

TP-LINK[®]

User Guide

TL-WA5210G

2.4GHz High Power Wireless Outdoor CPE



COPYRIGHT & TRADEMARKS

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

No part of the specifications may be reproduced in any form or by any means or used to make any derivative such as translation, transformation, or adaptation without permission from TP-LINK TECHNOLOGIES CO., LTD. Copyright © 2010 TP-LINK TECHNOLOGIES CO., LTD.

All rights reserved.

<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.

Note: The manufacturer is not responsible for any radio or tv interference caused by unauthorized modifications to this equipment. Such modifications 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 30 cm from all persons and must not be co-located or operating in conjunction with any other antenna or transmitter."

IMPORTANT Statement

This device is equipped with a high gain directional dual-Polarized directional antenna and designed with high output power, only long distance point-to-point using is allowed to comply with FCC Rules. The antenna's beam width is "Horizontal: 60° Vertical: 30°", which can not be used for wireless network coverage. Anyone who privately replaces the antenna with an omni-directional antenna for point-to-multiply point using is illegal!

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: **2.4GHz High Power Wireless Outdoor CPE**

Model No.: **TL-WA5210G**

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

EN 61000-3-2:2006

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

EN60950-1:2009

EN62311:2008

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

Person is responsible for marking this declaration:



Yang Hongliang

Product Manager 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 | 1 |
| Chapter 1 Product Overview | 2 |
| 1.1 Overview of the Product..... | 2 |
| 1.2 Features | 2 |
| 1.3 Conventions..... | 3 |
| Chapter 2 Hardware Installation | 4 |
| 2.1 LED Explanation | 4 |
| 2.2 Interfaces and button | 4 |
| 2.3 System Requirements..... | 5 |
| 2.4 Environment Requirements..... | 5 |
| 2.5 Connecting the Device | 5 |
| Chapter 3 Quick Installation Guide | 7 |
| 3.1 Configure the Device..... | 7 |
| 3.2 Quick Setup | 8 |
| Chapter 4 AP Client Router & AP Router Operation Mode | 13 |
| 4.1 Login | 13 |
| 4.2 Status | 13 |
| 4.3 Quick Setup..... | 15 |
| 4.4 Operation Mode | 15 |
| 4.5 Network | 15 |
| 4.5.1 LAN..... | 16 |
| 4.5.2 WAN..... | 16 |
| 4.5.3 MAC Clone..... | 21 |
| 4.6 Wireless..... | 21 |
| 4.6.1 Basic Settings..... | 22 |
| 4.6.2 Wireless Mode..... | 23 |
| 4.6.3 Security Settings..... | 24 |
| 4.6.4 Wireless Statistics | 27 |
| 4.6.5 Distance Setting | 27 |
| 4.6.6 Antenna Alignment | 28 |
| 4.6.7 Throughput Monitor | 28 |
| 4.7 DHCP | 29 |
| 4.7.1 DHCP Settings | 30 |
| 4.7.2 DHCP Clients List..... | 31 |
| 4.7.3 Address Reservation | 31 |
| 4.8 Wireless settings..... | 32 |

| | | |
|------------------|-------------------------------|-----------|
| 4.9 | Forwarding..... | 33 |
| 4.9.1 | Virtual Servers..... | 34 |
| 4.9.2 | Port Triggering..... | 35 |
| 4.9.3 | DMZ..... | 37 |
| 4.9.4 | UPnP..... | 38 |
| 4.10 | Security..... | 38 |
| 4.10.1 | Firewall..... | 39 |
| 4.10.2 | IP Address Filtering..... | 40 |
| 4.10.3 | Domain Filtering..... | 41 |
| 4.10.4 | MAC Address Filtering..... | 43 |
| 4.10.5 | Remote Management..... | 44 |
| 4.10.6 | Advanced Security..... | 45 |
| 4.11 | Static Routing..... | 47 |
| 4.12 | IP & MAC Binding..... | 48 |
| 4.12.1 | Binding Setting..... | 48 |
| 4.12.2 | ARP List..... | 49 |
| 4.13 | Dynamic DNS..... | 50 |
| 4.13.1 | Dyndns.org DDNS..... | 50 |
| 4.13.2 | Oray.net DDNS..... | 51 |
| 4.13.3 | Comexe.cn DDNS..... | 52 |
| 4.14 | SNMP..... | 53 |
| 4.14.1 | Community Setting..... | 53 |
| 4.14.2 | SNMP System Setting..... | 54 |
| 4.15 | System Tools..... | 55 |
| 4.15.1 | Time..... | 55 |
| 4.15.2 | Firmware..... | 56 |
| 4.15.3 | Factory Defaults..... | 57 |
| 4.15.4 | Backup & Restore..... | 58 |
| 4.15.5 | Ping Watch Dog..... | 58 |
| 4.15.6 | Speed Test..... | 59 |
| 4.15.7 | Reboot..... | 60 |
| 4.15.8 | Password..... | 61 |
| 4.15.9 | Syslog..... | 61 |
| 4.15.10 | Statistics..... | 62 |
| Chapter 5 | AP Operation Mode..... | 64 |
| 5.1 | Login..... | 64 |
| 5.2 | Status..... | 64 |
| 5.3 | Quick Setup..... | 65 |

| | | |
|--|---------------------------|-----------|
| 5.4 | Operation Mode | 66 |
| 5.5 | Network | 66 |
| 5.6 | Wireless..... | 67 |
| 5.6.1 | Basic Settings..... | 67 |
| 5.6.2 | Wireless Mode..... | 69 |
| 5.6.3 | Security Settings..... | 71 |
| 5.6.4 | Wireless Statistics | 73 |
| 5.6.5 | Distance Setting | 73 |
| 5.6.6 | Antenna Alignment | 74 |
| 5.6.7 | Throughput Monitor | 75 |
| 5.7 | DHCP | 75 |
| 5.7.1 | DHCP Settings | 76 |
| 5.7.2 | DHCP Clients List..... | 77 |
| 5.7.3 | Address Reservation | 77 |
| 5.8 | Wireless settings..... | 78 |
| 5.9 | SNMP | 79 |
| 5.9.1 | Community Setting | 80 |
| 5.9.2 | SNMP System Setting | 81 |
| 5.10 | System Tools..... | 81 |
| 5.10.1 | Firmware | 82 |
| 5.10.2 | Factory Defaults | 82 |
| 5.10.3 | Backup & Restore..... | 83 |
| 5.10.4 | Ping Watch Dog..... | 83 |
| 5.10.5 | Speed Test..... | 84 |
| 5.10.6 | Reboot | 85 |
| 5.10.7 | Password | 86 |
| 5.10.8 | Syslog..... | 86 |
| Appendix A: FAQ..... | | 88 |
| Appendix B: Configuring the PC..... | | 92 |
| Appendix C: Specifications..... | | 96 |
| Appendix D: Glossary | | 97 |

Package Contents

The following items should be found in your package:

- One TL-WA5210G 2.4GHz High Power Wireless Outdoor CPE
- One power Adapter for TL-WA5210G 2.4GHz High Power Wireless Outdoor CPE
- One Power Injector
- Mounting Kits
- Quick Installation Guide
- One Resource CD for TL-WA5210G 2.4GHz High Power Wireless Outdoor CPE, 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-WA5210G 2.4GHz High Power Wireless Outdoor CPE**

1.1 Overview of the Product

The TL-WA5210G 2.4GHz High Power Wireless Outdoor CPE is dedicated to WISP CPE and long distance point to point wireless connection solutions. For WISP CPE solution, the TL-WA5210G is in AP Client Router Mode, it can access the Internet via the Wireless form WISP. For long distance point to point connection solutions, using two of the TL-WA5210G in Bridge (or one AP Router, the other AP Client; or repeater) modes, it can connect two LAN through the long distance wireless transmission.

In order to fulfill the requirement of solutions above, the TL-WA5210G is designed with outdoor weatherproof, 12dBi Dual-Polarized Directional Antenna, High Output power, and multiple working mode.

With the most attentive wireless security, the TL-WA5210G 2.4GHz High Power Wireless Outdoor CPE 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-WA5210G 2.4GHz High Power Wireless Outdoor CPE 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.

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-WA5210G, or device mentioned in this User guide stands for TL-WA5210G 2.4GHz High Power Wireless Outdoor CPE 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 LED Explanation

TL-WA5210G consists of several LED indicators, which is designed to indicate connections and wireless signal.

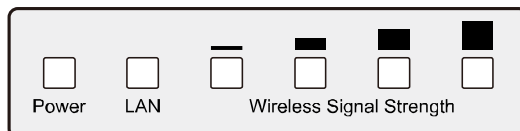


Figure 2-1 Front Panel sketch

View from left to right.

| Name | Status | Indication | |
|--------------------------|----------|--|-------------------------|
| Power | Off | No Power | |
| | On | Power on | |
| 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 | |
| Wireless Signal Strength | Off | There is no remote wireless signal | Client or Repeater mode |
| | On | Indicates the wireless signal strength of a remote AP | |

Table 2-1

Note:

For **Wireless Signal Strength** LEDs:

- In **AP or Bridge** mode, all the four LEDs will light up.
- In **Client or Repeater** mode, the corresponding LED(s) will light up when the RSSI value (wireless signal strength value) reaches the RSSI Threshold. The value of RSSI Threshold can be set on Wireless Advanced Settings page as shown in Figure 4-23.

For example, if the RSSI value is 30, the RSSI Threshold of the four LED are 15, 25, 35, 45 respectively, and then the LEDs whose RSSI Threshold are 15 and 25 will light up.

2.2 Interfaces and button

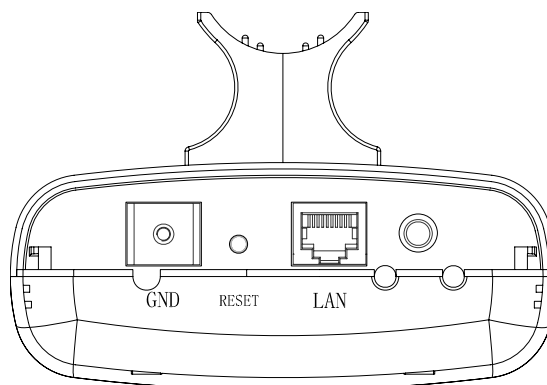



Figure 2-2 Rear Panel sketch

View from left to right, the parts are explained below.

- : This is where you can connect an outside antenna. For this AP, the antenna is built inside, and usually there is not necessary to connect an outside one.
- **LAN:** This port is used to connect to the POE port of the provided Power Injector.
- **RESET:**
There are two 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 **RESET** button for at least 5 seconds, and then the AP reboots after the LED at the rightmost in Figure 2-1 flashes.

 **Note:**

Ensure the AP is powered on before it restarts completely.

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).

2.4 Environment Requirements

- Operating temperature: -30°C~70°C
- Operating Humidity: 10%~90% RH, Non-condensing

2.5 Connecting the Device

To establish an infrastructure network in AP Client Router mode as Figure 2-3, 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 AP to get a best signal.
5. Power on the AP and then you can configure the AP on the web-based page on your computer.



Figure 2-3

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-WA5210G is 192.168.1.254. 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 1 to 253), Subnet Mask is 255.255.255.0, and Gateway is 192.168.1.254 (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 192.168.1.254*, 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.

```
Pinging 192.168.1.254 with 32 bytes of data:

Reply from 192.168.1.254: bytes=32 time=1ms TTL=64
Reply from 192.168.1.254: bytes=32 time<1ms TTL=64
Reply from 192.168.1.254: bytes=32 time<1ms TTL=64
Reply from 192.168.1.254: bytes=32 time<1ms TTL=64

Ping statistics for 192.168.1.254:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

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.

```
Pinging 192.168.1.254 with 32 bytes of data: :

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

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 192.168.1.254, your PC's IP address must be within the range of 192.168.1.1 ~ 192.168.1.253, the gateway must be 192.168.1.254.

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-WA5210G. 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 (192.168.1.254) 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.

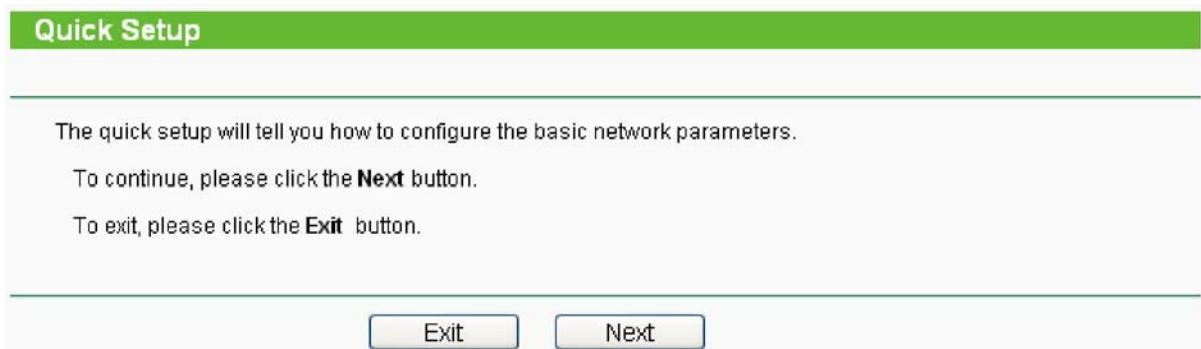


Figure 3-5 Quick Setup

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

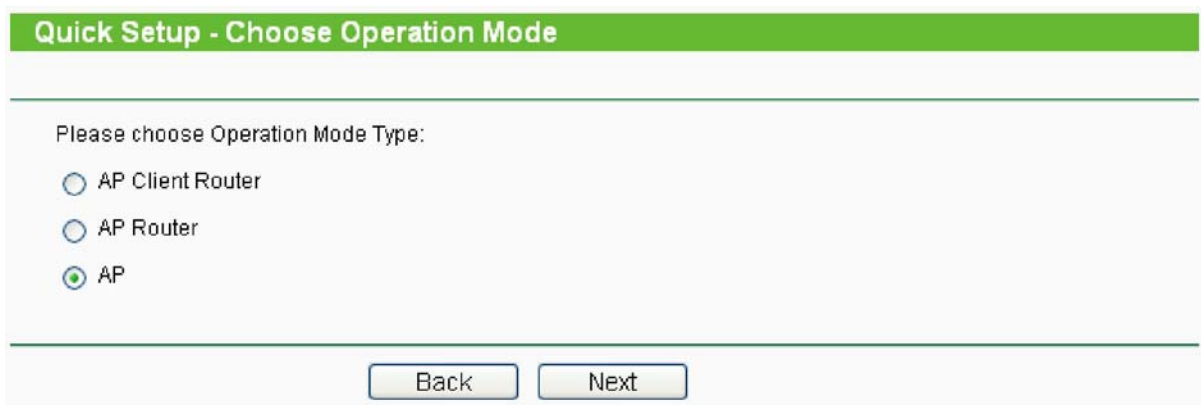


Figure 3-6 Choose Operation mode

Note:

The AP supports three mode operation modes: 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 and AP Mode, it can establish a long distance point to point wireless connection between two LANs. 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** in Figure 3-6, and then **Choose WAN Connection Type** page will appear, shown in Figure 3-7:

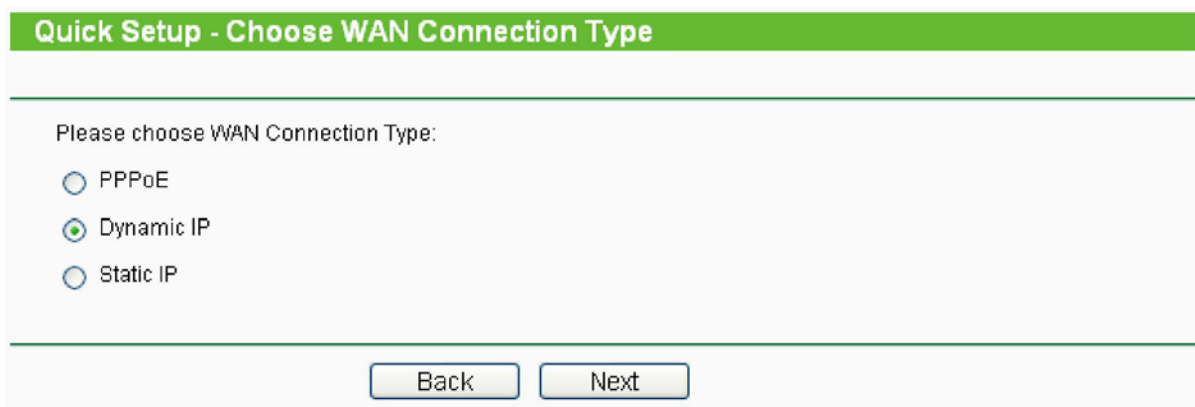


Figure 3-7 Choose WAN Connection Type

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** in Figure 3-7 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_XXXXXX This value is case-sensitive. For example, *TEST* is NOT the same as *test*.
- **Region** - Specifies the region where the wireless function of the AP can be used. Select your region from the drop-down list. The default is United States. If your country or region is not listed, please contact your local government agency for assistance.

Note:

Restricted by local law regulations, version for North America does not have region selection option. The wireless basic settings for this version are shown below.

- **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 settings will take effect after rebooting.

Chapter 4 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 fourteen main menus on the left of the Web-based management page. Submenus will be available after you click one of the main menus. The fourteen main menus are: **Status**, **Quick Setup**, **Operation Mode**, **Network**, **Wireless**, **DHCP**, **Wireless Settings**, **Forwarding**, **Security**, **Static Routing**, **IP & MAC Binding**, **Dynamic DNS**, **SNMP** 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

Selecting **Status** will enable you to view the AP's current status and configuration, all of which is read-only.

Status

Firmware Version: 4.4.0 Build 100120 Rel.52294n
Hardware Version: WA5210G v1 081640EF

LAN

MAC Address: 00-0A-EB-90-00-08
IP Address: 192.168.1.254
Subnet Mask: 255.255.255.0

Wireless

Wireless Radio: Enable
Signal:
SSID: TP-LINK_900008
Channel: 4
Mode: 11Mbps (802.11b)
MAC Address: 00-0A-EB-90-00-09

WAN

MAC Address: 00-0A-EB-90-00-09
IP Address: 0.0.0.0 Dynamic IP
Subnet Mask: 0.0.0.0
Default Gateway: 0.0.0.0 [Obtaining network parameters...](#)
DNS Server: 0.0.0.0, 0.0.0.0

Traffic Statistics

| | Received | Sent |
|-----------------|----------|------|
| Bytes: | 0 | 0 |
| Packets: | 0 | 0 |

System Up Time: 0 day(s) 00:16:13

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**, and **Wireless MAC 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

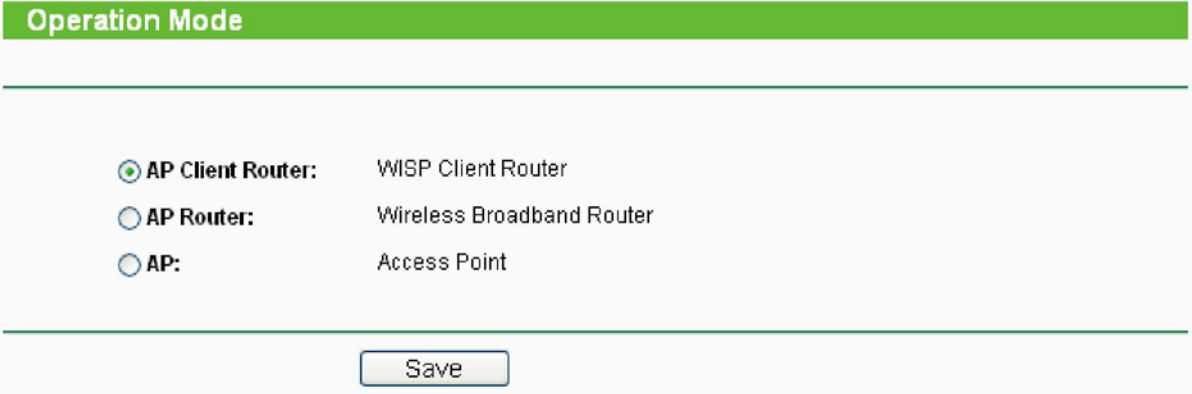
The total up time of the router since it was powered on or reset.

4.3 Quick Setup

Please refer to Section [3.2: "Quick Setup"](#).

4.4 Operation Mode

Selecting **Operation Mode** will allow you to choose the operation mode for the AP. The AP supports three operation mode types, **AP Client Router**, **AP Router** and **AP**. Please select the one you want as shown in Figure 4-2. Click **Save** to save your choice.



| Operation Mode | |
|---|---------------------------|
| <input checked="" type="radio"/> AP Client Router: | WISP Client Router |
| <input type="radio"/> AP Router: | Wireless Broadband Router |
| <input type="radio"/> AP: | Access Point |

Figure 4-2 Operation Mode

- **AP Client Router** - In this mode, the device enables user to access 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 can establish a long distance connection between two LANs in different segments. Because the data transmit between different segments need Router's IP Address Translation.
- **AP** - In this mode, the device can establish a long distance connection between two LANs in same segments.

4.5 Network

The **Network** option allows you to customize your local network manually by changing the default settings of the AP.

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.



Figure 4-3 the Network menu

4.5.1 LAN

Selecting **Network > LAN** will enable you to configure the IP parameters of LAN port on this page.

A screenshot of the LAN configuration page. The page has a green header with the word "LAN". Below the header, there are three rows of configuration fields. The first row is "MAC Address:" with the value "00-0A-EB-90-00-08". The second row is "IP Address:" with a text box containing "192.168.1.254". The third row is "Subnet Mask:" with a text box containing "255.255.255.0". At the bottom of the page, there is a "Save" button.

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: 192.168.1.254).
- **Subnet Mask** - An address code that determines the size of the network. Normally use 255.255.255.0 as the subnet mask.

Note:

- 1) If you change the IP Address of LAN, you must use the new IP Address to login the Router.
- 2) 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.
- 3) 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

Selecting **Network > WAN** will enable you to configure the IP parameters of WAN port 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 shown in Figure 4-5.

WAN

WAN Connection Type: Dynamic IP ▾

Host Name:

IP Address: 0.0.0.0

Subnet Mask: 0.0.0.0

Default Gateway: 0.0.0.0

Obtaining network parameters...

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

Use These DNS Servers

Primary DNS: 0.0.0.0

Secondary DNS: 0.0.0.0 (Optional)

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

Figure 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 as shown in Figure 4-6.

WAN Connection Type: ▼

IP Address:

Subnet Mask:

Default Gateway: (Optional)

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

Primary DNS: (Optional)

Secondary DNS: (Optional)

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 as shown in Figure 4-7.

WAN

WAN Connection Type: PPPoE ▼

User Name: username

Password: *****

WAN Connection Mode:

Connect on Demand
 Max Idle Time: 15 minutes (0 means remaining active all the time.)

Connect Automatically

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

Connect Manually
 Max Idle Time: 15 minutes (0 means remaining active all the time.)

Connect
Disconnect
Disconnected

Save
Advanced

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.

MTU Size (in bytes): (The default is 1480, do not change unless necessary.)

Service Name:

AC Name:

Use IP address specified by ISP

ISP Specified IP Address:

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

Use the following DNS Servers

Primary DNS:

Secondary DNS: (Optional)

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

MAC Clone allows you to clone the MAC address of the managing PC's adapter to the WAN port. This is because some ISPs require that you register the MAC address of your adapter. Usually, you do not need to change anything here.

Selecting **Network > MAC Clone** will enable you to configure the MAC address of the WAN port on this page as shown in Figure 4-9.

| MAC Clone | |
|-------------------------------------|--|
| WAN MAC Address: | <input type="text" value="00-0A-EB-90-00-09"/> <input type="button" value="Restore Factory MAC"/> |
| Your PC's MAC Address: | <input type="text" value="00-19-66-CB-45-66"/> <input type="button" value="Clone MAC Address To"/> |
| <input type="button" value="Save"/> | |

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

The **Wireless** option, improving functionality and performance for wireless network, can help you to make the AP an ideal solution for your wireless network.

Here you can create a wireless local area network just through a few settings. Basic Settings is used for the configuration of some basic parameters of the AP. Wireless Mode allows you to select the mode that AP works on. Security Settings provides three different security types to secure your data and thus provide greater security for your wireless network. MAC filtering allows you to control the access of wireless stations to the AP. Wireless Statistics shows you the statistics of current connected Wireless stations. Distance Setting is used to adjust the wireless range in outdoor conditions. Antenna Alignment shows how remote AP's signal strength changes while changing the antenna's direction. Throughput Monitor helps to watch wireless throughput information. Wireless statistics enables you to get detailed information about the current connected wireless stations.

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.

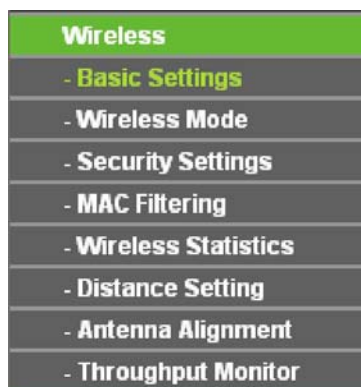


Figure 4-10 Wireless menu

4.6.1 Basic Settings

Selecting **Wireless > Basic Settings** will enable you to configure the basic settings for your wireless network on the screen below (Figure 4-11).

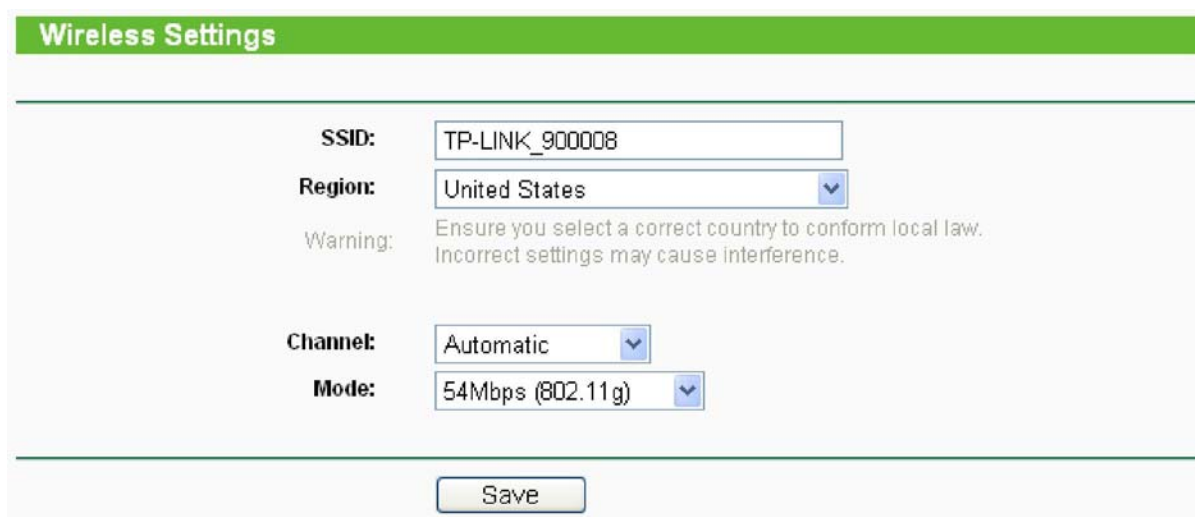
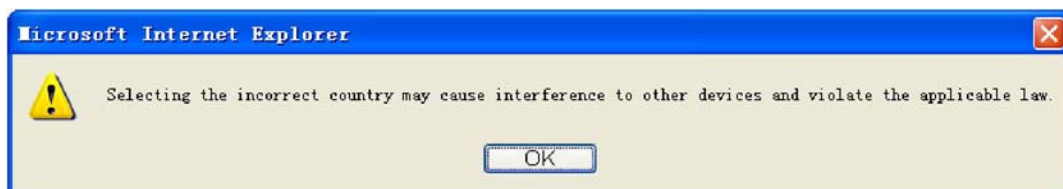
A screenshot of the "Wireless Settings" configuration page. The title "Wireless Settings" is in a green header. Below it, there are four fields: "SSID" with a text input containing "TP-LINK_900008"; "Region" with a dropdown menu showing "United States"; "Channel" with a dropdown menu showing "Automatic"; and "Mode" with a dropdown menu showing "54Mbps (802.11g)". A "Warning:" message is displayed below the Region field: "Ensure you select a correct country to conform local law. Incorrect settings may cause interference." At the bottom of the form is a "Save" button.

Figure 4-11 Wireless Settings in AP Client Router mode

- **SSID** - Enter a string of up to 32 characters. The same Name (SSID) must be assigned to all wireless devices in your network. The default SSID is set to be TP-LINK_XXXXXX (XXXXXX indicates the last unique six characters of each device's MAC address), which can ensure your wireless network security. But it is strongly recommended that you change your networks name (SSID) to a different value. This value is case-sensitive. For example, *TEST* is NOT the same as *test*.
- **Region** - Select your region from the pull-down list. This field 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.

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



Note Dialog

 **Note:**

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

- **Channel** - This field determines which operating frequency will be used. It is not necessary to change the wireless channel unless you notice interference problems with another nearby access point.
- **Mode** - Select the desired wireless mode. The options are:
 - **54Mbps (802.11g)** - Both 802.11g and 802.11b wireless stations can connect to the router.
 - **11Mbps (802.11b)** - Only 802.11b wireless stations can connect to the router.
- **Region** - Specifies the region where the wireless function of the AP can be used. Select your region from the drop-down list. If your country or region is not listed, please contact your local government agency for assistance.

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

Selecting **Wireless > Wireless Mode** will enable you to configure the wireless mode for your device on the page.

- **Access Point** – Pair with another TL-WA5210G in Client Router or Client mode to establish a long distance point to point connection.
 - **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. Pair with another TL-WA5210G in AP or AP Router mode to establish a long distance point to point connection.
 - **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 connect. 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 4-12 and you can choose one to connect to.

| AP List | | | | | | |
|--------------|-------------------|----------------|--------|---------|----------|-------------------------|
| AP Count: 33 | | | | | | |
| ID | BSSID | SSID | Signal | Channel | Security | Choose |
| 1 | 00-1D-0F-01-06-18 | TP-LINK_010618 | 31 dB | 2 | OFF | Connect |
| 2 | 00-19-E0-94-51-F4 | TP-LINK | 20 dB | 1 | ON | Connect |
| 3 | 00-27-19-C4-BC-58 | TP-LINK_C4BC58 | 19 dB | 2 | OFF | Connect |
| 4 | 00-0A-EB-00-01-C1 | TP-LINK_0001C1 | 13 dB | 9 | ON | Connect |
| 5 | 00-27-19-C4-BE-8E | TP-LINK_C4BE8E | 23 dB | 8 | OFF | Connect |
| 6 | 00-0A-EB-CE-1E-1B | TP-LINK_CE1E1B | 27 dB | 5 | OFF | Connect |

Figure 4-12 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 错误! 未找到引用源。 .

 **Note:**

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

4.6.3 Security Settings

Selecting **Wireless > Security Settings** will enable you to configure the security of the wireless network for your device on the page as shown in Figure 4-13.

Disable Security

WEP

Type:

WEP Key Format:

| Key Selected | WEP Key | Key Type |
|---|----------------------|-------------------------------|
| Key 1: <input checked="" type="radio"/> | <input type="text"/> | Disabled <input type="text"/> |
| Key 2: <input type="radio"/> | <input type="text"/> | Disabled <input type="text"/> |
| Key 3: <input type="radio"/> | <input type="text"/> | Disabled <input type="text"/> |
| Key 4: <input type="radio"/> | <input type="text"/> | Disabled <input type="text"/> |

WPA/WPA2

Version:

Encryption:

Radius Server IP:

Radius Port: (1-65535, 0 stands for default port 1812)

Radius Password:

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

WPA-PSK/WPA2-PSK

Version:

Encryption:

PSK Passphrase:

(The Passphrase is between 8 and 63 characters long)

Group Key Update Period: (in second, minimum is 30, 0 means no update, only be valid in AP mode.)

Note: Some security mode can not be selected since it can not be supported by the current wireless mode.

Figure 4-13 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 Wireless Statistics

Selecting **Wireless > Wireless Statistics** will allow you to see the wireless transmission information in the following screen shown in Figure 4-14.

| ID | MAC Address | Current Status | Received Packets | Sent Packets |
|----|-------------------|----------------|------------------|--------------|
| 1 | 00-0A-EB-90-00-09 | AP-DOWN | 0 | 32088 |

Figure 4-14 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
- **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.

4.6.5 Distance Setting

Selecting **Wireless > Distance Setting** will allow you to adjust the wireless range in outdoor conditions as shown in Figure 4-15. 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.

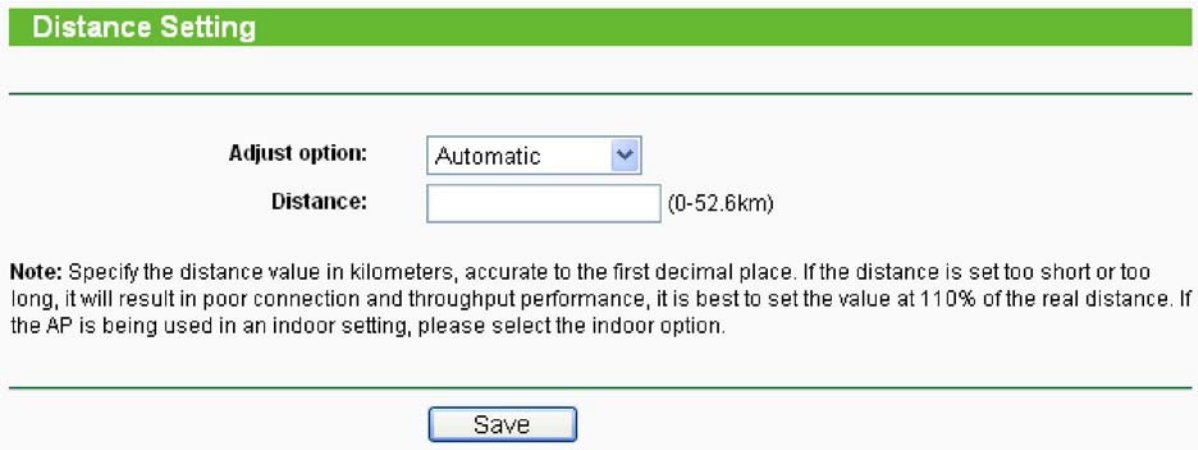


Figure 4-15 Distance Setting

- **Adjust option** - Keep the default setting if the AP is used for outdoor environment. Or you can change the distance manually.
- **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 indoor option.

Click **Save** to keep your settings.

4.6.6 Antenna Alignment

Selecting **Wireless > Antenna Alignment** will allow you to view how remote AP's signal strength changes while changing the antenna's direction.

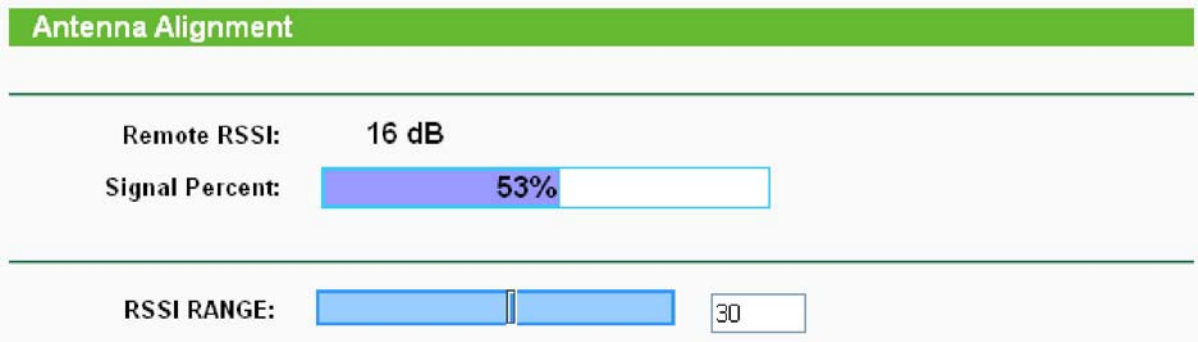


Figure 4-16 Antenna Alignment

- **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.

4.6.7 Throughput Monitor

Selecting **Wireless > Throughput Monitor** will helps to watch wireless throughput information in

the following screen shown in Figure 4-17.

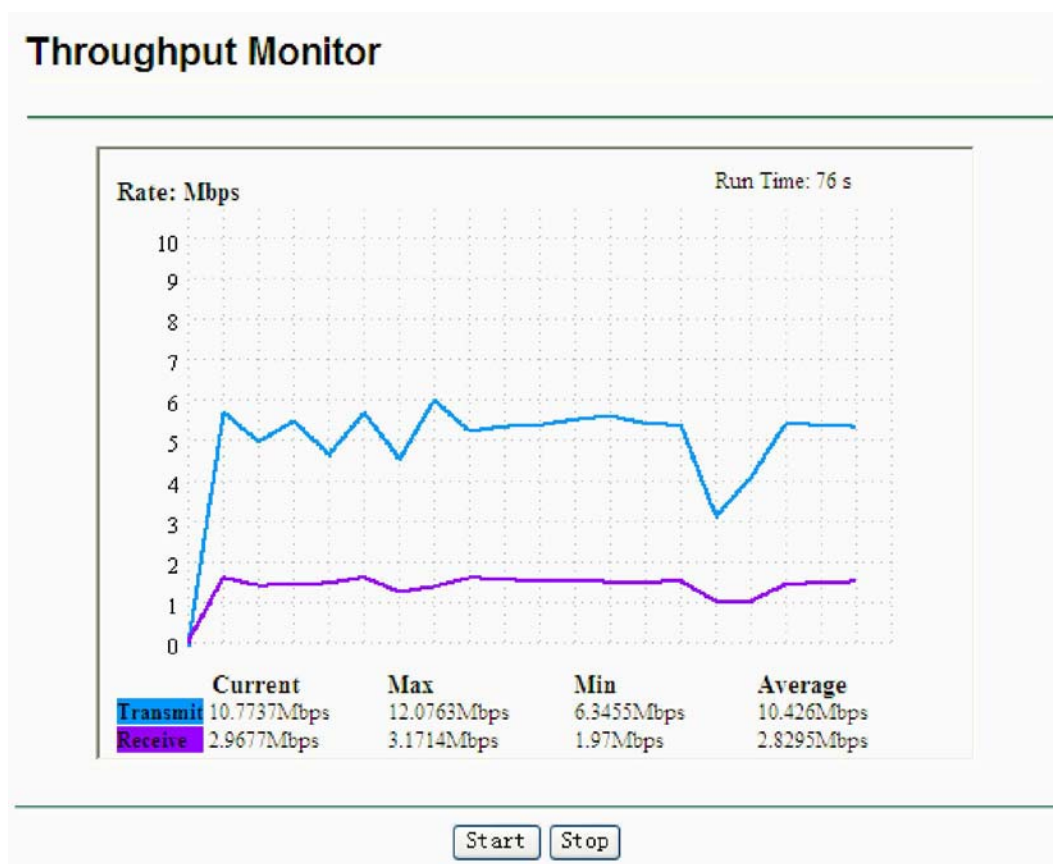


Figure 4-17 Wireless Throughput

- **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.

4.7 DHCP

DHCP stands for Dynamic Host Configuration Protocol. The DHCP Server will automatically assign dynamic IP addresses to the computers on the network. This protocol simplifies network management and allows new wireless devices to receive IP addresses automatically without the need to manually assign new IP addresses.

There are three submenus under the DHCP menu (shown as Figure 4-18): **DHCP Settings**, **DHCP Clients List** and **Address Reservation**. Clicking any of them will enable you to configure the corresponding function. The detailed explanations for each submenu are provided below.

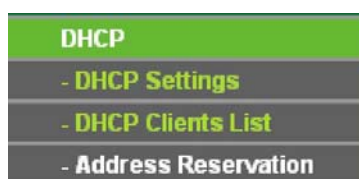


Figure 4-18 The DHCP menu

4.7.1 DHCP Settings

Selecting **DHCP > DHCP Settings** will enable you to set up the AP as a DHCP (Dynamic Host Configuration Protocol) server, which provides the TCP/IP configuration for all the PCs that are connected to the system on the LAN. The DHCP Server can be configured on the page (shown as Figure 4-19).

The screenshot shows the DHCP Settings configuration page. At the top, there is a green header with the text "DHCP Settings". Below the header, the configuration options are as follows:

- DHCP Server:** Radio buttons for "Disable" (selected) and "Enable".
- Start IP Address:** Text box containing "192.168.1.100".
- End IP Address:** Text box containing "192.168.1.199".
- Address Lease Time:** Text box containing "120" with a note "minutes (1~2880 minutes, the default value is 120)".
- Default Gateway:** Text box containing "0.0.0.0" with "(optional)" to its right.
- Default Domain:** Text box with "(optional)" to its right.
- Primary DNS:** Text box containing "0.0.0.0" with "(optional)" to its right.
- Secondary DNS:** Text box containing "0.0.0.0" with "(optional)" to its right.

At the bottom of the form is a "Save" button.

Figure 4-19 DHCP Settings

- **DHCP Server** - Selecting the radio button before **Disable/Enable** will disable/enable the DHCP server on your AP. The default setting is **Disable**. If you disable the Server, you must have another DHCP server within your network or else you must manually configure the computer.
- **Start IP Address** - This field specifies the first address in the IP Address pool. 192.168.1.100 is the default start IP address.
- **End IP Address** - This field specifies the last address in the IP Address pool. 192.168.1.199 is the default end IP address.
- **Address Lease Time** - Enter the amount of time for the PC to connect to the AP with its current assigned dynamic IP address. The time is measured in minutes. After the time is up, the PC will be automatically assigned a new dynamic IP address. The range of the time is 1 ~ 2880 minutes. The default value is 120 minutes.
- **Default Gateway (optional)** - Enter the IP address of the gateway for your LAN. The factory default setting is 0.0.0.0.
- **Default Domain (optional)** - Enter the domain name of the your DHCP server. You can leave the field blank.
- **Primary DNS (optional)** - Enter the DNS IP address provided by your ISP. Consult your ISP if you don't know the DNS value. The factory default setting is 0.0.0.0.
- **Secondary DNS (optional)** - Enter the IP address of another DNS server if your ISP provides two DNS servers. The factory default setting is 0.0.0.0.

Click **Save** to save the changes.

Note:

To use the DHCP server function of the device, you should configure all computers in the LAN as "Obtain an IP Address automatically" mode. This function will not take effect until the device reboots.

4.7.2 DHCP Clients List

Selecting **DHCP > DHCP Clients List** will enable you to view the Client Name, MAC Address, Assigned IP and Lease Time for each DHCP Client attached to the device (Figure 4-20).

| ID | Client Name | MAC Address | Assigned IP | Lease Time |
|----|-------------|-------------------|---------------|------------|
| 1 | microsoft | 00-19-66-CB-45-66 | 192.168.1.100 | 01:56:59 |

Figure 4-20 DHCP Clients List

- **ID** - Here displays the index of the DHCP client.
- **Client Name** - Here displays the name of the DHCP client.
- **MAC Address** - Here displays the MAC address of the DHCP client.
- **Assigned IP** - Here displays the IP address that the AP has allocated to the DHCP client.
- **Lease Time** - Here displays 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

Selecting **DHCP > Address Reservation** will enable you to specify a reserved IP address for a PC on the LAN, so the PC will always obtain the same IP address each time when it accesses the AP. Reserved IP addresses should be assigned to servers that require permanent IP settings. The screen below is used for address reservation (shown in Figure 4-21).

| ID | MAC Address | Reserved IP Address | Status | Modify |
|----|-------------|---------------------|--------|--------|
|----|-------------|---------------------|--------|--------|

Figure 4-21 Address Reservation

- **MAC Address** - Here displays the MAC address of the PC for which you want to reserve an IP address.
- **Reserved IP Address** - Here displays the IP address that the AP is reserved.

- **Status** - Here 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 4-22) 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.



Add or Modify an Address Reservation Entry

MAC Address: 00-0A-EB-00-07-5F

Reserved IP Address: 192.168.1.23

Status: Enabled

Save Back

Figure 4-22 Add or Modify an Address Reservation Entry

To modify A Reserved IP address:

1. Select the reserved address entry to your needs and click **Modify**. If you wish to delete the entry, click **Delete**.
2. Click **Save** to keep your changes.

To delete all Reserved IP addresses:

1. Click **Clear All**.

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

Note:

The changes won't take effect until the device reboots.

4.8 Wireless settings

Selecting **Wireless Settings** will allow you to do some advanced settings for the device in the following screen as shown in Figure 4-23.

Wireless Advanced Settings

Enable WMM

Enable AP Isolation

Disable short preamble

RTS Threshold: (1-2346)

Fragmentation Threshold: (256-2346)

Beacon Interval: (20-1000ms)

Power: Obey Regulatory Power

Antenna Settings:

LED1 LED2 LED3 LED4

Signal LED Thresholds: (0-99dB)

Figure 4-23 Wireless settings

- **Enable WMM** - WMM function can guarantee the packets with high- priority messages being transmitted preferentially. It is strongly recommended enabled.
- **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. 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.
- **Antenna Settings** - The polarization of an antenna.
- **Signal LED Thresholds** - The RSSI thresholds of the signal LEDs.

4.9 Forwarding

There are four submenus under the Forwarding menu (shown in Figure 4-24): **Virtual Servers**, **Port Triggering**, **DMZ** and **UPnP**. Click any of them, and you will be able to configure the corresponding function. The detailed explanations for each submenu are provided below.

Virtual servers 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. Port Triggering is used for some applications that cannot work with a pure NAT router, like Internet games, video conferencing, Internet calling and so on, which

require multiple connections. 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. 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.

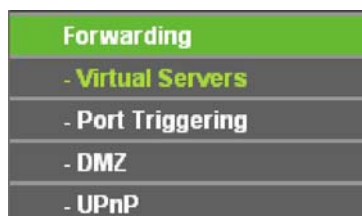


Figure 4-24 The Forwarding menu

4.9.1 Virtual Servers

Selecting **Forwarding > Virtual Servers** will allow you to set up virtual servers on the page as shown in Figure 4-25.

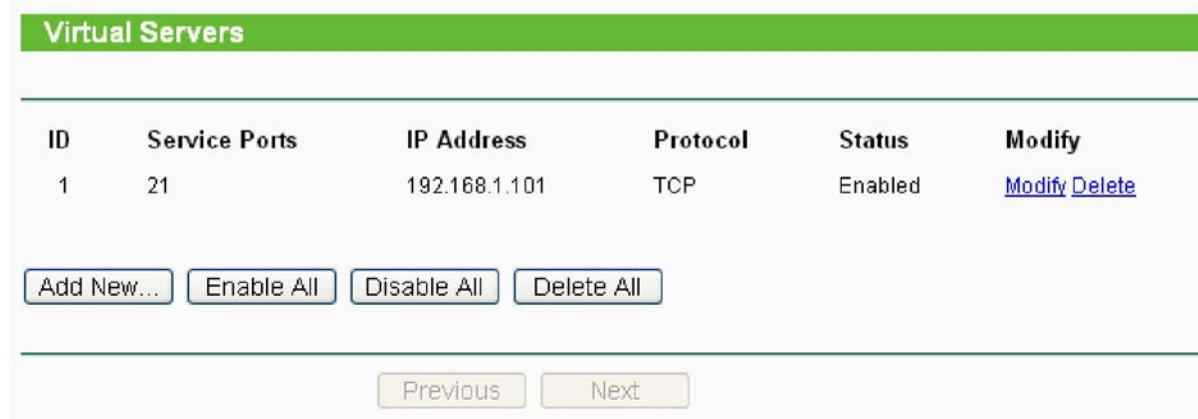


Figure 4-25 Virtual Servers

- **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 4-26)
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.

5. Select the **Enable** option to enable the virtual server.
6. Click the **Save** button.

Figure 4-26 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

Selecting **Forwarding > Port Triggering** will enable you to set up Port Triggering entries on the page as shown in Figure 4-27.

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

Figure 4-27 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 4-28)
2. Select a common application from the **Common Applications** drop-list then the port parameters will be automatically filled in the corresponding field. If the **Common Applications** list does not have the application you want, type the port parameters manually.
3. Select the protocol used for **Trigger Port** and **Incoming Ports** from the corresponding pull-down list.
4. Select the **Enable** option in the **Status** pull-down list..
5. Click the **Save** button to save the new rule.

Figure 4-28 Add or Modify a Triggering Entry

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

Selecting **Forwarding > DMZ** will allow you to set up an DMZ host on the page as shown in Figure 4-29.

Figure 4-29 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 desired to be set as the 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

Selecting **Forwarding > UPnP** will enable you to configure the UPnP function on the page as shown in Figure 4-30:

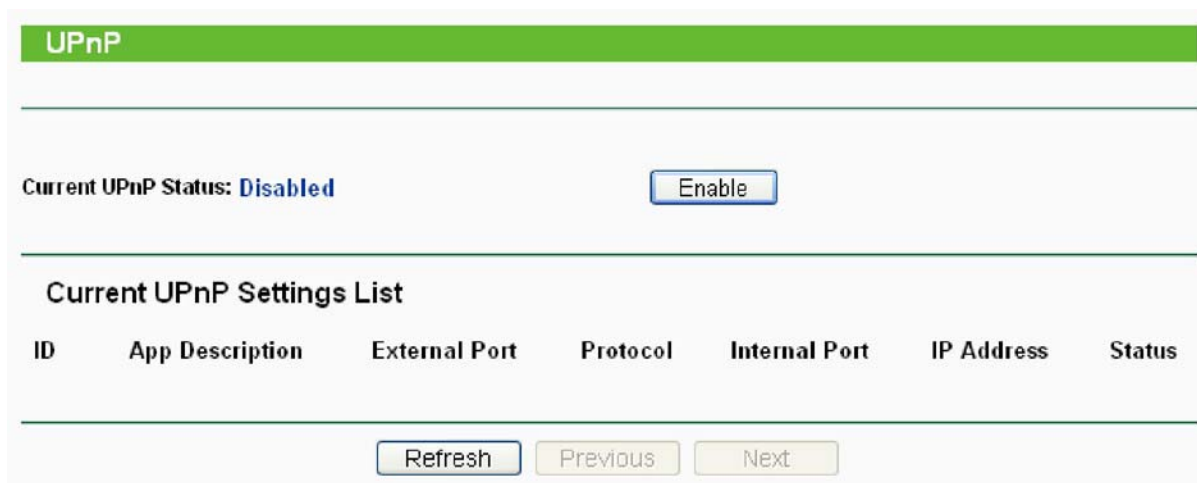


Figure 4-30 UPnP Settings

- **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

Security option is used for secure your network. IP address Filtering allows you to control the Internet Access of specific users on your LAN based on their IP addresses. Domain Filtering allows you to control the access to certain websites on the Internet by specifying their domains or key words. Like the IP Address Filtering, MAC Address Filtering allows you to control access to the Internet of users on your local network based on their MAC Address. Advanced Security helps to protect the router from some attacks. Remote Management allows you to manage your Router

from a remote location via the Internet.

There are six submenus under the Security menu (shown in Figure 4-31): **Firewall**, **IP Address Filtering**, **Domain Filtering**, **MAC Address Filtering**, **Remote Management** and **Advanced Security**. Click any of them, and you will be able to configure the corresponding function. The detailed explanations for each submenu are provided below.



Figure 4-31 The Security menu

4.10.1 Firewall

Selecting **Security > Firewall** will allow you to turn on or off the general firewall switch as shown in Figure 4-32. 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.

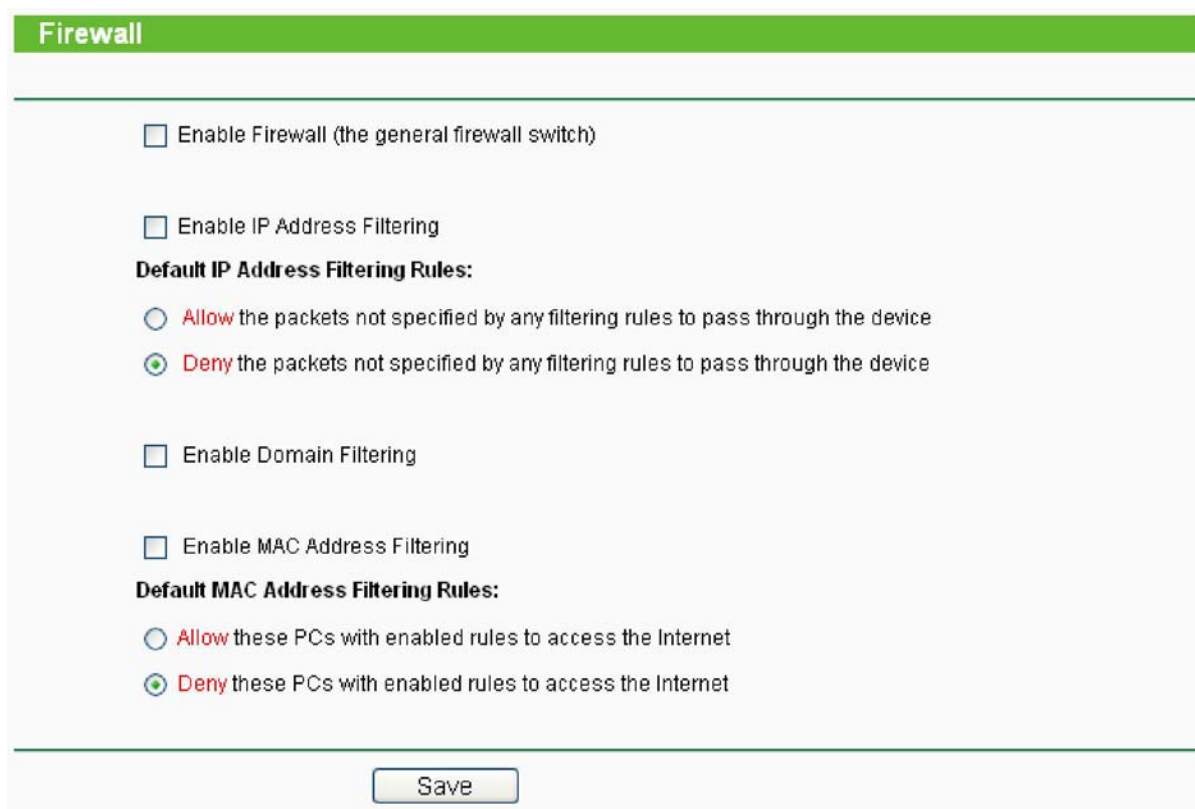


Figure 4-32 Firewall Settings

- **Enable Firewall** - Check this box to enable Firewall.
- **Enable IP Address Filtering** - Check this box to enable 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** - Check this box to enable Domain Filtering.

- **Enable MAC Filtering** - Check this box to enable 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

Selecting **Security > IP Address Filtering** will allow you to configure the IP address filtering entry on the page as shown in Figure 4-33.

Figure 4-33 IP address Filtering

To disable the IP Address Filtering feature, keep the default setting. To set up an IP Address Filtering entry, you should first **Enable** Firewall and **Enable** IP Address Filtering on the Firewall page as shown in Figure 4-32, and then click the **Add New...** button in Figure 4-33. The page "**Add or Modify an IP Address Filtering entry**" will appear shown in Figure 4-34.

Figure 4-34 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 Address | LAN Port | WAN IP Address | 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

Selecting **Security > Domain Filtering** will allows you to configure the domain filtering entry as shown in Figure 4-35.

Domain Filtering

Firewall Settings (You can change them on Firewall page)

Enable Firewall: **Disabled**

Enable Domain Filtering: **Disabled**

| ID | Effective time | Domain Name | Status | Modify |
|----|----------------|-------------|--------|--------|
|----|----------------|-------------|--------|--------|

Figure 4-35 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 as shown in Figure 4-32. To Add a Domain filtering entry, click the **Add New...** button in Figure 4-35. The page "**Add or Modify a Domain Filtering entry**" will appear, shown in Figure 4-36.

Add or Modify an Domain Filtering Entry

Effective Time: -

Domain Name:

Status: ▼

Figure 4-36 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.cn | Enabled | Modify Delete |
| 2 | 0000-2400 | www.aabbcc.com | Enabled | Modify Delete |
| 3 | 0000-2400 | .net | Enabled | Modify Delete |

4.10.4 MAC Address Filtering

Selecting **Security > Domain Filtering** will allows to configure the MAC address filtering entry on the page as shown in Figure 4-37.

MAC Address Filtering

Firewall Settings (You can change them on Firewall page)

Enable Firewall: **Disabled**

Enable MAC Address Filtering: **Disabled**

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

| ID | MAC Address | Description | Status | Modify |
|----|-------------|-------------|--------|--------|
|----|-------------|-------------|--------|--------|

Figure 4-37 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 as shown in Figure 4-32. To Add a MAC Address filtering entry, clicking the **Add New...** button in Figure 4-37. The page "**Add or Modify a MAC Address Filtering entry**" will appear, shown in Figure 4-38:

Add or Modify a MAC Address Filtering Entry

MAC Address:

Description:

Status: Enabled ▼

Save
Back

Figure 4-38 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.

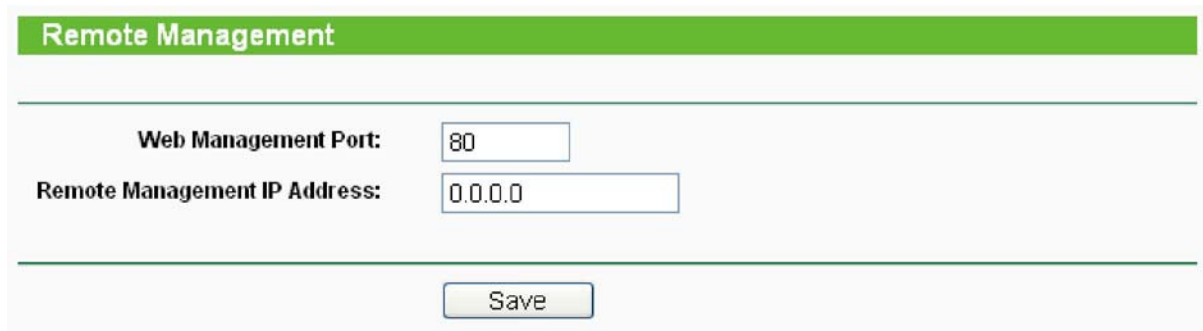
Fox example: If you want to block the PC with MAC addresses 00-0A-EB-00-07-BE and 00-0A-EB-00-07-5F to access the Internet, first, enable the **Firewall** and **MAC Address Filtering** on the **Firewall** page, then, you should specify the Default MAC Address Filtering Rule "**Deny these PC(s) with effective 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 PC | Enabled | Modify Delete |
| 2 | 00-0A-EB-00-07-5F | Alice's PC | Enabled | Modify Delete |

4.10.5 Remote Management

Selecting **Security > Remote Management** will allow you to configure the Remote Management function in the screen as shown in Figure 4-39. This feature allows you to manage your Router

from a remote location via the Internet.



The screenshot shows a web interface for configuring remote management. At the top, there is a green header bar with the text "Remote Management". Below this, there are two rows of configuration options. The first row is "Web Management Port:" followed by a text input box containing the number "80". The second row is "Remote Management IP Address:" followed by a text input box containing "0.0.0.0". Below these fields, there is a "Save" button.

Figure 4-39 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 port to a custom port by entering that number in the 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. This function is disabled when the IP address is set to the default value of 0.0.0.0. To enable this function change 0.0.0.0 to a valid IP address. If set to 255.255.255.255, then all the hosts can access the Router from internet.

 **Note:**

- 1) To access the Router, you should type your Router's WAN IP address into your browser's address (in IE) or Location (in Navigator) box, followed by a colon and the custom port number. For example, if your Router's WAN address is 202.96.12.8, and the port number used is 8080, please enter `http://202.96.12.8:8080` in your browser. Later, you may be asked for the Router's password. After successfully entering the username and password, you will be able to access the Router's web-based utility.
- 2) Be sure to change the Router's default password to a very secure password.

4.10.6 Advanced Security

Selecting **Security > Advanced Security** will enable you to protect the router from being attacked by TCP-SYN Flood, UDP Flood and ICMP-Flood from LAN as shown in Figure 4-40.

Advanced Security

Packets Statistics Interval (5 ~ 60): Seconds

DoS Protection: Disable Enable

Enable ICMP-FLOOD Attack Filtering

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

Enable UDP-FLOOD Filtering

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

Enable TCP-SYN-FLOOD Attack Filtering

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

Ignore Ping Packet From WAN Port

Forbid Ping Packet From LAN Port

Figure 4-40 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 **UDP-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.

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 as shown in Figure 4-41.

| ID | Destination IP Address | Subnet Mask | Default Gateway | Status | Modify |
|----|------------------------|-------------|-----------------|--------|--------|
|----|------------------------|-------------|-----------------|--------|--------|

Figure 4-41 Static Routing

To add static routing entries:

1. Click the **Add New** button. (pop up Figure 4-42)
2. Enter the following parameters.
 - **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.

Add or Modify a Static Route Entry

Destination IP Address:

Subnet Mask:

Default Gateway:

Status: