no update)

Figure 5-16a WPA-PSK/WPA2-PSK

➢ **PSK Passphrase -** You can enter a WPA or WPA2 passphrase between 8 and 63 characters long.

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

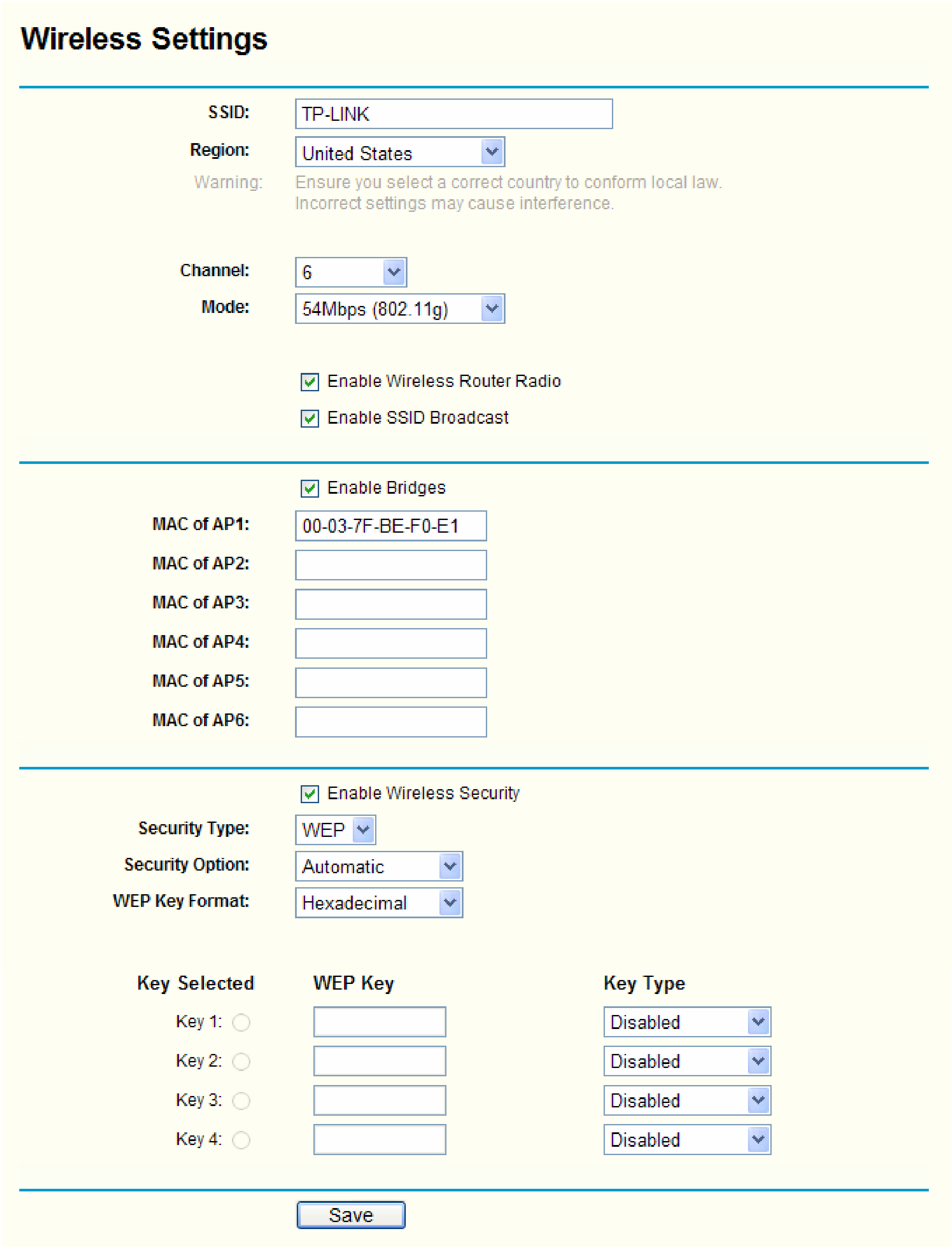


Security Type:	WPA/WPA2
Security Option:	Automatic
Encryption:	Automatic
Radius Server IP:	
Radius Port:	1812 (1-65535, 0 means the default port 1812)
Radius password:	
Group Key Update Period:	30 (in second, minimum is 30, 0 means no update)

Figure 5-16b WPA/WPA2

- **Radius Server IP -** Enter the IP address of the Radius Server
- **Radius Port -** Enter the port number that the radius service used.
- **Radius Password -** Enter the password for the Radius Server.

If you select **AP Router,** the basic settings for the wireless network are set on this page. Figure 5-17:



Wireless Settings

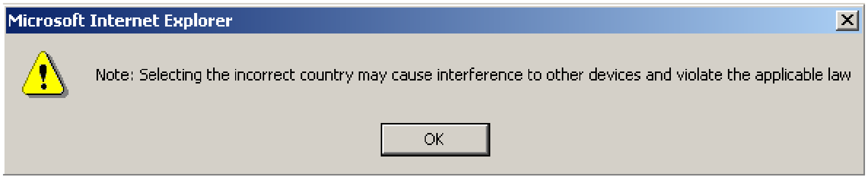
SSID:	TP-LINK
Region:	United States
Warning:	Ensure you select a correct country to conform local law. Incorrect settings may cause interference.
Channel:	6
Mode:	54Mbps (802.11g)
	☑ Enable Wireless Router Radio
	☑ Enable SSID Broadcast
	☑ Enable Bridges
MAC of AP1:	00-03-7F-BE-F0-E1
MAC of AP2:	
MAC of AP3:	
MAC of AP4:	
MAC of AP5:	
MAC of AP6:	
	☑ Enable Wireless Security
Security Type:	WEP
Security Option:	Automatic
WEP Key Format:	Hexadecimal

Key Selected	WEP Key	Key Type
Key 1: ○		Disabled
Key 2: ○		Disabled
Key 3: ○		Disabled
Key 4: ○		Disabled

Figure 5-17 Wireless Settings in AP Router mode

- **Region** - Select your region from the pull-down list. This field specifies the region where the wireless function of the router can be used. It may be illegal to use the wireless function of the router in a region other than one of those specified in this field. If your country or region is not listed, please contact your local government agency for assistance.

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



Microsoft Internet Explorer

Note: Selecting the incorrect country may cause interference to other devices and violate the applicable law

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. It is not necessary to change the wireless channel unless you notice interference problems with another nearby access point.
- **Mode -** Select the desired wireless mode. The options are:
  - **54Mbps (802.11g) -** Both 802.11g and 802.11b wireless stations can connect to the router.
  - **11Mbps (802.11b) -** Only 802.11b wireless stations can connect to the router.

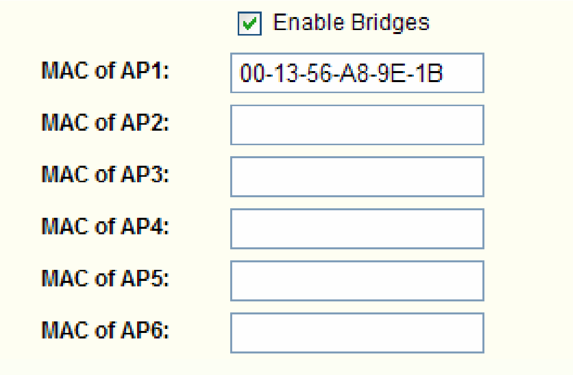
☞ **Note:**

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

- **Enable Wireless Router Radio -** The wireless radio of this Router can be enabled or disabled to allow wireless stations access. If enabled, wireless stations will be able to access the router. Otherwise, wireless stations will not be able to access.
- **Enable SSID Broadcast -** If you select the **Enable SSID Broadcast** checkbox, the Wireless Router SSID will broadcast its name (SSID) on the air.
- **Enable Bridges** – If you select the **Enable Bridges** checkbox, you can input MAC address of other APs to communicate with them wirelessly in Bridge mode.
  - MAC of AP (1-6): Input the MAC address of the AP which you want to communicate with. There are six entries can be configured.

  The APs can communicate with each other in Bridge mode unless they know each other's MAC address. For example, if the router whose MAC address is 00-13-56-A8-9E-1A wants to communicate with an AP whose MAC address is 00-13-56-A8-9E-1B in Bridge mode, you should do as following:

  1. Select **Enable Bridges** and input 00-13-56-A8-9E-1B as following screen shown.



☑ Enable Bridges

MAC of AP1:	00-13-56-A8-9E-1B
MAC of AP2:	
MAC of AP3:	
MAC of AP4:	
MAC of AP5:	
MAC of AP6:	

  2. Access the AP's Web-based utility and configure the AP under Bridge mode, then input 00-13-56-A8-9E-1A in corresponding Blank.

☞ **Note:**

If Bridges is enabled in AP Client mode, there is only one **Security Type** (WEP) for you to encrypt the wireless network. Otherwise, there are three **Security Type** (WEP, WPA-PSK/WPA2-PSK and WPA/WPA2).

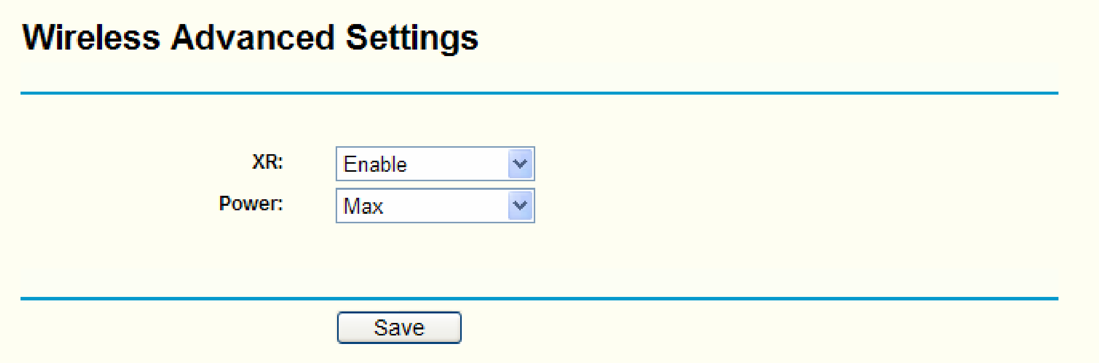
Be sure to click the **Save** button to save your settings on this page.

☞ **Note:**

The router will reboot automatically after you click **Save**.

5.6.2 Advanced Settings

This page shows some advanced settings about this router for you.



Wireless Advanced Settings

XR: Enable

Power: Max

Figure 5-18

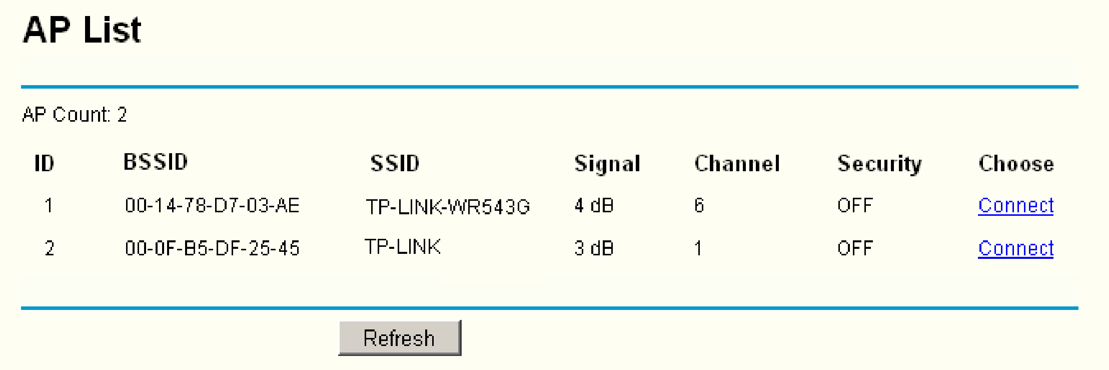
- **XR -** The short of eXtended Range™. If enabled, the wireless transmission distance will be longer in the same condition of circumstance.
- **Power -** The transmit power of the access point. There are five options for you to select in the pull-down list: **Max**, **1/2**, **1/4**, **1/8** and **Min**.

☞ **Note:**

The router will reboot automatically after you click the **Save** button.

5.6.3 Site Survey

This Page shows the site list of scanning result, and you can choose one to connect to.



AP List

AP Count: 2

ID	BSSID	SSID	Signal	Channel	Security	Choose
1	00-14-78-D7-03-AE	TP-LINK-WR543G	4 dB	6	OFF	Connect
2	00-0F-B5-DF-25-45	TP-LINK	3 dB	1	OFF	Connect

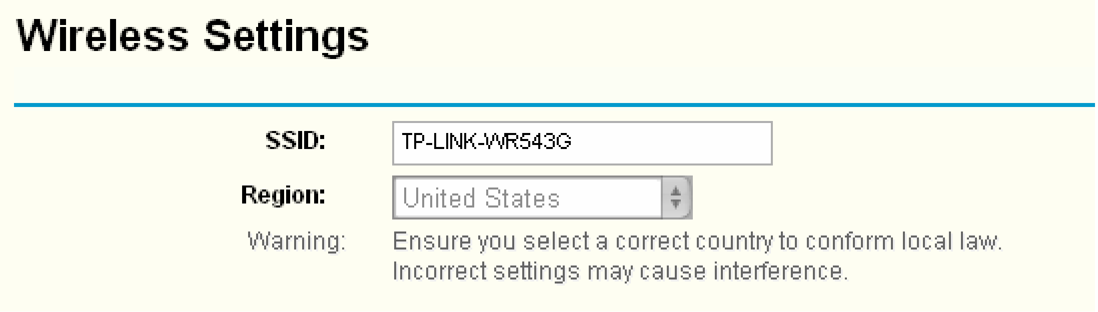
Figure 5-19 AP List

- **BSSID -**The BSSID of the AP, usually also the MAC address of the AP.
- **SSID -**The SSID of the AP.
- **Signal -**The signal received from the AP.
- **Channel -**The channel the AP works in.
- **Security -**The AP communicates in privacy.

- **Choose -** Choose one AP from list to connect to.

If you click the **Connect**, the Figure 5-16 will be shown. And the **SSID** has been configured.

E.g. If you see the page as Figure 5-19 and you want to connect to the **TP-LINK- WR543G** site, you can click **Connect**. The Figure 5-16 will display and the **SSID** is TP-LINK-WR543G. Shown in Figure 5-20:



Wireless Settings

SSID: TP-LINK-WR543G

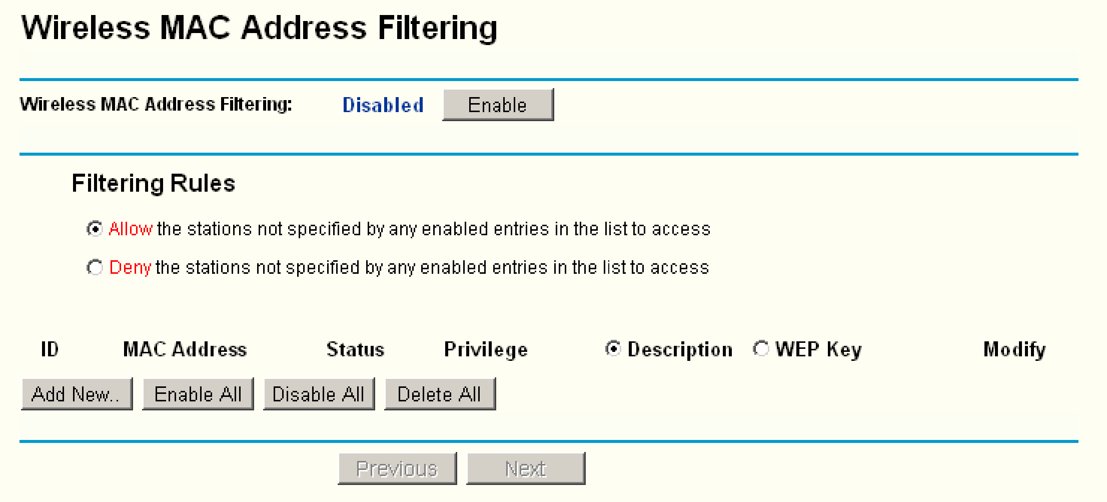
Region: United States

Warning: Ensure you select a correct country to conform local law. Incorrect settings may cause interference.

Figure 5-20 the SSID of Wireless Settings

5.6.4 MAC Filtering

The Wireless MAC Filtering for wireless networks are set on this page. Figure 5-21:



Wireless MAC Address Filtering

Wireless MAC Address Filtering: Disabled

Filtering Rules

● Allow the stations not specified by any enabled entries in the list to access

○ Deny the stations not specified by any enabled entries in the list to access

ID	MAC Address	Status	Privilege	● Description ○ WEP Key	Modify

Figure 5-21 Wireless MAC address Filtering

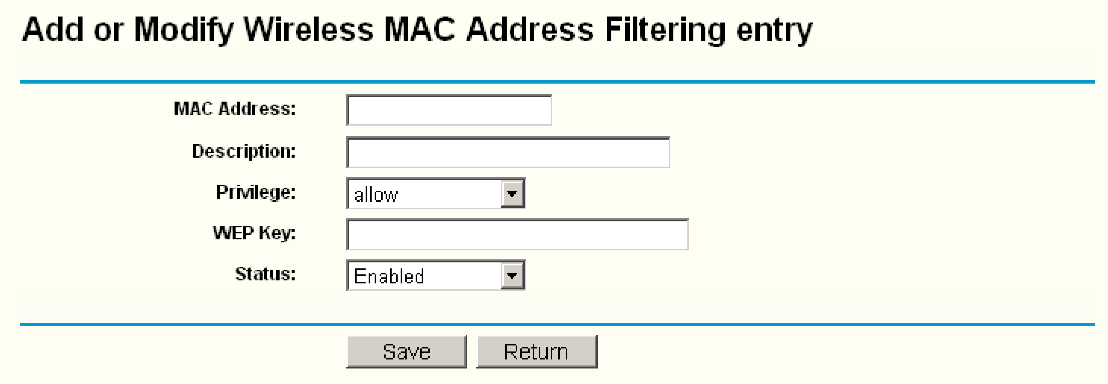
The Wireless MAC Address Filtering feature allows you to control wireless stations accessing the router, which depend on the station's MAC addresses.

- **MAC Address -** The wireless station's MAC address that you want to access.
- **Status -** The status of this entry either **Enabled** or **Disabled**.
- **Privilege -** Select the privileges for this entry. You may select one of the following **Allow** / **Deny** / **64-bit** / **128-bit** / **152-bit**.
- **Description -** A simple description of the wireless station.
- **WEP Key -** Specify a unique WEP key (in Hexadecimal format) to access the router.

To set up an entry, follow these instructions:

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

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 5-22:



Add or Modify Wireless MAC Address Filtering entry

MAC Address:

Description:

Privilege: allow

WEP Key:

Status: Enabled

Figure 5-22 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. **Privilege** - Select the privileges for this entry, one of **Allow** / **Deny** / **64-bit** / **128-bit** / **152-bit**.
4. WEP Key - If you select **64-bit**, **128-bit** or **152-bit** in the **Privilege** field, enter any combination of hexadecimal digits (0-9, a-f, A-F) in the specified length. For example: 2F34D20BE2.
5. **Status** - Select **Enabled** or **Disabled** for this entry on the **Status** pull-down list.
6. Click the **Save** button to save this entry.

To add additional entries, repeat steps 1-6.

☞ **Note:**

When 64-bit, or 128-bit, or 152-bit is selected, WEP Key will be enabled.

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.

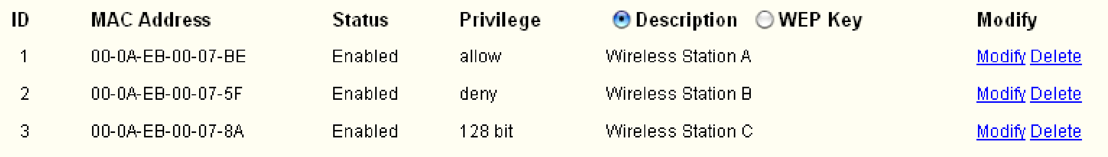
Click the **Delete All** button to delete all entries

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 be able to access the router. The wireless station B with MAC address 00-0A-EB- 00-07-5F not be able to access the router, and the wireless station C with MAC address 00-0A-EB-00-07-8A be able to access the router when its WEP key is 2F34D20BE2E 54B326C5476586A, while all other wireless stations cannot access the router, you should 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 in the **MAC Address** field, enter wireless station A in the **Description** field, select **Allow** in the **Privilege** pull-down list and select **Enabled** in the **Status** pull-down list. Click the **Save** and the **Return** button.
5. Click the **Add New...** button and enter the MAC address 00-0A-EB-00-07-5F in the **MAC Address** field, enter wireless station B in the **Description** field, select **Deny** in the **Privilege** pull-down list and select **Enabled** in the **Status** pull-down list. Click the **Save** and the **Return** button.
6. Click the **Add New...** button and enter the MAC address 00-0A-EB-00-07-8A in the **MAC Address** field, enter wireless station C in the **Description** field, select **128-bit** in the **Privilege** pull-down list, enter 2F34D20BE2E54B326C5476586A in the **WEP Key** field and select **Enabled** in the **Status** pull-down list. Click the **Save** and the **Return** button.

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



ID	MAC Address	Status	Privilege	● Description ○ WEP Key	Modify
1	00-0A-EB-00-07-BE	Enabled	allow	Wireless Station A	Modify Delete
2	00-0A-EB-00-07-5F	Enabled	deny	Wireless Station B	Modify Delete
3	00-0A-EB-00-07-8A	Enabled	128 bit	Wireless Station C	Modify Delete

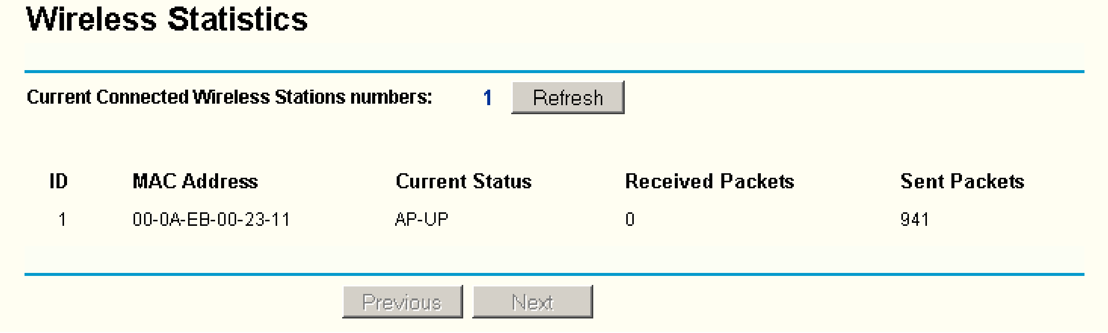
☞ **Note:**

1) If you select the radio button **Allow the stations not specified by any enabled entries in the list to access** for **Filtering Rules,** the wireless station B will still not be able to access the router, however, other wireless stations that are not in the list will be able to access the router.

2) If you enable the function and select the **Deny the stations not specified by any enabled entries in the list to access** for **Filtering Rules,** and there are not any enable entries in the list, thus, no wireless stations can access the router.

5.6.5 Wireless Statistics

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



Wireless Statistics

Current Connected Wireless Stations numbers: 1 Refresh

ID	MAC Address	Current Status	Received Packets	Sent Packets
1	00-0A-EB-00-23-11	AP-UP	0	941

Figure 5-23 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 / AP-UP / WPA / WPA-PSK /WPA2/WPA2-PSK/None
- **Received Packets -** Packets received by the station
- **Sent Packets -** Packets sent by the station

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

5.7 DHCP

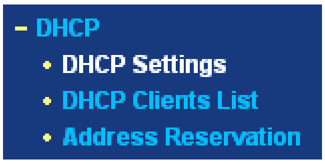
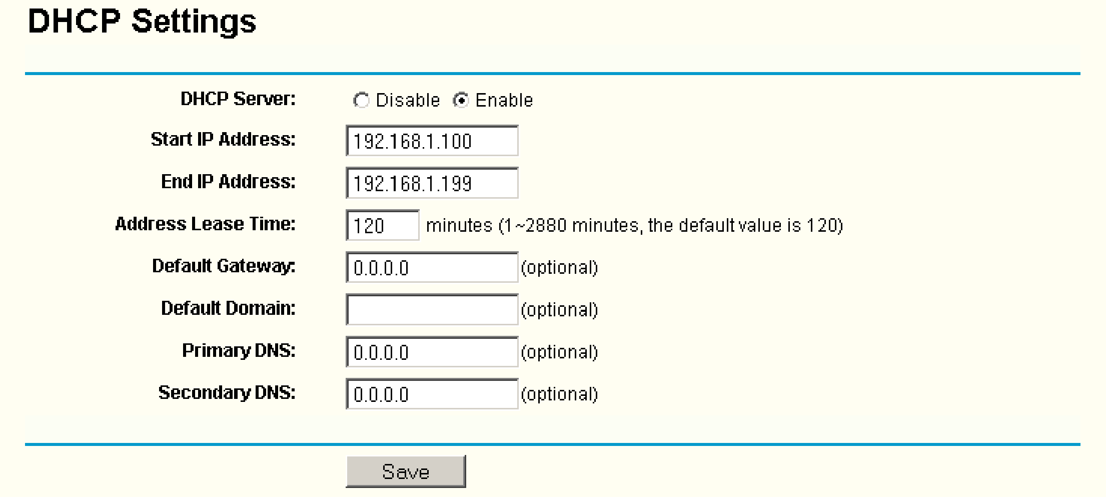


Figure 5-24 The DHCP menu

There are three submenus under the DHCP menu (shown in Figure 5-24): **DHCP Settings**, **DHCP Clients List** and **Address Reservation.** Click any of them, and you will be able to configure the corresponding function. The detailed explanations for each submenu are provided below.

5.7.1 DHCP Settings

The router is set up by default as a DHCP (Dynamic Host Configuration Protocol) server, which provides the TCP/IP configuration for all the PC(s) that are connected to the router on the LAN. The DHCP Server can be configured on the page (shown in Figure 5-25):



DHCP Settings

DHCP Server: ○ Disable ● Enable

Start IP Address: 192.168.1.100

End IP Address: 192.168.1.199

Address Lease Time: 120 minutes (1~2880 minutes, the default value is 120)

Default Gateway: 0.0.0.0 (optional)

Default Domain: (optional)

Primary DNS: 0.0.0.0 (optional)

Secondary DNS: 0.0.0.0 (optional)

Figure 5-25 DHCP Settings

- **DHCP Server - Enable** or **Disable** the DHCP server. If you disable the Server, you must have another DHCP server within your network or else you must manually configure the computer.
- **Start IP Address -** This field specifies the first of the addresses in the IP address pool. 192.168.1.100 is the default start address.
- **End IP Address -** This field specifies the last of the addresses in the IP address pool. 192.168.1.199 is the default end address.

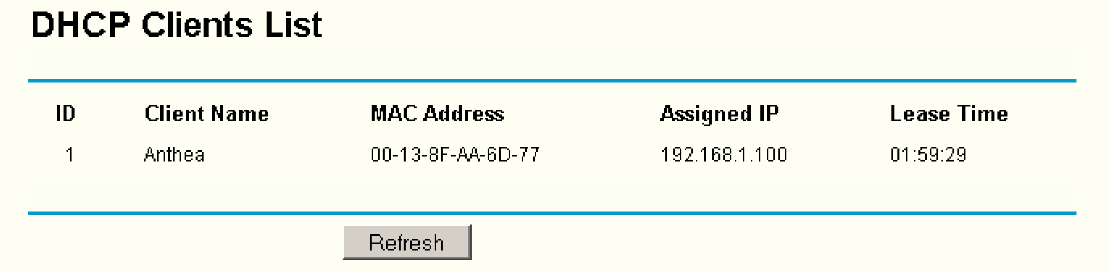
- **Address Lease Time -** The **Address Lease Time** is the amount of time in which a network user will be allowed connection to the router with their current dynamic IP Address. Enter the amount of time, in minutes. The user will be "leased" this dynamic IP Address. The range of the time is 1 ~ 2880 minutes. The default value is 120 minutes.
- **Default Gateway -** (Optional.) Suggest to input the IP address of the LAN port of the router, default value is 192.168.1.1
- **Default Domain -** (Optional.) Input the domain name of your network.
- **Primary DNS -** (Optional.) Input the DNS IP address provided by your ISP. Or consult your ISP.
- **Secondary DNS -** (Optional.) Input the IP address of another DNS server if your ISP provides two DNS servers.

☞ **Note:**

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

5.7.2 DHCP Clients List

This page shows **Client Name, MAC Address, Assigned IP,** and **Lease Time** for each DHCP Client attached to the router (Figure 5-26):



DHCP Clients List

ID	Client Name	MAC Address	Assigned IP	Lease Time
1	Anthea	00-13-8F-AA-6D-77	192.168.1.100	01:59:29

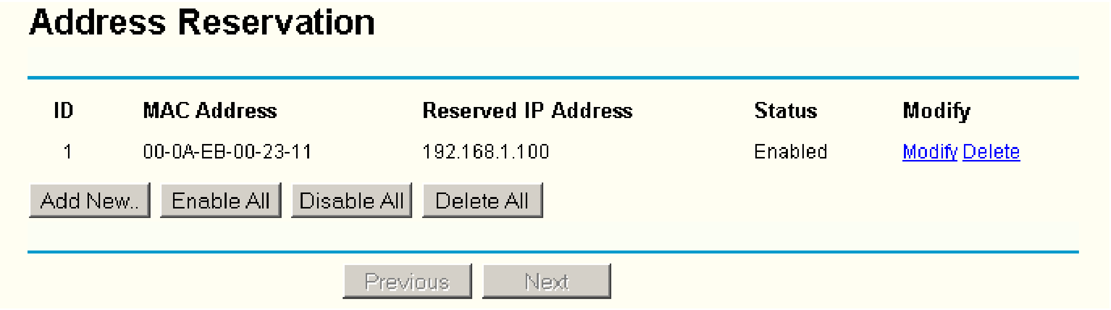
Figure 5-26 DHCP Clients List

- **Index -** The index of the DHCP Client
- **Client Name -** The name of the DHCP client
- **MAC Address -** The MAC address of the DHCP client
- **Assigned IP -** The IP address that the router has allocated to the DHCP client.
- **Lease Time -** The time of the DHCP client leased. Before the time is up, DHCP client will request to renew the lease automatically.

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

5.7.3 Address Reservation

When you specify a reserved IP address for a PC on the LAN, that PC will always receive the same IP address each time when it accesses the DHCP server. Reserved IP addresses should be assigned to servers that require permanent IP settings. This page is used for address reservation (shown in Figure 5-27).



Address Reservation

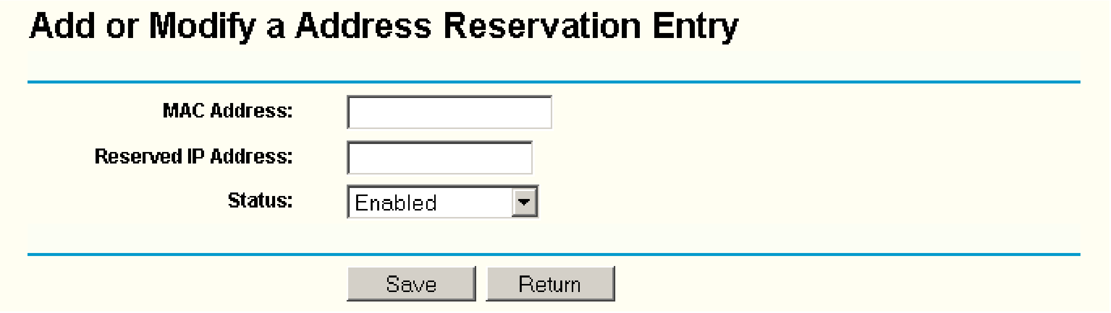
ID	MAC Address	Reserved IP Address	Status	Modify
1	00-0A-EB-00-23-11	192.168.1.100	Enabled	Modify Delete

Figure 5-27 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 5-28)
2. Enter the MAC address (The format for the MAC Address is XX-XX-XX-XX-XX-XX.) and IP address in dotted-decimal notation of the computer you wish to add.
3. Click the **Save** button when finished.



Add or Modify a Address Reservation Entry

MAC Address:

Reserved IP Address:

Status: Enabled

Figure 5-28 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 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 the previous page.

☞ **Note:**

The function won't take effect until the router reboots.

5.8 Forwarding

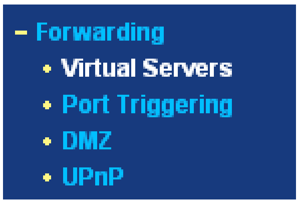
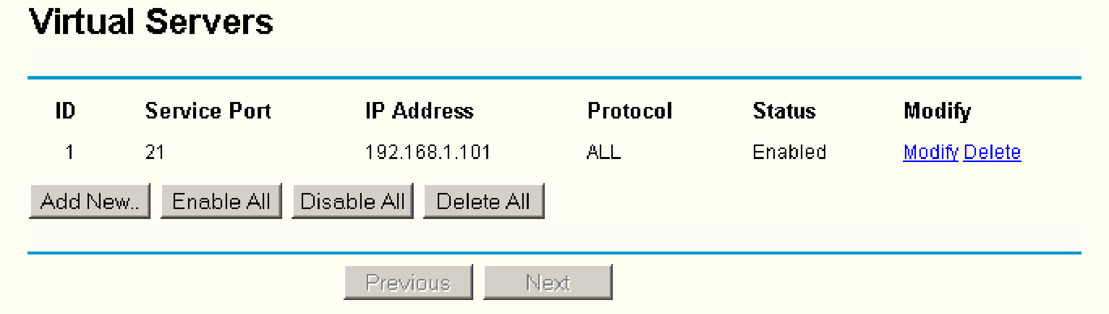


Figure 5-29 The Forwarding menu

There are four submenus under the Forwarding menu (shown in Figure 5-29): **Virtual Servers**, **Port Triggering**, **DMZ** and **UPnP**. Click any of them, and you will be able to configure the corresponding function. The detailed explanations for each submenu are provided below.

5.8.1 Virtual Servers

Virtual servers can be used for setting up public services on your LAN, such as DNS, Email and FTP. A virtual server is defined as a service port, and all requests from the Internet to this service port will be redirected to the computer specified by the server IP. Any PC that was used for a virtual server must have a static or reserved IP Address because its IP Address may change when using the DHCP function. You can set up virtual servers on this page, shown in Figure 5-30:


Virtual Servers

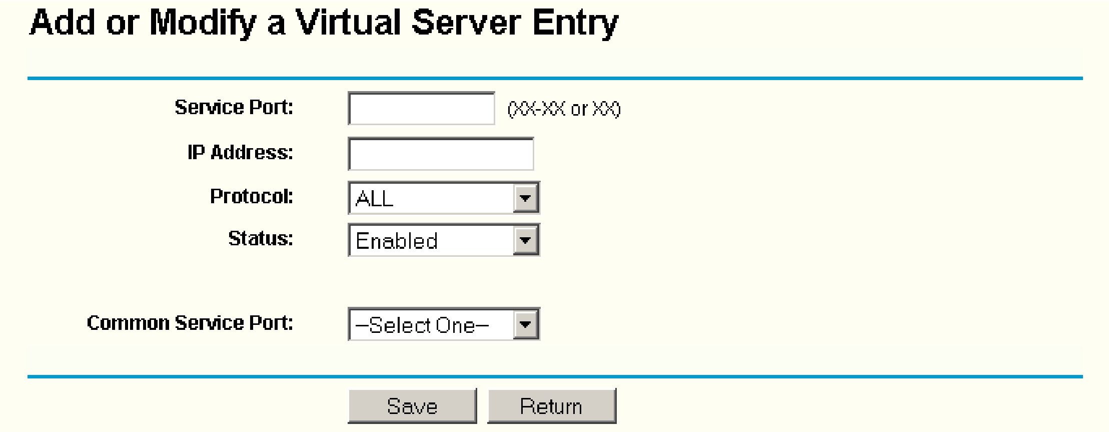
ID	Service Port	IP Address	Protocol	Status	Modify
1	21	192.168.1.101	ALL	Enabled	Modify Delete

Figure 5-30 Virtual Servers

- **Service Port -** The numbers of External Ports. You can type a service port or a range of service ports (the format is XXX – YYY, XXX is the start port, YYY is the end port).
- **IP Address -** The IP Address of the PC providing the service application.
- **Protocol -** The protocol used for this application, either **TCP**, **UDP**, or **All** (all protocols supported by the router).
- **Status -** The status of this entry either **Enabled** or **Disabled**.

To setup a virtual server entry:

1. Click the **Add New button**. (pop-up Figure 5-31)
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** checkbox to enable the virtual server.
6. Click the **Save** button.



Add or Modify a Virtual Server Entry

Service Port:	(XX-XX or XX)
IP Address:	
Protocol:	ALL
Status:	Enabled
Common Service Port:	--Select One--

Figure 5-31 Add or Modify a Virtual Server Entry

☞ **Note:**

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

To modify or delete an existing entry:

1. Click 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.

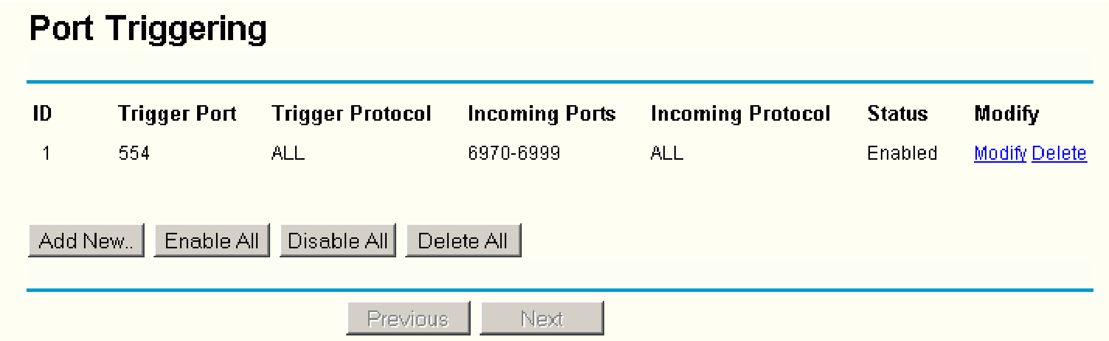
Click the Next button to go to the next page and Click the Previous button to return the previous page.

☞ **Note:**

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

5.8.2 Port Triggering

Some applications require multiple connections, like Internet games, video conferencing, Internet calling and so on. These applications cannot work with a pure NAT router. Port Triggering is used for some of these applications that can work with an NAT router. You can set up Port Triggering on this page shown in Figure 5-32:



Port Triggering

ID	Trigger Port	Trigger Protocol	Incoming Ports	Incoming Protocol	Status	Modify
1	554	ALL	6970-6999	ALL	Enabled	Modify Delete

Figure 5-32 Port Triggering

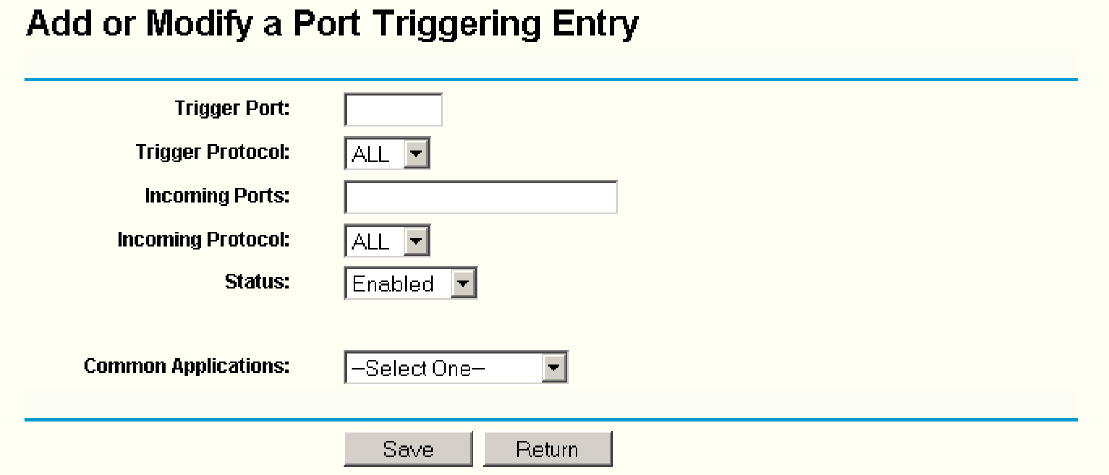
Once configured, operation is as follows:

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 5-33)
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.



Add or Modify a Port Triggering Entry

Trigger Port:

Trigger Protocol: ALL

Incoming Ports:

Incoming Protocol: ALL

Status: Enabled

Common Applications: --Select One--

Figure 5-33 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:**

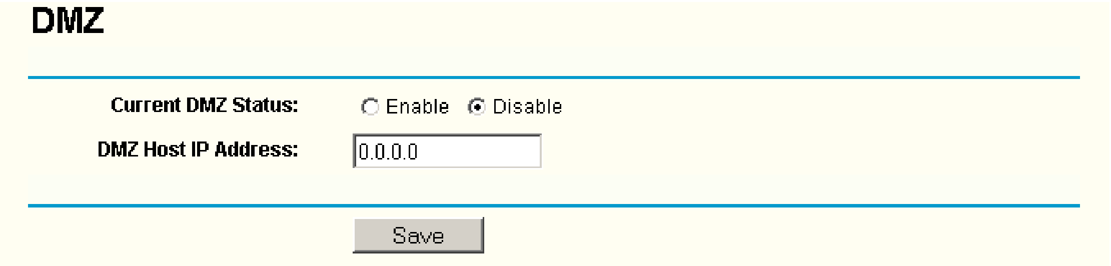
1) When the trigger connection is released, the according opening ports will be closed.

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.

5.8.3 DMZ

The DMZ host feature allows one local host to be exposed to the Internet for a special-purpose service such as Internet gaming or videoconferencing. DMZ host forwards all the ports at the same time. Any PC whose port is being forwarded must have its DHCP client function disabled and should have a new static IP Address assigned to it because its IP Address may change when using the DHCP function. You can set up DMZ host on this page shown in Figure 5-33:



DMZ

Current DMZ Status: ○ Enable ● Disable

DMZ Host IP Address: 0.0.0.0

Figure 5-34 DMZ

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

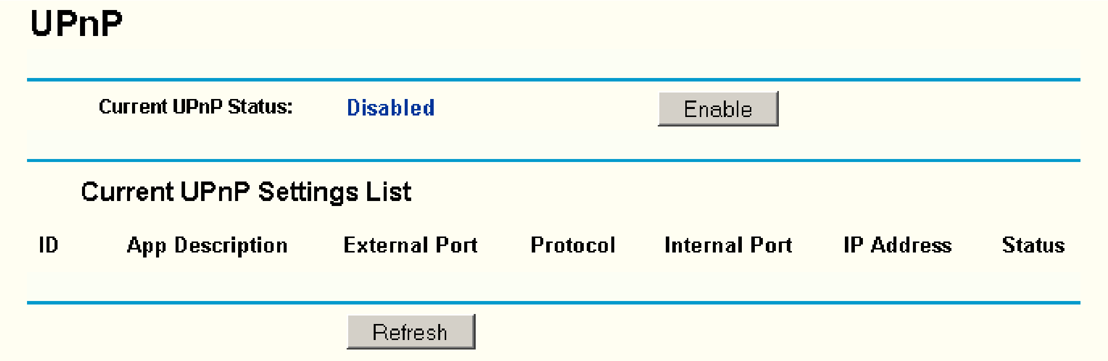
1. Click the **Enable** radio button
2. Enter the local host IP Address in the **DMZ Host IP Address** field
3. Click the **Save** button.

☞ **Note:**

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

5.8.4 UPnP

The Universal Plug and Play (UPnP) feature allows the devices, such as Internet computers, to access the local host resources or devices as needed. UPnP devices can be automatically discovered by the UPnP service application on the LAN. You can configure UPnP on this page that shown in Figure 5-35:



UPnP

Current UPnP Status: Disabled

Current UPnP Settings List

ID	App Description	External Port	Protocol	Internal Port	IP Address	Status

Figure 5-35 UPnP Settings

- **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 -** Either Enabled or Disabled, "Enabled" means that port is still active. Otherwise, the port is inactive.

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

5.9 Security

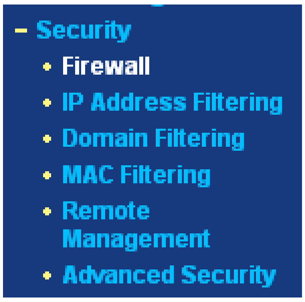
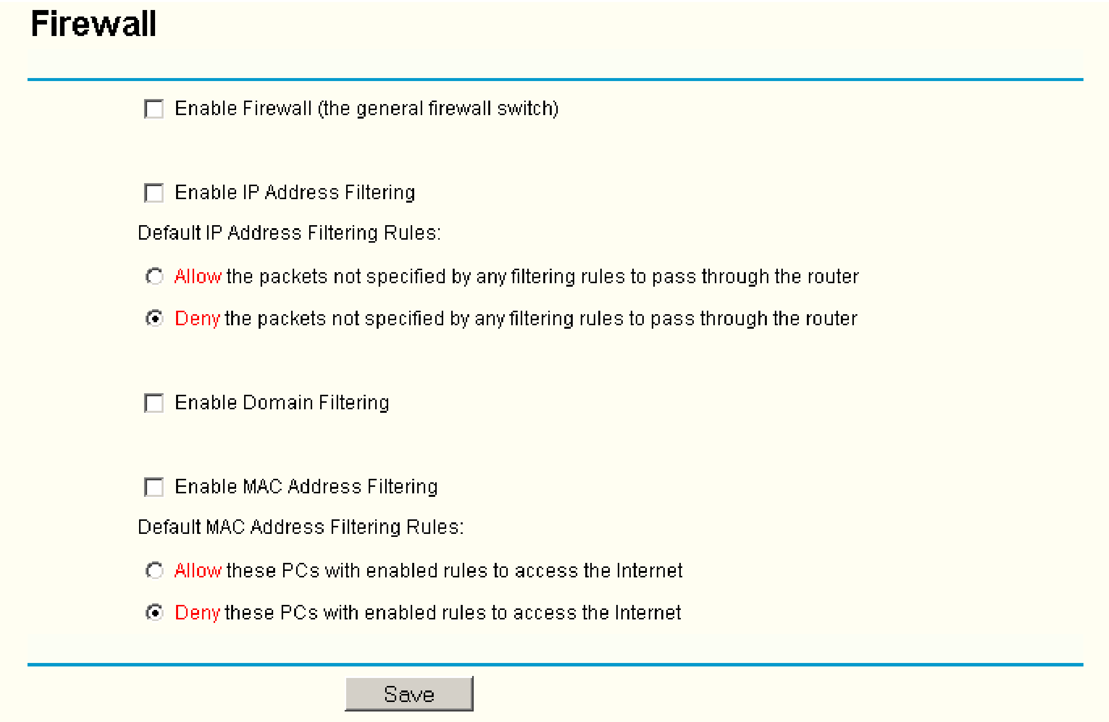


Figure 5-36 The Security menu

There are six submenus under the Security menu (shown in Figure 5-36): **Firewall**, **IP Address Filtering, Domain Filtering, MAC Filtering, Remote Management** and **Advanced Security.** Click any of them, and you will be able to configure the corresponding function. The detailed explanations for each submenu are provided below.

5.9.1 Firewall

Using the Firewall page (shown in Figure 5-37), you can turn the general firewall switch on or off. The default setting for the switch is off. If the general firewall switch is off, even if IP Address Filtering, DNS Filtering and MAC Filtering are enabled, their settings are ineffective.



Firewall

□ Enable Firewall (the general firewall switch)

□ Enable IP Address Filtering

Default IP Address Filtering Rules:

○ Allow the packets not specified by any filtering rules to pass through the router

● Deny the packets not specified by any filtering rules to pass through the router

□ Enable Domain Filtering

□ Enable MAC Address Filtering

Default MAC Address Filtering Rules:

○ Allow these PCs with enabled rules to access the Internet

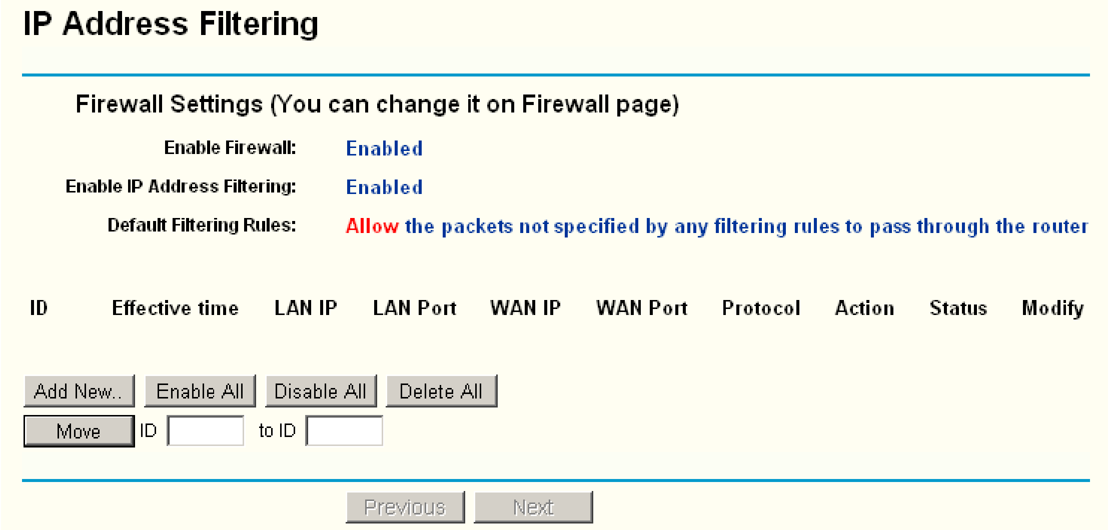
● Deny these PCs with enabled rules to access the Internet

Figure 5-37 Firewall Settings

- **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.

5.9.2 IP Address Filtering

The IP address Filtering feature allows you to control the Internet Access by specific users on your LAN based on their IP addresses. The IP address filtering is set on this page, Figure 5-38:



IP Address Filtering

Firewall Settings (You can change it on Firewall page)

Enable Firewall: Enabled

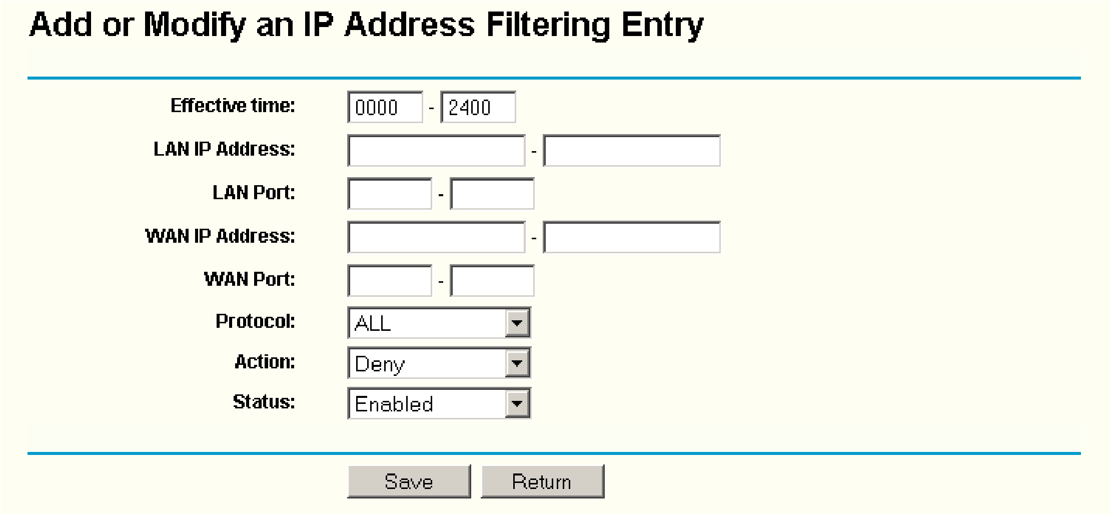
Enable IP Address Filtering: Enabled

Default Filtering Rules: Allow the packets not specified by any filtering rules to pass through the router

ID	Effective time	LAN IP	LAN Port	WAN IP	WAN Port	Protocol	Action	Status	Modify

Figure 5-38 IP address Filtering

To disable the IP Address Filtering feature, keep the default setting, **Disabled**. To set up an IP Address Filtering entry, click **Enable** Firewall and **Enable** IP Address Filtering on the Firewall page, and click the **Add New…** button. The page "**Add or Modify an IP Address Filtering entry**" will appear shown in Figure 5-39:



Add or Modify an IP Address Filtering Entry

Effective time: 0000 - 2400

LAN IP Address: -

LAN Port: -

WAN IP Address: -

WAN Port: -

Protocol: ALL

Action: Deny

Status: Enabled

Figure 5-39 Add or Modify an IP Address Filtering Entry

To create or modify an IP Address Filtering entry, please follow these instructions:

1. **Effective Time -** Enter a range of time in HHMM format, which point to the range time for the entry to take effect. For example, 0803 - 1705, the entry will take effect from 08:03 to 17:05.
2. **LAN IP Address -** Enter a LAN IP Address or a range of LAN IP addresses in the field, in dotted-decimal notation format. For example, 192.168.1.20 - 192.168.1.30. Keep the field open, which means all LAN IP Addresses have been put into the field.
3. **LAN Port -** Enter a LAN Port or a range of LAN ports in the field. For example, 1030 - 2000. Keep the field open, which means all LAN ports have been put into the field.
4. **WAN IP Address -** Enter a WAN IP Address or a range of WAN IP Addresses in the field, in dotted-decimal notation format. For example, 61.145.238.6 – 61.145.238.47. Keep the field open, which means all WAN IP Addresses have been put into the field.
5. **WAN Port -**Enter a WAN Port or a range of WAN Ports in the field. For example, 25 – 110. Keep the field open, which means all WAN Ports have been put into the field.
6. **Protocol -** Select which protocol is to be used, either **TCP, UDP**, or **All** (all protocols supported by the router).
7. **Pass -** Select either **Allow** or **Deny** through the router.
8. **Status -** Select **Enabled** or **Disabled** for this entry on the **Status** pull-down list.
9. 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

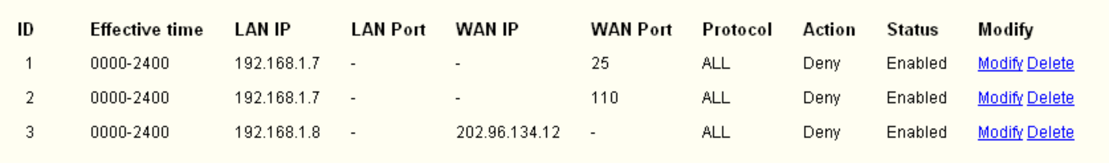
Click the **Disabled All** button to make all entries disabled.

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

You can change the entry’s order as desired. Fore entries are before hind entries. Enter the ID number in the first box you want to move and another ID number in second box you want to move to, and then click the **Move** button to change the entry's order.

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

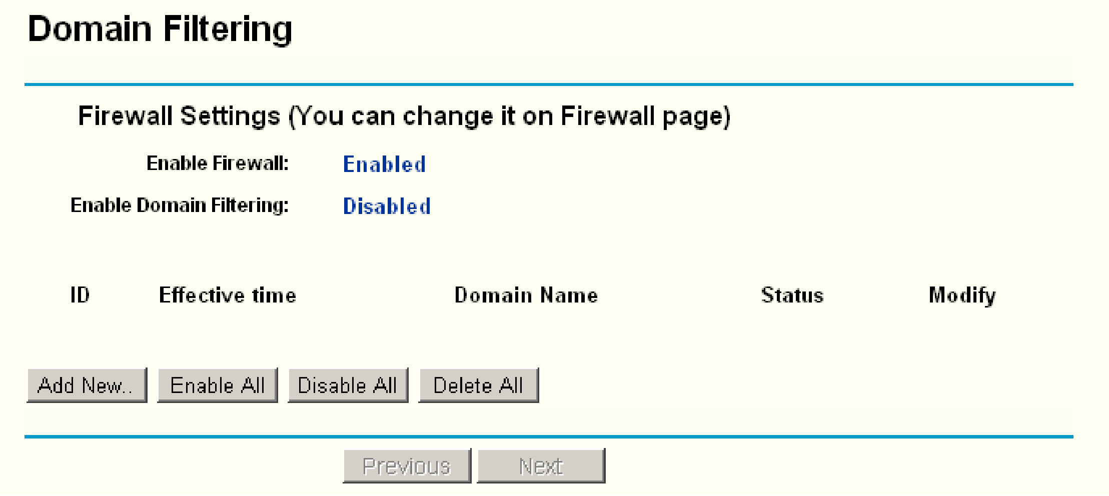
For example: If you desire to block E-mail received and sent by the IP Address 192.168.1.7 on your local network, and to make the PC with IP Address 192.168.1.8 unable to visit the website of IP Address 202.96.134.12, while other PC(s) have no limit you should specify the following IP address filtering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



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

5.9.3 Domain Filtering

The Domain Filtering page (shown in Figure 5-40) allows you to control access to certain websites on the Internet by specifying their domains or key words.



Domain Filtering

Firewall Settings (You can change it on Firewall page)

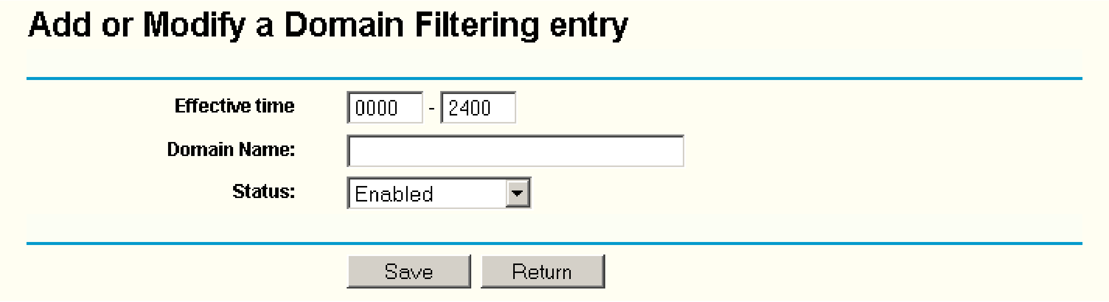
Enable Firewall: Enabled

Enable Domain Filtering: Disabled

ID	Effective time	Domain Name	Status	Modify

Figure 5-40 Domain Filtering

Before adding a Domain Filtering entry, you must ensure that **Enable** Firewall and **Enable** Domain Filtering have been selected on the Firewall page. To Add a Domain filtering entry, click the **Add New…** button. The page "**Add or Modify a Domain Filtering entry**" will appear, shown in Figure 5-41:



Add or Modify a Domain Filtering entry

Effective time 0000 - 2400

Domain Name:

Status: Enabled

Figure 5-41 Add or Modify a Domain Filtering entry

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

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

2. **Domain Name -** Type the domain or key word as desired in the field. A blank in the domain

field means all websites on the Internet. For example: www.xxyy.com.cn, .net.

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

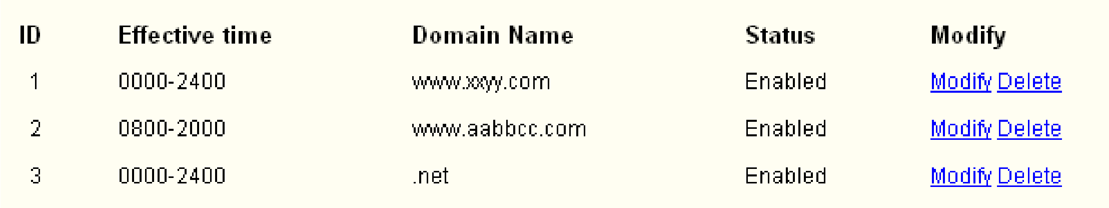
Click the **Enabled All** button to make all entries enabled.

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 the **Previous** button to return to the previous page.

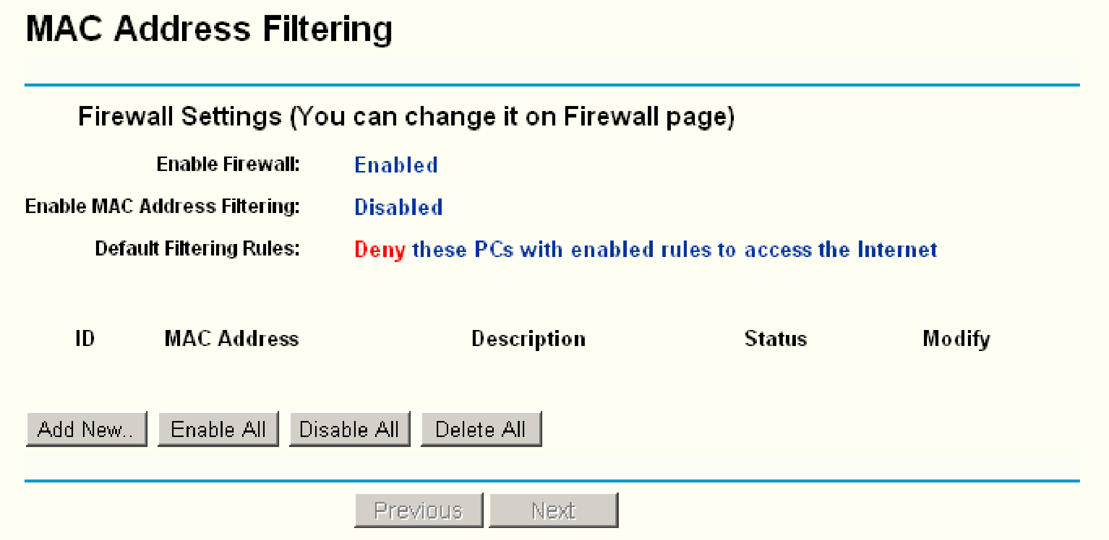
For example, if you want to block the PC(s) on your LAN to access websites www.xxyy.com.cn, www.aabbcc.com and websites with .net in the end on the Internet while no limit for other websites, you should specify the following Domain filtering list:



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

5.9.4 MAC Filtering

Like the IP Address Filtering page, the MAC Address Filtering page (shown in Figure 5-42) allows you to control access to the Internet by users on your local network based on their MAC Address.



MAC Address Filtering

Firewall Settings (You can change it on Firewall page)

Enable Firewall: Enabled

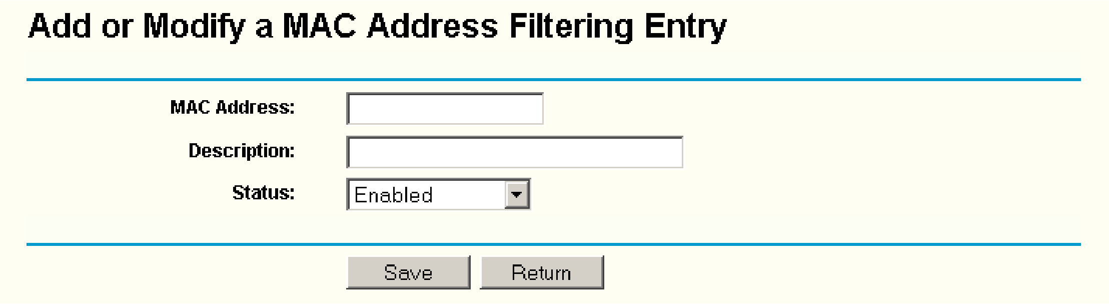
Enable MAC Address Filtering: Disabled

Default Filtering Rules: Deny these PCs with enabled rules to access the Internet

ID	MAC Address	Description	Status	Modify

Figure 5-42 MAC address Filtering

Before setting up MAC Filtering entries, you must ensure that **Enable** Firewall and **Enable** MAC Filtering have been selected on the Firewall page. To Add a MAC Address filtering entry, clicking the **Add New…** button. The page "**Add or Modify a MAC Address Filtering entry**" will appear, shown in Figure 5-43:



Add or Modify a MAC Address Filtering Entry

MAC Address:

Description:

Status: Enabled

Figure 5-43 Add or Modify a MAC Address Filtering entry

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

1. Enter the appropriate MAC Address into the **MAC Address** field. The format of the MAC Address is XX-XX-XX-XX-XX-XX (X is any hexadecimal digit). For example: 00-0E-AE-B0-00-0B.
2. Type the description of the PC in the **Description** field. Fox example: John's PC.
3. **Status** - Select **Enabled** or **Disabled** for this entry on the **Status** pull-down list.
4. Click the **Save** button to save this entry.

To add additional entries, repeat steps 1-4.

When finished, click the **Return** button to return to the **MAC Address Filtering** page.

To modify or delete an existing entry:

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

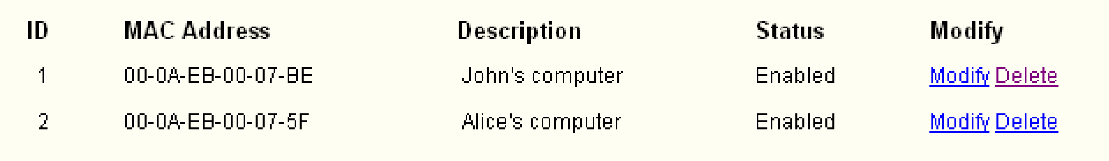
Click the **Enable All** button to make all entries enabled.

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.

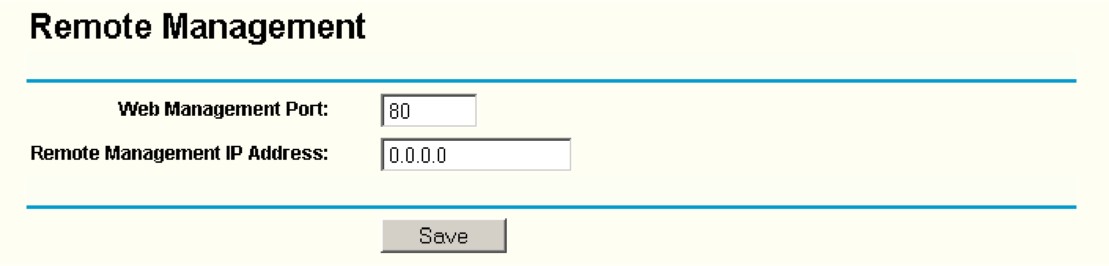
Fox example: If you want to block the PC with MAC addresses 00-0A-EB-00-07-BE and 00-0A-EB-00-07-5F to access the Internet, first, enable the **Firewall** and **MAC Address Filtering** on the **Firewall** page, then, you should specify the Default MAC Address Filtering Rule "**Deny these PC(s) with effective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



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

5.9.5 Remote Management

You can configure the Remote Management function on this page shown in Figure 5-44. This feature allows you to manage your Router from a remote location, via the Internet.



Remote Management

Web Management Port: 80

Remote Management IP Address: 0.0.0.0

Figure 5-44 Remote Management

- **Web Management Port -** Web browser access normally uses the standard HTTP service port 80. This router’s default remote management Web port number is 80. For greater security, you can change the remote management Web interface to a custom port by entering that number in this box provided. Choose a number between 1024 and 65534, but do not use the number of any common service port.
- **Remote Management IP Address -** This is the current address you will use when accessing your router from the Internet. The default IP Address is 0.0.0.0. It means this function is disabled. To enable this function, change the default IP Address to another IP Address as desired.

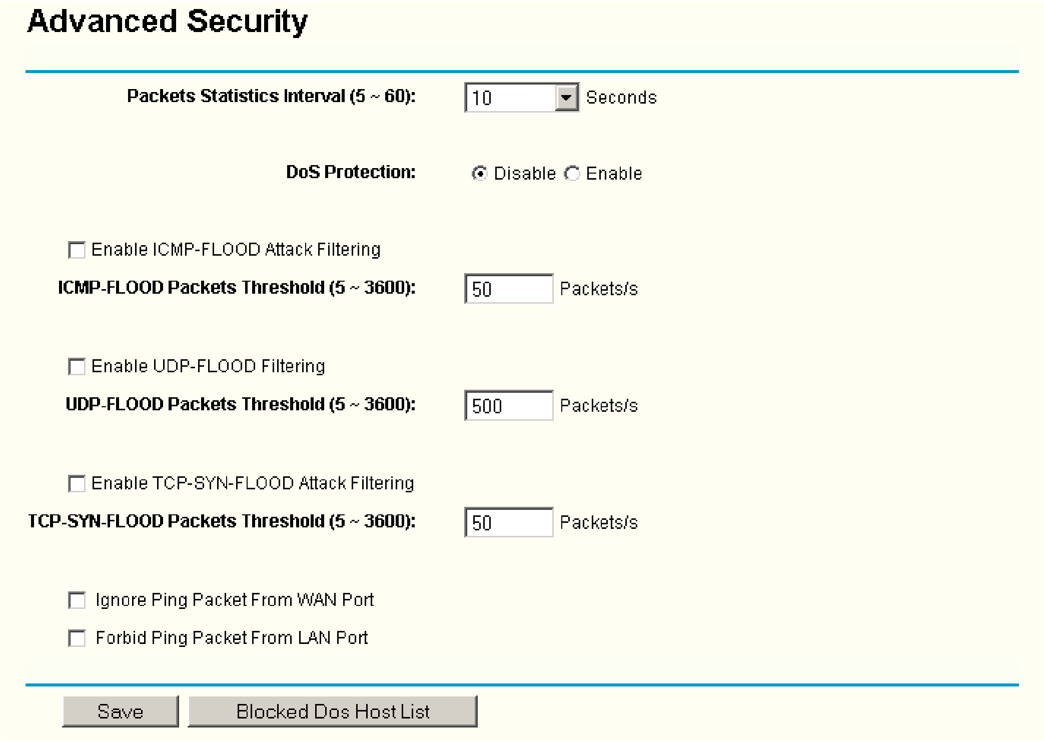
To access the router, you will type your router's WAN IP Address into your browser's Address (in IE) or Location (in Navigator) box, followed by a colon and the custom port number. For example, if your Router's WAN address is 202.96.12.8 and you use port number 8080, enter in your browser: http://202.96.12.8:8080. You will be asked for the router's password. After successfully entering the password, you will be able to access the router's Web-based utility.

☞ **Note:**

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

5.9.6 Advanced Security

Using Advanced Security page (shown in Figure 5-45), you can protect the router from being attacked by TCP-SYN Flood, UDP Flood and ICMP-Flood from LAN.



Advanced Security

Packets Statistics Interval (5 ~ 60): 10 Seconds

DoS Protection: ● Disable ○ Enable

□ Enable ICMP-FLOOD Attack Filtering

ICMP-FLOOD Packets Threshold (5 ~ 3600): 50 Packets/s

□ Enable UDP-FLOOD Filtering

UDP-FLOOD Packets Threshold (5 ~ 3600): 500 Packets/s

□ Enable TCP-SYN-FLOOD Attack Filtering

TCP-SYN-FLOOD Packets Threshold (5 ~ 3600): 50 Packets/s

□ Ignore Ping Packet From WAN Port

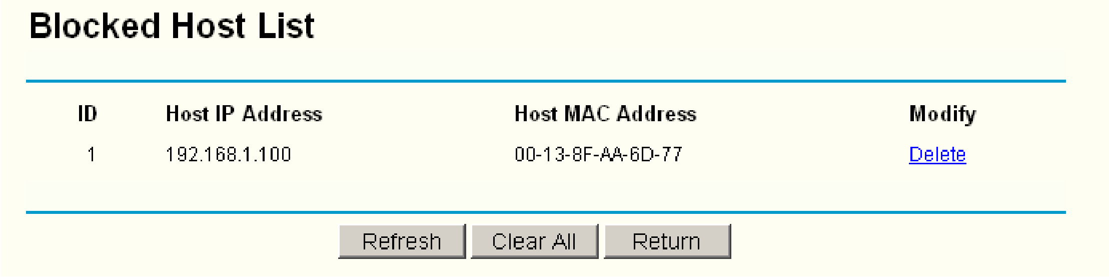
□ Forbid Ping Packet From LAN Port

Figure 5-45 Advanced Security settings

- **Packets Statistic interval (5 ~ 60) -** The default value is 10. Select a value between 5 and 60 seconds in the pull-down list. The **Packets Statistic interval** value indicates the time section of the packets statistic. The result of the statistic used for analysis by **SYN Flood**, **UDP Flood** and **ICMP-Flood**.
- **DoS protection - Enable** or **Disable** the DoS protection function. Only when it is enabled, will the flood filters be effective.
- **Enable ICMP-FLOOD Attack Filtering - Enable** or **Disable** the **ICMP-FLOOD** Attack Filtering.
- **ICMP-FLOOD Packets threshold: (5 ~ 3600) -** The default value is 50. Enter a value between 5 ~ 3600 packets. When the current **ICMP-FLOOD** Packets number sis beyond the set value, the router will start up the blocking function immediately.
- **Enable UDP-FLOOD Filtering - Enable** or **Disable** the **UDP-FLOOD** Filtering.
- **UDP-FLOOD Packets threshold: (5 ~ 3600) -** The default value is 50. Enter a value between 5 ~ 3600 packets. When the current **UPD-FLOOD** Packets numbers is beyond the set value, the router will start up the blocking function immediately.
- **Enable TCP-SYN-FLOOD Attack Filtering - Enable** or **Disable** the **TCP-SYN- FLOOD** Attack Filtering.
- **TCP-SYN-FLOOD Packets threshold: (5 ~ 3600) -** The default value is 50. Enter a value between 5 ~ 3600 packets. When the current **TCP-SYN-FLOOD** Packets numbers is beyond the set value, the router will start up the blocking function immediately.
- **Ignore Ping Packet from WAN Port - Enable** or **Disable** ignore ping packet from WAN port. The default is disabled. If enabled, the ping packet from the Internet cannot access the router.
- **Forbid Ping Packet from LAN Port -** Enable or Disable forbidding Ping Packet to access the router from the LAN port. The default value is disabled. If enabled, the ping packet from the LAN port cannot access the router. (Defends against some viruses)

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

Click the **Blocked DoS Host Table** button to display the DoS host table by blocking. The page will appear that shown in Figure 5-46:



Blocked Host List

ID	Host IP Address	Host MAC Address	Modify
1	192.168.1.100	00-13-8F-AA-6D-77	Delete

Figure 5-46 Thwarted DoS Host Table

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

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

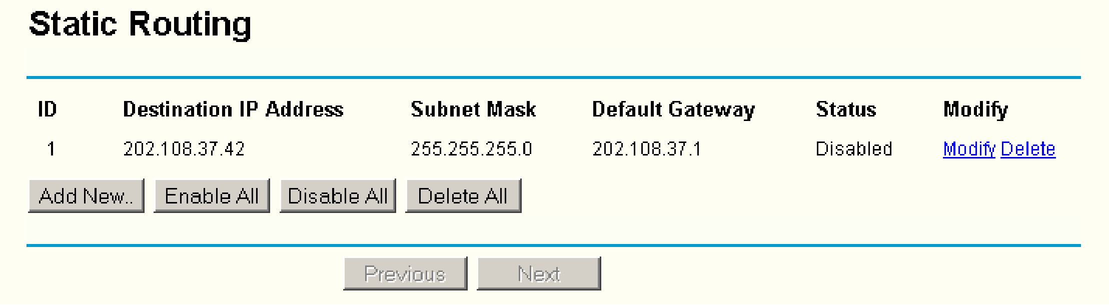
To update this page and to show the current blocked host, click on the **Refresh** button.

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

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

5.10 Static Routing

A static route is a pre-determined path that network information must travel to reach a specific host or network. To add or delete a route, work in the area under the Static Routing page (shown in Figure 5-47).



Static Routing

ID	Destination IP Address	Subnet Mask	Default Gateway	Status	Modify
1	202.108.37.42	255.255.255.0	202.108.37.1	Disabled	Modify Delete

Figure 5-47 Static Routing

To add static routing entries:

1. Click the **Add New** button. (pop up Figure 5-48)

2. Enter the following data:

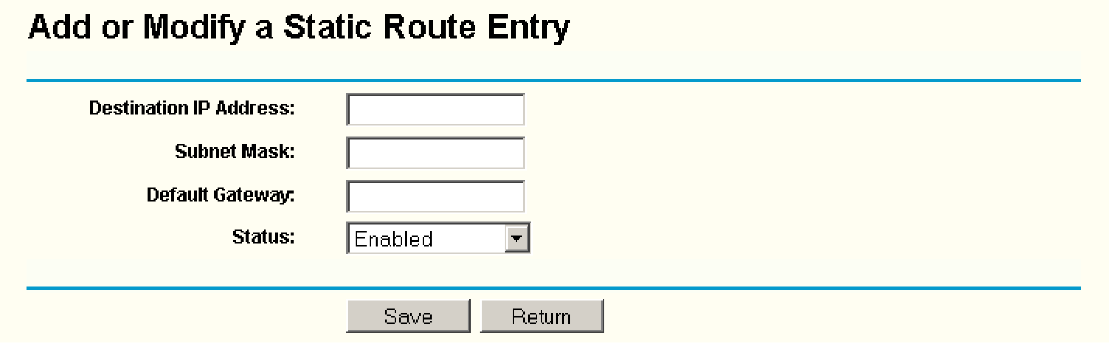
- **Destination IP Address -** The **Destination IP Address** is the address of the network or host that you want to assign to a static route.

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

- **Default 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 save it.



Add or Modify a Static Route Entry

Destination IP Address:
Subnet Mask:
Default Gateway:
Status: Enabled

Figure 5-48 Add or Modify a Static Route 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

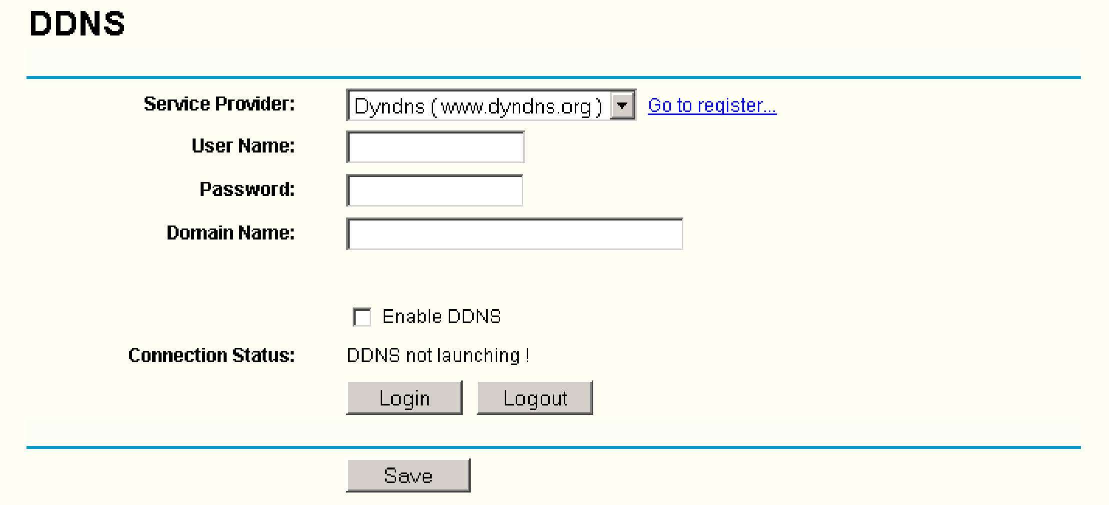
5.11 Dynamic DNS

The router offers a Dynamic Domain Name System (**DDNS**) feature. DDNS lets you assign a fixed host and domain name to a dynamic Internet IP Address. It is useful when you are hosting your own website, FTP server, or other server behind the router. Before using this feature, you need to sign up for DDNS service providers such as www.dyndns.org, www.oray.net or www.comexe.cn. The Dynamic DNS client service provider will give you a password or key.

To set up for DDNS, follow these instructions:

5.11.1 Dyndns.org DDNS

If your selected dynamic DNS **Service Provider** is www.dyndns.org, the page will appear as shown in Figure 5-49:



DDNS

Service Provider: Dyndns (www.dyndns.org) Go to register...

User Name:

Password:

Domain Name:

□ Enable DDNS

Connection Status: DDNS not launching !

Figure 5-49 Dyndns.org DDNS Settings

To set up for DDNS, follow these instructions:

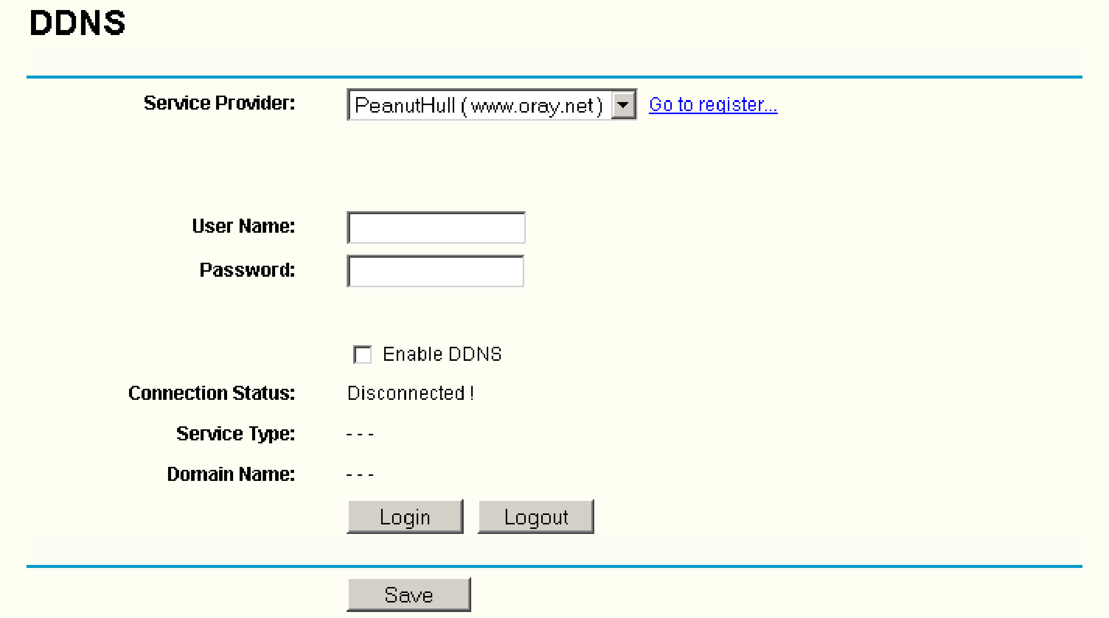
1. Type the **domain names** your dynamic DNS service provider gave.
2. **Type the User Name for** your DDNS account.
3. Type the **Password** for your DDNS account.
4. Click the **Login** button to login to the DDNS service.

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

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

5.11.2 Oray.net DDNS

If your selected dynamic DNS **Service Provider** is www.oray.net, the page will appear as shown in Figure 5-50:



DDNS

Service Provider: PeanutHull (www.oray.net) Go to register...

User Name:

Password:

□ Enable DDNS

Connection Status: Disconnected !

Service Type: - - -

Domain Name: - - -

Figure 5-50 Oray.net DDNS Settings

To set up for DDNS, follow these instructions:

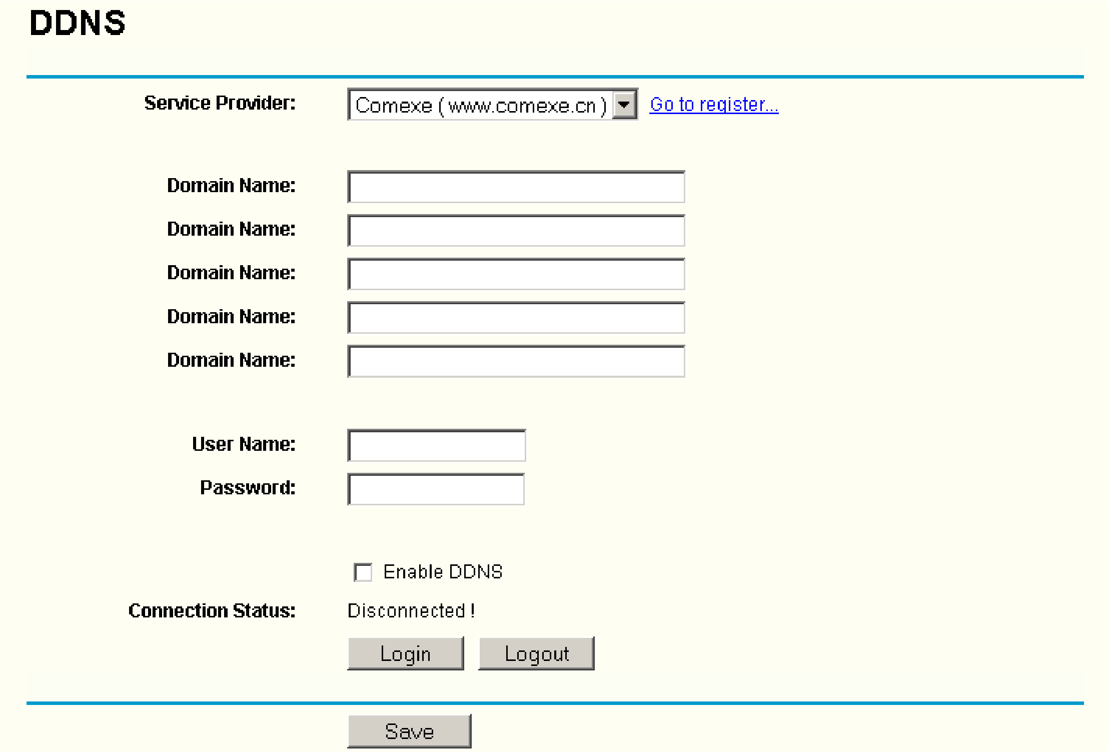
1. Type the **User Name** for your DDNS account.
2. Type the **Password** for your DDNS account.
3. Click the **Login** button to login the DDNS service.

- **Connection Status -** The status of the DDNS service connection is displayed here.
- **Domain Name -** The domain names are displayed here.

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

5.11.3 Comexe.cn DDNS

If your selected dynamic DNS **Service Provider** is www.comexe.cn, the page will appear as shown in Figure 5-51:



DDNS

Service Provider: Comexe (www.comexe.cn)

Domain Name:

Domain Name:

Domain Name:

Domain Name:

Domain Name:

User Name:

Password:

□ Enable DDNS

Connection Status: Disconnected !

Figure 5-51 Comexe.cn DDNS Settings

To set up for DDNS, follow these instructions:

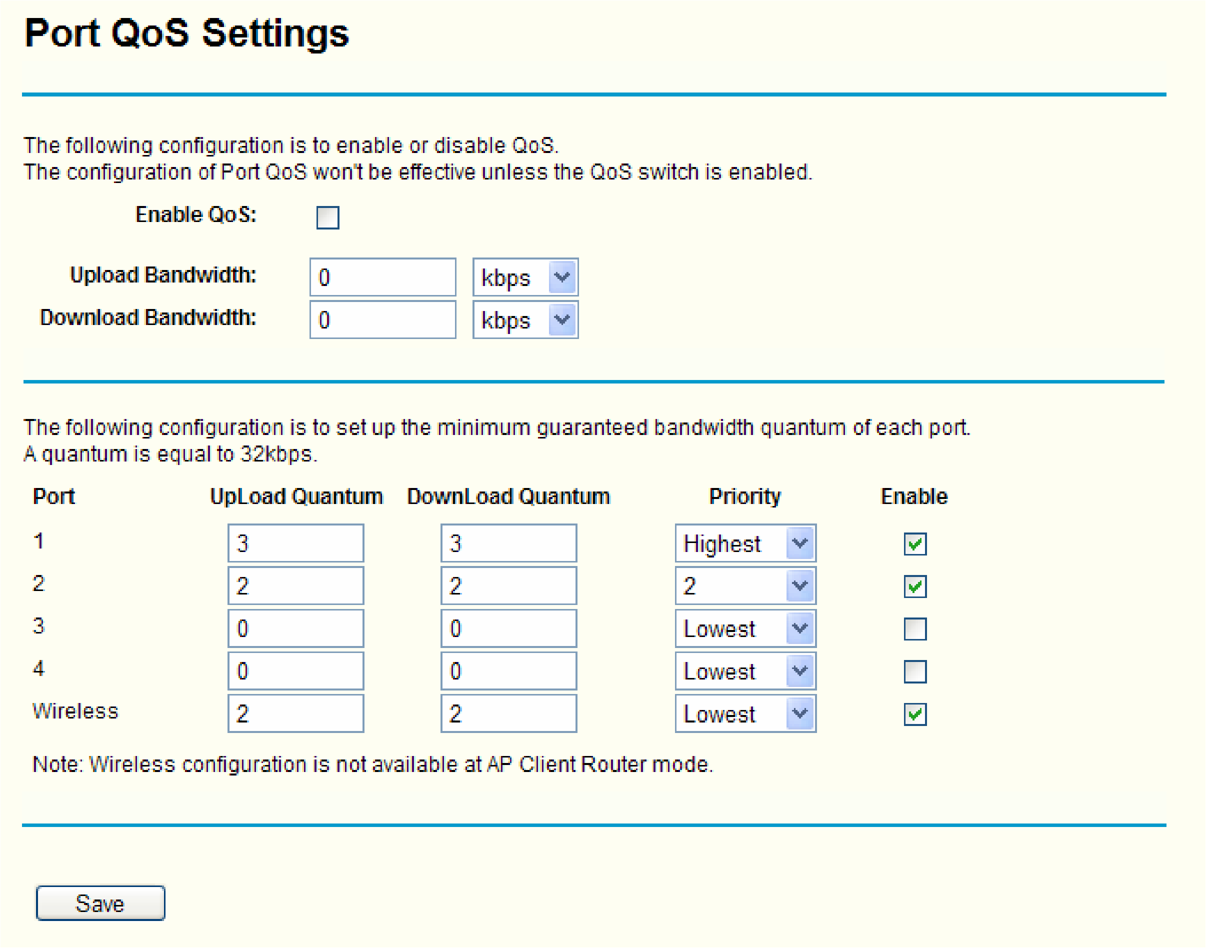
1. Type the **domain names** your dynamic DNS service provider gave.
2. Type the **User Name** for your DDNS account.
3. Type the **Password** for your DDNS account.
4. Click the **Login** button to login to the DDNS service.

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

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

5.12 Port QoS

Port QoS helps you to use the network resources more reasonable. It allows you to set the bandwidth priority for every LAN port (LAN1-4) and wireless communication. The port that has the highest priority can get the best bandwidth. You can configure the **Port QoS** on this page, shown in Figure 5-52.



Port QoS Settings

The following configuration is to enable or disable QoS.
The configuration of Port QoS won't be effective unless the QoS switch is enabled.

Enable QoS: □

Upload Bandwidth: 0 kbps

Download Bandwidth: 0 kbps

The following configuration is to set up the minimum guaranteed bandwidth quantum of each port.
A quantum is equal to 32kbps.

Port	UpLoad Quantum	DownLoad Quantum	Priority	Enable
1	3	3	Highest	☑
2	2	2	2	☑
3	0	0	Lowest	□
4	0	0	Lowest	□
Wireless	2	2	Lowest	☑

Note: Wireless configuration is not available at AP Client Router mode.

Figure 5-52 Port QoS Settings

- **Enable QoS -** Enable or Disable QoS function. It is the switch of QoS. The following Port QoS Configuration won't be effective unless it is enabled.
- **UpLoad Bandwidth -** The upload bandwidth provided by your ISP.
- **DownLoad Bandwidth -** The download bandwidth provided by your ISP.
- **Port** - There are five ports, **1**,**2**,**3**,**4** and **Wireless**, which means four physical LAN port and one wireless interface. You can set the priority for each of them.
- **Upload Quantum -** The minimum upload guaranteed bandwidth specified for corresponding port. The unitage is 32kbps. The sum of all ports' upload quantum can't be larger than Upload Bandwidth.
- **Download Quantum -** The minimum download guaranteed bandwidth specified for the corresponding port. The unitage is 32kbps. The sum of all ports' download quantum must not be larger than Download Bandwidth.
- **Priority -** Administer the distribution of surplus bandwidth. There are five priorities listed in descending order: Highest, 1, 2, 3 and Lowest. If there is still surplus bandwidth after the guaranteed bandwidth of all ports have been satisfied, the surplus bandwidth would be assigned to the highest priority port. If you specify the same priority for multi-ports at the same time, the surplus bandwidth will be shared alike by them.
- **Enable -** Enable or Disable QoS function for corresponding port. If Disabled, the port configuration will be the default value: Upload Quantum is 0, Download Quantum is 0 and Priority is "Lowest".

For example, we assume that the **UpLoad Bandwidth** and **DownLoad Bandwidth** supplied by ISP are 10Mbps respectively. If you desire **highest** priority to port 1, lower priority (take **2** level for example) to port 2 and **lowest** priority to wireless communication, you can configure the router as Figure 5-52 shown.

☞ **Note:**

1. In configuring system Bandwidth, there are two unitages provided: "kbps" means 1000 bit/sec; "Mbps" means 1000,000 bit/sec.
2. You can ask your ISP or network administrator for the actual value of system upload and download Bandwidth. If you can't get it, it is recommended strongly that you set a conservative value to avoid the configure value overstep the actual value.
3. Because a quantum is equal to 32kbps, the port guaranteed bandwidth that you configure is always multiples of 32kbps.
4. Because the wireless communication will engross good-sized of CPU, we strongly recommended that you should choose the lowest priority for wireless to avoid the excessive use of CPU.
5. For G.729A VoIP, both the recommendatory upload and download guaranteed bandwidth are 8kbps and the workable quantum is 1; For H.264 video, both the recommendatory upload and download guaranteed bandwidth are 64kbps and the workable quantum is 2.
6. Be sure to click **Save** to save the new settings for the router.
7. Wireless configuration is not available at AP Client Router mode.

5.13 System Tools

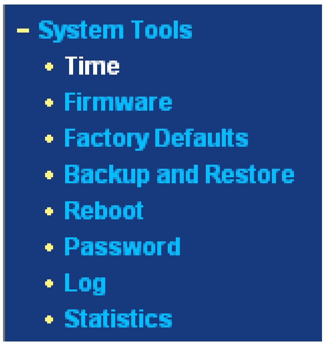
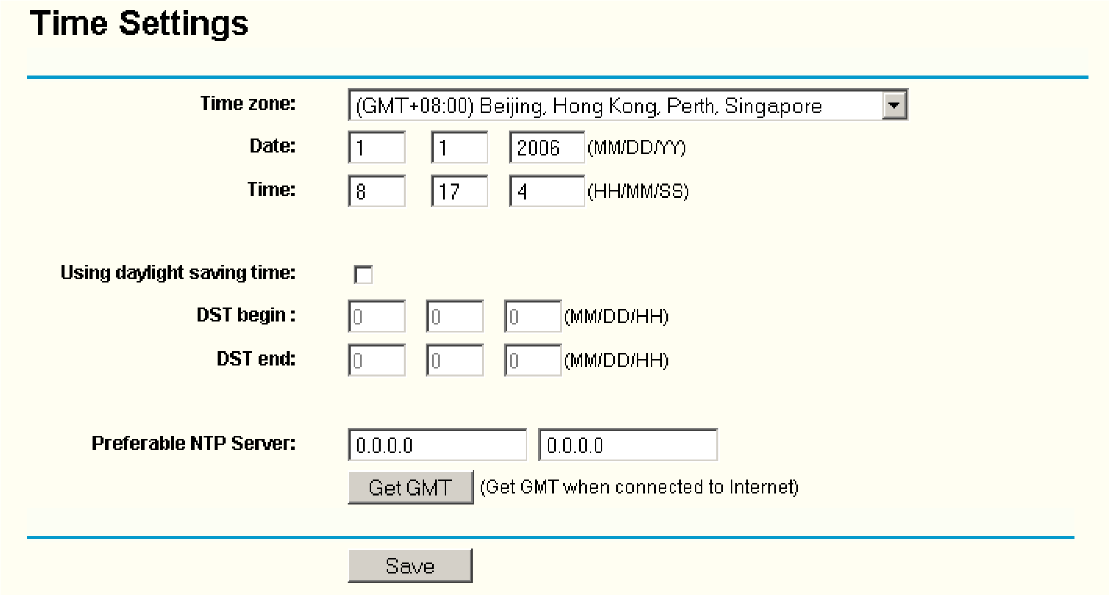


Figure 5-53 The System Tools menu

There are eight submenus under the System Tools menu (shown in Figure 5-53): **Time**, **Firmware**, **Factory Defaults, Backup and Restore, Reboot, Password, Log** 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.

5.13.1 Time

You can set time manually or get GMT from the Internet for the router on this page (shown in Figure 5-54):



Time Settings

Time zone:	(GMT+08:00) Beijing, Hong Kong, Perth, Singapore			
Date:	1	1	2006	(MM/DD/YY)
Time:	8	17	4	(HH/MM/SS)
Using daylight saving time:	□			
DST begin :	0	0	0	(MM/DD/HH)
DST end:	0	0	0	(MM/DD/HH)
Preferable NTP Server:	0.0.0.0	0.0.0.0		
	Get GMT	(Get GMT when connected to Internet)		

Figure 5-54 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.

Time setting follows these steps below:

1. Select your local time zone.
2. Enter date and time in the right blanks
3. Click **Save**.

Click the **Get GMT** button to get GMT time from the Internet if you have connected to the Internet.

If you're using Daylight saving time, please follow the steps below.

1. Select **using daylight saving time**.
2. Enter daylight saving beginning time and end time in the right blanks.

☞ **Note:**

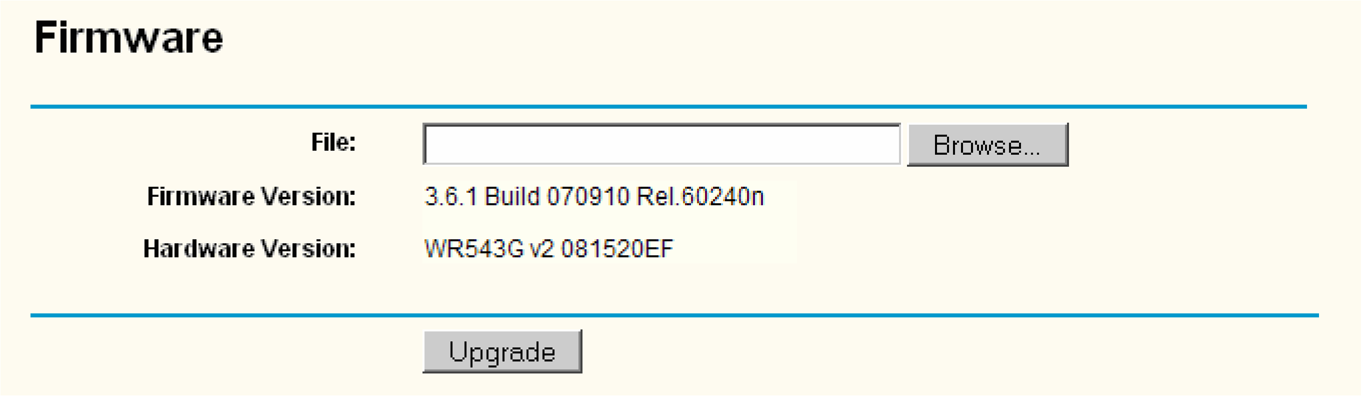
1 This setting will be used for some time-based functions such as firewall. You must specify your time zone once you login to the router successfully, if not, the time limited on these functions will not take effect.

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

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

5.13.2 Firmware

The page (shown in Figure 5-55) allows you to upgrade the latest version firmware to keep your router up-to-date.



Firmware

File:

Firmware Version: 3.6.1 Build 070910 Rel.60240n

Hardware Version: WR543G v2 081520EF

Figure 5-55 Firmware Upgrade

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

☞ **Note:**

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

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

1. Download the latest firmware upgrade file from the TP-LINK website (www.tp-link.com).
2. Click **Browse** to view the folders and select the downloaded file.
3. Click the **Upgrade** button.

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

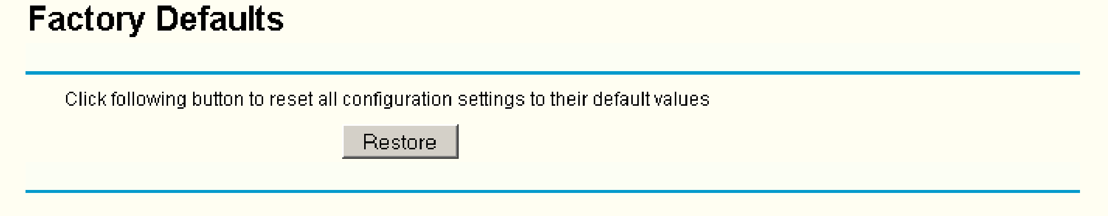
☞ **Note:**

1 Do not turn off the router or press the Reset button while the firmware is being upgraded.

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

5.13.3 Factory Defaults

This page (shown in Figure 5-56) allows you to restore the factory default settings for the router.



Factory Defaults

Click following button to reset all configuration settings to their default values

Figure 5-56 Restore Factory Default

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

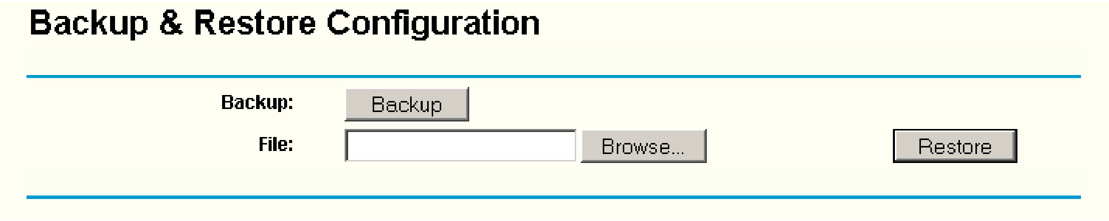
- The default **User Name**: admin
- The default **Password**: admin
- The default **IP Address**: 192.168.1.1
- The default **Subnet Mask**: 255.255.255.0

☞ **Note:**

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

5.13.4 Backup and Restore

This page (shown in Figure 5-57) allows you to save current configuration of router as backup or restore the configuration file you saved before.



Backup & Restore Configuration

Backup: Backup

File: Browse... Restore

Figure 5-57 Backup & Restore Configuration

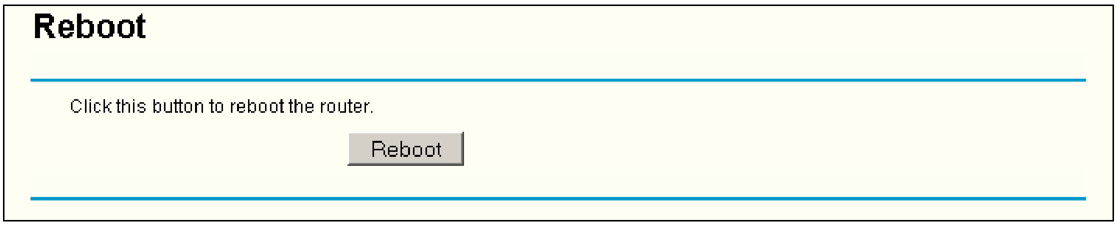
- Click the **Backup** button to save all configuration settings as a backup file in your local computer.
- To restore the router's configuration, follow these instructions:
  - Click the **Browse** button to select the backup file which you want to restore.
  - Click the **Restore** button.

☞ **Note:**

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

5.13.5 Reboot

This page (shown in Figure 5-58) allows you to reboot the router.



Reboot

Click this button to reboot the router.

Reboot

Figure 5-58 Reboot the router

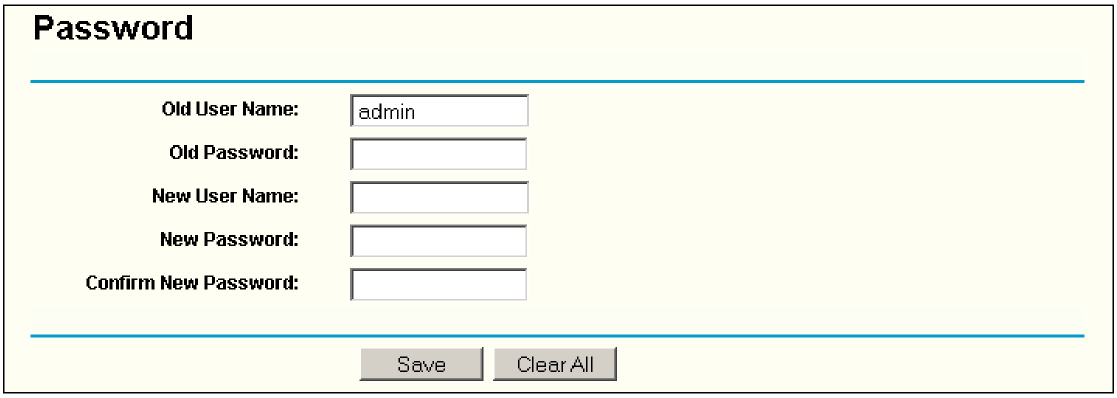
Click the **Reboot** button to reboot the router.

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

- Change LAN IP Address. (System will reboot automatically)
- MAC Clone (system will reboot automatically)
- DHCP service function.
- Static address assignment of DHCP server.
- 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).

5.13.6 Password

This page (shown in Figure 5-59) allows you to change the factory default user name and password of the router.



Password

Old User Name:	admin
Old Password:	
New User Name:	
New Password:	
Confirm New Password:	

Figure 5-59 Password

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

☞ **Note:**

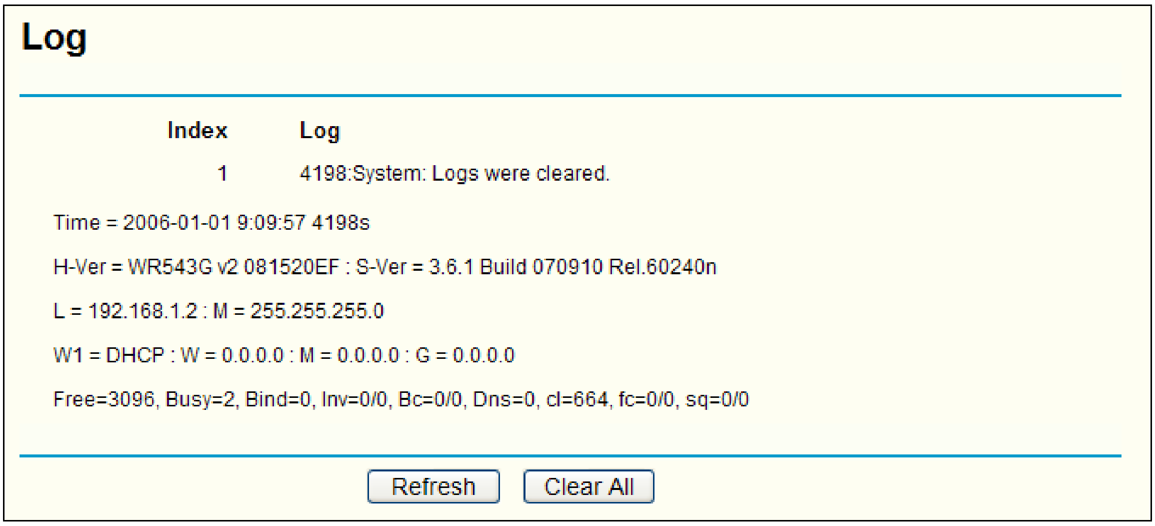
The new user name and password must not exceed 14 characters in length and must not include any spaces. Enter the new Password twice to confirm it.

Click the **Save** button when finished.

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

5.13.7 Log

This page (shown in Figure 5-60) allows you to query the logs of the router.



Log

Index	Log
1	4198:System: Logs were cleared.

```
Time = 2006-01-01 9:09:57 4198s
H-Ver = WR543G v2 081520EF : S-Ver = 3.6.1 Build 070910 Rel.60240n
L = 192.168.1.2 : M = 255.255.255.0
W1 = DHCP : W = 0.0.0.0 : M = 0.0.0.0 : G = 0.0.0.0
Free=3096, Busy=2, Bind=0, Inv=0/0, Bc=0/0, Dns=0, cl=664, fc=0/0, sq=0/0
```

Figure 5-60 System Log

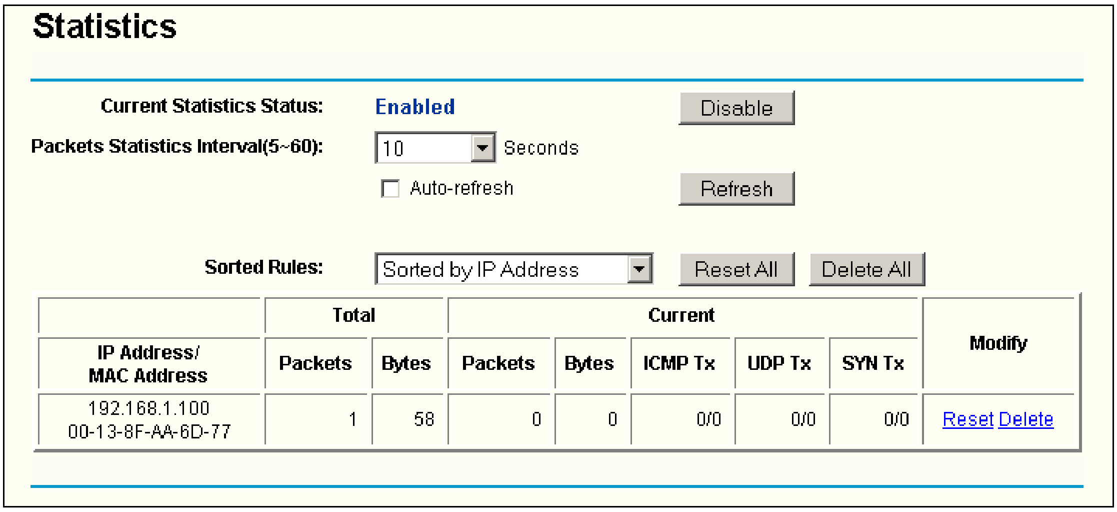
The router can keep logs of all traffic. You can query the logs to find what happened to the router.

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

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

5.13.8 Statistics

The Statistics page (shown in Figure 5-61) displays the network traffic of each PC in LAN, including total traffic and traffic of the last **Packets Statistic interval** seconds.



Statistics

Current Statistics Status: Enabled

Packets Statistics Interval(5~60): 10 Seconds

□ Auto-refresh

Sorted Rules: Sorted by IP Address

	Total		Current					Modify
IP Address/ MAC Address	Packets	Bytes	Packets	Bytes	ICMP Tx	UDP Tx	SYN Tx	
192.168.1.100 00-13-8F-AA-6D-77	1	58	0	0	0/0	0/0	0/0	Reset Delete

Figure 5-61 Statistics

- **Current Statistics Status -** Enable or Disable. The default value is disabled. To enable, click the **Enable** button. If disabled, the function of DoS protection in Security settings will be ineffective.
- **Packets Statistics Interval -** The default value is 10. Select a value between 5 and 60 seconds in the pull-down list. The Packets Statistic interval indicates the time section of the packets statistic.
- **Sorted Rules -** Here displays sort as desired

Statistics Table:

IP Address		The IP Address displayed with statistics
Total	**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.

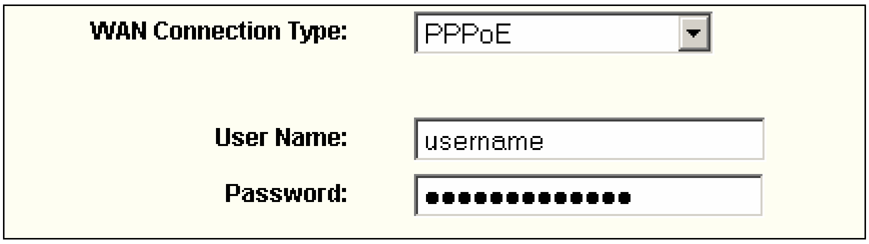
Appendix A: FAQ

1. How do I configure the router to access the 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”.



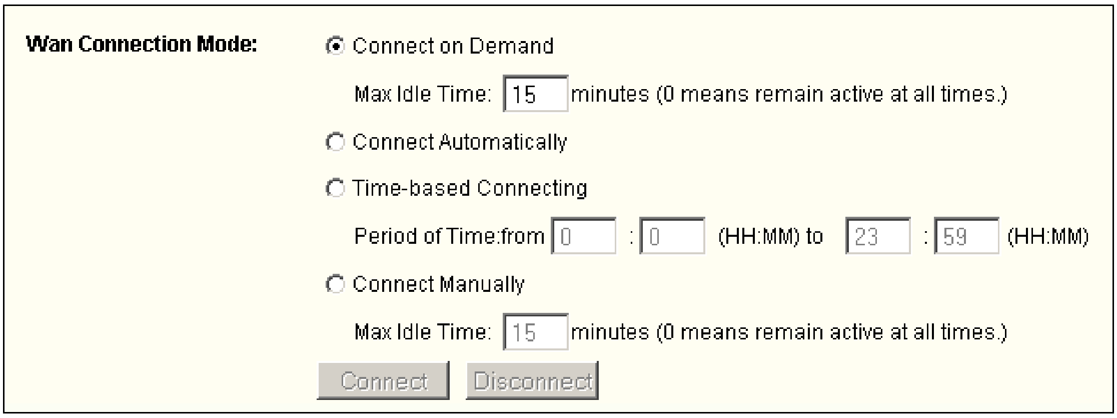
WAN Connection Type: PPPoE

User Name: username

Password: ●●●●●●●●●●●●●●

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 the Internet connection mode. Type an appropriate number for “Max Idle Time” to avoid wasting paid time. Otherwise, you can select “Auto-connecting” for the Internet connection mode.



Wan Connection Mode: ● Connect on Demand

Max Idle Time: 15 minutes (0 means remain active at all times.)

○ Connect Automatically

○ Time-based Connecting

Period of Time:from 0 : 0 (HH:MM) to 23 : 59 (HH:MM)

○ Connect Manually

Max Idle Time: 15 minutes (0 means remain active at all times.)

Figure A-2 PPPoE Connection Mode

☞ **Note:**

1. 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.

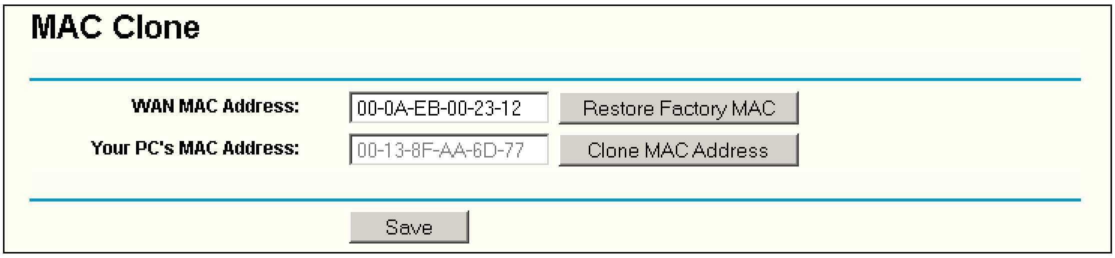
2. If you are a Cable user, please configure the router following the above steps.

2. How do I configure the router to access the 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.



MAC Clone

WAN MAC Address: 00-0A-EB-00-23-12

Your PC's MAC Address: 00-13-8F-AA-6D-77

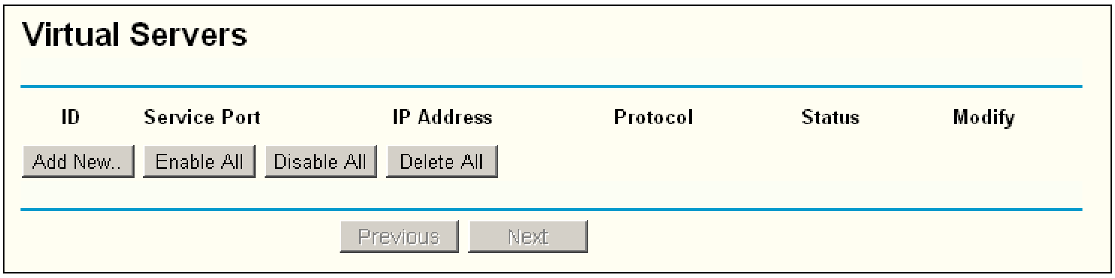
Figure A-3 MAC Clone

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.

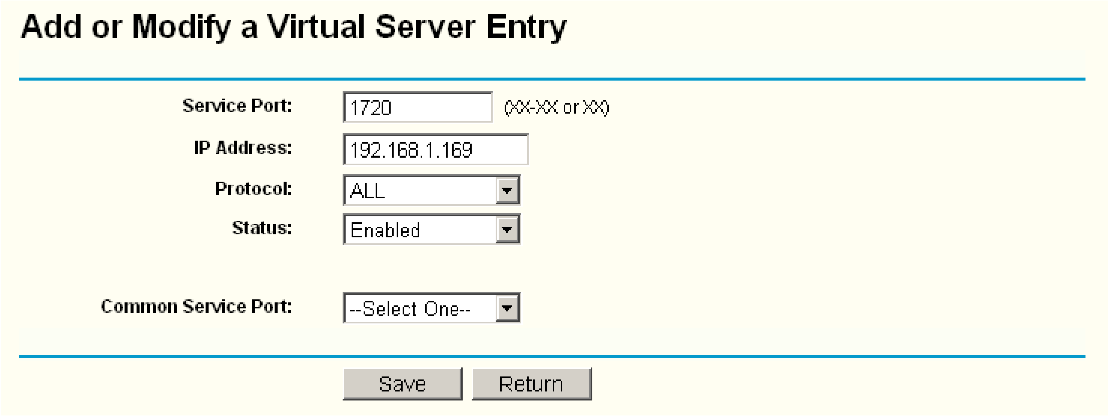
3) How to configure Virtual Server: Login to the router, click the "Forwarding" menu on the left of your browser, and click "Virtual Servers" submenu. On the "Virtual Server" page, click **Add New,** then on the "Add or Modify a Virtual Server" page, enter "1720" into the blank behind the "Service Port", and your IP address behind the IP Address, assuming 192.168.1.169 for an example, remember to "Enable" and "Save".



Virtual Servers

ID	Service Port	IP Address	Protocol	Status	Modify

Figure A-4 Virtual Servers



Add or Modify a Virtual Server Entry

Service Port: 1720 (XX-XX or XX)

IP Address: 192.168.1.169

Protocol: ALL

Status: Enabled

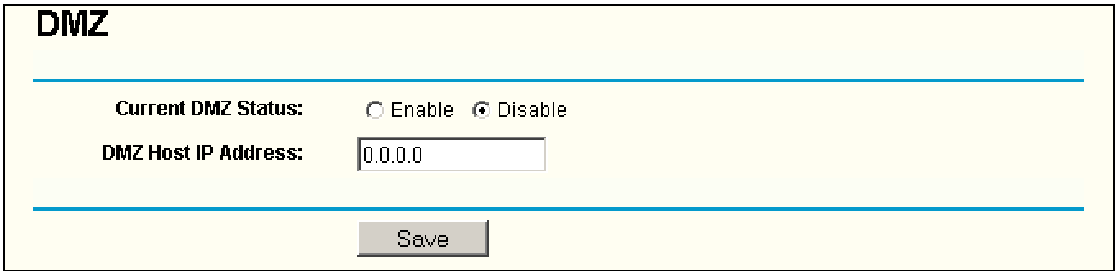
Common Service Port: --Select One--

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.



DMZ

Current DMZ Status: ○ Enable ● Disable

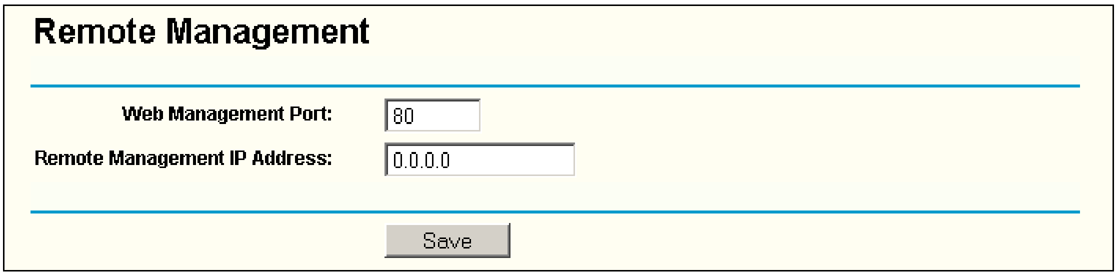
DMZ Host IP Address: 0.0.0.0

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.



Remote Management

Web Management Port: 80

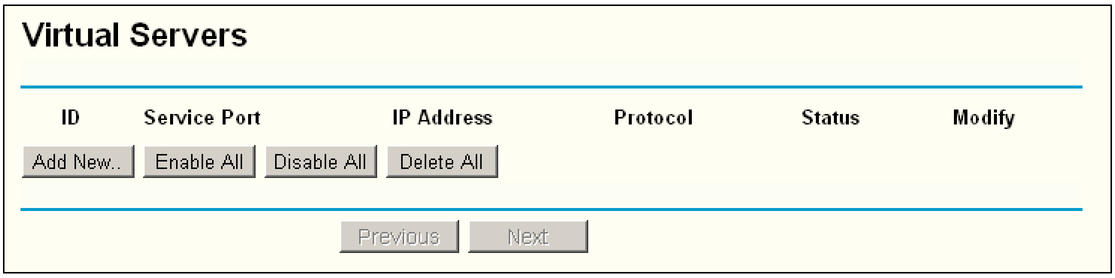
Remote Management IP Address: 0.0.0.0

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.

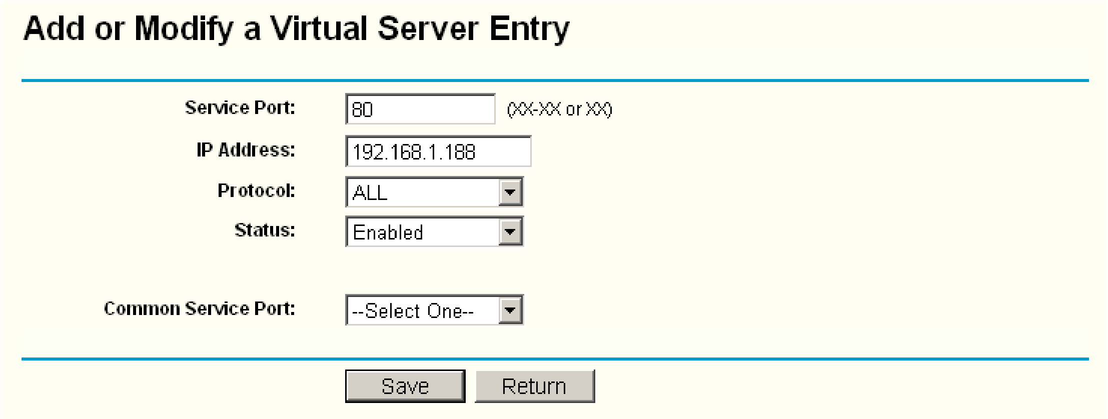
3) Login to the router, click the “Forwarding” menu on the left of your browser, and click the "Virtual Servers" submenu. On the "Virtual Server" page, click **Add New,** then on the “Add or Modify a Virtual Server” page, enter “80” into the blank behind the “Service Port”, and your IP address behind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



Virtual Servers

ID	Service Port	IP Address	Protocol	Status	Modify

Figure A-8 Virtual Servers



Add or Modify a Virtual Server Entry

Service Port: 80 (XX-XX or XX)

IP Address: 192.168.1.188

Protocol: ALL

Status: Enabled

Common Service Port: --Select One--

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 the 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 PC

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.

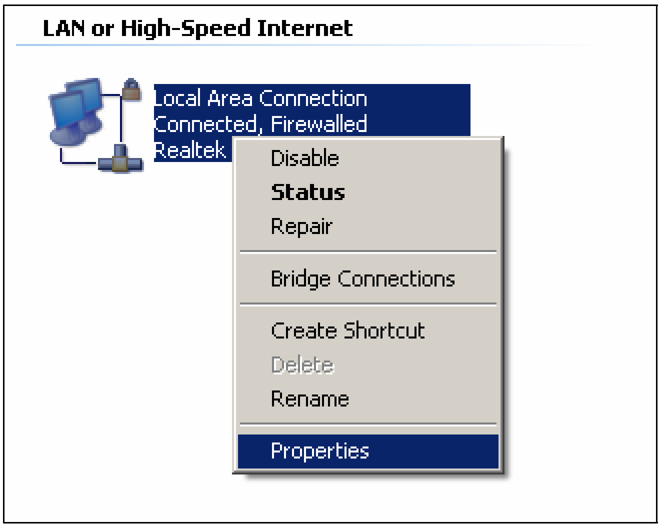
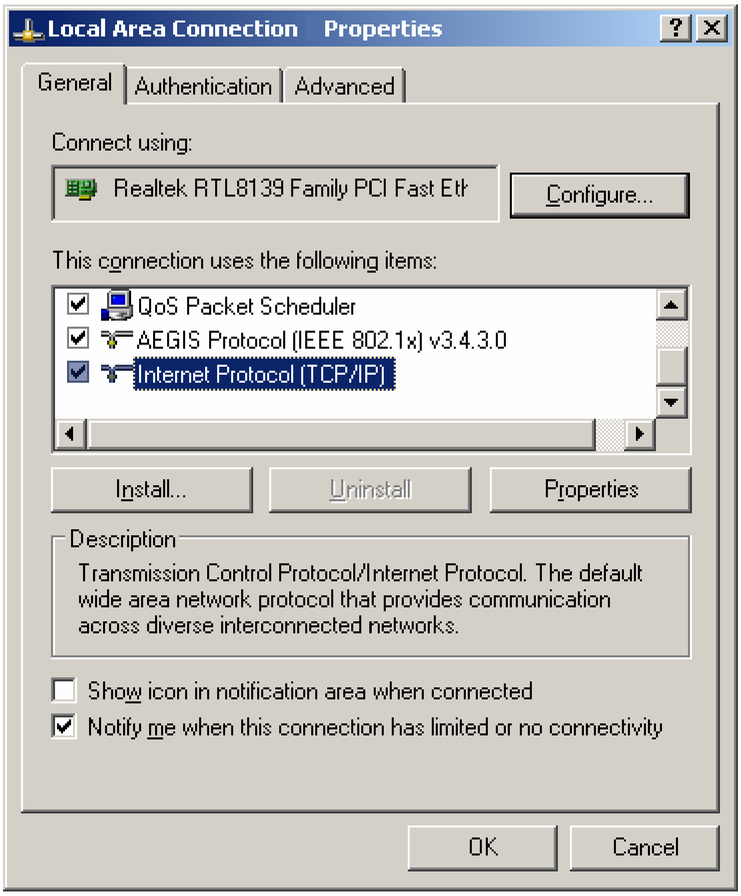


Figure 1

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



Connect using:

Realtek RTL8139 Family PCI Fast Eth

This connection uses the following items:

☑ QoS Packet Scheduler
☑ AEGIS Protocol (IEEE 802.1x) v3.4.3.0
☑ Internet Protocol (TCP/IP)

Description

Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.

☐ Show icon in notification area when connected
☑ Notify me when this connection has limited or no connectivity

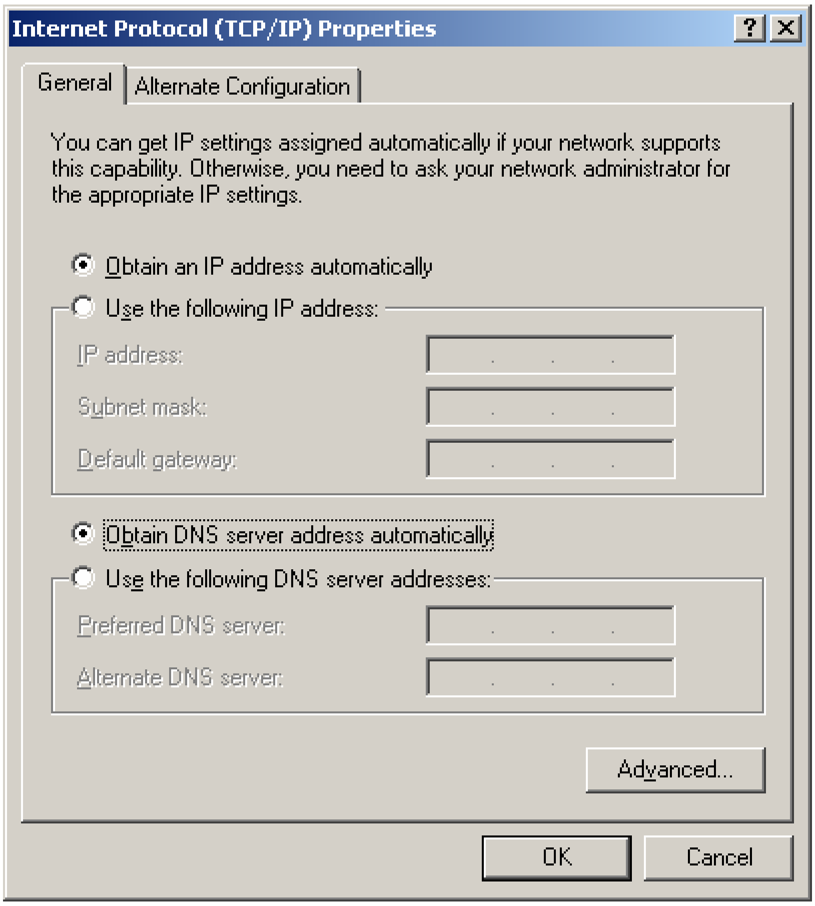
Figure 2

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:



Internet Protocol (TCP/IP) Properties

General | Alternate Configuration

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: . . .

Subnet mask: . . .

Default gateway: . . .

● Obtain DNS server address automatically

○ Use the following DNS server addresses:

Preferred DNS server: . . .

Alternate DNS server: . . .

Figure 3

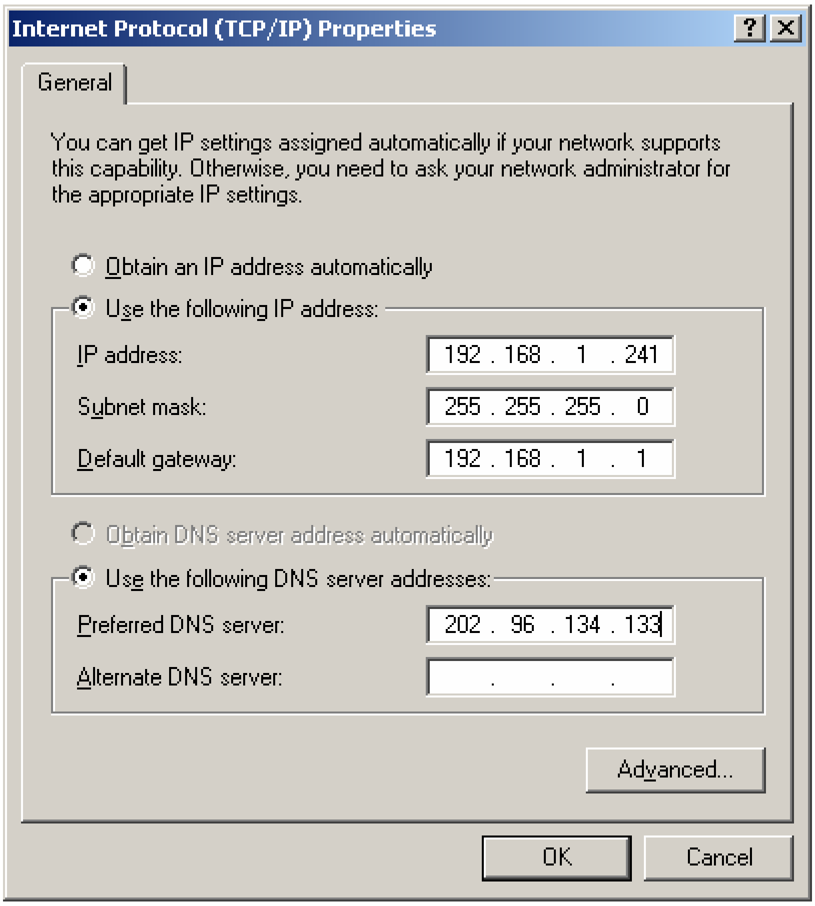
- **Setting IP address manually**

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: . . .

Figure 4

Appendix C: Specifications

General	
Standards	IEEE 802.3, 802.3u, 802.11b and 802.11g
Protocols	TCP/IP, PPPoE, DHCP, ICMP, NAT, SNTP
Ports	One 10/100M Auto-Negotiation WAN RJ45 port, Four 10/100M Auto-Negotiation LAN RJ45 ports supporting Auto MDI/MDIX
Cabling Type	10BASE-T: 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)
Radio Data Rate	54/48/36/24/18/12/9/6Mbps or 11/5.5/3/2/1Mbps
LEDs	Power, SYS, WLAN, WAN, 1-4
Safety & Emissions	FCC, CE

Environmental and Physical	
Operating Temp.	0℃~40℃ (32℉~104℉)
Operating Humidity	10% - 90% RH, Non-condensing

Appendix D: Glossary

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

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

- **802.11g -** 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** (**Dem**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.

- **DoS** (**D**enial **o**f **S**ervice) **-** A hacker attack designed to prevent your computer or network from operating or communicating.

- **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.

http://www.tp-link.com