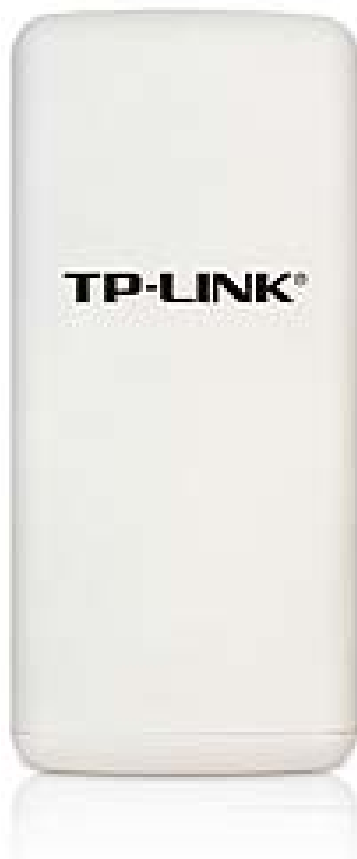


TP-LINK®

User Guide

TL-WA7210N

**2.4GHz 150Mbps Outdoor Wireless Access
Point**



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 © 2013 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 20 cm from all persons and must not be co-located or operating in conjunction with any other antenna or transmitter."

CE Mark Warning



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

Canadian Compliance Statement

This device complies with Industry Canada license-exempt RSS standard(s). Operation is subject to the following two conditions:

- (1) This device may not cause interference, and
- (2) This device must accept any interference, including interference that may cause undesired operation of the device.

Cet appareil est conforme aux norms CNR exemptes de licence d'Industrie Canada. Le fonctionnement est soumis aux deux conditions suivantes:

- (1) cet appareil ne doit pas provoquer d'interférences et
- (2) cet appareil doit accepter toute interférence, y compris celles susceptibles de provoquer un fonctionnement non souhaité de l'appareil.

Industry Canada Statement

Complies with the Canadian ICES-003 Class B specifications.

Cet appareil numérique de la classe B est conforme à la norme NMB-003 du Canada.

This device complies with RSS 210 of Industry Canada. This Class B device meets all the requirements of the Canadian interference-causing equipment regulations.

Cet appareil numérique de la Classe B respecte toutes les exigences du Règlement sur le matériel brouilleur du Canada.

Korea Warning Statements

당해 무선설비는 운용중 전파혼신 가능성이 있음.

NCC Notice & BSMI Notice

注意！

依據 低功率電波輻射性電機管理辦法

第十二條

經型式認證合格之低功率射頻電機，非經許可，公司、商號或使用者均不得擅自變更頻率、加大功率或變更原設計之特性或功能。

第十四條

低功率射頻電機之使用不得影響飛航安全及干擾合法通行；經發現有干擾現象時，應立即停用，並改善至無干擾時方得繼續使用。前項合法通信，指依電信規定作業之無線電信。低功率射頻電機需忍受合法通信或工業、科學以及醫療用電波輻射性電機設備之干擾。

安全諮詢及注意事項

- 請使用原裝電源供應器或只能按照本產品注明的電源類型使用本產品。
- 清潔本產品之前請先拔掉電源線。請勿使用液體、噴霧清潔劑或濕布進行清潔。
- 注意防潮，請勿將水或其他液體潑灑到本產品上。
- 插槽與開口供通風使用，以確保本產品的操作可靠並防止過熱，請勿堵塞或覆蓋開口。
- 請勿將本產品置放於靠近熱源的地方。除非有正常的通風，否則不可放在密閉位置中。
- 請不要私自打開機殼，不要嘗試自行維修本產品，請由授權的專業人士進行此項工作。



Продукт сертифіковано згідно с правилами системи УкрСЕПРО на відповідність вимогам нормативних документів та вимогам, що передбачені чинними законодавчими актами України.

Safety Information

- When product has power button, the power button is one of the way to shut off the product; when there is no power button, the only way to completely shut off power is to disconnect the product or the power adapter from the power source.
- Don't disassemble the product, or make repairs yourself. You run the risk of electric shock and voiding the limited warranty. If you need service, please contact us.
- Avoid water and wet locations.

This product can be used in the following countries:

AT	BG	BY	CA	CZ	DE	DK	EE
ES	FI	FR	GB	GR	HU	IE	IT
LT	LV	MT	NL	NO	PL	PT	RO
RU	SE	SK	TR	UA			

DECLARATION OF CONFORMITY

For the following equipment:

Product Description: 2.4GHz 150Mbps Outdoor Wireless Access Point

Model No.: TL-WA7210N

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, Directives 2004/108/EC, Directives 2006/95/EC, Directives 1999/519/EC, Directives 2011/65/EU

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 V1.9.2:2011& ETSI EN 301 489-17 V2.1.1:2009

EN 55022:2010

EN 55024:2010

EN 61000-3-2:2006+A1:2009+A2:2009

EN 61000-3-3:2008

EN 60950-1:2006+A11: 2009+A1:2010+A12:2011

EN 62311:2008

The product carries the CE Mark:

CE 1588

Person responsible for marking this declaration:



Yang Hongliang

Product Manager of International Business

Date of issue: 2013

TP-LINK TECHNOLOGIES CO., LTD.

Building 24 (floors 1, 3, 4, 5), and 28 (floors 1-4) Central Science and Technology Park, Shennan Rd, Nanshan, Shenzhen, China

CONTENTS

Package Contents	1
Chapter 1. Introduction	2
1.1 Overview of the Product	2
1.2 Features	2
1.3 Conventions	4
1.4 Panel Layout	4
1.4.1 The Front Panel	4
1.4.2 The Rear Panel	5
Chapter 2. Connecting the Device	6
2.1 System Requirements	6
2.2 Installation Environment Requirements	6
2.3 Connecting the Device	6
2.3.1 AP Client Router Mode	7
2.3.2 AP Router Mode	7
2.3.3 Access Point	8
2.3.4 Multi-SSID	8
2.3.5 Repeater and Universal Repeater	9
2.3.6 Bridge with AP	9
2.3.7 Client	10
Chapter 3. Quick Installation Guide	11
3.1 Configure the Device	11
3.2 Quick Setup	12
3.2.1 AP Client Router	15
3.2.2 AP Router	19
3.2.3 Access Point	23
3.2.4 Multi-SSID	26
3.2.5 Repeater (Range Extender)	28
3.2.6 Bridge with AP	32
3.2.7 Client	35
Chapter 4. AP & Multi-SSID & Repeater (Range Extender) & Bridge with AP & Client Operation Mode	40
4.1 Login	40
4.2 Status	40
4.3 Quick Setup	41
4.4 Operation Mode	41
4.5 WPS	42

4.6	Network	43
4.6.1	LAN.....	43
4.7	Wireless.....	44
4.7.1	Wireless Settings.....	45
4.7.2	Wireless Security.....	46
4.7.3	Wireless MAC Filtering	48
4.7.4	Wireless Advanced	51
4.7.5	Antenna Alignment	52
4.7.6	Distance Setting	52
4.7.7	Throughput Monitor	53
4.7.8	Wireless Statistics.....	53
4.8	DHCP	54
4.8.1	DHCP Settings	54
4.8.2	DHCP Clients List.....	55
4.8.3	Address Reservation	56
4.9	System Tools	57
4.9.1	SNMP.....	57
4.9.2	Time Settings	58
4.9.3	Diagnostic	60
4.9.4	Ping Watch Dog.....	61
4.9.5	Speed Test	61
4.9.6	Firmware Upgrade.....	62
4.9.7	Factory Defaults	63
4.9.8	Backup & Restore.....	63
4.9.9	Reboot	64
4.9.10	Password	64
4.9.11	System log.....	65
4.9.12	Statistics.....	66
Chapter 5.	AP Client Router & AP Router Operation Mode	68
5.1	Login	68
5.2	Status.....	68
5.3	Quick Setup	70
5.4	Operation Mode.....	70
5.5	WPS.....	71
5.6	Network	72
5.6.1	WAN.....	72
5.6.2	MAC Clone.....	80
5.6.3	LAN.....	81

5.7	Wireless.....	81
5.7.1	Wireless Settings.....	82
5.7.2	Wireless Security.....	87
5.7.3	MAC Filtering.....	89
5.7.4	Wireless Advanced.....	91
5.7.5	Antenna Alignment.....	92
5.7.6	Distance Setting.....	92
5.7.7	Throughput Monitor.....	93
5.7.8	Wireless Statistics.....	93
5.8	DHCP.....	94
5.8.1	DHCP Settings.....	94
5.8.2	DHCP Clients List.....	95
5.8.3	Address Reservation.....	96
5.9	Forwarding.....	97
5.9.1	Virtual Servers.....	97
5.9.2	Port Triggering.....	99
5.9.3	DMZ.....	100
5.9.4	UPnP.....	101
5.10	Security.....	101
5.10.1	Basic Security.....	102
5.10.2	Advanced Security.....	103
5.10.3	Local Management.....	104
5.10.4	Remote Management.....	105
5.11	Parental Control.....	105
5.12	Access Control.....	107
5.12.1	Rule.....	107
5.12.2	Host.....	109
5.12.3	Target.....	110
5.12.4	Schedule.....	111
5.13	Advanced Routing.....	112
5.13.1	Static Routing List.....	112
5.13.2	System Routing Table.....	113
5.14	Bandwidth Control.....	114
5.14.1	Control Settings.....	114
5.14.2	Rules List.....	114
5.15	IP & MAC Binding.....	115
5.15.1	Binding Setting.....	115
5.15.2	ARP List.....	116

5.16	Dynamic DNS	117
5.17	System Tools	120
5.17.1	Time Settings	121
5.17.2	Diagnostic	122
5.17.3	Firmware Upgrade	123
5.17.4	Factory Defaults	124
5.17.5	Backup & Restore	124
5.17.6	Reboot	125
5.17.7	Password	125
5.17.8	System log	126
5.17.9	Statistics	128
Appendix A: FAQ		130
Appendix B: Configuring the PC		134
Appendix C: Specifications		138
Appendix D: Glossary		139

Package Contents

The following items should be found in your package:

- One TL-WA7210N 2.4GHz 150Mbps Outdoor Wireless Access Point
- One power Adapter for TL-WA7210N 2.4GHz 150Mbps Outdoor Wireless Access Point
- One Power Injector
- Mounting Kits
- Quick Installation Guide
- One Resource CD for TL-WA7210N 2.4GHz 150Mbps Outdoor Wireless Access Point, including:
 - This User Guide
 - Other helpful information

 **Note:**

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

Chapter 1. Introduction

1.1 Overview of the Product

The TL-WA7210N 2.4GHz 150Mbps Outdoor Wireless Access Point is dedicated to Outdoor wireless network solutions. The TL-WA7210N 2.4GHz 150Mbps Outdoor Wireless Access Point will allow you to connect your network with other wireless devices wirelessly, sharing Internet Access, files and fun, easily and securely. The high power design will also help you build a more stable link or cover more area outdoors.

The TL-WA7210N 2.4GHz 150Mbps Outdoor Wireless Access Point provides 7 operation modes for multi-user to access the Internet: AP Client Router, AP Router, Access Point, Multi-SSID, Repeater (Range Extender), Bridge with AP and Client. In AP Client Router mode, it works as a WISP CPE and can access the Internet wirelessly via your WISP. In AP Router mode, it can access the Internet via an ADSL/Cable Modem, while sharing data wirelessly.

With the most attentive wireless security, the TL-WA7210N 2.4GHz 150Mbps Outdoor Wireless Access Point provides multiple protection measures. It can be set to turn off wireless network name (SSID) broadcast so that only stations that have the SSID can be connected. The AP provides wireless LAN 64/128/152-bit WEP encryption security, and WPA/WPA2 and WPA-PSK/WPA2-PSK authentication, as well as TKIP/AES encryption security. It also supports VPN pass-through for sensitive data secure transmission.

The TL-WA7210N 2.4GHz 150Mbps Outdoor Wireless Access Point complies with the IEEE 802.11n, IEEE 802.11g and IEEE 802.11b standards so that the data transmission rate is up to 150Mbps. The wireless transmission range can extend up to tens of kilometers.

1.2 Features

- Complies with IEEE 802.11n, IEEE 802.11g, IEEE 802.11b, IEEE 802.3, IEEE 802.3u standards.
- Wireless Data transfer rates up to 150Mbps.
- Supports AP Client Router, AP Router, Access Point, Multi-SSID, Repeater (Range Extender), Bridge with AP, Client 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.
- Output transmit power adjustable.
- Supports PPPoE, Dynamic IP, Static IP Internet Access.
- Built-in NAT and DHCP server supporting static IP address distributing.

- Provides WLAN ACL (Access Control List).
- Supports configuration backup/restore and firmware upgrade.
- Supports Web management.
- Supports Remote Management.
- 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.

1.3 Conventions

The AP or TL-WA7210N, or device mentioned in this User guide stands for TL-WA7210N 2.4GHz 150Mbps Outdoor Wireless Access Point without any explanations.

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

You can set the parameters according to your demand.

1.4 Panel Layout

1.4.1 The Front Panel

TL-WA7210N consists of several LED indicators, which is designed to indicate connections and wireless signal.

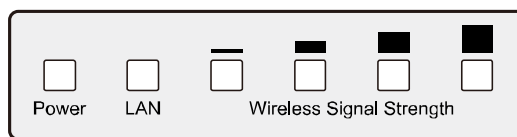


Figure 1-1 Front Panel sketch

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 Antenna Alignment page as shown in Figure 4-12.

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.

1.4.2 The Rear Panel

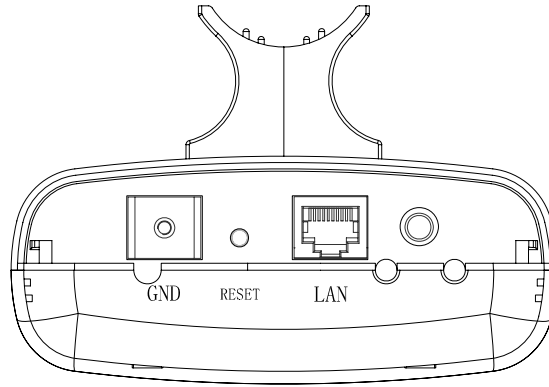



Figure 1-2 Rear Panel sketch

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 1-1 flashes.

 **Note:**

Ensure the AP is powered on before it restarts completely.

Chapter 2. Connecting the Device

2.1 System Requirements

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

2.2 Installation Environment Requirements

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

2.3 Connecting the Device

To connect the AP, please follow the steps below:

1. Power off your PC, Cable/DSL Modem, and the AP.
2. Locate an optimum location for the AP. The best place is usually at the center of your wireless network. The place must accord with the [Installation Environment Requirements](#).
3. Adjust the direction of the antenna. Normally, upright is a good direction.

After finishing the steps above, please choose the operation mode you need and carry out the corresponding steps. There are seven operation mode supported by this AP: **AP Client Router**, **AP Router**, **Access Point**, **Multi-SSID**, **Repeater (Range Extender)**, **Bridge with AP** and **Client**.

2.3.1 AP Client Router Mode

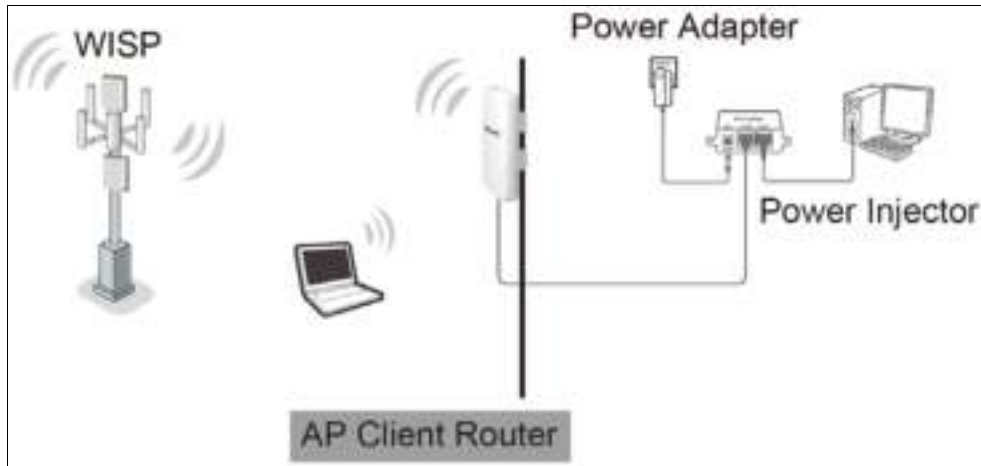


Figure 2-1 Hardware Installation of the TL-WA7210N in AP Client Router mode

1. Connect the LAN port of TL-WA7210N to the POE port of the Power Injector with an Ethernet cable.
2. Connect the PC to the LAN port of the Power Injector with an Ethernet cable.
3. Plug one end of the Power Adapter into the DC jack on the Power Injector, and the other end in electrical wall socket.
4. Power on the PC(s) and notebook(s).

2.3.2 AP Router Mode

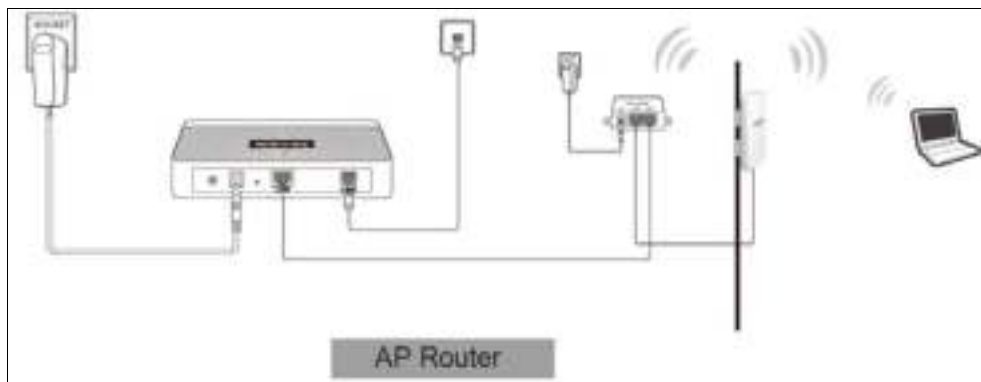


Figure 2-2 Hardware Installation of the TL-WA7210N in AP Router mode

1. Connect the LAN port of TL-WA7210N to the POE port of the Power Injector with an Ethernet cable.
2. Connect the DSL/Cable Modem to the LAN port of the Power Injector with an Ethernet cable.
3. Plug one end of the Power Adapter into the DC jack on the Power Injector, and the other end in electrical wall socket.
4. Power on the PC(s) and other connected devices (such as the ADSL modem).

Note:

In this mode, the LAN port of the Power Injector (connected to the LAN port of the Device) works as the WAN port.

2.3.3 Access Point

This operation mode allows wireless stations to access.

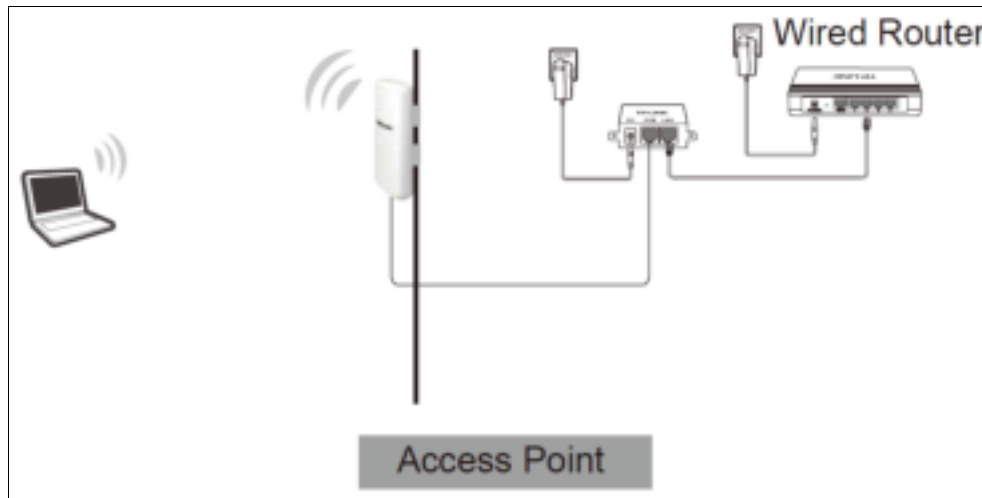


Figure 2-3 Hardware Installation of the TL-WA7210N in Access Point mode

1. Connect the LAN port of TL-WA7210N to the POE port of the Power Injector with an Ethernet cable.
2. Connect the LAN port of the Power Injector to the wired network port with an Ethernet cable.
3. Plug one end of the Power Adapter into the DC jack on the Power Injector, and the other end in the electrical wall socket.
4. Power on the notebook(s) and other connected devices (such as the Wired Router).

2.3.4 Multi-SSID

In this mode, AP can support up to 4 SSID.

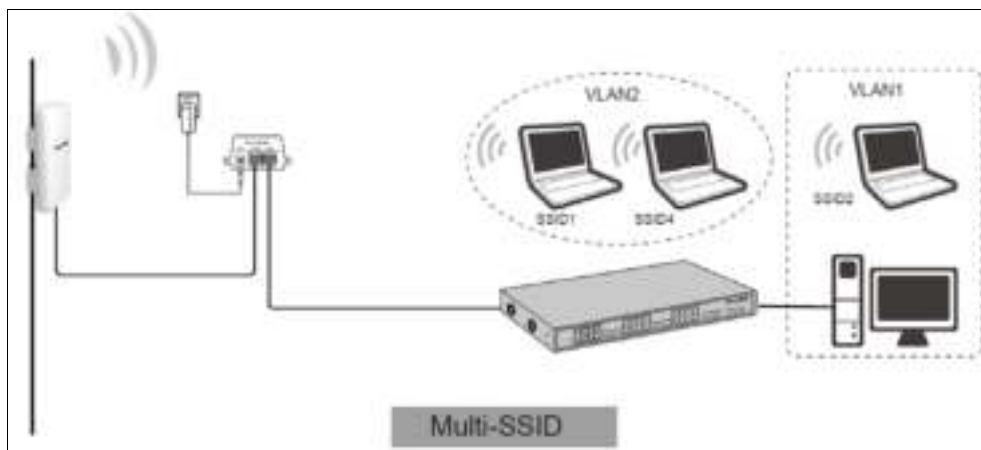


Figure 2-4 Hardware Installation of the TL-WA7210N in Multi-SSID mode

1. Connect the LAN port of TL-WA7210N to the POE port of the Power Injector with an Ethernet cable.
2. Connect the LAN port of the Power Injector to the wired network port with an Ethernet cable.
3. Plug one end of the Power Adapter into the DC jack on the Power Injector, and the other end in the electrical wall socket.
4. Power on the notebooks and other connected devices (such as the Switch).

2.3.5 Repeater and Universal Repeater

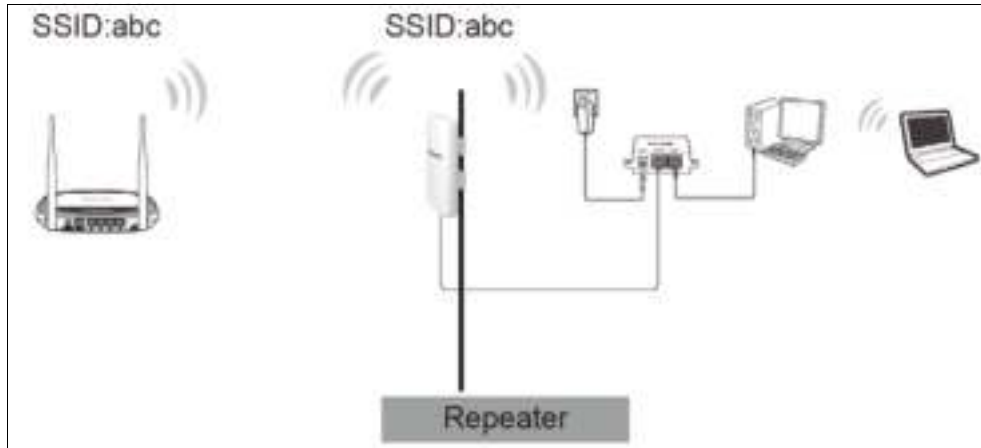


Figure 2-5 Hardware Installation of the TL-WA7210N in (Universal) Repeater mode

1. Connect the LAN port of TL-WA7210N to the POE port of the Power Injector with an Ethernet cable.
2. Plug one end of the Power Adapter into the DC jack on the Power Injector, and the other end in electrical wall socket.
3. Power on the PC(s) and other connected devices (such as the Router).

Note:

Both Repeater and Universal Repeater modes allow the AP with its own BSS to relay data to a root AP. The wireless repeater relays signal between its stations and the root AP for greater wireless range. However, in Repeater mode, the WDS associated is enabled, while in Universal Repeater mode, the WDS associated is disabled.

2.3.6 Bridge with AP

Two Devices are needed in this mode.

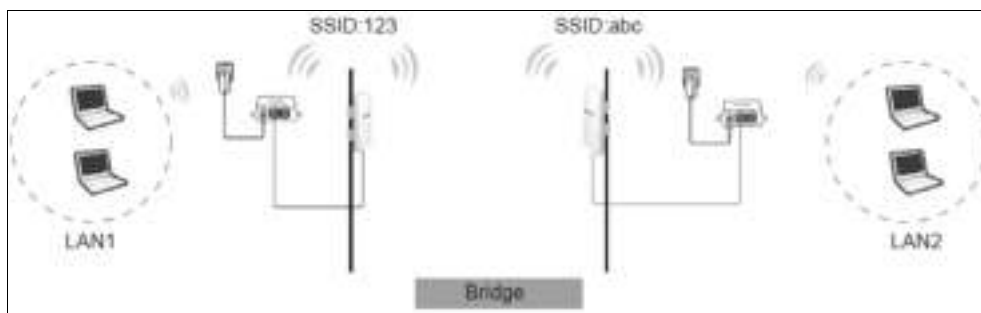


Figure 2-6 Hardware Installation of the TL-WA7210N in Standard AP -- Bridge mode

1. Connect the LAN port of TL-WA7210N to the POE port of the Power Injector with an Ethernet cable.
2. Plug one end of the Power Adapter into the DC jack on the Power Injector, and the other end in electrical wall socket.
3. Power on the PC(s).

Note:

It is recommended that you connect a PC/notebook to the LAN port of the Device with an Ethernet cable, and then login the Device from the PC/notebook to set the Device in Bridge with AP mode.

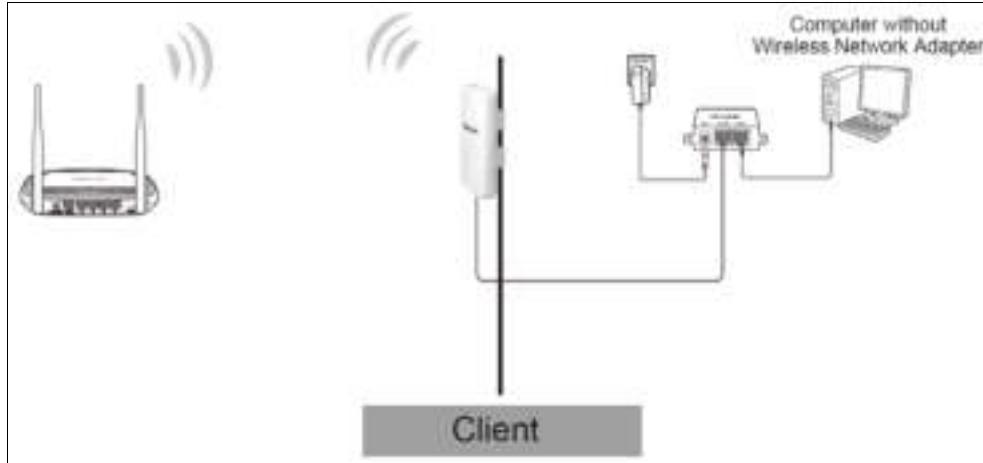
2.3.7 Client

Figure 2-7 Hardware Installation of the TL-WA7210N in Client mode

1. Connect the LAN port of TL-WA7210N to the POE port of the Power Injector with an Ethernet cable.
2. Connect the PC to the LAN port of the Power Injector with an Ethernet cable.
3. Plug one end of the Power Adapter into the DC jack on the Power Injector, and the other end in electrical wall socket.
4. Power on the PC(s) and other connected devices (such as the Router).

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.

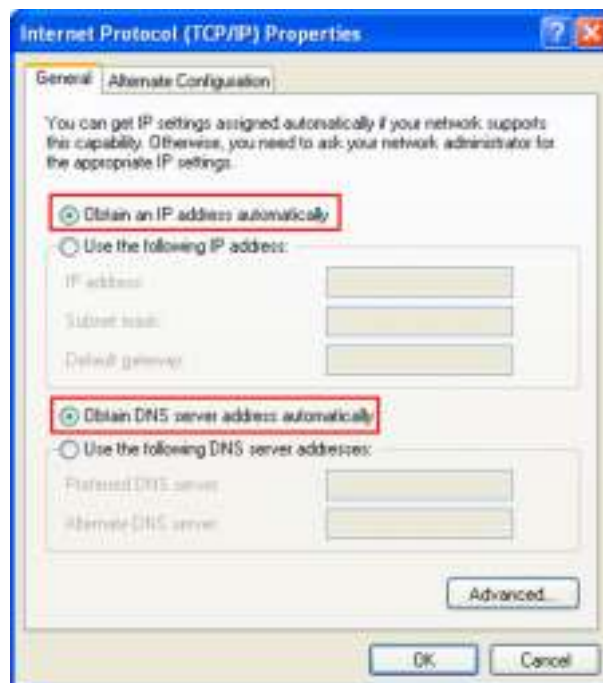
The default IP address of the TL-WA7210N 2.4GHz 150Mbps Outdoor Wireless Access Point is 192.168.0.254. And the default Subnet Mask is 255.255.255.0. These values can be seen from the LAN. They can be changed as you desire, as an example we use the default values for description in this guide.

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 192.168.0.xxx ("xxx" is from 2 to 253), Subnet Mask is 255.255.255.0

Note:

If you configure your device by this way, please remember to change the configuration of your PC to the figure as shown below to make your PC connect to the Internet successfully.



- Obtain an IP address automatically

This method can be available only when **DHCP** in [section 4.8.1](#) 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 192.168.0.254`, 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 192.168.0.254 with 32 bytes of data:

Reply from 192.168.0.254: bytes=32 time<1ms TTL=64
Reply from 192.168.0.254: bytes=32 time<1ms TTL=64
Reply from 192.168.0.254: bytes=32 time<1ms TTL=64
Reply from 192.168.0.254: bytes=32 time<1ms TTL=64

Ping statistics for 192.168.0.254:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, 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 192.168.0.254 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 192.168.0.254, your PC's IP address must be within the range of 192.168.0.2 ~ 192.168.0.253.

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-WA7210N 2.4GHz 150Mbps Outdoor Wireless Access Point. The Web-based utility can be used on any Windows, Macintosh or UNIX OS with a Web browser.

Open your web browser and enter the IP address of the AP (192.168.0.254) 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.

Note:

If the device has been restored, the **Welcome** page will appear as shown in Figure 3-5, please read the **TERMS OF USE** carefully. Then select **I agree to these terms of use** and click **Login** to continue.

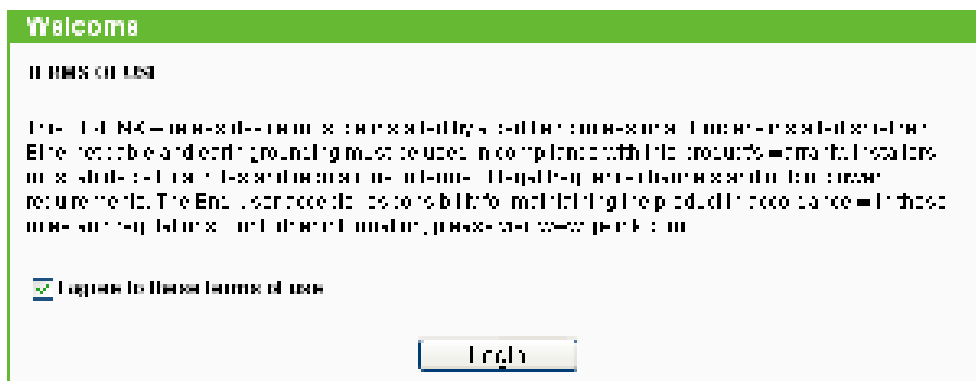


Figure 3-5 Welcome page

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.

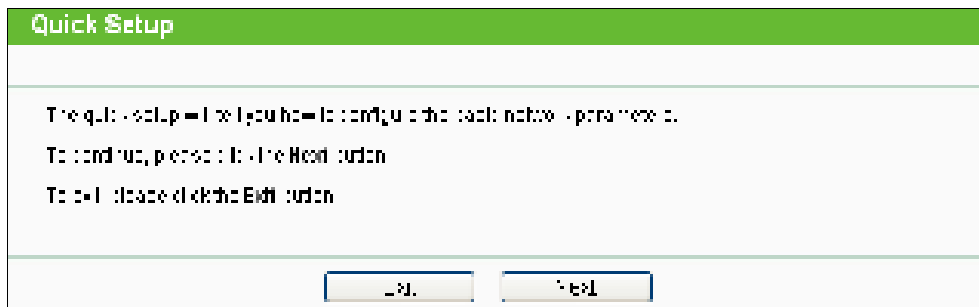


Figure 3-6 Quick Setup

Click **Next**, and then **Operation Mode** page will appear, shown in Figure 3-7:

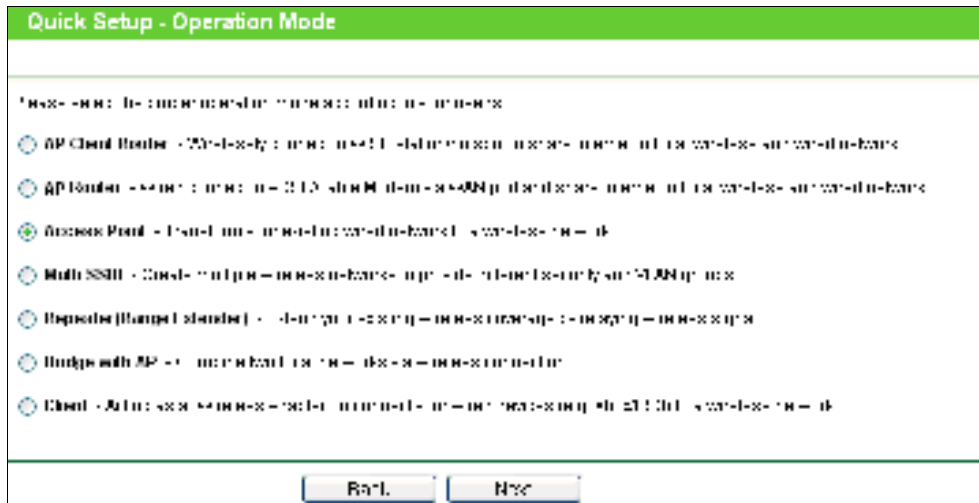


Figure 3-7 Operation Mode

- **AP Client Router** - In this mode, the device enables multi-users to share Internet from WISP. The LAN port devices share the same IP from WISP through Wireless port. While connecting to WISP, the Wireless port works as a WAN port at AP Client Router mode. The Ethernet port acts as a LAN port.
- **AP Router** - In this mode, the device enables multi-users to share Internet via ADSL/Cable Modem. The wireless port share the same IP to ISP through Ethernet WAN port. The Wireless port acts the same as a LAN port while at AP Router mode.
- **Access Point** - In this mode, the device can be connected to a wired network and transform the wired access into wireless that multiple devices can share together, especially for a home, office or hotel where only wired network is available.
- **Multi-SSID** - In this mode, the device can create up to 4 wireless networks labeled with different SSIDs and assign each SSID with different security or VLAN, especially for the situation when the various access policies and functions are required.
- **Repeater(Range Extender)** - In this mode, the device can copy and reinforce the existing wireless signal to extend the coverage of the signal, especially for a large space to eliminate signal-blind corners.
- **Bridge with AP** - In this mode, the device can be used to combine multiple local networks together to the same one via wireless connections, especially for a home or office where separated networks can't be connected easily together with a cable.
- **Client** - In this mode, the device can be connected to another device via Ethernet port and act as an adaptor to grant your wired devices access to a wireless network, especially for a Smart TV, Media Player, or game console only with an Ethernet port.

 **Note:**

When you change the operation mode to Client/Repeater, WPS function will stay disabled. Please manually enable this function if needed when you switch back to Access Point/Multi-SSID/Bridge mode.

3.2.1 AP Client Router

When you choose **AP Client Router Mode** on **Operation Mode** page in Figure 3-7, take the following steps:

1. Click **Next** in Figure 3-7, and then **WAN Connection Type** page will appear as shown in Figure 3-8.

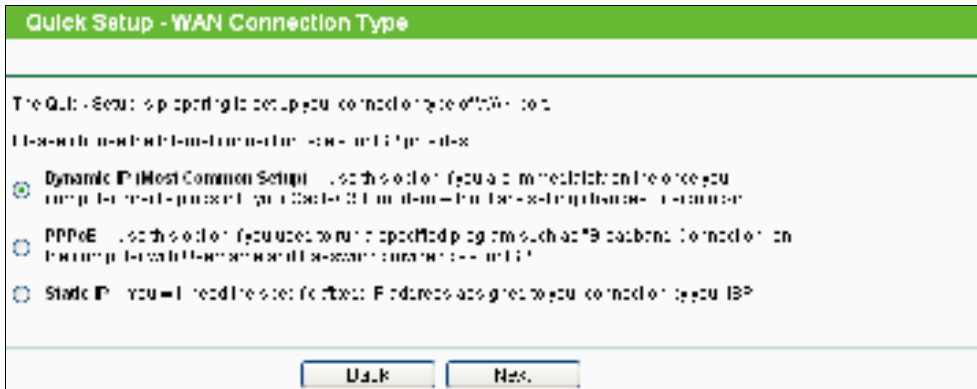


Figure 3-8 WAN Connection Type

- **Dynamic IP**- When the Device connects to a DHCP server, or the ISP supplies you with DHCP connection, please choose this type. The Device will get the IP address automatically from the DHCP server or the WISP if you choose the Dynamic IP type.

If you choose **Dynamic IP** in Figure 3-8 and then click **Next**, the wireless setting page as in Figure 3-10 will appear.

- **PPPoE** - If you have applied ADSL to realize Dial-up service, you should choose this type. In this condition, you should fill in both the User Name and Password that your ISP supplies.

- 1) If you choose **PPPoE** in Figure 3-8 and then click **Next**, Figure 3-9 will appear.

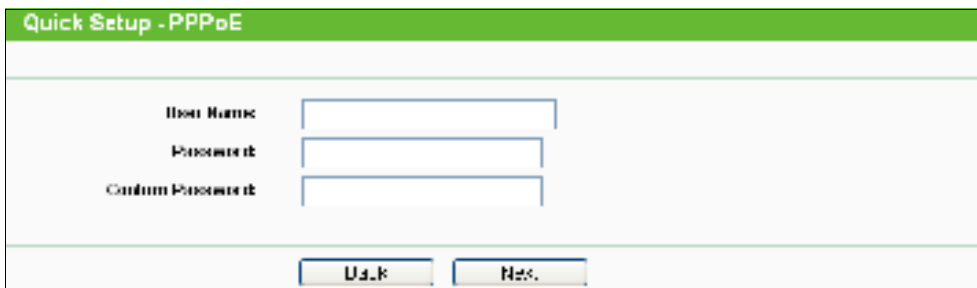


Figure 3-9 PPPoE

- 2) Enter the **User Name** and **Password** provided by your ISP, then click **Next**, Figure 3-10 will appear.

Figure 3-10 WISP Station Setting

- **Wireless Name of WISP Station** - The SSID of the AP your Device is going to connect to as a client. You can also use the search function to select the SSID to join.
- **MAC Address of WISP Station** - The BSSID of the AP your Device is going to connect to as a client. You can also use the search function to select the BSSID to join.
- **Survey** - Click this button, you can search the AP which runs in the current channel.
- **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, the Note Dialog of **TERMS OF USE** will pop up. Select **I agree to these terms of use**, and click **Accept** to continue.

Note Dialog

Note:

Ensure you select a correct country to comply with local laws. Incorrect settings may cause interference.

- **Transmission Power** - The available options of transmission power are determined by the region selected.

- **Wireless Security Mode** - This option should be chosen according to the AP's security configuration. It is recommended that the security type is the same as your AP's security type.
 - **Wireless Password** - If the AP your Device is going to connect needs password, you need to fill the password in this blank.
- **Static IP** - In this type, you should manually fill in the **IP address**, **Subnet Mask**, **Default Gateway**, and **DNS** IP address, which are specified by your ISP.
- 1) If you choose **Static IP** in Figure 3-8 and then click **Next**, Figure 3-11 will appear.

Figure 3-11 Static IP

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

 **Note:**

The IP parameters should have been provided by your WISP.

- 2) After you have entered the above necessary parameters and then click **Next**, the wireless setting page as shown in Figure 3-10 will then appear.
2. Click **Survey** in Figure 3-10 to scan the wireless networks, then the AP List page will pop up as shown in , choose the target one, click **Connect**. You will then return to the previous page. If the AP your Device is going to connect needs password, you need to fill the password. Click **Next**.

ID	BSSID	SSID	Signal	Channel	Security	Connect
1	23 23 23 23 23 23		20dB		OFF	Connect
2	14 E6 E4 D7 1C EC	TP-LINK_3.4G-2_D71CE0	138dB		WPA/WPA2 PSK	Connect
3	D8 9C 41 4C 17 D4	TP-LINK_40 7C4	0dB		OFF	Connect
4	4C F3 C 97 E8 39	TP-LINK_7B82C	13dB		OFF	Connect
5	1E E6 E4 D7 1C EC	TP-LINK_3.4G-2_D71CE0	0dB		OFF	Connect
6	EC 7 3F 74 33 D8		94dB	4	OFF	Connect
7	0C 1C 0F 0 9C 94		90dB	4	OFF	Connect
8	94 01 6C 2F 31 EE	TP-LINK_700000	84dB	4	WPA/WPA2 PSK	Connect
9	14 E6 E4 E9 87 50		13dB	3	WPA/WPA2 PSK	Connect
0	4C F3 C 9C 27 31	TP-LINK_393730	9 dB	3	OFF	Connect
1	14 E6 E4 E9 4E 8C	TP-LINK_100	90dB	1	WPA/WPA2 PSK	Connect

Figure 3-12 AP List

- The page below will appear. Create a name for the **Local Wireless Network**. The security settings for the local network will be set the same as your WISP by default. Then click **Next**.

Quick Setup - Local Wireless AP Setting

Local Wireless Name:

Use the same security settings for the local wireless network as the remote WISP station

Figure 3-13 Local Wireless AP Setting

Ticking off **Use the same security settings for the local wireless network as the remote WISP station**, the page will show as below. You can choose the **Wireless Security Mode** and fill in **Wireless Password** for the **Local Wireless Network**.

Quick Setup - Local Wireless AP Setting

Local Wireless Name:

Use the same security settings for the local wireless network as the remote WISP station

Wireless Security Mode:

Wireless Password:

Figure 3-14 Local Wireless AP Setting

- When you have finished the wireless settings above, you will come to the **Finish** page shown as Figure 3-15. Please check the configurations you have made. If anything is wrong, please go **Back** to reset. When confirmed, please click **Finish/Reboot** button in Figure 3-15 to make all the configurations take effect.

Quick Setup - Finish

Click Next to go to the next page. If you click Finish, you will be able to configure the device.

Click **Finish** to save the configuration and exit the setup.

Wireless Setting

Operation Mode: **AP Router**

Internet Connection Type: **LAN**

PPPoE User Name: **pppoeuser**

PPPoE Password: **pppoeuser**

Wireless Name of Default AP: **TL-WA7210N**

MAC Address of Default AP: **98-00-00-00-00-00**

Wireless Security Mode: **WPA-PSK (TKIP+AES)**

Wireless Password: **1234567890**

Local Wireless Name (SSID): **TL-WA7210N**

Wireless Channel: **1**

Wireless Security Mode: **WPA-PSK (TKIP+AES)**

Wireless Password: **1234567890**

Region: **China (UTC+8)**

Transmit Power: **100%**

Save these settings to a profile for future reference.

Figure 3-15 Finish page

3.2.2 AP Router

When you choose **AP Router Mode** on **Operation Mode** page in Figure 3-7, take the following steps:

1. Click **Next** in Figure 3-7, and then **WAN Connection Type** page will appear as shown in Figure 3-16.

Quick Setup - WAN Connection Type

The Quick Setup is designed to help you set up your connection type of WAN port.

You can directly select the Internet connection type and click **Next** to go to the Auto Detect page. The table you need to specify the connection type manually:

Dynamic IP (Auto) Common Setup: If you select this option, you can connect to the Internet through a dynamic IP address (e.g., ADSL, Cable, DSL, etc.) without connecting to a specific ISP.

PPPoE: If you select this option, you will be asked to enter your ISP's Username and Password for the connection. The Username and Password are added by your ISP.

Static IP: You can select this option if you have a static IP address. You can connect to the Internet through a static IP address.

Figure 3-16 WAN Connection Type

- **PPPoE** - If you have applied ADSL to realize Dial-up service, you should choose this type. In this condition, you should fill in both the User Name and Password that your ISP provides.
- 1) If you choose **PPPoE** in Figure 3-16 and then click **Next**, Figure 3-17 will appear.

Figure 3-17 PPPoE

- 2) Enter the **User Name** and **Password** provided by your ISP and then click **Next**, Figure 3-18 will appear.

Figure 3-18 Wireless

- **Wireless Network Name (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 recommended strongly that you change your networks name (SSID) to a different value. This value is case-sensitive. For example, **MYSSID** is NOT the same as **MySSID**.
- **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, the Note Dialog of **TERMS OF USE** will pop up. Select **I agree to these terms of use**, and click **Accept** to continue.

Note Dialog

 **Note:**

Ensure you select a correct country to comply with local laws. Incorrect settings may cause interference.

- **Transmission Power** - The available options of transmission power are determined by the region selected.
 - **Wireless Security Mode** - You can select one of the following security options:
 - **WPA/WPA2-PSK** - Select WPA based on pre-shared passphrase.
 - **WEP** - Select WEP based on none pre-shared passphrase.
 - **No Security** - The wireless security function is disabled. The wireless stations will be able to connect the Device without encryption.
 - **Auth Type** - This option should be chosen if the Security Mode is WEP. It indicates the authorization type of the Root AP.
 - **Key Format** - This option should be chosen if the Security Mode is WEP. It indicates the format of the WEP key.
 - **Wireless Password** - If the AP your Device is going to connect needs password, you need to fill the password in this blank.
- **Dynamic IP**- When the Device connects to a DHCP server, or the ISP supplies you with DHCP connection, please choose this type. The Device will get the IP address automatically from the DHCP server or the ISP if you choose the Dynamic IP type.
- 1) If you choose **Dynamic IP** in Figure 3-16 and then click **Next**, Figure 3-20 will appear.

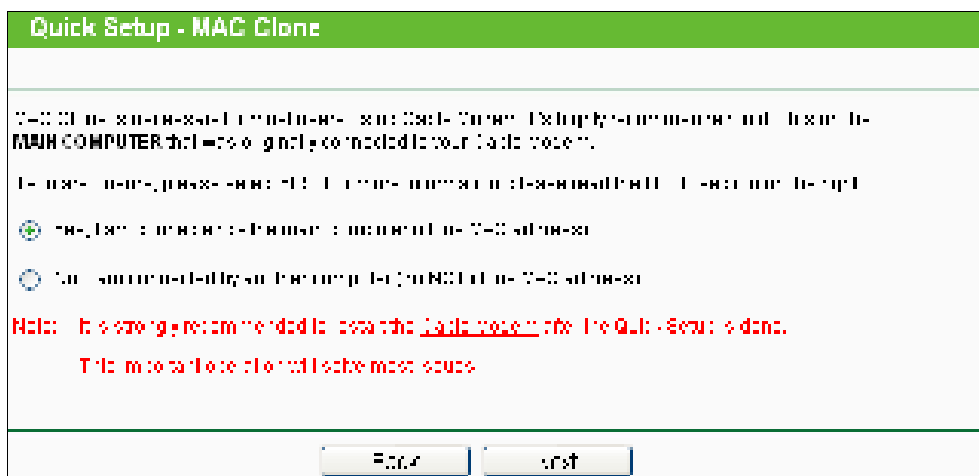


Figure 3-19 MAC Clone

Most Cable ISPs (Internet Service Provider) register the unique MAC Address from the wired connection on your MAIN COMPUTER - the last computer used to be connected with the Cable Modem and had Internet connection.

If you add a router to the network, your ISP may not recognize the MAC address of the router and not allow it to connect.

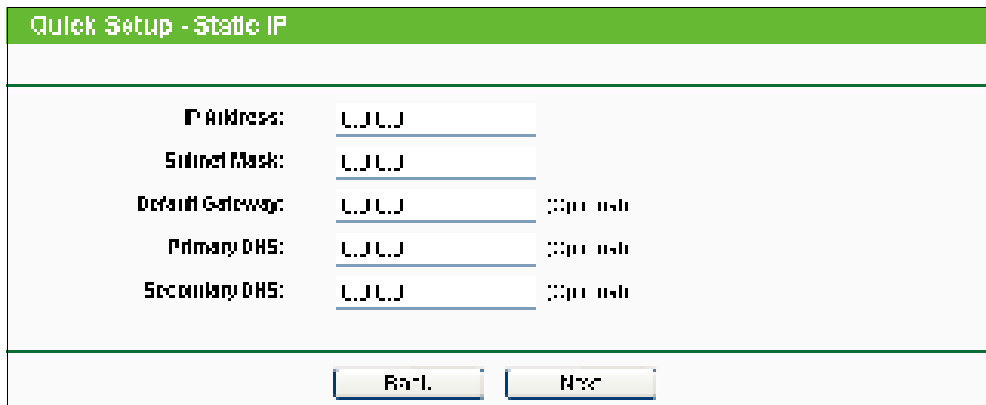
However, TP-LINK router can "clone" or replicate the registered MAC address of the MAIN COMPUTER. Then your ISP can release the Internet connection to the router and all the computers.

Click the **Next** button to continue, or the **Back** button to return to the previous page.

 **Note:**

It is strongly recommended to restart the Cable Modem after the Quick Setup is done. This important operation will solve most issues.

- 2) Choose to clone MAC address or not, if you are unsure, please select YES. Then click **Next**, and you will come to the page shown in Figure 3-18.
- **Static IP** - In this type, you should manually fill in the **IP address**, **Subnet Mask**, **Default Gateway**, and **DNS IP address**, which are specified by your ISP.
- 1) If you choose **Static IP** in Figure 3-16 and then click **Next**, Figure 3-20 will appear.






Quick Setup - Static IP	
IP Address:	0.0.0.0
Subnet Mask:	0.0.0.0
Default Gateway:	0.0.0.0 
Primary DNS:	0.0.0.0 
Secondary DNS:	0.0.0.0 
<input type="button" value="Back"/> <input type="button" value="Next"/>	

Figure 3-20 Static IP

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

 **Note:**

The IP parameters should have been provided by your ISP.

After you have entered the above necessary parameters and then click **Next**, Figure 3-18 will then appear.

2. When you finish the wireless setting in Figure 3-18 and click **Next**, then Figure 3-21 will appear, where you can click **Finish** button to complete the **Quick Setup**.

Quick Setup - Finish

Please click the Finish button to make all configurations take effect.

Wireless Setting

Operation Mode	Access Point
Internet Connection Type	Ethernet
Wireless Network Name (SSID)	TP-LINK_XXXXXX
Wireless Security Mode	WPA/WPA2-PSK
Wireless Password	1234567890
Region	United States
Transmission Power	Auto

Save these settings to a local file for future reference.

Back Finish

Figure 3-21 Finish page

3.2.3 Access Point

When you choose **Access Point** on **Operation Mode** page in Figure 3-7, take the following steps:

1. Click **Next** in Figure 3-7, and then **Wireless** page will appear as shown in Figure 3-22. Create an easy-to-remember name for your wireless network. Select **Most Secure (WPA/WPA2-PSK)** mode and enter a wireless password below to prevent unauthorized access to your AP. Then click **Next**.

Quick Setup - Wireless

Wireless Network Name (SSID): TP-LINK_XXXXXX

Region: United States

Warning: End-user security certificate for wireless LAN

Transmission Power: 70 dBm

Wireless Security Mode: WPA/WPA2-PSK

Wireless Password: 1234567890

You can only use 0-9, letters between a-z and A-Z or special characters to create a password.

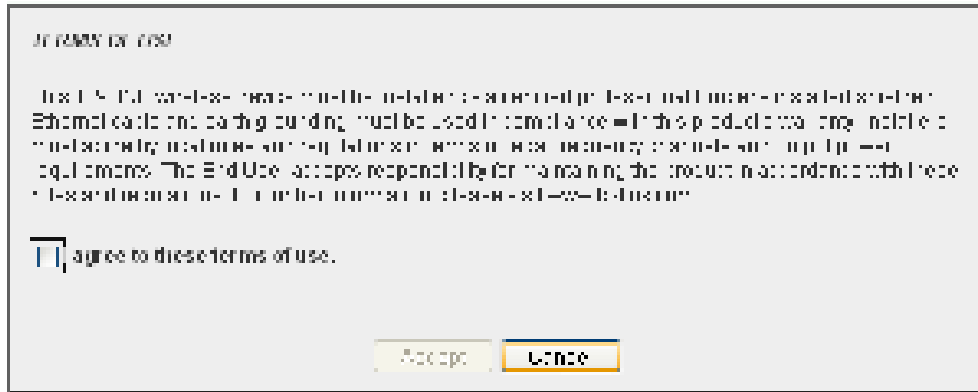
Back Next

Figure 3-22 Wireless

- **Wireless Network Name** - 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 recommended strongly that you change your networks name (SSID) to a different value. This value is case-sensitive. For example, **MYSSID** is NOT the same as **MySSID**.

- **Region** - Select your region from the pull-down list. This field specifies the region where the wireless function of the AP can be used. It may be illegal to use the wireless function of the AP 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, the Note Dialog of **TERMS OF USE** will pop up. Select **I agree to these terms of use**, and click **Accept** to continue.



Note Dialog

Note:

Ensure you select a correct country to comply with local laws. Incorrect settings may cause interference.

- **Transmission Power** - The available options of transmission power are determined by the region selected.
- **Wireless Security Mode** - You can select one of the following security options:
 - **WPA/WPA2-PSK** - Select WPA based on pre-shared passphrase.
 - **WEP** - Select WEP based on none pre-shared passphrase.
 - **No Security** - The wireless security function is disabled. The wireless stations will be able to connect the Device without encryption.
- **Auth Type** - This option should be chosen if the Security Mode is WEP. It indicates the authorization type of the Root AP.
- **Key Format** - This option should be chosen if the Security Mode is WEP. It indicates the format of the WEP key.
- **WEP Index** - This option should be chosen if the Security Mode is WEP. It indicates the index of the WEP key.
- **Wireless Password** - If the AP your Device is going to connect needs password, you need to fill the password in this blank.

Note:

The operating distance or range of your wireless connection varies significantly based on the physical placement of the Device. For best results, place your Device

- Near the center of the area in which your wireless stations will operate.
- In an elevated location such as a high shelf.
- Away from the potential sources of interference, such as PCs, microwaves, and cordless phones.
- With the Antenna in the upright position.

- Away from large metal surfaces.

Failure to follow these guidelines can result in significant performance degradation or inability to wirelessly connect to the Device.

2. The Network Setting page will appear then. It is recommended that you keep the default settings on this page. Click **Next**.

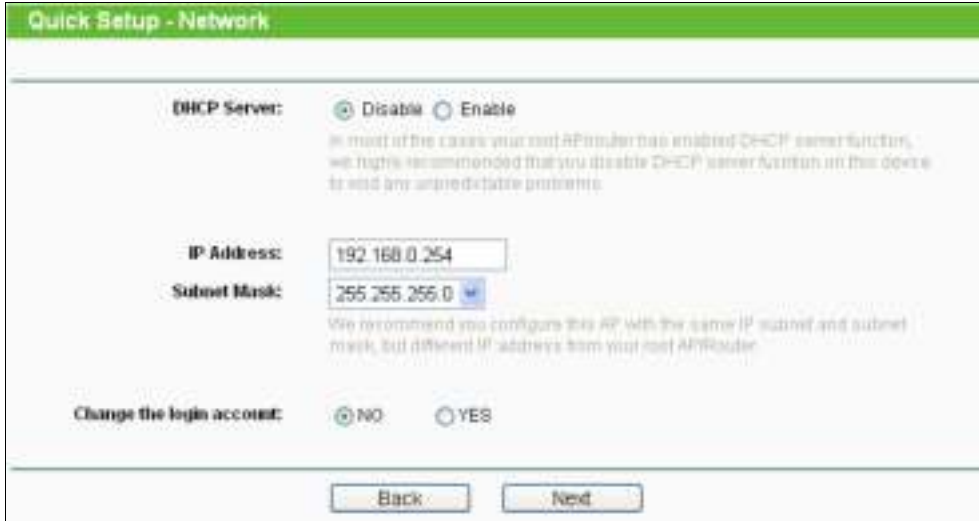


Figure 3-23 Network

3. When you finish the wireless setting in Figure 3-23 and click **Next**, then Figure 3-24 will appear, where you can click **Finish** button to complete the **Quick Setup**.

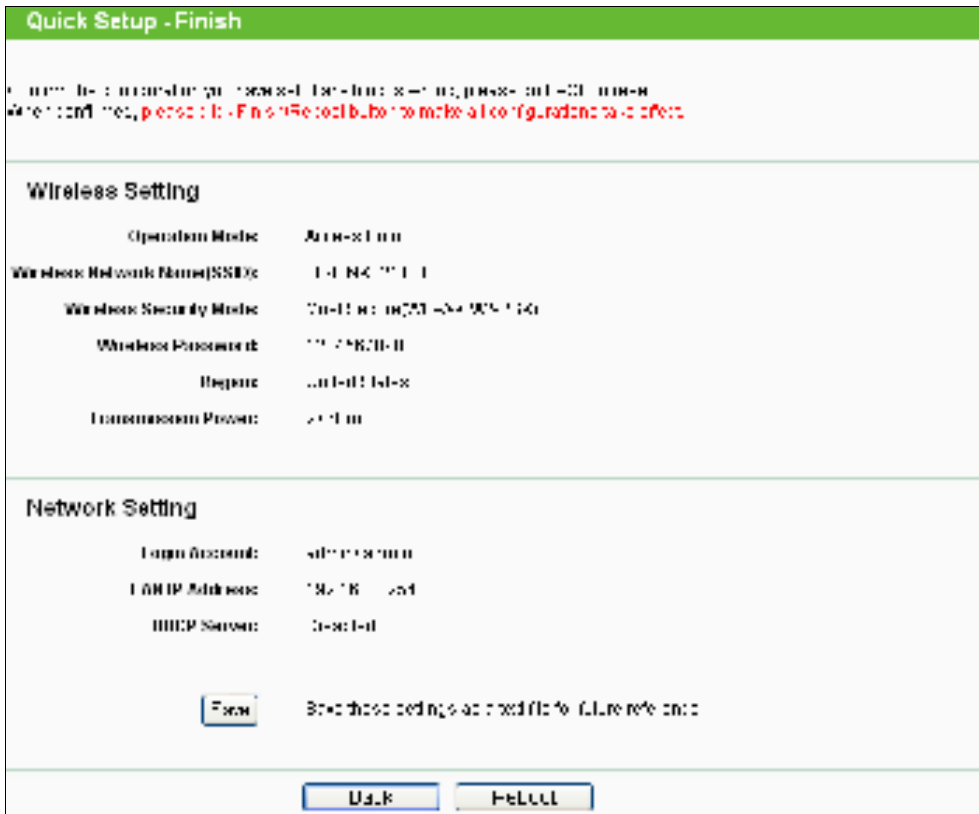


Figure 3-24 Finish page

3.2.4 Multi-SSID

When you choose **Multi-SSID** on **Operation Mode** page in Figure 3-7, take the following steps:

1. Click **Next** in Figure 3-7, and then **Wireless** page will appear as shown in Figure 3-25. Select **Enable VLAN**. Create different SSIDs and enter the password separately for your VLANs depending on the security requirements for your wireless networks. Click **Save** button to make each configuration take effect. Click **Next** to continue.

Note:

The operating distance or range of your wireless connection varies significantly based on the physical placement of the Device. For best results, place your Device

- Near the center of the area in which your wireless stations will operate.
- In an elevated location such as a high shelf.
- Away from the potential sources of interference, such as PCs, microwaves, and cordless phones.
- With the Antenna in the upright position.
- Away from large metal surfaces.

Failure to follow these guidelines can result in significant performance degradation or inability to wirelessly connect to the Device.

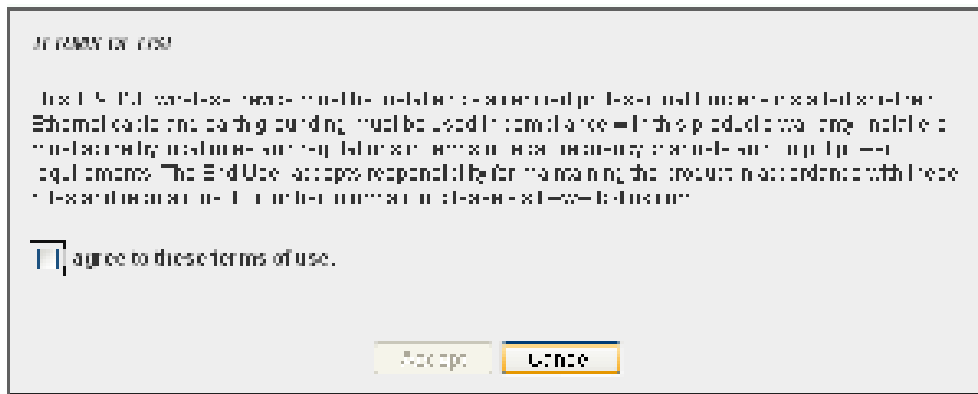
The screenshot shows the 'Quick Setup - Wireless' configuration page. At the top, there is a green header with the text 'Quick Setup - Wireless'. Below the header, there is a section for 'Enable VLAN' with a checkbox. Underneath, there are four rows for configuring SSIDs and VLAN IDs. The first row is for SSID1, and the others are for SSID2, SSID3, and SSID4. Each row has a text input field for the SSID and a dropdown menu for the VLAN ID. Below this section, there is a 'Region' dropdown menu set to 'United States'. A 'Warning' message is displayed, stating 'Ensure you select a correct country to comply local law. Incorrect settings may cause interference.' Below the warning, there is a 'Transmission Power' dropdown menu set to '27 dBm'. The next section is for 'Wireless Security Mode', with a dropdown menu set to 'Most Secure(WPA/WPA2-PSK)'. Below this, there is a 'Wireless Password' text input field. A 'Save' button is located at the bottom of the form. Below the 'Save' button, there are 'Back' and 'Next' buttons.

Figure 3-25 Wireless

- **Enable VLAN** - **ON** or **OFF** the VLAN function. The AP supports up to 4 VLANs. All wireless PCs in the VLANs are able to access this AP. The AP can also work with an IEEE 802.1Q Tag VLAN supporting Switch. If this Switch enables the Tag VLAN function, besides all wireless PCs, only the PCs in the VLAN same with SSID1 are able to access the AP. If a PC is directly connected to the LAN port of the AP, please make sure that its adapter supports Tag function, or this PC will not be able to access the AP.
- **SSID** - Enter a value of up to 32 characters. The same Name (SSID) must be assigned to all wireless devices in your network. In Multi-SSID operation mode, enter SSID for each BSS in the field "SSID1" ~ "SSID4".

- **VLAN ID** - The ID of a VLAN. Only in the same VLAN can a Wireless PC and a wired PC communicate with each other. The value can be between 1 and 4095. If the VLAN function is enabled, when AP forwards packets, the packets out from the LAN port will be added with an IEEE 802.1Q VLAN Tag, whose VLAN ID is just the ID of the VLAN where the sender belongs.
- **Region** - Select your region from the pull-down list. This field specifies the region where the wireless function of the AP can be used. It may be illegal to use the wireless function of the AP 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, the Note Dialog of **TERMS OF USE** will pop up. Select **I agree to these terms of use**, and click **Accept** to continue.



Note Dialog

Note:

Ensure you select a correct country to comply with local laws. Incorrect settings may cause interference.

- **Transmission Power** - The available options of transmission power are determined by the region selected.
 - **Wireless Security Mode** - You can select one of the following security options:
 - **WPA/WPA2-PSK** - Select WPA based on pre-shared passphrase.
 - **No Security** - The wireless security function is disabled. The wireless stations will be able to connect the Device without encryption.
 - **Wireless Password** - If the AP your Device is going to connect needs password, you need to fill the password in this blank.
 - **Save** - Save the current security configurations for the selected SSID.
2. The Network Setting page will appear then. It is recommended that you keep the default settings on this page. Click **Next**.

Quick Setup - Network

DHCP Server: Disable Enable
In most of the cases your root AP/Router has enabled DHCP server function, we highly recommend that you disable DHCP server function on this device to avoid any unpredictable problems.

IP Address: 192.168.0.254
Subnet Mask: 255.255.255.0
We recommend you configure this AP with the same IP subnet and subnet mask, but different IP address from your root AP/Router.

Change the login account: NO YES

Figure 3-26 Network

- When you finish the wireless setting in Figure 3-26 and click **Next**, then Figure 3-27 will appear, where you can click **Finish** button to complete the **Quick Setup**.

Quick Setup - Finish

Confirm the configuration you have set. Please click **Finish** to apply.
Minimum limit: 8 characters, 1-26/255 characters, must contain numbers and letters.

Wireless Setting

Operation Mode: WPA2-PSK

SSID1: TP-LINK_21_0_0
Wireless Security Mode: WPA2-PSK [WPA2-PSK]
Wireless Password: 1234567890

SSID2: TP-LINK_21_0_0_2
Wireless Security Mode: WPA2-PSK [WPA2-PSK]
Wireless Password: 1234567890

SSID3: Disabled
SSID4: Disabled

Region: United States
Transmission Power: 27dBm

Network Setting

Login Account: admin [admin]
LAN IP Address: 192.168.0.254
DHCP Server: Disabled

Figure 3-27 Finish page

3.2.5 Repeater (Range Extender)

When you choose **Repeater (Range Extender)** on **Operation Mode** page in Figure 3-7, take the following steps:

- Click **Next** in Figure 3-7, and then **Wireless** page will appear as shown in Figure 3-28. Click **Survey** button to scan the wireless networks.

Quick Setup - Wireless

Repeater Mode: Universal Repeater WDS Repeater

Wireless Name of Root AP: (also called SSID)

MAC Address of Root AP:

Click Survey button to scan the wireless networks, and choose the target one to setup.

Region:

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

Transmission Power:

Wireless Security Mode:

All security settings, for example the wireless password should match the root AP/router.

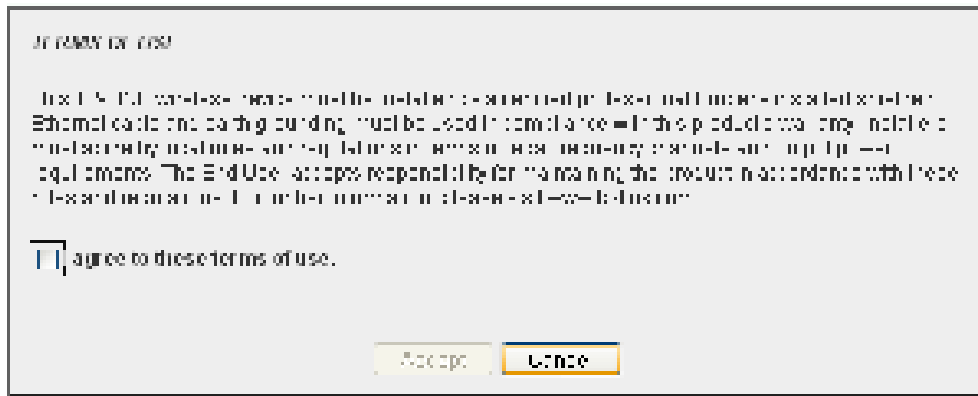
Wireless Password:

You can enter ASCII characters between 8 and 63 or Hexadecimal characters between 8 and 64.

Figure 3-28 Wireless

- **Repeater Mode** - Choose mode for repeater.
 - **WDS Repeater** - In WDS Repeater mode, the AP with WDS enabled will relays data to an associated root AP. AP function is enabled meanwhile. The wireless repeater relays signal between its stations and the root AP for greater wireless range. Please input the MAC address of root AP in the field "**MAC of AP**".
 - **Universal Repeater** - In Universal Repeater mode, the AP with WDS disabled will relays data to an associated root AP. AP function is enabled meanwhile. The wireless repeater relays signal between its stations and the root AP for greater wireless range. Please input the MAC address of root AP in the field "**MAC of AP**".
- **Wireless Name of Root AP** - The SSID of the AP your Device is going to connect to as a client. You can also use the survey function to select the SSID to join.
- **MAC Address of Root AP** - The Mac Address of the AP your Device is going to connect to as a client. You can also use the survey function to select the BSSID to join.
- **Survey** - Click this button, you can search the APs.
- **Region** - Select your region from the pull-down list. This field specifies the region where the wireless function of the AP can be used. It may be illegal to use the wireless function of the AP in a region other than one of those specified in this filed. 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, the Note Dialog of **TERMS OF USE** will pop up. Select **I agree to these terms of use**, and click **Accept** to continue.



Note Dialog

Note:

Ensure you select a correct country to comply with local laws. Incorrect settings may cause interference.

- **Transmission Power** - The available options of transmission power are determined by the region selected.
- **Wireless Security Mode** - You can select one of the following security options:
 - **WPA/WPA2-PSK** - Select WPA based on pre-shared passphrase.
 - **WEP** - Select WEP based on none pre-shared passphrase.
 - **No Security** - The wireless security function is disabled. The wireless stations will be able to connect the Device without encryption.
- **Auth Type** - This option should be chosen if the Security Mode is WEP. It indicates the authorization type of the Root AP.
- **Key Format** - This option should be chosen if the Security Mode is WEP. It indicates the format of the WEP key.
- **WEP Index** - This option should be chosen if the Security Mode is WEP. It indicates the index of the WEP key.
- **Wireless Password** - If the AP your Device is going to connect needs password, you need to fill the password in this blank.

Note:

The operating distance or range of your wireless connection varies significantly based on the physical placement of the Device. For best results, place your Device

- Near the center of the area in which your wireless stations will operate.
- In an elevated location such as a high shelf.
- Away from the potential sources of interference, such as PCs, microwaves, and cordless phones.
- With the Antenna in the upright position.
- Away from large metal surfaces.

Failure to follow these guidelines can result in significant performance degradation or inability to wirelessly connect to the Device.

2. The AP List page will appear shown as Figure 3-29. Find the BSSID (the same as the MAC address) of the remote AP that you want to repeat, and then click **Connect** on the right side of the line.

ID	BSSID	SSID	Signal	Channel	Security	Connect
1	23 23 23 23 23 23		20dB		OFF	Connect
2	14 E6 E4 D7 1C EC	TP-LINK_2.4G-2_D71CE0	138dB		WPA/WPA2 PSK	Connect
3	D8 9C 41 4C 17 D4	TP-LINK_40 71A	0dB		OFF	Connect
4	4C F3 C 97 E8 39	TP-LINK_7982C	13dB		OFF	Connect
5	1E E6 E4 D7 1C EC	TP-LINK_2.4G-2_D71CE0	0dB		OFF	Connect
6	EC 7 3F 74 33 28		94dB	4	OFF	Connect
7	0C 1C 0F 0 9C 94		92dB	4	OFF	Connect
8	94 01 6C 2F 31 EE	TP-LINK_network	84dB	4	WPA/WPA2 PSK	Connect
9	14 E6 E4 E9 87 5A		13dB	1	WPA/WPA2 PSK	Connect
0	4C F3 C 9C 27 31	TP-LINK_39373C	9 dB	1	OFF	Connect
1	14 E6 E4 E9 4E 8C	TP-LINK	92dB	1	WPA/WPA2 PSK	Connect

Figure 3-29 AP List

You will then return to the Wireless page as shown in Figure 3-28. The security mode will be selected automatically, please confirm it and enter the same password as is on your router or access point, then click **Next**.

- The Network Setting page will appear then. It is recommended that you keep the default settings on this page. Click **Next**.

Quick Setup - Network

DHCP Server: Disable Enable
In most of the cases your root AP/router has enabled DHCP server function, we highly recommend that you disable DHCP server function on this device to avoid any unpredictable problems.

IP Address:
Subnet Mask:
We recommend you configure this AP with the same IP subnet and subnet mask, but different IP address from your root AP/router.

Change the login account: NO YES

Figure 3-30 Network

- When you finish the wireless setting in Figure 3-30 and click **Next**, then Figure 3-31 will appear, where you can click **Finish** button to complete the **Quick Setup**.

Quick Setup - Finish

Confirm the configuration you have set. Proceeding to saving. Please go Back to avoid
 Mis-configuration. Please refer to the manual for more details. [Mis-configuration](#)

Wireless Setting

Operation Mode: Uplink Repeater
 Wireless Name of Root AP: TP-LINK_20408
 MAC Address of Root AP: 00:0E:EE:13:34:4E
 Wireless Security Mode: Most Secure(WPA/WPA2-PSK)
 Wireless Password: 1234567890
 Region: United States
 Transmission Power: 27dBm

Network Setting

Login Account: admin@tplink.com
 LAN IP Address: 192.168.0.254
 DHCP Server: Disabled

[192.168.0.254](#) [192.168.0.254](#) [192.168.0.254](#)

Figure 3-31 Finish page

3.2.6 Bridge with AP

When you choose **Bridge with AP** on **Operation Mode** page in Figure 3-7, take the following steps:

1. Click **Next** in Figure 3-7, and then **Wireless** page will appear as shown in Figure 3-32. Click **Survey** button to scan the wireless networks.

Quick Setup - Wireless Bridge Setting

Wireless Name of Remote AP: (also called SSID)
 MAC Address of Remote AP:

 Click Survey button to scan the wireless networks, and choose the target one to setup.

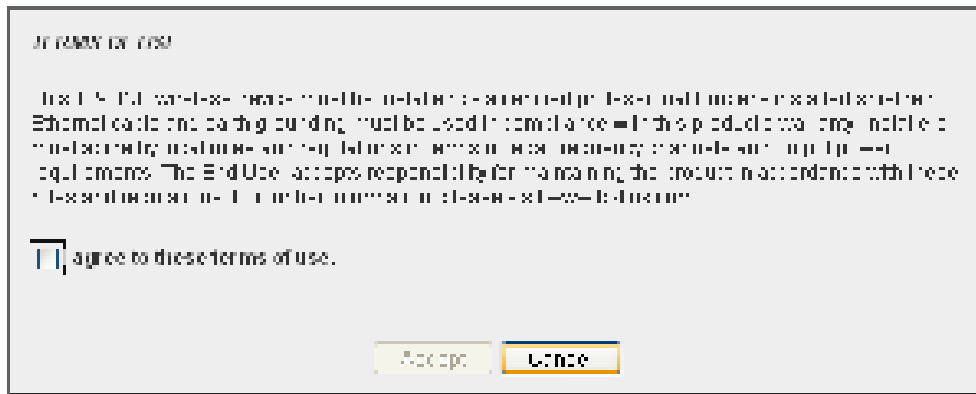
Region: United States
 Warning: Ensure you select a correct country to comply local law. Incorrect settings may cause interference.
 Transmission Power: 27 dBm
 Channel: 1
 Wireless Security Mode: Most Secure(WPA/WPA2-PSK)
 Wireless Password:
 All security settings, for example the wireless password should match the root AP's login.
 You can enter ASCII characters between ! and @ or hexadecimal characters between 0 and FF.

Figure 3-32 Wireless Bridge Setting

- **Wireless Name of Remote AP** - The SSID of the AP your Device is going to connect to as a client. You can also use the survey function to select the SSID to join.

- **Mac Address of Remote AP:** - The Mac Address of the AP your Device is going to connect to as a client. You can also use the survey function to select the BSSID to join.
- **Survey** - Click this button, you can search the APs.
- **Region** - Select your region from the pull-down list. This field specifies the region where the wireless function of the Router can be used. It may be illegal to use the wireless function of the Router in a region other than one of those specified in this field. If your country or region is not listed, please contact your local government agency for assistance.

When you select your local region from the pull-down list, the Note Dialog of **TERMS OF USE** will pop up. Select **I agree to these terms of use**, and click **Accept** to continue.



Note Dialog

Note:

Ensure you select a correct country to comply with local laws. Incorrect settings may cause interference.

- **Transmission Power** - The available options of transmission power are determined by the region selected.
- **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.
- **Wireless Security Mode** - This option should be chosen according to the AP's security configuration. It is recommended that the security type is the same as your AP's security type.
 - **WPA/WPA2-PSK** - Select WPA based on pre-shared passphrase.
 - **WEP** - Select WEP based on none pre-shared passphrase.
 - **No Security** - The wireless security function is disabled. The wireless stations will be able to connect the Device without encryption.
- **Auth Type** - This option should be chosen if the Security Mode is WEP. It indicates the authorization type of the Root AP.
- **Key Format** - This option should be chosen if the Security Mode is WEP. It indicates the format of the WEP key.
- **WEP Index** - This option should be chosen if the Security Mode is WEP. It indicates the index of the WEP key.
- **Wireless Password** - If the AP your Device is going to connect needs password, you need to fill the password in this blank.

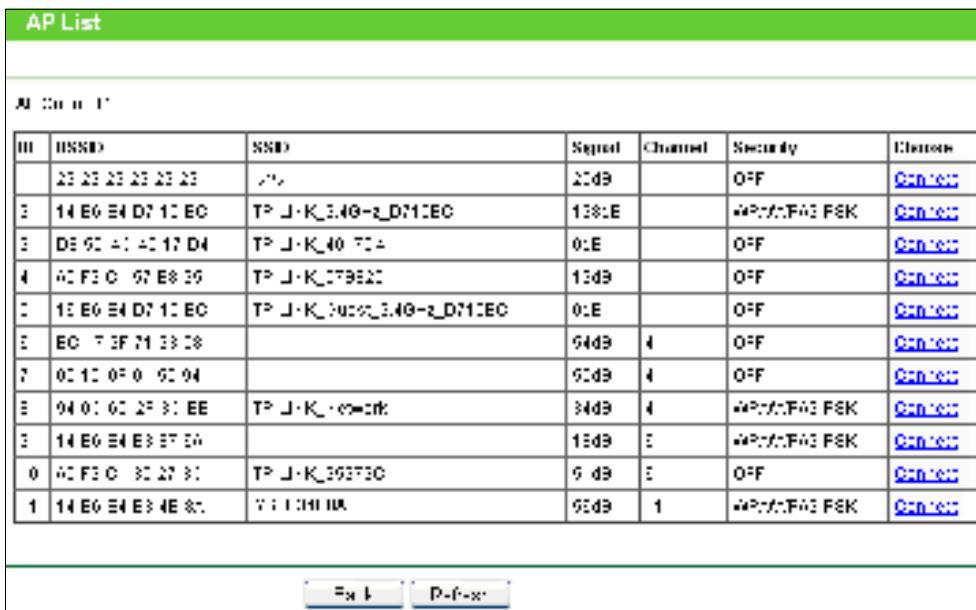
 **Note:**

The operating distance or range of your wireless connection varies significantly based on the physical placement of the Device. For best results, place your Device

- Near the center of the area in which your wireless stations will operate.
- In an elevated location such as a high shelf.
- Away from the potential sources of interference, such as PCs, microwaves, and cordless phones.
- With the Antenna in the upright position.
- Away from large metal surfaces.

Failure to follow these guidelines can result in significant performance degradation or inability to wirelessly connect to the Device.

2. The AP List page will appear shown as Figure 3-33. Find the BSSID (the same as the MAC address) of the remote AP that you want to bridge, and then click **Connect** on the right side of the line.

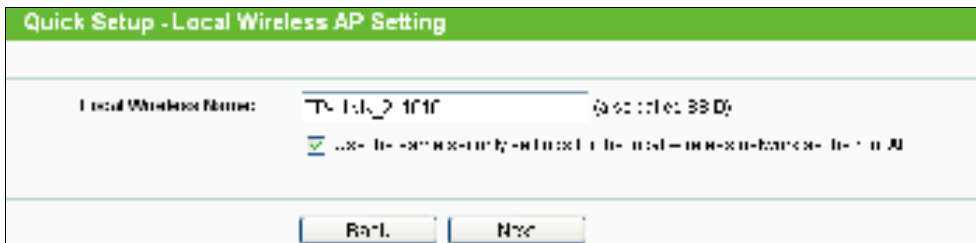


ID	BSSID	SSID	Signal	Channel	Security	Connect
	23 23 23 23 23 23		20dB		OFF	Connect
3	14 E6 E4 D7 1C EC	TP-LINK_3.4G-2_D71CE0	138dB		WPA:TKIP PSK	Connect
3	D8 9C 41 4C 17 D4	TP-LINK_40 70A	0dB		OFF	Connect
4	AC F3 C 97 E8 39	TP-LINK_07B522	13dB		OFF	Connect
2	12 E6 E4 D7 1C EC	TP-LINK_0002_3.4G-2_D71CE0	0dB		OFF	Connect
5	EC 7 3F 74 33 C8		94dB	4	OFF	Connect
7	0C 1C 0F 0 9C 94		92dB	4	OFF	Connect
3	94 01 6C 2F 31 EE	TP-LINK_000000	34dB	4	WPA:TKIP PSK	Connect
3	14 E6 E4 E3 37 56		13dB	1	WPA:TKIP PSK	Connect
0	AC F3 C 8C 27 31	TP-LINK_393730	9 dB	1	OFF	Connect
1	14 E6 E4 E3 4E 81	TP-LINK_000000	92dB	1	WPA:TKIP PSK	Connect

Figure 3-33 AP List

You will then return to the Wireless page as shown in Figure 3-32. The security mode will be selected automatically, please confirm it and enter the same password as is on your router or access point, then click **Next**.

3. Create a name for the Local Wireless Network. The security settings for the local network will be set the same as your root AP by default. Click **Next**.



Quick Setup - Local Wireless AP Setting

Local Wireless Name: (00:11:10:33:00)

WPA:TKIP PSK (Security Mode)

Figure 3-34 Local Wireless AP Setting

4. The Network Setting page will appear then. It is recommended that you keep the default settings on this page. Click **Next**.

Quick Setup - Network

DHCP Server: Disable Enable
In most of the cases your root AP/router has enabled DHCP server function, we highly recommend that you disable DHCP server function on this device to avoid any unpredictable problems.

IP Address:
Subnet Mask:
We recommend you configure this AP with the same IP subnet and subnet mask, but different IP address from your root AP/router.

Change the login account: NO YES

Figure 3-35 Network

- When you finish the wireless setting in Figure 3-35 and click **Next**, then Figure 3-36 will appear, where you can click **Finish** button to complete the **Quick Setup**.

Quick Setup - Finish

Click the **Finish** button to complete the configuration and save the settings.

Wireless Setting

Operation Mode	Factory Default
Wireless Name of Remote AP	TL-WA7210N
MAC Address of Remote AP	00:00:00:00:00:00
Wireless Security Mode	WPA-PSK (TKIP)
Wireless Password	1234567890
Local Wireless Name (SSID)	TL-WA7210N
Wireless Channel	1
Wireless Security Mode	WPA-PSK (TKIP)
Wireless Password	1234567890
Region	China
Transmission Power	High

Network Setting

Login Account	admin
LAN IP Address	192.168.0.254
DHCP Server	Disable

Click the **Finish** button to complete the configuration and save the settings.

Figure 3-36 Finish page

3.2.7 Client

When you choose **Client** on **Operation Mode** page in Figure 3-7, take the following steps:

1. Click **Next** in Figure 3-7, and then **Wireless** page will appear as shown in Figure 3-37. Click **Survey** button to scan the wireless networks.

Figure 3-37 Wireless

- **Wireless Name of Remote AP** - The SSID of the AP your Device is going to connect to as a client. You can also use the survey function to select the SSID to join.
- **Mac Address of Remote AP:** - The Mac Address of the AP your Device is going to connect to as a client. You can also use the survey function to select the BSSID to join.
- **Survey** - Click this button, you can search the APs.
- **Region** - Select your region from the pull-down list. This field specifies the region where the wireless function of the Router can be used. It may be illegal to use the wireless function of the Router in a region other than one of those specified in this filed. 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, the Note Dialog of **TERMS OF USE** will pop up. Select **I agree to these terms of use**, and click **Accept** to continue.

Note Dialog

Note:

Ensure you select a correct country to comply with local laws. Incorrect settings may cause interference.

- **Transmission Power** - The available options of transmission power are determined by the region selected.
- **Wireless Security Mode** - This option should be chosen according to the AP's security configuration. It is recommended that the security type is the same as your AP's security type.
 - **WPA/WPA2-PSK** - Select WPA based on pre-shared passphrase.
 - **WEP** - Select WEP based on none pre-shared passphrase.
 - **No Security** - The wireless security function is disabled. The wireless stations will be able to connect the Device without encryption.
- **Auth Type** - This option should be chosen if the Security Mode is WEP. It indicates the authorization type of the Root AP.
- **Key Format** - This option should be chosen if the Security Mode is WEP. It indicates the format of the WEP key.
- **WEP Index** - This option should be chosen if the Security Mode is WEP. It indicates the index of the WEP key.
- **Wireless Password** - If the AP your Device is going to connect needs password, you need to fill the password in this blank.

Note:

The operating distance or range of your wireless connection varies significantly based on the physical placement of the Device. For best results, place your Device

- Near the center of the area in which your wireless stations will operate.
- In an elevated location such as a high shelf.
- Away from the potential sources of interference, such as PCs, microwaves, and cordless phones.
- With the Antenna in the upright position.
- Away from large metal surfaces.

Failure to follow these guidelines can result in significant performance degradation or inability to wirelessly connect to the Device.

2. The AP List page will appear shown as Figure 3-38. Find the BSSID (the same as the MAC address) of the remote AP that you want to repeat, and then click **Connect** on the right side of the line.

AP List						
Id	BSSID	SSID	Signal	Channel	Security	Connect
	23 23 23 23 23 23		20dB		OFF	Connect
3	14 E6 E4 D7 1C EC	TP-LINK_3.4G-2_D71CEC	138dB		WPA/WPA2 PSK	Connect
3	D8 9C 41 42 17 D4	TP-LINK_40 724	0dB		OFF	Connect
4	42 F3 C 97 E8 39	TP-LINK_079E27	13dB		OFF	Connect
5	12 E6 E4 D7 1C EC	TP-LINK_3.4G-2_D71CEC	0dB		OFF	Connect
5	EC 73F 71 33 28		94dB	4	OFF	Connect
7	02 12 0F 0 92 94		92dB	4	OFF	Connect
8	94 01 62 2F 31 EE	TP-LINK_00=ink	34dB	4	WPA/WPA2 PSK	Connect
8	14 E6 E4 E3 37 3A		15dB	1	WPA/WPA2 PSK	Connect
0	42 F3 C 82 27 31	TP-LINK_36373C	9 dB	1	OFF	Connect
1	14 E6 E4 E3 4E 8C	TP-LINK_10A	95dB	1	WPA/WPA2 PSK	Connect

Figure 3-38 AP List

You will then return to the Wireless page as shown in Figure 3-37. The security mode will be selected automatically, please confirm it and enter the same password as is on your router or access point, then click **Next**.

3. The Network Setting page will appear then. It is recommended that you keep the default settings on this page. Click **Next**.

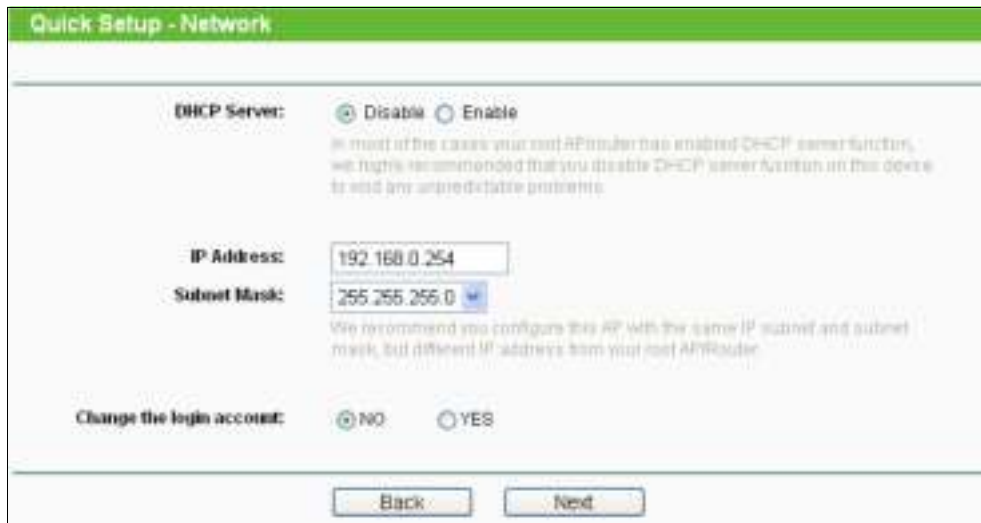


Figure 3-39 Network

4. When you finish the wireless setting in Figure 3-30 and click **Next**, then Figure 3-31 will appear, where you can click **Finish** button to complete the **Quick Setup**.

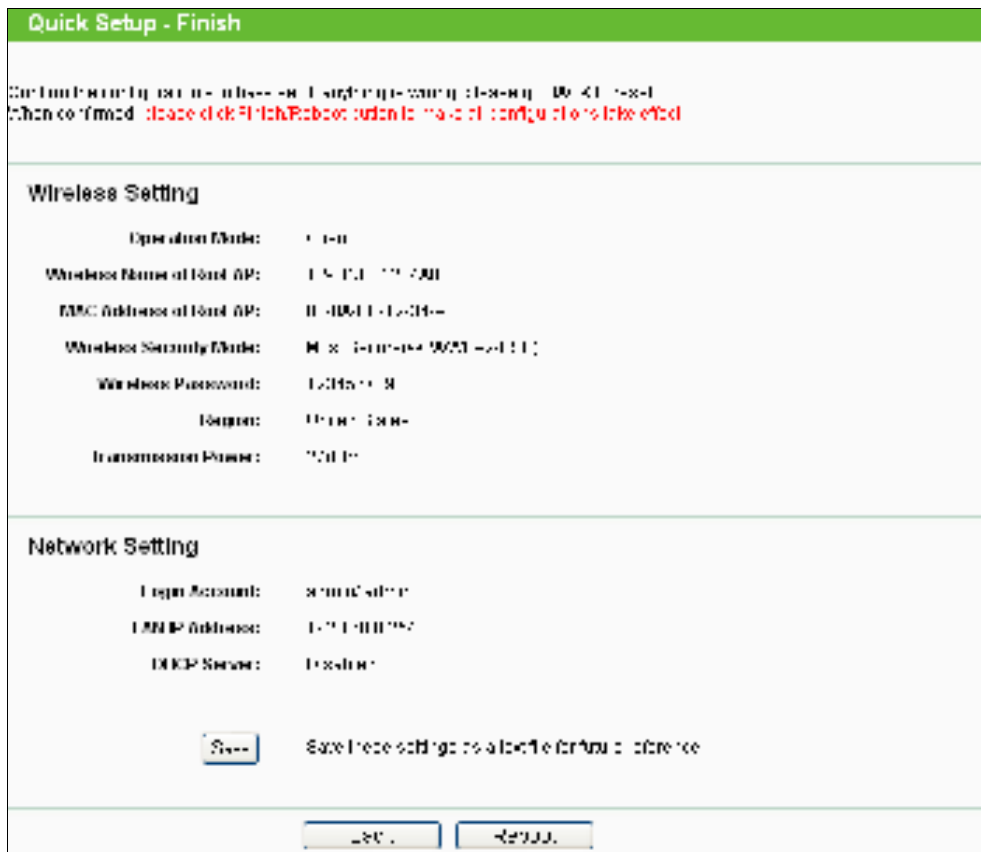
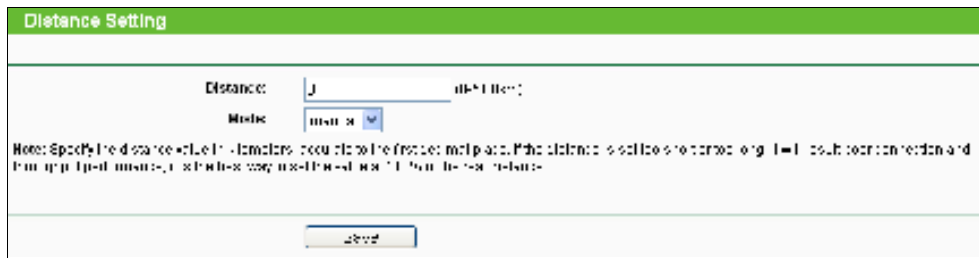


Figure 3-40 Finish page

Note:

If the wireless connection is poor after basic configuration of operation mode, please select **Wireless > Distance Setting**, and set the outdoor distance value at 110% of the real distance as shown in Figure 3-41. It will help you stabilize outdoor links.



The screenshot shows a web interface titled "Distance Setting". It features a "Distance:" input field with the value "1" and a "Unit:" dropdown menu with "meter" selected. Below the input fields is a note: "Note: Specify the distance value in kilometers, kilometers, meters, millimeters. The distance is set to 100% by default. For application, you may use the value of 110% to stabilize links." At the bottom of the form is a "Save" button.

Figure 3-41 Distance Setting

Chapter 4. AP & Multi-SSID & Repeater (Range Extender) & Bridge with AP & Client Operation Mode

This Chapter describes how to configure some advanced settings for your Access Point through the web-based management page in standard AP operation mode including AP, Multi-SSID, Repeater (Range Extender), Bridge with AP and Client mode. In the following explanations, we will take the device in Access Point operation mode for example.

4.1 Login

After your successful login, you can configure and manage the Access Point. There are eight main menus on the left of the Web-based management page. Submenus will be available after you click one of the main menus. The eight main menus are: **Status**, **Quick Setup**, **Operation Mode**, **WPS**, **Network**, **Wireless**, **DHCP** 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:	3.01 Build 201008163844	
Hardware Version:	V072 0-1202020202	
Wired		
MAC Address:	14-72-031-0-0	
IP Address:	93.68.0.294	
Subnet Mask:	255.255.255.0	
Wireless		
Operation Mode:	Access Point	
Name (SSID):	TL-WA7210N	
Channel:	Auto (Current Channel)	
Mode:	11g/n/b/g	
Channel Width:	Auto (40MHz)	
MAC Address:	14-72-031-0-0	
Traffic Statistics		
	Received	Sent
Bytes:	0	80/20
Packets:	0	2/0
System Up Time:	2 days 02: 04: 42	
		Refresh

Figure 4-1 Status

1. Wired

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 **Operation Mode**, **Name (SSID)**, **Channel**, **Mode**, **Channel Width** and **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 seven operation mode types, **AP Client Router**, **AP Router**, **Access Point**, **Multi-SSID**, **Repeater (Range Extender)**, **Bridge with AP** and **Client**. Please select the one you want as shown in Figure 4-2. Click **Save** to save your choice.



Figure 4-2 Operation Mode

- **AP Client Router** - In this mode, the device enables multi-users to share Internet from WISP. The LAN port devices share the same IP from WISP through Wireless port. While connecting to WISP, the Wireless port works as a WAN port at AP Client Router mode. The Ethernet port acts as a LAN port.

- **AP Router** - In this mode, the device enables multi-users to share Internet via ADSL/Cable Modem. The wireless port share the same IP to ISP through Ethernet WAN port. The Wireless port acts the same as a LAN port while at AP Router mode.
- **Access Point** - In this mode, the device can be connected to a wired network and transform the wired access into wireless that multiple devices can share together, especially for a home, office or hotel where only wired network is available.
- **Multi-SSID** - In this mode, the device can create up to 4 wireless networks labeled with different SSIDs and assign each SSID with different security or VLAN, especially for the situation when the various access policies and functions are required.
- **Repeater(Range Extender)** - In this mode, the device can copy and reinforce the existing wireless signal to extend the coverage of the signal, especially for a large space to eliminate signal-blind corners.
- **Bridge with AP** - In this mode, the device can be used to combine multiple local networks together to the same one via wireless connections, especially for a home or office where separated networks can't be connected easily together with a cable.
- **Client** - In this mode, the device can be connected to another device via Ethernet port and act as an adaptor to grant your wired devices access to a wireless network, especially for a Smart TV, Media Player, or game console only with an Ethernet port.

 **Note:**

When you change the operation mode to Client/Repeater, WPS function will stay disabled. Please manually enable this function if needed when you switch back to Access Point/Multi-SSID/Bridge mode.

4.5 WPS

Choose **WPS** in the main menu, you will see the page as shown in Figure 4-3. The WPS function is disabled and cannot be configured in the standard AP mode.

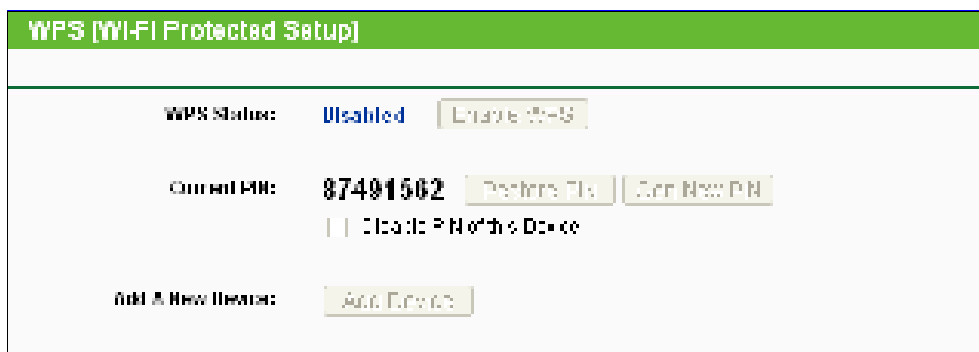


Figure 4-3 WPS

- **Selected SSID** - If Multi-SSID is enabled, you can choose one of the SSIDs from the pull-down list.

- **WPS Status** - Enable or disable the WPS function here.
- **Current PIN** - The current value of the device's PIN displayed here. The default PIN of the device can be found in the label or User Guide.
- **Restore PIN** - Restore the PIN of the device to its default.
- **Gen New PIN** - Click this button, and then you can get a new random value for the device's PIN. You can ensure the network security by generating a new PIN.
- **Disable PIN of this Device** - WPS external registrar of entering the device's PIN can be disabled or enabled manually. If the device receives multiple failed attempts to authenticate an external Registrar, this function will be disabled automatically.
- **Add Device** - You can add the new device to the existing network manually by clicking this button.

4.6 Network

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



Figure 4-4 the Network menu

4.6.1 LAN

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

Figure 4-5 LAN

- **MAC Address** - The physical address of the router, as seen from the LAN. The value can't

be changed.

- **Type** - Choosing dynamic IP to get IP address from DHCP server, or choosing static IP to configure IP address manually.
- **IP Address** - Enter the IP address of your router in dotted-decimal notation (factory default: 192.168.0.254).
- **Subnet Mask** - An address code that determines the size of the network. Normally use 255.255.255.0 as the subnet mask.
- **Gateway** - The gateway should be in the same subnet as your IP address.

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

4.7 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 4-6): **Wireless Settings**, **Wireless Security**, **Wireless MAC Filtering**, **Wireless Advanced**, **Antenna Alignment**, **Distance Setting**, **Throughput Monitor** and **Wireless Statistics**. Click any of them, and you will be able to configure the corresponding function. The detailed explanations for each submenu are provided below.



Figure 4-6 Wireless menu

4.7.1 Wireless Settings

Selecting **Wireless > Wireless Settings** will enable you to configure the basic settings for your wireless network on the screen below (Figure 4-7).

Figure 4-7 Wireless Settings in AP Client Router mode

- **Wireless Network Name** - 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 (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, the Note Dialog of **TERMS OF USE** will pop up. Select **I agree to these terms of use**, and click **Accept** to continue.

Note Dialog

Note:

Ensure you select a correct country to comply with local laws. Incorrect settings may cause interference.

- **Transmission Power** - The available options of transmission power are determined by the region selected.

- **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** - This field determines the wireless mode which the AP works on. The options includes: 11b only, 11g only, 11n only, 11bg mixed, 11bgn mixed.
- **Channel Width** - The bandwidth of the wireless channel.
- **Enable Wireless Radio** - The wireless radio of the AP can be enabled or disabled to allow or deny wireless stations to access. If enabled, the wireless stations will be able to access the AP, otherwise, wireless stations will not be able to access the AP.
- **Enable SSID Broadcast** - If you select the **Enable SSID Broadcast** checkbox, the AP will broadcast its name (SSID) on the air.

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.

4.7.2 Wireless Security

Selecting **Wireless > Wireless Security** will enable you to configure the security of the wireless network for your device on the page as shown in Figure 4-8.

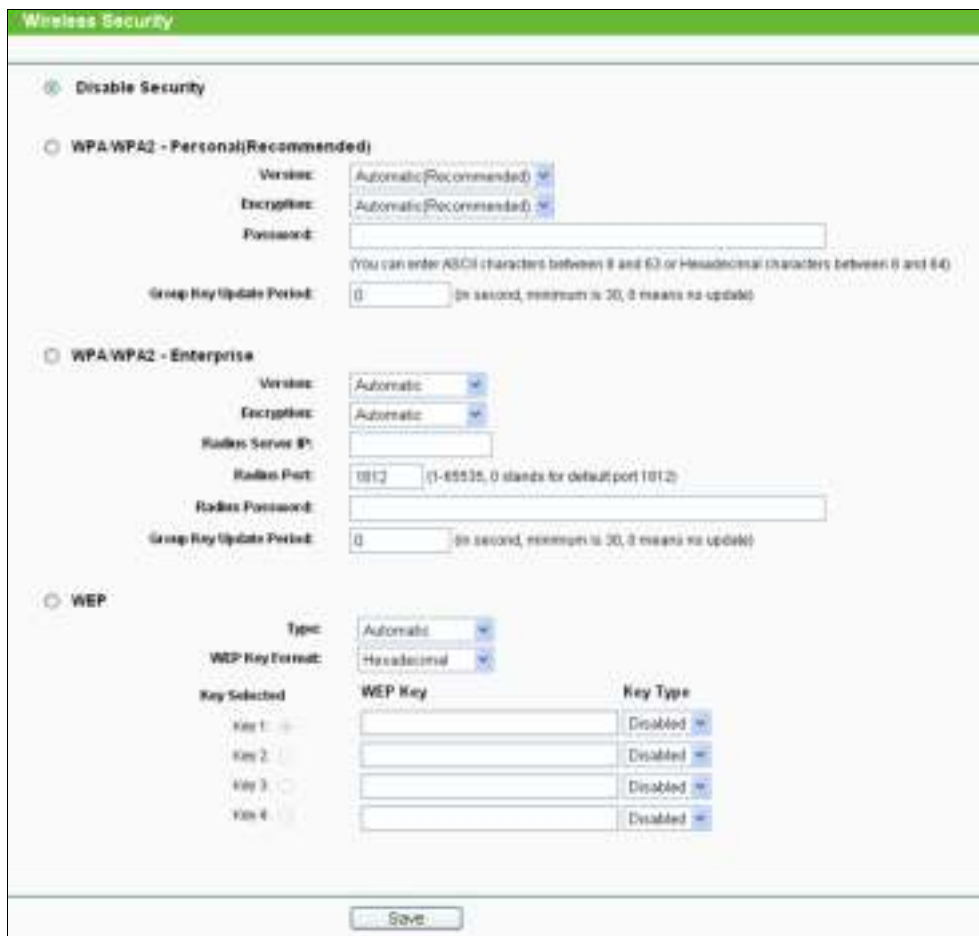


Figure 4-8 Wireless Security

- **Selected SSID:** If Multi-SSID is enabled, you can choose one of the SSIDs from the pull-down list.

- **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.
- **WPA/WPA2-Personal** - Select WPA based on Radius Server.
- **WPA/WPA2-Enterprise** - Select WPA based on pre-shared passphrase.
- **WEP** - Select 802.11 WEP security.

Each security option has its own settings as described below:

WPA/WPA2 – Personal (Recommended)

- **WEP** - Select 802.11 WEP security.
- **Version** - You can select one of following versions:
 - **Automatic** - Select **WPA-Personal** or **WPA2-Personal** automatically based on the wireless station's capability and request.
 - **WPA-Personal** - Pre-shared key of WPA.
 - **WPA2-Personal** - Pre-shared key of WPA2.
- **Encryption** - You can select either **Automatic**, or **TKIP** or **AES**.
- **Password** - You can enter **ASCII** or **Hexadecimal** characters. For **Hexadecimal**, the length should be between 8 and 64 characters; for **ASCII**, the length should be between 8 and 63 characters.
- **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/WPA2 - Enterprise

- **WEP** - Select 802.11 WEP security.
- **Version** - You can select one of following versions:

- **Automatic** - Select **WPA** or **WPA2** automatically based on the wireless station's capability and request.
- **WPA** - Wi-Fi Protected Access.
- **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 uses.
- **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.

WEP

- **Type** - You can select one of following types:
 - **Automatic** - Select **Shared Key** or **Open System** authentication type automatically based on the wireless station's capability and request.
 - **Open System** - Select 802.11 Open System authentication.
 - **Shared Key** - Select 802.11 Shared Key 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 settings** - Select which of the four keys will be used and enter the matching WEP key information for your network in the selected key radio button. These values must be identical on all wireless stations in your network.
- **Key Type** - You can select the WEP key length (**64-bit**, or **128-bit**, or **152-bit**.) for encryption. "Disabled" means this WEP key entry is invalid.
 - For **64-bit** encryption - You can enter 10 hexadecimal digits (any combination of 0-9, a-f, A-F, and null key is not permitted) or 5 ASCII characters.
 - For **128-bit** encryption - You can enter 26 hexadecimal digits (any combination of 0-9, a-f, A-F, and null key is not permitted) or 13 ASCII characters.
 - For **152-bit** encryption - You can enter 32 hexadecimal digits (any combination of 0-9, a-f, A-F, and null 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.

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

4.7.3 Wireless MAC Filtering

Selecting **Wireless > Wireless MAC Filtering** will allow you to set up some filtering rules to control wireless stations accessing the device, which depend on the station's MAC address on the following screen as shown Figure 4-9.

Figure 4-9 Wireless MAC address Filtering

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

- **Selected SSID** - If Multi-SSID is enabled, you can choose one of the SSIDs from the pull-down list.

- **MAC Address** - The wireless station's MAC address that you want to access.
- **Status** - The status of this entry either **Enabled** or **Disabled**.
- **Description** - A simple description of the wireless station.
- **Modify** - Here you can modify or delete an existing rule.

To disable the Wireless MAC Address Filters feature, keep the default setting, **Disable**.

To set up an entry, click **Enable**, and follow these instructions:

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

To Add a Wireless MAC Address filtering entry, clicking the **Add New...** button, and following these instructions: The “**Add or Modify Wireless MAC Address Filtering entry**” page will appear, shown in Figure 4-10.

Figure 4-10 Add or Modify Wireless MAC Address Filtering entry

1. Enter the appropriate MAC Address into the **MAC Address** field. The format of the MAC Address is XX-XX-XX-XX-XX-XX (X is any hexadecimal digit). For example, 00-0A-EB-B0-00-0B.
2. Enter a simple description of the wireless station in the **Description** field. For example, Wireless station A.
3. **Status** - Select **Enabled** or **Disabled** for this entry on the **Status** pull-down list.
4. Click the **Save** button to save this entry.

To add another entries, repeat steps 1~4.

To modify or delete an existing entry:

1. Click the **Modify** or **Delete** button in the **modify** column in the MAC Address Filtering Table.
2. Enter the value as desired in the **Add or Modify Wireless MAC Address Filtering entry** page, and click the **Save** button.

You can click the **Enable All** button to make all the Entries enabled, click the **Disable All** button to make all the Entries disabled, click the **Delete All** button to delete all the entries.

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

Note: If you enable the function and select the **Allow the stations specified by any enabled entries in the list to access** for **Filtering Rules**, and there are not any enable entries in the list, thus, no wireless stations can access the AP.

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

1. Click the **Enable** button to enable this function.
2. Select the radio button: **Allow the stations specified by any enabled entries in the list to access** for **Filtering Rules**.
3. Delete all or disable all entries if there are any entries already.
4. Click the **Add New...** button and enter the MAC address 00-0A-EB-00-07-BE in the **MAC Address** field, enter wireless station A in the **Description** field and select **Enabled** in the **Status** pull-down list. Click the **Save** button.
5. Click the **Add New...** button and enter the MAC address 00-0A-EB-00-07-5F in the **MAC Address** field, enter wireless station B in the **Description** field and select **Disabled** in the **Status** pull-down list. Click the **Save** button.

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

ID	MAC Address	Status	Description	Modify
1	00-0A-EE-00-07-EE	Enabled	wireless station A	Modify Delete
2	00-0A-EE-00-07-5F	Disabled	wireless station B	Modify Delete

Note:

- 1) If you select the radio button **Deny the stations specified by any enabled entries in the list to access** for **Filtering Rules**, the wireless station B will still not be able to access the router, however, other wireless stations that are not in the list will be able to access the router.
- 2) If you enable the function and select the **Allow the stations specified by any enabled entries in the list to access** for **Filtering Rules**, and there are not any enable entries in the list, thus, no wireless stations can access the router.

4.7.4 Wireless Advanced

Selecting **Wireless > Wireless Advanced** will allow you to do some advanced settings for the device in the following screen as shown in Figure 4-11. As the configuration for each operation mode is almost the same, we take Access Point mode for example here.

Figure 4-11 Wireless Advanced

- **Antenna Settings** - The polarization of an antenna. You can select Vertical Antenna, Horizontal Antenna or External Antenna.
- **Beacon Interval** - The beacons are the packets sent by the Device to synchronize a wireless network. Beacon Interval value determines the time interval of the beacons. You can specify a value between 20-1000 milliseconds. The default value is 100.
- **RTS Threshold** - Here you can specify the RTS (Request to Send) Threshold. If the packet is larger than the specified RTS Threshold size, the Device will send RTS frames to a particular receiving station and negotiate the sending of a data frame. The default value is 2346.
- **Fragmentation Threshold** - This value is the maximum size determining whether packets will be fragmented. Setting the Fragmentation Threshold too low may result in poor network performance since excessive packets. 2346 is the default setting and is recommended.
- **DTIM Interval** - This value determines the interval of the Delivery Traffic Indication Message (DTIM). You can specify the value between 1-255 Beacon Intervals. The default value is 1, which indicates the DTIM Interval is the same as Beacon Interval.
- **Enable WMM** - WMM function can guarantee the packets with high-priority messages being transmitted preferentially. It is strongly recommended enabled.
- **Enable Short GI** - This function is recommended, for it will increase the data capacity by reducing the guard interval time.

- **Enable AP Isolation** - Isolate all connected wireless stations so that wireless stations cannot access each other through WLAN. This function will be disabled if WDS/Bridge is enabled.

Note:

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

4.7.5 Antenna Alignment

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

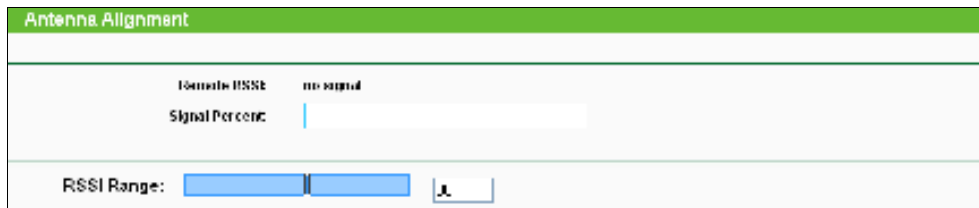


Figure 4-12 Antenna Alignment

- **Remote 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.

4.7.6 Distance Setting

Selecting **Wireless > Distance Setting** will allow you to adjust the wireless range in outdoor conditions as shown in Figure 4-13. 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.

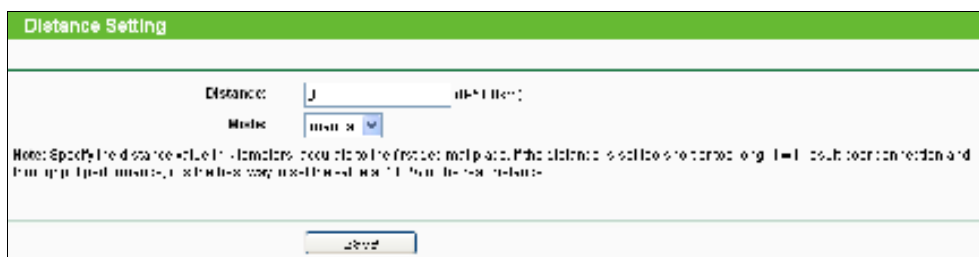


Figure 4-13 Distance Setting

- **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.

Note:

One hundred-meter is the smallest unit of this setting.

- **Mode** - You can select manual or indoor for the mode.

Click **Save** to keep your settings.

4.7.7 Throughput Monitor

Selecting **Wireless > Throughput Monitor** will help to watch wireless throughput information in the following screen shown in Figure 4-14.

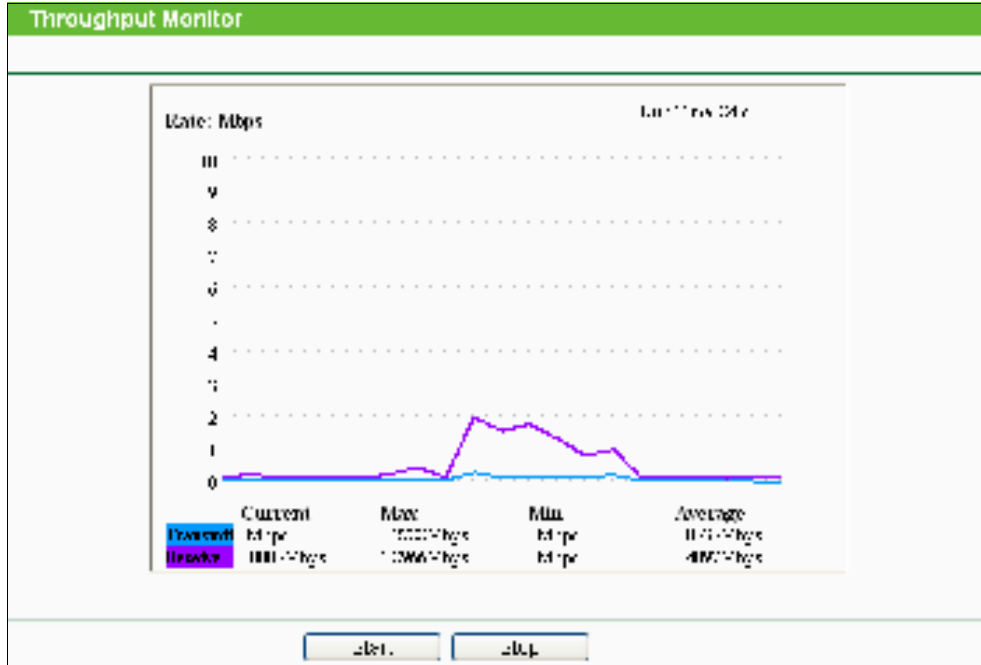


Figure 4-14 Wireless Throughput

- **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.

4.7.8 Wireless Statistics

Selecting **Wireless > Wireless Statistics** will allow you to see the wireless transmission information in the following screen shown in Figure 4-15.

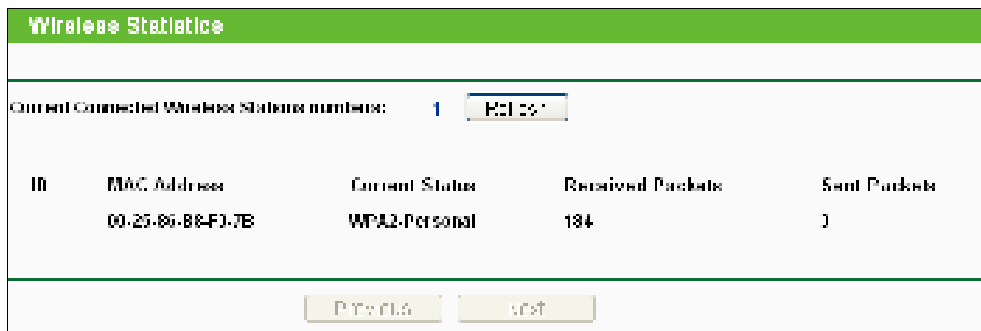


Figure 4-15 The router attached wireless stations

- **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.

4.8 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 4-16): **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.

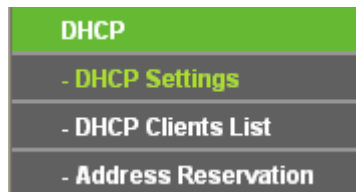


Figure 4-16 The DHCP menu

4.8.1 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 4-17).

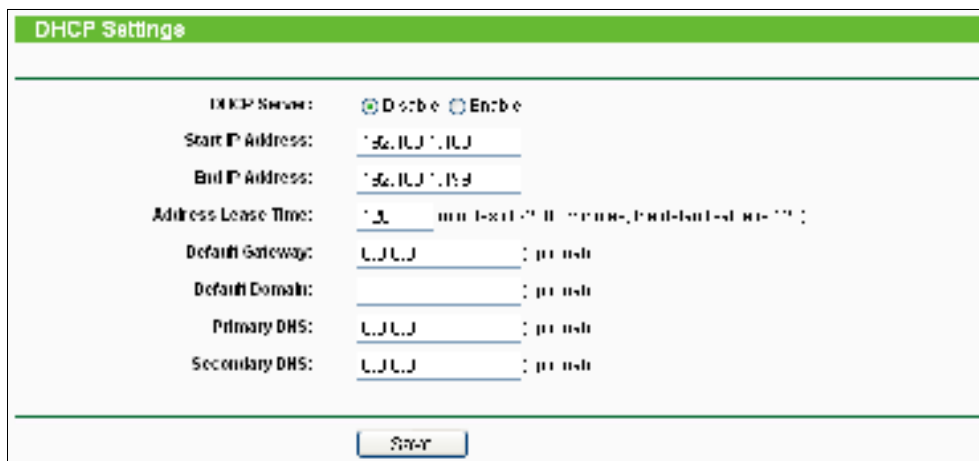


Figure 4-17 DHCP Settings

- **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. 192.168.0.100 is the default start IP address.
- **End IP Address** - This field specifies the last address in the IP Address pool. 192.168.0.199 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.

4.8.2 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 4-18).

DHCP Clients List				
ID	Client Name	MAC Address	Assigned IP	Lease Time
1	Client1	00-11-22-33-44-55	192.168.0.100	120 min

Figure 4-18 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.

4.8.3 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 4-19).



Figure 4-19 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 4-20) will display.
2. Enter the MAC address (the format for the MAC Address is XX-XX-XX-XX-XX-XX) and IP address in dotted-decimal notation of the computer you want to add.
3. Click the **Save** button after finish configuring.

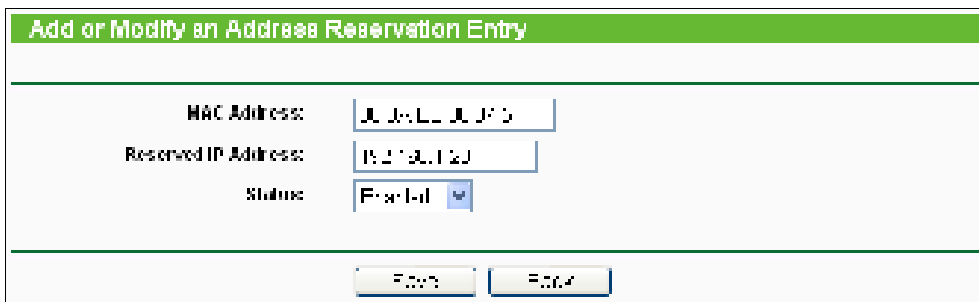


Figure 4-20 Add or Modify an Address Reservation Entry

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:

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.

4.9 System Tools

System Tools option helps you to optimize the configuration of your device. You can upgrade the AP to the latest version of firmware as well as backup or restore the AP's configuration files. Ping Watch Dog can help to continuously monitor a particular connection to a remote host. Speed Test helps to test the connection speed to and from any reachable IP address on current network, especially when we are building wireless network between devices which are far away from each other. It's suggested that you change the default password to a more secure one because it controls access to the device's web-based management page. Besides, you can find out what happened to the system in System Log.

There are twelve submenus under the **System Tools** menu (shown as Figure 4-21): **SNMP**, **Time Settings**, **Diagnostic**, **Ping Watch Dog**, **Speed Test**, **Firmware Upgrade**, **Factory Defaults**, **Backup & Restore**, **Reboot**, **Password**, **System log** and **Statistics**. Clicking any of them will enable you to configure the corresponding function. The detailed explanations for each submenu are provided below.



Figure 4-21 The System Tools menu

4.9.1 SNMP

Simple Network Management Protocol (SNMP) is a popular network monitoring and management protocol.

Choose menu "**System Tools > SNMP**", and then you can configure the SNMP on the following screen.

Figure 4-22

SNMP Agent - Choose **Enable** to open this function if you want to have remote control through SNMPv1/v2 agent with MIB-II. Choose **Disable** to close this function.

SysContact - The textual identification of the contact person for this managed node.

SysName - An administratively-assigned name for this managed node.

SysLocation - The physical location of this node.

Note:

Specifying one of these values via the Device's Web-Based Utility makes the corresponding object read-only. If there isn't such a config setting, then the write request will succeed (assuming suitable access control settings), but the new value would be forgotten the next time the agent was restarted.

Get Community - Enter the community name that allows Read-Only access to the Device's SNMP information. The community name can be considered a group password. The default setting is **public**.

Get Source - Get source defines the IP address or subnet for management systems that can read information from this 'get' community device.

Set Community - Enter the community name that allows Read/Write access to the Device's SNMP information. The community name can be considered a group password. The default setting is **private**.

Set Source - Set source defines the IP address or subnet for management systems that can control this 'set' community device.

Note:

A restricted source can be a specific IP address (e.g. 10.10.10.1), or a subnet - represented as IP/BITS (e.g. 10.10.10.0/24). If an IP Address of 0.0.0.0 is specified, the agent will accept all requests under the corresponding community name.

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

4.9.2 Time Settings

Choose menu "**System Tools > Time Settings**", and then you can configure the time on the following screen.

Figure 4-23 Time settings

- **Time Zone** - Select your local time zone from this pull-down list.
 - **To set time manually:**
 1. Select your local time zone.
 2. Enter the **Date** in Month/Day/Year format.
 3. Enter the **Time** in Hour/Minute/Second format.
 4. Click **Save**.
 - **For automatic time synchronization:**
 1. Enter the address or domain of the **NTP Server I** or **NTP Server II**.
 2. Click the **Get GMT** button to get GMT from the Internet.
 - **To enable Daylight Saving:**
 1. Select the **Enable Daylight Saving** checkbox to enable daylight saving function.
 2. Schedule the span of time which this function will effect. For example, if you want this function work at 0 o'clock(am) on the 1st Sunday of April and last until at 6 o'clock(pm) on the 2nd Saturday of September, you need choose "Apr", "1st", "Sun", "0am" at **Start** part and choose "Sep", "2nd", "Sat", "6pm" at the **End** part.
 3. Click the **Save** button to effect this function.
- Note:**
- 1) This setting will be used for some time-based functions such as firewall functions. These time dependant functions will not work if time is not set. So, it is important to specify time settings as soon as you successfully login to the Device.
 - 2) The time will be lost if the Device is turned off.
 - 3) The Device will automatically obtain GMT from the Internet if it is configured accordingly.
 - 4) In daylight saving configuration, start time and end time shall be within one year and start time shall be earlier than end time.
 - 5) After you enable daylight saving function, it will take action in one minute.

4.9.3 Diagnostic

Choose menu “**System Tools > Diagnostic**”, and then you can transact Ping or Traceroute function to check connectivity of your network in the following screen.

Figure 4-24 Diagnostic Tools

- **Diagnostic Tool** - Click the radio button to select one diagnostic tool:
 - **Ping** - This diagnostic tool troubleshoots connectivity, reachability, and name resolution to a given host or gateway.
 - **Traceroute** - This diagnostic tool tests the performance of a connection.

Note:

You can use ping/traceroute to test both numeric IP address or domain name. If pinging/tracerouting the IP address is successful, but pinging/tracerouting the domain name is not, you might have a name resolution problem. In this case, ensure that the domain name you are specifying can be resolved by using Domain Name System (DNS) queries.

- **IP Address/ Domain Name** - Enter the IP Address or Domain Name of the PC whose connection you wish to diagnose.
- **Ping Count** - Specifies the number of Echo Request messages sent. The default is 4.
- **Ping Packet Size** - Specifies the number of data bytes to be sent. The default is 64.
- **Ping Timeout** - Time to wait for a response, in milliseconds. The default is 800.
- **Traceroute Max TTL** - Set the maximum number of hops (max TTL to be reached) in the path to search for the target (destination). The default is 20.

Click the **Start** button to start the diagnostic procedure.

The **Diagnostic Results** page (as shown in Figure 4-25) displays the result of diagnosis.

If the result is similar to the following screen, the connectivity of the Internet is fine.

```

Diagnostic Results
-----
Pinging 202.108.22.5 with 64 bytes of data:

Reply from 202.108.22.5: bytes=64 time=1 TTL=127 seq=1
Reply from 202.108.22.5: bytes=64 time=1 TTL=127 seq=2
Reply from 202.108.22.5: bytes=64 time=1 TTL=127 seq=3
Reply from 202.108.22.5: bytes=64 time=1 TTL=127 seq=4

Ping statistics for 202.108.22.5
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milliseconds:
Minimum = 1, Maximum = 1, Average = 1

```

Figure 4-25 Diagnostic Results

Note:

- 1) Only one user can use the diagnostic tools at one time.
- 2) "Ping Count", "Ping Packet Size" and "Ping Timeout" are Ping Parameters, and "Traceroute Max TTL" is Traceroute Parameter.

4.9.4 Ping Watch Dog

Selecting **System Tools > Ping Watch Dog** allows you to continuously monitor the particular connection between the device to a remote host. It makes this device continuously ping a user defined IP address (it can be the internet gateway for example). If it is unable to ping under the user defined constraints, this device will automatically reboot.

Figure 4-26 Ping Watch Dog Utility

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

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

4.9.5 Speed Test

Selecting **System > Speed Test** allows you to test the connection speed to and from any reachable IP address on current network on the page as shown in Figure 4-27. The speed test is especially used when you are building wireless network between devices which are far away from

each other. It should be used for the preliminary throughput estimation between two network devices. The estimation is rough. You can input the remote device's administrator Username and Password under **Advance options** to get a precise estimation if the remote device is TL-WA7210N too.

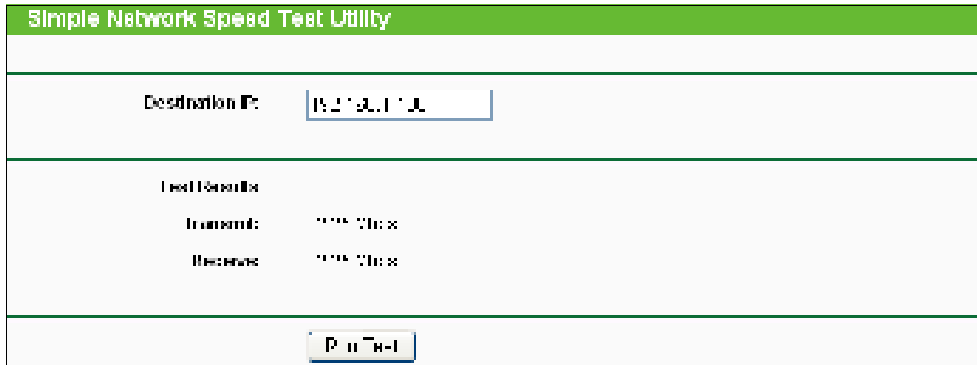


Figure 4-27 Speed Test

- **Destination IP** - The Remote device's IP address.
- **Transmit** - Estimate the outgoing throughput (Tx).
- **Receive** - Estimate the ingoing throughput (Rx).

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

4.9.6 Firmware Upgrade

Choose menu **System Tools > Firmware Upgrade**, and then you can update the latest version of firmware for the Device on the following screen.

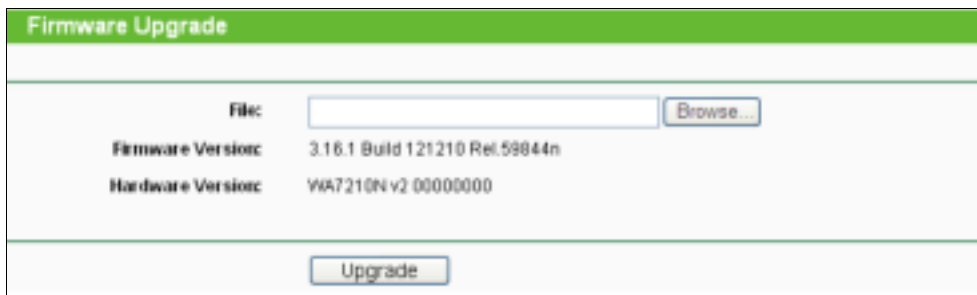


Figure 4-28 Firmware Upgrade

- **To upgrade the Device's firmware, follow these instructions:**
 1. Download a most recent firmware upgrade file from our website (www.tp-link.com).
 2. Enter or select the path name where you save the downloaded file on the computer into the **File Name** blank.
 3. Click the **Upgrade** button.
 4. The Device will reboot while the upgrading has been finished.
- **Firmware Version** - Displays the current firmware version.
- **Hardware Version** - Displays the current hardware version. The hardware version of the upgrade file must accord with the current hardware version.

 **Note:**

The firmware version must correspond to the hardware. The upgrade process takes a few moments and the Device restarts automatically when the upgrade is complete. It is important to keep power applied during the entire process. Loss of power during the upgrade could damage the Device.

4.9.7 Factory Defaults

Choose menu **System Tools > Factory Defaults**, and you can restore the configurations of the Device to factory defaults on the following screen.

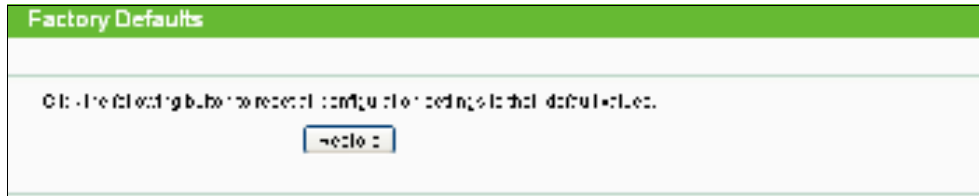


Figure 4-29 Restore Factory Default

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

- Default User Name - **admin**.
- Default Password - **admin**.
- Default IP Address - **192.168.0.254**.
- Default Subnet Mask - **255.255.255.0**.

 **Note:**

All changed settings will be lost when defaults are restored.

4.9.8 Backup & Restore

Choose menu "**System Tools > Backup & Restore**", and then you can save the current configuration of the Device as a backup file and restore the configuration via a backup file as shown in Figure 4-30.



Figure 4-30 Backup & Restore

Click the **Backup** button to save all configuration settings to your local computer as a file.

➤ To restore the AP's configuration, follow these instructions:

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

 **Note:**

The current configuration will be covered with the uploading configuration file. Wrong process will lead the device unmanaged. The restoring process lasts for 20 seconds and the AP will restart automatically then. Keep the power of the AP on during the process, in case of any damage.

4.9.9 Reboot

Choose menu **System Tools > Reboot**, and then you can click the **Reboot** button to reboot the Device via the next screen.

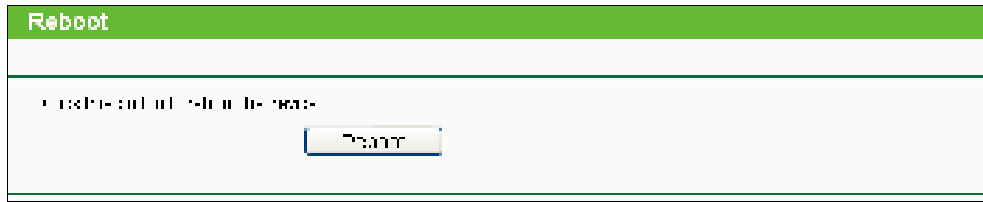


Figure 4-31 Reboot the Device

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

- Some settings of the Device will take effect only after rebooting, including:
 - Change the LAN IP Address (system will reboot automatically).
 - Change the DHCP Settings.
 - Change the Wireless configurations.
 - Change the Web Management Port.
 - Upgrade the firmware of the Device (system will reboot automatically.).
 - Restore the Device's settings to the factory defaults (system will reboot automatically.).
 - Update the configuration with the file (system will reboot automatically.).

4.9.10 Password

Choose menu **System Tools > Password**, and then you can change the factory default user name and password of the Device in the next screen as shown in Figure 4-32.

Figure 4-32 Password

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

 **Note:**

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

Click the **Save** button when finished.

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

4.9.11 System log

Choose menu **System Tools > System Log**, and then you can view the logs of the Device.

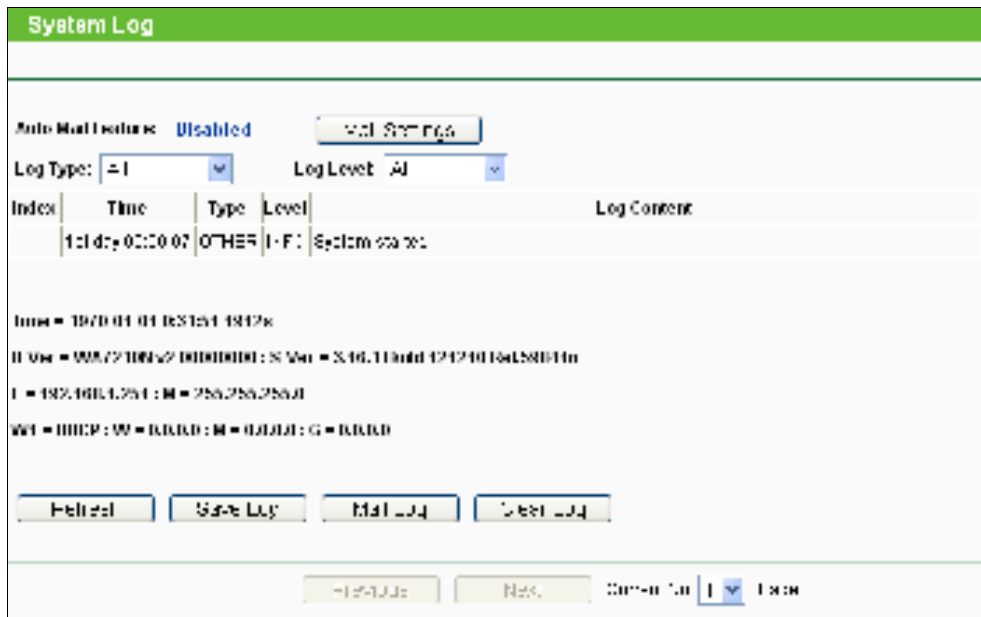


Figure 4-33 System Log

- **Auto Mail Feature** - Indicates whether auto mail feature is enabled or not.
- **Mail Settings** - Set the receiving and sending mailbox address, server address, validation information as well as the timetable for Auto Mail Feature.

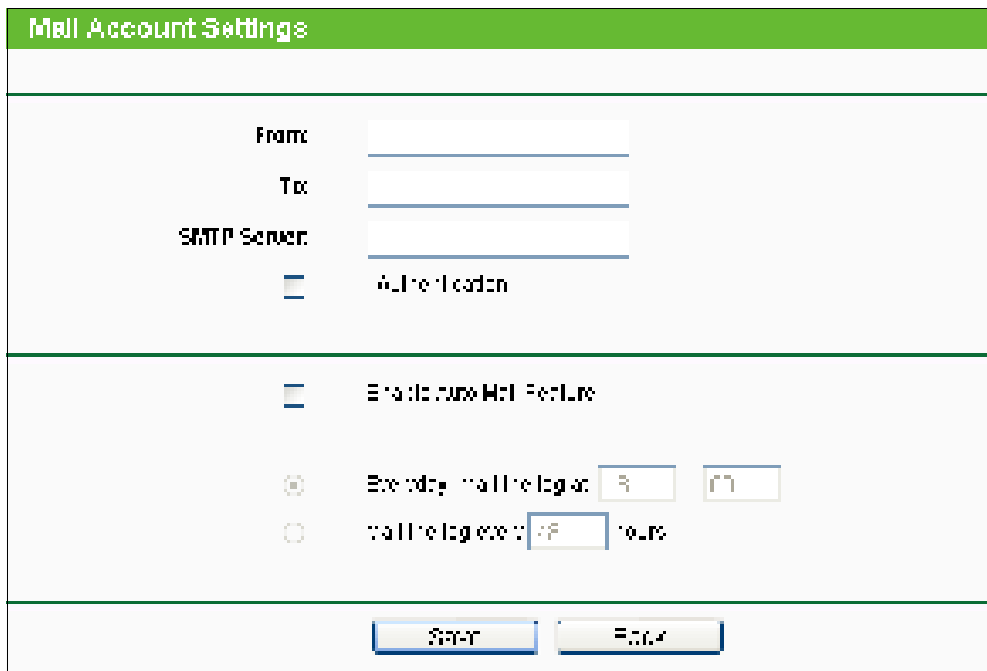


Figure 4-34 Mail Account Settings

- **From** - Your mail box address.
- **To** - Recipient's address.
- **SMTP Server** - Your SMTP server.
- **Authentication** - Most SMTP Server requires Authentication.

Note:

Only when you select **Authentication**, do you have to enter the User Name and Password in the following fields.

- **User Name** - Your mail account name.
- **Password** - Your mail account password.
- **Auto Mail Feature** will help you monitor how your Device is running.

Everyday, at specified time, the Device will automatically send the log to specified mailbox. Every few hours, such as 2 hours, the Device will automatically send the log to specified mailbox.

- **Log Type** - By selecting the log type, only logs of this type will be shown.
- **Log Level** - By selecting the log level, only logs of this level will be shown.
- **Refresh** - Refresh the page to show the latest log list.
- **Save Log** - Click to save all the logs in a txt file.
- **Mail Log** - Click to send an email of current logs manually according to the address and validation information set in Mail Settings. The result will be shown in the later log soon.
- **Clear Log** - All the logs will be deleted from the Device permanently, not just from the page.

Click the **Next** button to go to the next page.

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

4.9.12 Statistics

Choose menu **System Tools > Statistics**, and then you can view the statistics of the Device, including total traffic and current traffic of the last Packets Statistic Interval.

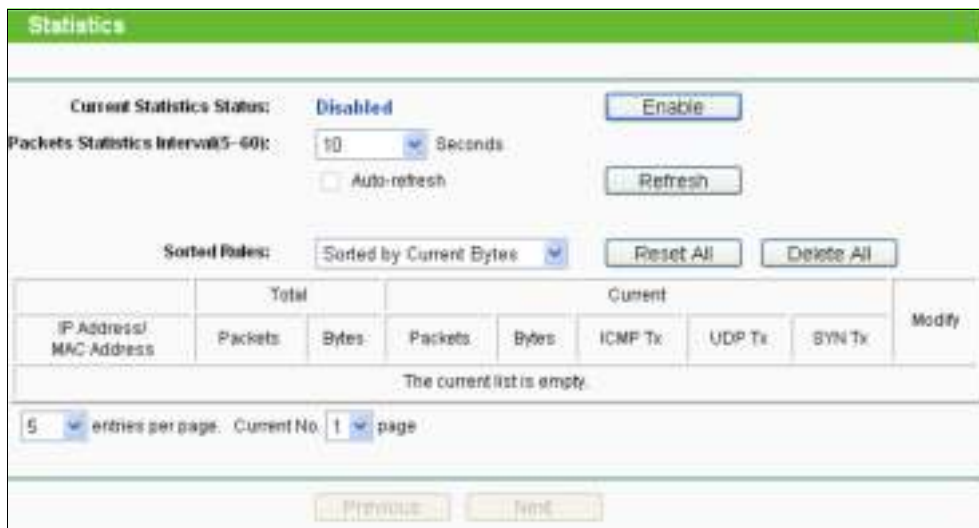


Figure 4-35 Statistics

The Statistics page shows the network traffic of each PC on the LAN, including total traffic and the value of the last **Packets Statistic interval** in seconds.

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

- **Packets Statistics Interval** - The default value is 10. Select a value between 5 and 60 seconds in the pull-down list. The Packets Statistic interval value indicates the time section of the packets statistic.
- **Sorted Rules** - Choose how displayed statistics are sorted.

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

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

Click the **Reset All** button to reset the values of all entries to zero.

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

➤ Statistics Table

Address MAC Address	Total		Current					Modify
	Packets	Bytes	Packets	Bytes	ICMP Tx	UDP Tx	TCP SYN Tx	
The current is empty								
Page: 5 of 10 Current No.: 10 Page								
<input type="button" value="Previous"/> <input type="button" value="Next"/>								

Figure 4-36 Statistics Table

- **IP Address/MAC Address** - The IP Address and MAC address are displayed with related statistics.
- **Total**
 - **Packets** - The total number of packets received and transmitted by the Device.
 - **Bytes** - The total number of bytes received and transmitted by the Device.
- **Current**
 - **Packets** - The total number of packets received and transmitted in the last Packets Statistics interval seconds.
 - **Bytes** - The total number of bytes received and transmitted in the last Packets Statistics interval seconds.
 - **ICMP Tx** - The number of ICMP packets transmitted to the WAN per second at the specified Packets Statistics interval. It is shown like "current transmitting rate / Max transmitting rate".
 - **UDP Tx** - The number of UDP packets transmitted to the WAN per second at the specified Packets Statistics interval. It is shown like "current transmitting rate / Max transmitting rate".
 - **TCP SYN Tx** - The number of TCP SYN packets transmitted to the WAN per second at the specified Packets Statistics interval. It is shown like "current transmitting rate / Max transmitting rate".
- **Modify**
 - **Reset** - Reset the values of the entry to zero.
 - **Delete** - Delete the existing entry in the table.

Chapter 5. 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.

5.1 Login

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

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

5.2 Status

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

Status		
Firmware Version:	3.15.0_B.14131311_Fe.2014-4n	
Hardware Version:	V4-7210N-3.0000000	
LAN		
MAC Address:	04:73:10:2:10:10	
IP Address:	192.168.0.254	
Subnet Mask:	255.255.255.0	
Wireless		
Wireless Radio:	Enable	
Name (SSID):	TP-LINK_31_0_0	
Channel:	1	
Mode:	11b/g/n+2d	
Channel Width:	Auto	
MAC Address:	04:73:10:2:10:10	
Client Status:	Full	
WAN		
MAC Address:	04:73:10:2:10:10	
IP Address:	192.168.1.7	Default IP
Subnet Mask:	255.255.255.0	
Default Gateway:	192.168.1.1	<input type="button" value="Connect"/>
DNS Server:	192.168.1.1, 0.0.0.0	
Traffic Statistics		
	Received	Sent
Bytes:	0	0
Packets:	0	0
System Up Time:	0 days 00:30:38	<input type="button" value="Refresh"/>

Figure 5-1 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**, **Name (SSID)**, **Channel**, **Mode**, **Channel Width**, **MAC address** and **Client Status**.

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.

5.3 Quick Setup

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

5.4 Operation Mode

Selecting **Operation Mode** will allow you to choose the operation mode for the AP. The AP supports seven operation mode types, **AP Client Router**, **AP Router**, **Access Point**, **Multi-SSID**, **Repeater (Range Extender)**, **Bridge with AP** and **Client**. Please select the one you want as shown in Figure 4-2. Click **Save** to save your choice.

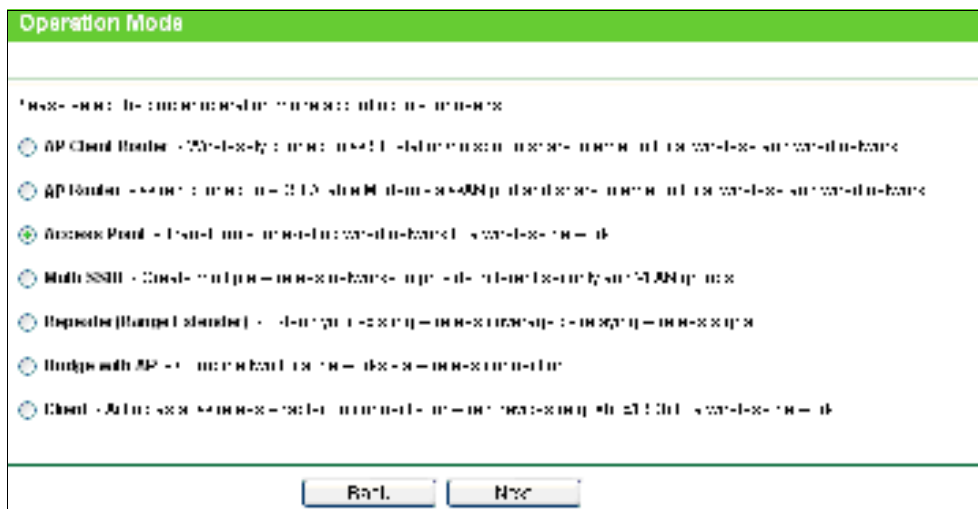


Figure 5-2 Operation Mode

- **AP Client Router** - In this mode, the device enables multi-users to share Internet from WISP. The LAN port devices share the same IP from WISP through Wireless port. While connecting to WISP, the Wireless port works as a WAN port at AP Client Router mode. The Ethernet port acts as a LAN port.
- **AP Router** - In this mode, the device enables multi-users to share Internet via ADSL/Cable Modem. The wireless port share the same IP to ISP through Ethernet WAN port. The Wireless port acts the same as a LAN port while at AP Router mode.
- **Access Point** - In this mode, the device can be connected to a wired network and transform the wired access into wireless that multiple devices can share together, especially for a home, office or hotel where only wired network is available.
- **Multi-SSID** - In this mode, the device can create up to 4 wireless networks labeled with different SSIDs and assign each SSID with different security or VLAN, especially for the situation when the various access policies and functions are required.
- **Repeater(Range Extender)** - In this mode, the device can copy and reinforce the existing wireless signal to extend the coverage of the signal, especially for a large space to eliminate signal-blind corners.
- **Bridge with AP** - In this mode, the device can be used to combine multiple local networks together to the same one via wireless connections, especially for a home or office where separated networks can't be connected easily together with a cable.

- **Client** - In this mode, the device can be connected to another device via Ethernet port and act as an adaptor to grant your wired devices access to a wireless network, especially for a Smart TV, Media Player, or game console only with an Ethernet port.

Note:

When you change the operation mode to Client/Repeater, WPS function will stay disabled. Please manually enable this function if needed when you switch back to Access Point/Multi-SSID/Bridge mode.

5.5 WPS

WPS function will help you add a new device to the network quickly. If the new device supports Wi-Fi Protected Setup and is equipped with a configuration button, you can add it to the network by pressing the configuration button on the device and then press the button on the device within two minutes. The status LED on the device will light green for five minutes if the device has been successfully added to the network. If the new device supports Wi-Fi Protected Setup and the connection way using PIN, you can add it to the network by entering the device's PIN.

Select menu **WPS**, then you will see the next screen (shown in Figure 5-3).

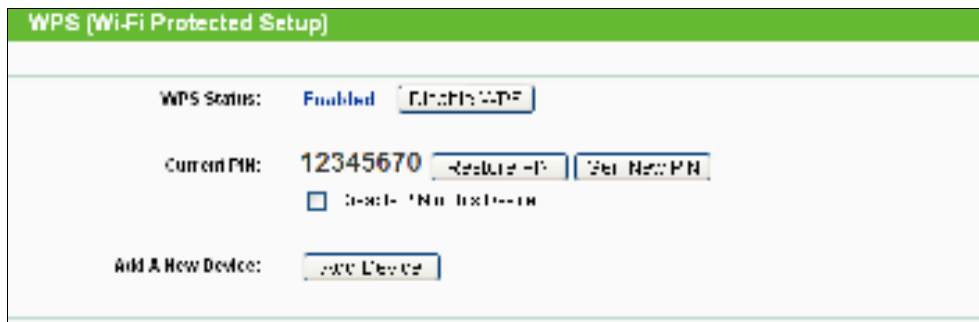


Figure 5-3

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

Note:

The **WPS** function cannot be configured if the Wireless Function of the Device is disabled. Please make sure the Wireless Function is enabled before configuring the **WPS**.

To add a new device:

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

Note:

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

I. Enter the client device’s PIN on the Router

Use this method if your client device has a Wi-Fi Protected Setup PIN number.

Step 1: Keep the default Status as **Enabled** and click the **Add Device** button in 错误! 未找到引用源。 , then the following screen will appear.

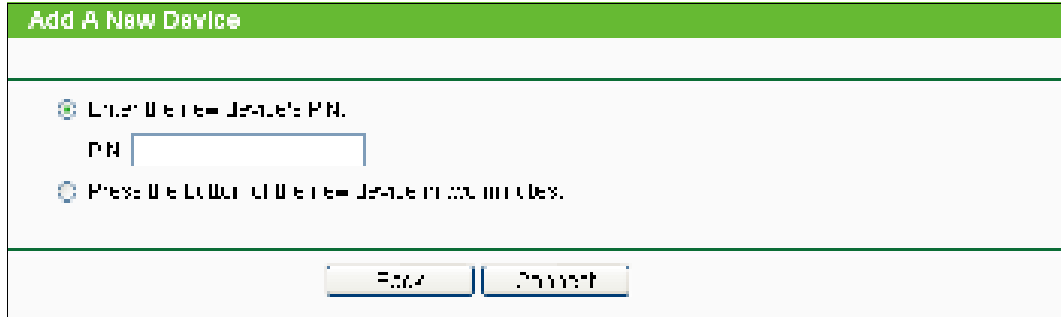


Figure 5-4 Add A New Device

Step 2: Enter the PIN number from the client device in the field on the above WPS screen. Then click **Connect** button.

Step 3: “**Connect successfully**” will appear on the screen of Figure 5-4, which means the client device has successfully connected to the Router.

II. Enter the Router’s PIN on your client device

Use this method if your client device asks for the Router’s PIN number.

Step 1: On the client device, enter the PIN number listed on the Router’s Wi-Fi Protected Setup screen. (It is also labeled on the bottom of the Router.)

Step 2: The Wi-Fi Protected Setup LED flashes for two minutes during the Wi-Fi Protected Setup process.

Step 3: When the WPS LED is on, the client device has successfully connected to the Router.

Step 4: Refer back to your client device or its documentation for further instructions.

5.6 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 5-5): **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.

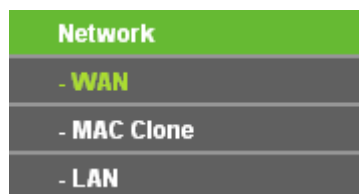


Figure 5-5 the Network menu

5.6.1 WAN

Choose menu **Network > WAN**, and then you can configure the IP parameters of the WAN on the screen below. There are six WAN connection types: Dynamic IP, Static IP, PPPoE/Russia PPPoE, BigPond Cable, L2TP/Russia L2TP, and PPTP/Russia PPTP; while there is one more type in AP Router mode, BigPond Cable.

1. If your ISP is running a DHCP server, select the **Dynamic IP** option. Then the Device will automatically get IP parameters from your ISP. You can see the page as follow (Figure 5-6).

The screenshot shows the WAN configuration interface. At the top, there's a green header with the word 'WAN'. Below it, the 'WAN Connection Type' is set to 'Dynamic IP'. There are 'Renew' and 'Release' buttons next to it. The 'IP Address' field contains '1.1.1.1', 'Subnet Mask' contains '255.255.255.0', and 'Default Gateway' contains '1.1.1.1'. Below these is an 'MTU Size (in bytes)' field with '1500' and a note: 'The normal MTU (Maximum Transmission Unit) value for most Ethernet networks is 1500 Bytes. For some ISPs you 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.' There are two radio buttons: 'Use These DNS Servers' (selected) and 'Use Dynamic DNS Servers'. The 'Primary DNS' field has '8.8.8.8' and 'Secondary DNS' has '8.8.4.4'. The 'Host Name' field has 'lan7210n'. At the bottom, there is a 'Save' button.

Figure 5-6 WAN – Dynamic IP

This page displays the WAN IP parameters assigned dynamically by your ISP, including IP address, Subnet Mask, Default Gateway, etc.

- **IP Address** - The IP address assigned by your ISP dynamically.
- **Subnet Mask** - The subnet mask assigned by your ISP dynamically.
- **Default Gateway** - The default gateway assigned dynamically by your ISP.
- **MTU Size (in bytes)** - The normal MTU (Maximum Transmission Unit) value for most Ethernet networks is 1500 Bytes. For some ISPs you 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.

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

- **Primary DNS** - Enter the DNS IP address in dotted-decimal notation provided by your ISP.
- **Secondary DNS** - Enter another DNS IP address in dotted-decimal notation provided by your ISP.

Click the **Renew** button to renew the IP parameters from your ISP.

Click the **Release** button to release the IP parameters.

Note:

If you get Address not found error when you access 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 can't get the IP Address normally, you can choose Unicast. You generally need not to check this option.

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

2. If your ISP provides a static or fixed IP Address, Subnet Mask, Gateway and DNS setting, select the **Static IP** option. The **Static IP** settings page will appear as shown in Figure 5-7.

Figure 5-7 WAN - Static IP

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

3. If your ISP provides a PPPoE connection, select **PPPoE/Russia PPPoE** option. Then you should enter the following parameters (Figure 5-8):

Figure 5-8 WAN – PPPoE/Russia PPPoE

➤ **PPPoE Connection**

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

- **Secondary Connection** - It's available only for PPPoE Connection. If your ISP provides an extra Connection type such as Dynamic/Static IP to connect to a local area network, then you can check the radio button of Dynamic/Static IP to activate this secondary connection.
 - **Disabled** - The Secondary Connection is disabled by default, so there is PPPoE connection only. This is recommended.
 - **Dynamic IP** - Use dynamic IP address to connect to the local area network provided by ISP.
 - **Static IP** - Use static IP address to connect to the local area network provided by ISP.
- **WAN Connection Mode**
 - **Connect on Demand** - You can configure the Device to disconnect your Internet connection after a specified period of the Internet connectivity (**Max Idle Time**). If your Internet connection has been terminated due to inactivity, **Connect on Demand** enables the Device to automatically re-establish your connection when you attempt to access the Internet again. If you wish to activate **Connect on Demand**, put a check mark in the circle. If you want your Internet connection to remain active all the time, enter **0** in the **Max Idle Time** field.

 **Note:**

Sometimes the connection cannot be disconnected although you specify a time to **Max Idle Time** (0~99 mins) because some applications visit the Internet continually in the background.

- **Connect Automatically** - Connect automatically after the Device is disconnected. To use this option, click the radio button.
- **Time-based Connecting** - You can configure the Device to make it connect or disconnect based on time. Enter the start time in HH-MM for connecting and end time in HH-MM for disconnecting in the **Period of Time** fields.
- **Connect Manually** - You can configure the Device to make it connect or disconnect manually. After a specified period of inactivity (**Max Idle Time**), the Device will disconnect your Internet connection, and 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 all the times, enter 0 in the **Max Idle Time** field. Otherwise, enter the number in minutes that you wish to have the Internet connecting last unless a new link is requested.

 **Note:**

- 1) Sometimes the connection cannot be disconnected although you specify a **Max Idle Time** (0~99 mins) because some applications visit the Internet continually in the background.
- 2) Only when you have set the system time on **System Tools** → **Time Settings** page, the **Time-based Connecting** function can take effect.

Click the **Connect** button to connect immediately.

Click the **Disconnect** button to disconnect immediately.

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

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

- If you want to do some advanced configurations, please click the **Advanced** button, and then the page shown in Figure 5-9 will appear.

Figure 5-9 PPPoE Advanced Settings

- **MTU Size** - The default MTU (Maximum Transmission Unit) size is 1480 bytes, which 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** - They should not be done unless you are sure it is necessary for your ISP.
- **ISP Specified IP Address** - If you know that your ISP does not automatically transmit IP address to the Device during login, click "**Use the IP Address specified by ISP**" checkbox and enter the IP address in dotted-decimal notation, which is provided by your ISP.
- **Detect Online Interval** - The default value is 0. You can input the value between 0 and 120. The Device will detect Access Concentrator online every interval seconds. If the value is 0, it means not detecting.
- **Use the following DNS Servers** - If your ISP specifies a DNS server IP address for you, click the checkbox, and fill the **Primary DNS** and **Secondary DNS** blanks below. The **Secondary DNS** is optional. Otherwise, the DNS servers will be assigned dynamically from ISP.
- **Primary DNS** - (Optional) Enter the DNS IP address in dotted-decimal notation provided by your ISP.
- **Secondary DNS** - (Optional) Enter another DNS IP address in dotted-decimal notation provided by your ISP.

 **Note:**

The new advanced PPPoE parameters will not take effect until you dial-up again.

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

Click the **Back** button when finished.

4. If your ISP provides BigPond Cable (or Heart Beat Signal) connection, please select **BigPond Cable** option. And then you should enter the following parameters as in Figure 5-10.

Figure 5-10 WAN – BigPond Cable

- **User Name/Password** - Enter the User Name and Password provided by your ISP. These fields are case-sensitive.
- **Auth Server** - Enter the authenticating server IP address or host name.
- **Auth Domain** - Type in the domain suffix server name based on your location.
 - NSW / ACT - **nsw.bigpond.net.au**
 - VIC / TAS / WA / SA / NT - **vic.bigpond.net.au**
 - QLD - **qld.bigpond.net.au**
- **MTU Size** - The normal **MTU** (Maximum Transmission Unit) value for most Ethernet networks is 1500 Bytes. It is not recommended that you change the default **MTU Size** unless required by your ISP.
- **Connect on Demand** - In this mode, the Internet connection can be terminated automatically after a specified inactivity period (**Max Idle Time**) and be re-established when you attempt to access the Internet again. If you want your Internet connection keeps active all the time, please enter “0” in the **Max Idle Time** field. Otherwise, enter the number of minutes you want to have elapsed before your Internet access disconnects.
- **Connect Automatically** - The connection can be re-established automatically when it was down.
- **Connect Manually** - You can click the **Connect/Disconnect** button to connect/disconnect immediately. This mode also supports the **Max Idle Time** function as **Connect on Demand** mode. The Internet connection can be disconnected automatically after a specified inactivity period and re-established when you attempt to access the Internet again.
- Click the **Connect** button to connect immediately. Click the **Disconnect** button to disconnect immediately.

 **Note:**

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

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

5. If your ISP provides L2TP connection, please select **L2TP/Russia L2TP** option. Then you should enter the following parameters in Figure 5-11.



The screenshot shows the WAN configuration interface for L2TP/Russia L2TP. The 'WAN Connection Type' is set to 'L2TP/Russia L2TP'. The 'User Name' field contains 'username' and the 'Password' field is masked with asterisks. There are 'Connect' and 'Disconnect' buttons, with a 'Disconnected!' status indicator. The 'Dynamic IP' radio button is selected, and the 'Static IP' radio button is unselected. The 'Server IP Address Name' field is empty. The 'IP Address', 'Subnet Mask', 'Gateway', and 'DNS' fields all contain '0.0.0.0'. The 'Internet IP Address' and 'Internet DNS' fields also contain '0.0.0.0'. The 'MTU Size (in bytes)' field is set to '1460' with a note: '(The default is 1460, do not change unless necessary)'. The 'Connection Mode' has three options: 'Connect on Demand' (selected), 'Connect Automatically', and 'Connect Manually'. The 'Max Idle Time' field is set to '15' minutes, with a note: '(0 means remain active at all times.)'. A 'Save' button is located at the bottom of the form.

Figure 5-11 WAN – L2TP/Russia L2TP

- **User Name/Password** - Enter the User Name and Password provided by your ISP. These fields are case-sensitive.
- **Dynamic IP/ Static IP** - Choose either one as you are given by your ISP. Click the **Connect** button to connect immediately. Click the **Disconnect** button to disconnect immediately.
- **Connect on Demand** - You can configure the Device to disconnect from your Internet connection after a specified period of inactivity (**Max Idle Time**). If your Internet connection has been terminated due to inactivity, **Connect on Demand** enables the Device to automatically re-establish your connection as soon as you attempt to access the Internet again. If you wish to activate **Connect on Demand**, check the radio button. If you want your Internet connection to remain active at all time, enter 0 in the **Max Idle Time** field. Otherwise, enter the number of minutes you want to have elapsed before your Internet connection terminates.
- **Connect Automatically** - Connect automatically after the Device is disconnected. To use this option, check the radio button.

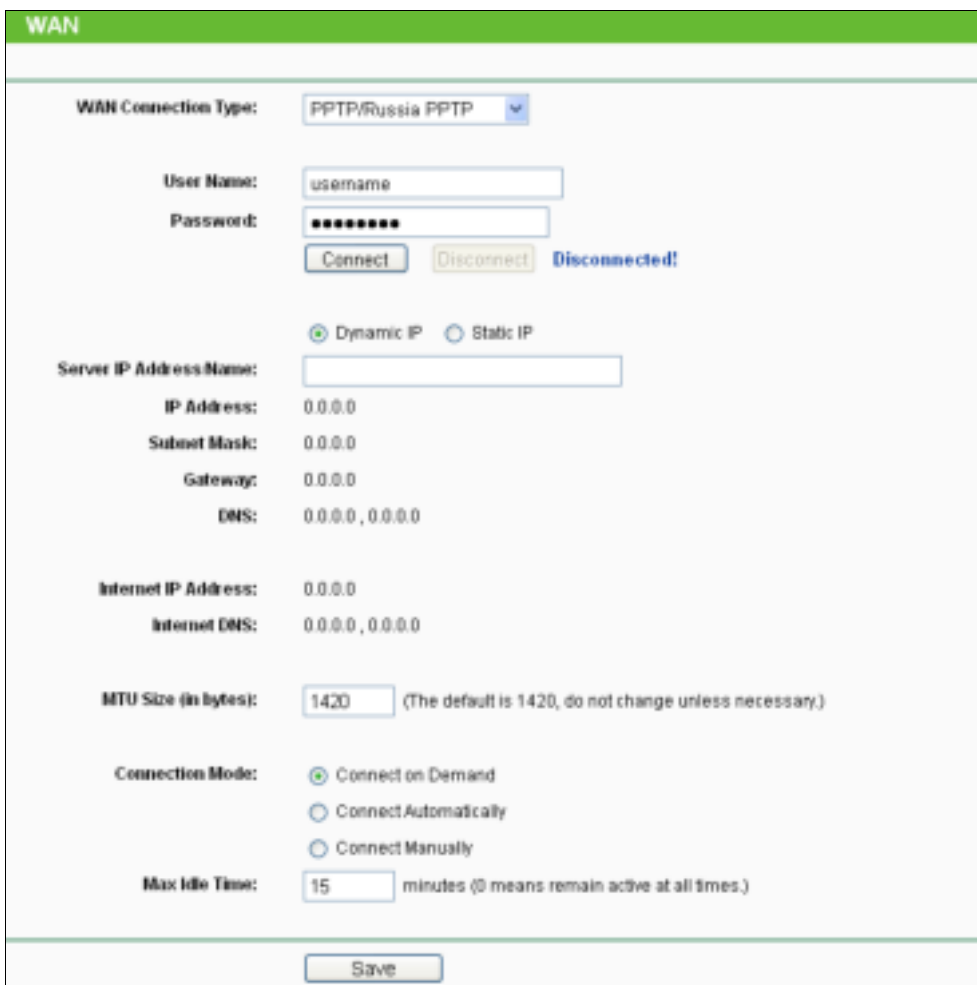
- **Connect Manually** - You can configure the Device to make it connect or disconnect manually. After a specified period of inactivity (**Max Idle Time**), the Device will disconnect from your Internet connection, and you will not be able to re-establish your connection automatically as soon as you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

 **Note:**

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

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

6. If your ISP provides PPTP connection, please select **PPTP/Russia PPTP** option. And you should enter the following parameters (Figure 5-12):



The screenshot shows the WAN configuration interface for a PPTP/Russia PPTP connection. The 'WAN Connection Type' is set to 'PPTP/Russia PPTP'. The 'User Name' field contains 'username' and the 'Password' field contains '*****'. Below the password field are 'Connect' and 'Disconnect' buttons, with a 'Disconnected!' status indicator. The 'Dynamic IP' radio button is selected, and the 'Static IP' radio button is unselected. The 'Server IP Address Name' field is empty. The 'IP Address', 'Subnet Mask', 'Gateway', and 'DNS' fields all contain '0.0.0.0'. The 'Internet IP Address' and 'Internet DNS' fields also contain '0.0.0.0'. The 'MTU Size (in bytes)' field contains '1420' with a note '(The default is 1420, do not change unless necessary.)'. The 'Connection Mode' section has three radio buttons: 'Connect on Demand' (selected), 'Connect Automatically', and 'Connect Manually'. The 'Max Idle Time' field contains '15' minutes, with a note '(0 means remain active at all times.)'. A 'Save' button is located at the bottom of the form.

Figure 5-12 WAN – PPTP/Russia PPTP

- **User Name/Password** - Enter the User Name and Password provided by your ISP. These fields are case-sensitive.
- **Dynamic IP/ Static IP** - Choose either as you are given by your ISP and enter the ISP's IP address or the domain name.
 - If you choose static IP and enter the domain name, you should also enter the DNS assigned by your ISP. And click the **Save** button.
 - Click the **Connect** button to connect immediately. Click the **Disconnect** button to disconnect immediately.

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

 **Note:**

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

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

5.6.2 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 5-13.

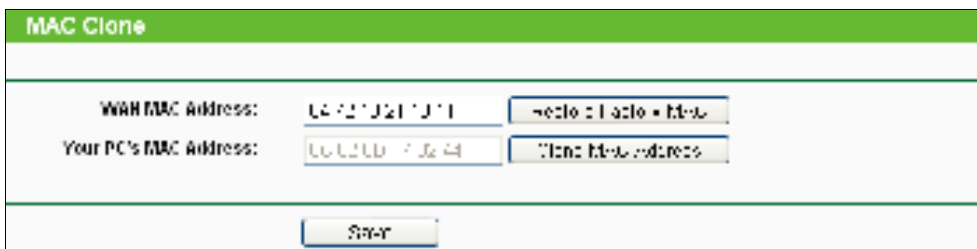


Figure 5-13 MAC Address Clone

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

- **WAN MAC Address** - This field displays the current MAC address of the WAN port, which is used for the WAN port. If your ISP requires that you register the MAC address, please enter the correct MAC address into this field. The format for the MAC Address is XX-XX-XX-XX-XX-XX (X is any hexadecimal digit).
- **Your PC's MAC Address** - This field displays the MAC address of the PC that is managing the router. If the MAC address is required, you can click the **Clone MAC Address** button and this MAC address will fill in the **WAN MAC Address** field.

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

Click **Save** to save your settings.

Note:

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

5.6.3 LAN

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

Figure 5-14 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.

5.7 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 5-15): **Wireless Settings**, **Wireless Security**, **Wireless MAC Filtering**, **Wireless Advanced**, **Antenna Alignment**, **Distance Setting**, **Throughput Monitor** and **Wireless Statistics**. Click any of them, and you will

be able to configure the corresponding function. The detailed explanations for each submenu are provided below.



Figure 5-15 Wireless menu

5.7.1 Wireless Settings

Choose menu **Wireless > Wireless Settings**, and then you can configure the basic settings for the wireless network on the **Wireless Settings** page (Figure 5-16 & Figure 5-17) .

 **Note:**

There are differences between the Wireless Settings page in AP Router mode and that in AP Client Router mode, as shown in Figure 5-16 & Figure 5-17.

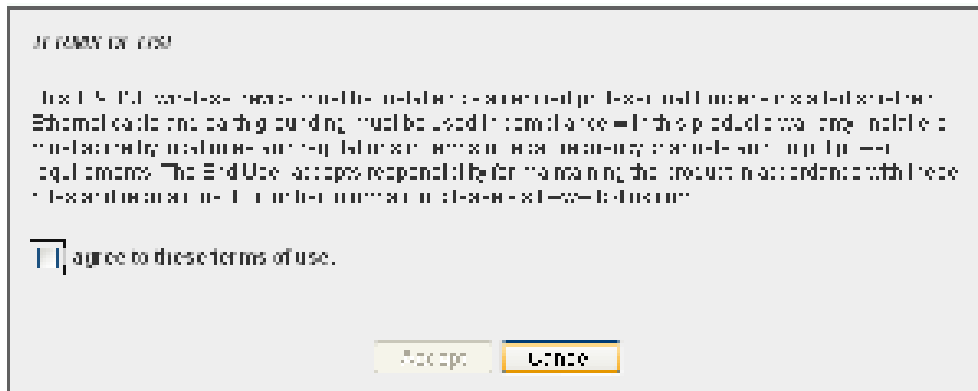
1. Wireless settings in AP Router mode

Figure 5-16 Wireless Settings in AP Router mode

- **Wireless Network Name** - 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 recommended strongly that you change your networks name (SSID) to a different value. This value is case-sensitive. For example, **MYSSID** is NOT the same as **MySSID**.
- **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 file. 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, the Note Dialog of **TERMS OF USE** will pop up. Select **I agree to these terms of use**, and click **Accept** to continue.



Note Dialog

Note:

Ensure you select a correct country to comply with local laws. Incorrect settings may cause interference.

- **Transmission Power** - The available options of transmission power are determined by the region selected.
- **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. If you select auto, then the Device will select the best channel automatically.
- **Mode**- This field determines the wireless mode which the Device works on.
- **Channel Width** - The bandwidth of the wireless channel.
- **Enable Wireless Device Radio** - The wireless radio of the Device can be enabled or disabled to allow wireless stations access. If enabled, the wireless stations will be able to access the Device, otherwise, wireless stations will not be able to access the Device.
- **Enable SSID Broadcast** - If you select the **Enable SSID Broadcast** checkbox, the wireless Device will broadcast its name (SSID) on the air.

2. Wireless settings in AP Client Router mode

The screenshot shows the 'Wireless Settings - Client Router' configuration interface. It is divided into two main sections:

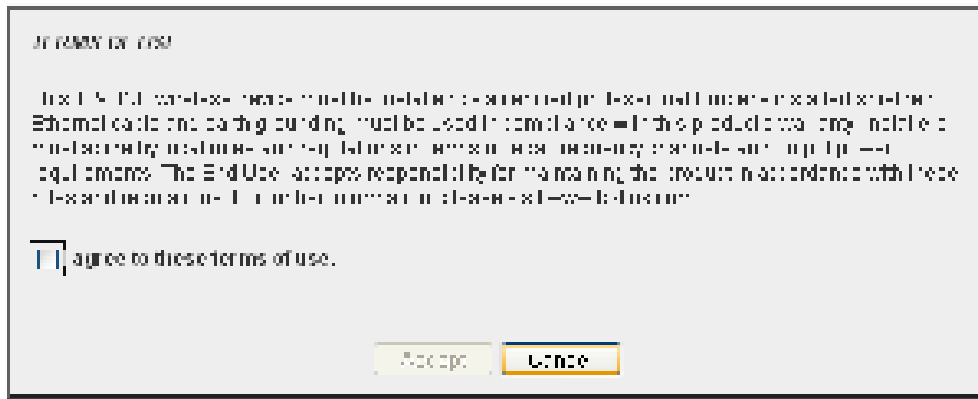
- WISP Station Setting:**
 - Wireless Name of WISP Station: [Text input field]
 - MAC Address of WISP Station: [Text input field]
 - Survey: [Button]
 - Key type: [Dropdown menu]
 - Auth type: [Dropdown menu]
 - WEP Index: [Dropdown menu]
 - Password: [Text input field]
- Local Wireless AP Setting:**
 - Local Wireless Name: [Text input field]
 - Region: [Dropdown menu]
 - Warning: [Text area]
 - Transmission Power: [Dropdown menu]
 - Enable 802.11b/g/n Mode: [Checked checkbox]
 - Enable 802.11n Mode: [Checked checkbox]
 - Enable Local Wireless Access: [Checked checkbox]

A 'Save' button is located at the bottom center of the page.

Figure 5-17 Wireless Settings in AP Client Router mode

- **Wireless Name of WISP Station** - The SSID of the AP your Device is going to connect to as a client. You can also use the search function to select a SSID to join.
- **MAC Address of WISP Station** - The BSSID of the AP your Device is going to connect to as a client. You can also use the search function to select a BSSID to join.
- **Survey** - Click this button, you can search the AP which runs in the current channel.
- **Key type** - This option should be chosen according to the AP's security configuration. It is recommended that the security type is the same as your AP's security type.
- **Auth Type** - This option should be chosen if the key type is WEP (ASCII) or WEP (HEX). It indicates the authorization type of the Root AP.
- **WEP Index** - This option should be chosen if the key type is WEP (ASCII) or WEP (HEX). It indicates the index of the WEP key.
- **Password** - If the AP your Device is going to connect needs password, you need to fill the password in this blank.
- **Local Wireless Name** - Enter a value of up to 32 characters. The same Name (SSID) must be assigned to all wireless devices in your network.
- **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 filed. 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, the Note Dialog of **TERMS OF USE** will pop up. Select **I agree to these terms of use**, and click **Accept** to continue.



Note Dialog

 **Note:**

Ensure you select a correct country to comply with local laws. Incorrect settings may cause interference.

- **Transmission Power** - The available options of transmission power are determined by the region selected.
- **Enable Wireless Radio** - The wireless radio of the Device can be enabled or disabled to allow wireless stations access. If enabled, the wireless stations will be able to access the Device; otherwise, wireless stations will not be able to access the Device.
- **Enable SSID Broadcast** - If you select the **Enable SSID Broadcast** checkbox, the AP Router will broadcast its name (SSID) on the air.
- **Disable Local Wireless Access** - If you select the **Disable Local Wireless Access** checkbox, the wireless Device will disable local wireless access; other stations will not be able to access the Device by wireless.

Click **Survey** button on the Wireless page shown as Figure 5-17, and then AP List page will appear, as shown in Figure 5-18. Find the SSID of the Access Point you want to access, and click **Connect** in the corresponding row. For example, the desired item is selected. The target network's SSID will be automatically filled into the corresponding box which is shown as the Figure 5-19.

AP List						
All Channels						
ID	BSSID	SSID	Signal	Channel	Security	Connect
1	23 23 23 23 23 23	7777	20dB		OFF	Connect
2	14 E6 E4 D7 1C EC	TP-LINK_2.4G-2_D71CEC	138dB		WPA/WPA2 PSK	Connect
3	D8 9C A1 4C 17 D4	TP-LINK_40_7D4	0dB		OFF	Connect
4	AC F3 C 97 E8 30	TP-LINK_07982C	13dB		OFF	Connect
5	13 E6 E4 D7 1C EC	TP-LINK_2.4G-2_D71CEC	0dB		OFF	Connect
6	EC 7 3F 74 33 28		94dB	4	OFF	Connect
7	0C 1C 0F 0 9C 94		90dB	4	OFF	Connect
8	94 01 6C 2F 31 EE	TP-LINK_94016C	84dB	4	WPA/WPA2 PSK	Connect
9	14 E6 E4 E3 87 5A		13dB	3	WPA/WPA2 PSK	Connect
0	AC F3 C 9C 27 31	TP-LINK_9CF3C9	9 dB	3	OFF	Connect
1	14 E6 E4 E3 4E 8C	TP-LINK_14E6E4	92dB	1	WPA/WPA2 PSK	Connect

Figure 5-18 AP List

Wireless Settings - Client Router

WISP Station Setting

Wireless Name of WISP Station: (Optional: 38 D5)

MAC Address of WISP Station: (Example: 0C-1C-0F-0-9C-94)

Keytype: (WPA/WPA2 PSK)

Password:

Local Wireless AP Setting

Local Wireless Name: (Optional: 38 D5)

Region:

Warning: Transmission Power is limited to comply with local regulations. Please refer to the local regulations for more information.

Transmission Power:

Enable WPA/WPA2 PSK

Enable WPA/WPA2 Enterprise

Enable WPA/WPA2 Enterprise

Figure 5-19

Note:

If you know the SSID of the desired AP, you can also input it to the field "Wireless Name of WISP Station" manually.

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

Note:

The operating distance or range of your wireless connection varies significantly based on the physical placement of the Device. For best results, place your Device:

- Near the center of the area in which your wireless stations will operate;
- In an elevated location such as a high shelf;
- Away from the potential sources of interference, such as PCs, microwaves, and cordless phones;
- With the Antenna in the upright position;
- Away from large metal surfaces.

Note:

Failure to follow these guidelines can result in significant performance degradation or inability to wirelessly connect to the Device.

5.7.2 Wireless Security

Selecting **Wireless > Wireless Security** will enable you to configure the security of the wireless network for your device on the page as shown in Figure 4-8.

Figure 5-20 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.
- **WPA/WPA2-Personal** - Select WPA based on Radius Server.
- **WPA/WPA2-Enterprise** - Select WPA based on pre-shared passphrase.
- **WEP** - Select 802.11 WEP security.

Each security option has its own settings as described below:

WPA/WPA2 – Personal (Recommended)

- **WEP** - Select 802.11 WEP security.
- **Version** - You can select one of following versions:
 - **Automatic** - Select **WPA-Personal** or **WPA2-Personal** automatically based on the wireless station's capability and request.
 - **WPA-Personal** - Pre-shared key of WPA.
 - **WPA2-Personal** - Pre-shared key of WPA2.
- **Encryption** - You can select either **Automatic**, or **TKIP** or **AES**.
- **Password** - You can enter **ASCII** or **Hexadecimal** characters. For **Hexadecimal**, the length should be between 8 and 64 characters; for **ASCII**, the length should be between 8 and 63 characters.
- **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/WPA2 - Enterprise

- **WEP** - Select 802.11 WEP security.
- **Version** - You can select one of following versions:
 - **Automatic** - Select **WPA** or **WPA2** automatically based on the wireless station's capability and request.
 - **WPA** - Wi-Fi Protected Access.
 - **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 uses.
- **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.

WEP

- **Type** - You can select one of following types:
 - **Automatic** - Select **Shared Key** or **Open System** authentication type automatically based on the wireless station's capability and request.
 - **Open System** - Select 802.11 Open System authentication.
 - **Shared Key** - Select 802.11 Shared Key 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 settings** - Select which of the four keys will be used and enter the matching WEP key information for your network in the selected key radio button. These values must be identical on all wireless stations in your network.
- **Key Type** - You can select the WEP key length (**64-bit**, or **128-bit**, or **152-bit**.) for encryption. "Disabled" means this WEP key entry is invalid.
 - For **64-bit** encryption - You can enter 10 hexadecimal digits (any combination of 0-9, a-f, A-F, and null key is not permitted) or 5 ASCII characters.

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

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

5.7.3 MAC Filtering

Selecting **Wireless > Wireless MAC Filtering** will allow you to set up some filtering rules to control wireless stations accessing the device, which depend on the station's MAC address on the following screen as shown Figure 4-9.



Figure 5-21 Wireless MAC address Filtering

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

- **MAC Address** - The wireless station's MAC address that you want to access.
- **Status** - The status of this entry either **Enabled** or **Disabled**.
- **Description** - A simple description of the wireless station.
- **Modify** - Here you can modify or delete an existing rule.

To disable the Wireless MAC Address Filters feature, keep the default setting, **Disable**.

To set up an entry, click **Enable**, and follow these instructions:

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

To Add a Wireless MAC Address filtering entry, clicking the **Add New...** button, and following these instructions: The “**Add or Modify Wireless MAC Address Filtering entry**” page will appear, shown in Figure 5-22.

Figure 5-22 Add or Modify Wireless MAC Address Filtering entry

1. Enter the appropriate MAC Address into the **MAC Address** field. The format of the MAC Address is XX-XX-XX-XX-XX-XX (X is any hexadecimal digit). For example, 00-0A-EB-B0-00-0B.
2. Enter a simple description of the wireless station in the **Description** field. For example, Wireless station A.
3. **Status** - Select **Enabled** or **Disabled** for this entry on the **Status** pull-down list.
4. Click the **Save** button to save this entry.

To add another entries, repeat steps 1~4.

To modify or delete an existing entry:

3. Click the **Modify** or **Delete** button in the **modify** column in the MAC Address Filtering Table.
4. Enter the value as desired in the **Add or Modify Wireless MAC Address Filtering entry** page, and click the **Save** button.

You can click the **Enable All** button to make all the Entries enabled, click the **Disable All** button to make all the Entries disabled, click the **Delete All** button to delete all the entries.

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

Note: If you enable the function and select the **Allow the stations specified by any enabled entries in the list to access for Filtering Rules**, and there are not any enable entries in the list, thus, no wireless stations can access the AP.

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

1. Click the **Enable** button to enable this function.
2. Select the radio button: **Allow the stations specified by any enabled entries in the list to access for Filtering Rules**.
3. Delete all or disable all entries if there are any entries already.
4. Click the **Add New...** button and enter the MAC address 00-0A-EB-00-07-BE in the **MAC Address** field, enter wireless station A in the **Description** field and select **Enabled** in the **Status** pull-down list. Click the **Save** button.
5. Click the **Add New...** button and enter the MAC address 00-0A-EB-00-07-5F in the **MAC Address** field, enter wireless station B in the **Description** field and select **Disabled** in the **Status** pull-down list. Click the **Save** button.

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

ID	MAC Address	Status	Description	Modify
1	00-0A-EB-00-07-BE	Enabled	wireless station A	Modify Delete
2	00-0A-EB-00-07-5F	Disabled	wireless station B	Modify Delete

 **Note:**

- 1) If you select the radio button **Deny the stations specified by any enabled entries in the list to access** for **Filtering Rules**, the wireless station B will still not be able to access the router, however, other wireless stations that are not in the list will be able to access the router.
- 2) If you enable the function and select the **Allow the stations specified by any enabled entries in the list to access** for **Filtering Rules**, and there are not any enable entries in the list, thus, no wireless stations can access the router.

5.7.4 Wireless Advanced

Selecting **Wireless > Wireless Advanced** will allow you to do some advanced settings for the device in the following screen as shown in Figure 5-23. As the configuration for each operation mode is almost the same, we take Access Point mode for example here.

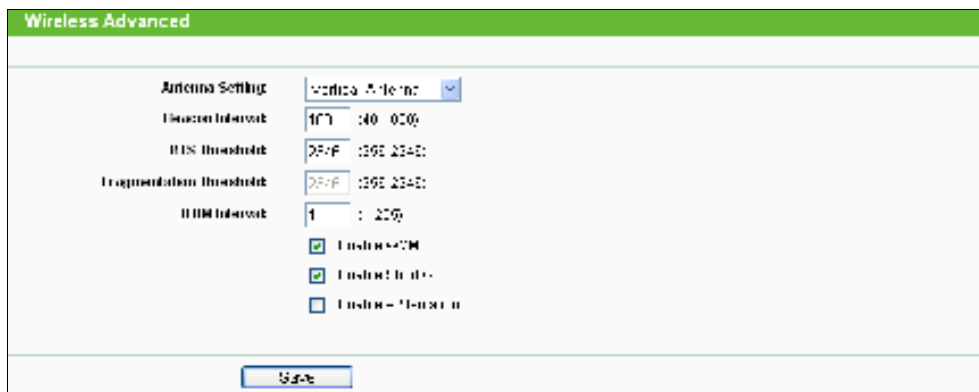


Figure 5-23 Wireless Advanced

- **Antenna Settings** - The polarization of an antenna. You can select Vertical Antenna, Horizontal Antenna or External Antenna.
- **Beacon Interval** - The beacons are the packets sent by the Device to synchronize a wireless network. Beacon Interval value determines the time interval of the beacons. You can specify a value between 20-1000 milliseconds. The default value is 100.
- **RTS Threshold** - Here you can specify the RTS (Request to Send) Threshold. If the packet is larger than the specified RTS Threshold size, the Device will send RTS frames to a particular receiving station and negotiate the sending of a data frame. The default value is 2346.
- **Fragmentation Threshold** - This value is the maximum size determining whether packets will be fragmented. Setting the Fragmentation Threshold too low may result in poor network performance since excessive packets. 2346 is the default setting and is recommended.
- **DTIM Interval** - This value determines the interval of the Delivery Traffic Indication Message (DTIM). You can specify the value between 1-255 Beacon Intervals. The default value is 1, which indicates the DTIM Interval is the same as Beacon Interval.
- **Enable WMM** - WMM function can guarantee the packets with high-priority messages being transmitted preferentially. It is strongly recommended enabled.
- **Enable Short GI** - This function is recommended, for it will increase the data capacity by reducing the guard interval time.
- **Enable AP Isolation** - Isolate all connected wireless stations so that wireless stations cannot access each other through WLAN. This function will be disabled if WDS/Bridge is enabled.

Note:

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

5.7.5 Antenna Alignment

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

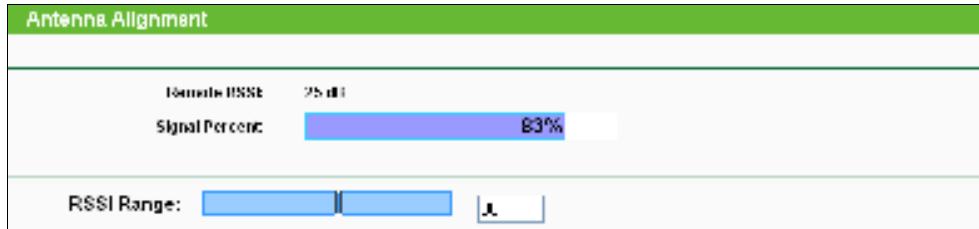


Figure 5-24 Antenna Alignment

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

Note:

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

5.7.6 Distance Setting

Selecting **Wireless > Distance Setting** will allow you to adjust the wireless range in outdoor conditions as shown in Figure 5-25. This is a critical feature required for stabilizing outdoor links. Enter the distance of your wireless link and the software will optimize the frame ACK timeout value automatically.

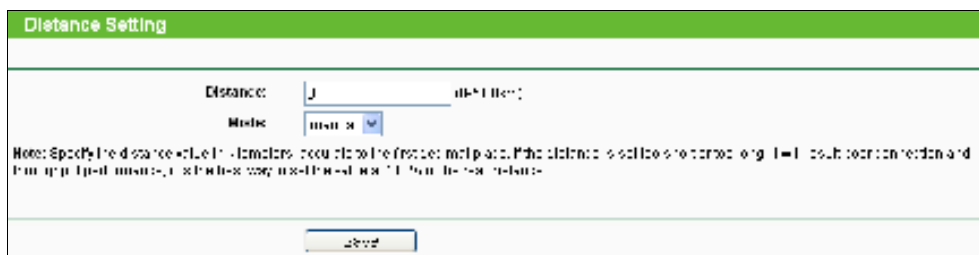


Figure 5-25 Distance Setting

- **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.

Note:

One hundred-meter is the smallest unit of this setting.

- **Mode** - You can select manual or indoor for the mode.

Click **Save** to keep your settings.

5.7.7 Throughput Monitor

Selecting **Wireless > Throughput Monitor** will help to watch wireless throughput information in the following screen shown in Figure 5-26.

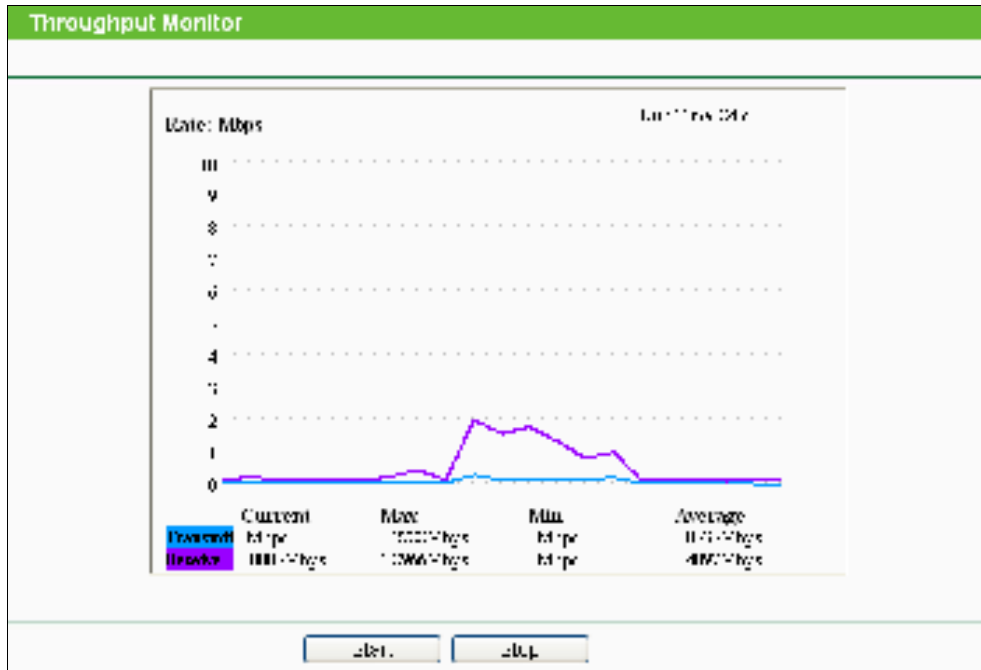


Figure 5-26 Wireless Throughput

- **Rate** - The Throughput unit.
- **Run Time** - How long this function is running.
- **Transmit**- Wireless transmit rate information.
- **Receive**- Wireless receive rate information.

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

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

5.7.8 Wireless Statistics

Selecting **Wireless > Wireless Statistics** will allow you to see the wireless transmission information in the following screen shown in Figure 5-27.

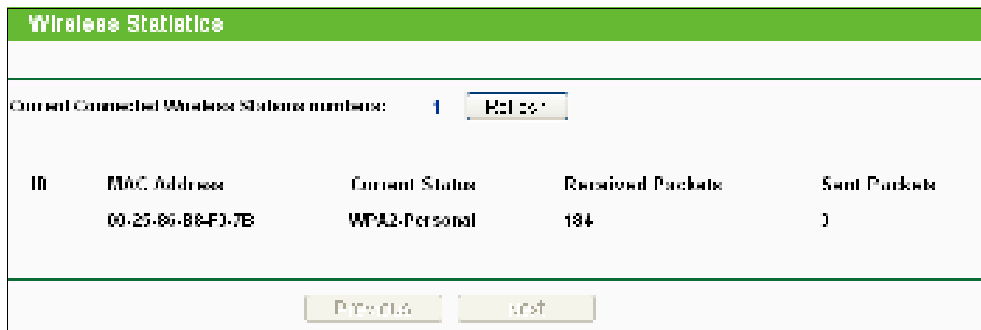


Figure 5-27 The router attached wireless stations

- **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.

5.8 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 5-28): **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.

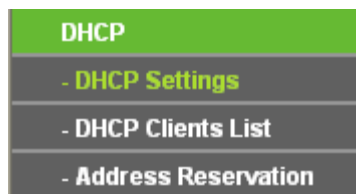


Figure 5-28 The DHCP menu

5.8.1 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 5-29).

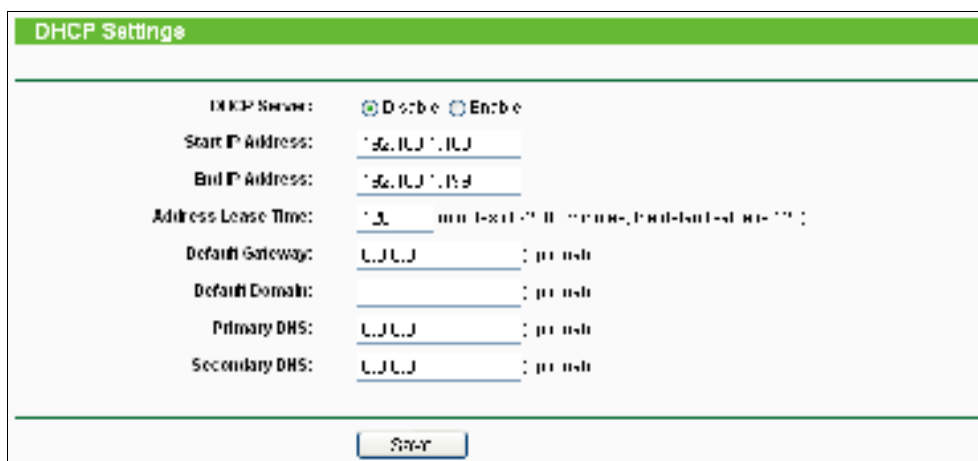


Figure 5-29 DHCP Settings

- **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. 192.168.0.100 is the default start IP address.
- **End IP Address** - This field specifies the last address in the IP Address pool. 192.168.0.199 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.

5.8.2 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 5-30).

DHCP Clients List				
ID	Client Name	MAC Address	Assigned IP	Lease Time
1	192.168.0.100	08:00:27:00:00:00	192.168.0.100	120 min

Figure 5-30 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.

5.8.3 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 5-31).

ID	MAC Address	Reserved IP Address	Status	Modify
<input type="button" value="Add New"/> <input type="button" value="Enabled"/> <input type="button" value="Disabled"/> <input type="button" value="Default"/>				
<input type="button" value="Previous"/> <input type="button" value="Next"/>				

Figure 5-31 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 5-32) 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.

MAC Address:	<input type="text" value="00:00:00:00:00:00"/>
Reserved IP Address:	<input type="text" value="192.168.1.20"/>
Status:	<input type="text" value="Enabled"/>
<input type="button" value="Save"/> <input type="button" value="Cancel"/>	

Figure 5-32 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:

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.

5.9 Forwarding

There are four submenus under the Forwarding menu (shown in Figure 5-33): **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.

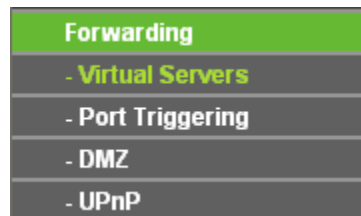


Figure 5-33 The Forwarding menu

5.9.1 Virtual Servers

Selecting **Forwarding > Virtual Servers** will allow you to set up virtual servers on the page as shown in Figure 5-34.

ID	Service Port	Internal Port	IP Address	Protocol	Status	Modify
1	2	2	192.168.0.121	TCP	Enabled	Modify

Buttons: Add New, Forward All, Disable All, Enable All, Refresh, New

Figure 5-34 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).
- **Internal Port** - The Internal Service Port number of the PC running the service application. You can leave it blank if the **Internal Port** is the same as the **Service Port**, or enter a specific port number when **Service Port** is a single one.
- **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 5-35)
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 5-35 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.

5.9.2 Port Triggering

Selecting **Forwarding > Port Triggering** will enable you to set up Port Triggering entries on the page as shown in Figure 5-36.

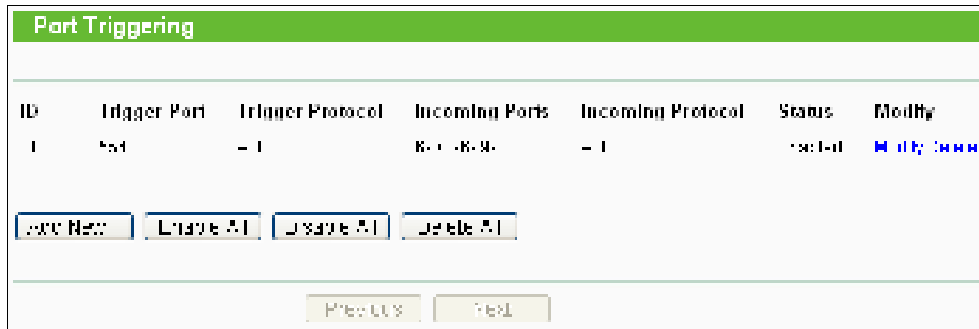


Figure 5-36 Port Triggering

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 5-37)
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.

The screenshot shows a web interface titled "Add or Modify a Port Triggering Entry". It contains the following fields and controls:

- Trigger Port:** A dropdown menu set to "LAN".
- Trigger Protocol:** A dropdown menu set to "All".
- Incoming Ports:** A text input field containing "20.0-20.0".
- Incoming Protocol:** A dropdown menu set to "All".
- Status:** A dropdown menu set to "Enabled".
- Common Applications:** A dropdown menu set to "Circus Time".

At the bottom of the form, there are two buttons: "Apply" and "Cancel".

Figure 5-37 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.

5.9.3 DMZ

Selecting **Forwarding > DMZ** will allow you to set up an DMZ host on the page as shown in Figure 5-38.

The screenshot shows a web interface titled "DMZ". It contains the following fields and controls:

- Current DMZ Status:** Two radio buttons, "Enable" and "Disable". The "Disable" button is selected.
- DMZ Host IP Address:** A text input field containing "1.1.1.1".

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

Figure 5-38 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.

5.9.4 UPnP

Selecting **Forwarding > UPnP** will enable you to configure the UPnP function on the page as shown in Figure 5-39:



Figure 5-39 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.

5.10 Security



Figure 5-40 The Security menu

There are four submenus under the Security menu as shown in Figure 5-40: **Basic Security**, **Advanced Security**, **Local Management** and **Remote Management**. Click any of them, and you will be able to configure the corresponding function.

5.10.1 Basic Security

Choose menu **Security > Basic Security**, and then you can configure the basic security in the screen as shown in Figure 5-41.

Basic Security	
Firewall	
SPI Firewall:	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
VPN	
PPTP Passthrough:	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
L2TP Passthrough:	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
IPSec Passthrough:	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
ALG	
FTP ALG:	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
HTTP ALG:	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
HTTPS ALG:	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
<input type="button" value="Save"/>	

Figure 5-41 Basic Security

- **Firewall** - Here you can enable or disable the Device's firewall.
 - **SPI Firewall** - Stateful Packet Inspection (SPI) helps to prevent cyber attacks by tracking more state per session. It validates that the traffic passing through the session conforms to the protocol. SPI Firewall is enabled by factory default. If you want all the computers on the LAN exposed to the outside world, you can disable it.
- **VPN** - VPN Passthrough must be enabled if you want to allow VPN tunnels using VPN protocols to pass through the Device.
 - **PPTP Passthrough** - PPTP (Point-to-Point Tunneling Protocol) allows the Point-to-Point Protocol (PPP) to be tunneled through an IP network. To allow PPTP tunnels to pass through the Device, click Enable.
 - **L2TP Passthrough** - L2TP (Layer Two Tunneling Protocol) is the method used to enable Point-to-Point sessions via the Internet on the Layer Two level. To allow L2TP tunnels to pass through the Device, click Enable.
 - **IPSec Passthrough** - IPSec (Internet Protocol security) is a suite of protocols for ensuring private, secure communications over IP (Internet Protocol) networks, through the use of cryptographic security services. To allow IPSec tunnels to pass through the Device, click **Enable**.
- **ALG** - It is recommended to enable Application Layer Gateway (ALG) because ALG allows customized Network Address Translation (NAT) traversal filters to be plugged into the gateway to support address and port translation for certain application layer "control/data" protocols such as FTP, TFTP, H323 etc.
 - **FTP ALG** - To allow FTP clients and servers to transfer data across NAT, click Enable.

- **TFTP ALG** - To allow TFTP clients and servers to transfer data across NAT, click Enable.
- **H323 ALG** - To allow Microsoft NetMeeting clients to communicate across NAT, click Enable.

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

5.10.2 Advanced Security

Choose menu **Security > Advanced Security**, and then you can protect the Device from being attacked by ICMP-Flood, UDP Flood and TCP-SYN Flood in the screen as shown in Figure 5-42.

Figure 5-42 Advanced Security

Note:

FLOOD Filtering will take effect only when the **Traffic Statistics** in **System Tools** is enabled.

- **Packets Statistics interval (5~60)** - The default value is 10. Select a value between 5 and 60 seconds in the pull-down list. The Packets Statistic interval value indicates the time section of the packets statistic. The result of the statistic used for analysis by ICMP-Flood, UDP Flood and TCP-SYN Flood.
- **DoS Protection** - Enable or Disable the DoS protection function. Only when it is enabled, will the flood filters be enabled.
- **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. When the current ICMP-FLOOD Packets number is beyond the set value, the Device 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 500. Enter a value between 5 ~ 3600. When the current UPD-FLOOD Packets number is beyond the set value, the Device 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. When the current TCP-SYN-FLOOD Packets numbers is beyond the set value, the Device will start up the blocking function immediately.
- **Ignore Ping Packet From WAN Port** - Enable or Disable Ignore Ping Packet From WAN Port. The default setting is Disabled. If enabled, the ping packet from Internet cannot access the Device.
- **Forbid Ping Packet From LAN Port** - Enable or Disable Forbid Ping Packet From LAN Port. The default setting is Disabled. If enabled, the ping packet from LAN cannot access the Device and defend against some viruses.

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

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

5.10.3 Local Management

Choose menu **Security > Local Management**, and then you can configure the management rule in the screen as shown in Figure 5-43. The management feature allows you to deny computers in LAN from accessing the Device.

The screenshot shows the 'Local Management' configuration interface. At the top, there is a green header with the text 'Local Management'. Below this, the 'Management Rules' section contains two radio buttons. The first radio button, labeled 'All the PCs on the LAN are allowed to access the Router's Web-Based Utility', is selected. The second radio button, labeled 'Only the PCs listed can browse the built-in web pages to perform Administrator tasks', is unselected. Below the second radio button, there are four input fields labeled 'MAC 1', 'MAC 2', 'MAC 3', and 'MAC 4'. At the bottom of the form, there is a field labeled 'Your PC's MAC Address:' containing the text '000000000000' and an 'Add' button. A 'Save' button is located at the bottom center of the page.

Figure 5-43 Local Management

By default, the radio button **All the PCs on the LAN are allowed to access the Router's Web-Based Utility** is selected. If you want to allow PCs with specific MAC Addresses to access the Setup page of the Device's Web-Based Utility locally, from inside the network, click the radio button **Only the PCs listed can browse the built-in web pages to perform Administrator tasks**, and then enter each MAC Address in a separate field. The format for the MAC Address is XX-XX-XX-XX-XX-XX (X is any hexadecimal digit). Only the PCs with the MAC address listed can use the password to browse the built-in web pages to perform Administrator tasks and all the others will be blocked.

After click the **Add** button, your PC's MAC Address will be placed in the Control List above.

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

Note:

If your PC is blocked and you want to access the Device again, use a pin to press and hold the **Reset Button** on the back panel about 5 seconds to reset the Device's factory defaults in the Device's Web-Based Utility.

5.10.4 Remote Management

Choose menu **Security > Remote Management**, and then you can configure the Remote Management function in the screen as shown in Figure 5-44. This feature allows you to manage your Device from a remote location via the Internet.

Remote Management	
Web Management Port:	<input type="text" value="80"/>
Remote Management IP Address:	<input type="text" value="0.0.0.0"/> (Enter 255.255.255.255 for all)
<input type="button" value="Save"/>	

Figure 5-44 Remote Management

- **Web Management Port** - Web browser access normally uses the standard HTTP service port 80. This Device'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 65535 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 Device 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 you should change 0.0.0.0 to a valid IP address. If set to be 255.255.255.255, then all the hosts can access the Device from Internet.

To access the Device, you should enter your Device's WAN IP address into your browser's address (in IE) or location (in Netscape) box, followed by a colon and the custom port number you set in the Web Management Port box.

- For example, if your Device's WAN address is 202.96.12.8 and you use port number 8080, enter `http://202.96.12.8:8080` in your browser. You will be asked for the Device's password. After successfully entering the password, you will be able to access the Device's web-based utility.

Note:

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

5.11 Parental Control

Choose menu **Parental Control**, and then you can configure the parental control in the screen as shown in Figure 5-45. The Parental Control function can be used to control the Internet activities of the children, their access to certain websites, as well as the time of surfing.

Figure 5-45 Parental Control Settings

- **Parental Control** - Check **Enable** if you want this function to take effect; otherwise check **Disable**.
- **MAC Address of Parental PC** - In this field, enter the MAC address of the controlling PC, or you can make use of the **Copy To Above** button below.
- **MAC Address of Your PC** - This field displays the MAC address of the PC that is managing this Device. If the MAC Address of your adapter is registered, you can click the **Copy To Above** button to fill this address to the MAC Address of Parental PC field above.
- **Website Description** - Description of the allowed website for the PC controlled.
- **Schedule** - The time period allowed for the PC controlled to access the Internet. For detailed information, please go to **Access Control > Schedule**.
- **Modify** - Here you can edit or delete an existing entry.
- **For example:** If you desire that the children's PC with MAC address 00-11-22-33-44-AA can access www.google.com on Saturday only while the parent PC with MAC address 00-11-22-33-44-BB is without any restriction, you should follow the settings below:
 1. Click **Parental Control** menu on the left to enter the Parental Control Settings page. Check **Enable** and enter the MAC address 00-11-22-33-44-BB in the MAC Address of Parental PC field.
 2. Click **Access Control > Schedule** on the left to enter the **Schedule** Settings page. Click **Add New...** button to create a new schedule with Schedule Description is **Schedule_1**, Day is **Sat** and Time is "**all day-24 hours**".
 3. Click **Parental Control** menu on the left to go back to the Parental Control Settings page, and then follow the instructions below.
 - 1) Click **Add New...** button.
 - 2) Enter 00-11-22-33-44-AA in the **MAC Address of Child PC** field.
 - 3) Enter **Allow Google** in the **Website Description** field.
 - 4) Enter **www.google.com** in the **Allowed Domain Name** field.
 - 5) Select **Schedule_1** you create just now from the **Effective Time** drop-down list.
 - 6) In **Status** field, select **Enable**.
 - 7) Click **Save** to complete the settings.

4. Then you will go back to the **Parental Control** Settings page and see the following list.

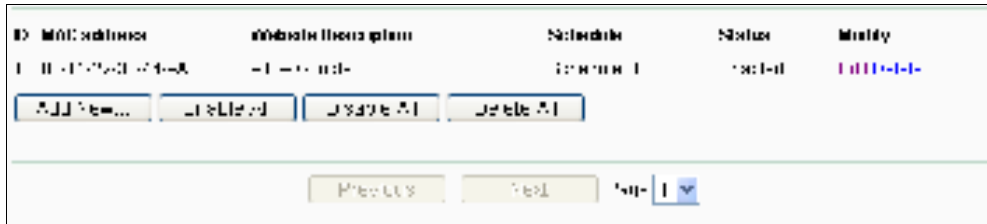


Figure 5-46 Parental Control List

Click the **Add New...** button to add a new Parental Control entry.

Click the **Enable All** button to enable all the rules in the list.

Click the **Disable All** button to disable all the rules in the list.

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

Click the **Next** button to go to the next page.

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

5.12 Access Control



Figure 5-47 Access Control

There are four submenus under the Access Control menu as shown in Figure 5-47: **Rule**, **Host**, **Target** and **Schedule**. Click any of them, and you will be able to configure the corresponding function.

The Device, providing convenient and strong **Internet access control** function, can control the Internet activities of hosts in the LAN. Moreover, you can flexibly combine the **Host List**, **Target List** and **Schedule** to restrict the Internet surfing of these hosts.

5.12.1 Rule

Choose menu **Access Control > Rule**, and then you can view and set Access Control rules in the screen as shown in Figure 5-48.



Figure 5-48 Access Control Rule Management

- **Enable Internet Access Control** - Select the check box to enable the Internet Access Control function, and then the **Default Filter Policy** can take effect.
- **Rule Name** - Here displays the name of the rule and this name is unique.
- **Host** - Here displays the host selected in the corresponding rule.
- **Target** - Here displays the target selected in the corresponding rule.
- **Schedule** - Here displays the schedule selected in the corresponding rule.
- **Status** - This field displays the status of the rule. **Enabled** means the rule will take effect, **Disabled** means the rule will not take effect.
- **Modify** - Here you can edit or delete an existing rule.

For example: If you desire to allow the host with MAC address 00-11-22-33-44-AA to access www.google.com only from 18:00 to 20:00 on Saturday and Sunday, and forbid other hosts in the LAN to access the Internet, you should follow the settings below:

1. Click the submenu **Rule** of **Access Control** in the left to return to the Rule List page. Select **Enable Internet Access Control** and choose **Allow the packets specified by any enabled access control policy to pass through the Device**.
2. We recommend that you click **Setup Wizard** button to finish all the following settings.
3. Click the submenu **Host** of **Access Control** on the left to enter the **Host Setting** page. Add a new entry with the Host Description as Host_1 and MAC Address as 00-11-22-33-44-AA.
4. Click the submenu **Target** of **Access Control** on the left to enter the **Target Settings** page. Add a new entry with the Target Description as Target_1 and Domain Name as www.google.com.
5. Click the submenu **Schedule** of **Access Control** on the left to enter the **Schedule Settings** page. Add a new entry with the Schedule Description as Schedule_1, Day as Sat and Sun, Start Time as 1800 and Stop Time as 2000.
6. Click **Add New...** button to add a new rule as follows:

- 1) In Rule Name field, create a name for the rule. Note that this name should be unique, for example Rule_1.
- 2) In Host field, select Host_1.
- 3) In Target field, select Target_1.
- 4) In Schedule field, select Schedule_1.
- 5) In Action field, select Allow.
- 6) In Status field, select Enable.
- 7) Click **Save** to complete the settings.
7. Then you will go back to the **Access Control Rule Management** page and see the following list.

ID	Rule Name	Host	Target	Schedule	Status	Modify
	Rule_1	Host_1	Target_1	Schedule_1	<input checked="" type="checkbox"/>	Edit Delete

Buttons: Add New..., Enable All, Disable All, Delete All, Next, Previous, Current Page: 1

Figure 5-49 Access Control List

- Click the **Add New...** button to add a new host list entry.
- Click the **Enable All** button to enable all the rules in the list.
- Click the **Disable All** button to disable all the rules in the list.
- Click the **Delete All** button to delete all the entries in the table.
- Click the **Next** button to go to the next page.
- Click the **Previous** button return to the previous page.

5.12.2 Host

Choose menu **Access Control > Host**, and then you can view and set a Host list in the screen as shown in Figure 5-50. The host list is necessary for the Access Control Rule.

ID	Host Description	Information	Modify
Host_1		08:00:12:34:56:78	Edit Delete

Buttons: Add New, Delete All, Previous, Next, Current Page: 1

Figure 5-50 Host Settings

- **Host Description** - Here displays the description of the host and this description is **unique**.
- **Information** - Here displays the information about the host. It can be IP or MAC.
- **Modify** - To modify or delete an existing entry.

- **For example:** If you desire to restrict the Internet activities of host with MAC address 00-11-22-33-44-AA, you should follow the settings below:
 1. Click **Add New...** button to enter the **Add or Modify a Host Entry** page.
 2. In Mode field, select MAC Address from the drop-down list.
 3. In Host Name field, create a unique description for the host, for example Host_1.
 4. In MAC Address field, enter 00-11-22-33-44-AA.
 5. Click **Save** to complete the settings.
 6. Go back to the **Host Settings** page and you will see the following list.



Figure 5-51 Host List

- Click the **Add New...** button to add a new host list entry.
- Click the **Delete All** button to delete all the entries in the table.
- Click the **Next** button to go to the next page.
- Click the **Previous** button return to the previous page.

5.12.3 Target

Choose menu **Access Control > Target**, and then you can view and set a Target list in the screen as shown in Figure 5-52. The target list is necessary for the Access Control Rule.

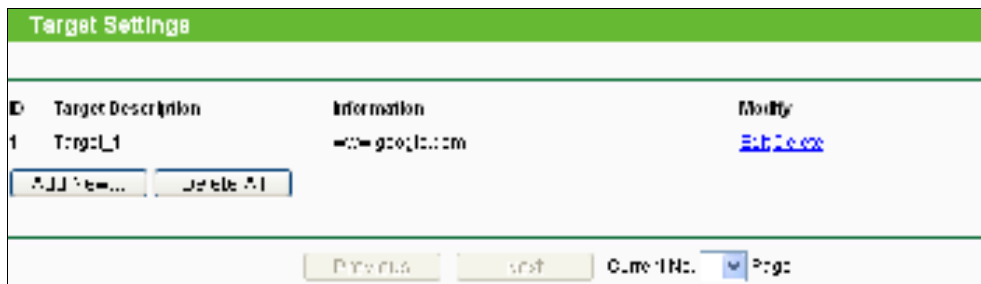


Figure 5-52 Target Settings

- **Target Description** - Here displays the description about the target and this description is **unique**.
- **Information** - The target can be IP address, port, or domain name.
- **Modify** - To modify or delete an existing entry.
- **For example:** If you desire to restrict the Internet activities of host with MAC address 00-11-22-33-44-AA in the LAN to access www.google.com only, you should first follow the settings below:
 1. Click **Add New...** button to enter **Add or Modify an Access Target Entry** page.
 2. In Mode field, select Domain Name from the drop-down list.
 3. In Target Description field, create a unique description for the target, for example Target_1.

4. In Domain Name field, enter www.google.com.
5. Click **Save** to complete the settings.
6. Go back to the **Target Settings** page and see the following list

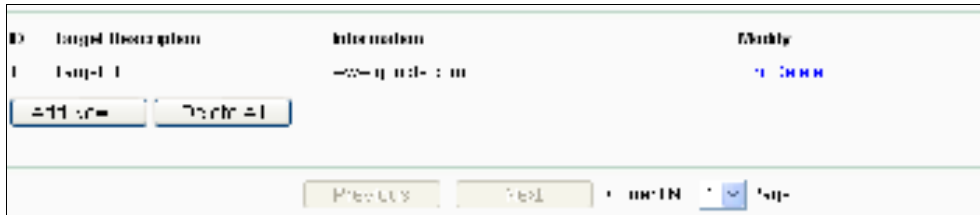


Figure 5-53 Access Target List

- Click the **Add New...** button to add a new target entry.
- Click the **Delete All** button to delete all the entries in the table.
- Click the **Next** button to go to the next page.
- Click the **Previous** button return to the previous page.

5.12.4 Schedule

Choose menu **Access Control > Schedule**, you can view and set a Schedule list in the next screen as shown in Figure 5-54. The Schedule list is necessary for the Access Control Rule.

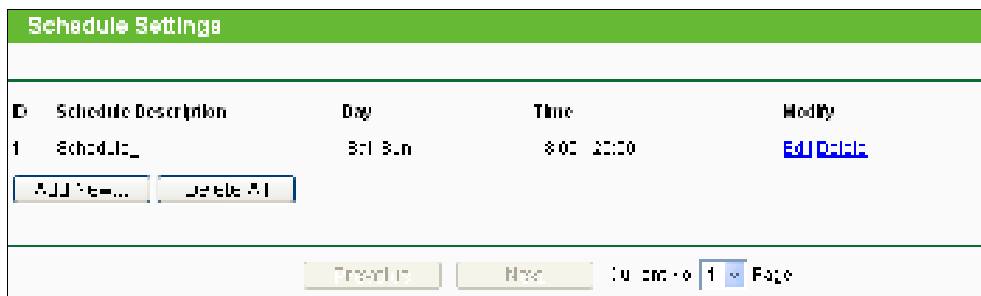


Figure 5-54 Schedule Settings

- **Schedule Description** - Here displays the description of the schedule and this description is **unique**.
- **Day** - Here displays the day(s) in a week.
- **Time** - Here displays the time period in a day.
- **Modify** - Here you can edit or delete an existing schedule.
- **For example:** If you desire to restrict the Internet activities of host with MAC address 00-11-22-33-44-AA to access www.google.com only from 18:00 to 20:00 on Saturday and Sunday, you should first follow the settings below:
 1. Click **Add New...** button to enter the **Advance Schedule Settings** page.
 2. In Schedule Description field, create a unique description for the schedule, for example Schedule_1.
 3. In Day field, choose **Select Days** and select Sat and Sun.
 4. In Time field, enter 1800 in Start Time and 2000 in Stop Time.
 5. Click **Save** to complete the settings.
 6. Go back to the **Schedule Settings** page and see the following list

ID	Schedule Description	Day	Time	Modify
1	Schedule...	Sun	00:00	Edit/Delete

Buttons: Add New..., Delete All, Previous, Next, Page 1

Figure 5-55 Schedule List

Click the **Add New...** button to add a new target entry.

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

Click the **Next** button to go to the next page.

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

5.13 Advanced Routing

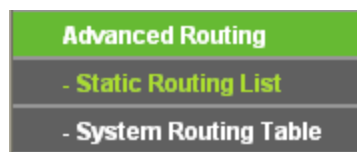


Figure 5-56 Access Control

There are two submenus under the Advanced Routing as shown in Figure 5-56: **Static Routing List** and **System Routing Table**. Click any of them, and you will be able to configure the corresponding function.

5.13.1 Static Routing List

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 5-57.

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

Buttons: Add New..., Enabled, Disabled, Deleted, Previous, Next

Figure 5-57 Static Routing

To add static routing entries:

1. Click the **Add New** button. (pop up Figure 5-58)
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.

Figure 5-58 Add or Modify a Static Route Entry

To modify or delete an existing entry:

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

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

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

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

5.13.2 System Routing Table

Choose menu **System Routing Table > Rule**, and then you can view all of the valid route entries in use in the screen as shown in Figure 5-59. The Destination IP address, Subnet Mask, Gateway, and Interface will be displayed for each entry.

ID	Destination Network	Subnet Mask	Gateway	Interface
1	132.138.1.0	255.255.255.0	0.0.0.0	eth0
2	132.138.0.0	255.255.255.0	0.0.0.0	eth0
3	0.0.0.0	0.0.0.0	0.0.0.0	eth0

Figure 5-59 System Routing Table

- **Destination Network** - The Destination Network is the address of the network or host to which the static route is assigned.
- **Subnet Mask** - The Subnet Mask determines which portion of an IP address is the network portion, and which portion is the host portion.
- **Gateway** - This is the IP address of the gateway device that allows for contact between the Device and the network or host.
- **Interface** - This interface tells you whether the Destination IP Address is on the **LAN & WLAN** (internal wired and wireless networks), the **WAN(Internet)**.

You can click the **Refresh** button to refresh the data displayed.

5.14 Bandwidth Control



Figure 5-60 Bandwidth Control

There are two submenus under the Bandwidth Control menu as shown in Figure 5-60: **Control Settings** and **Rules List**. Click any of them, and you will be able to configure the corresponding function. The detailed explanations for each submenu are provided below.

5.14.1 Control Settings

Choose menu **Bandwidth Control > Control Settings**, and then you can configure the Egress Bandwidth and Ingress Bandwidth in the next screen (shown in Figure 5-61). Their values should be configured less than 1000000Kbps.

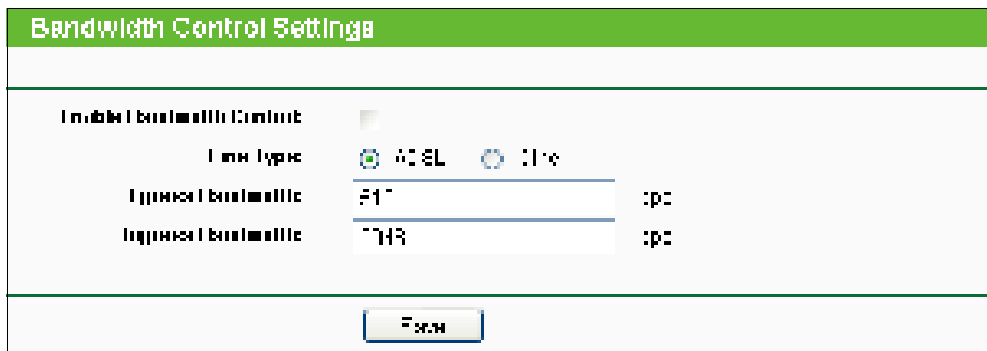


Figure 5-61 Bandwidth Control Settings

- **Enable Bandwidth Control** - If enabled, the Bandwidth Control rules will take effect.
- **Egress Bandwidth** - The upload speed through the WAN port.
- **Ingress Bandwidth** - The download speed through the WAN port.

5.14.2 Rules List

Choose menu “**Bandwidth Control > Rules List**”, and then you can view and configure the Bandwidth Control rules in the screen below.

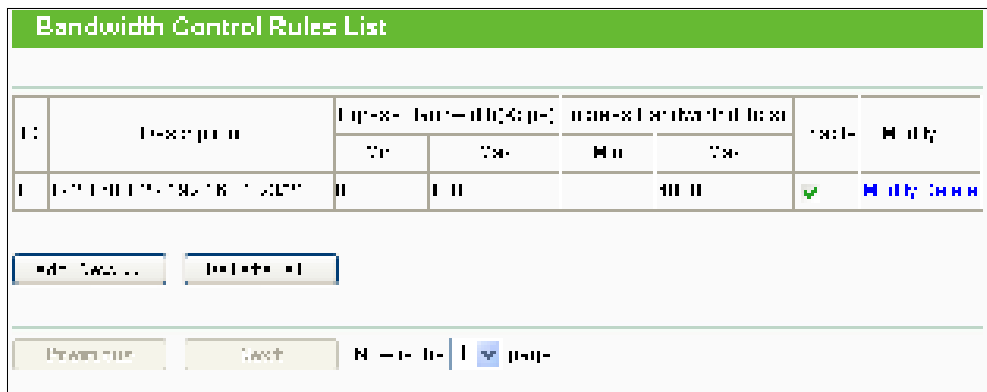


Figure 5-62 Bandwidth Control Rules List

- **ID** - The sequence of entry.

- **Description** - The information of description include address range, the port range and protocol of transport layer.
- **Egress Bandwidth** - The max upload speed which through the WAN port. The default number is 0.
- **Ingress Bandwidth** - The max download speed which through the WAN port. The default number is 0.
- **Enable** - Rule status, which shows whether the rule takes effect.
- **Modify** - Choose to modify or delete an existing entry.

5.15 IP & MAC Binding

ARP Binding is useful for controlling access of specific computers in the LAN. This page displays the **IP & MAC Binding Setting** table; you can operate it in accord with your desire.

There are two submenus under the IP & MAC Binding menu (shown in Figure 5-63): **Binding Setting** and **ARP List**. Click any of them, and you will be able to configure the corresponding function. The detailed explanations for each submenu are provided below.

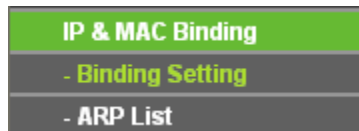


Figure 5-63 the IP & MAC Binding menu

5.15.1 Binding Setting

Selecting **IP & MAC Binding > Binding Setting** will allow you to configure the binding entries, as shown in Figure 5-64.

 A screenshot of a web interface titled "Binding Settings". At the top, there is a section for "ARP Binding" with radio buttons for "Disable" and "Enable" (the "Enable" button is selected), and a "Save" button. Below this is a table with the following columns: "ID", "MAC Address", "IP Address", "Bind", and "Modify". The table contains one row with the following data: ID: 1, MAC Address: 00-13-4F-A9-E6-CA, IP Address: 192.168.0.101, Bind: [checked checkbox], and Modify: [Modify Delete link]. Below the table are five buttons: "Add New", "Enable All", "Disable All", "Delete All", and "Find". At the bottom of the page are navigation buttons: "Previous", "Next", "Current No. 1", and "Page".

Figure 5-64 Binding Setting

- **MAC Address** - The MAC address of the controlled computer in the LAN.
- **IP Address** - The assigned IP address of the controlled computer in the LAN.
- **Bind** - Check this option to enable ARP binding for a specific device.
- **Modify** - To modify or delete an existing entry.

When you want to add or modify an IP & MAC Binding entry, you can click the **Add New** button or **Modify** button, and then you will go to the next page. This page is used for adding or modifying an IP & MAC Binding entry (shown in Figure 5-65).

Figure 5-65 IP & MAC Binding Setting (Add & Modify)

To add IP & MAC Binding entries, follow the steps below.

1. Click the **Add New...** button as shown in Figure 5-64.
2. Enter the MAC Address and IP Address.
3. Select the **Bind** checkbox.
4. Click the **Save** button to save it.

To modify or delete an existing entry, follow the steps below.

1. Find the desired entry in the table.
2. Click **Modify** or **Delete** as desired on the **Modify** column.

To find an existing entry, follow the steps below.

1. Click the **Find** button as shown in Figure 5-64.
2. Enter the MAC Address or IP Address.
3. Click the **Find** button in the page as shown in Figure 5-66.

Figure 5-66 Find IP & MAC Binding Entry

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

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

5.15.2 ARP List

Selecting **IP & MAC Binding > ARP List** will enable you to observe the computers in the LAN by checking the relationship of MAC address and IP address on the ARP list, and you could configure the items on the ARP list also. This page displays the ARP List; it shows all the existing IP & MAC Binding entries (shown in Figure 5-67).

ID	MAC Address	IP Address	Status	Configure
1	08-00-27-00-00-00	192.168.1.1	Bound	Load All
2	08-00-27-00-00-01	192.168.1.10	Bound	Load All

Figure 5-67 ARP List

- **MAC Address** - The MAC address of the controlled computer in the LAN.
- **IP Address** - The assigned IP address of the controlled computer in the LAN.
- **Status** - Indicates whether or not the MAC and IP addresses are bound.
- **Configure** - Load or delete an item.
 - **Load** - Load the item to the IP & MAC Binding list.
 - **Delete** - Delete the item.

Click the **Bind All** button to bind all the current items, available after enable.

Click the **Load All** button to load all items to the IP & MAC Binding list.

Click the **Refresh** button to refresh all items.

 **Note:**

An item could not be loaded to the IP & MAC Binding list if the IP address of the item has been loaded before. Error warning will prompt as well. Likewise, "Load All" only loads the items without interference to the IP & MAC Binding list.

5.16 Dynamic DNS

The Device offers a Dynamic Domain Name System (**DDNS**) feature. DDNS lets you assign a fixed host and domain name to a dynamic Internet IP address. It is useful when you are hosting your own website, FTP server, or other server behind the Device. Before using this feature, you need to sign up for DDNS service providers such as www.comexe.cn, www.dyndns.org, or www.no-ip.com. The Dynamic DNS client service provider will give you a password or key.

1. If the dynamic DNS **Service Provider** you select is www.comexe.cn, the page will appear as shown in Figure 5-68.

DDNS

Service Provider: Comexe (www.comexe.cn) [Go to register...](#)

Domain Name:

Domain Name:

Domain Name:

Domain Name:

Domain Name:

User Name:

Password:

Enable DDNS

Connection Status: DDNS not launching!

Figure 5-68 Comexe.cn DDNS Settings

➤ **To set up for DDNS, follow these instructions:**

- 1) Enter the **Domain Names** your dynamic DNS service provider gave.
- 2) Enter the **User Name** for your DDNS account.
- 3) Enter the **Password** for your DDNS account.
- 4) Click the **Login** button to login the DDNS service.

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

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

 **Note:**

If you want to login again with another account after a successful login, please click the Logout button, then input your new username and password and click the Login button.

2. If the dynamic DNS **Service Provider** you select is www.dyndns.org, the page will appear as shown in Figure 5-69.

The screenshot shows a web interface for configuring DDNS. At the top, a green bar contains the text 'DDNS'. Below this, the 'Service Provider' is set to 'DynDNS.org'. There are three input fields: 'User Name' (containing 'u-*****'), 'Password' (containing '*****'), and 'Human Name' (empty). Below these fields is a 'Connection Status' section with the text 'DDNS not logging' and two buttons labeled 'Login' and 'Logout'. At the bottom of the form is a 'Save' button.

Figure 5-69 DynDNS.org DDNS Settings

➤ **To set up for DDNS, follow these instructions:**

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

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

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

 **Note:**

If you want to login again with another account after a successful login, please click the Logout button, then input your new username and password and click the Login button.

3. If the dynamic DNS **Service Provider** you select is www.no-ip.com, the page will appear as shown in Figure 5-70.

Figure 5-70 No-ip.com DDNS Settings

➤ **To set up for DDNS, follow these instructions:**

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

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

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

 **Note:**

If you want to login again with another account after a successful login, please click the Logout button, then input your new username and password and click the Login button.

5.17 System Tools

System Tools option helps you to optimize the configuration of your device. You can upgrade the AP to the latest version of firmware as well as backup or restore the AP's configuration files. Ping Watch Dog can help to continuously monitor a particular connection to a remote host. Speed Test helps to test the connection speed to and from any reachable IP address on current network, especially when we are building wireless network between devices which are far away from each other. It's suggested that you change the default password to a more secure one because it controls access to the device's web-based management page. Besides, you can find out what happened to the system in System Log.

There are twelve submenus under the **System Tools** menu (shown as Figure 4-21): **SNMP**, **Time Settings**, **Diagnostic**, **Ping Watch Dog**, **Speed Test**, **Firmware Upgrade**, **Factory Defaults**, **Backup & Restore**, **Reboot**, **Password**, **System log** and **Statistics**. Clicking any of them will enable you to configure the corresponding function. The detailed explanations for each submenu are provided below.



Figure 5-71 The System Tools menu

5.17.1 Time Settings

Choose menu “**System Tools > Time Settings**”, and then you can configure the time on the following screen.

Figure 5-72 Time settings

- **Time Zone** - Select your local time zone from this pull-down list.
- **To set time manually:**
 1. Select your local time zone.
 2. Enter the **Date** in Month/Day/Year format.
 3. Enter the **Time** in Hour/Minute/Second format.
 4. Click **Save**.
- **For automatic time synchronization:**
 1. Enter the address or domain of the **NTP Server I** or **NTP Server II**.

2. Click the **Get GMT** button to get GMT from the Internet.

➤ **To enable Daylight Saving:**

1. Select the **Enable Daylight Saving** checkbox to enable daylight saving function.
2. Schedule the span of time which this function will effect. For example, if you want this function work at 0 o'clock(am) on the 1st Sunday of April and last until at 6 o'clock(pm) on the 2nd Saturday of September, you need choose "Apr", "1st", "Sun", "0am" at **Start** part and choose "Sep", "2nd", "Sat", "6pm" at the **End** part.
3. Click the **Save** button to effect this function.

👉 **Note:**

- 1) This setting will be used for some time-based functions such as firewall functions. These time dependant functions will not work if time is not set. So, it is important to specify time settings as soon as you successfully login to the Device.
- 2) The time will be lost if the Device is turned off.
- 3) The Device will automatically obtain GMT from the Internet if it is configured accordingly.
- 4) In daylight saving configuration, start time and end time shall be within one year and start time shall be earlier than end time.
- 5) After you enable daylight saving function, it will take action in one minute.

5.17.2 Diagnostic

Choose menu "**System Tools > Diagnostic**", and then you can transact Ping or Traceroute function to check connectivity of your network in the following screen.

The screenshot shows the 'Diagnostic Tools' configuration page. It features a green header bar. Underneath, the 'Diagnostic Parameters' section includes a 'Diagnostic Tool' selector with 'Ping' selected and 'Traceroute' unselected. Below this are five input fields: 'IP Address/Hostname' (empty), 'Ping Count' (value: 2), 'Ping Packet Size' (value: 54), 'Ping Timeout' (value: 3000), and 'Traceroute Max TTL' (value: 30). The 'Diagnostic Results' section contains a large text area for output and a 'Start' button at the bottom center.

Figure 5-73 Diagnostic Tools

➤ **Diagnostic Tool** - Click the radio button to select one diagnostic tool:

- **Ping** - This diagnostic tool troubleshoots connectivity, reachability, and name resolution to a given host or gateway.
- **Traceroute** - This diagnostic tool tests the performance of a connection.

 **Note:**

You can use ping/traceroute to test both numeric IP address or domain name. If pinging/tracerouting the IP address is successful, but pinging/tracerouting the domain name is not, you might have a name resolution problem. In this case, ensure that the domain name you are specifying can be resolved by using Domain Name System (DNS) queries.

- **IP Address/ Domain Name** - Enter the IP Address or Domain Name of the PC whose connection you wish to diagnose.
- **Ping Count** - Specifies the number of Echo Request messages sent. The default is 4.
- **Ping Packet Size** - Specifies the number of data bytes to be sent. The default is 64.
- **Ping Timeout** - Time to wait for a response, in milliseconds. The default is 800.
- **Traceroute Max TTL** - Set the maximum number of hops (max TTL to be reached) in the path to search for the target (destination). The default is 20.

Click the **Start** button to start the diagnostic procedure.

The **Diagnostic Results** page (as shown in Figure 4-25) displays the result of diagnosis.

If the result is similar to the following screen, the connectivity of the Internet is fine.

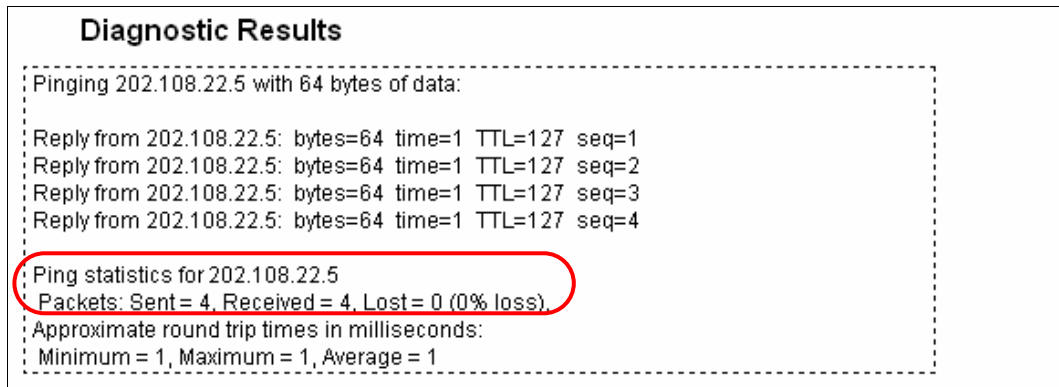


Figure 5-74 Diagnostic Results

 **Note:**

- 1) Only one user can use the diagnostic tools at one time.
- 2) "Ping Count", "Ping Packet Size" and "Ping Timeout" are Ping Parameters, and "Traceroute Max TTL" is Traceroute Parameter.

5.17.3 Firmware Upgrade

Choose menu "**System Tools > Firmware Upgrade**", and then you can update the latest version of firmware for the Device on the following screen.

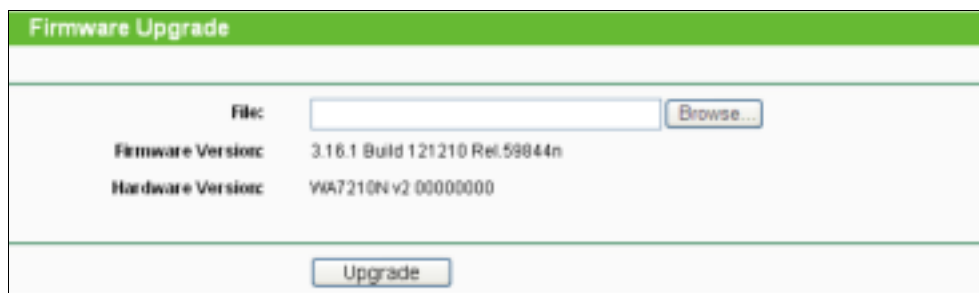


Figure 5-75 Firmware Upgrade

- **To upgrade the Device's firmware, follow these instructions:**

1. Download a most recent firmware upgrade file from our website (www.tp-link.com).
 2. Enter or select the path name where you save the downloaded file on the computer into the **File Name** blank.
 3. Click the **Upgrade** button.
 4. The Device will reboot while the upgrading has been finished.
- **Firmware Version** - Displays the current firmware version.
- **Hardware Version** - Displays the current hardware version. The hardware version of the upgrade file must accord with the current hardware version.

 **Note:**

The firmware version must correspond to the hardware. The upgrade process takes a few moments and the Device restarts automatically when the upgrade is complete. It is important to keep power applied during the entire process. Loss of power during the upgrade could damage the Device.

5.17.4 Factory Defaults

Choose menu “**System Tools > Factory Defaults**”, and you can restore the configurations of the Device to factory defaults on the following screen.

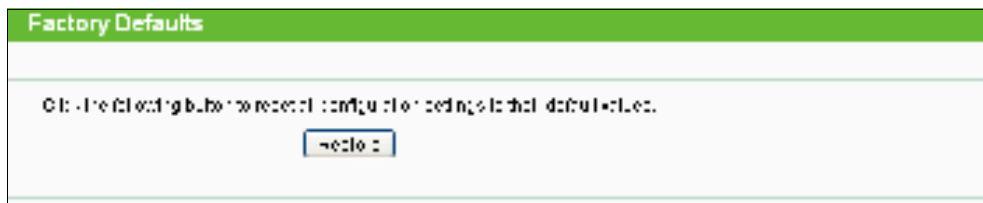


Figure 5-76 Restore Factory Default

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

- Default User Name - **admin**.
- Default Password - **admin**.
- Default IP Address - **192.168.0.254**.
- Default Subnet Mask - **255.255.255.0**.

 **Note:**

All changed settings will be lost when defaults are restored.

5.17.5 Backup & Restore

Choose menu “**System Tools > Backup & Restore**”, and then you can save the current configuration of the Device as a backup file and restore the configuration via a backup file as shown in Figure 4-30.



Figure 5-77 Backup & Restore

Click the **Backup** button to save all configuration settings to your local computer as a file.

- To restore the AP's configuration, follow these instructions:
 1. Click the **Browse** button to find the configuration file which you want to restore.
 2. Click the **Restore** button to update the configuration with the file whose path is the one you have input or selected in the blank.

 **Note:**

The current configuration will be covered with the uploading configuration file. Wrong process will lead the device unmanaged. The restoring process lasts for 20 seconds and the AP will restart automatically then. Keep the power of the AP on during the process, in case of any damage.

5.17.6 Reboot

Choose menu “**System Tools > Reboot**”, and then you can click the **Reboot** button to reboot the Device via the next screen.

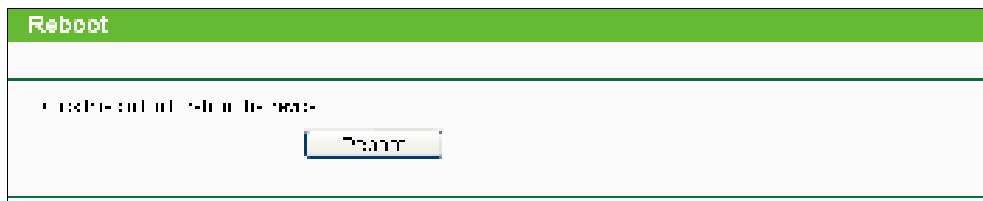


Figure 5-78 Reboot the Device

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

- Some settings of the Device will take effect only after rebooting, including:
 - Change the LAN IP Address (system will reboot automatically).
 - Change the DHCP Settings.
 - Change the Wireless configurations.
 - Change the Web Management Port.
 - Upgrade the firmware of the Device (system will reboot automatically.).
 - Restore the Device's settings to the factory defaults (system will reboot automatically.).
 - Update the configuration with the file (system will reboot automatically.).

5.17.7 Password

Choose menu “**System Tools > Password**”, and then you can change the factory default user name and password of the Device in the next screen as shown in Figure 4-32.

Figure 5-79 Password

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

 **Note:**

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

Click the **Save** button when finished.

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

5.17.8 System log

Choose menu “**System Tools > System Log**”, and then you can view the logs of the Device.

Figure 5-80 System Log

- **Auto Mail Feature** - Indicates whether auto mail feature is enabled or not.
- **Mail Settings** - Set the receiving and sending mailbox address, server address, validation information as well as the timetable for Auto Mail Feature.

Figure 5-81 Mail Account Settings

- **From** - Your mail box address.
- **To** - Recipient's address.
- **SMTP Server** - Your SMTP server.
- **Authentication** - Most SMTP Server requires Authentication.

 **Note:**

Only when you select **Authentication**, do you have to enter the User Name and Password in the following fields.

- **User Name** - Your mail account name.
- **Password** - Your mail account password.
- **Auto Mail Feature** will help you monitor how your Device is running. Everyday, at specified time, the Device will automatically send the log to specified mailbox. Every few hours, such as 2 hours, the Device will automatically send the log to specified mailbox.
- **Log Type** - By selecting the log type, only logs of this type will be shown.
- **Log Level** - By selecting the log level, only logs of this level will be shown.
- **Refresh** - Refresh the page to show the latest log list.
- **Save Log** - Click to save all the logs in a txt file.
- **Mail Log** - Click to send an email of current logs manually according to the address and validation information set in Mail Settings. The result will be shown in the later log soon.
- **Clear Log** - All the logs will be deleted from the Device permanently, not just from the page.

Click the **Next** button to go to the next page.

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

5.17.9 Statistics

Choose menu “**System Tools > Statistics**”, and then you can view the statistics of the Device, including total traffic and current traffic of the last Packets Statistic Interval.



Figure 5-82 Statistics

The Statistics page shows the network traffic of each PC on the LAN, including total traffic and the value of the last **Packets Statistic interval** in seconds.

- **Current Statistics Status** - Enabled or Disabled. The default value is disabled. To enable, click the Enable button. If disabled, the function of DoS protection in Security settings will be disabled.
- **Packets Statistics Interval** - The default value is 10. Select a value between 5 and 60 seconds in the pull-down list. The Packets Statistic interval value indicates the time section of the packets statistic.
- **Sorted Rules** - Choose how displayed statistics are sorted.

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

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

Click the **Reset All** button to reset the values of all entries to zero.

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

➤ Statistics Table

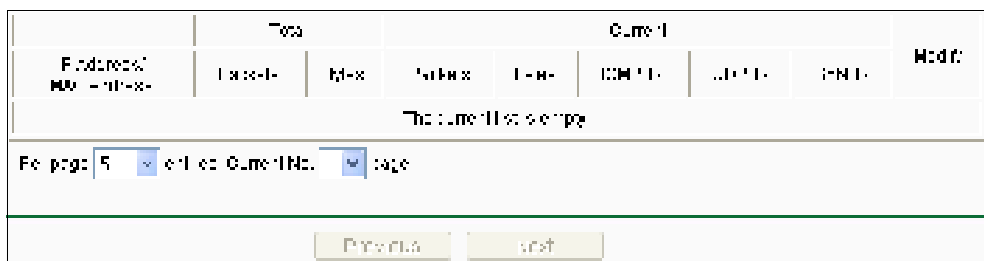


Figure 5-83 Statistics Table

- **IP Address/MAC Address** - The IP Address and MAC address are displayed with related statistics.

- **Total**
 - **Packets** - The total number of packets received and transmitted by the Device.
 - **Bytes** - The total number of bytes received and transmitted by the Device.
- **Current**
 - **Packets** - The total number of packets received and transmitted in the last Packets Statistics interval seconds.
 - **Bytes** - The total number of bytes received and transmitted in the last Packets Statistics interval seconds.
 - **ICMP Tx** - The number of ICMP packets transmitted to the WAN per second at the specified Packets Statistics interval. It is shown like "current transmitting rate / Max transmitting rate".
 - **UDP Tx** - The number of UDP packets transmitted to the WAN per second at the specified Packets Statistics interval. It is shown like "current transmitting rate / Max transmitting rate".
 - **TCP SYN Tx** - The number of TCP SYN packets transmitted to the WAN per second at the specified Packets Statistics interval. It is shown like "current transmitting rate / Max transmitting rate".
- **Modify**
 - **Reset** - Reset the values of the entry to zero.
 - **Delete** - Delete the existing entry in the table.

Appendix A: FAQ

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

- 1) First, configure the ADSL Modem configured in RFC1483 bridge model.
- 2) Connect the Ethernet cable from your ADSL Modem to the WAN port on the router. The telephone cord plugs into the Line port of the ADSL Modem.
- 3) Login to the router, click the "Network" menu on the left of your browser, and click "WAN" submenu. On the WAN page, select "PPPoE" for WAN Connection Type. Type user name in the "User Name" field and password in the "Password" field, finish by clicking "Connect".

WAN Connection Type:

PPPoE Connection:

User Name:

Password:

Figure A-1 PPPoE Connection Type

- 4) If your ADSL lease is in "pay-according-time" mode, select "Connect on Demand" or "Connect Manually" for the Internet connection mode. Type an appropriate number for "Max Idle Time" to avoid wasting paid time. Otherwise, you can select "Auto-connecting" for the Internet connection mode.

Wan Connection Mode:

Connect on Demand
Max Idle Time: minutes (0 means remain active at all times.)

Connect Automatically

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

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

Disconnected!

Figure A-2 PPPoE Connection Mode

Note:

- 1) Sometimes the connection cannot be disconnected although you specify a time to Max Idle Time, since some applications is visiting the Internet continually in the background.
- 2) If you are a Cable user, please configure the router following the above steps.

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

- 1) Login to the router, click the "Network" menu on the left of your browser, and click "WAN" submenu. On the WAN page, select "Dynamic IP" for "WAN Connection Type", finish by clicking "Save".
- 2) Some ISPs require that you register the MAC Address of your adapter, which is connected to your cable/DSL Modem during installation. If your ISP requires MAC register, login to the

router and click the "Network" menu link on the left of your browser, and then click "MAC Clone" submenu link. On the "MAC Clone" page, if your PC's MAC address is proper MAC address, click the "Clone MAC Address" button and your PC's MAC address will fill in the "WAN MAC Address" field. Or else, type the MAC Address into the "WAN MAC Address" field. The format for the MAC Address is XX-XX-XX-XX-XX-XX. Then click the "Save" button. It will take effect after rebooting.

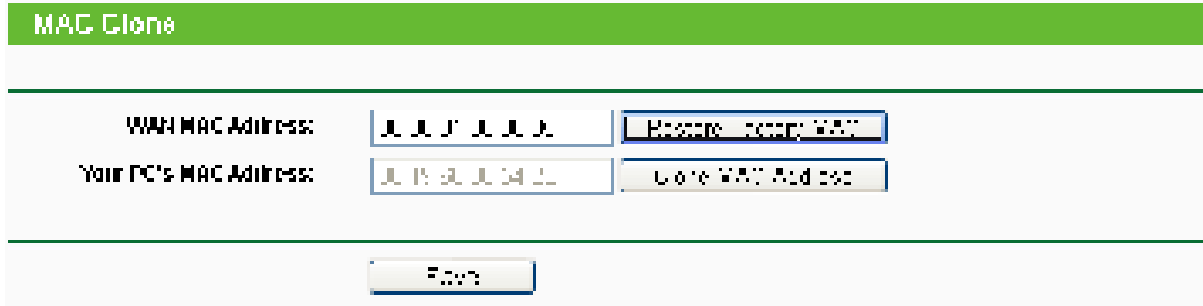


Figure A-3 MAC Clone

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

- 1) If you start Netmeeting as a sponsor, you don't need to do anything with the router.
- 2) If you start as a response, you need to configure Virtual Server or DMZ Host.
- 3) How to configure Virtual Server: Login to the router, click the "Forwarding" menu on the left of your browser, and click "Virtual Servers" submenu. On the "Virtual Server" page, click **Add New**, then on the "Add or Modify a Virtual Server" page, enter "1720" into the blank behind the "Service Port", and your IP address behind the IP Address, assuming 192.168.0.169 for an example, remember to "Enable" and "Save".



Figure A-4 Virtual Servers

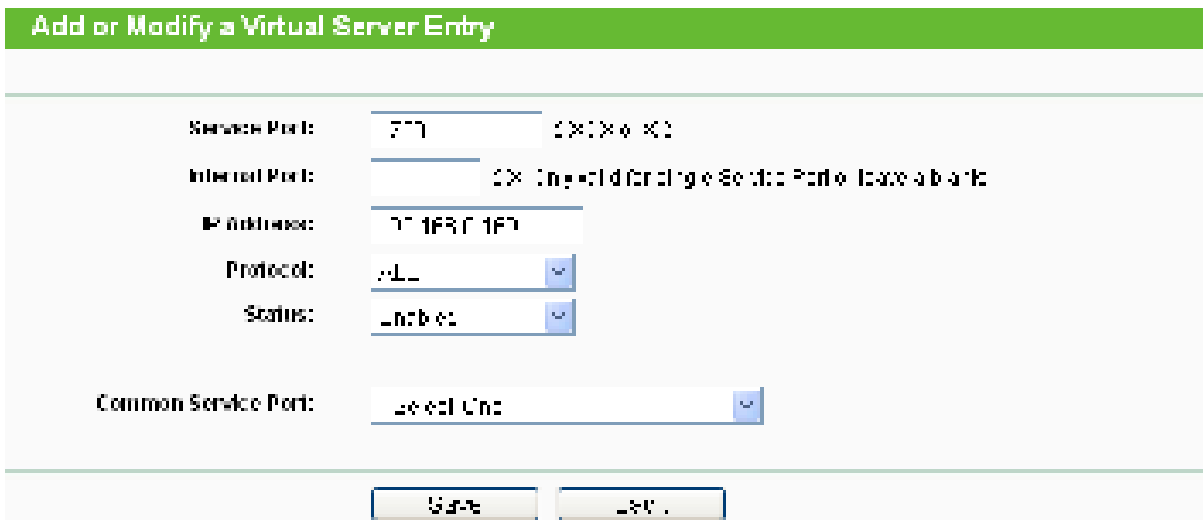


Figure A-5 Add or Modify a Virtual server Entry

Note:

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

- 4) How to enable DMZ Host: Login to the router, click the “Forwarding” menu on the left of your browser, and click “DMZ” submenu. On the “DMZ” page, click “Enable” radio and type your IP address into the “DMZ Host IP Address” field, using 192.168.0.169 as an example, remember to click the **Save** button.

Figure A-6 DMZ

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

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

Figure A-7 Remote Management

Note:

If the above configuration takes effect, to configure to the router by typing <http://192.168.0.254:88/> (the router’s LAN IP address: Web Management Port) in the address field of the Web browser.

- 3) Login to the router, click the “Forwarding” menu on the left of your browser, and click the “Virtual Servers” submenu. On the “Virtual Server” page, click **Add New**, then on the “Add or Modify a Virtual Server” page, enter “80” into the blank behind the “Service Port”, and your IP address behind the IP Address, assuming 192.168.0.188 for an example, remember to “Enable” and “Save”.

Virtual Servers						
ID	Service Port	Internal Port	IP Address	Protocol	Status	Modify
<div style="display: flex; justify-content: space-around;"> Add New Refresh All Delete All Export All </div>						
<div style="display: flex; justify-content: center; gap: 20px;"> Previous Next </div>						

Figure A-8 Virtual Servers

Add or Modify a Virtual Server Entry	
Service Port:	<input type="text" value="80"/> (0-65535)
Internal Port:	<input type="text" value="80"/> (0-65535) (Single Service Port only)
IP Address:	<input type="text" value="192.168.1.1"/> (0-255)
Protocol:	<input type="text" value="ALL"/> (v)
Status:	<input type="text" value="Enabled"/> (v)
Common Service Port:	<input type="text" value="Select One"/> (v)
<div style="display: flex; justify-content: center; gap: 20px;"> Save Cancel </div>	

A-9 Add or Modify a Virtual server Entry

5. The wireless stations cannot connect to the router.

- 1) Make sure the "AP Router Radio" is enabled.
- 2) Make sure that the wireless stations' SSID accord with the router's SSID.
- 3) Make sure the wireless stations have the right KEY for encryption when the router is encrypted.
- 4) If the wireless connection is ready, but you can't access the router, check the IP Address of your wireless stations.

Appendix B: Configuring the PC

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

1. Configure TCP/IP component

- 1) On the Windows taskbar, click the **start** button, and then click **Control Panel**.
- 2) Click the **Network and Internet Connections** icon, and then click on the **Network Connections** tab in the appearing window.
- 3) Right click the icon that showed below, select Properties on the prompt page.

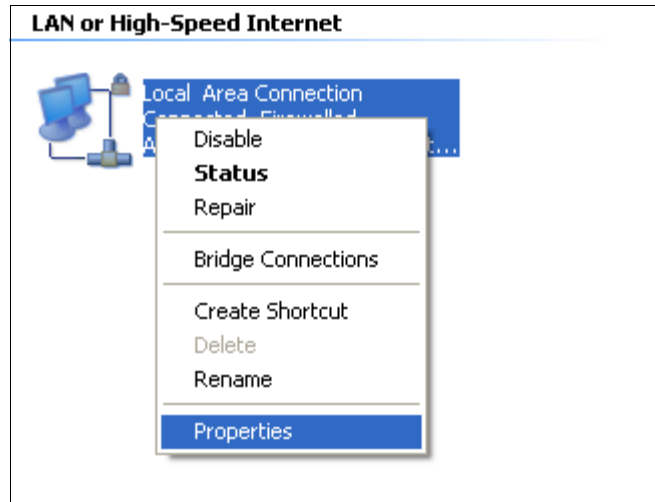


Figure B-1

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

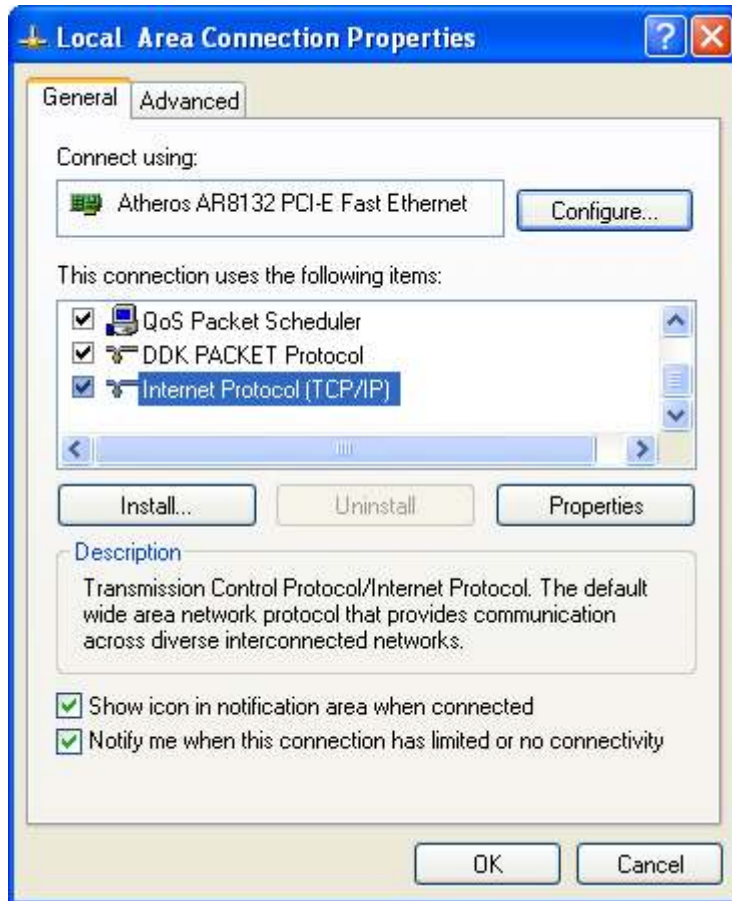


Figure B-2

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

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

➤ **Setting IP address automatically**

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

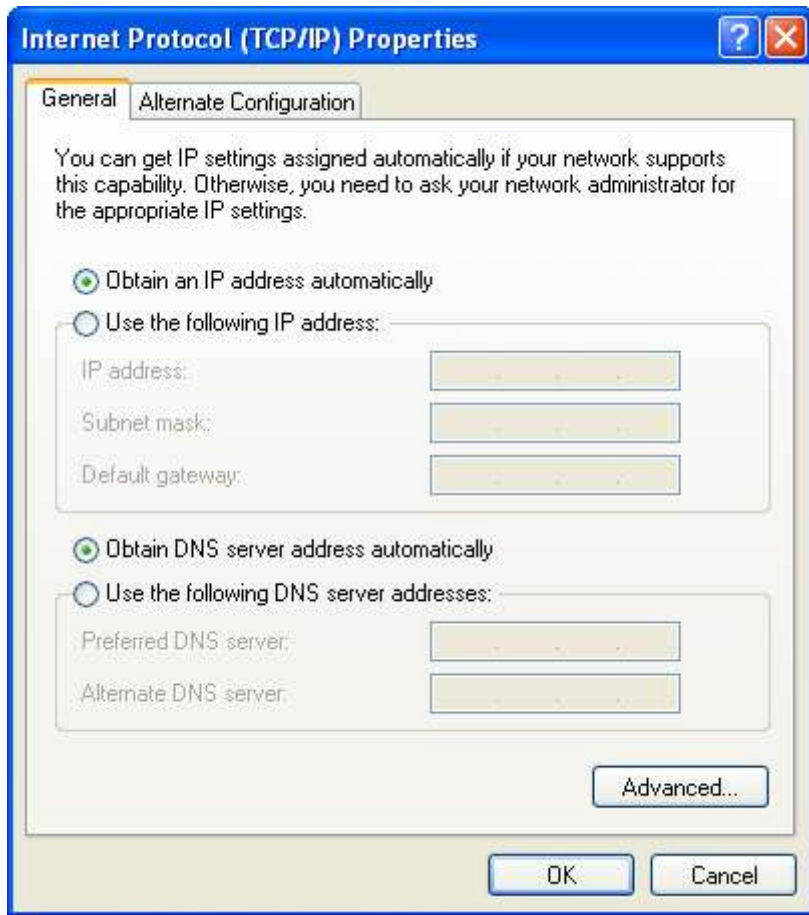


Figure B-3

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

➤ **Setting IP address manually**

1. Select **Use the following IP address** radio button. And the following items available
2. If the router's LAN IP address is 192.168.0.254, specify the **IP address** as 192.168.0.x (x is from 2 to 253), and the **Subnet mask** as 255.255.255.0.
3. Type the router's LAN IP address (the default IP is 192.168.0.254) into the **Default gateway** field.
4. Select **Use the following DNS server addresses**. In the **Preferred DNS Server** field you can enter the same value as the **Default gateway** or type the local DNS server IP address.

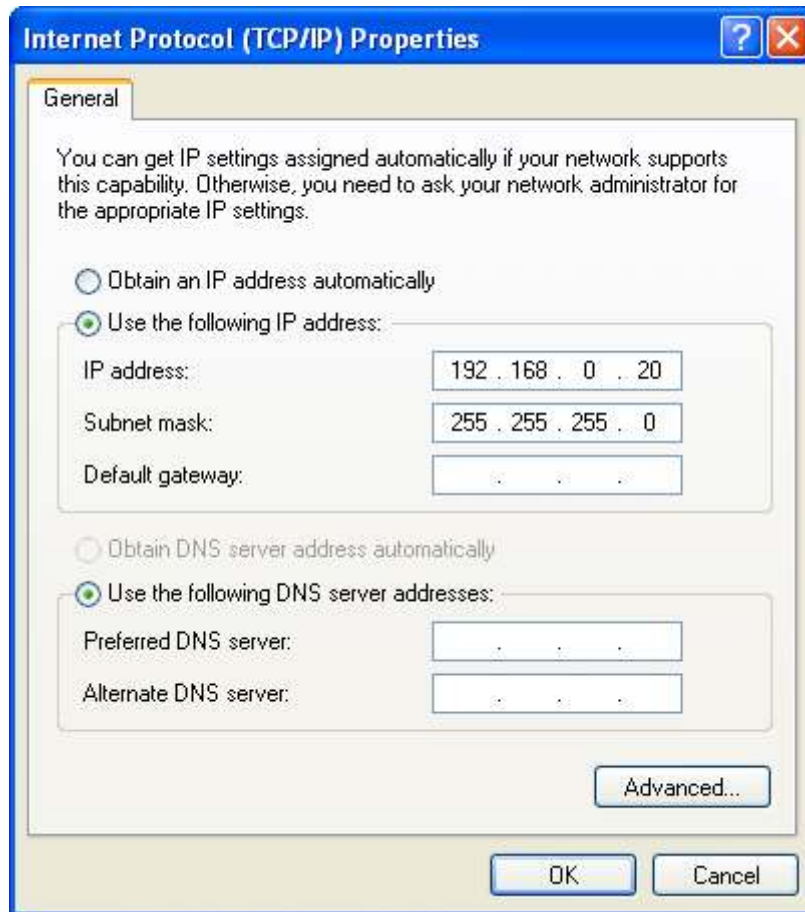


Figure B-4

Now:

Click **OK** to keep your settings.

Appendix C: Specifications

General	
Standards and Protocols	IEEE 802.3, 802.3u, 802.11b, 802.11g and 802.11n, TCP/IP, DHCP
Safety & Emission	FCC, CE
Ports	One 10/100M Auto-Negotiation LAN RJ45 port, supporting passive PoE
Cabling Type	10BASE-T: UTP category 3, 4, 5 cable (maximum 100m) EIA/TIA-568 100Ω STP (maximum 100m) 100BASE-TX: UTP category 5, 5e cable (maximum 100m) EIA/TIA-568 100Ω STP (maximum 100m)
Wireless	
Wireless Data Rates	up to 150 Mbps
Wireless Encryptions	64/128/152-bit WEP, WPA/WPA2, WPA-PSK/WPA2-PSK
Physical and Environment	
Working Temperature	-30°C~70°C
Working Humidity	10% ~ 90% RH, Non-condensing
Storage Temperature	-40°C~70°C (-40°F~158°F)
Storage Humidity	5% ~ 90% RH, Non-condensing

Appendix D: Glossary

- **802.11n** - 802.11n builds upon previous 802.11 standards by adding MIMO (multiple-input multiple-output). MIMO uses multiple transmitter and receiver antennas to allow for increased data throughput via spatial multiplexing and increased range by exploiting the spatial diversity, perhaps through coding schemes like Alamouti coding. The Enhanced Wireless Consortium (EWC) was formed to help accelerate the IEEE 802.11n development process and promote a technology specification for interoperability of next-generation wireless local area networking (WLAN) products.
- **802.11b** - The 802.11b standard specifies a wireless networking at 11 Mbps using direct-sequence spread-spectrum (DSSS) technology and operating in the unlicensed radio spectrum at 2.4GHz, and WEP encryption for security. 802.11b networks are also referred to as Wi-Fi networks.
- **802.11g** - specification for wireless networking at 54 Mbps using direct-sequence spread-spectrum (DSSS) technology, using OFDM modulation and operating in the unlicensed radio spectrum at 2.4GHz, and backward compatibility with IEEE 802.11b devices, and WEP encryption for security.
- **DDNS (Dynamic Domain Name System)** - The capability of assigning a fixed host and domain name to a dynamic Internet IP Address.
- **DHCP (Dynamic Host Configuration Protocol)** - A protocol that automatically configure the TCP/IP parameters for the all the PC(s) that are connected to a DHCP server.
- **DMZ (Demilitarized Zone)** - A Demilitarized Zone allows one local host to be exposed to the Internet for a special-purpose service such as Internet gaming or videoconferencing.
- **DNS (Domain Name System)** – An Internet Service that translates the names of websites into IP addresses.
- **Domain Name** - A descriptive name for an address or group of addresses on the Internet.
- **DoS (Denial of Service)** - A hacker attack designed to prevent your computer or network from operating or communicating.
- **DSL (Digital Subscriber Line)** - A technology that allows data to be sent or received over existing traditional phone lines.
- **ISP (Internet Service Provider)** - A company that provides access to the Internet.
- **MTU (Maximum Transmission Unit)** - The size in bytes of the largest packet that can be transmitted.
- **NAT (Network Address Translation)** - NAT technology translates IP addresses of a local area network to a different IP address for the Internet.
- **PPPoE (Point to Point Protocol over Ethernet)** - PPPoE is a protocol for connecting remote hosts to the Internet over an always-on connection by simulating a dial-up connection.
- **SSID** - A **S**ervice **S**et **I**dentification is a thirty-two character (maximum) alphanumeric key identifying a wireless local area network. For the wireless devices in a network to communicate with each other, all devices must be configured with the same SSID. This is typically the configuration parameter for a wireless PC card. It corresponds to the ESSID in the wireless Access Point and to the wireless network name.
- **WEP (Wired Equivalent Privacy)** - A data privacy mechanism based on a 64-bit or 128-bit or 152-bit shared key algorithm, as described in the IEEE 802.11 standard.
- **Wi-Fi** - is a trademark of the Wi-Fi Alliance, founded in 1999 as Wireless Internet Compatibility

Alliance (WICA), comprising more than 300 companies, whose products are certified by the Wi-Fi Alliance, based on the IEEE 802.11 standards (also called Wireless LAN (WLAN) and Wi-Fi). This certification warrants interoperability between different wireless devices.

- **WISP - Wireless Internet Service Providers (WISPs)** are Internet service providers with networks built around wireless networking. The technology used ranges from commonplace Wi-Fi mesh networking or proprietary equipment designed to operate over open 900MHz, 2.4GHz, 4.9, 5.2, 5.4, and 5.8GHz bands or licensed frequencies in the UHF or MMDS bands.
- **WLAN (Wireless Local Area Network)** - A group of computers and associated devices communicate with each other wirelessly, which network serving users are limited in a local area.