TP-LINK®

User Guide

TL-WA5110G

54M High Power Wireless Access Point

Rev: 1.0.0
1910010154

COPYRIGHT & TRADEMARKS

http://www.tp-link.com

FCC STATEMENT

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

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

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

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

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

FCC RF Radiation Exposure Statement

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

"To comply with FCC RF exposure compliance requirements, this grant is applicable to only Mobile Configurations. The antennas used for this transmitter must be installed to provide a separation distance of at least 20 cm from all persons and must not be co-located or operating in conjunction with any other antenna or transmitter."

CE Mark Warning

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

Note: It’s not used outdoors in France.

DECLARATION OF CONFORMITY

For the following equipment:

Product Description: **54 M High Power Wireless Access Point**

Model No.: **TL-WA5110G**

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 V1.7.1: 2006

ETSI EN 301 489-1 V1.8.1:2008 & ETSI EN 301 489-17 V1.3.2:2008

EN60950-1:2006

EN62311:2008

Directives 2004/108/EC

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

EN 55022:2006+A1:2007

EN 55024:1998+A1:2001+A2:2003

EN 61000-3-2:2006

EN 61000-3-3:1995+A1:2001+A2:2005

Directives 2006/95/EC

The above product is in conformity with the following standards or other normative documents **EN60950-1:2006**

Person is responsible for marking this declaration:

Zhao Jianjun

Director of International Business

TP-LINK TECHNOLOGIES CO., LTD.

South Building, No.5 Keyuan Road, Central Zone, Science & Technology Park, Nanshan,

Shenzhen, P. R. China

CONTENTS

Package Contents

The following items should be found in your package:

- One TL-WA5110G 54M High Power Wireless Access Point
- One AC power Adapter for TL-WA5110G 54M High Power Wireless Access Point
- One Power Injector
- Quick Installation Guide
- One Resource CD for TL-WA5110G 54M High Power Wireless Access Point, including:
  - This User Guide
  - Other Helpful Information

☞ **Note:**

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

Chapter 1. Product Overview

Thank you for choosing **TL-WA5110G 54M High Power Wireless Access Point**

1.1 Overview of the Product

The TL-WA5110G 54M High Power Wireless Access Point is dedicated to Small Office/Home Office (SOHO) wireless network solutions. The TL-WA5110G 54M High Power Wireless Access Point will allow you to connect your network with other wireless devices wirelessly, sharing Internet Access, files and fun, easily and securely. The high power design will also help you build a more stable link or cover more area whether indoors or outdoors.

The TL-WA5110G 54M High Power Wireless Access Point provides 3 operation modes for multi-user to access the Internet: AP client router, AP router and AP. In AP client router mode, it works as a WISP CPE and can access the Internet wirelessly via your WISP. In AP router mode, it can access the Internet via an ADSL/Cable Modem, while sharing data wirelessly. In AP mode it can work in various modes, such as Access Point/Client/WDS Bridge/Repeater.

With the most attentive wireless security, the TL-WA5110G 54M High Power Wireless Access Point provides multiple protection measures. It can be set to turn off wireless network name (SSID) broadcast so that only stations that have the SSID can be connected. The AP 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-WA5110G 54M High Power Wireless Access Point complies with the IEEE 802.11g and IEEE 802.11b standards so that the data transmission rate is up to 54Mbps. The wireless transmission range can extend up to tens of kilometers.

The TL-WA5110G 54M High Power Wireless Access Point 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 more quickly and easily.

1.2 Features

- Complies with IEEE 802.11g, IEEE 802.11b, IEEE 802.3, IEEE 802.3u standards.
- Wireless Data transfer rates up to 54Mbps.
- Supports AP Client Router, AP Router and AP operation mode.
- High output transmit power and receive sensitivity optimized.
- Supports Client Router Mode for WISP CPE
- Supports passive power over Ethernet.
- Supports Wireless Distribution System (WDS).
- ACK timeout adjustment for long range transmission, up to 50km.
- Supports Antenna Alignment.
- Provides throughput monitor indicating the current wireless throughput.
- Supports Layer 2 User Isolation.
- Supports Ping Watch Dog.
- Supports link speed test.
- Supports Remote Management
- Output transmit power adjustable.

- Supports PPPoE, Dynamic IP, Static IP Internet Access.
- Built-in NAT and DHCP server supporting static IP address distributing.
- Supports UPnP, Dynamic DNS, Static Routing, VPN Pass-through.
- Supports 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).
- Supports configuration backup/restore and firmware upgrade.
- Supports Web management.

1.3 Conventions

The AP or TL-WA5110G, or device mentioned in this User guide stands for TL-WA5110G 54M High Power Wireless Access Point without any explanations.

Parameters provided in the pictures are just references for setting up the product, which may differ from the actual situation.

You can set the parameters according to your demand.

Chapter 2. Hardware Installation

2.1. The Front Panel

The front panel of the TL-WA5110G 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

LED Explanation：

Name	Status	Indication
Power	Off	No Power
	On	Power on
System	Off	The AP has a hardware error
	On	The AP is initialising
	Flashing	The AP is working properly
LAN	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
WLAN	Off	The Wireless Radio function is disabled
	Flashing	The Wireless Radio function is enabled

Table 2-1

2.2. The Rear Panel

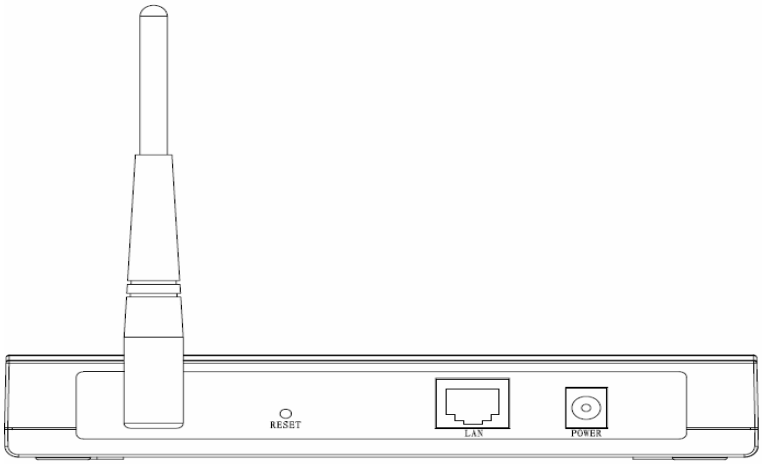


Figure 2-2 Rear Panel sketch

- Wireless antenna
- Factory Default Reset button
- There are three ways to reset the AP's factory defaults:

- Use the **Factory Defaults** function on **System Tools** -> **Factory Defaults** page in the AP's Web-based Utility.
- Use the Factory Default Reset button: Press and hold the default Reset button for 5 seconds, and then the AP reboot after the System led flash 5 times.
- Use the Factory Default Reset button: First, turn off the AP's power. Second, press and hold the default Reset button then turn on the AP's power, until the system LED lights up (about 3 seconds). Last, release the reset button and wait for the AP to reboot.

☞ **Note:**

Ensure the AP is powered on before it restarts completely.

- One LAN 10/100Mbps RJ45 port for connecting the AP to hub or switch
- AC power socket: only use the power adapter supplied with the TL-WA5110G 54Mbps Wireless Access Point, use of a different adapter may result in product damage.

2.3. 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)

2.4. 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

2.5. Connecting the Device

Figure 2-3 is an example of an infrastructure network incorporating the TL-WA5110G. An Infrastructure network contains an access point or a wireless router. To establish an infrastructure network in AP mode, please take the following steps:

1. You will need broadband Internet access (a Cable or DSL-subscriber line into your home or office). Consult with your Cable or DSL provider for proper installation of the modem.
2. Connect the Cable or DSL modem to a Router. Quickly install the router.
3. Locate an optimum location for the AP. The best place is usually near the center of the area in which your PC(s) will wirelessly connect. The place must accord with the Installation Environment Requirements.

4. Adjust the direction of the antenna. Normally, upright is a good direction.
5. Connect the Ethernet Broadband Router to the TL-WA5110G AP. Power on the AP.
6. If you are connecting a desktop PC or laptop to your network, install the TP-LINK Wireless Adapter on the PC.

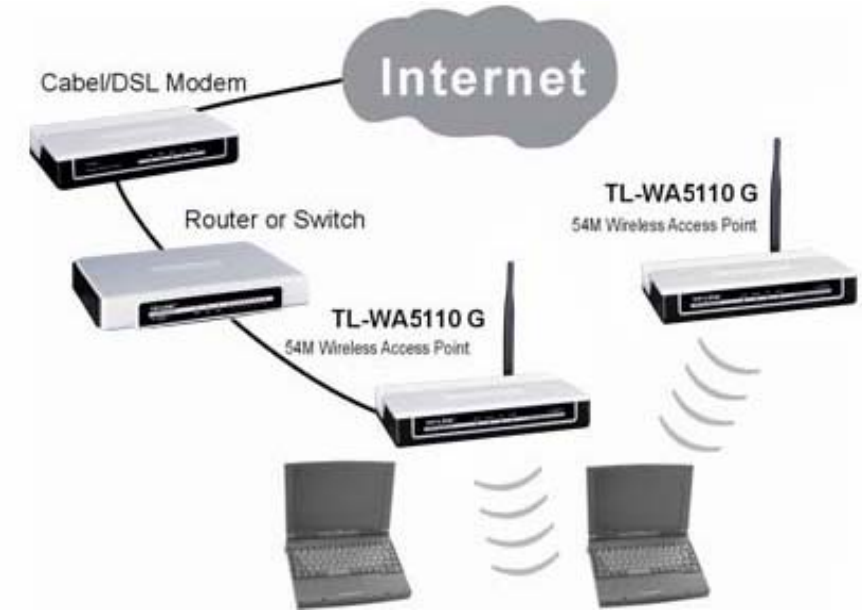


Figure 2-3

To establish an infrastructure network in AP Client Router mode as Figure 2-4, please take the following steps:

1. Make sure you are provided with wireless Internet service by your WISP(Wireless Internet Service Provider).
2. Locate an optimum location for the AP. Try to place your AP in an appropriate position where it can well receive the signal from WISP.
3. Connect the AP to the desktop PC.
4. Adjust the direction of the antenna. Normally, upright is a good direction.
5. Power on the AP and then you can configure the AP on the web-based page on your computer.

Figure 2-4

Chapter 3. Quick Installation Guide

This Chapter will guide you to configure the AP to function in your network and gain access to the internet through your ISP immediately after successful configuration. More detailed description of the AP's web-based utility and functions can be found in "Chapter 4 Configuring the AP"

3.1. Configure the Device

The instructions in this section will help you configure each of your PCs to be able to communicate with the AP.

The default IP address of the TL-WA5110G 54M High Power Wireless Access Point 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 AP. 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 AP's default IP address)

- Obtain an IP address automatically

  This method can be available only when **DHCP** in section 4.7.1 is enabled.

  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 AP and PC. Then turn on the AP and restart the PC. The built-in DHCP server will assign IP address for the PC.

☞ **Note:**

For Windows 98 OS or earlier, the PC and AP may need to be restarted.

Now, you can run the Ping command in the **command prompt** to verify the network connection between your PC and the AP. 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 3-1, the connection between your PC and the AP has been established.

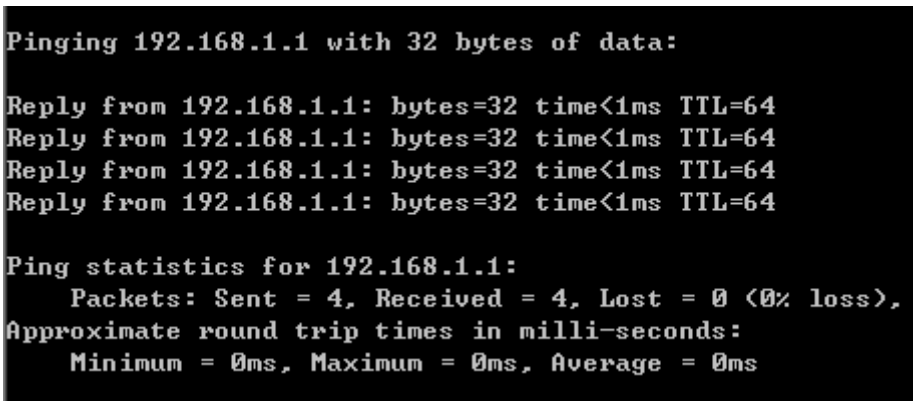


Figure 3-1 Success result of Ping command

If the result displayed is similar to that shown in Figure 3-2, it means that your PC has not connected to the AP.

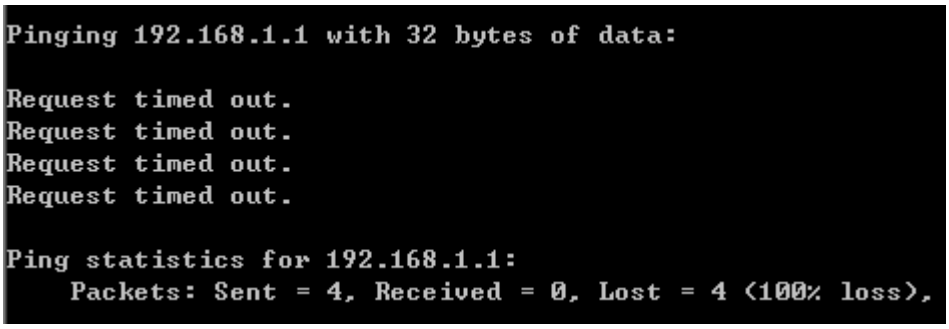


Figure 3-2 Failure result of Ping command

Please check the connection following these steps:

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

☞ **Note:**

The LED of LAN port you link to on the AP and LEDs on your PC's adapter should be lit.

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

☞ **Note:**

If the AP'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

3.2. Quick Setup

The following instructions will guide you through a few easy steps to configure your AP and connect to Internet. With a Web-based (Internet Explorer or Netscape® Navigator) utility, it is easy to configure and manage the TL-WA5110G 54M High Power Wireless Access Point. The Web-based utility can be used on any Windows, Macintosh or UNIX OS with a Web browser.

Open your web browser and enter the IP address of the AP (192.168.1.1), and a login screen will display(shown in Figure 3-3).

Figure 3-3 Login the router

Enter **admin** for Username and Password(both in lower case letters) on the following login screen. Click **OK** or press **Enter** of your keyboard, and the management page will display.

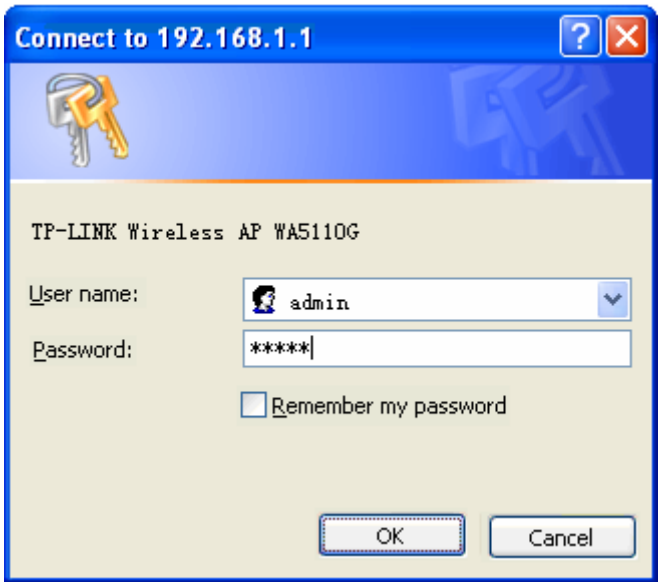


Figure 3-4 Login Windows

Note:

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

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

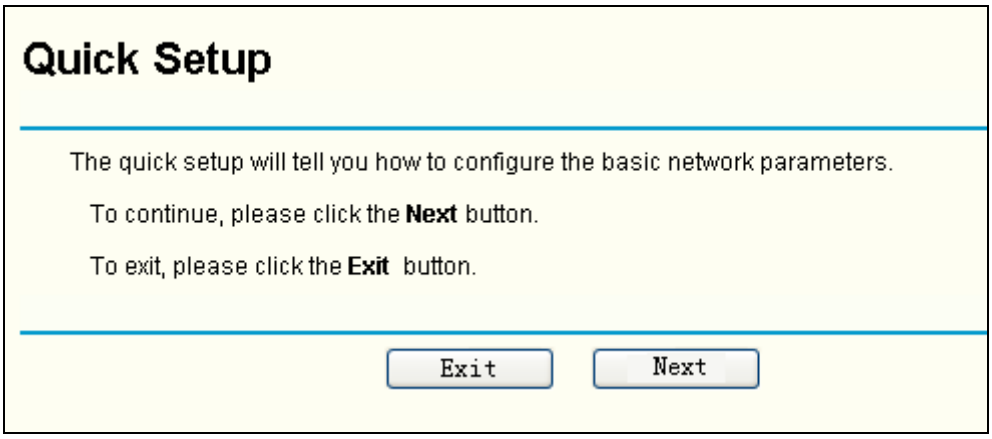


Figure 3-5 Quick Setup

Click **Next**, and then **Choose Operation mode** page will appear, shown in Figure 3-6:

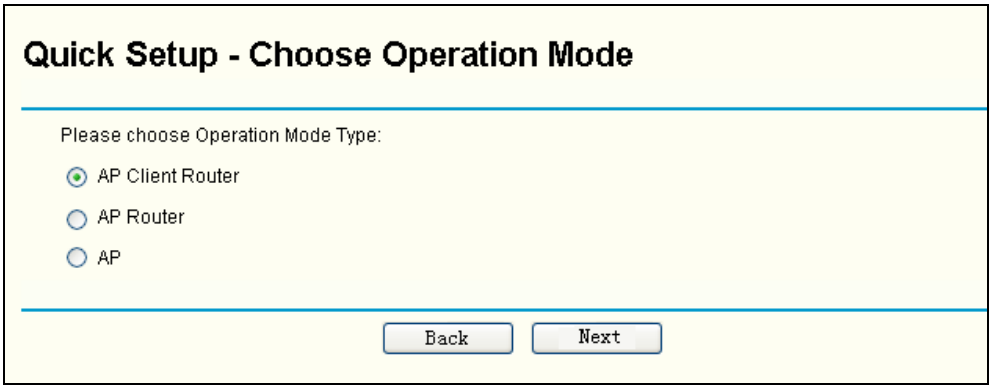


Figure 3-6 Choose Operation mode

☞ Note:

The AP supports three mode operation modes for multi-user to access the Internet: AP client router, AP router and AP. 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 AP mode, it can access a wireless network by using WIFI. You can configure your device quickly by the following steps in different modes.

A. When you choose **AP Client Router** or **AP Router mode**, take the following steps:

1. click **Next**, and then **Choose WAN Connection Type** page will appear, shown in Figure 3-7:

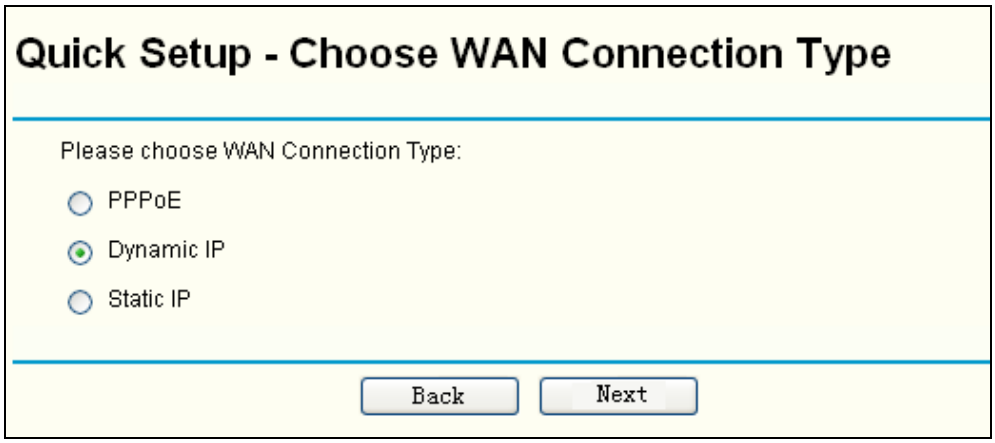


Figure 3-7 Choose WAN Connection Type

The AP in AP Client Router and AP Router mode supports three popular ways to connect to the Internet. Please select one compatible with your ISP.

2. Click **Next** to enter the necessary network parameters.

   a). If you choose "**PPPoE**", you will see this page shown in Figure 3-8:

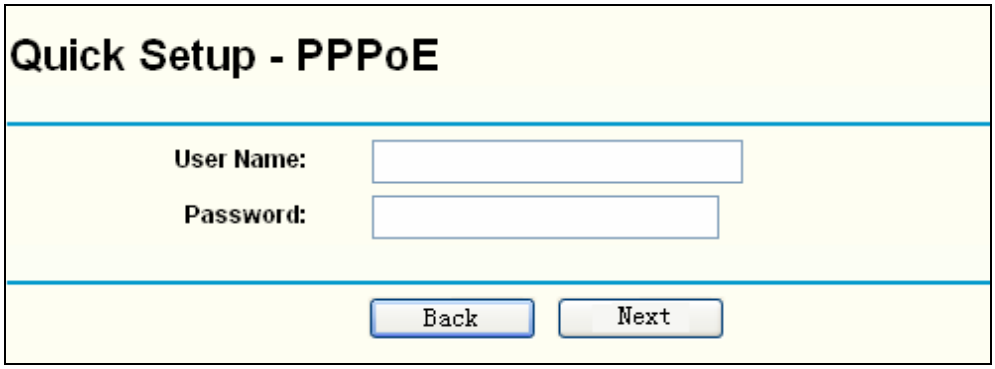


Figure 3-8 Quick Setup - PPPoE

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

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

   c). If you Choose "**Static IP**", the Static IP settings page will appear, shown in Figure 3-9:

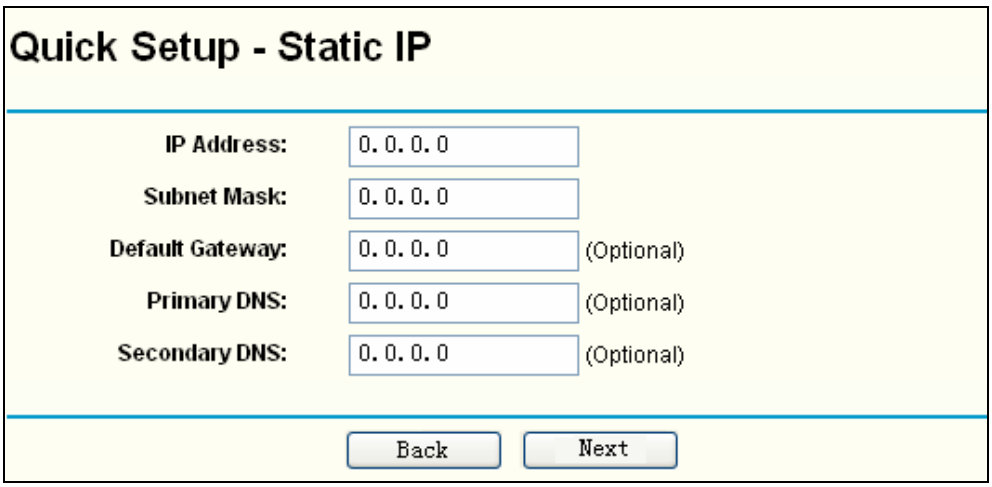


Figure 3-9 Quick Setup - Static IP

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.

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

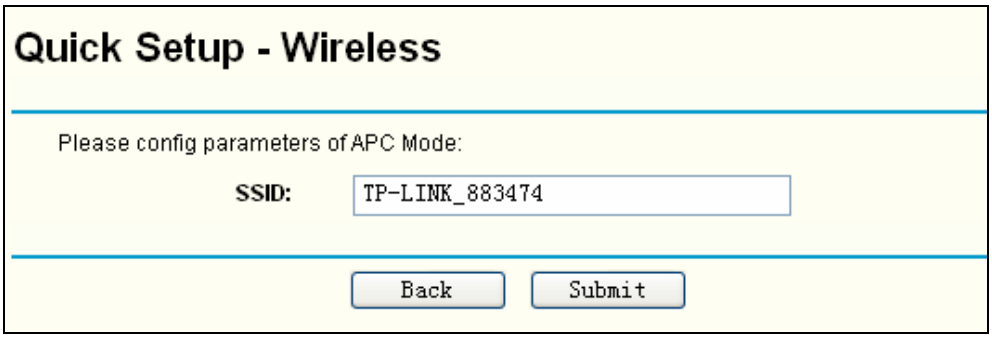


Figure 3-10 Quick Setup - Wireless settings

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

Note:

The **Quick Setup - Wireless** page differs in different modes. If you choose the AP Router mode, you will see the Wireless page as below

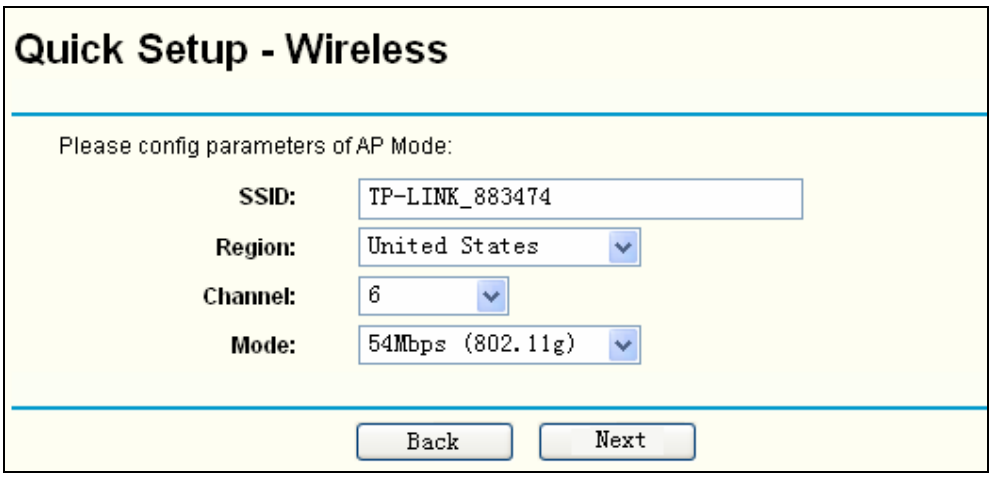


Figure 3-11 Quick Setup - Wireless settings

- **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 4.6: "Wireless."

B. When you choose **AP mode** on **Quick Setup - Choose Operation Mode** page (shown as Figure 3-6), you will directly go to the Wireless page as Figure 3-11 above.

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

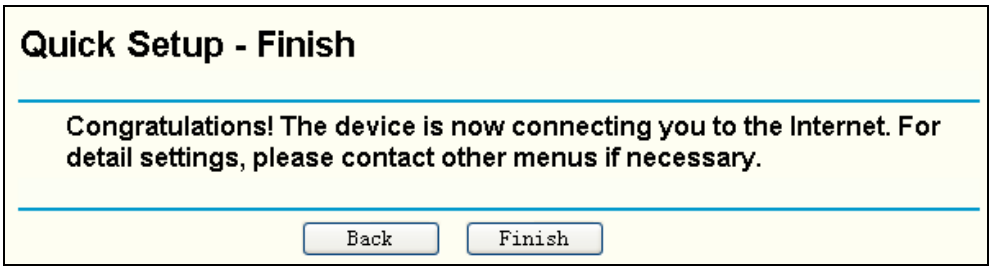


Figure 3-12 Quick Setup - Finish

After finishing all configurations of basic network parameters, please click **Finish** button to exit this **Quick Setup** and wait your device reboot automatically. The changes of wireless settings will take effect after rebooting.

Chapter 4. Configuring the Device in AP Client Router & AP Router Operation Mode

This Chapter describes how to configure some advanced settings for your Access Point through the web-based management page. In the following explanations, we will take the device in AP Client Router operation mode for example.

4.1 Login

After your successful login, you can configure and manage the Access Point. There are thirteen main menus on the left of the Web-based management page. Submenus will be available after you click one of the main menus. The thirteen main menus are: **Status, Quick Setup, Operation Mode, Network, Wireless, DHCP, Wireless Settings, Forwarding, Security, Static Routing, IP & MAC Binding, Dynamic DNS** and **System Tools.** On the right of the Web-based management page, there are the detailed explanations and instructions for the corresponding page. To apply any settings you have altered on the page, please click **Save**.

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

4.2 Status

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

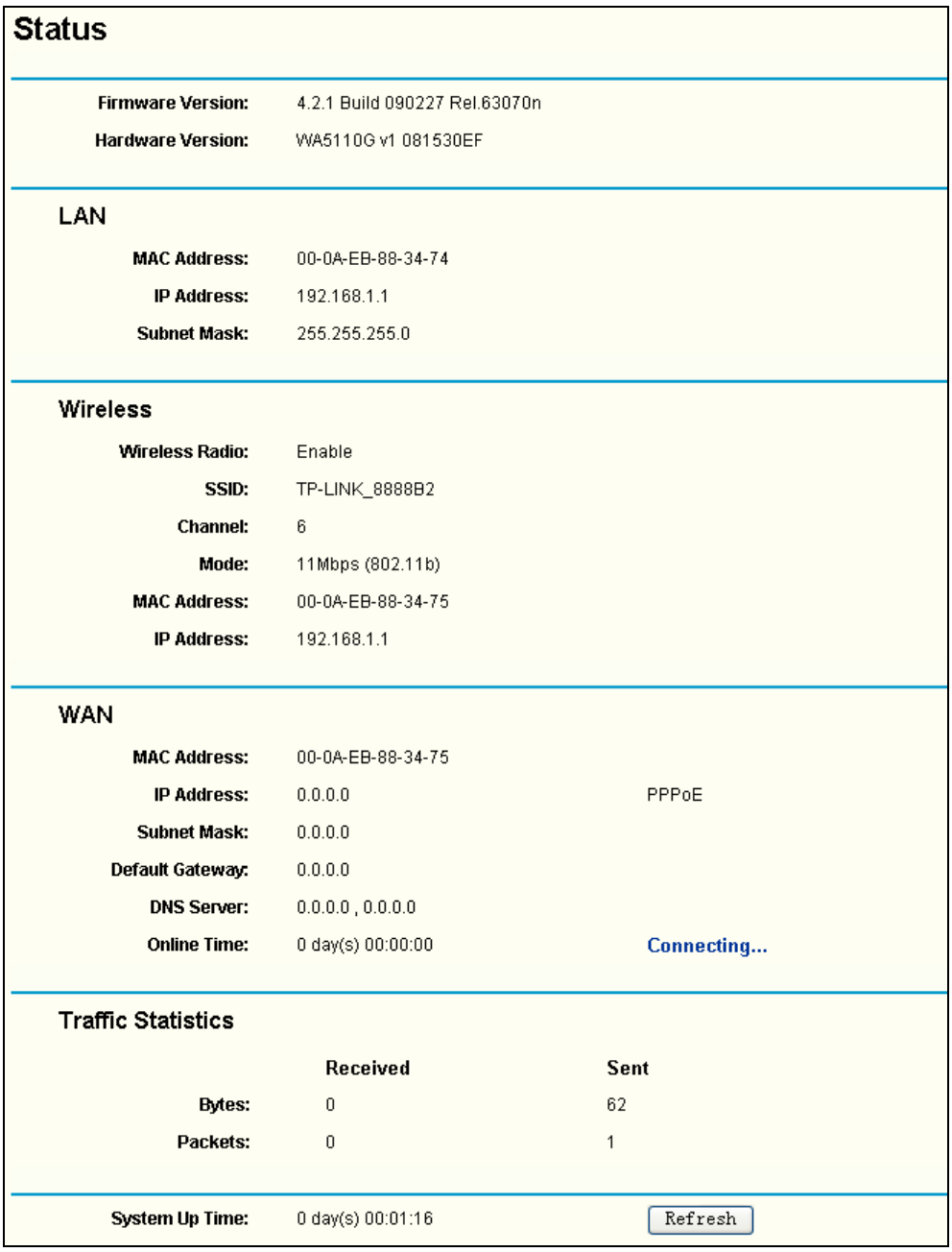


Figure 4-1 Status

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** and **DNS server** 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.

4. **Traffic Statistics**

This field displays the router's traffic statistics.

5. **System Up Time**

The total up time of the router since it was powered on or reset.

4.3 Quick Setup

Please refer to Section 3.2: "Quick Setup."

4.4 Operation Mode

The AP supports three operation mode types, **AP Client Router**, **AP Router** and **AP**. Please select one your want. Click **Save** to save your choice. Figure 4-2:

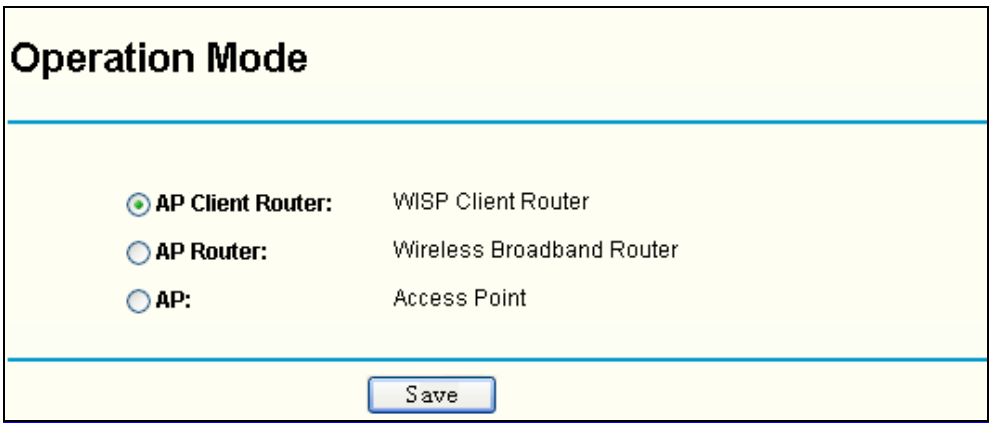


Figure 4-2 Operation Mode

- **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 port acts as a LAN port.
- **AP Router:** In this mode, the device enables multi-user to share the Internet via ADSL/Cable Modem. 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.
- **AP:** In this mode, the device allows wireless communication devices to access a wireless network by using WIFI. The Ethernet port and the wireless port both work as LAN ports.

4.5 Network

Figure 4-3 the Network menu

There are three submenus under the Network menu (shown in Figure 4-3): **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.

4.5.1 LAN

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

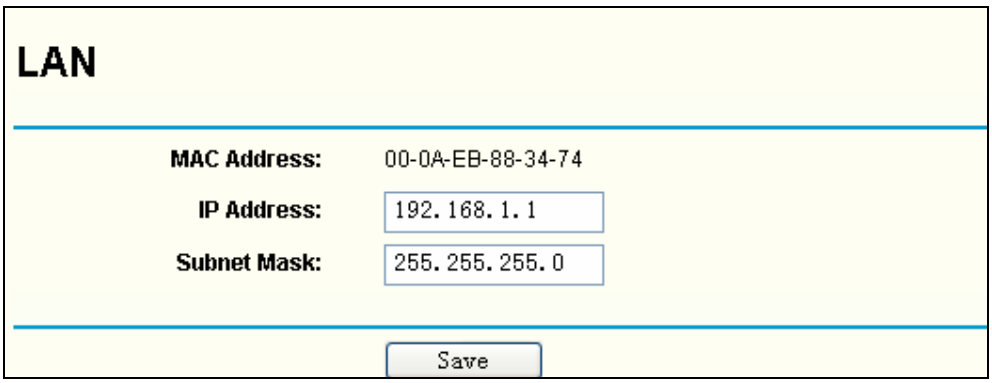


Figure 4-4 LAN

- **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.

4.5.2 WAN

You can configure the WAN port parameters on this page.

First, please choose the WAN Connection Type (Dynamic IP/Static IP/PPPoE) for the Internet. The default type is **Dynamic IP**. If you aren't given any login parameters (fixed IP Address, logging ID, etc), please select **Dynamic 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). 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 4-5):

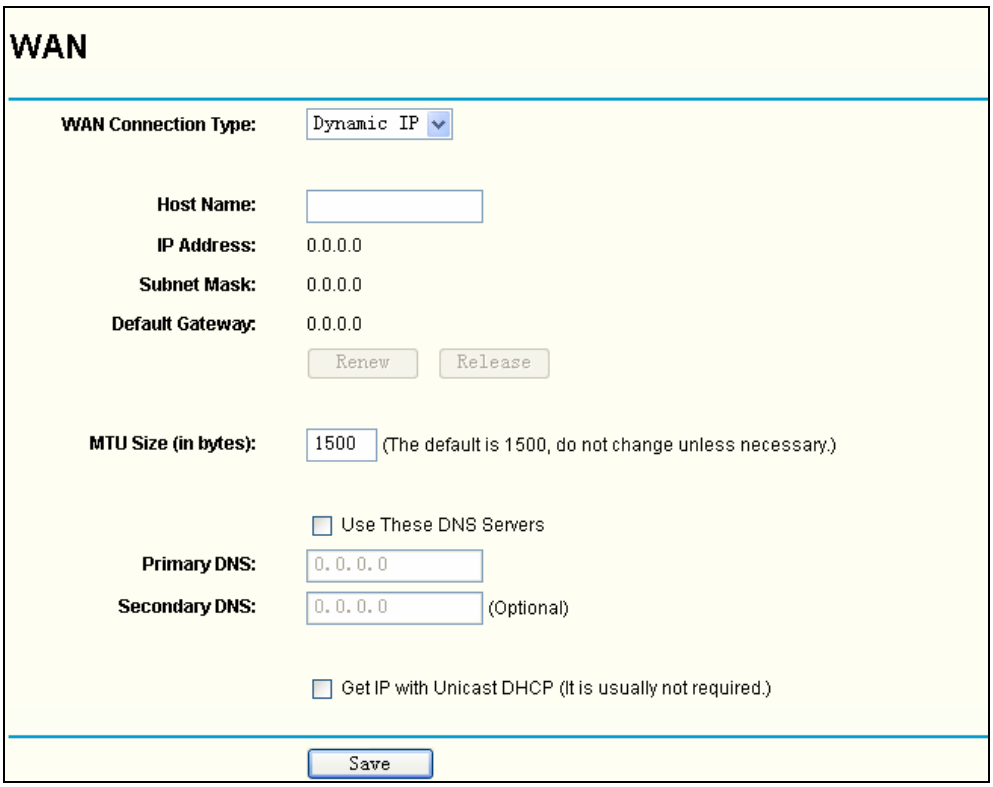


Figure 4-5 WAN – Dynamic IP

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

MTU Size - The normal MTU (Maximum Transmission Unit) value for most Ethernet networks is 1500 Bytes. 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 4-6:

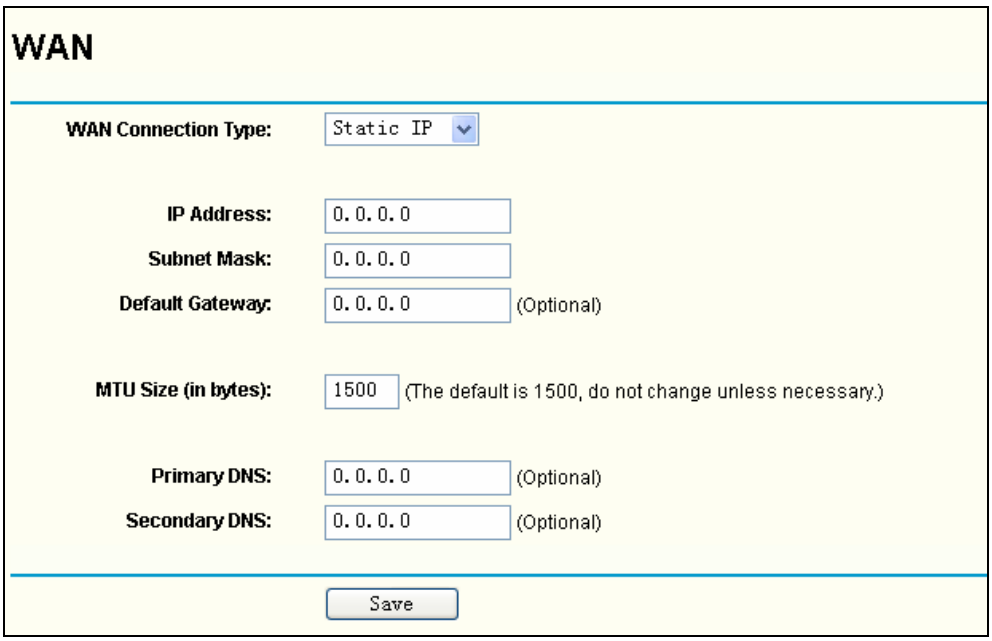


Figure 4-6 WAN - Static IP

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 4-7):

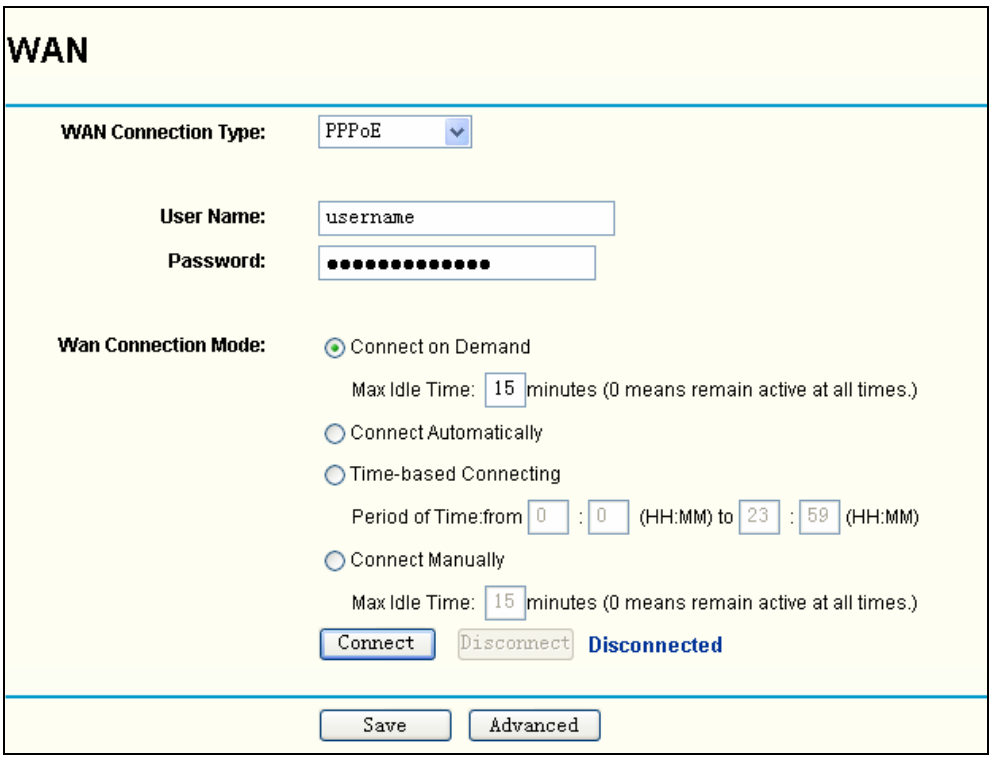


Figure 4-7 WAN - PPPoE

- **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 4-8 will then appear:

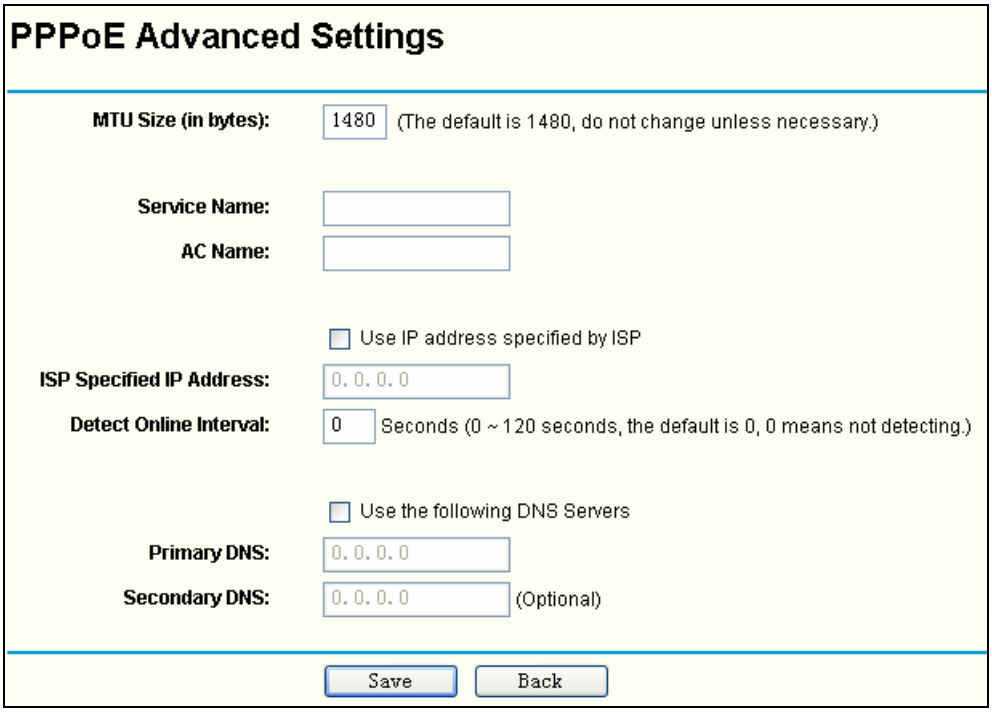


Figure 4-8 PPPoE Advanced Settings

- **Packet MTU -** The default MTU size is 1480 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.

4.5.3 MAC Clone

You can configure the MAC address of the WAN port on this page, Figure 4-9:

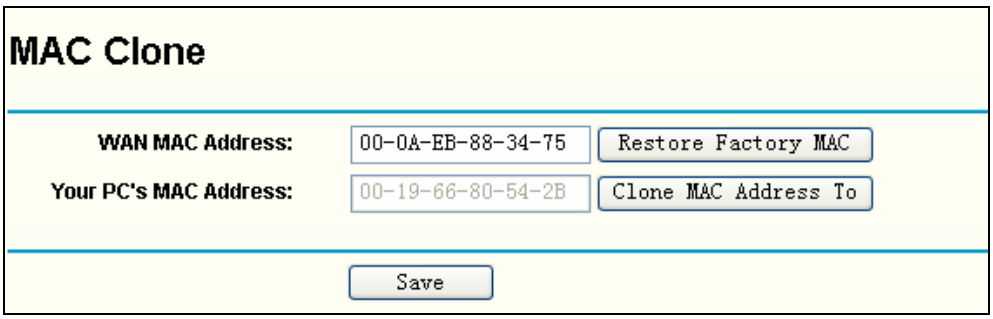


Figure 4-9 MAC Address Clone

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 To** button and this MAC address will fill in the **WAN MAC Address** field.

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

Click **Save** to save your settings.

☞ **Note:**

1) Only the PC on your LAN can use the **Clone MAC Address To** feature.
2) If you click **Save**, the router will prompt you to reboot.

4.6 Wireless

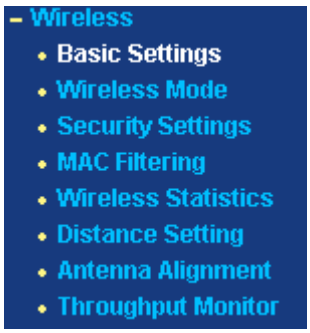


Figure 4-10 Wireless menu

There are eight submenus under the Wireless menu (shown in Figure 4-10):**Basic Settings**, **Wireless Mode, Security Settings, MAC Filtering, Wireless Statistics, Distance Setting, Antenna Alignment** and **Throughput Monitor.** Click any of them, and you will be able to configure the corresponding function. The detailed explanations for each submenu are provided below.

4.6.1 Basic Settings

The basic settings for the wireless network in AP Client Router operation mode are set on this page.

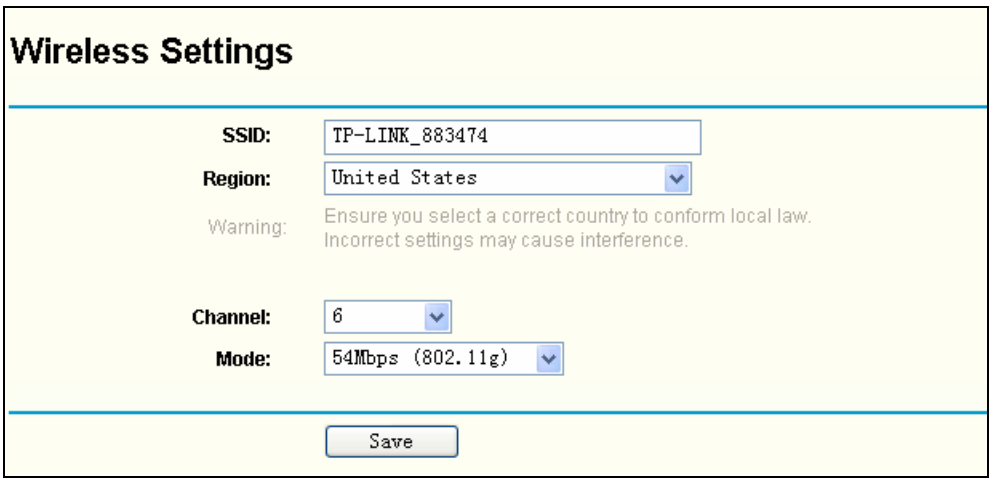


Figure 4-11 Wireless Settings in AP Client Router mode

- **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_xxxxxx (xxxxxx indicates the last six unique characters of each device's MAC address). This value is case-sensitive. For example, *TP-LINK* is NOT the same as *tp-link*.
- **Region**-Select your region from the drop-down list. This filed specifies the region where the wireless function of the device can be used. It may be illegal to use the wireless function of the device in a region other than one of those specified in this field. If your country or region is not listed, please contact your local government agency for assistance.
- **Channel** – This field determines which operating frequency will be used. It is not necessary to change the wireless channel unless you notice 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.

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

☞ **Note:**

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

4.6.2 Wireless Mode

This page allows you to configure the wireless mode for your device:

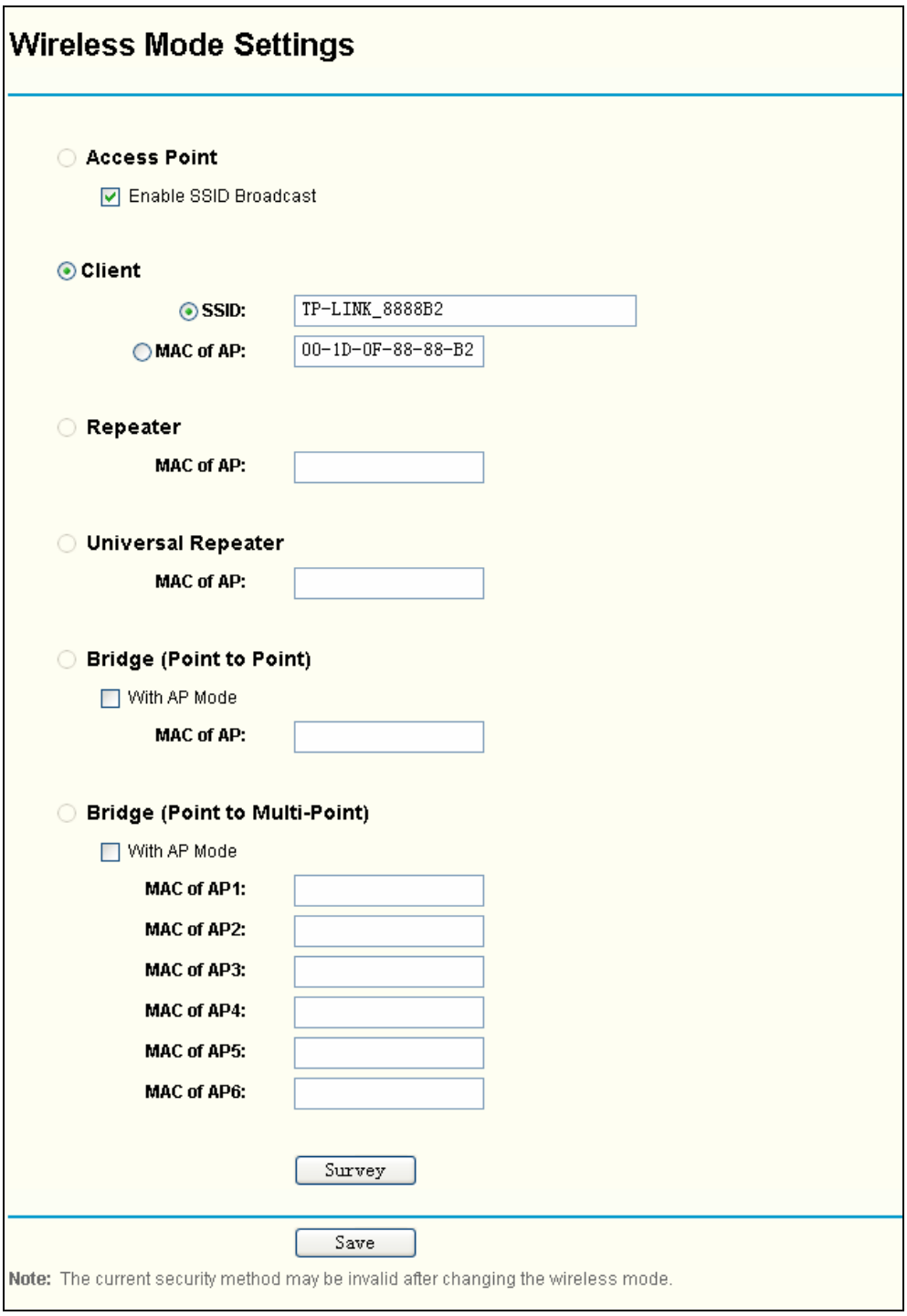


Figure 4-12 Wireless Mode

Note:

In AP Client Router, there is only Client mode available shown as Figure 4-12 while in AP Router there is only Access Point mode available shown as Figure 4-14.

- **Access Point** - Access Point mode allows wireless stations including AP clients to access the router.
  - **Enable SSID Broadcast** - If you select the **Enable SSID Broadcast** checkbox, the Wireless AP will broadcast its name (SSID) on the air.
- **Client** - In **Client** mode, AP will act as a wireless station to enable wired host(s) to access wireless AP.

- **SSID** - Enter the SSID of AP that you want to access. If you select the radio before **SSID**, the AP client will connect to AP according SSID.
- **MAC of AP** - Enter the MAC address of AP that you want to access. If you select the radio before **MAC of AP**, the AP client will connect to AP according MAC address.

Note:

To apply any settings you have altered on the page, please click the **Save** button, and wait the AP reboot automatically.

Click **Survey** will show the site list of scanning result shown as Figure 4-13 and you can choose one to connect to.

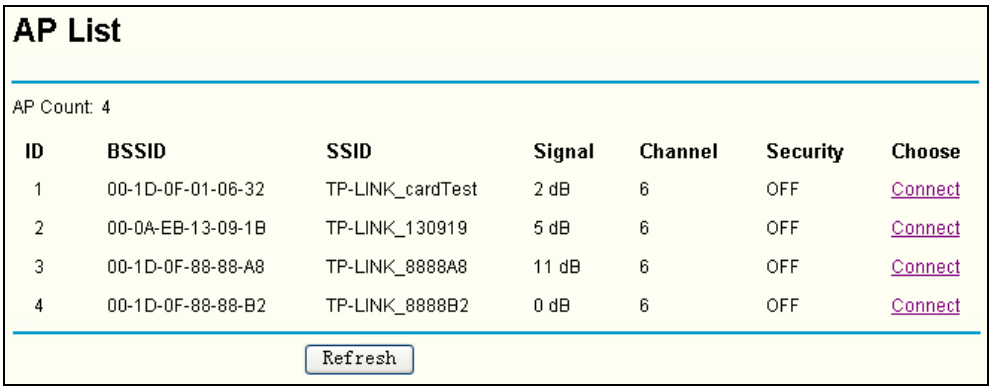


Figure 4-13 AP List

- **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 values you selected will be filled in the **SSID** and **MAC of AP** fields on Figure 4-12.

Note:

If you want to configure other wireless mode settings, you can change your AP to AP operation mode on **Operation Mode** page as Figure 4-2.

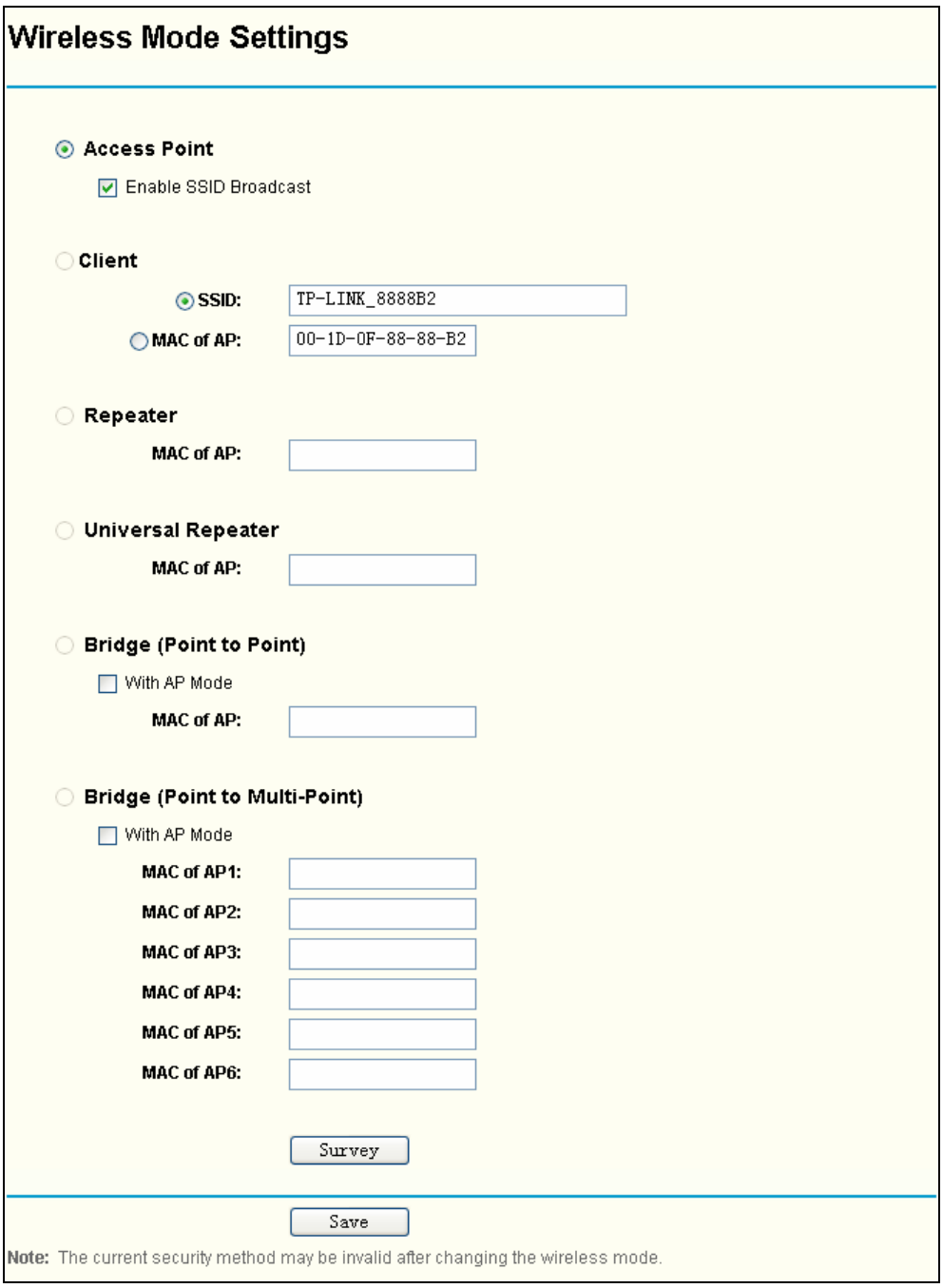


Figure 4-14 Wireless Mode settings in AP Router mode

4.6.3 Security Settings

You can select one of the following security options:

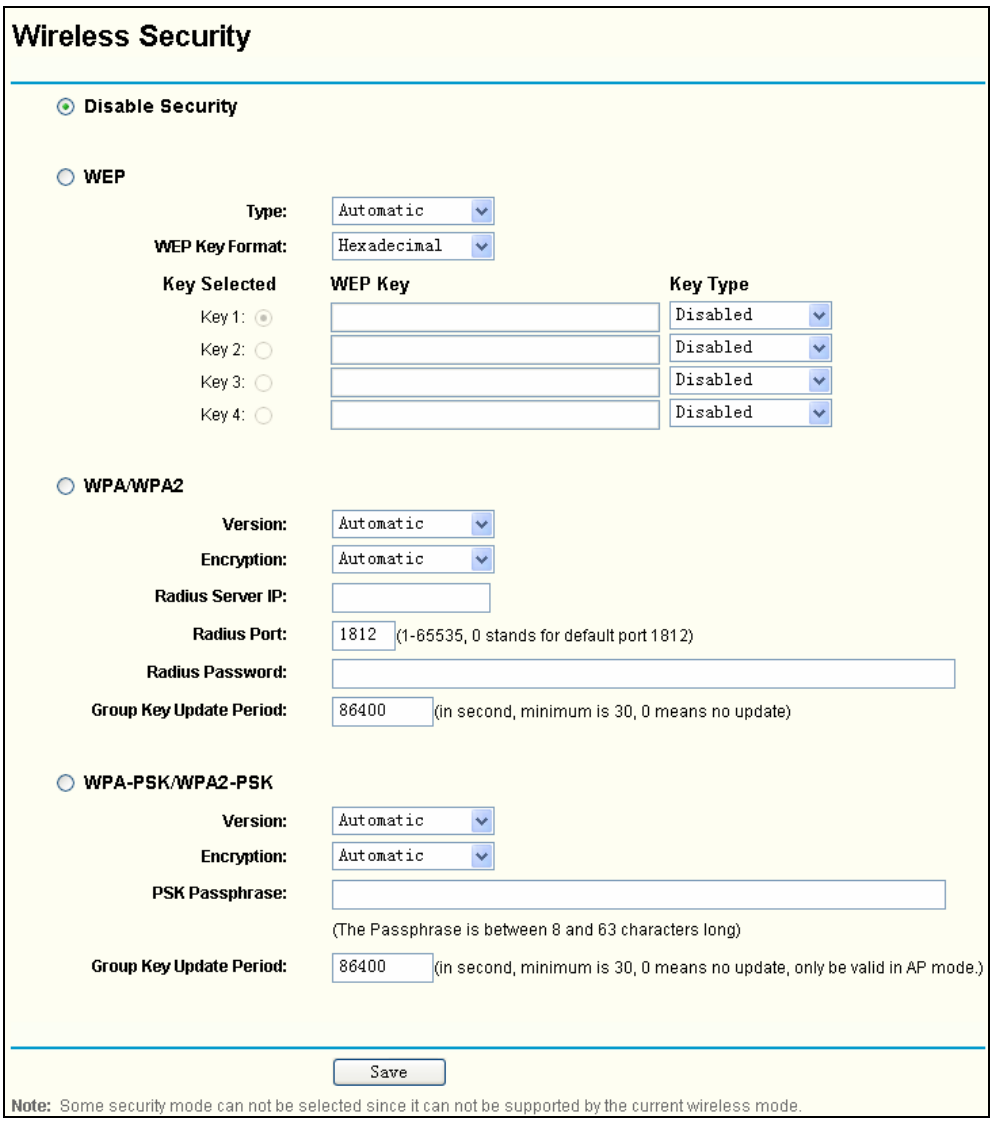


Figure 4-15 Wireless Security

- **Disable Security** - The wireless security function can be enabled or disabled. If disabled, the wireless stations will be able to connect the device without encryption. It is recommended strongly that you choose one of following options to enable security.
- **WEP** - Select 802.11 WEP security.
  - **Type** - You can select one of following types,

  1). **Automatic** - Select **Shared Key** or **Open System** authentication type automatically based on the wireless station's capability and request.

  2). **Shared Key** - Select 802.11 Shared Key authentication.

  3). **Open System** - Select 802.11 Open System authentication.

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

1). 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.

2). 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.

3). 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.

☞ **Note:**

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

➢ **WPA/WPA2 -** Select WPA/WPA2 based on Radius Server.

- **Version** - You can select one of following versions,

1). **Automatic** - Select **WPA** or **WPA2** automatically based on the wireless station's capability and request.

2). **WPA** - Wi-Fi Protected Access.

3). **WPA2** - WPA version 2.

- **Encryption** - You can select either **Automatic**, or **TKIP** or **AES**.
- **Radius Server IP** - Enter the IP address of the Radius Server.
- **Radius Port** - Enter the port that radius service used.
- **Radius Password** - Enter the password for the Radius Server.
- **Group Key Update Period** - Specify the group key update interval in seconds. The value can be either 0 or at least 30. Enter 0 to disable the update.

➢ **WPA-PSK/ WPA2-PSK -** Select WPA based on pre-shared passphrase.

- **Version** - You can select one of following versions,

1). **Automatic** - Select **WPA-PSK** or **WPA2-PSK** automatically based on the wireless station's capability and request.

2). **WPA-PSK** - Pre-shared key of WPA.

3). **WPA2-PSK** - Pre-shared key of WPA2.

- **Encryption** - When you select **WPA-PSK** or **WPA2-PSK** for **Authentication Type** you can select either **Automatic**, or **TKIP** or **AES** as **Encryption**.
- **PSK Passphrase** - You can enter a passphrase between 8 and 63 characters long.
- **Group Key Update Period** - Specify the group key update interval in seconds. The value can be either 0 or at least 30. Enter 0 to disable the update.

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

☞ **Note:**

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

4.6.4 MAC Filtering

The Wireless MAC Filtering for wireless networks are set on this page .Figure 4-16:

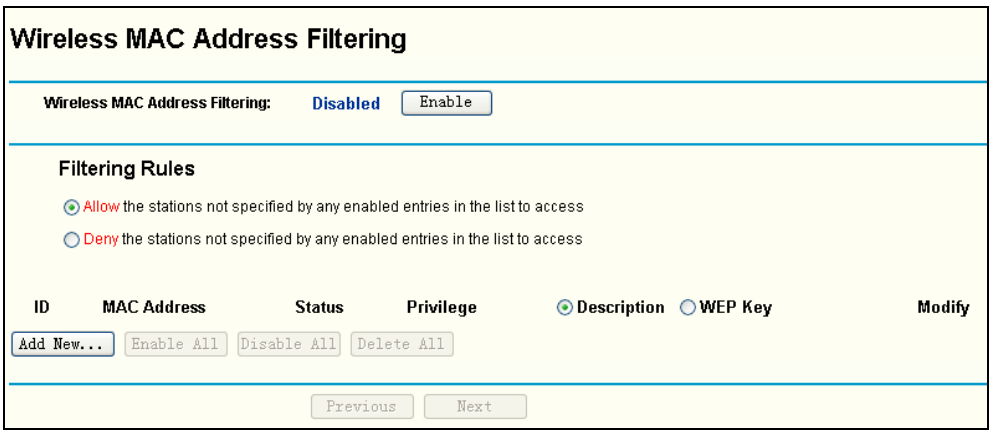


Figure 4-16 Wireless MAC address Filtering

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 4-17

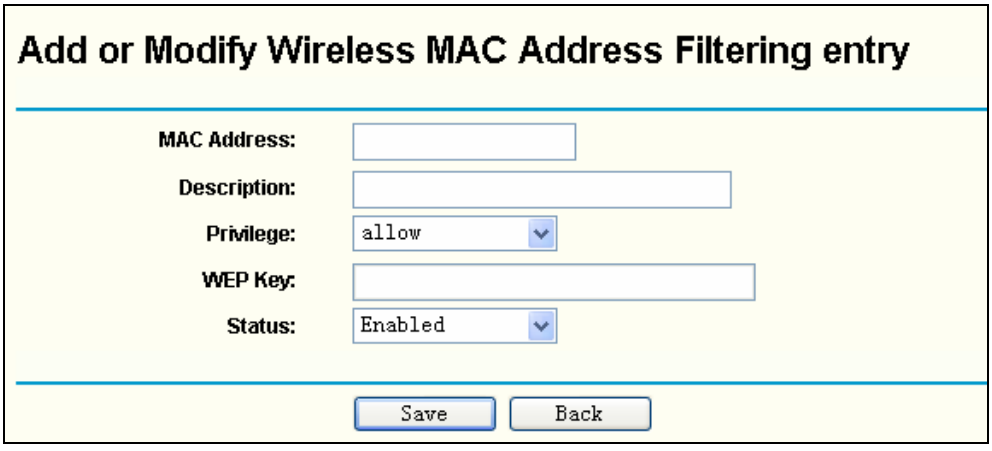


Figure 4-17 Add or Modify Wireless MAC Address Filtering entry

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.

4.6.5 Wireless Statistics

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

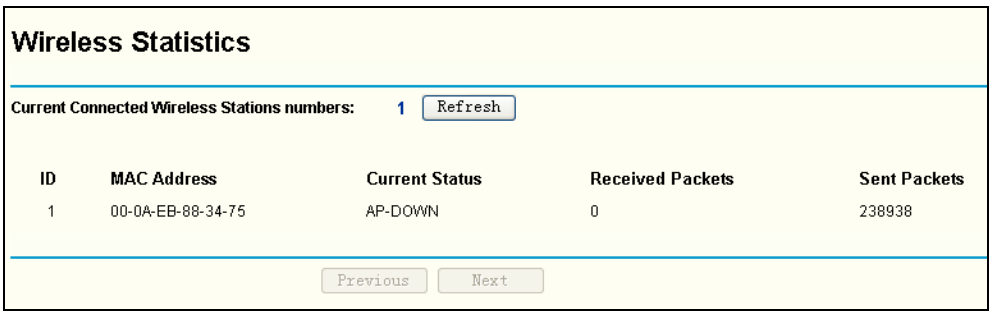


Figure 4-18 The router attached wireless stations

- **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.

4.6.6 Distance Setting

This feature is used to adjust the wireless range in outdoor conditions. This is a critical feature required for stabilizing outdoor links. Enter the distance of your wireless link and the software will optimize the frame ACK timeout value automatically.

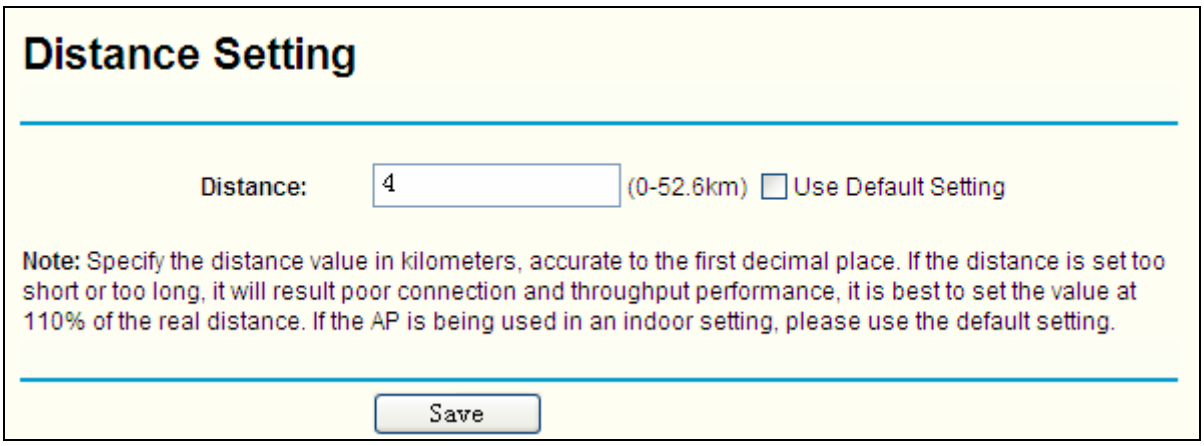


Figure 4-19 Distance Setting

- **Use Default Setting:** Keep the default setting if the AP is used for indoor environment. If you want to change the distance, please uncheck the **Use Default Setting** box.
- **Distance:** Specify the distance value in kilometers, accurate to the first decimal place. If the distance is set too short or too long, it will result poor connection and throughput performance, it is best to set the value at 110% of the real distance. If the AP is being used in an indoor setting, please use the default setting.

Click **Save** to keep your settings.

4.6.7 Antenna Alignment

This page shows how remote AP's signal strength changes while aligning the antenna's direction.

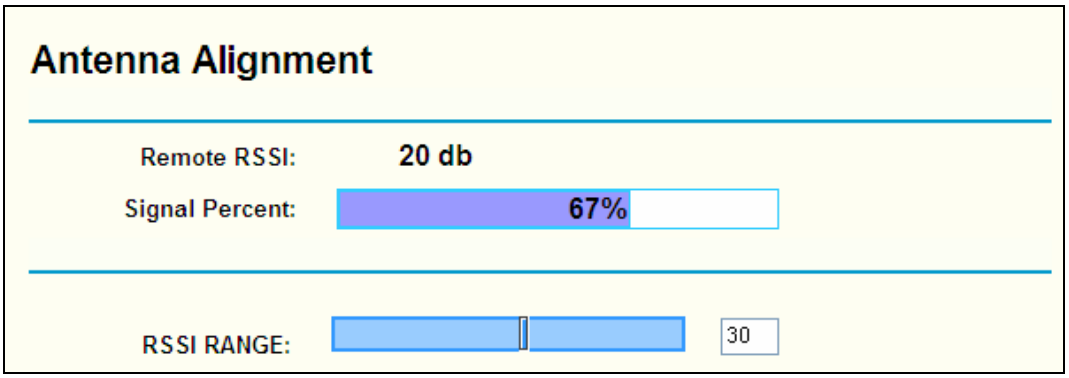


Figure 4-20 Antenna Alignment

- **Remote AP RSSI** - Remote AP's signal strength value.
- **Signal percent** - The ratio of RSSI to RSSI RANGE in percentage.
- **RSSI RANGE** - You can drag the slider bar to set or input the RSSI RANGE value. The slider bar allows the range of the meter to be either increased or reduced. If the range is reduced, the color change will be more sensitive to signal fluctuations. The slider bar actually changes an offset of the maximum indicator value scale.

☞ **Note:**

It only works after you have established connection to remote AP under client mode.

4.6.8 Throughput Monitor

This page allows you to view the wireless throughput information

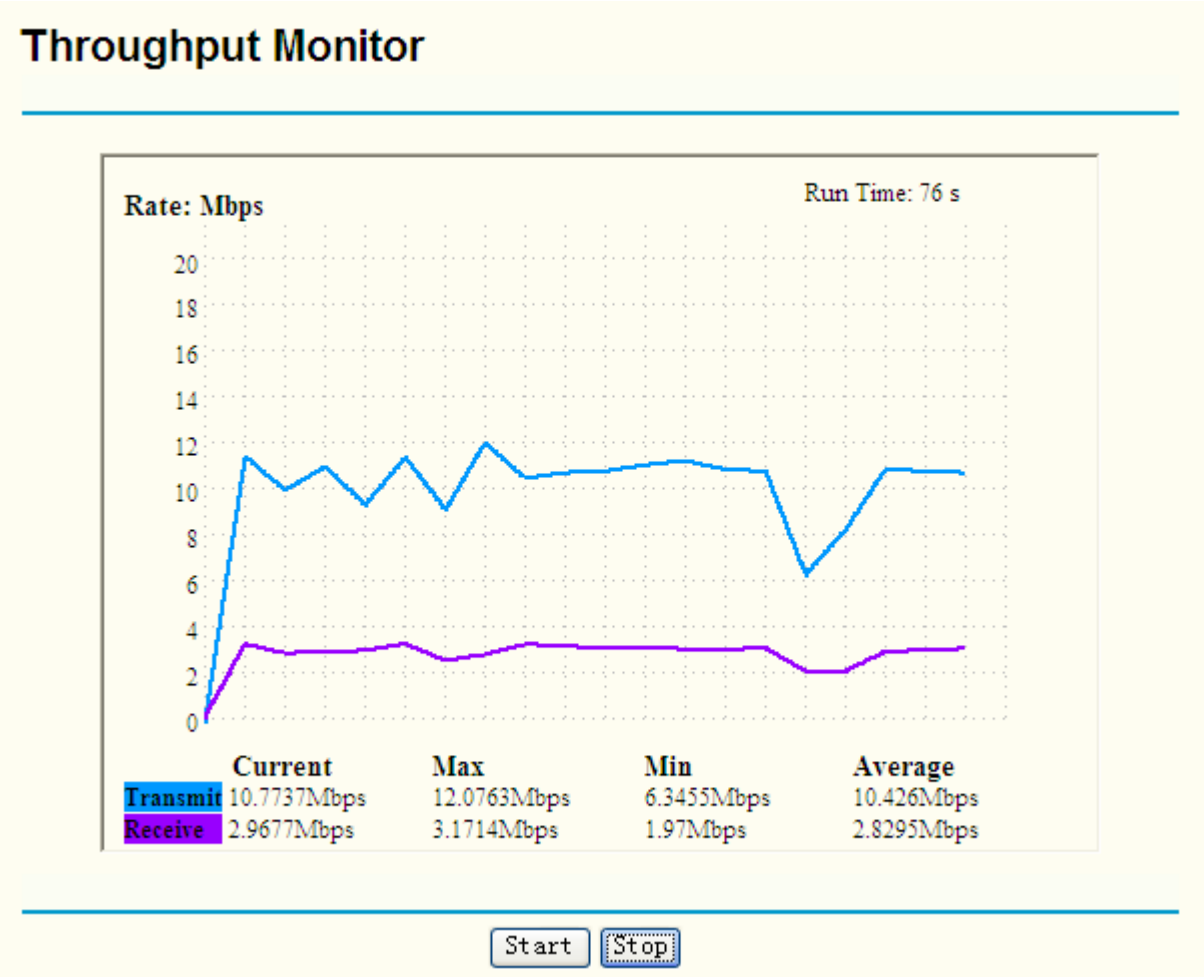


Figure 4-21 Wireless Throughput

Rate - The Throughput unit.

Run Time - How long this function is running.

Transmit- Wireless transmit rate information.

Receive- Wireless receive rate information.

Click the **Start** button to start wireless throughput monitor.

Click the **Stop** button to stop wireless throughput monitor.

4.7 DHCP

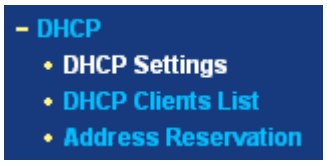


Figure 4-22 The DHCP menu

There are three submenus under the DHCP menu (shown in Figure 4-22): **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.

4.7.1 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 4-23):

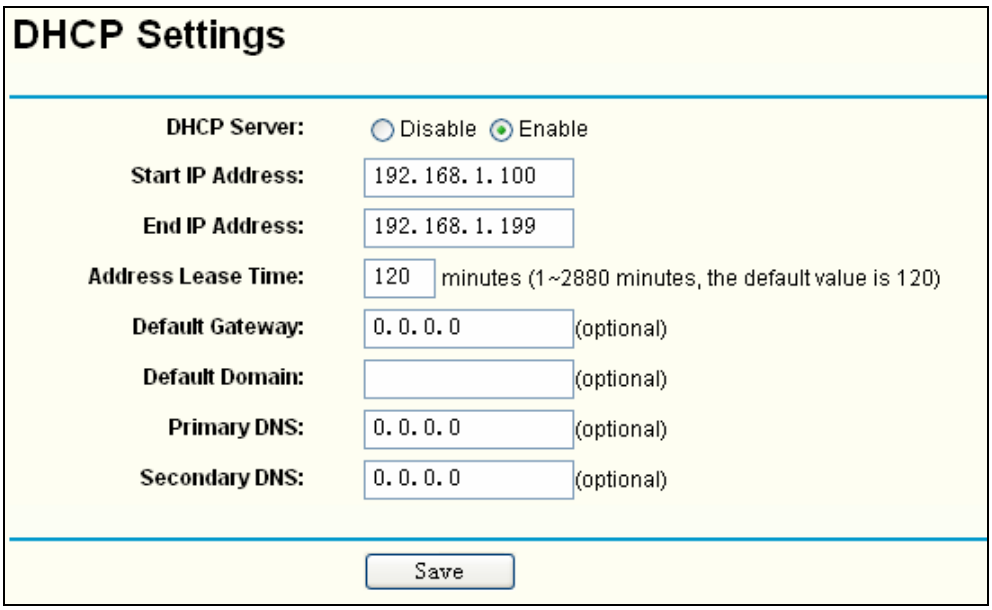


Figure 4-23 DHCP Settings

- **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 have to 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 to connect to the router with their current dynamic IP Address. Enter the amount of time in minute. 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.

Click **Save** to save the new settings to the router

4.7.2 DHCP Clients List

This page shows **Client Name, MAC Address, Assigned IP,** and **Lease Time** for each DHCP Client attached to the router Figure 4-24:

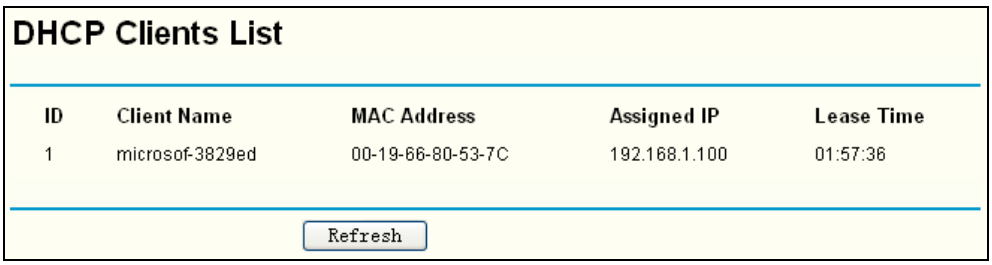


Figure 4-24 DHCP Clients List

- **Index(ID)-** The index of the DHCP Client
- **Client Name -** The name of the DHCP client
- **MAC Address -** The MAC address of the DHCP client
- **Assigned IP -** The IP address that the router has allocated to the DHCP client.
- **Lease Time -** The time of the DHCP client leased. 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.

4.7.3 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 4-25).

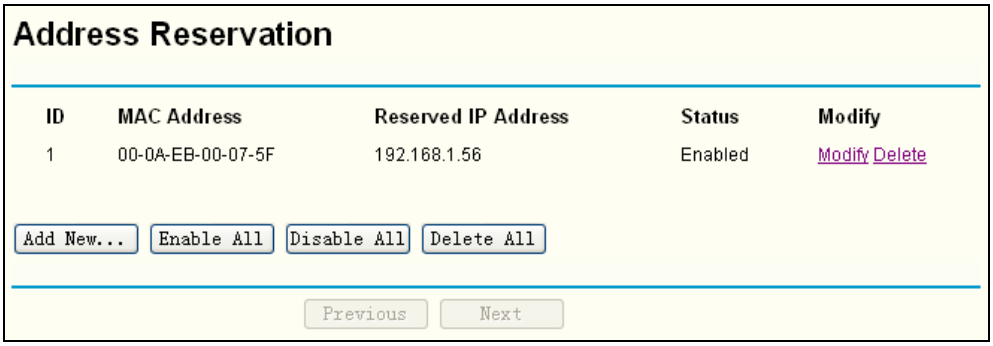


Figure 4-25 Address Reservation

- **MAC Address -** The MAC address of the PC which you want to reserve IP address for.
- **Reserved IP Address -** The IP address of the router reserved.
- **Status -** It shows whether the entry is enabled or not.
- **Modify –** To modify or delete an existing entry.

To Reserve IP addresses:

1. Click the **Add New button** in the page of **Address Reservation**, the following page(Figure 4-26) will display.
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 want to add.
3. Click the **Save** button after finish configuring.

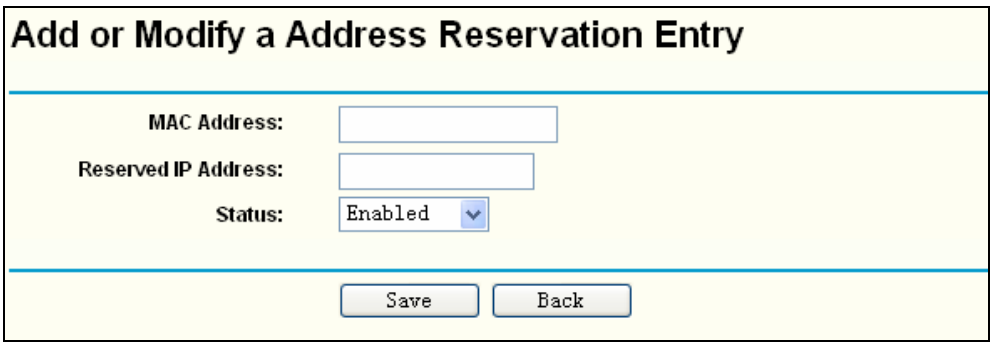


Figure 4-26 Add or Modify an Address Reservation Entry

To modify or delete an existing entry:

1. Select a reserved address entry, Click the **Modify** in the entry if you want to modify it. If you want to delete the entry, click the **Delete**.
2. 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, or Click the **Previous** button to return the previous page.

☞ **Note:**

The change of the address reservation won't take effect until the device reboot.

4.8 Wireless settings

This page allows you to configure some settings for your wireless network, which is shown in Figure 4-27.

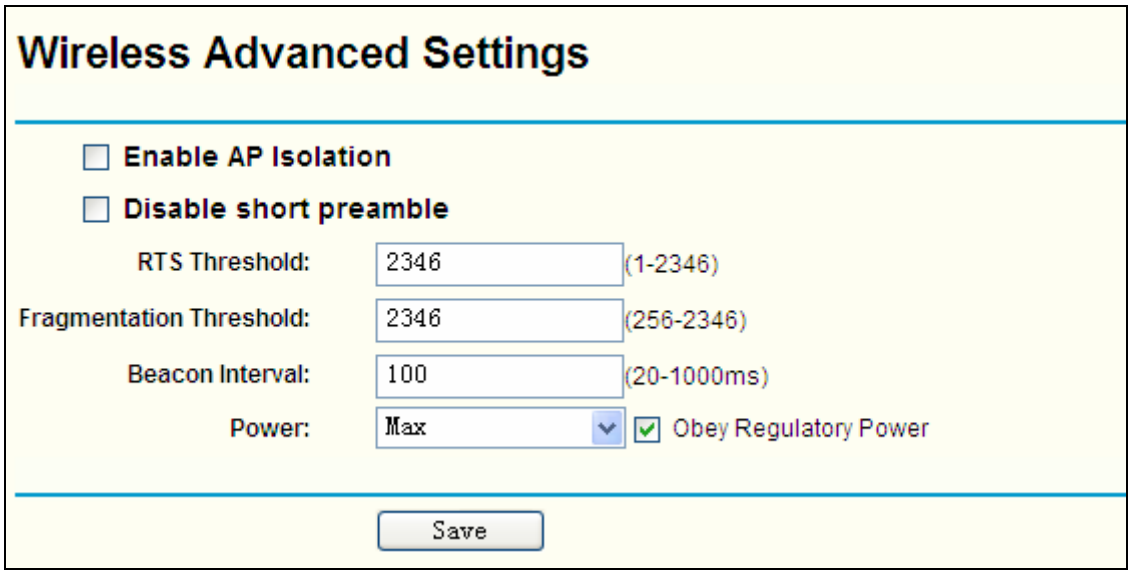


Figure 4-27 Wireless settings

- **Enable AP Isolation** - Isolate all connected wireless stations so that wireless stations can not access each other through WLAN. This option is available only for AP mode.

- **Disable short preamble** - Disable short preamble and use long preamble only. 802.11b mode supports only long preamble and this parameter will be ignored. It is recommended that you do not change these settings.
- **RTS threshold** - RTS/CTS Threshold, the packet size that is used to determine if RTS/CTS should be sent.
- **Fragmentation threshold** - The maximum packet size used for fragmentation.
- **Beacon Interval** - The interval time between two successive beacons.
- **Power** - The transmit power of the access point. The checkbox determines the transmit power that whether it obeys regulatory power or not. Un-checking the **Obey Regulatory Power** option may cause interference to other devices and violate the applicable law.

4.9 Forwarding

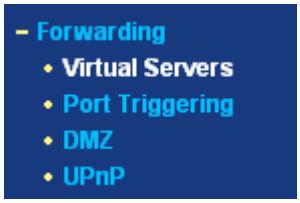


Figure 4-28 The Forwarding menu

There are four submenus under the Forwarding menu (shown in Figure 4-28): **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.

4.9.1 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 4-29:

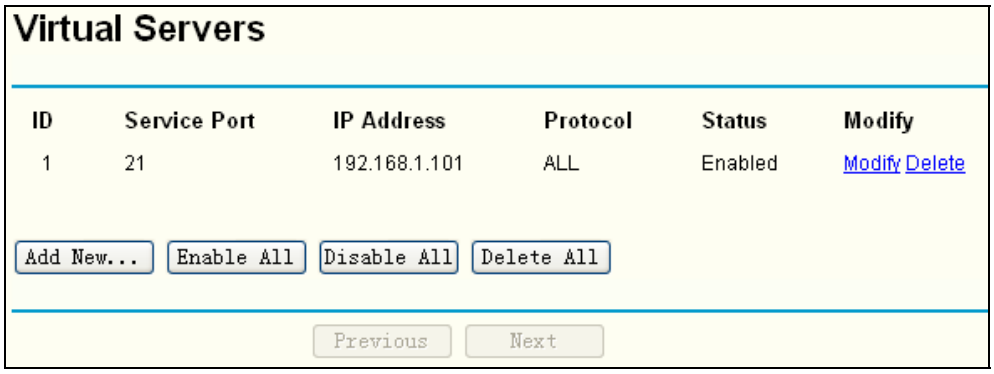


Figure 4-29 Virtual Servers

- **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 is either **Enabled** or **Disabled**.
- **Modify** - To modify or delete an existing entry.

To setup a virtual server entry, please take the following steps:

1. Click the **Add New…**in virtual servers page. (pop-up Figure 4-30)
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, **TCP** ,**UDP**, or **All**.
5. Select the **Enable** option to enable the virtual server.
6. Click the **Save** button.

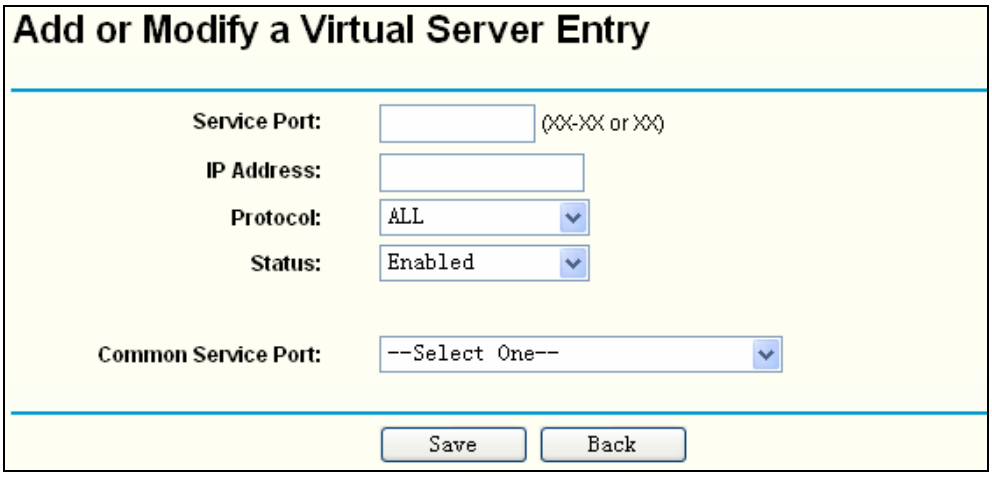


Figure 4-30 Add or Modify a Virtual Server Entry

- **Common Service Port** - Some common services already exist in the pull-down list.

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 **System Tools –> Remote Management** page to be any value except 80 such as 8080. Or else there will be a conflict to disable the virtual server.

4.9.2 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 a NAT router. You can set up Port Triggering on this page shown in Figure 4-31:

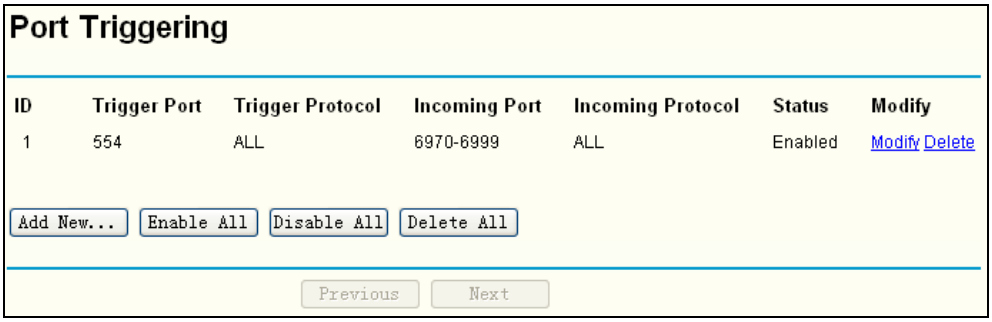


Figure 4-31 Port Triggering

Once configured, operation is as follows:

1. A local host makes an outgoing connection to an external host 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, **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, TCP , UDP, or ALL (all protocols supported by the router).
- **Status -** The status of this entry is either **Enabled** or **Disabled**.

To add a new rule, please take the following steps:

1. Click the **Add New…** in Port Triggering page.. (pop-up Figure 4-32)
2. Enter a port number used by the application to send an outgoing request in the **Trigger Port** box.
3. Select the protocol used for **Trigger Port** from the pull-down list of **Trigger Protocol**, **TCP**, **UDP**, or **All.**
4. Enter the range of port numbers used by the remote system when it responds to the PC's request in the **Incoming Ports** box.
5. Select the protocol used for **Incoming Ports** Range from the pull-down list, **TCP** , **UDP**, or **All.**
6. Select the **Enable** option in the **Status** pull-down list..

7. Click the **Save** button to save the new rule.

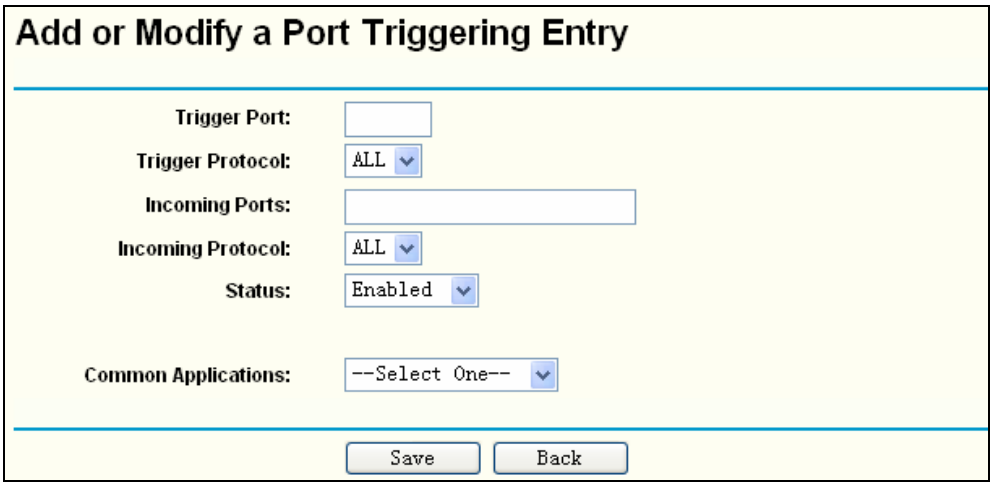


Figure 4-32 Add or Modify a Triggering Entry

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

To modify or delete an existing entry, please take the following steps:

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

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

Click **Delete All** to delete all entries

☞ **Note:**

1) When the trigger connection is released, the corresponding opening ports will be closed.
2) Each rule can only be used by one host on the LAN at a time. The trigger connection of other hosts on the LAN will be refused.
3) Incoming Port Range enabled cannot overlap each other at the same time.

4.9.3 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 4-33

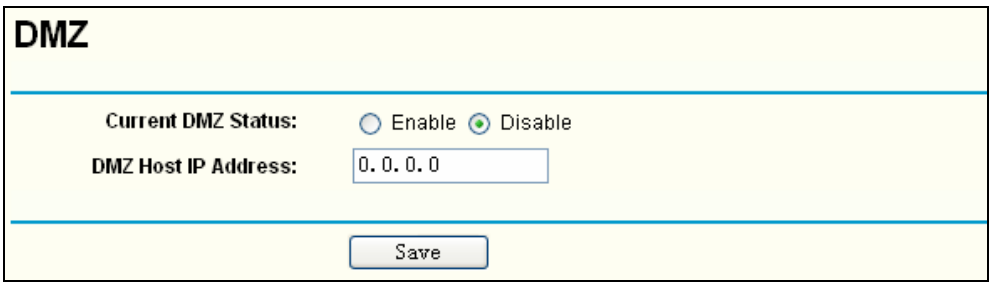


Figure 4-33 DMZ

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

1. Click the **Enable** radio button
2. Enter the IP address of a local PC that is set to be DMZ host in the **DMZ Host IP Address** field
3. Click the **Save** button.

☞ **Note:**

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

4.9.4 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 4-34:

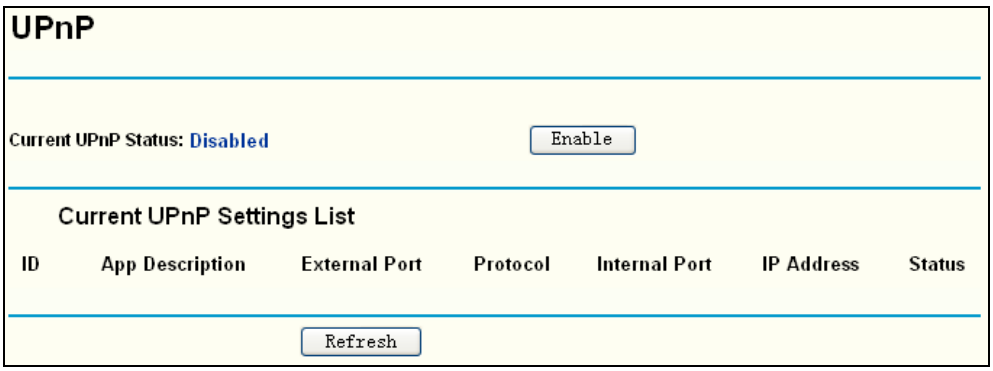


Figure 4-34 UPnP Settings

- **Current UPnP Status -** UPnP can be enabled or disabled by clicking the **Enable** or **Disable** button. As enabling UPnP 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 IP address of the local host which initiates the UPnP request.
  - **Status -** Either Enabled or Disabled, “Enabled” means that port is still active. Otherwise, the port is inactive.

Click **Enable** to enable UPnP.

Click **Disable** to disable UPnP

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

4.10 Security

Figure 4-35 The Security menu

There are five submenus under the Security menu (shown in Figure 4-35): **Firewall**, **IP Address Filtering, Domain Filtering, MAC Address Filtering** 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.

4.10.1 Firewall

Using the Firewall page (shown in Figure 4-36), you can turn the general firewall switch on or off. The default setting for the switch is off. Turning the general firewall switch to off will disable IP Filtering, Domain Filtering and MAC Filtering even if their individual settings are enabled.

If the general firewall switch is off, even if IP Address Filtering, DNS Filtering and MAC Filtering are enabled, their settings are ineffective.

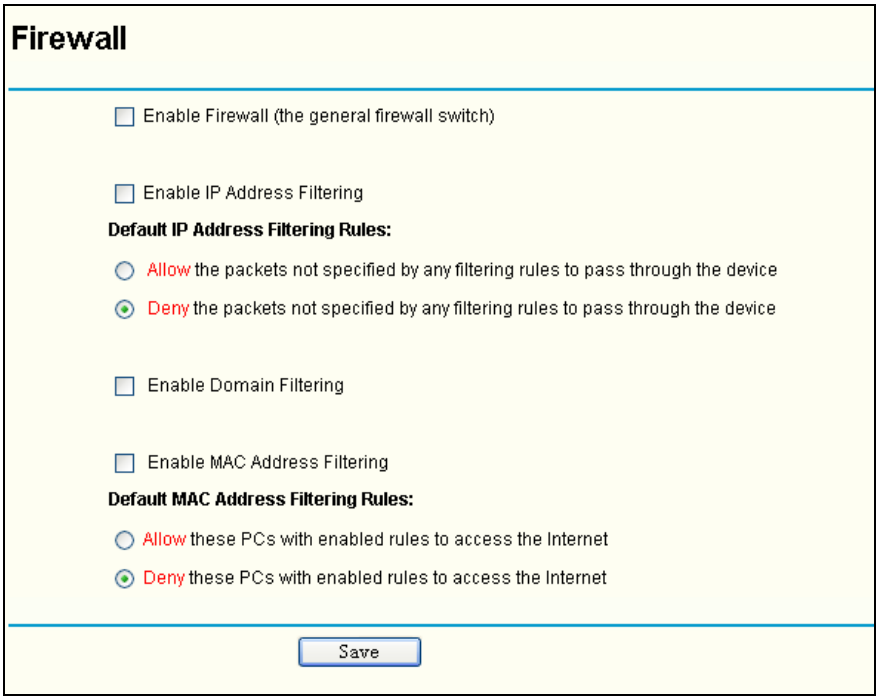


Figure 4-36 Firewall Settings

- **Enable Firewall -** Enable or disable Firewall.
- **Enable IP Address Filtering -** Enable or disable IP Address Filtering. There are two default filtering rules for IP Address Filtering: Allow or Deny the packets specified to pass through the router.
- **Enable Domain Filtering -** Enable or disable Domain Filtering.
- **Enable MAC Filtering -** Enable or disable MAC Address Filtering. There are two default

filtering rules for MAC Address Filtering: Allow or Deny the packets specified to pass through the router..

4.10.2 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 4-37:

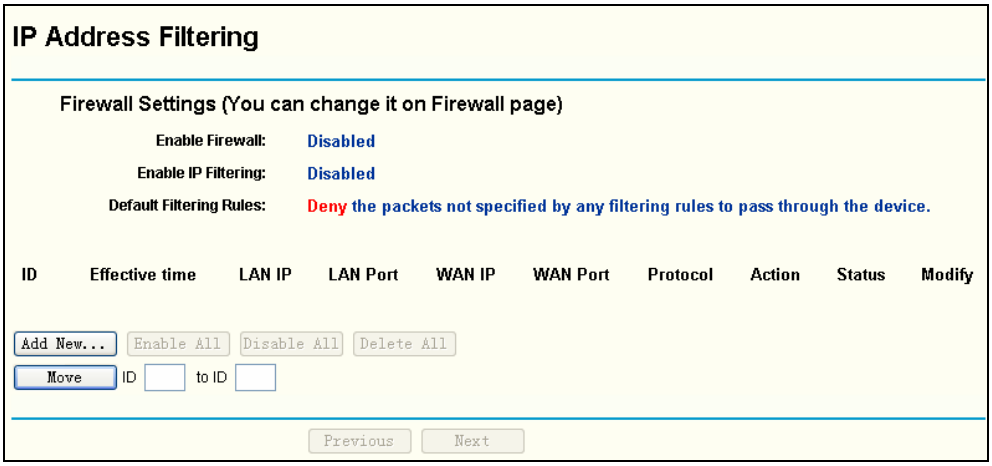


Figure 4-37 IP address Filtering

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 4-38:

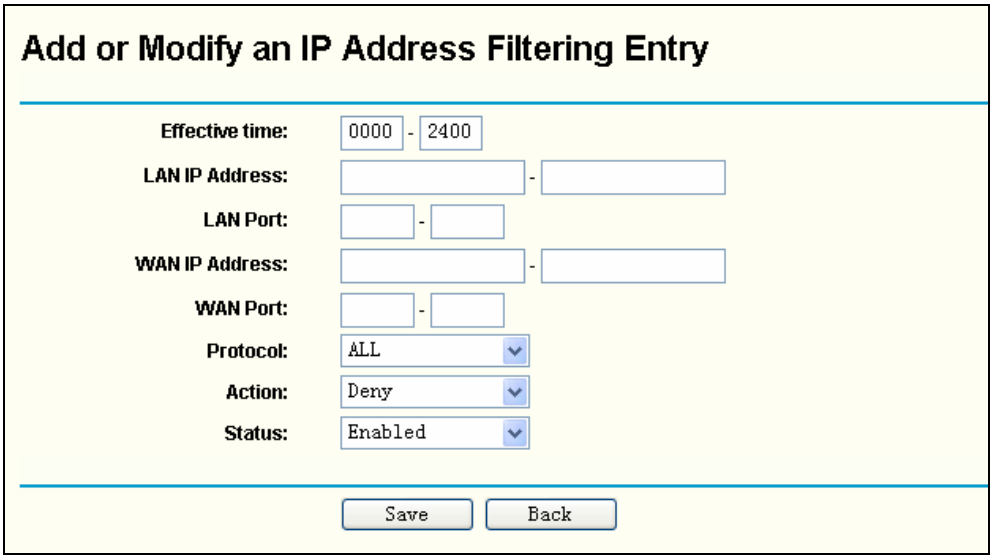


Figure 4-38 Add or Modify an IP Address Filtering Entry

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 points 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 blank, 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 blank, 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 blank, 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 blank, 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. **Action -** Select either **Allow** or **Deny** through the router.
8. **Status -** Select **Enabled** or **Disabled** for this entry from the **Status** pull-down list.

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

To add another entry, repeat steps 1-9.

When finished, click the **Back** button.

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

4.10.3 Domain Filtering

The Domain Filtering page (shown in Figure 4-39) allows you to control access to certain websites on the Internet by specifying their domains or key words.

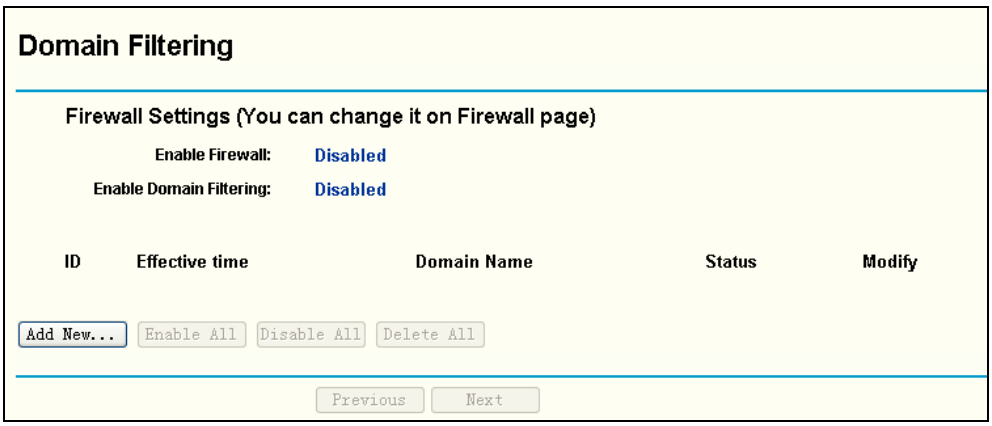


Figure 4-39 Domain Filtering

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 4-40:

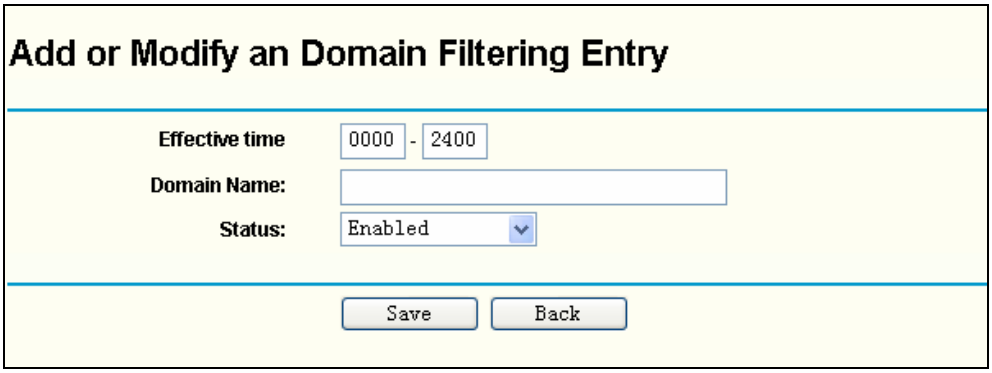


Figure 4-40 Add or Modify a Domain Filtering entry

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 button**.
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

4.10.4 MAC Address Filtering

Like the IP Address Filtering page, the MAC Address Filtering page (shown in Figure 4-41) allows you to control access to the Internet by users on your local network based on their MAC Address.

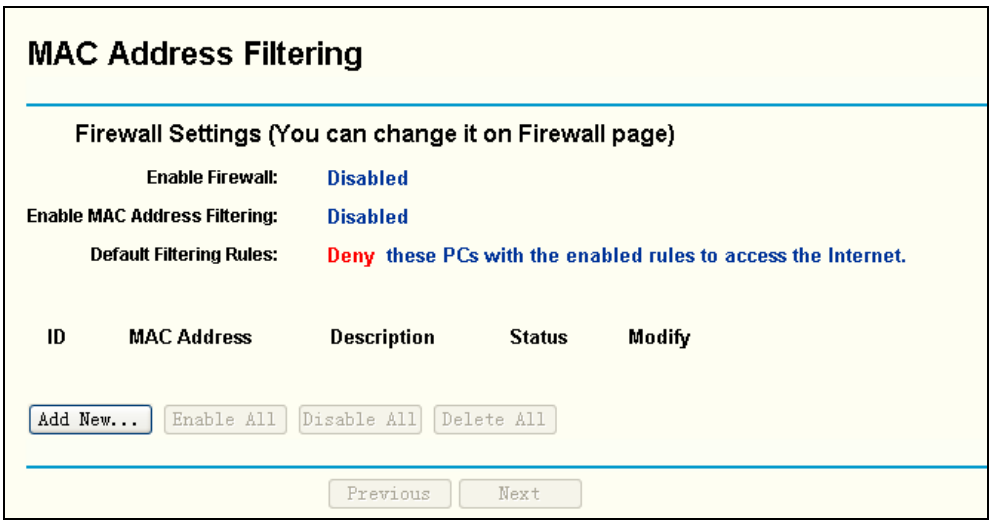


Figure 4-41 MAC address Filtering

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 4-42:

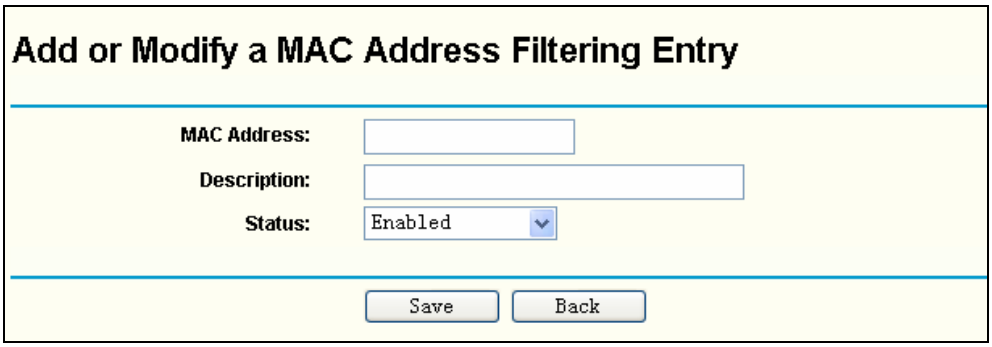


Figure 4-42 Add or Modify a MAC Address Filtering entry

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

4.10.5 Advanced Security

Using Advanced Security page (shown in Figure 4-43), you can protect the router from being attacked by TCP-SYN Flood, UDP Flood and ICMP-Flood from LAN.

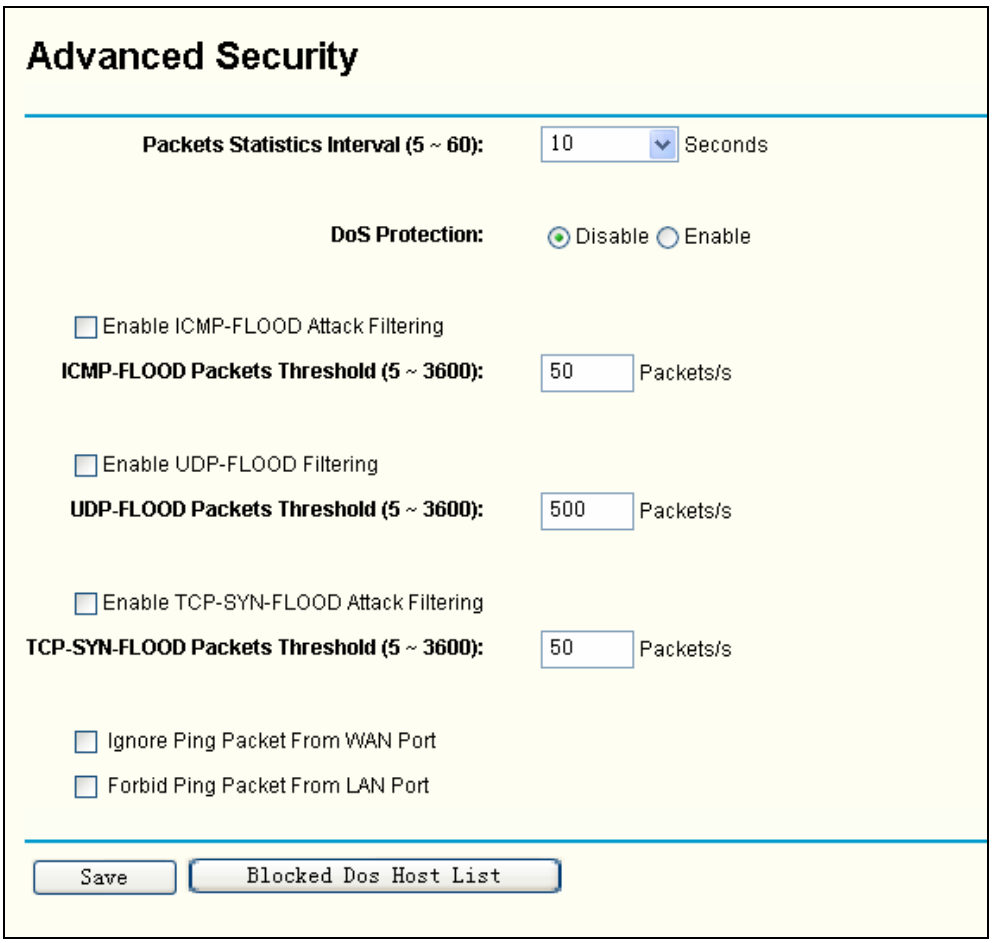


Figure 4-43 Advanced Security settings

- **Packets Statistic interval (5 ~ 60) -** The default value is 10. Select a value between 5 and 60 seconds from 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 is 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 4-44:

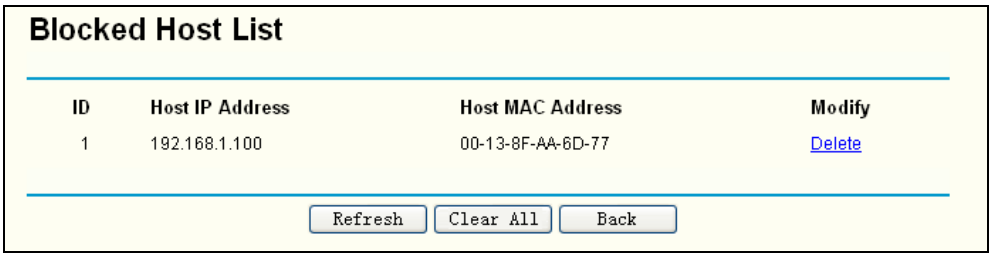


Figure 4-44 Thwarted DoS Host Table

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 **Back** button to return to the **Advanced Security** page

4.11 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 4-45).

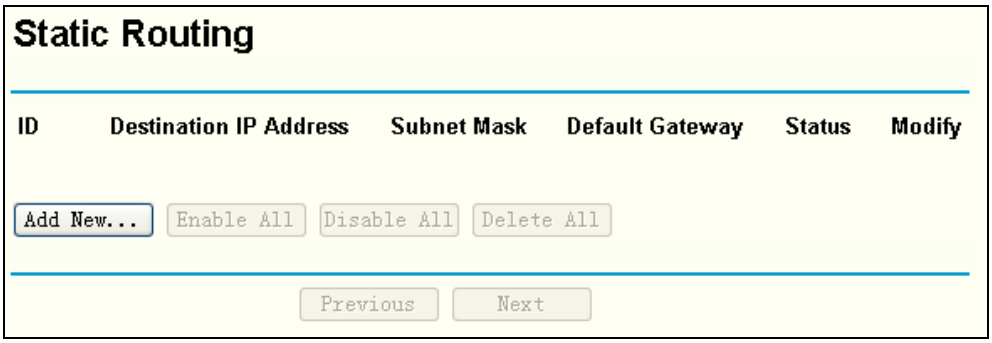


Figure 4-45 Static Routing

To add static routing entries:

1. Click the **Add New** button. (pop up Figure 4-46)
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 from the **Status** pull-down list.
4. Click the **Save** button to save the changes.

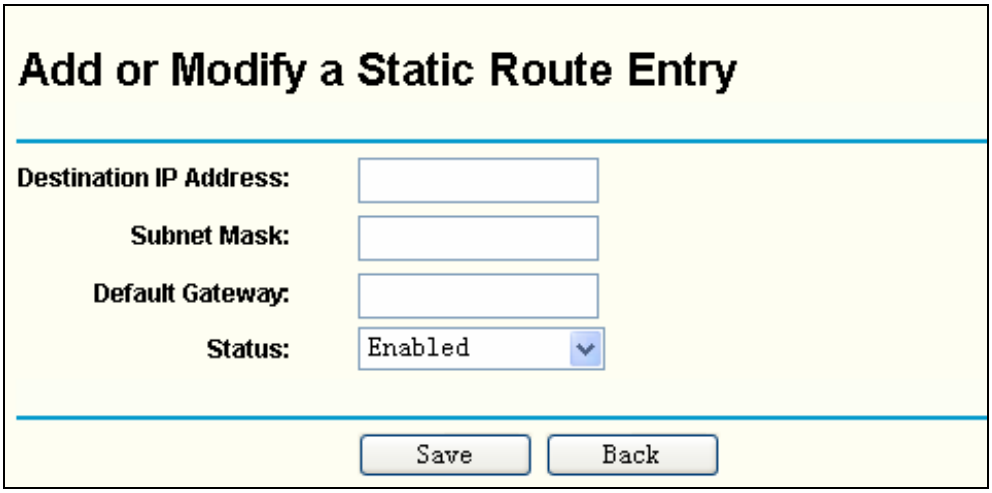


Figure 4-46 Add or Modify a Static Route Entry

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

4.12 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:

4.12.1 Dyndns.org DDNS

If your selected dynamic DNS **Service Provider** is www.dyndns.org, the page will appear as shown in Figure 4-47:

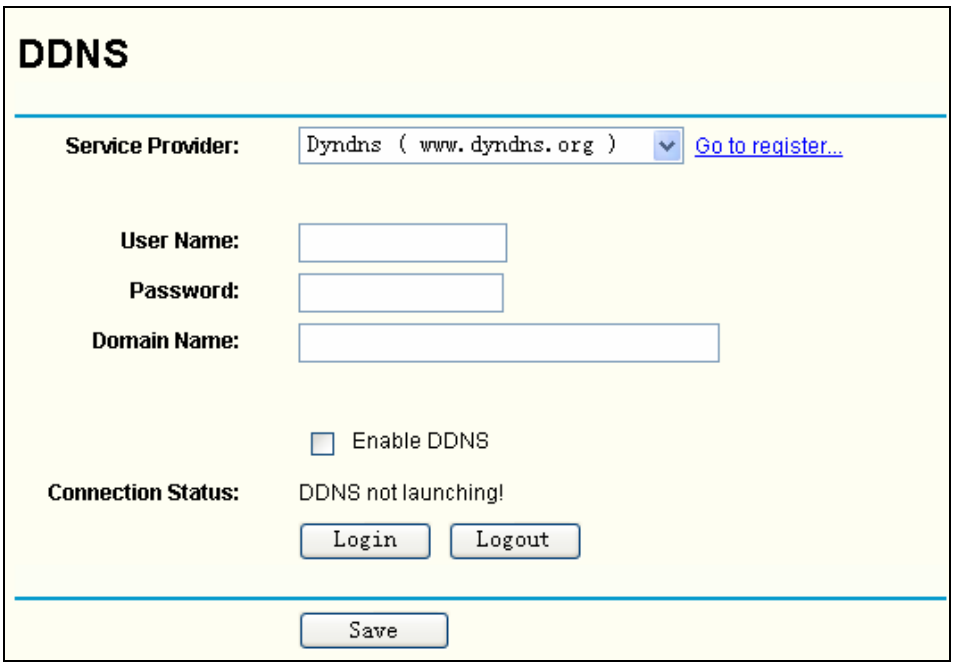


Figure 4-47 Dyndns.org DDNS Settings

To set up for DDNS, follow these instructions:

1. Enter the **User Name** for your DDNS account.
2. Enter the **Password** for your DDNS account.
3. Enter the **Domain Name** you received from dynamic DNS service provider
4. Click the **Login** button to log in to the DDNS service.

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

Click **Logout** to log out the DDNS service.

4.12.2 Oray.net DDNS

If your selected dynamic DNS **Service Provider** is www.oray.net, the page will appear as shown in Figure 4-48:

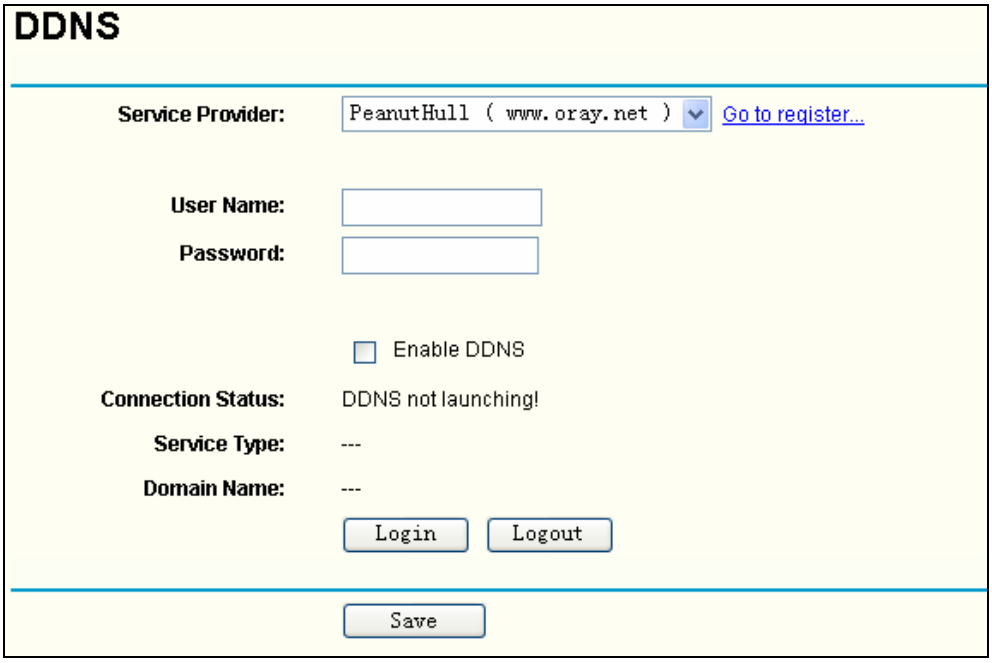


Figure 4-48 Oray.net DDNS Settings

To set up for DDNS, follow these instructions:

1. Enter the **User Name** for your DDNS account.
2. Enter the **Password** for your DDNS account.
3. Click the **Login** button to log in to 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 log out the DDNS service.

4.12.3 Comexe.cn DDNS

If your selected dynamic DNS **Service Provider** is www.comexe.cn, the page will appear as shown in Figure 4-49:

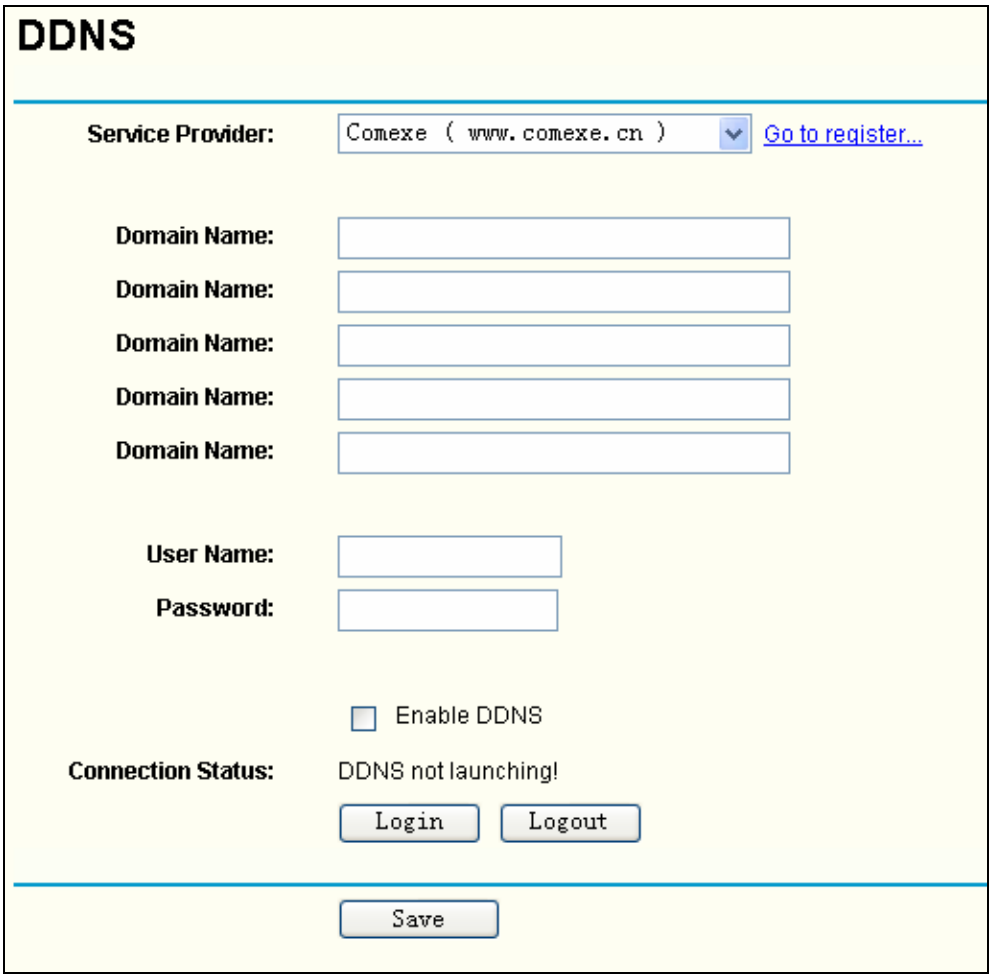


Figure 4-49 Comexe.cn DDNS Settings

To set up for DDNS, follow these instructions:

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

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

Click **Logout** to log out the DDNS service.

4.13 System Tools

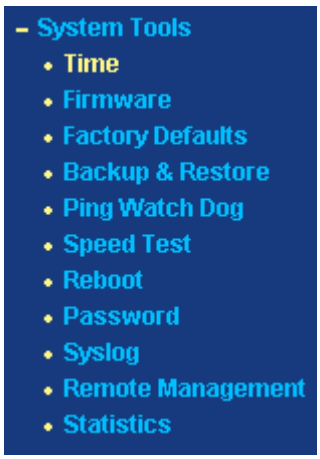


Figure 4-50 The System Tools menu

There are eleven submenus under the System Tools menu (shown in Figure 4-50): **Time**, **Firmware**, **Factory Defaults**, **Backup & Restore**, **Ping Watch Dog**, **Speed Test**, **Reboot**, **Password**, **Syslog**, **Remote Management** and **Statistics.** Click any of them, and you will be able to configure the corresponding function. The detailed explanations for each submenu are provided below.

4.13.1 Time

You can set time manually or get GMT from the Internet for the router on this page (shown in Figure 4-51):

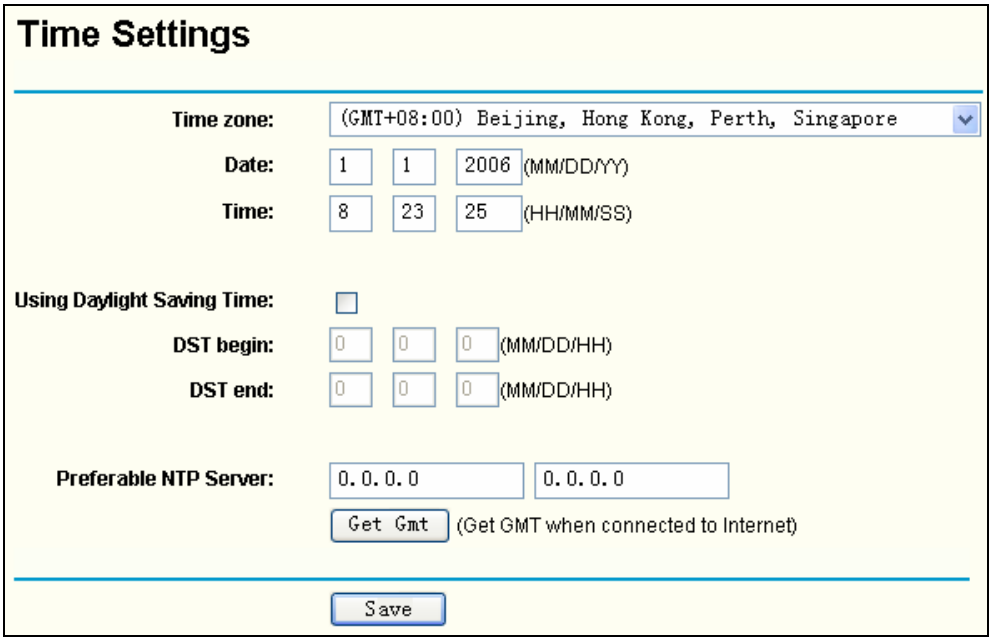


Figure 4-51 Time settings

- **Time Zone -** Select your local time zone from this drop-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.

To configure Time settings, please follow 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 begin 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 log in 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 When it connects to Internet.

4.13.2 Firmware

The page (shown in Figure 4-52) allows you to upgrade the latest version firmware to keep your router up-to-date.

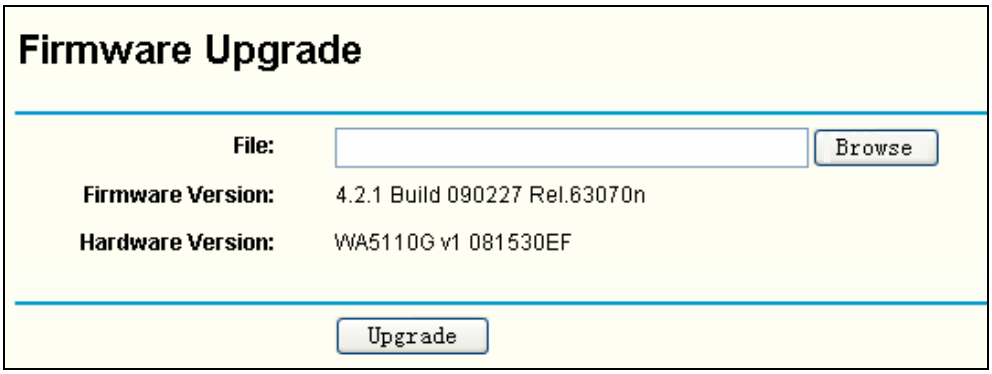


Figure 4-52 Firmware Upgrade

New firmware is posted on www.tp-link.com and can be downloaded for free. There is no need to upgrade the firmware unless the new firmware has a new feature you want to use. However, when experiencing problems caused by the AP itself, you can try to upgrade the firmware.

☞ **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 is finished.

4.13.3 Factory Defaults

This page (shown in Figure 4-53) allows you to restore the factory default settings for the router.

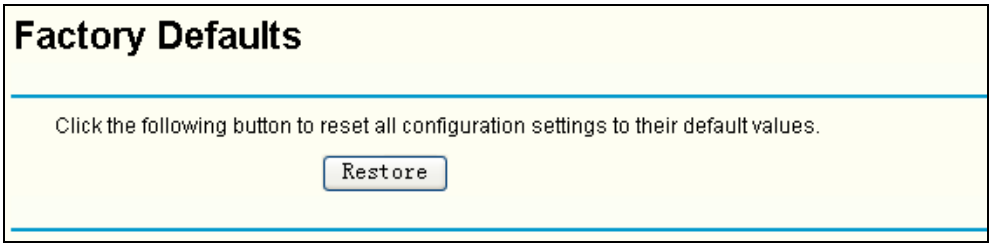


Figure 4-53 Restore Factory Default

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:**

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

4.13.4 Backup & Restore

This page (shown in Figure 4-54) allows you to save current configuration of router as backup or to restore the configuration file you saved before.

Figure 4-54 Backup & Restore Configuration

- Click the **Backup** button to save all configuration settings as a backup file to 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 by 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.

4.13.5 Ping Watch Dog

The **Ping Watch Dog** is dedicated for continuous monitoring of the particular connection to remote host using the Ping tool. It makes this device continuously ping a user defined IP address (it can be the internet gateway for example). If it is unable to ping under the user defined constraints, this device will automatically reboot.

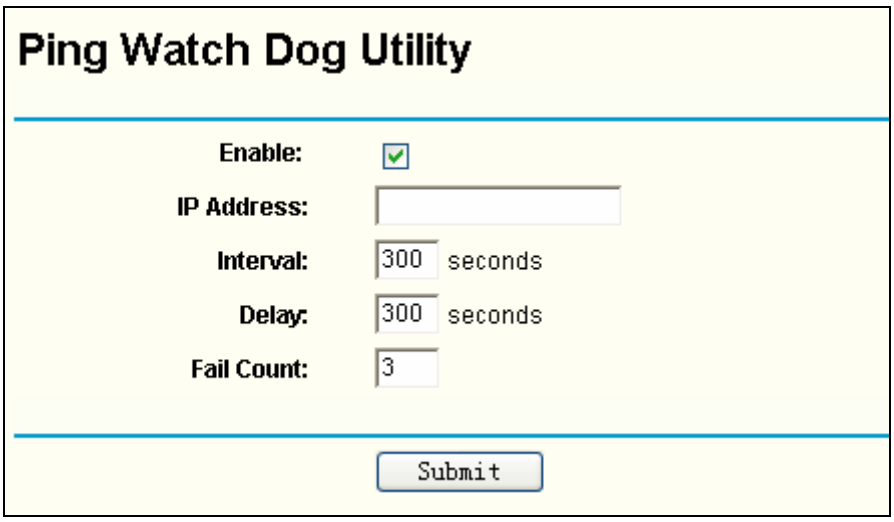


Figure 4-55 Ping Watch Dog Utility

- **Enable**: Turn on/off Ping Watch Dog.
- **IP Address**: The IP address of the target host where the Ping Watch Dog Utility is sending ping packets.
- **Interval**: Time internal between two ping packets which are sent out continuously.
- **Delay**: Time delay before first ping packet is sent out when the device is restarted.
- **Fail Count:** Upper limit of the ping packet the device can drop continuously. If this value is overrun, the device will restart automatically.

Be sure to click the **Submit** button to make your settings in operation.

4.13.6 Speed Test

The **Speed Test** is dedicated for testing the connection speed to and from any reachable IP address on current network, especially when we are building wireless network between devices which are far away from each other. It should be used for the preliminary throughput estimation between two network devices. The estimation is rough. You can input the remote device's administrator Username and Password under **Advance options** to get a precise estimation if the remote device is **TL-WA5110G** too.

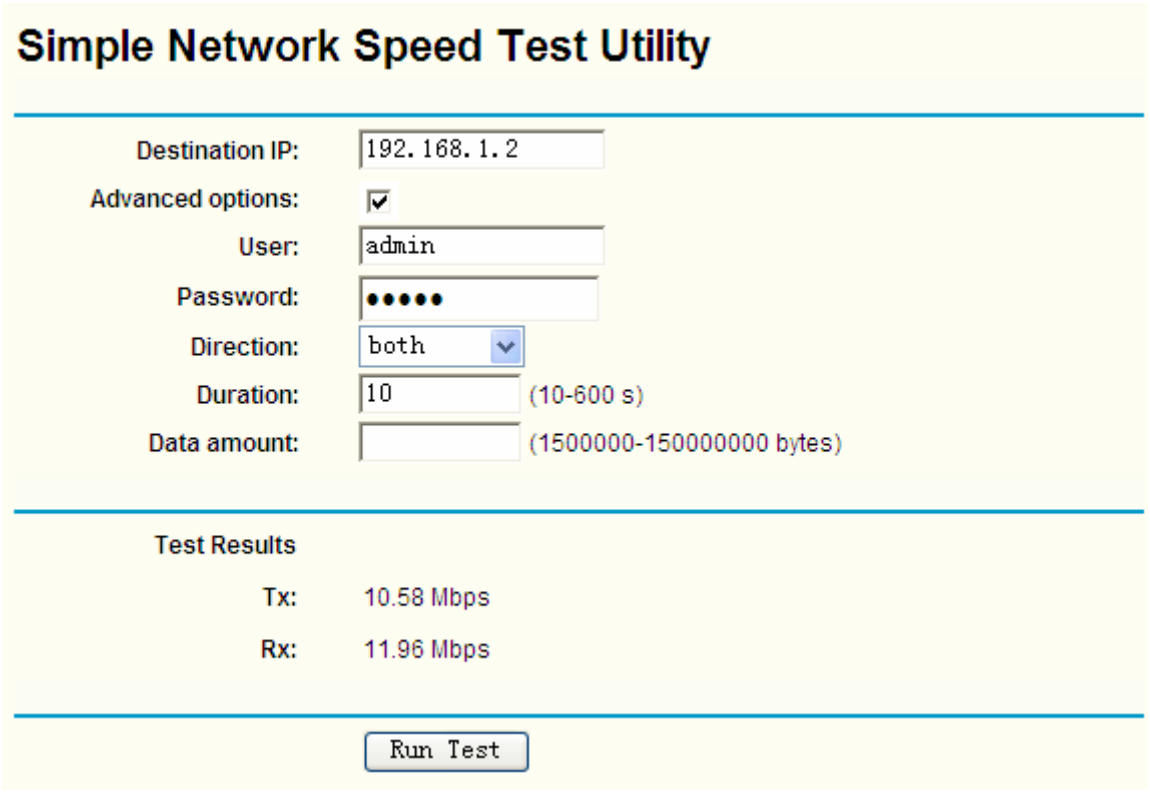


Figure 4-56 Speed Test

- **Destination IP**: The Remote device's IP address.
- **Advanced options**: This is switch to show advanced test options which are used only for precise estimation.
- **User**: Administrator password of the remote device. It should be filled correctly if you want to get a precise estimation. Otherwise, keep it blank.

☞ **Note:**

If either User or Password is incorrect, we will take a basic test instead. In other words, none of the advance options you set will take effect.

- **Direction**: There are 3 options available for the traffic direction while estimating the throughput.
  - **transmit**-Estimate the outgoing throughput (TX).
  - **receive**- Estimate the ingoing throughput (RX).
  - **both**- Estimate the incoming (RX) first and then the outgoing (TX) afterwards.
- **Duration**: The value you specify here indicate how much time the test should last.
- **Data amount**: The maximal data amount to be sent out during the whole test.

☞ **Note:**

If both Duration and Data amount are specified, the test will stop after any of them is met.

Be sure to click the **Run Test** button to start a new test after you filled enough information. You can also stop a running test by click Stop Test button at any time.

4.13.7 Reboot

This page (shown in Figure 4-57) allows you to reboot the router.

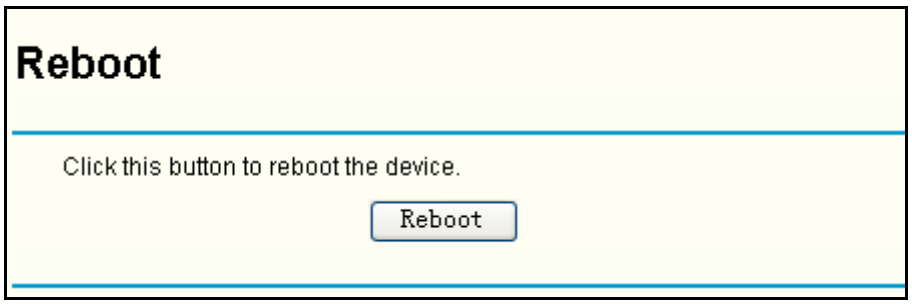


Figure 4-57 Reboot the router

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).

4.13.8 Password

This page (shown in Figure 4-58) allows you to change the factory default user name and password of the router.

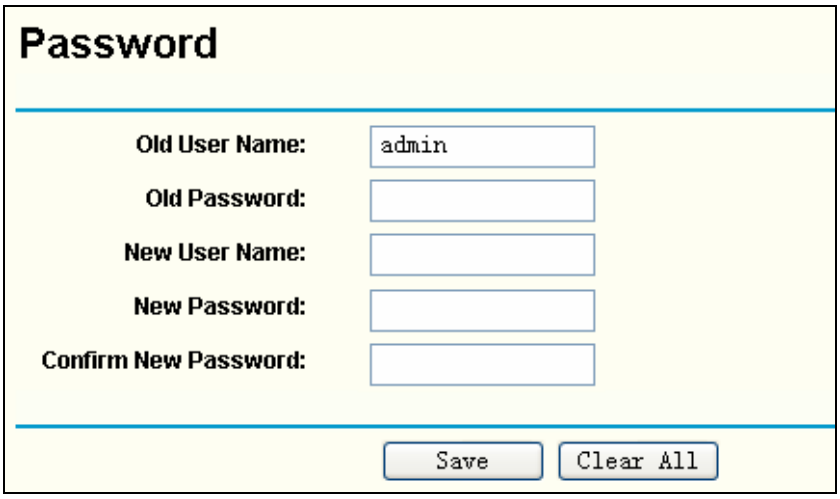


Figure 4-58 Password

It is strongly recommended 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.

4.13.9 Syslog

This page (shown in Figure 4-59) allows you to query the logs of the router.

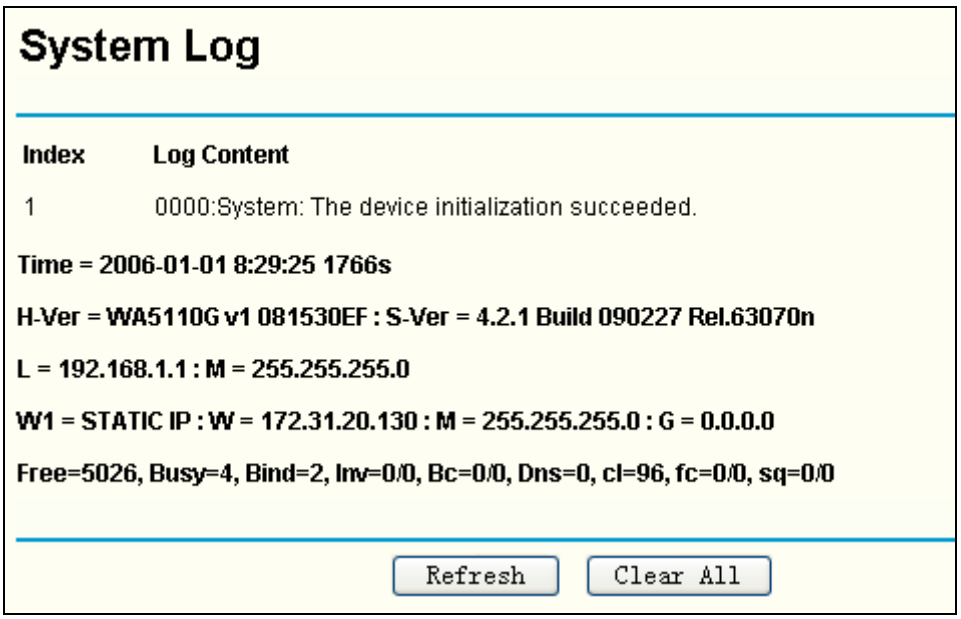


Figure 4-59 System Log

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.

4.13.10 Remote Management

You can configure the Remote Management function on this page shown in Figure 4-60. This feature allows you to manage your Router from a remote location via the Internet.

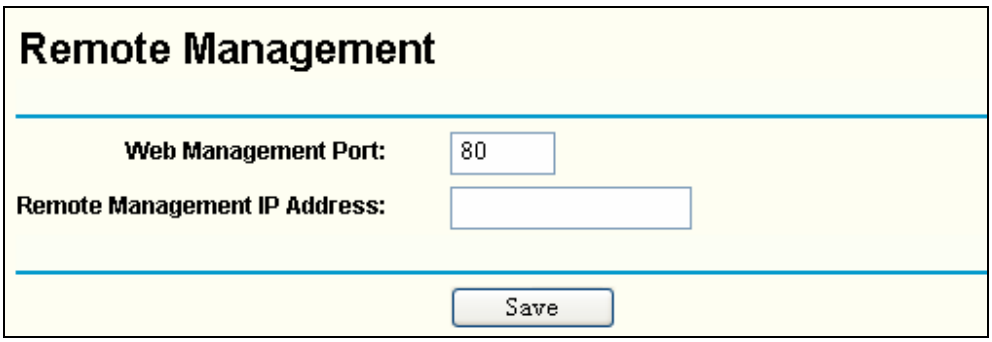


Figure 4-60 Remote Management

- **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 1 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. If it is set to 255.255.255.255, all the hosts can access the router from internet.

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. In AP mode, port 80 is only supported. The web management port number will be set to 80 when the operation mode changes to AP mode.

4.13.11 Statistics

The Statistics page (shown in Figure 4-61) displays the network traffic of each PC on the LAN, including total traffic and traffic of the last **Packets Statistic interval** seconds.

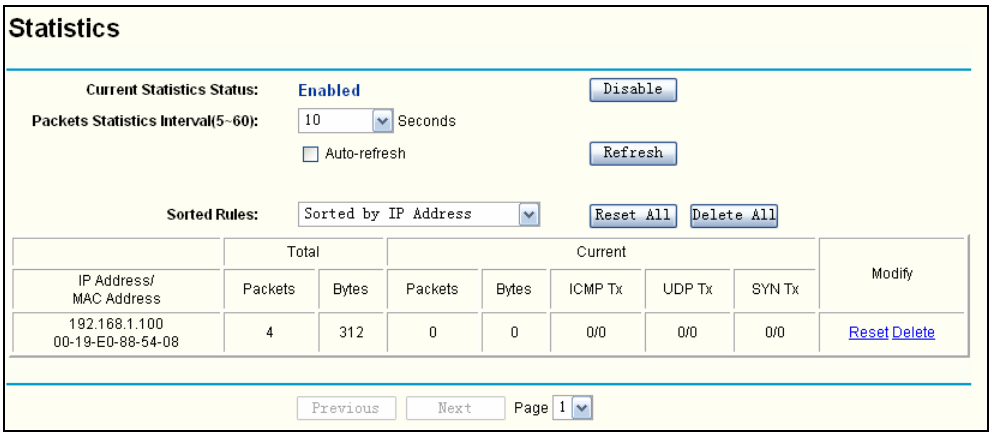


Figure 4-61 Statistics

- **Current Statistics Status -** Enabled or Disabled. 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 from 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.

Chapter 5. Configuring the Device in AP Operation Mode

This Chapter describes how to configure some advanced settings for your Access Point through the web-based management page in AP operation mode.

5.1 Login

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

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

5.2 Status

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

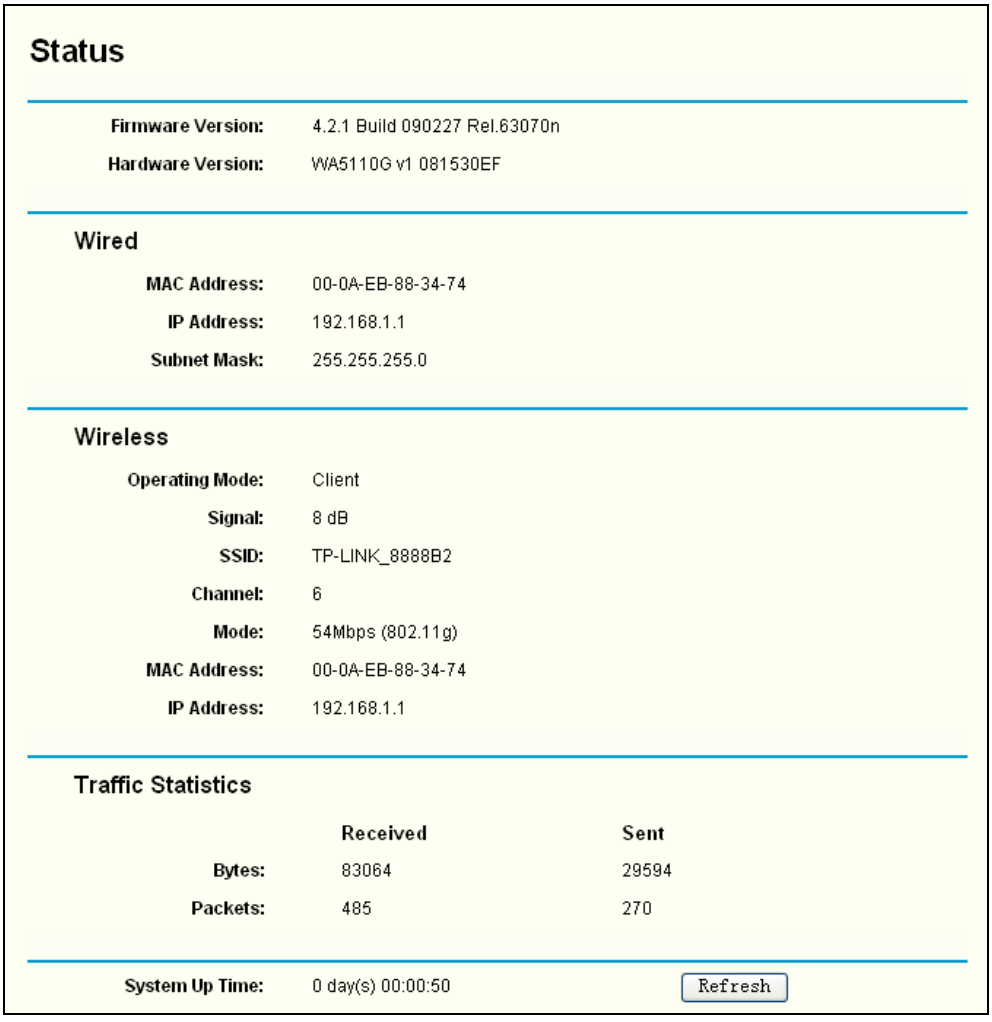


Figure 5-1

- **Wired -** This field displays the current settings or information for the Network, including the **MAC address, IP address** and **Subnet Mask**.
- **Wireless -** This field displays basic information or status for wireless function, including

Operating Mode, Signal, SSID, Channel, Mode, MAC Address and **IP Address**.

- **Traffic Statistics -** This field displays the AP's traffic statistics.
- **System Up Time -** The time of the AP running from it's powered on or reset.

5.3 Quick Setup

Please refer to Section 3.2: "Quick Setup."

5.4 Operation Mode

The AP supports three operation modes, **AP Client Router**, **AP Router** and **AP**. Please select one your want. Click **Save** to save your choice. Figure 5-2:

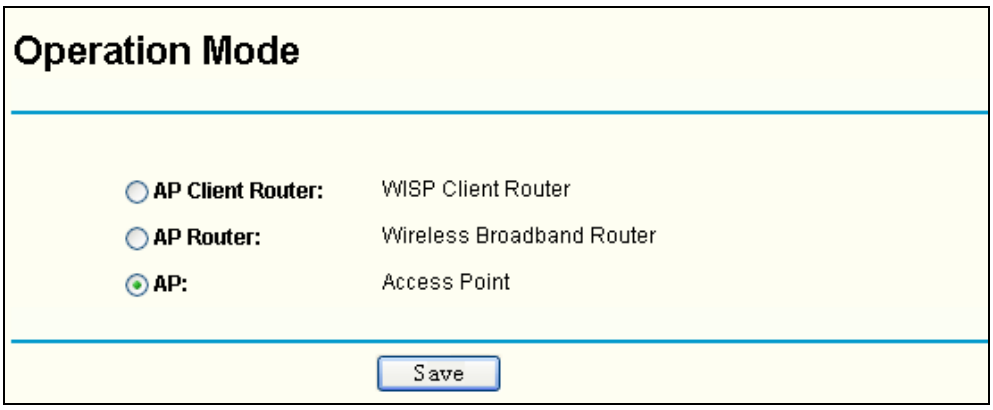


Figure 5-2 Operation Mode

- **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 port acts as a LAN port.
- **AP Router:** In this mode, the device enables multi-user to share the Internet via ADSL/Cable Modem. 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.
- **AP:** In this mode, the device allows wireless communication devices to access a wireless network by using WIFI. The Ethernet port and the wireless port both work as LAN ports.

5.5 Network

Click **Network** on the main menu. You can configure the IP parameter on the following page .

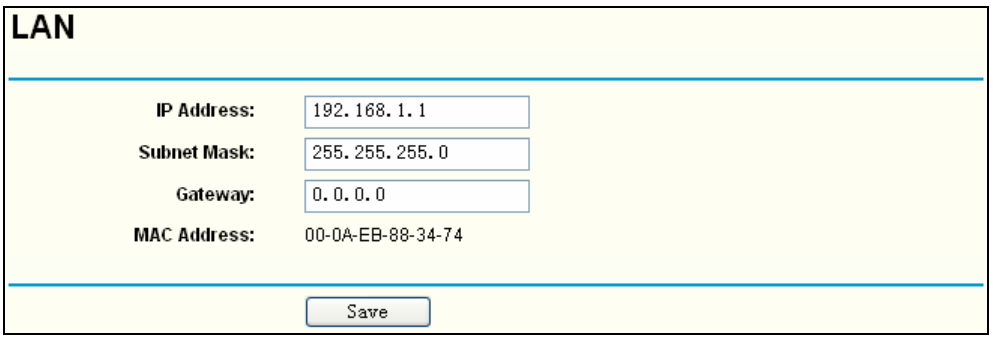


Figure 5-3 Network

- **IP Address -** Enter the IP address of your AP 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.

- **Gateway -** The gateway should be in the same subnet as your IP address.
- **MAC Address -** the physical address of the AP, as seen from the LAN. This value can't be changed.

Note:

1） If you change the IP Address, you must use the new IP Address to log in the AP.

2） If the new LAN IP Address you set is not in the same subnet, the IP Address pool in the DHCP sever will not take effect unless they are re-configured.

3） The device will reboot automatically after clicking **Save**.

5.6 Wireless

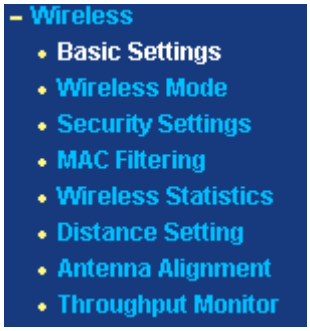


Figure 5-4 Wireless menu

There are eight submenus under the Wireless menu (shown in Figure 5-4):**Basic Settings**, **Wireless Mode**, **Security Settings**, **MAC Filtering**, **Wireless Statistics**, **Distance Setting**, **Antenna Alignment** and **Throughput Monitor**. Click any of them, and you will be able to configure the corresponding function. The detailed explanations for each submenu are provided below.

5.6.1 Basic Settings

The basic settings for the wireless network in AP operation mode are set on this page.

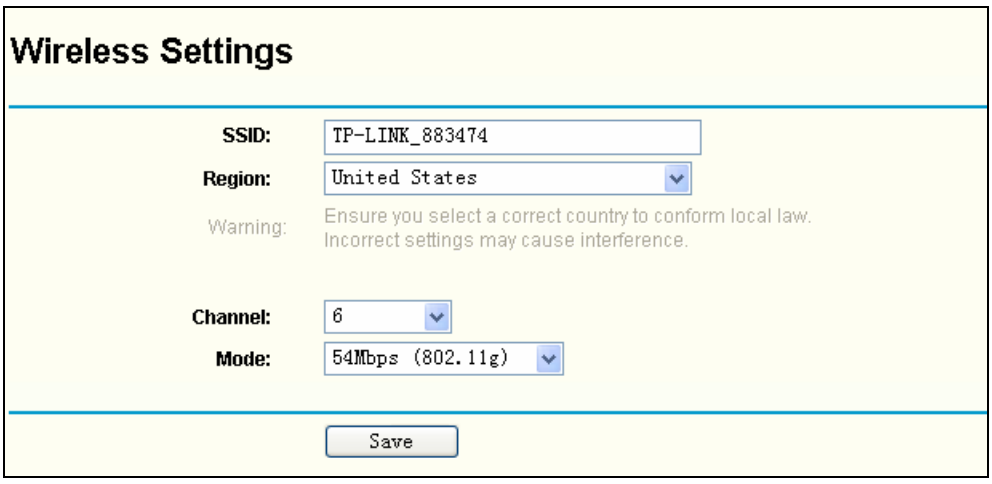


Figure 5-5 Wireless Settings in AP mode

- **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_xxxxxx (xxxxxx indicates the

last six unique characters of each device's MAC address). This value is case-sensitive. For example, *TP-LINK* is NOT the same as *tp-link*.

- **Region**-Select your region from the drop-down list. This filed specifies the region where the wireless function of the device can be used. It may be illegal to use the wireless function of the device in a region other than one of those specified in this field. If your country or region is not listed, please contact your local government agency for assistance.
- **Channel** – This field determines which operating frequency will be used. It is not necessary to change the wireless channel unless you notice 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.

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

☞ **Note:**

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

5.6.2 Wireless Mode

This page allows you to configure the wireless mode for your device:

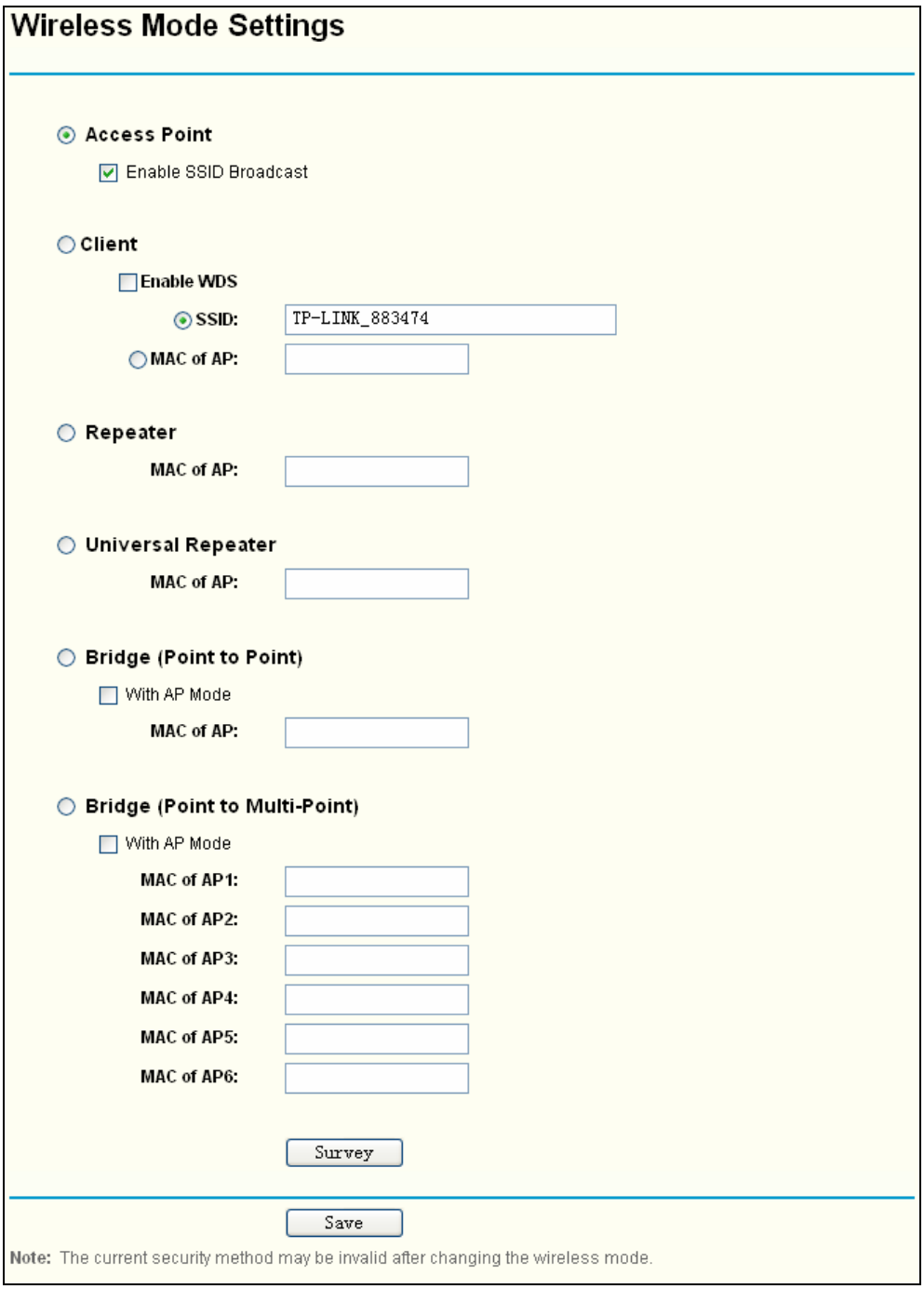


Figure 5-6 Wireless Mode

Note:

AP provides five operational modes: Access Point, Client, Repeater, Bridge (point to point), Bridge (point to Multi-point).

- **Access Point** - Access Point mode allows wireless stations including AP clients to access the router..
  - **Enable SSID Broadcast** - If you select the **Enable SSID Broadcast** checkbox, the Wireless AP will broadcast its name (SSID) on the air.
- **Client** - In **Client** mode, AP will act as a wireless station to enable wired host(s) to access wireless AP.

- **Enable WDS** - The AP client can connect to AP with WDS enabled or disabled. If WDS is enabled, all traffic from wired networks will be forwarded in the format of WDS frames consist of four address fields. If WDS is disabled, three address frames are used. If your AP supports WDS well, please select the option.
- **SSID** - Enter the SSID of AP that you want to access. If you select the radio before **SSID**, the AP client will connect to AP according SSID.
- **MAC of AP** - Enter the MAC address of AP that you want to access. If you select the radio before **MAC of AP**, the AP client will connect to AP according MAC address.

➢ **Repeater** - The **Repeater** mode is the AP with its own BSS and with WDS enabled that relays data to a root AP, to which it is associated. The wireless repeater relays signal between its stations and the root AP for greater wireless range. Please input the MAC address of root AP in the field of **MAC of AP**.

➢ **Universal Repeater** - The **Universal Repeater** mode is the AP with its own BSS and with WDS disabled that relays data to a root AP, to which it is associated. The wireless repeater relays signal between its stations and the root AP for greater wireless range. Please input the MAC address of root AP in the field of **MAC of AP**.

☞ **Note:**

If the available AP can't support with WDS, you may select Client mode without WDS or Universal Repeater mode to associate with the AP.

Here is an example of how to configure wireless repeater. Please do the following:

1. Configure the Operating Mode of the TL-WA5110G High Power wireless Access Points.
    - Configure AP1 on LAN Segment 1 in Access Point mode.
    - Configure AP2 in Repeater mode with the MAC address of its root AP (AP1).
    - Configure AP3 in Repeater mode with the MAC address of its root AP (AP2).

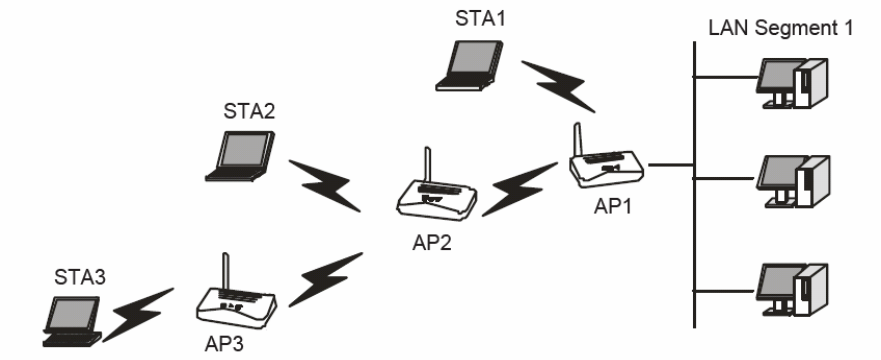


Figure 5-7 Wireless repeating

2. Verify the wireless security parameters for all access points, if any.
3. Verify connectivity across the LANs. A computer on any LAN segment should be able to connect to the Internet or share files and printers with any other PCs or servers connected to any of the three WLAN segments.

☞ **Note:**

You can extend this repeating by adding up to 2 additional TL-WA5110G High Power wireless Access Points configured in repeater mode. However, since Repeater configurations communicate in half-duplex mode, the bandwidth decreases as you add Repeaters to the

network. Also, you can extend the range of the wireless network with wireless antenna accessories.

- **Bridge (Point to Point)** - This mode bridges the AP and another AP also in bridge mode to connect two wired LANs. Please input the MAC address of the other AP in the field of **MAC of AP**. AP function can startup also.
  - **With AP mode:** If you select this option, you AP will also support AP mode when it is in Bridge (Point to Point) mode.

Here is an example of how to configure Point-to-Point Bridge. Please do the following:

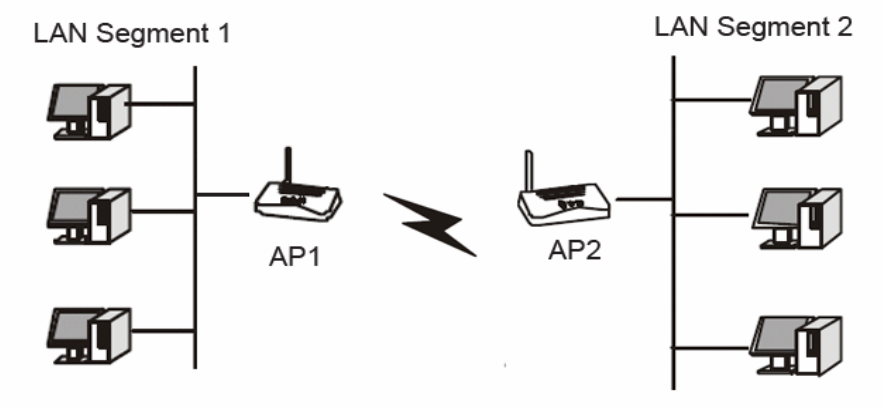


Figure 5-8 Point to Point Bridge

1. Configure the TL-WA5110G (AP1) on LAN Segment 1 in Point-to-Point Bridge mode.
2. Configure the TL-WA5110G (AP2) on LAN Segment 2 in Point-to-Point Bridge mode. AP1 must have AP2's MAC address in its MAC Address field and AP2 must have AP1's MAC address in its MAC Address field.
3. Configure and verify the following parameters for both access points:
   - Both use the same Channel and security settings if security is in use.

Verify connectivity across the LAN 1 and LAN 2. A computer on either LAN segment should be able to connect to the Internet or share files and printers of any other PCs or servers connected to LAN Segment 1 or LAN Segment 2.

- **Bridge (Point to Multi-Point)** - This mode bridges the AP and up to 6 APs also in bridge mode to connect two or more wired LANs. Please input the MAC address of other APs in the field of **MAC of AP1** to **MAC of AP6**. AP function can startup also.
  - **With AP mode:** If you select this option, you AP will also support AP mode when it is in Bridge (Point to Multi-Point) mode.

Here is an example of how to configure multi-point bridging. Please do the following:

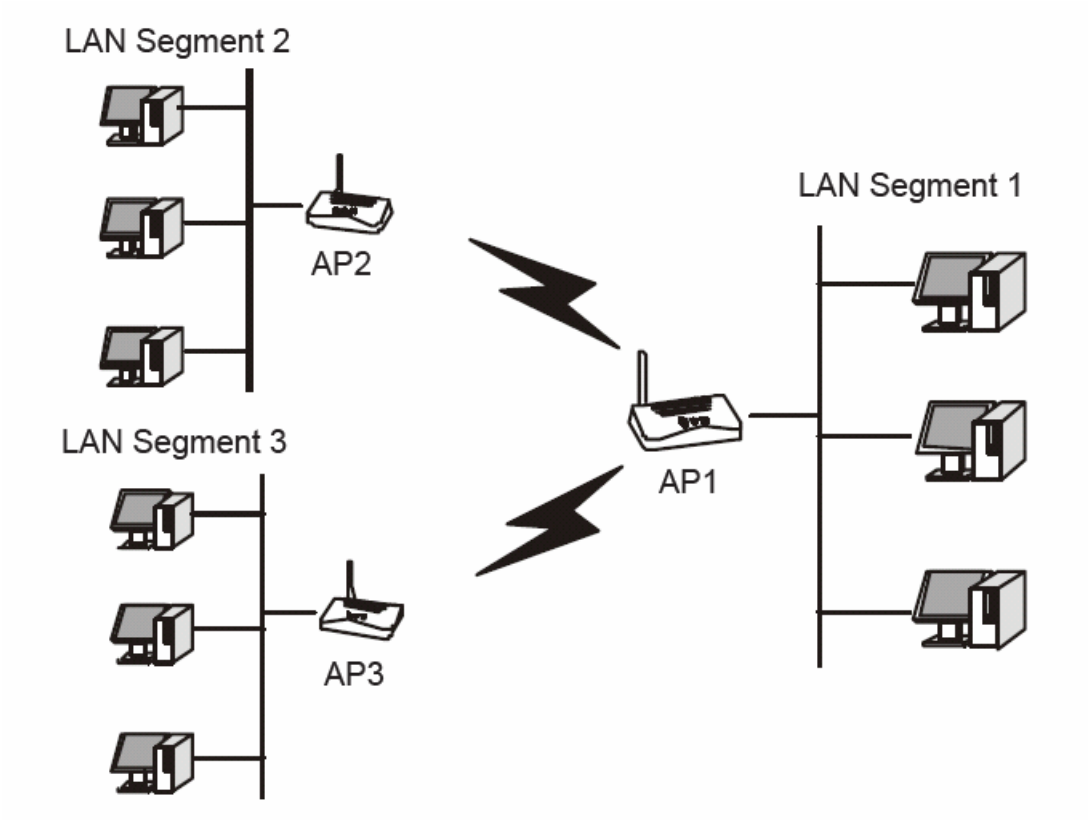


Figure 5-9 Point to Multi-point Bridge

1. Configure the Operating Mode of the TL-WA5110G High Power wireless Access Points.
   - Because it is in the central location, configure TL-WA5110G (AP1) on LAN Segment 1 in Point-to-Multi-Point Bridge mode. The MAC addresses of AP2 and AP3 are required in AP1.
   - Configure TL-WA5110G (AP2) on LAN Segment 2 in Point-to-Point Bridge mode with the MAC Address of AP1.
   - Configure the TL-WA5110G (AP3) on LAN 3 in Point-to-Point Bridge mode with the MAC Address of AP1.
2. Verify the following parameters for all access points.
   - All TL-WA5110G Access Points use the same Channel, and security settings if any.
   - All Point-to-Point APs must have AP1's MAC address in its AP MAC address field, and AP1 must have all All Point-to-Point APs' MAC addresses.
3. Verify connectivity across the LANs.
   - A computer on any LAN segment should be able to connect to the Internet or share files and printers with any other PCs or servers connected to any of the three LAN segments.

Wireless stations will not be able to connect to the TL-WA5110G High Power wireless Access Points in the illustration above. If you require wireless stations to access any LAN segment, you can add TL-WA5110G Access Points configured in Wireless Access Point mode to any LAN segment.

☞ **Note:**

You can extend this multi-point bridging by adding additional TL-WA5110Gs configured in Point-to-Point mode for each additional LAN segment. Furthermore, you can extend the range of

the wireless network with wireless antenna accessories.

Note:

To apply any settings you have altered on the page, please click the **Save** button, and wait the AP reboot automatically.

Click **Survey** will show the site list of scanning result shown as Figure 5-10.

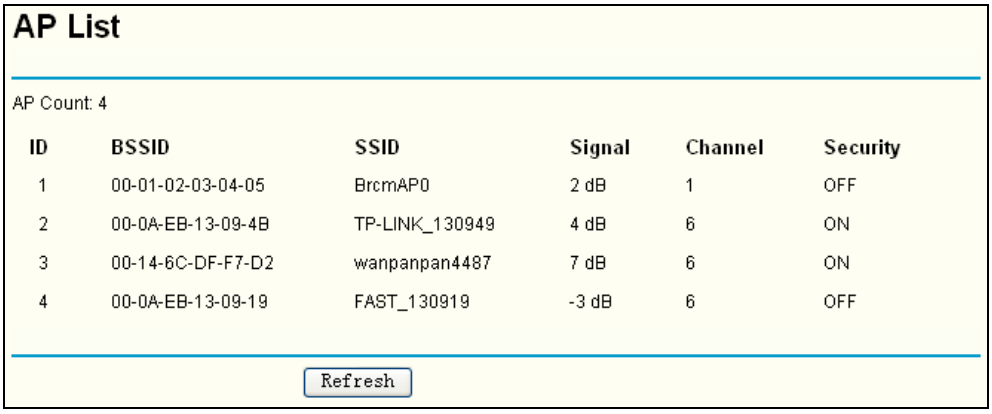


Figure 5-10 AP List

- **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.

5.6.3 Security Settings

You can select one of the following security options:

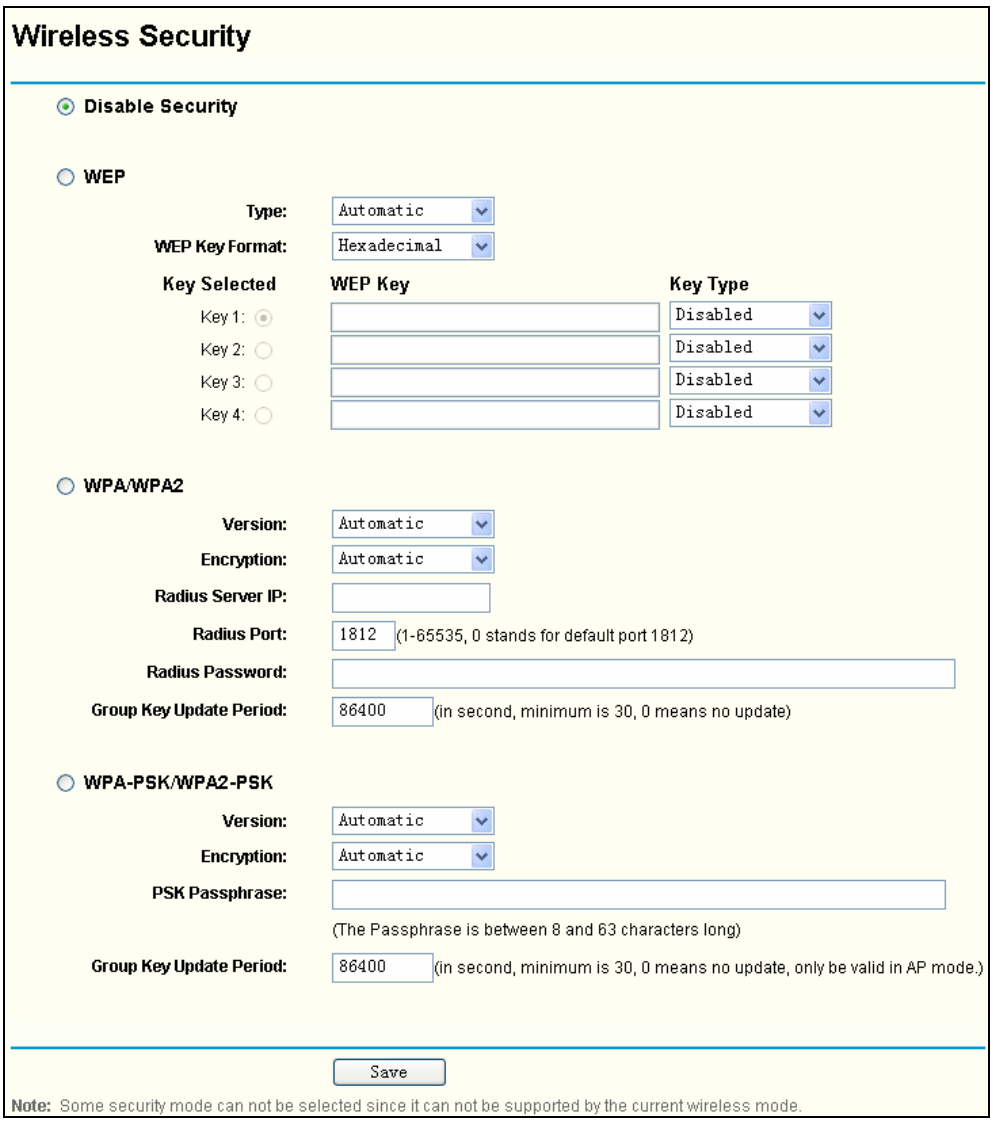


Figure 5-11 Wireless Security

- **Disable Security** - The wireless security function can be enabled or disabled. If disabled, the wireless stations will be able to connect the device without encryption. It is recommended strongly that you choose one of following options to enable security.
- **WEP** - Select 802.11 WEP security.
  - **Type** - You can select one of following types,

  1). **Automatic** - Select **Shared Key** or **Open System** authentication type automatically based on the wireless station's capability and request.

  2). **Shared Key** - Select 802.11 Shared Key authentication.

  3). **Open System** - Select 802.11 Open System authentication.

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

1). 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.

2). 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.

3). 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.

☞ **Note:**

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

➢ **WPA/WPA2 -** Select WPA/WPA2 based on Radius Server.

- **Version** - You can select one of following versions,

1). **Automatic** - Select **WPA** or **WPA2** automatically based on the wireless station's capability and request.

2). **WPA** - Wi-Fi Protected Access.

3). **WPA2** - WPA version 2.

- **Encryption** - You can select either **Automatic**, or **TKIP** or **AES**.
- **Radius Server IP** - Enter the IP address of the Radius Server.
- **Radius Port** - Enter the port that radius service used.
- **Radius Password** - Enter the password for the Radius Server.
- **Group Key Update Period** - Specify the group key update interval in seconds. The value can be either 0 or at least 30. Enter 0 to disable the update.

➢ **WPA-PSK/ WPA2-PSK -** Select WPA based on pre-shared passphrase.

- **Version** - You can select one of following versions,

1). **Automatic** - Select **WPA-PSK** or **WPA2-PSK** automatically based on the wireless station's capability and request.

2). **WPA-PSK** - Pre-shared key of WPA.

3). **WPA2-PSK** - Pre-shared key of WPA2.

- **Encryption** - When you select **WPA-PSK** or **WPA2-PSK** for **Authentication Type** you can select either **Automatic**, or **TKIP** or **AES** as **Encryption**.
- **PSK Passphrase** - You can enter a passphrase between 8 and 63 characters long.
- **Group Key Update Period** - Specify the group key update interval in seconds. The value can be either 0 or at least 30. Enter 0 to disable the update.

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

☞ **Note:**

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

5.6.4 MAC Filtering

The Wireless MAC Filtering for wireless networks are set on this page. Figure 5-12

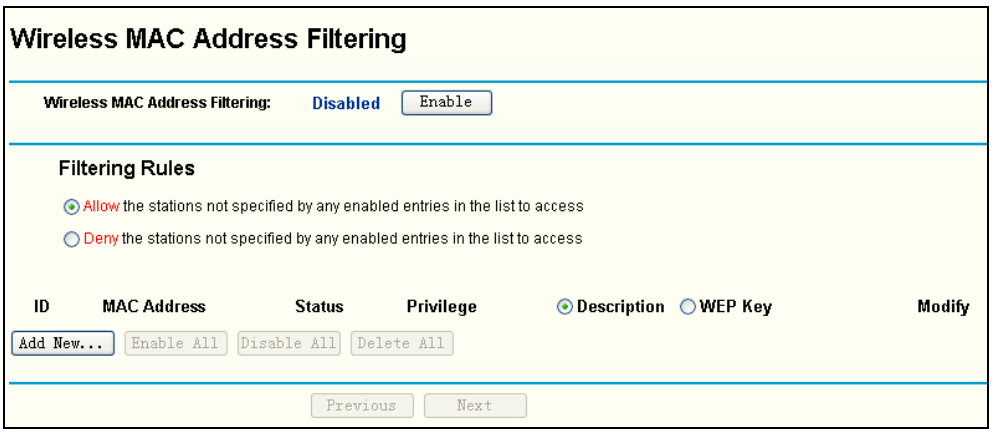


Figure 5-12 Wireless MAC address Filtering

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 5-13:

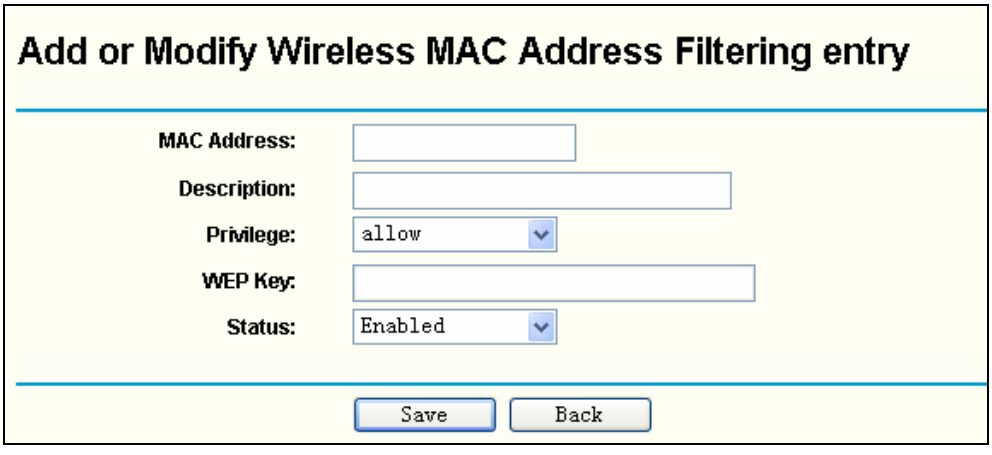


Figure 5-13 Add or Modify Wireless MAC Address Filtering entry

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.

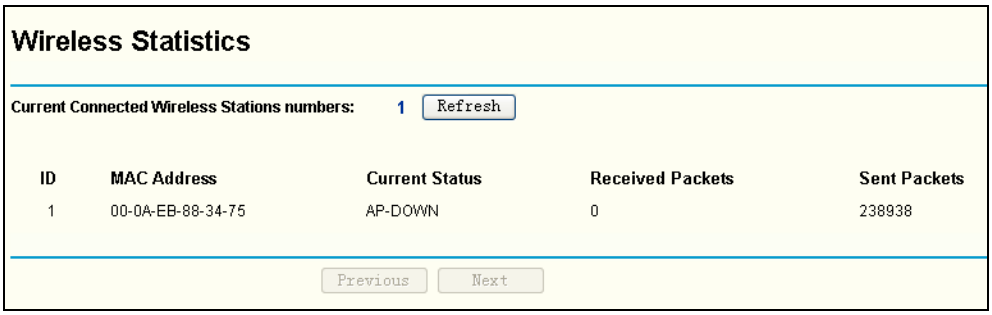


Figure 5-14 The router attached wireless stations

- **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.

5.6.6 Distance Setting

This feature is used to adjust the wireless range in outdoor conditions. This is a critical feature required for stabilizing outdoor links. Enter the distance of your wireless link and the software will optimize the frame ACK timeout value automatically.

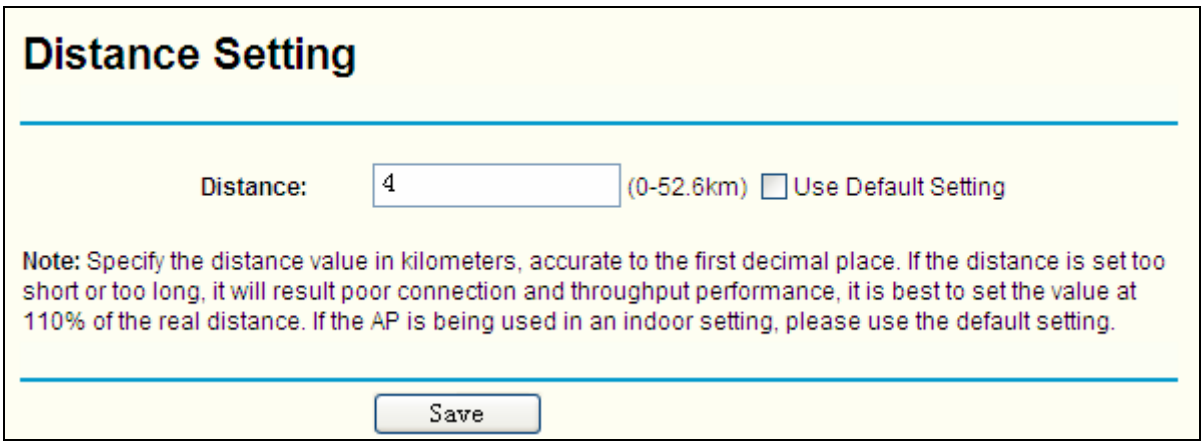


Figure 5-15 Distance Setting

- **Use Default Setting:** Keep the default setting if the AP is used for indoor environment. If you want to change the distance, please uncheck the **Use Default Setting** box.
- **Distance:** Specify the distance value in kilometers, accurate to the first decimal place. If the distance is set too short or too long, it will result poor connection and throughput performance, it is best to set the value at 110% of the real distance. If the AP is being used in an indoor setting, please use the default setting.

Click **Save** to keep your settings.

5.6.7 Antenna Alignment

This page shows how remote AP's signal strength changes while changing the antenna's direction.

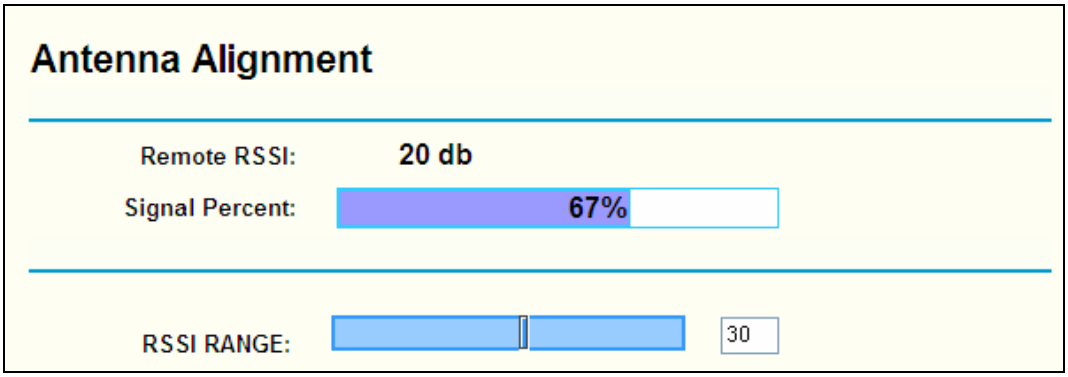


Figure 5-16 Antenna Alignment

- **Remote AP RSSI** - Remote AP's signal strength value.
- **Signal percent** - The ratio of RSSI to RSSI RANGE in percentage.
- **RSSI RANGE** - You can drag the slider bar to set or input the RSSI RANGE value. The slider bar allows the range of the meter to be either increased or reduced. If the range is reduced, the color change will be more sensitive to signal fluctuations. The slider bar actually changes an offset of the maximum indicator value scale.

☞ **Note:**

It only works after you have established connection to remote AP under client mode

5.6.8 Throughput Monitor

This page allows you to view the wireless throughput information

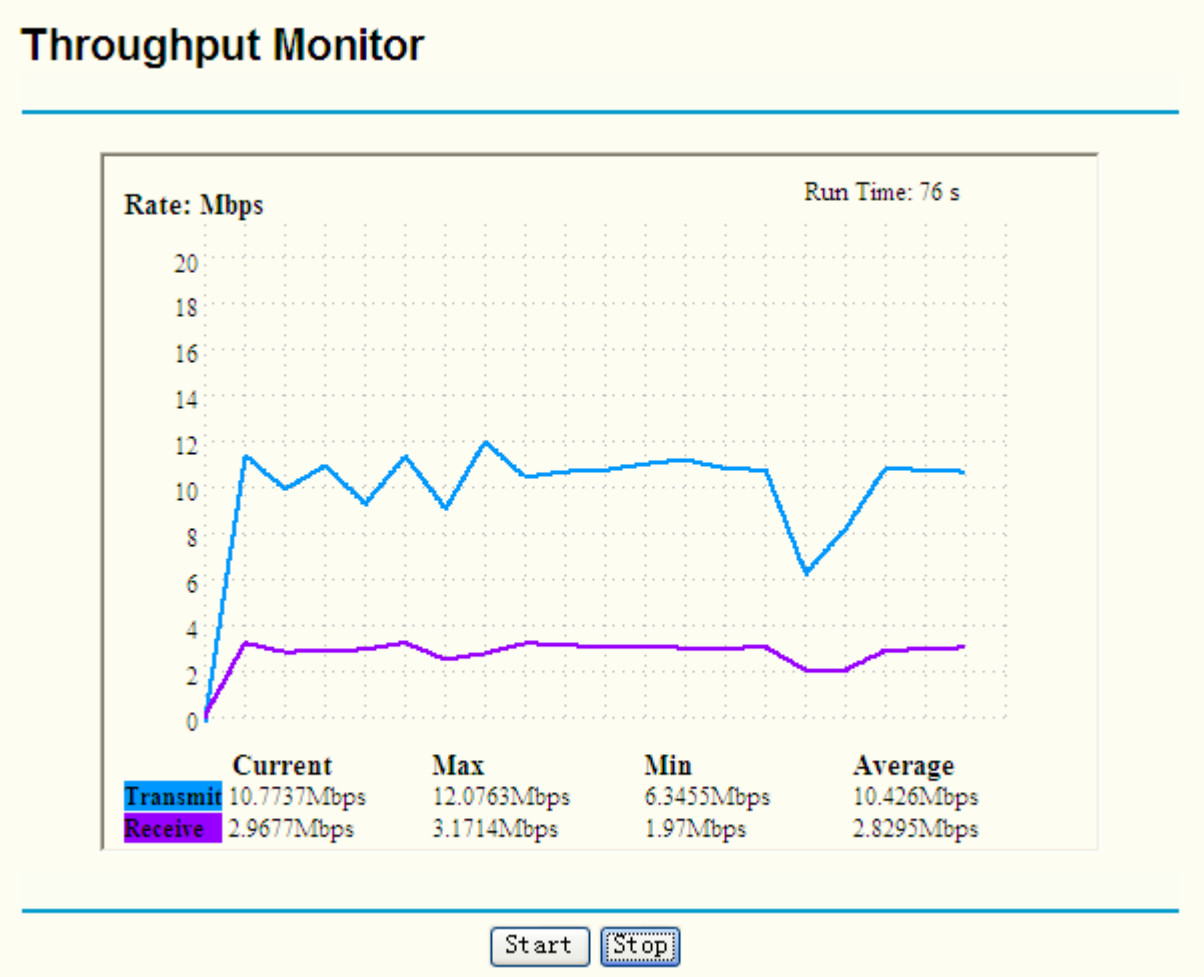


Figure 5-17 Wireless Throughput

Rate - The Throughput unit.

Run Time - How long this function is running.

Transmit- Wireless transmit rate information.

Receive- Wireless receive rate information.

Click the **Start** button to start wireless throughput monitor.

Click the **Stop** button to stop wireless throughput monitor.

5.7 DHCP

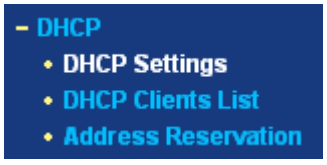


Figure 5-18 The DHCP menu

There are three submenus under the DHCP menu (shown in Figure 5-18): **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 5-19):

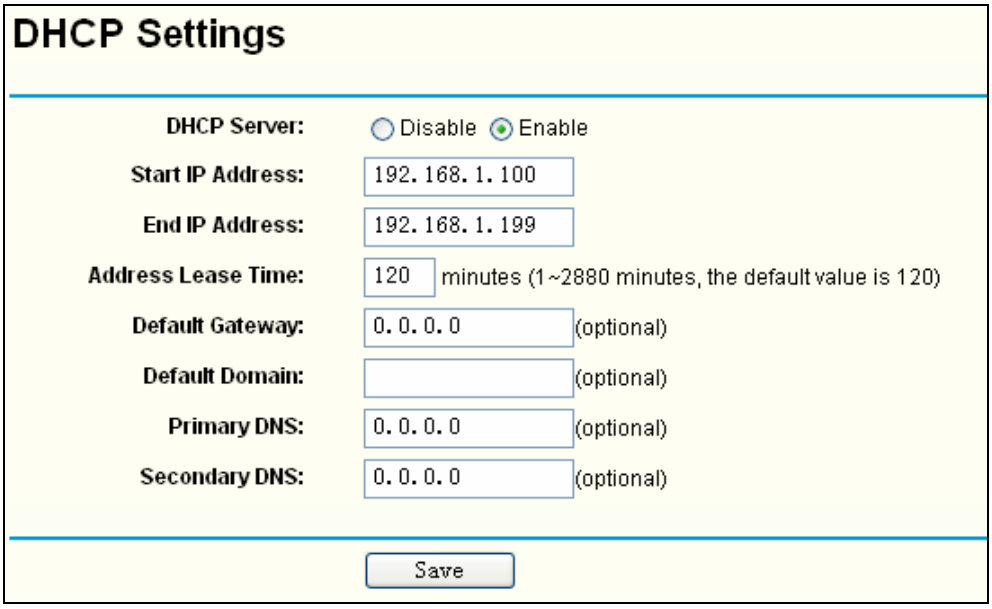


Figure 5-19 DHCP Settings

- **DHCP Server - Enable** or **Disable** the DHCP server. If you disable the Server, you must have another DHCP server within your network ， or else you have to 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 to connect to the router with their current dynamic IP Address. Enter the amount of time in minute. 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.

Click **Save** to save the new settings to the router

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 5-20.

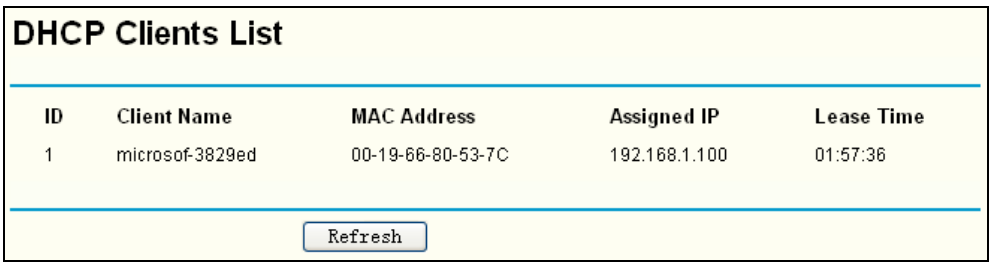


Figure 5-20 DHCP Clients List

- **Index(ID)-** The index of the DHCP Client
- **Client Name -** The name of the DHCP client
- **MAC Address -** The MAC address of the DHCP client
- **Assigned IP -** The IP address that the router has allocated to the DHCP client.
- **Lease Time -** The time of the DHCP client leased. 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 5-21).

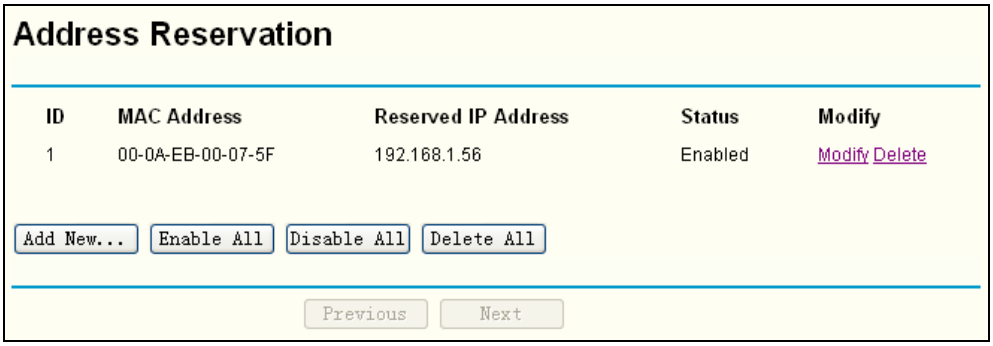


Figure 5-21 Address Reservation

- **MAC Address -** The MAC address of the PC which you want to reserve IP address for.
- **Reserved IP Address -** The IP address of the router reserved.
- **Status -** It shows whether the entry is enabled or not.
- **Modify –** To modify or delete an existing entry.

To Reserve IP addresses:

1. Click the **Add New button** in the page of **Address Reservation**, the following page(Figure 5-22) will display.
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 want to add.
3. Click the **Save** button after finish configuring.

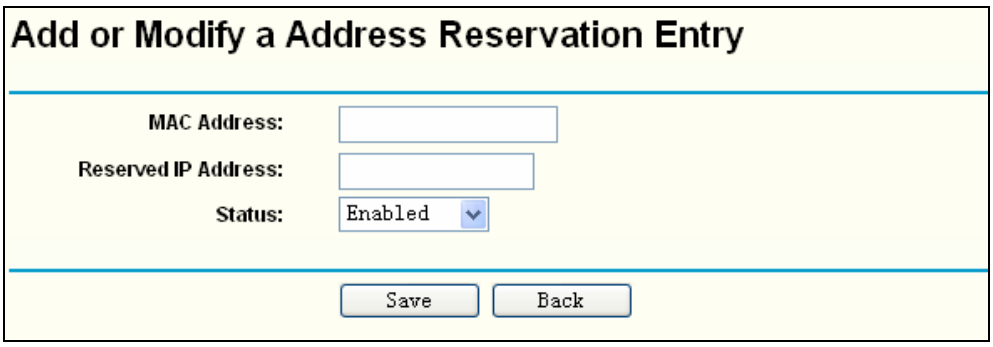


Figure 5-22 Add or Modify an Address Reservation Entry

To modify or delete an existing entry:

1. Select a reserved address entry, Click the **Modify** in the entry if you want to modify it. If you want to delete the entry, click the **Delete**.
2. 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, or Click the **Previous** button to return the previous page.

☞ **Note:**

The change of the address reservation won't take effect until the device reboot.

5.8 Wireless settings

This page allows you to configure some settings for your wireless network, which is shown in Figure 5-23 .

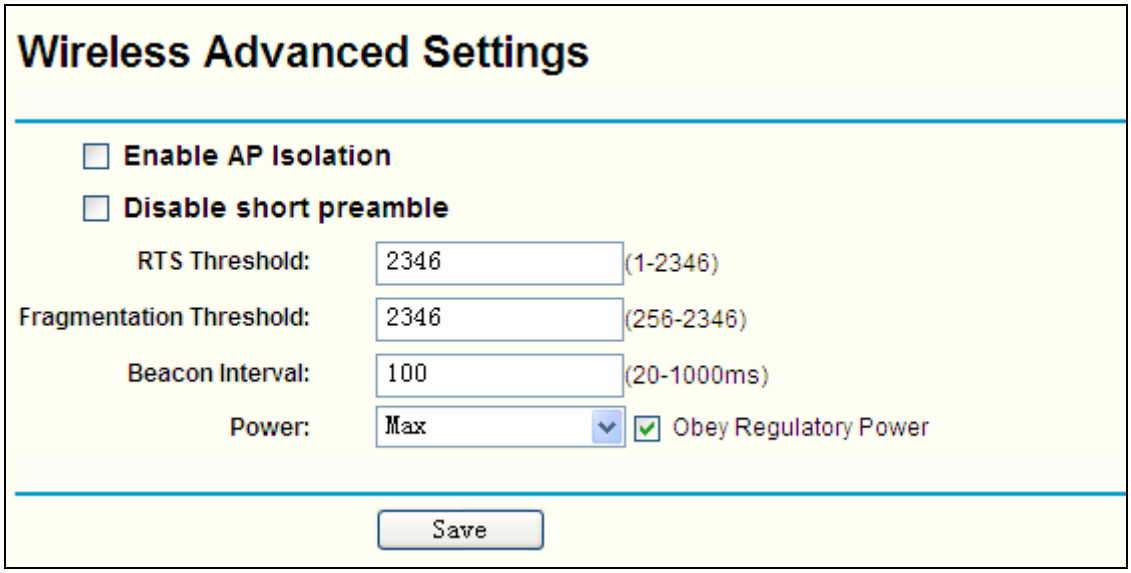


Figure 5-23 Wireless settings

- **Enable AP Isolation** - Isolate all connected wireless stations so that wireless stations can not access each other through WLAN. This option is available only for AP mode.
- **Disable short preamble** - Disable short preamble and use long preamble only. 802.11b mode supports only long preamble and this parameter will be ignored. It is recommended that you do not change these settings.

- **RTS threshold** - RTS/CTS Threshold, the packet size that is used to determine if RTS/CTS should be sent.
- **Fragmentation threshold** - The maximum packet size used for fragmentation.
- **Beacon Interval** - The interval time between two successive beacons.
- **Power** - The transmit power of the access point. The checkbox determines the transmit power that whether it obeys regulatory power or not. Un-checking the **Obey Regulatory Power** option may cause interference to other devices and violate the applicable law.

5.9 System Tools

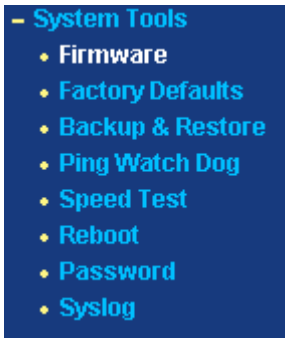


Figure 5-24 The System Tools menu

There are eight submenus under the System Tools menu (shown in Figure 5-24): **Firmware**, **Factory Defaults**, **Backup & Restore**, **Ping Watch Dog**, **Speed Test**, **Reboot**, **Password** and **Syslog**. 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 Firmware

The page allows you to upgrade the AP to the most recent version of firmware on the screen below (Figure 5-25).

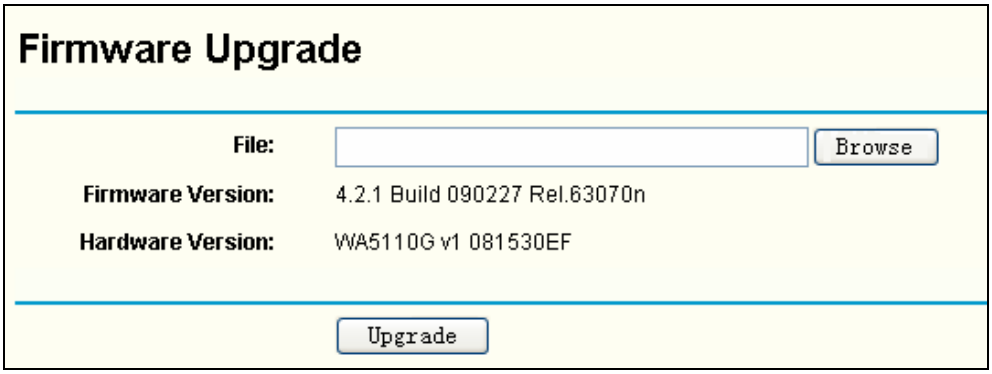


Figure 5-25 Firmware Upgrade

New firmware versions are posted at www.tp-link.com and can be downloaded for free. There is no need to upgrade the firmware unless the new firmware has a new feature you want to use. However, when experiencing problems caused by the AP itself, you can try to upgrade the firmware.

☞ **Note:**

Before upgrading the AP's firmware，you should write down some of your customized settings to avoid losing important configuration settings of AP.

To upgrade the AP's firmware, please take the following steps:

1. Download a more recent 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 **Upgrade**.

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

Note:

Do not turn off the AP or press the Reset button while the firmware is being upgraded. The AP will reboot after the Upgrading has been finished.

5.9.2 Factory Defaults

The page allows you to restore the factory default settings for the AP on the screen below (Figure 5-26).

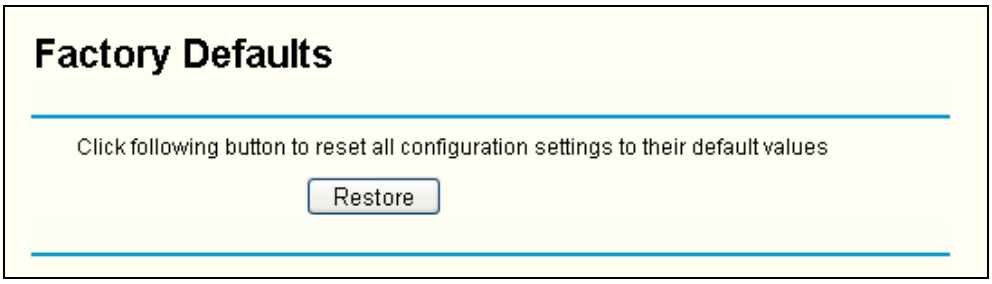


Figure 5-26 Restore Factory Default

Click **Restore** 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:

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

5.9.3 Backup & Restore

This page allows you to save all configuration settings to your local computer as a file or restore the AP's configuration.

Figure 5-27 Save or Restore the Configuration

Click **Backup** to save a backup configuration file to your local computer.

To restore the AP's configuration, please take the following steps:

- Click **Browse** to find the location of configuration file which you want to restore.
- Click **Restore** to update the configuration with the file whose path is the one you have input or selected in the blank.

☞ **Note:**

1. The current configuration will be covered by the uploading configuration file.
2. Wrong process will lead the device unmanaged.
3. The restoring process will last for 20 seconds and the AP will restart automatically. Do not power off the device during the process to avoid any damage.

5.9.4 Ping Watch Dog

The **Ping Watch Dog** is dedicated for continuous monitoring of the particular connection to remote host using the Ping tool. It makes this device continuously ping a user defined IP address (it can be the internet gateway for example). If it is unable to ping under the user defined constraints, this device will automatically reboot.

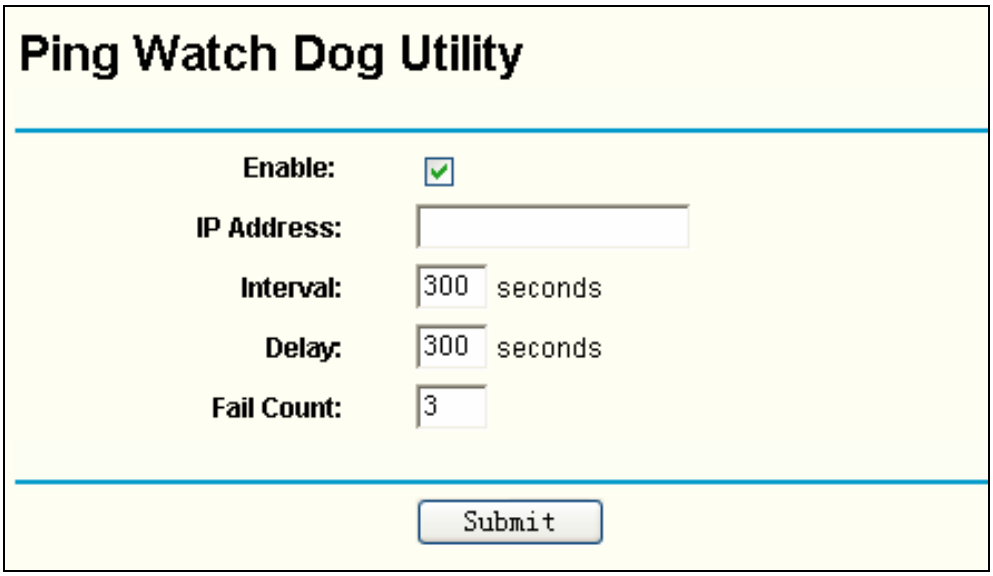


Figure 5-28 Ping Watch Dog Utility

- **Enable**: Turn on/off Ping Watch Dog.
- **IP Address**: The IP address of the target host where the Ping Watch Dog Utility is sending ping packets.
- **Interval**: Time internal between two ping packets which are sent out continuously.
- **Delay**: Time delay before first ping packet is sent out when the device is restarted.
- **Fail Count:** Upper limit of the ping packet the device can drop continuously. If this value is overrun, the device will restart automatically.

Be sure to click the **Submit** button to make your settings in operation.

5.9.5 Speed Test

The **Speed Test** is dedicated for testing the connection speed to and from any reachable IP address on current network, especially when we are building wireless network between devices which are far away from each other. It should be used for the preliminary throughput estimation between two network devices. The estimation is rough. You can input the remote device's

administrator Username and Password under **Advance options** to get a precise estimation if the remote device is **TL-WA5110G** too.

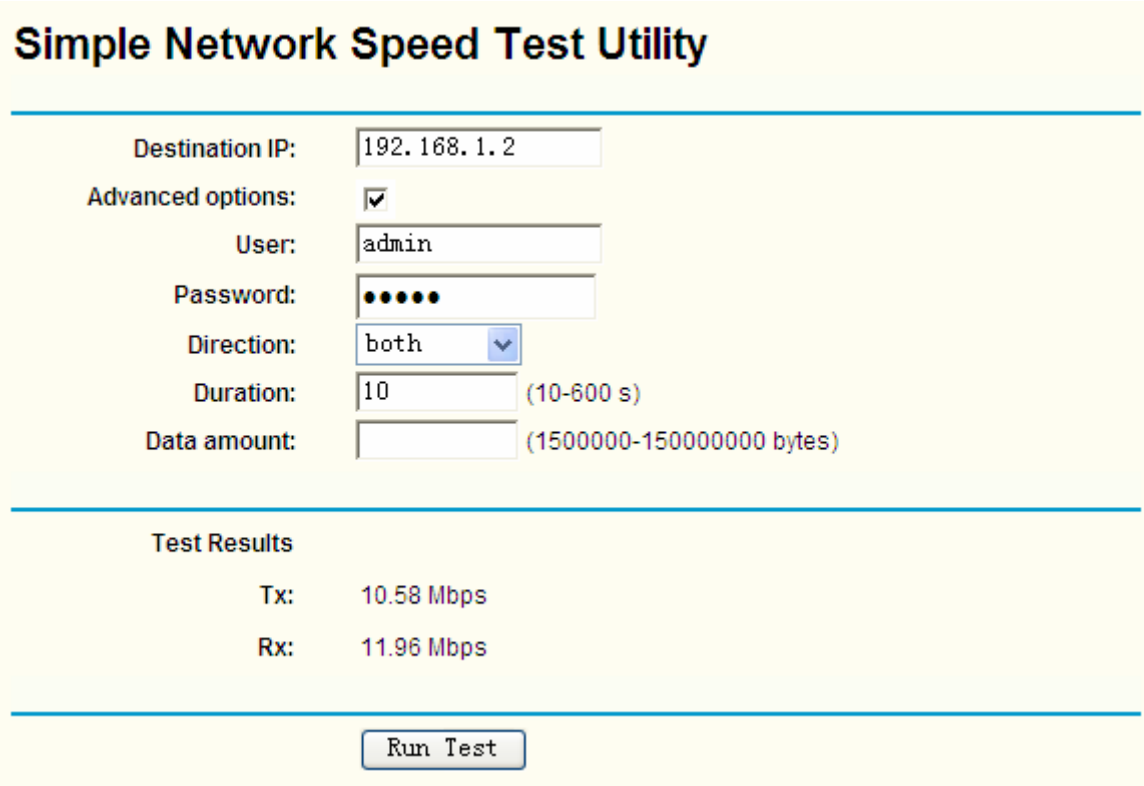


Figure 5-29 Speed Test

- **Destination IP**: The Remote device's IP address.
- **Advanced options**: This is switch to show advanced test options which are used only for precise estimation.
- **User**: Administrator password of the remote device. It should be filled correctly if you want to get a precise estimation. Otherwise, keep if clean.

Note:

If either User or Password is incorrect, we will take a basic test instead. In other words, none of the advance options you set will take effect.

- **Direction**: There are 3 options available for the traffic direction while estimating the throughput.
  - **transmit**-Estimate the outgoing throughput (TX).
  - **receive**- Estimate the ingoing throughput (RX).
  - **both**- Estimate the incoming (RX) first and then the outgoing (TX) afterwards.
- **Duration**: The value you specify here indicate how much time the test should last.
- **Data amount**: The maximal data amount to be sent out during the whole test.

Note:

If both Duration and Data amount are specified, the test will stop after any of them is met.

Be sure to click the **Run Test** button to start a new test after you filled enough information. You can also stop a running test by click Stop Test button at any time.

5.9.6 Reboot

This page allows you to reboot the AP on the screen below (Figure 5-30).

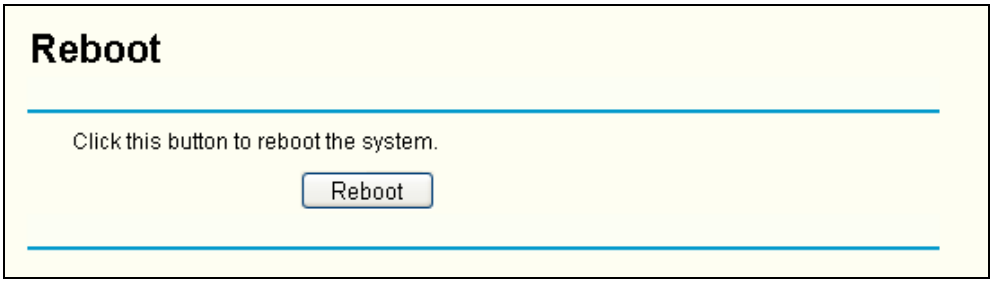


Figure 5-30 Reboot the AP

Click **Reboot** to reboot the AP.

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

- Change LAN IP Address. (System will reboot automatically)
- Upgrade the firmware of the AP (system will reboot automatically).
- Restore the AP's settings to factory default (system will reboot automatically).
- DHCP service function.
- Static address assignment of DHCP server.

5.9.7 Password

This page allows you to change the factory default user name and password of the AP on the screen below (Figure 5-31).

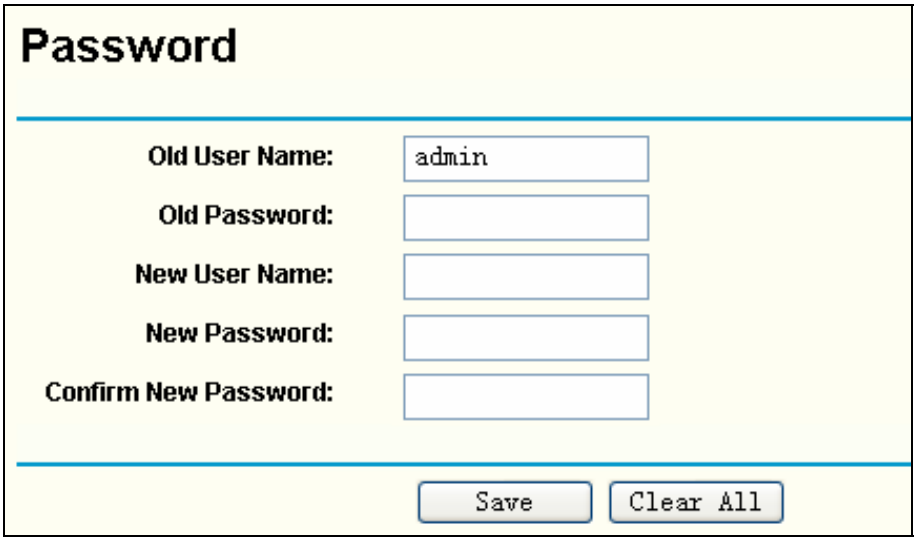


Figure 5-31 Password

It is strongly recommended that you change the factory default user name and password of the AP to more secure ones because they control access to the AP's web-based utility. All users who try to access the AP's web-based utility or Quick Setup will be prompted for the AP's user name and password.

☞ **Note:**

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

Click **Save** when finished.

Click **Clear All** to clear all.

5.9.8 Syslog

This page allows you to query the Logs of the AP on the screen below Figure 5-32).

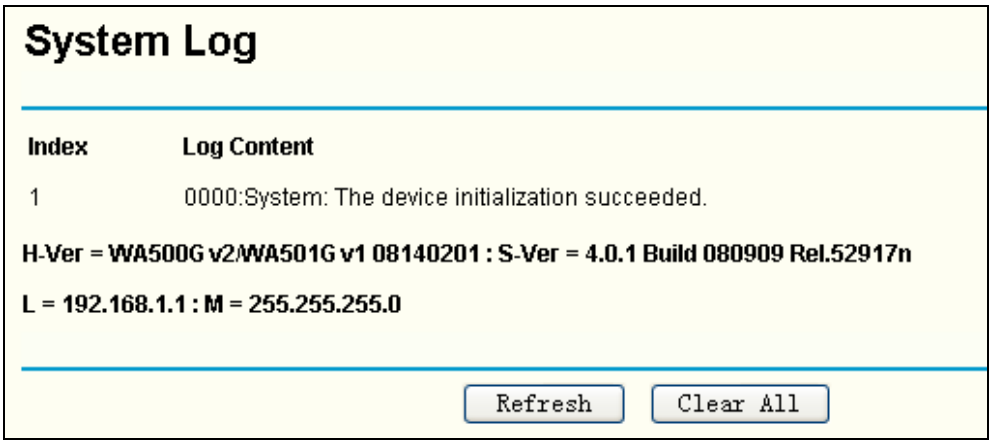


Figure 5-32 System Log

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

Click **Refresh** to refresh the logs.

Click **Clear ALL** to clear all the logs.

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”.

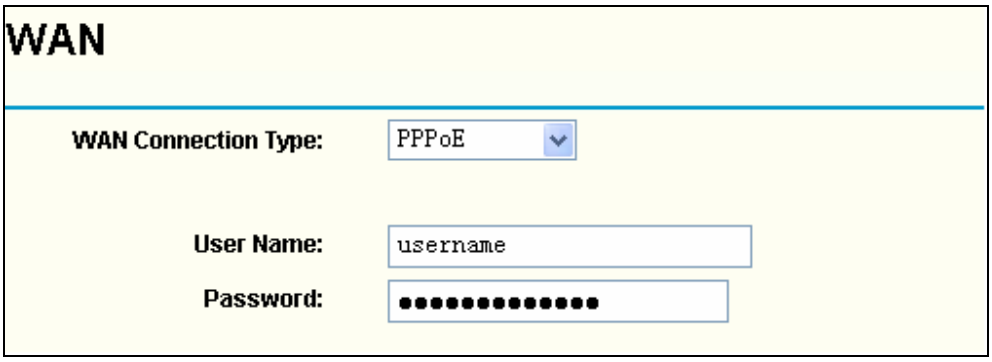


Figure A-1 PPPoE Connection Type

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.

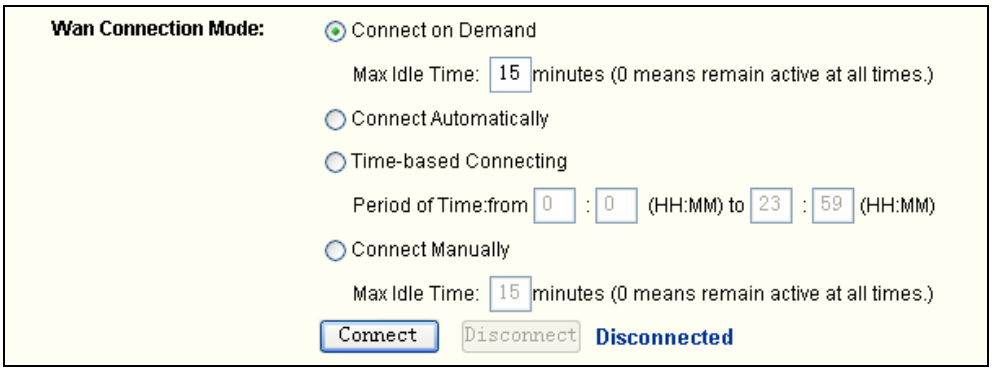


Figure A-2 PPPoE Connection Mode

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.

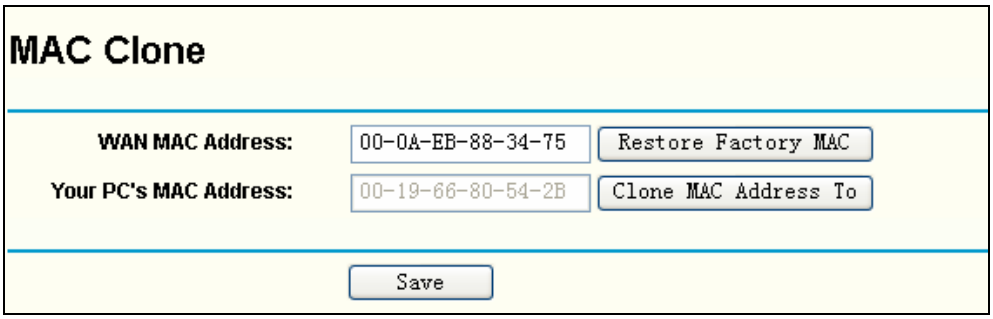


Figure A-3 MAC Clone

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".

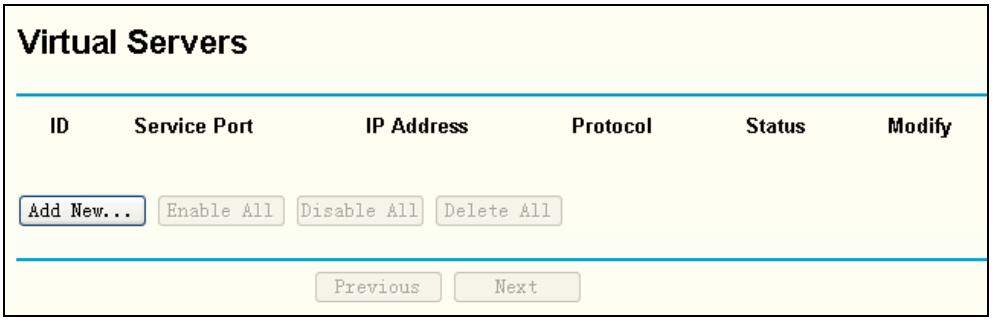
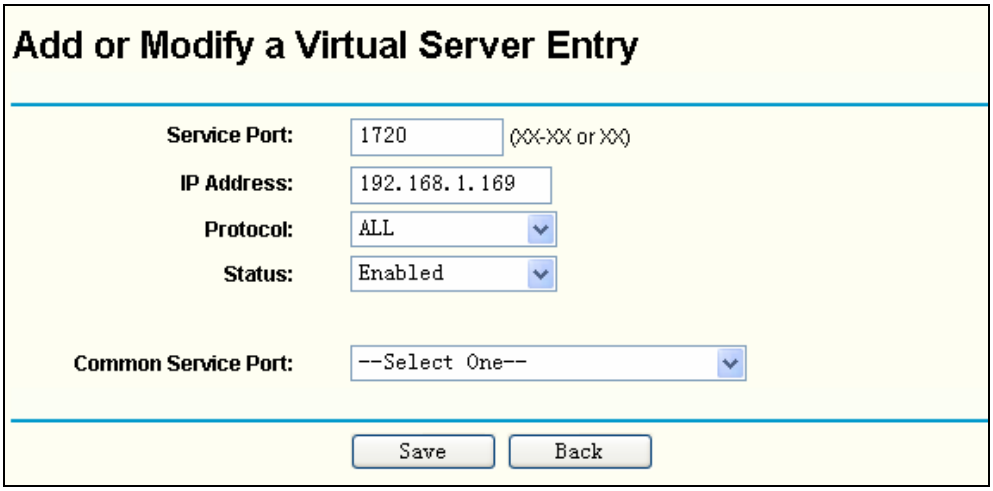


Figure A-4 Virtual Servers



A-5 Add or Modify a Virtual server Entry

Note:

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

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

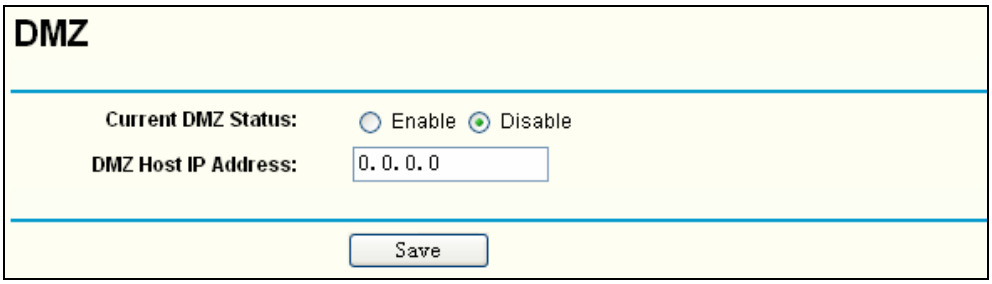


Figure A-6 DMZ

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

1) Because the Web Server port 80 will interfere with the Web management port 80 on the router, you must change the Web management port number to avoid interference.

2) To change the Web management port number: Login to the router, click the “Security” menu on the left of your browser, and click "Remote Management" submenu. On the "Remote Management" page, type a port number except 80, such as 88, into the "Web Management Port" field. Click “Save” and reboot the router.

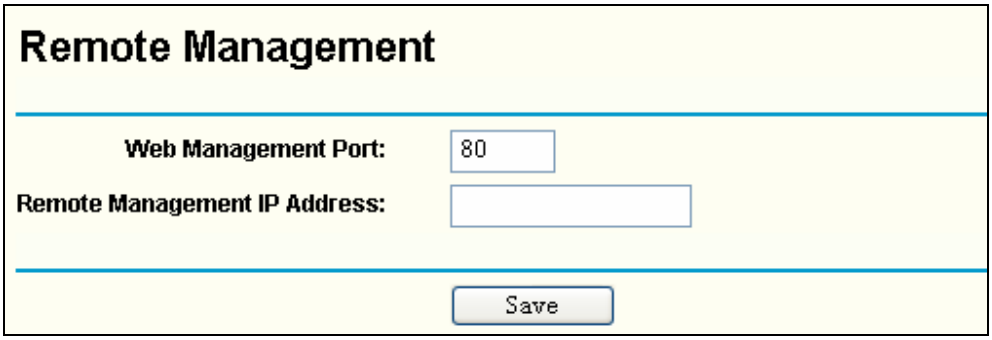


Figure A-7 Remote Management

Note:

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

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

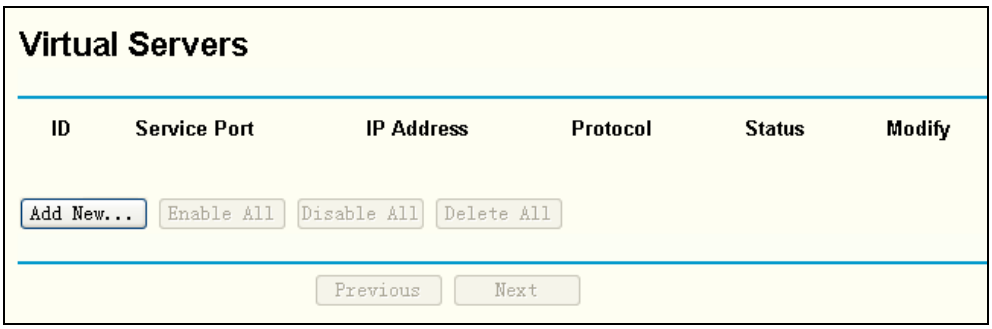
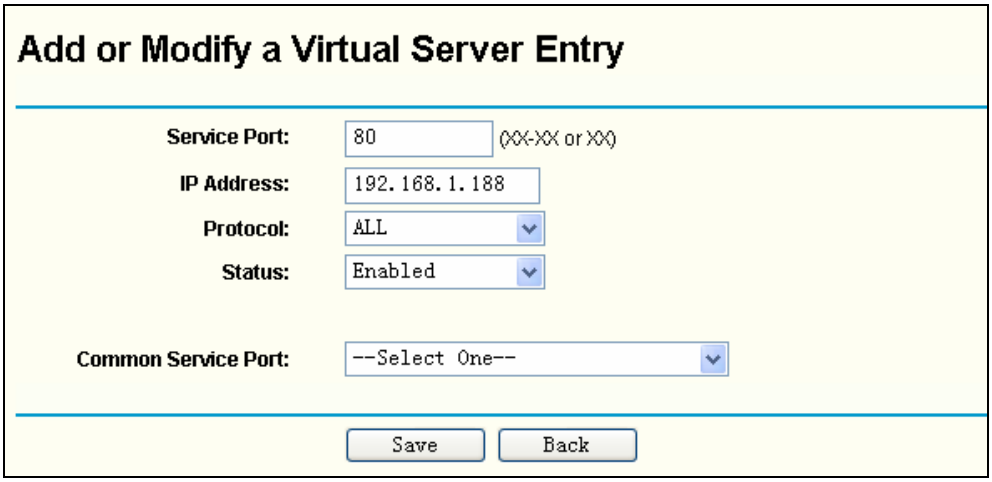


Figure A-8 Virtual Servers



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 PCs

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

1. Configure TCP/IP component

1) On the Windows taskbar, click the **Start** button, 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.

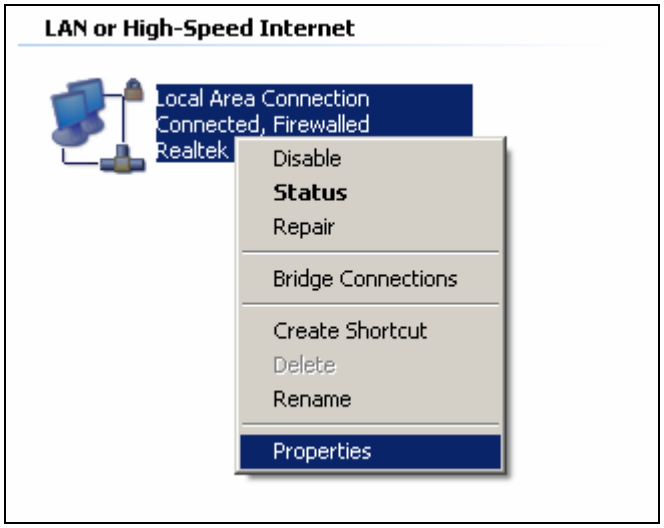


Figure 0-1

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

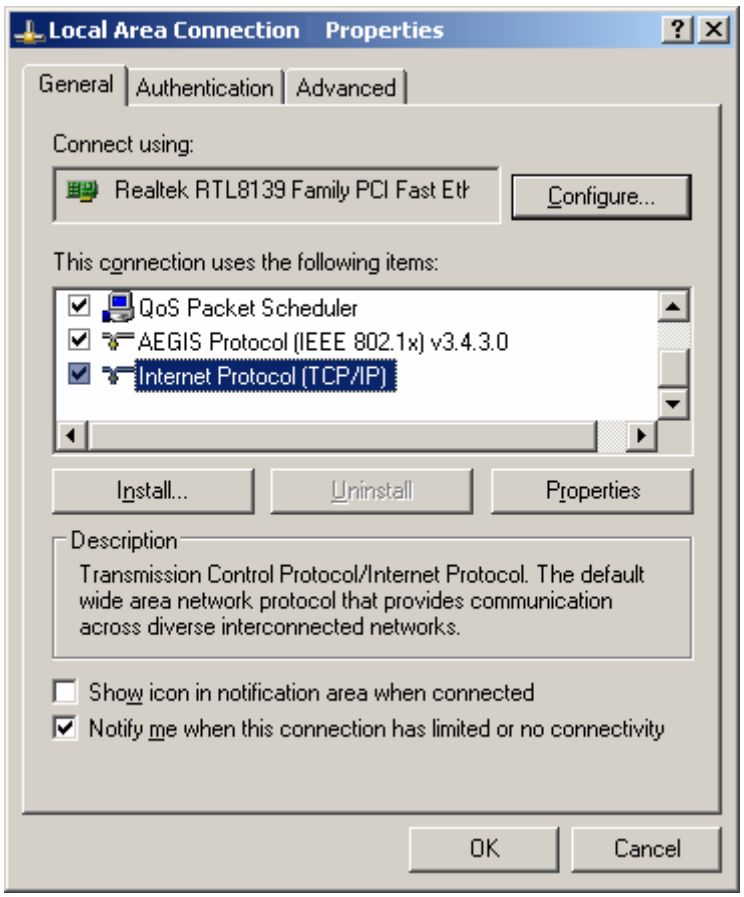


Figure 0-2

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

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

- **Setting IP address automatically**

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

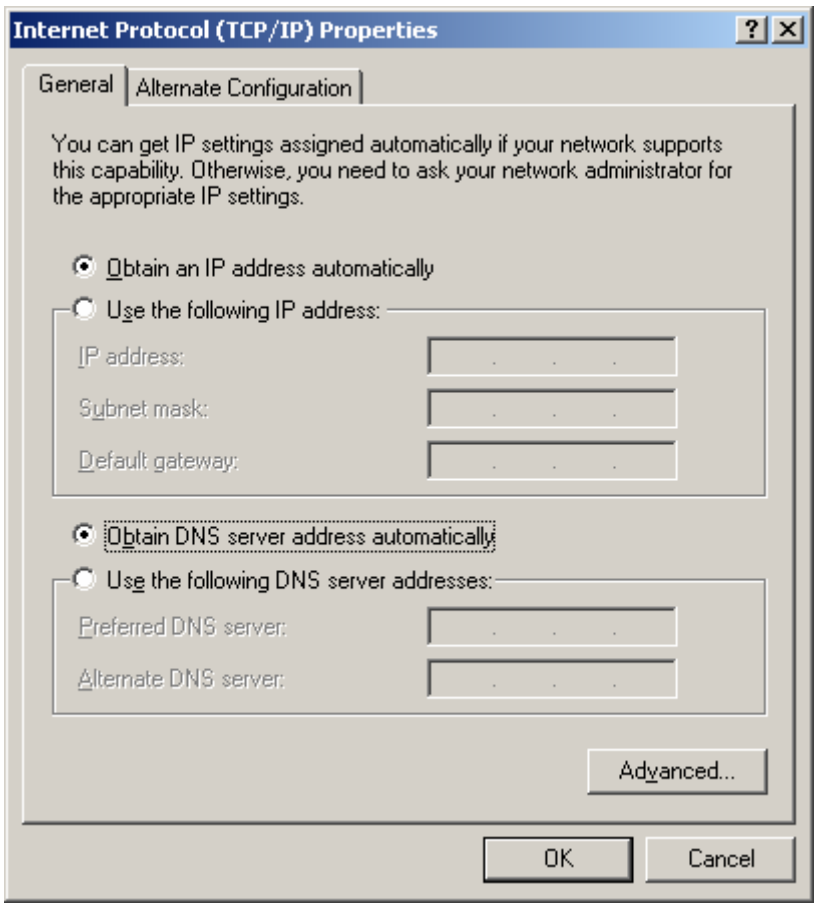


Figure 0-3

☞**Note:** For Windows 98 OS or before, the PC and router may need to be restarted.

➢ **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, specify the **IP address** as 192.168.1.x (x is from 2 to 254), and the **Subnet mask** as 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**. In the **Preferred DNS Server** field you can enter the same value as the **Default gateway** or type the local DNS server IP address.

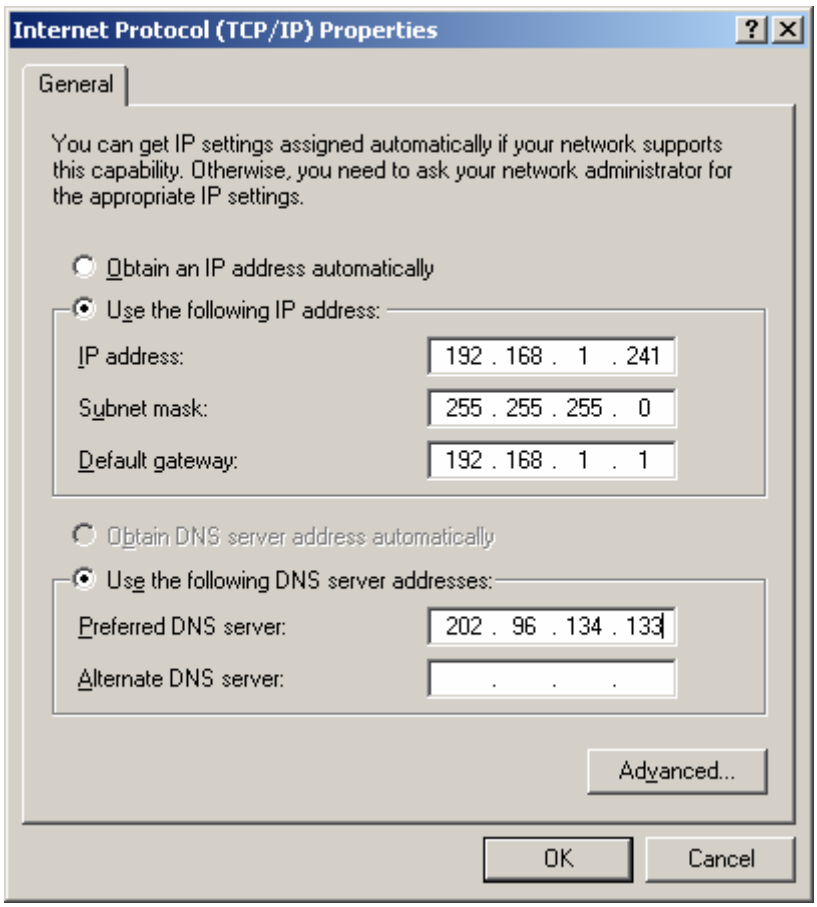


Figure 0-4

Now:

Click **OK** to keep your settings.

Appendix C: Specifications

General	
Standards and Protocols	IEEE 802.3, 802.3u, 802.11b and 802.11g, TCP/IP, DHCP
Safety & Emission	FCC、CE
Ports	One 10/100M Auto-Negotiation LAN RJ45 port, supporting passive PoE
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)
Wireless	
Wireless Data Rates	54/48/36/24/18/12/9/6Mbps or 11/5.5/3/2/1Mbps
Wireless Encryptions	64/128/152-bit WEP, WPA/WPA2, WPA-PSK/WPA2-PSK
Physical and Environment	
Working Temperature	-10℃~40℃
Working Humidity	10% ~ 90% RH, Non-condensing
Storage Temperature	-40℃~70℃(-40℉~158℉)
Storage Humidity	5% ~ 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 -** is a trademark of the Wi-Fi Alliance, founded in 1999 as Wireless Internet Compatibility Alliance (WICA), comprising more than 300 companies, whose products are certified by the Wi-Fi Alliance, based on the IEEE 802.11 standards (also called Wireless LAN (WLAN) and Wi-Fi). This certification warrants interoperability between different wireless devices.
- **WISP - Wireless Internet Service Providers** (**WISPs**) are Internet service providers with networks built around wireless networking. The technology used ranges from commonplace Wi-Fi mesh networking or proprietary equipment designed to operate over open 900MHz, 2.4GHz, 4.9, 5.2, 5.4, and 5.8GHz bands or licensed frequencies in the UHF or MMDS bands.
- **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