TP-LINK®

User Guide

TL-MR3020

Portable 3G/4G Wireless N Router

Rev: 1.1.2
1910010551

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

CE 1588

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: Portable 3G/4G Wireless N Router

Model No.: **TL-MR3020**

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 V2.2.1:2012

EN 55022:2010

EN 55024:2010

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

EN 61000-3-3:2008

EN60950-1:2006+A11：2009+A1:2010+A12:2011

EN62311:2008

The product carries the CE Mark:

CE1588

Person is 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 Router 2

1.2 Conventions 2

1.3 Main Features 3

1.4 Panel Layout 4

1.4.1 The Front Panel 4

1.4.2 The Rear Panel 5

Chapter 2. Connecting the Router **6**

2.1 System Requirements 6

2.2 Installation Environment Requirements 6

2.3 Connecting the Router 6

Chapter 3. Quick Installation Guide **10**

3.1 3G/4G Router Mode 10

3.1.1 PC configuration 10

3.1.2 Connect to Network 10

3.1.3 Router Configuration 10

3.2 WISP Mode 14

3.2.1 PC configuration 14

3.2.2 Connect to Network 14

3.2.3 Router Configuration 15

3.3 AP Mode 19

3.3.1 PC configuration 19

3.3.2 Connect to Network 19

3.3.3 Router Configuration 19

Chapter 4. Router Configuration-3G/4G Router Mode **27**

4.1 Login 27

4.2 Status 27

4.3 Quick Setup 28

4.4 WPS 28

4.5 Network 35

4.5.1 Internet Access 35

4.5.2 3G/4G 37

4.5.3 WAN 41

4.5.4 MAC Clone 51
4.5.5 LAN 51
4.6 Wireless 52
4.6.1 Wireless Settings 52
4.6.2 Wireless Security 55
4.6.3 Wireless MAC Filtering 58
4.6.4 Wireless Advanced 60
4.6.5 Wireless Statistics 61
4.7 DHCP 62
4.7.1 DHCP Settings 62
4.7.2 DHCP Clients List 64
4.7.3 Address Reservation 64
4.8 Forwarding 65
4.8.1 Virtual Servers 66
4.8.2 Port Triggering 67
4.8.3 DMZ 69
4.8.4 UPnP 70
4.9 Security 71
4.9.1 Basic Security 71
4.9.2 Advanced Security 73
4.9.3 Local Management 74
4.9.4 Remote Management 75
4.10 Parental Control 76
4.11 Access Control 79
4.11.1 Rule 79
4.11.2 Host 85
4.11.3 Target 87
4.11.4 Schedule 89
4.12 Advanced Routing 90
4.12.1 Static Routing List 91
4.12.2 System Routing Table 92
4.13 Bandwidth Control 92
4.13.1 Control Settings 93
4.13.2 Rules List 93
4.14 IP & MAC Binding 94
4.14.1 Binding Settings 94
4.14.2 ARP List 96

4.15 Dynamic DNS 97
4.15.1 Comexe.cn DDNS 97
4.15.2 Dyndns.org DDNS 98
4.15.3 No-ip.com DDNS 99
4.16 System Tools 100
4.16.1 Time Settings 101
4.16.2 Diagnostic 102
4.16.3 Firmware Upgrade 104
4.16.4 Factory Defaults 105
4.16.5 Backup & Restore 105
4.16.6 Reboot 106
4.16.7 Password 107
4.16.8 System Log 107
4.16.9 Working Mode 108
4.16.10 Statistics 109
Chapter 5. Router Configuration—WISP Mode 111
5.1 Login 111
5.2 Status 111
5.3 Quick Setup 112
5.4 WPS 112
5.5 Network 119
5.5.1 WAN 119
5.5.2 MAC Clone 129
5.5.3 LAN 129
5.6 Wireless 130
5.6.1 Wireless Settings 130
5.6.2 Wireless Security 133
5.6.3 Wireless MAC Filtering 136
5.6.4 Wireless Advanced 139
5.6.5 Wireless Statistics 140
5.7 DHCP 141
5.7.1 DHCP Settings 141
5.7.2 DHCP Clients List 142
5.7.3 Address Reservation 143
5.8 Forwarding 144
5.8.1 Virtual Servers 144
5.8.2 Port Triggering 146

5.8.3 DMZ 148
5.8.4 UPnP 149
5.9 Security 150
5.9.1 Basic Security 150
5.9.2 Advanced Security 151
5.9.3 Local Management 153
5.9.4 Remote Management 154
5.10 Parental Control 155
5.11 Access Control 158
5.11.1 Rule 158
5.11.2 Host 163
5.11.3 Target 165
5.11.4 Schedule 167
5.12 Advanced Routing 168
5.12.1 Static Routing List 169
5.12.2 System Routing Table 170
5.13 Bandwidth Control 170
5.13.1 Control Settings 171
5.13.2 Rules List 171
5.14 IP & MAC Binding Setting 172
5.14.1 Binding Settings 172
5.14.2 ARP List 174
5.15 Dynamic DNS 175
5.15.1 Comexe.cn DDNS 175
5.15.2 Dyndns.org DDNS 176
5.15.3 No-ip.com DDNS 177
5.16 System Tools 178
5.16.1 Time Setting 179
5.16.2 Diagnostic 180
5.16.3 Firmware Upgrade 182
5.16.4 Factory Defaults 183
5.16.5 Backup & Restore 183
5.16.6 Reboot 184
5.16.7 Password 185
5.16.8 System Log 185
5.16.9 Working Mode 186
5.16.10 Statistics 187

Chapter 6. Router Configuration—AP Mode 189
6.1 Login 189
6.2 Status 189
6.3 Quick Setup 191
6.4 WPS 191
6.5 Network 198
6.6 Wireless 199
6.6.1 Wireless Settings 200
6.6.2 Wireless Security 207
6.6.3 Wireless MAC Filtering 215
6.6.4 Wireless Advanced 218
6.6.5 Wireless Statistics 219
6.7 DHCP 219
6.7.1 DHCP Settings 220
6.7.2 DHCP Clients List 221
6.7.3 Address Reservation 222
6.8 System Tools 223
6.8.1 Time Setting 223
6.8.2 Diagnostic 225
6.8.3 Firmware Upgrade 227
6.8.4 Factory Defaults 228
6.8.5 Backup & Restore 228
6.8.6 Reboot 229
6.8.7 Password 230
6.8.8 System Log 230
6.8.9 Working Mode 231
6.8.10 Statistics 232
Appendix A: FAQ 234
Appendix B: Configuring the PCs 240
Appendix C: Specifications 244
Appendix D: Glossary 245
Appendix E: Compatible 3G/4G USB Modem 247

Package Contents

The following items should be found in your package:

- Portable 3G/4G Wireless N Router TL-MR3020
- Power Adapter for Portable 3G/4G Wireless N Router TL-MR3020
- USB Cable
- Ethernet cable
- Quick Installation Guide
- Resource CD for Portable 3G/4G Wireless N Router TL-MR3020, including:
  - This Guide
  - Other Helpful Information

☞ **Note:**

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

Chapter 1. Introduction

1.1 Overview of the Router

TP-LINK understands the need for sharing the 3G/4G connection on the go and so we've realized the convenience with our latest Portable Wireless N 3G/4G Router TL-MR3020 ----- it gives you the freedom to quickly set up a stable and high speed wireless network, up to 150Mbps, on-the-go and share a 3G/4G connection. By connecting a 3G/4G USB Card to the router, a Wi-Fi hotspot is instantly established allowing users to share a Internet connection anywhere 3G/4G coverage is available. So whether you're on the train, camping, or at a construction site, you'll have a reliable wireless connection to accommodate your networking needs.

Flexible Network Connection

The Portable 3G/4G Wireless N Router TL-MR3020 provides 3G/4G Router, WISP Client Router and Access Point modes for network connection, providing the best flexibility. The Router supports 3G/4G and WAN (PPPoE, Dynamic IP, Static IP, PPTP, L2TP Cable) broadband connections for Internet access. You can visit the Internet no matter at home or outside on business.

Excellent Compatibility

The Portable 3G/4G Wireless N Router TL-MR3020 is compatible with iPad, iTouch, Android Phone, Kindle and majority portable WiFi devices. With a standard USB 2.0 port for 3G/4G Modem, the Router is compatible with LTE/HSPA+/HSUPA/HSDPA/UMTS/EVDO USB 3G/4G modems.

Incredibly High Speed

TP-LINK 3G/4G wireless N Router provides up to 150Mbps, faster than that of traditional 11g products, surpasses 11g performance enabling the use of high bandwidth-consuming applications such as HD Videos. It provides 150Mbps wireless connectivity for the network share on the go.

Low Power Consumption

With a Mini USB port, the Router can be powered by laptop or Power Adapter with Low Power consumption.

1.2 Conventions

The Router or TL-MR3020 mentioned in this guide stands for Portable 3G/4G Wireless N Router TL-MR3020 without any explanation.

1.3 Main Features

- Travel size design, small enough to take on the road
- One 10/100M Auto-Negotiation RJ45 Ethernet port, one USB 2.0 Port,one mini USB port
- Compatible with IEEE 802.11n/g/b, IEEE802.3/3u
- Compatible with LTE/HSPA+/HSUPA/HSDPA/UMTS/EVDO USB 3G/4G Modem
- Compatible with iPad, iTouch, Android Phone, Kindle and majority portable WiFi devices
- Wireless Lite N speed up to 150Mbps
- Supports WPS one button security setup
- Provides WEP, WPA/WPA2, WPA-PSK/WPA2-PSK authentication, TKIP/AES encryption security
- Powered by laptop or Power Adapter with Low Power Consumption
- Supports 3G/4G Router Mode, WISP Client Router Mode, and AP Mode
- Supports 3G/4G/PPPoE/Dynamic IP/Static IP/PPTP/L2TP Cable Internet access
- Supports VPN Pass-through, Virtual Server and DMZ Host
- Supports UPnP, Dynamic DNS, Static Routing
- Provides Automatic-connection and Scheduled Connection on certain time to the Internet
- Built-in NAT and DHCP server supporting automatic and dynamic IP address IP address distribution
- Connects Internet on demand and disconnects from the Internet when idle for PPPoE
- Provides 64/128/152-bit WEP encryption security and wireless LAN ACL (Access Control List)
- Supports Flow Statistics
- Supports firmware upgrade and Web management

1.4 Panel Layout

1.4.1 The Front Panel

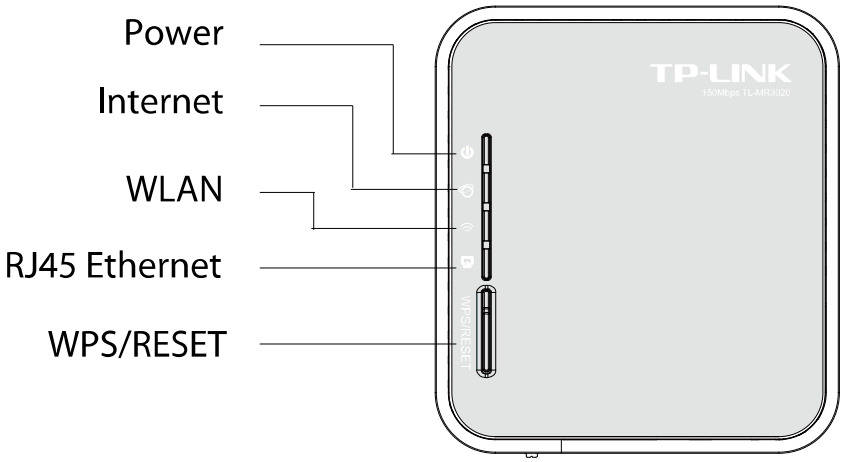


Figure 1-1 Front Panel sketch

The Router's LEDs are located on the front panel (View from top to bottom).

Name	Status	Indication
Power	On	Power is on.
	Off	Power is off.
Internet	On	The router is connected to the Internet, but there is no data being transferred.
	Flashing	The router is transferring data.
	Off	The router is not connected to the Internet.
WLAN	On	The Wireless function is enabled.
	Flashing	There is data being transferred through wireless.
	Off	The Wireless function is disabled.
RJ45 Ethernet	On	A device is linked to the corresponding port but there is no activity.
	Flashing	The Ethernet port is transferring data.
	Off	No device is linked to the corresponding port.

Table 1-1 The LEDs description

- **WPS/RESET:** To use WPS function, please push the button for less than 5 seconds, and then the WPS LED will flash; to reset the router, please push the button for at least 10 seconds.

1.4.2 The Rear Panel

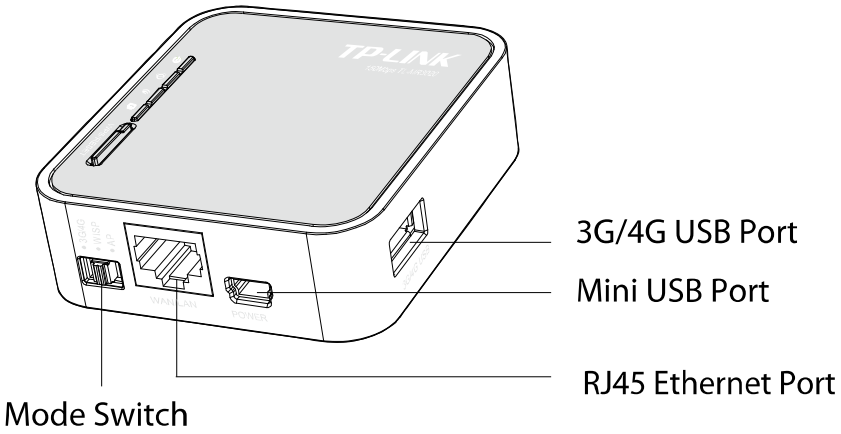


Figure 1-2 Rear Panel sketch

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

- **3G/4G USB Port:** This port is used to plug a 3G/4G modem/card.
- **Mini USB Port:** This port is used to connect the provided power adapter.
- **RJ45 Ethernet Port:** This port can be LAN or WAN port depending on the working mode.
- **Mode Switch:** This button is used to switch the working mode of the router.

Chapter 2. Connecting the Router

2.1 System Requirements

- 3G/4G Mobile Broadband Internet Access Service (With a LTE /HSPA+ /HSUPA /HSDPA /UMTS /EVDO USB dongle)
- PCs with a working Ethernet Adapter and an Ethernet cable with RJ45 connectors
- TCP/IP protocol on each PC
- Web browser, such as Microsoft Internet Explorer 5.0 , Netscape Navigator 6.0 or above

2.2 Installation Environment Requirements

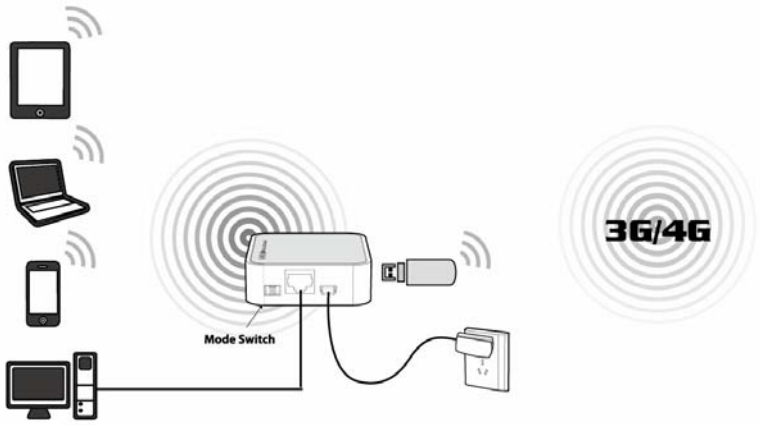
- Place the Router in a well ventilated place far from any heater or heating vent
- Avoid direct irradiation of any strong light (such as sunlight)
- Keep at least 2 inches (5 cm) of clear space around the Router
- Operating Temperature: 0℃~40℃ (32℉~104℉)
- Operating Humidity: 10%~90%RH, Non-condensing

2.3 Connecting the Router

The Router supports three modes, 3G/4G router mode, WISP mode and AP mode. You can deploy the mode appropriate to your actual network environment. To connect the Router, please take the following steps for different modes.

a. 3G/4G Router Mode

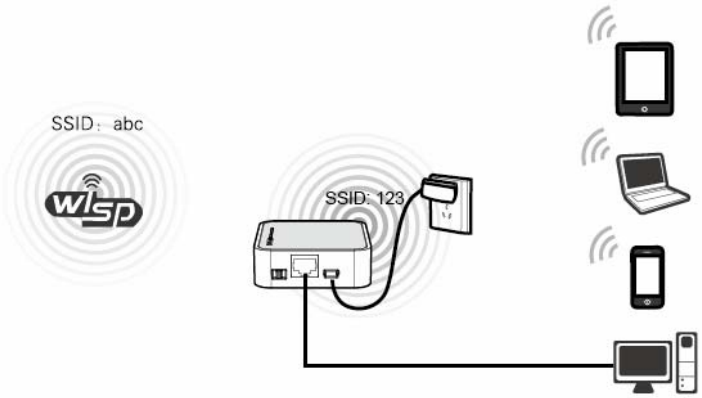
In 3G/4G router mode, with a 3G/4G modem/card, this Router can join a 3G/4G network as well as act as a wireless central hub to broadcast its SSID. Thus, the other wireless devices can connect to the Router so as to join the same 3G/4G network.



1. Switch the mode of the Router on 3G/4G Router mode.
2. Connect the notebook/PC to the Ethernet port of TL-MR3020 Router with an Ethernet cable.
3. Connect the 3G/4G modem/card to the 3G/4G USB port of the Router.
4. Connect one end of the provided USB cable to mini USB port of the Router and the other end to the power adapter, and then plug the power adapter to a standard electrical wall socket.

b. WISP Mode

In WISP mode, the Router will act as a wireless card to connect with WISP as well as a wireless central hub to broadcast its SSID for your wireless LAN clients, and the other wireless devices can connect to the Router for Internet connection.



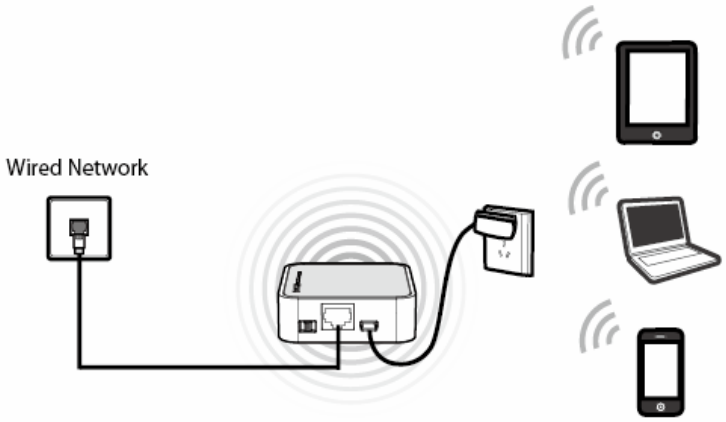
1. Switch the mode of the Router on WISP mode.
2. Connect the notebook/PC to the Ethernet port of TL-MR3020 Router with an Ethernet cable.
3. Connect one end of the provided USB cable to mini USB port of the Router and the other end to the power adapter, and then plug the power adapter to a standard electrical wall socket.

c. AP Mode

In AP mode, the Router will act as a wireless access point supporting four modes, Access Point mode, Repeater mode, Bridge with AP mode and Client mode. Please connect the Router according to your desired mode.

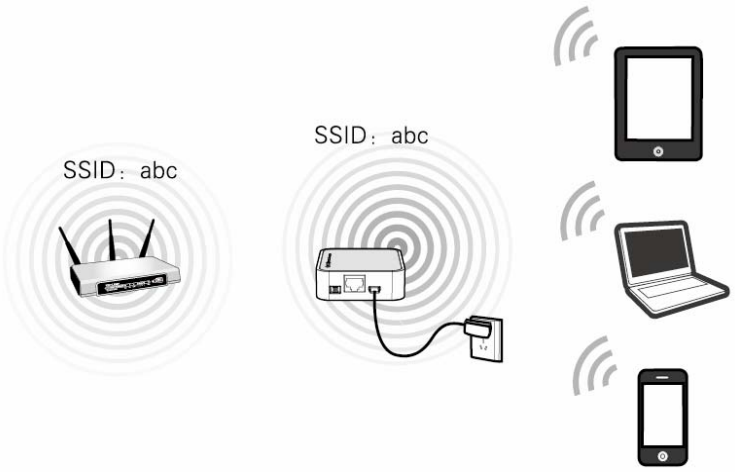
a) Access Point Mode

In this mode, the Router will act as a wireless central hub for your wireless LAN clients, giving a wireless extension for your current wired network.



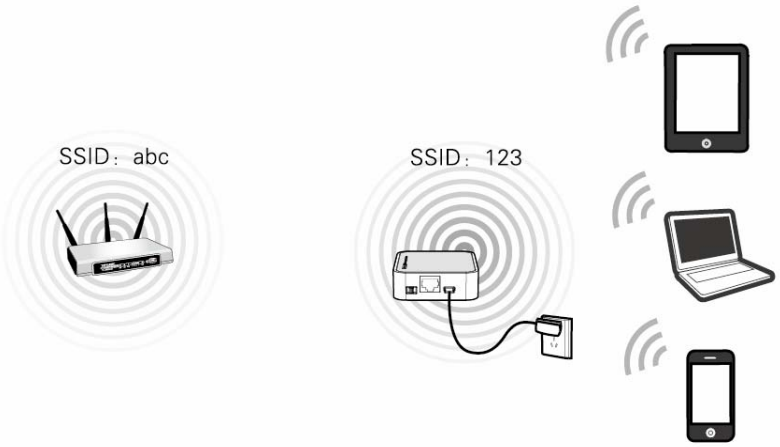
b) Repeater Mode

In this mode, the Router can extend the coverage of another wireless Access Point or Router.



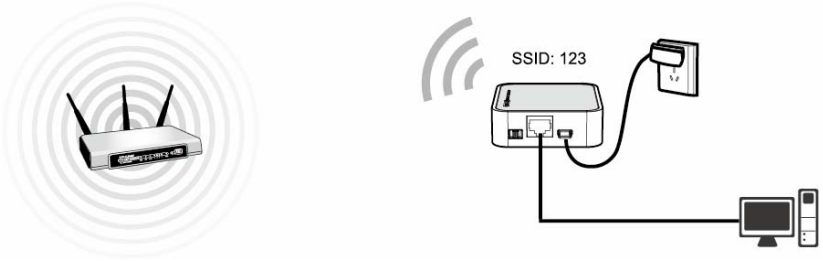
c) Bridge with AP Mode

In this mode, the Router can wirelessly connect two remote LANs together.



d) Client Mode

In this mode, the Router will act as a wireless card to connect with wireless network.



Chapter 3. Quick Installation Guide

This chapter will show you how to configure the basic functions of your Portable 3G/4G Wireless N Router using **Quick Setup Wizard** within minutes.

3.1 3G/4G Router Mode

The default IP address of the Portable 3G/4G Wireless N Router is 192.168.0.254 and the default Subnet Mask is 255.255.255.0. These values can be changed as you desire. In this guide, we all use the default values for description.

3.1.1 PC configuration

Here we take Wireless Network Connection as an example. (You can also go to Local Area Connection to configure the PC for wired network connection, and then configure the router. If you need instructions as to how to do this, please refer to Appendix B: "Configuring the PC.")

1. For Windows XP, please go to **Start → Settings → Control Panel → Network and Internet Connections → Network Connections**; for Windows 7, please go to **Start → Settings → Control Panel → View network status and tasks → Manage network connection**. Right click **Wireless Network Connection**, and select **Properties**.
2. For Windows XP, double click **Internet Protocol (TCP/IP)** in the item list; for Windows 7, double click **Internet Protocol Version 4 (TCP/IPv4)**.
3. Select "**Obtain an IP address automatically**" and "**Obtain DNS server address automatically**". Click **OK** to finish the settings.

3.1.2 Connect to Network

1. Click the icon at the bottom of your desktop.
2. Click "**Refresh network list**", and then select the network. Click **Connect**.

☞ **Note:**

The default SSID of the network is TP-LINK_POCKET_3020_xxxxxx. (The xxxxxx is the last six characters of the router's MAC address.)

3. When **Connected** appears, you've successfully connected to the wireless network.

3.1.3 Router Configuration

1. To access the configuration utility, open a web-browser and type the default address http://192.168.0.254 in the address field of the browser.

Figure 3-1 Login the Router

2. After a moment, a login window will appear, similar to the Figure 3-2. Enter **admin** for the User Name and Password, both in lower case letters. Then click the **OK** button or press the **Enter** key.

Figure 3-2 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.

3. Go to **Status** and check the 3G/4G status. When the 3G/4G USB Modem is identified, go to the next step.

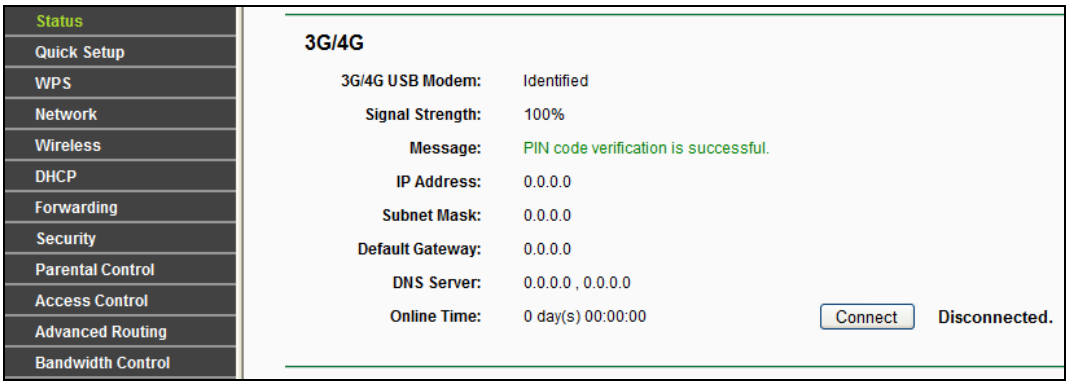


Figure 3-3 Status – 3G/4G

4. Go to **Quick Setup** and click **Next**.

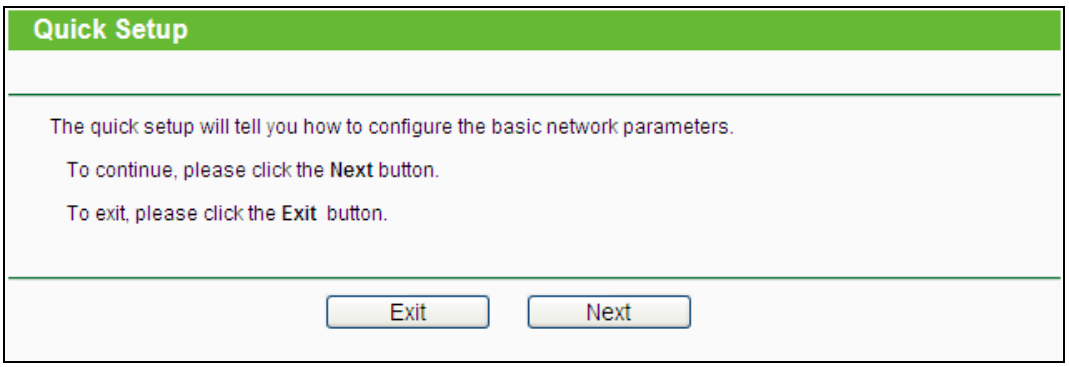


Figure 3-4 Quick Setup

5. Choose the **Internet Access** type, and then click **Next**. Here we take 3G/4G Only for example.

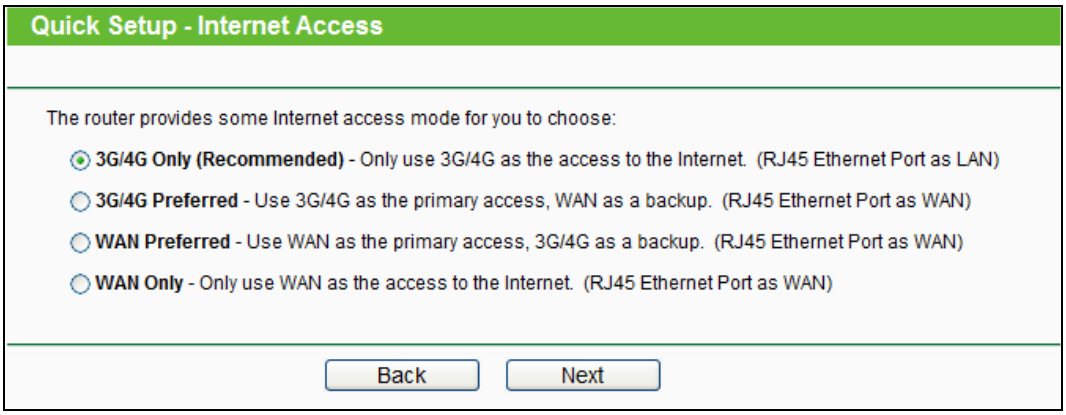


Figure 3-5 Quick Setup – Internet Access

- **3G/4G Only (Recommended) -** Only use 3G/4G as the access to the Internet. The Ethernet port is used as LAN port.
- **3G/4G Preferred -** Use 3G/4G as the primary access, WAN as a backup. The Ethernet port is used as WAN port.
- **WAN Preferred -** Use WAN as the primary access, 3G/4G as a backup. The Ethernet port is used as WAN port.
- **WAN Only -** Only use WAN as the access to the Internet. The Ethernet port is used as WAN port.

6. Select your location and Mobile ISP. You can tick "**Set the Dial Number, APN, Username and Password manually**" to manually set them according to the information your 3G/4G ISP provided. Then click **Next**.

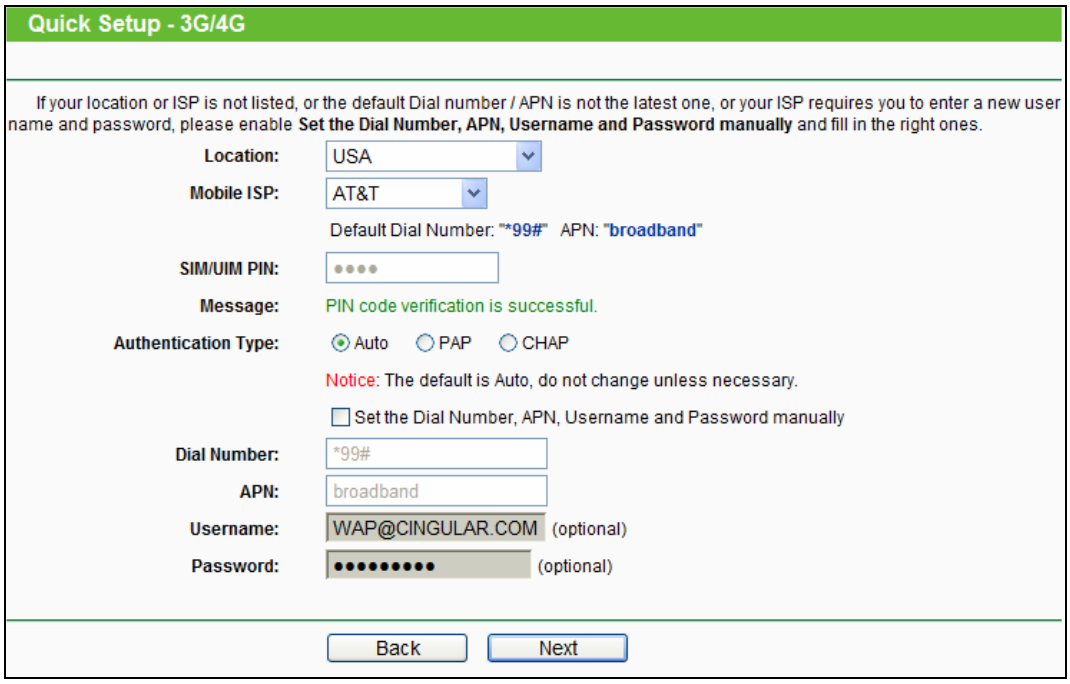


Figure 3-6 Quick Setup – 3G/4G

7. Set your wireless parameters. It's recommended that you edit the following two items, and then click **Next**.

   1) Create a unique and easy-to-remember **Wireless Network Name**.

   2) Select **WPA-Personal/WPA2-Personal** under **Wireless Security** and enter a password in the field.

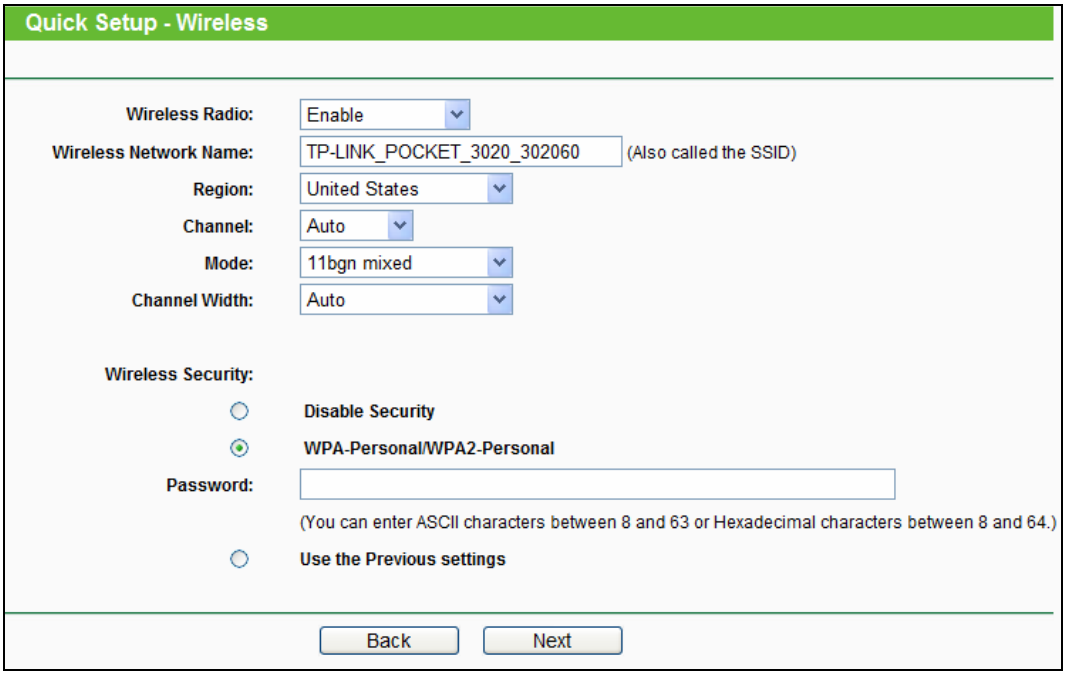


Figure 3-7 Quick Setup – Wireless

8. Click **Reboot** to make the settings take effect.

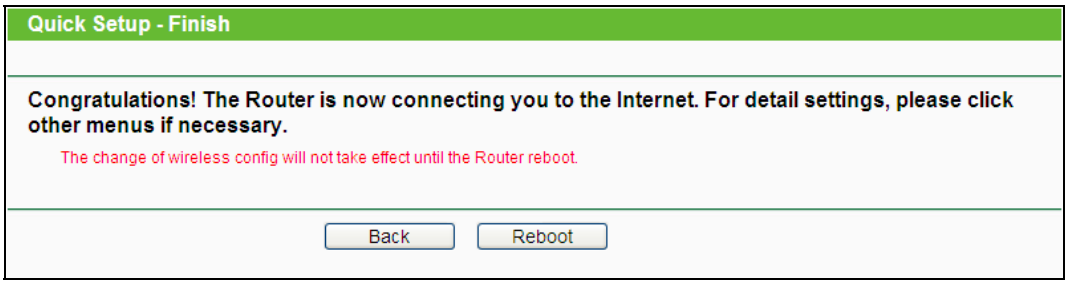


Figure 3-8 Quick Setup – Finish

Note:

After the rebooting, please reconnect to the network according to 3.1.2 Connect to Network. If Wireless Security is enabled, you need to enter the password you've just set to successfully finish the connecting.

3.2 WISP Mode

The default IP address of the Portable 3G/4G Wireless N Router is 192.168.0.254 and the default Subnet Mask is 255.255.255.0. These values can be changed as you desire. In this guide, we all use the default values for description.

3.2.1 PC configuration

Here we take Wireless Network Connection as an example. (You can also go to Local Area Connection to configure the PC for wired network connection, and then configure the router. If you need instructions as to how to do this, please refer to Appendix B: "Configuring the PC.")

1. For Windows XP, please go to **Start → Settings → Control Panel → Network and Internet Connections → Network Connections**; for Windows 7, please go to **Start → Settings → Control Panel → View network status and tasks → Manage network connection**. Right click **Wireless Network Connection**, and select **Properties**.
2. For Windows XP, double click **Internet Protocol (TCP/IP)** in the item list; for Windows 7, double click **Internet Protocol Version 4 (TCP/IPv4)**.
3. Select "**Obtain an IP address automatically**" and "**Obtain DNS server address automatically**". Click **OK** to finish the settings.

3.2.2 Connect to Network

1. Click the icon at the bottom of your desktop.
2. Click "**Refresh network list**", and then select the network. Click **Connect**.

Note:

The default SSID of the network is TP-LINK_POCKET_3020_xxxxxx. (The xxxxxx is the last six characters of the router's MAC address.)

3. When **Connected** appears, you've successfully connected to the wireless network.

3.2.3 Router Configuration

1. To access the configuration utility, open a web-browser and type the default address http://192.168.0.254 in the address field of the browser.

Figure 3-9 Login the Router

2. After a moment, a login window will appear, similar to the Figure 3-10. Enter **admin** for the User Name and Password, both in lower case letters. Then click the **OK** button or press the **Enter** key.

Figure 3-10 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.

3. Go to **Quick Setup** and click **Next**.

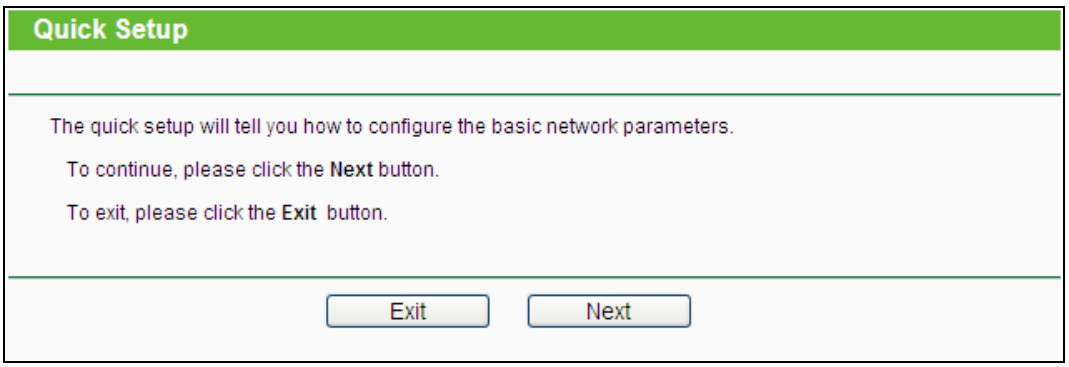


Figure 3-11 Quick Setup

4. Choose your **WAN Connection** type and click **Next** to continue.

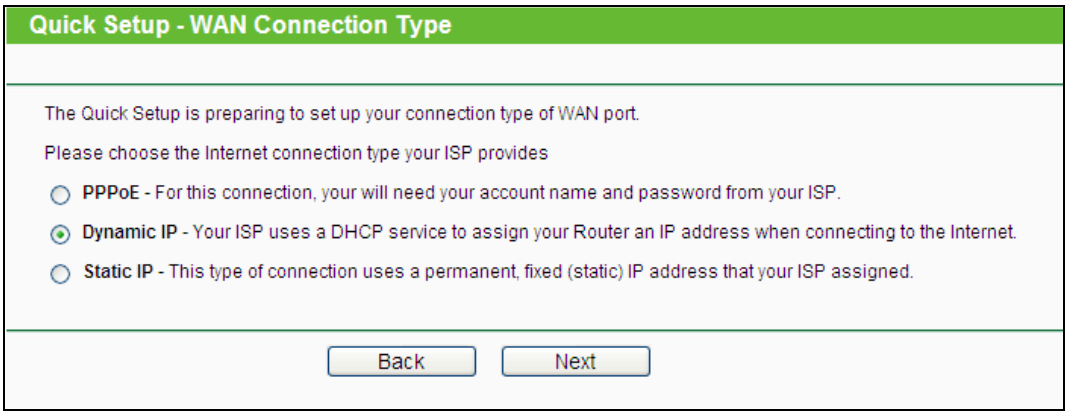


Figure 3-12 Quick Setup – WAN Connection Type

➢ If the connection type is **PPPoE**, the next screen will appear as shown in Figure 3-13.

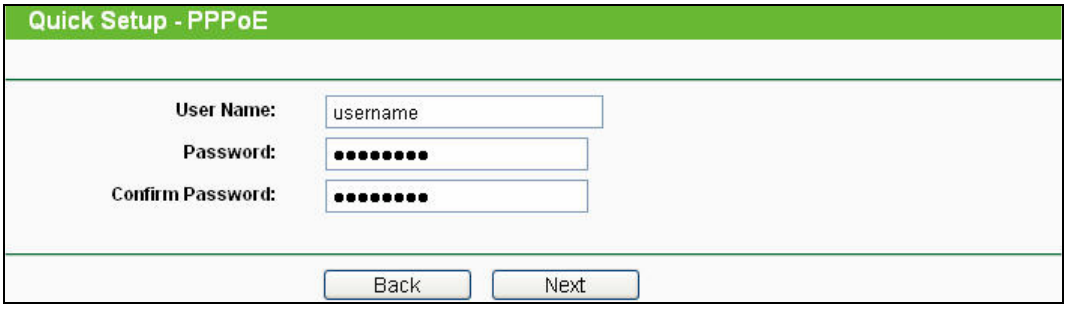


Figure 3-13 Quick Setup – PPPoE

- **User Name and Password -** Enter the **User Name** and **Password** provided by your ISP. These fields are case sensitive. If you have difficulty with this process, please contact your ISP.
- **Confirm Password -** Re-enter the password provided by your ISP to ensure the Password you entered is correct. If the Password is different from the Confirm Password, the screen will appear as shown below. Click **OK**, and re-enter the Password and Confirm Password.

➢ If the connection type is Dynamic IP, the next screen will appear as shown in Figure 3-14.

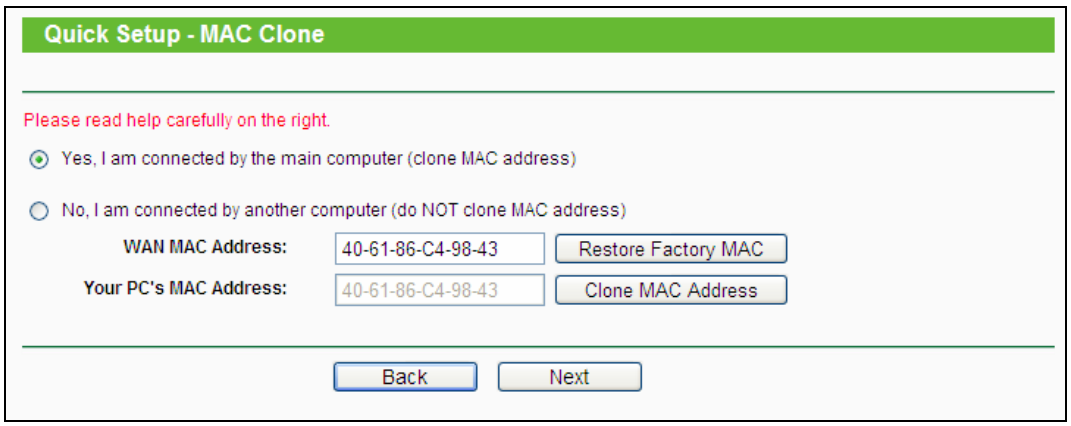


Figure 3-14 Quick Setup – MAC Clone

- If you are visiting the Router from the main computer, please select **Yes**, and then click **Clone MAC Address**.
- If you are visiting the Router from another computer, rather than the main computer, please select **No**, and then enter the main computer's MAC in the field **WAN MAC Address**.

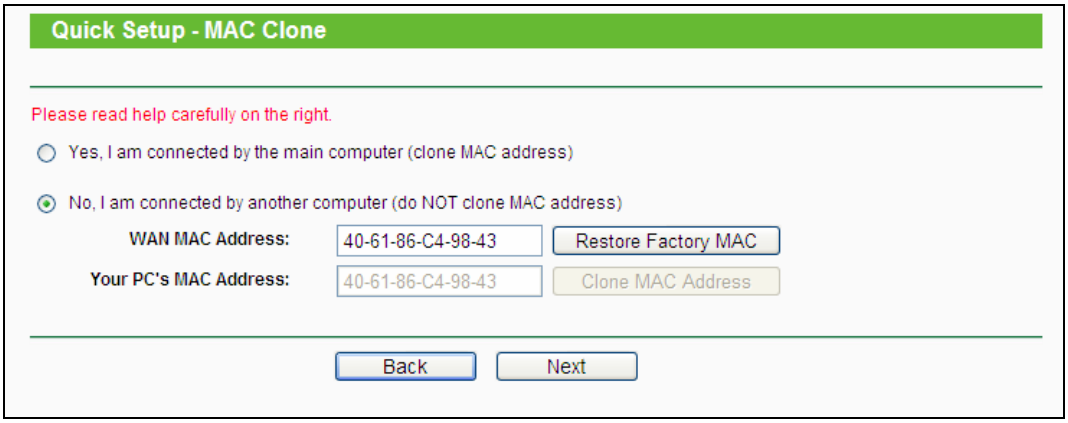


Figure 3-15 Quick Setup – MAC Clone

➢ If the connection type detected is Static IP, the next screen will appear as shown in Figure 3-16.

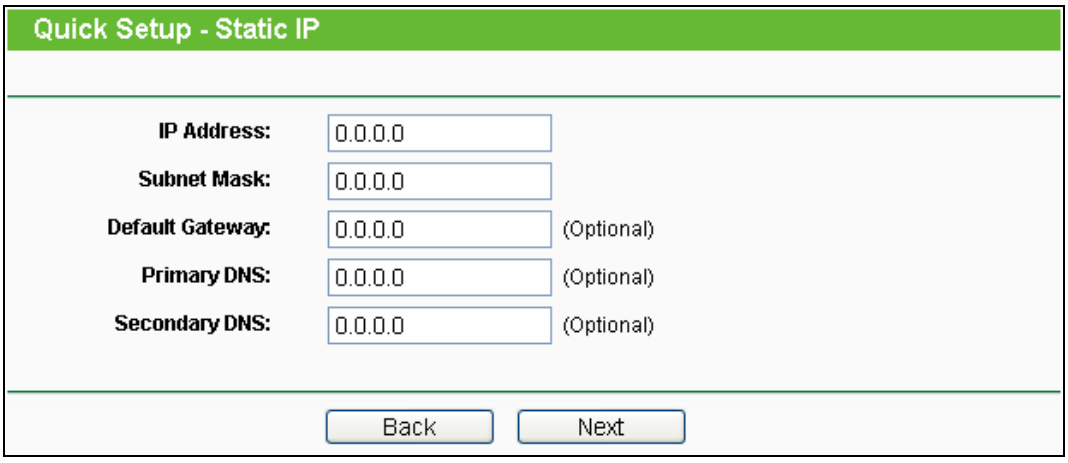


Figure 3-16 Quick Setup - Static IP

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

5. Click **Next** to continue, the Wireless settings page will appear as shown in Figure 3-17. Click **Survey** button to find the available wireless networks. Select the SSID of your target network and click **Connect**, and the SSID and BSSID will be filled automatically. If the network security is on, please select the Key type and enter the Password.

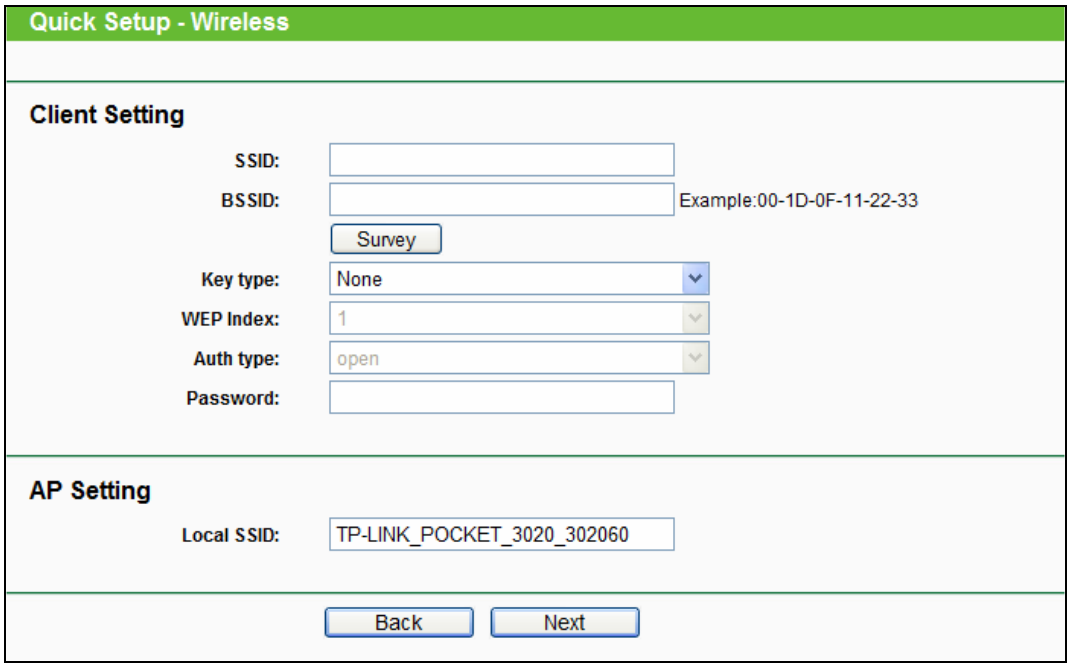


Figure 3-17 Quick Setup – Wireless

6. Click **Next** and you will see the page as shown in Figure 3-18. Click the **Reboot** button to make your wireless configuration take effect and finish the **Quick Setup**. (You're recommended to go to **Wireless** > **Wireless Security** to set up the wireless security.)

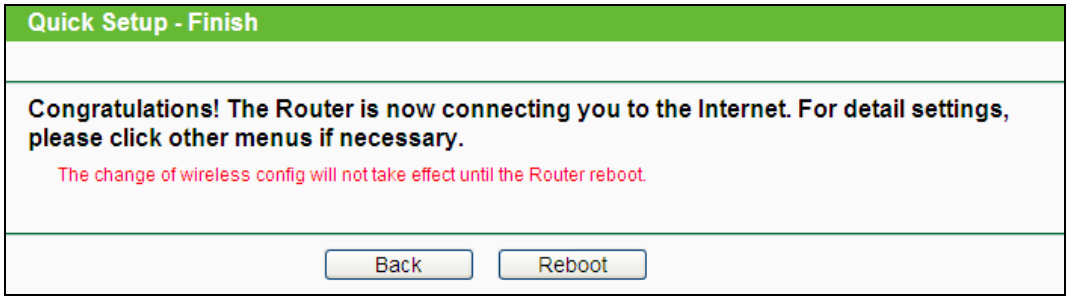


Figure 3-18 Quick Setup – Finish

☞ **Note:**

After the rebooting, please reconnect to the network according to 3.2.2 Connect to Network. If Wireless Security is enabled, you need to enter the password you've just set to successfully finish the connecting.

3.3 AP Mode

3.3.1 PC configuration

Here we take Wireless Network Connection as an example. (You can also go to Local Area Connection to configure the PC for wired network connection, and then configure the router. If you need instructions as to how to do this, please refer to Appendix B: "Configuring the PC.")

1. For Windows XP, please go to **Start → Settings → Control Panel → Network and Internet Connections → Network Connections**; for Windows 7, please go to **Start → Settings → Control Panel → View network status and tasks → Manage network connection**. Right click **Wireless Network Connection**, and select **Properties**.
2. For Windows XP, double click **Internet Protocol (TCP/IP)** in the item list; for Windows 7, double click **Internet Protocol Version 4 (TCP/IPv4)**.
3. Select "**Use the following IP address**", enter the 192.168.0.x as the IP address (x can be any number from 1 to 253), 255.255.255.0 as the Subnet mask; select "**Use the following DNS server addresses**", enter the DNS server address provided by your ISP or network administrator.
4. Click **OK** to finish the settings.

3.3.2 Connect to Network

1. Click the icon at the bottom of your desktop.
2. Click "**Refresh network list**", and then select the network. Click **Connect**.

☞ **Note:**

The default SSID of the network is TP-LINK_POCKET_3020_xxxxxx. (The xxxxxx is the last six characters of the router's MAC address.)

3. When **Connected** appears, you've successfully connected to the wireless network.

3.3.3 Router Configuration

1. To access the configuration utility, open a web-browser and type the default address http://192.168.0.254 in the address field of the browser.

Figure 3-19 Login the Router

2. After a moment, a login window will appear, similar to the Figure 3-20. Enter **admin** for the User Name and Password, both in lower case letters. Then click the **OK** button or press the **Enter** key.

Figure 3-20 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.

3. Go to **Quick Setup** and click **Next**.

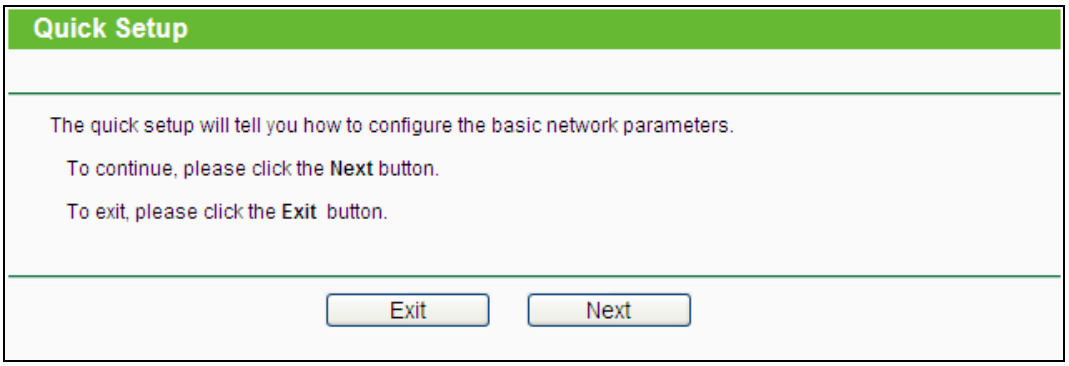


Figure 3-21 Quick Setup

4. Choose the **Wireless Operation Mode Type** and click **Next**.

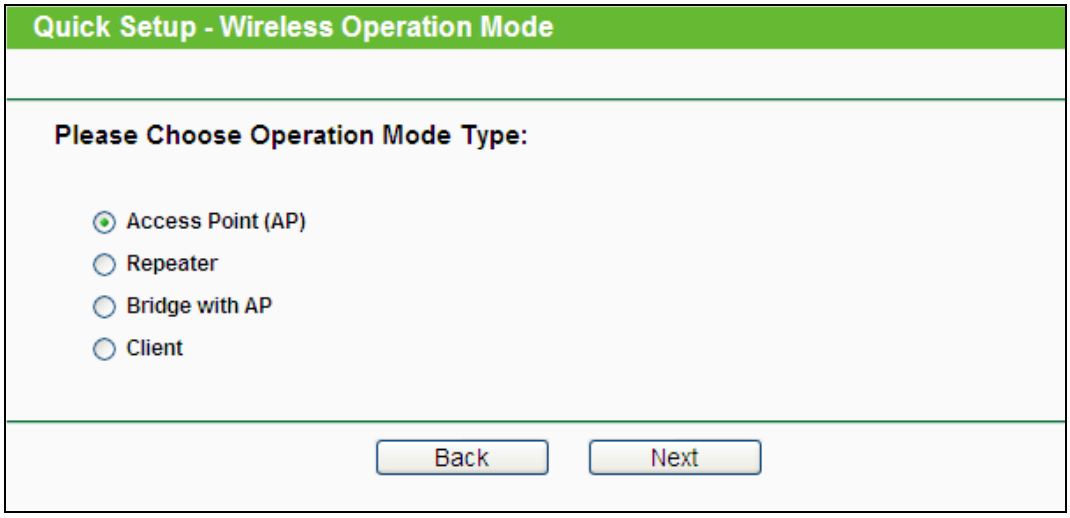


Figure 3-22 Quick Setup – Wireless Operation Mode

➢ If you choose **Access Point (AP)**, the next screen will appear as shown in Figure 3-23. This operation mode allows wireless stations to access.

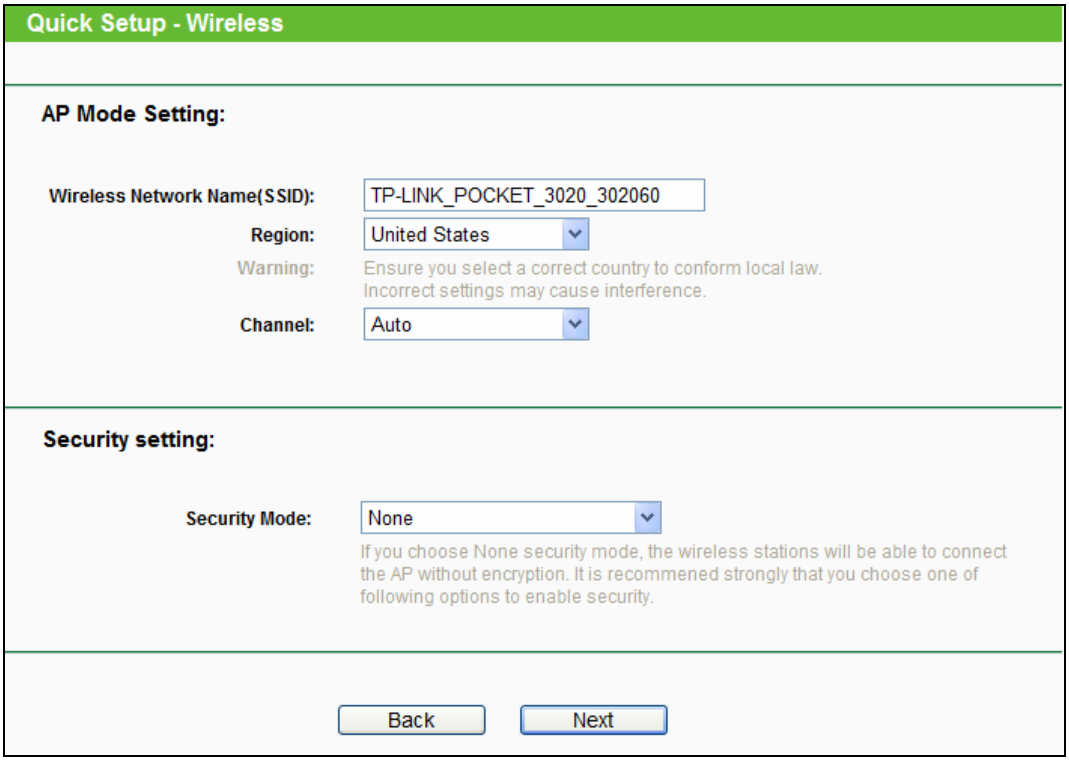


Figure 3-23 Quick Setup – AP

- **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_POCKET_xxxxxx** (xxxxxx indicates the last unique six characters of each Router'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 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.
- **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 AP will select the best channel automatically.

➢ If you choose **Repeater**, the next screen will appear as shown in Figure 3-24. In 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 Address"**.

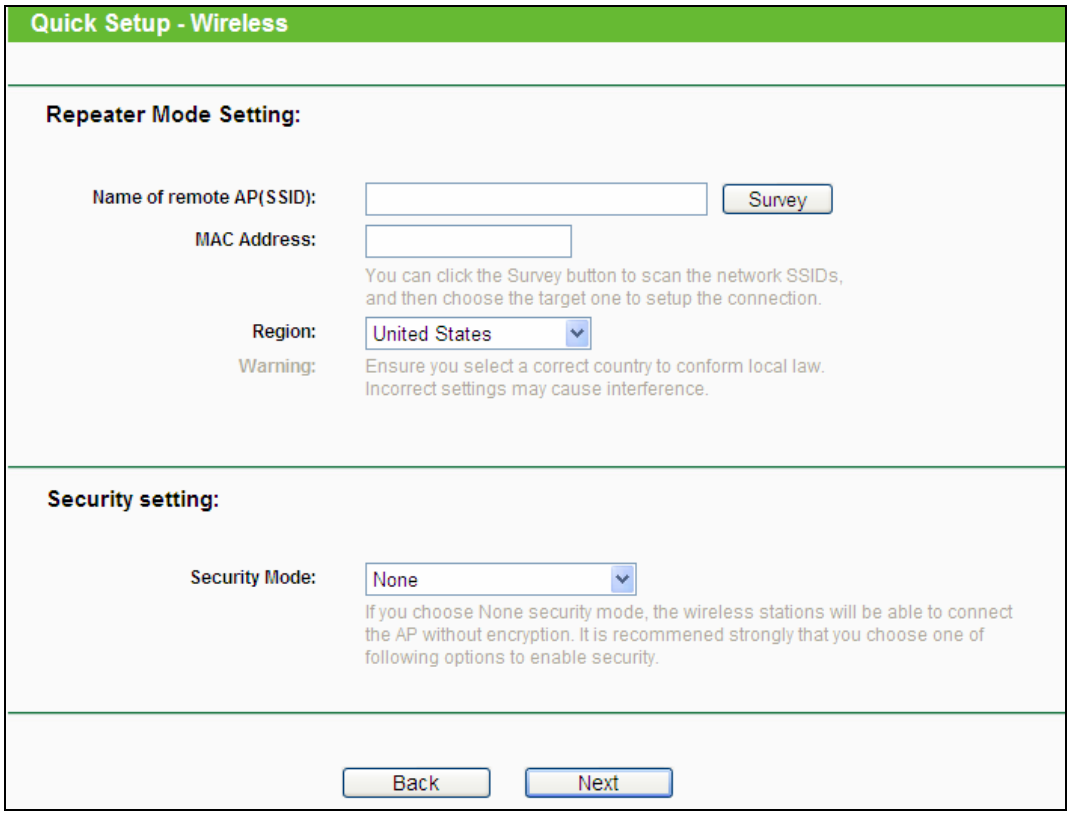


Figure 3-24 Quick Setup – Repeater

- **Name of remote AP (SSID)** - Enter the name of a remote AP (also called the SSID) that you want to access. Click the **Survey** button behind it, you can choose one of searching results to fill in this field.
- **MAC Address** - Enter the MAC address of AP that you want to access. When you use the survey function to fulfill the **Name of remote AP (SSID)**, this field will be filled in automatically.

- **Region** - This field determines which operating frequency will be used. To achieve more information, you can read the same glossary in Access Point part.

➢ If you choose **Bridge with AP**, the next screen will appear as shown in Figure 3-25. This operation mode bridges the AP and up to 4 APs also in bridge mode to connect two or more wired LANs.

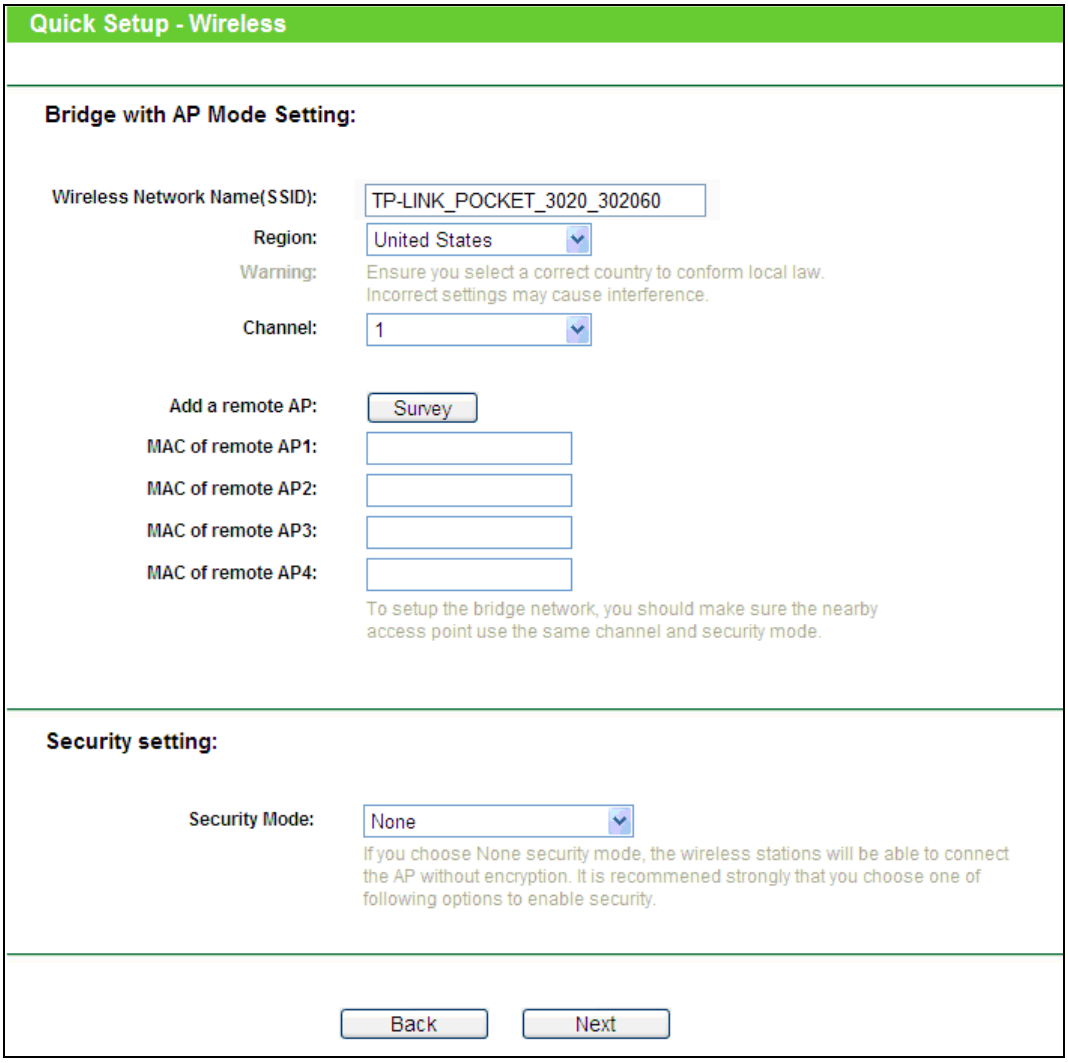


Figure 3-25 Quick Setup – Bridge with AP

- **Wireless Network Name (SSID)** - Enter a string of up to 32 characters. To achieve more information, you can read the same glossary in Access Point part.
- **Region** - This field determines which operating frequency will be used. To achieve more information, you can read the same glossary in Access Point part.
- **Channel** - This field determines which operating frequency will be used. To achieve more information, you can read the same glossary in Access Point part.
- **Add a remote AP -** Click the Survey button to fill in the **MAC of remote AP (1-4)** field.
- **MAC of remote AP (1-4)** - Enter the MAC address of AP that you want to access.

➢ If you choose **Client**, the next screen will appear as shown in Figure 3-26. This operation mode allows your device to work as a wireless station and enable wired host(s) to access AP.

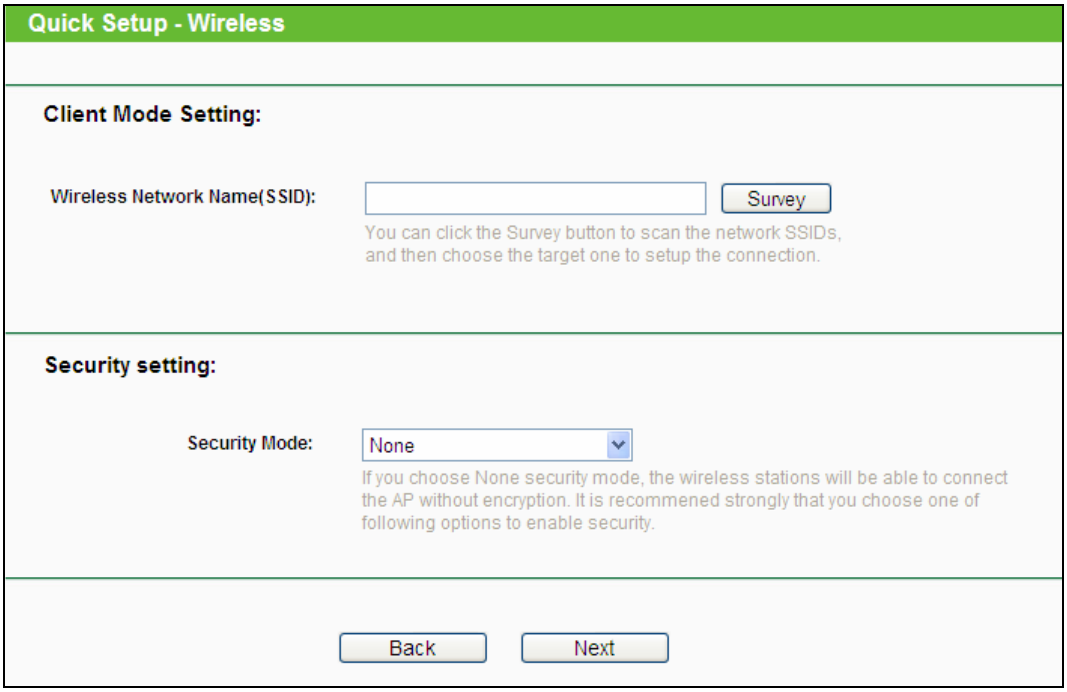


Figure 3-26 Quick Setup – Client

- **None** - The wireless security function can be enabled or disabled. If you select "None", the wireless stations will be able to connect the Router without encryption. It is recommended strongly that you choose one of following options to enable security.
- **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.

- **WPA/WPA2-Personal**

  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.

- **Not Change** - If you chose this option, wireless security configuration will not change!

5. Click **Next** and you will see the page as shown in Figure 3-27. Click **Reboot** to reboot the router and make the settings take effect.

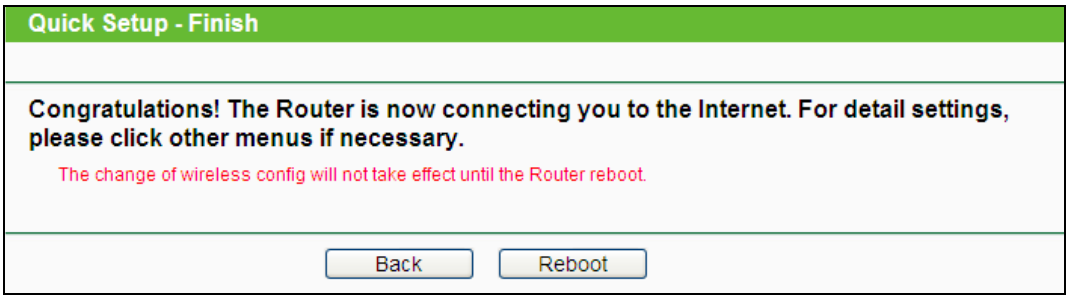


Figure 3-27 Quick Setup – Finish

☞ **Note:**

After the rebooting, please change the PC's TCP/IP settings to "**Obtain an IP address automatically**" and "**Obtain DNS server address automatically**" according to 3.3.1 PC

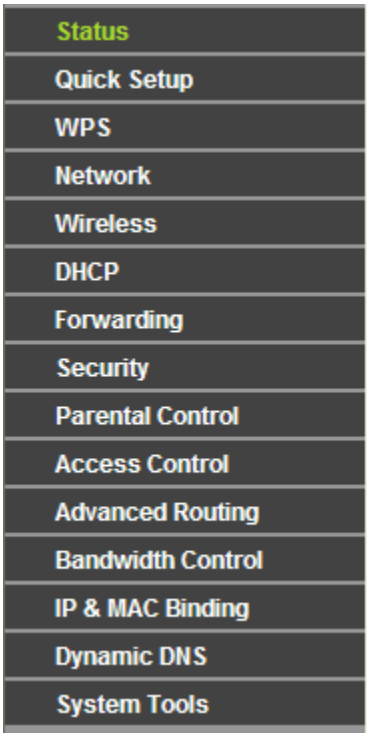
configuration, and then reconnect to the network according to 3.3.2 Connect to Network. If Wireless Security is enabled, you need to enter the password you've just set to successfully finish the connecting.

Chapter 4. Router Configuration-3G/4G Router Mode

This chapter will show each Web page's key functions and the configuration way on 3G/4G Router Mode.

4.1 Login

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



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

4.2 Status

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

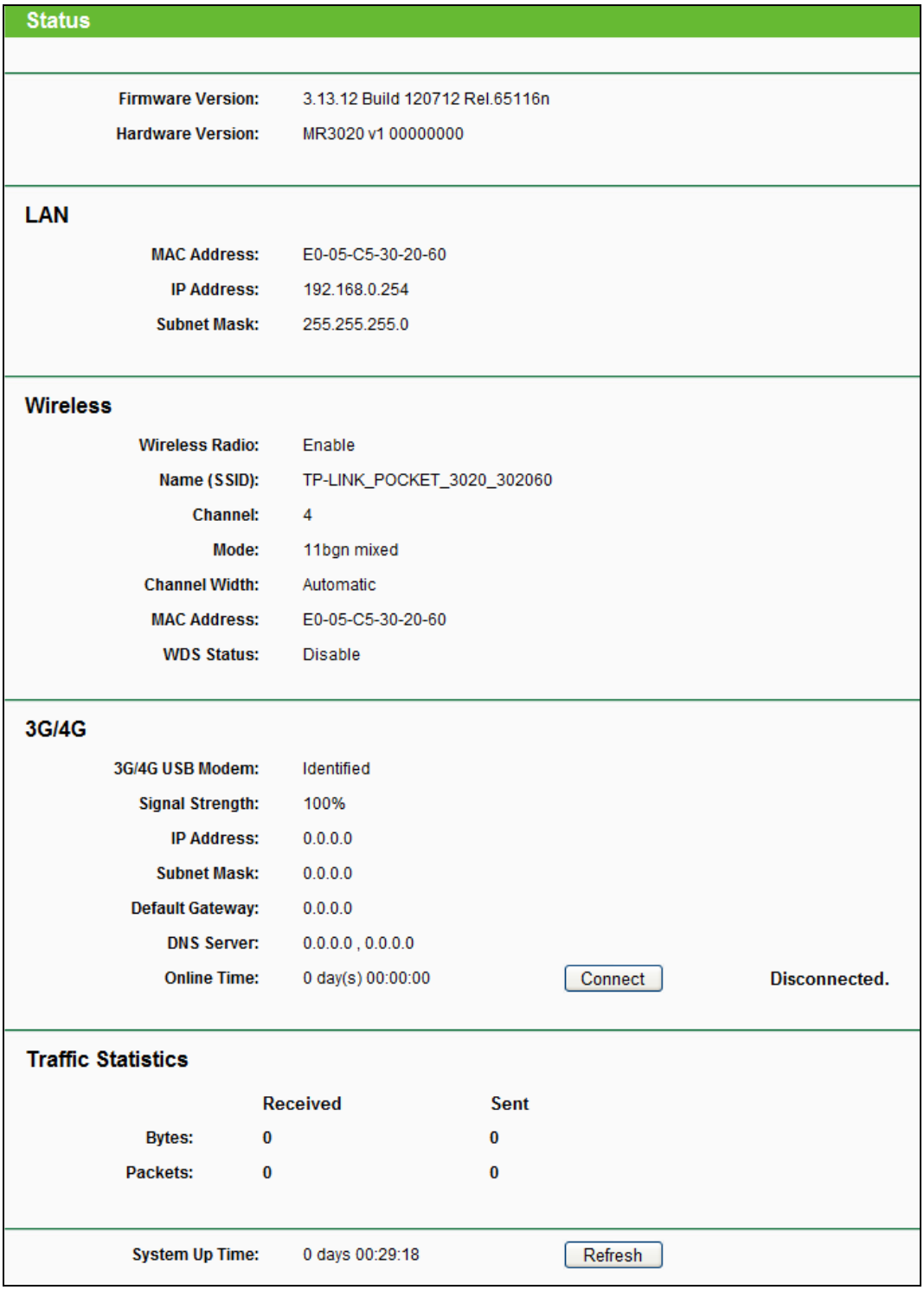


Figure 4-1 Router Status

4.3 Quick Setup

Please refer to Chapter 3: "Quick Installation Guide."

4.4 WPS

This section will guide you add a new wireless device to an existing network quickly by **WPS (Wi-Fi Protected Setup)** function.

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

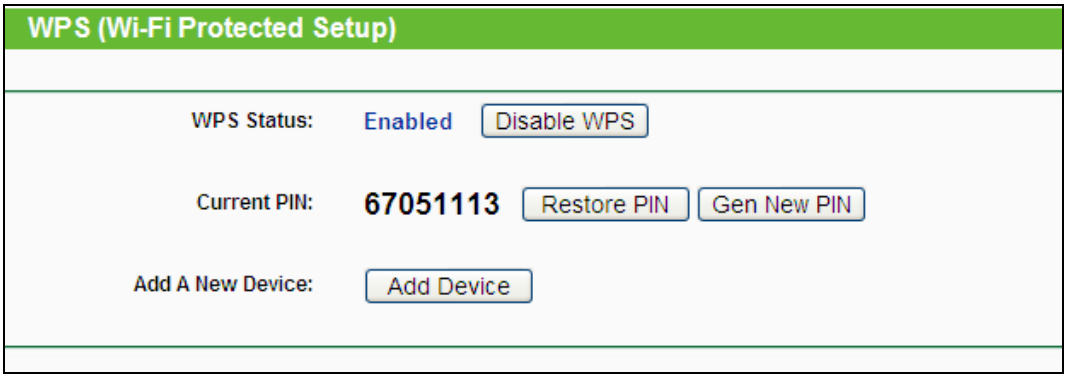


Figure 4-2 WPS

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

b). To add a new device:

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

☞ **Note:**

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

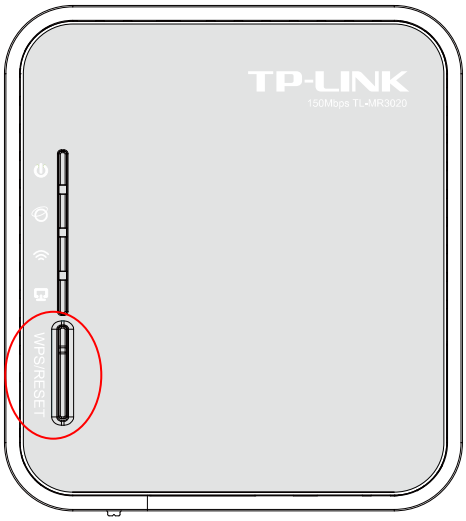
For the configuration of the new device, here takes the Wireless Adapter of our company for example.

I. By PBC

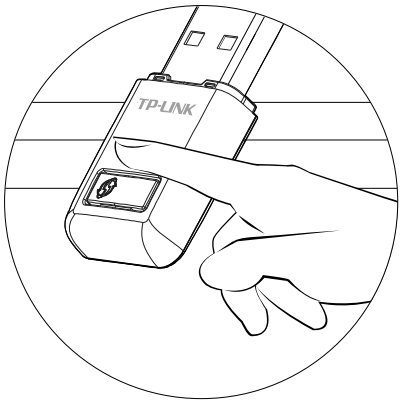
If the wireless adapter supports Wi-Fi Protected Setup and the Push Button Configuration (PBC) method, you can add it to the network by PBC with the following two methods.

Method One:

Step 1: Press the WPS/RESET button on the front panel of the Router for less than 5 seconds.



Step 2: Press and hold the WPS button of the adapter directly for 2 or 3 seconds.

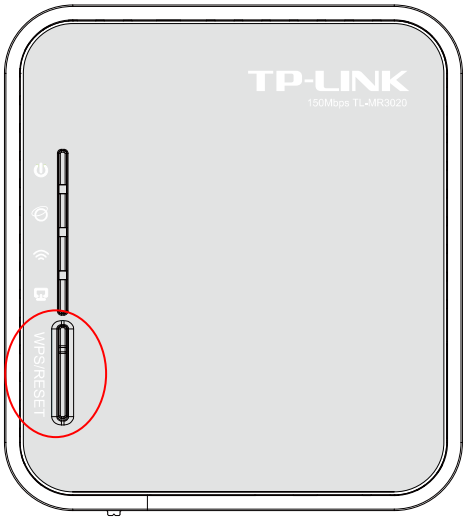


Step 3: Wait for a while until the next screen appears. Click **Finish** to complete the WPS configuration.

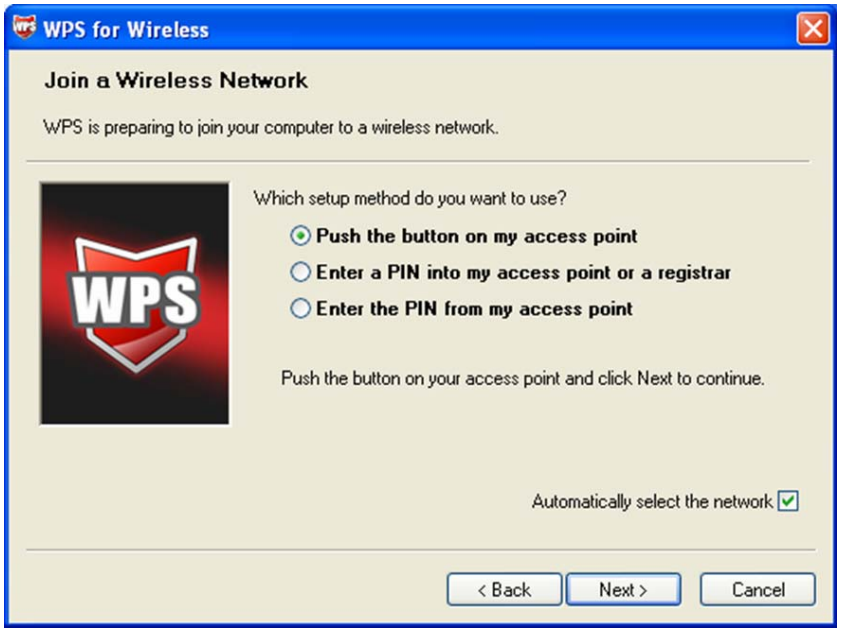
The WPS Configuration Screen of Wireless Adapter

Method Two:

Step 1: Press the WPS/RESET button on the front panel of the Router for less than 5 seconds.

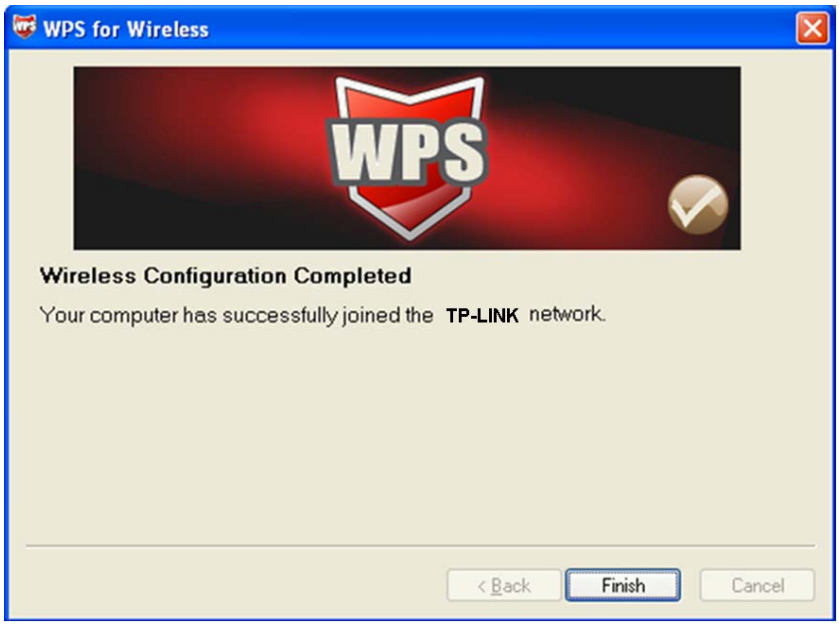


Step 2: For the configuration of the wireless adapter, please choose **Push the button on my access point** in the configuration utility of the WPS as below, and click **Next**.



The WPS Configuration Screen of Wireless Adapter

Step 3: Wait for a while until the next screen appears. Click **Finish** to complete the WPS configuration.



The WPS Configuration Screen of Wireless Adapter

Method Three:

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

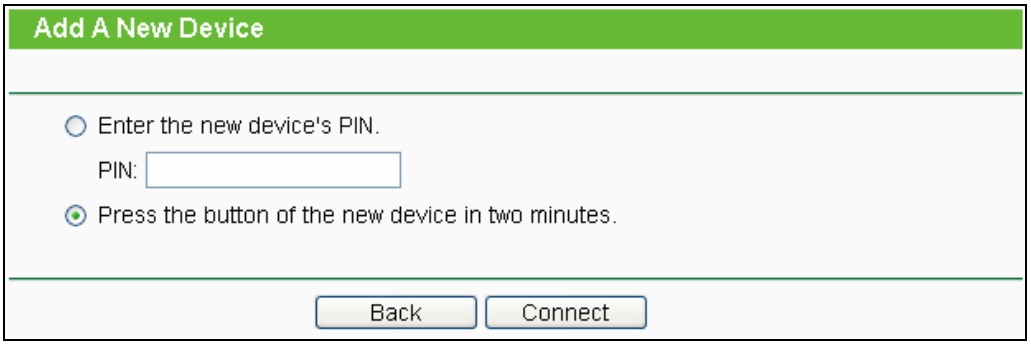
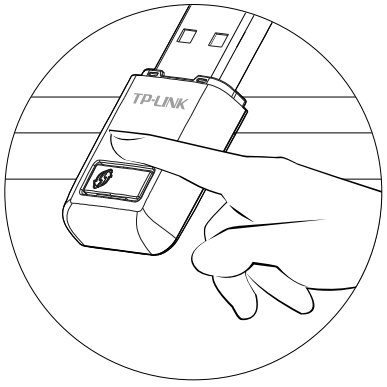


Figure 4-3 Add A New Device

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

Step 3. Press and hold the WPS button of the adapter directly for 2 or 3 seconds.



Step 4. Wait for a while until the next screen appears. Click **Finish** to complete the WPS configuration.

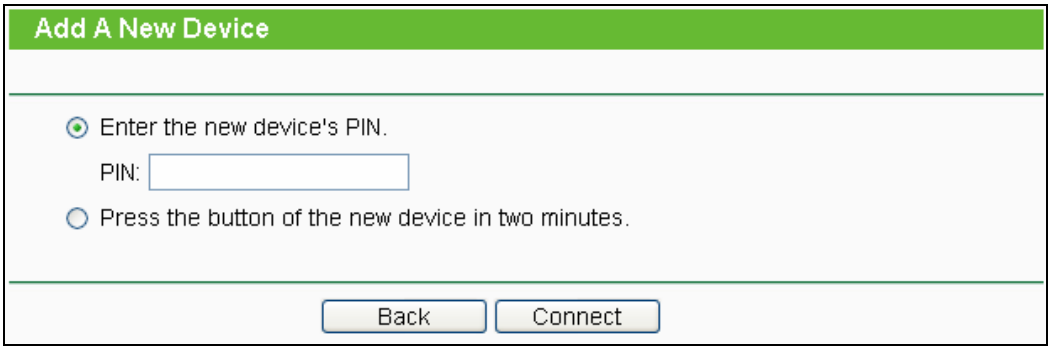
The WPS Configuration Screen of Wireless Adapter

II. By PIN

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

Method One: Enter the PIN into my Router

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

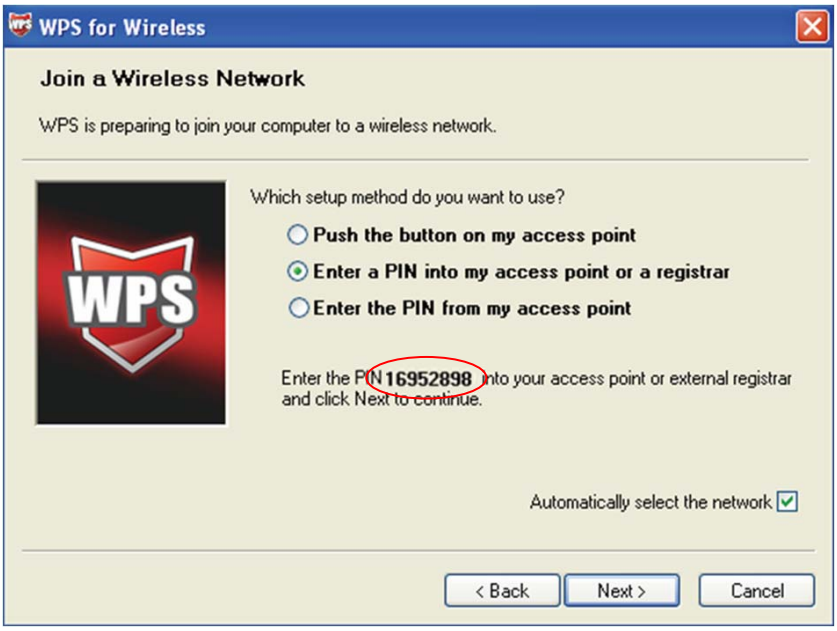


Step 2: Choose **Enter the new device's PIN** and enter the PIN code of the wireless adapter in the field behind **PIN** in the above figure. Then click **Connect.**

☞ **Note:**

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

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



The WPS Configuration Screen of Wireless Adapter

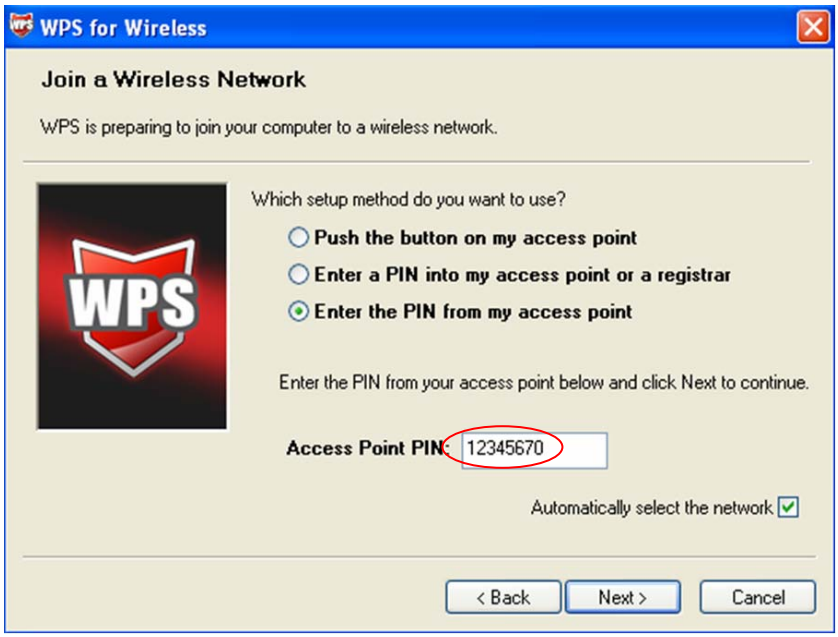
☞ **Note:**

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

Method Two: Enter the PIN from my Router

Step 1: Get the Current PIN code of the Router in Figure 4-2 (each Router has its unique PIN code. Here takes the PIN code 12345670 of this Router for example).

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

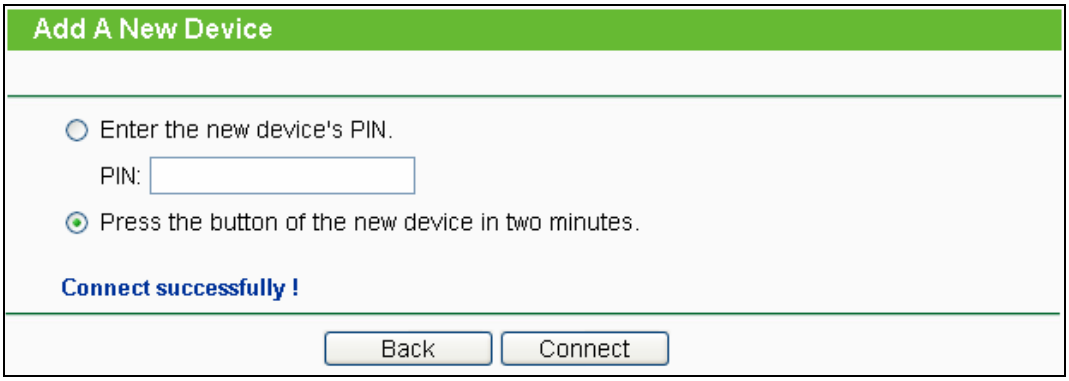


The WPS Configuration Screen of Wireless Adapter

Note:

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

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



Note:

1) The status LED on the Router will light green all the time if the device has been successfully added to the network.
2) The WPS function cannot be configured if the Wireless Function of the Router is disabled. Please make sure the Wireless Function is enabled before configuring the WPS.

4.5 Network

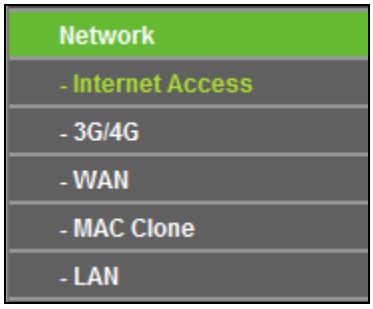


Figure 4-4 the Network menu

There are five submenus under the Network menu (shown in Figure 4-4): **Internet Access**, **3G/4G**, **WAN**, **MAC Clone** and **LAN**. Click any of them, and you will be able to configure the corresponding function.

4.5.1 Internet Access

Choose menu "**Network→Internet Access**", you can configure the access mode on the screen below. The router is designed to work with either WAN port or 3G/4G USB modem, and supports automatically take over back up with 3G/4G access as Ethernet WAN failover.

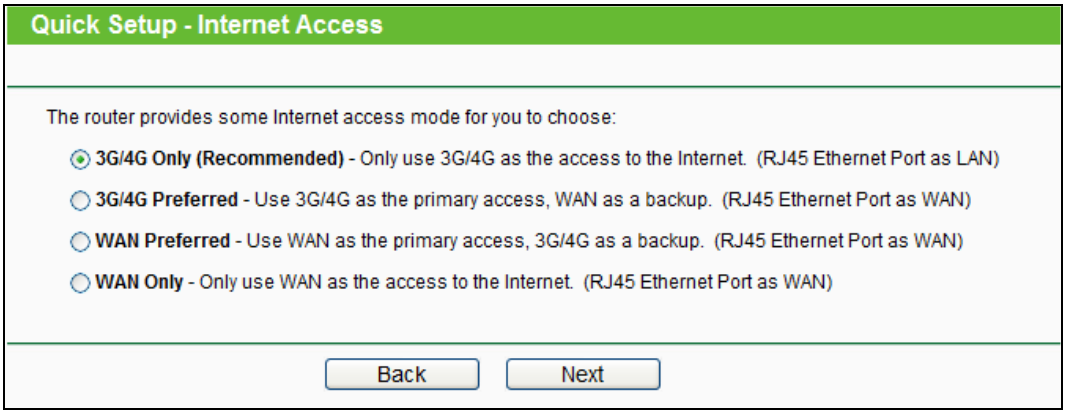


Figure 4-5 Internet Access Mode

- **3G/4G Only (Recommended)**

  In this mode, the router will try 3G/4G access only. WAN access is disabled.

- **3G/4G Preferred**

  In this mode, the router will try 3G/4G access first. When 3G/4G access fails and WAN access is valid, or when no 3G/4G USB modem is inserted, the router would switch to WAN access; when the router succeeds to connect to the 3G/4G network, the router would stop the WAN connection and switch back to 3G/4G access immediately.

- **WAN Preferred**

  In this mode, the router will try WAN access first. When the WAN access fails, and 3G/4G access is valid, the router would switch to 3G/4G access; when the router succeeds to connect to the WAN network, the router would stop the 3G/4G connection and switch back to WAN access immediately.

- **WAN Only**

  In this mode, the router will try WAN access only. 3G/4G access is disabled.

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

Note:

1) In 3G/4G preferred and WAN preferred modes, until 2010-5-18, the failover/backup function only works between 3G/4G link and PPPoE / Dynamic IP / Static IP.

2) The failover/backup feature between 3G/4G link and BigPond Cable / PPTP / L2TP will be available in the near future. Please visit our website to download the latest firmware: http://www.tp-link.com/support/download.asp

3) If you are using the **3G/4G Preferred** or **WAN Preferred**, the router would connect, disconnect or switch the current access automatically. The Connect/Disconnect button (on 3G/4G, PPPoE, PPTP, L2TP) and some related parameters could not be set manually.

4.5.2 3G/4G

Choose menu "**Network→3G/4G**", you can configure parameters for 3G/4G function on the screen below. To use the 3G/4G function, you should first insert your USB modem on the USB port of the Router. There is already much 3G/4G USB modem information embedded in the Router. The USB modem parameters will be set automatically if the card is supported by the Router. Take MA180 for example. If your USB modem inserted is supported by the Router, 3G/4G USB Modem will be **Identified** shown in Figure 4-6. If you want to check more advanced configuration parameters, please click the **Advanced Settings**, and the page shown in Figure 4-7 will then appear. Otherwise, "Unknown Modem" will be shown instead in Figure 4-8. Please visit our website http://www.tp-link.com to get the latest USB modems compatibility list.

Note:

3G/4G settings are unavailable when the Internet Access mode is set to WAN Only mode. Please change settings on 4.5.1 Internet Access if you want to use 3G/4G.

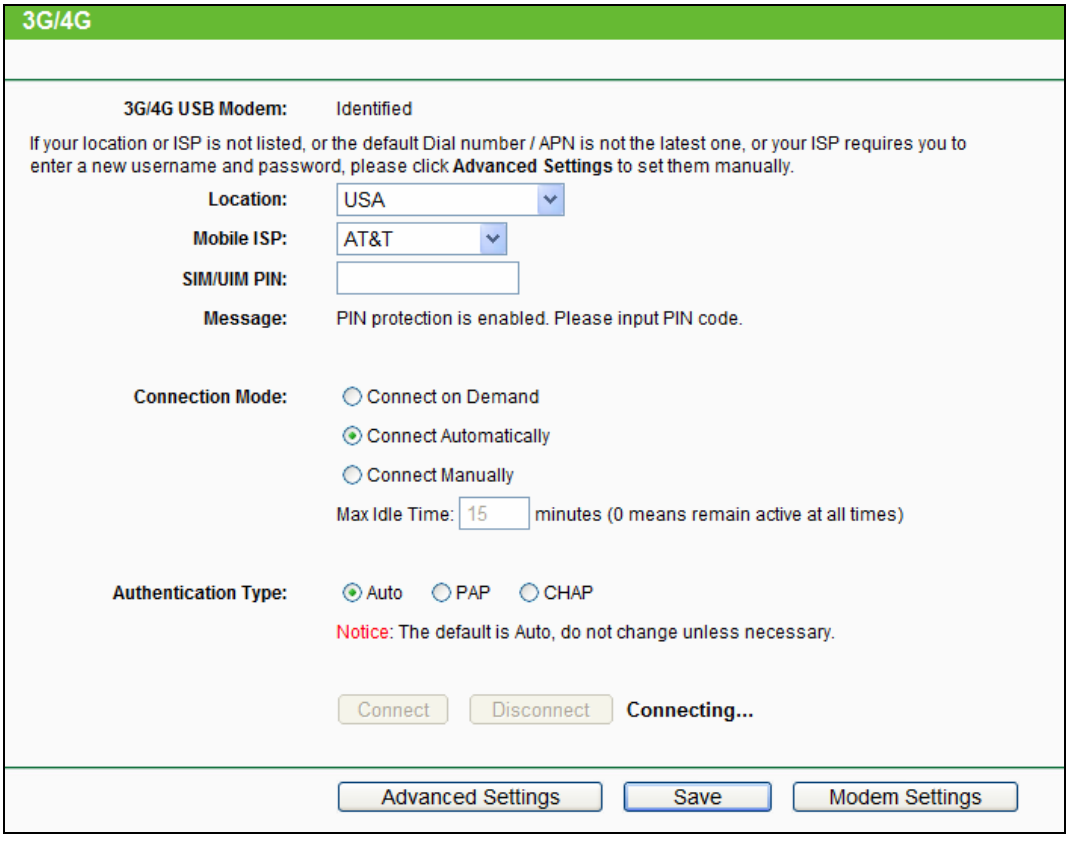


Figure 4-6 3G/4G

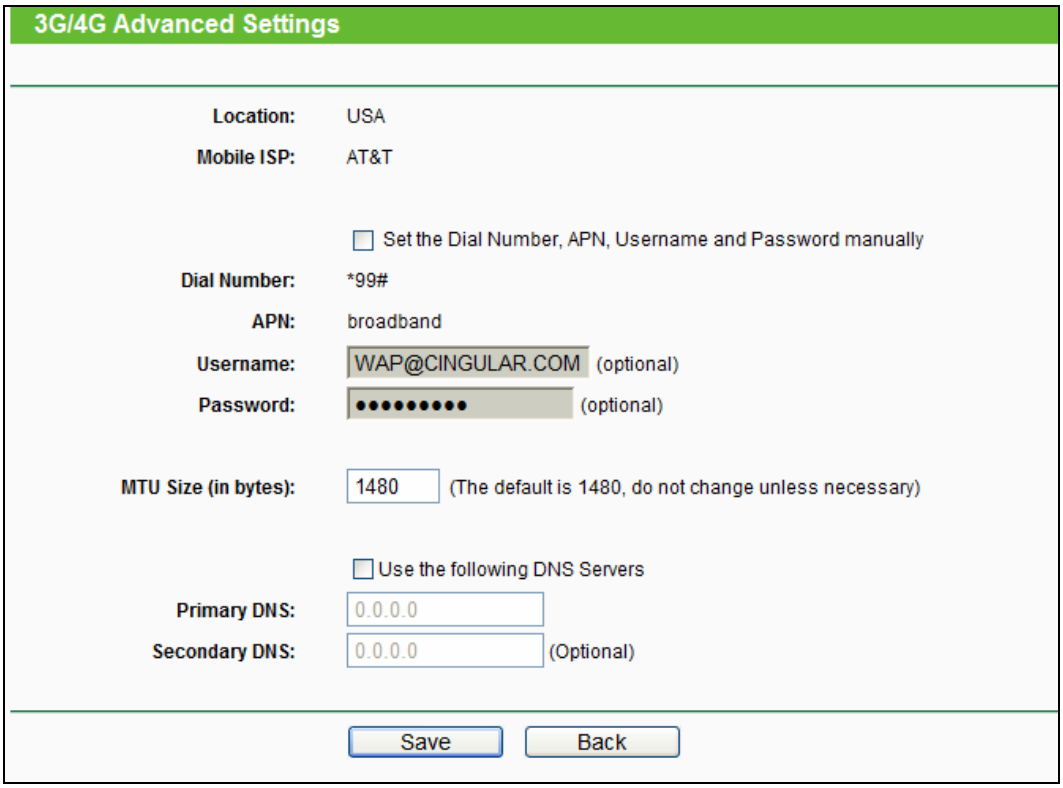


Figure 4-7

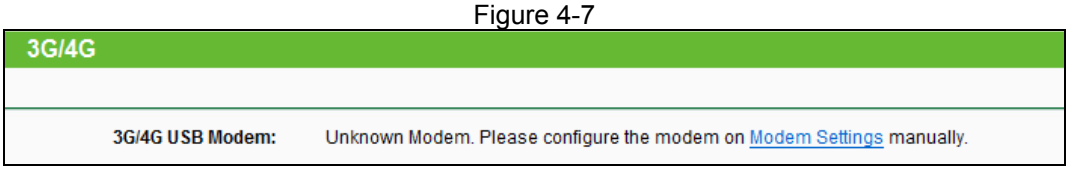


Figure 4-8

- **Location -** Please select the location where you're enjoying the 3G/4G card.
- **Mobile ISP -** Please select the ISP (Internet Service Provider) you apply to for 3G/4G service. The router will show the default Dial Number and APN of that ISP.
- **Set the Dial Number and APN manually -** Check the box and fill the Dial Number and APN blanks below if your ISP is not listed in the **Mobile ISP** list or the default values are not the latest ones.
- **Dial Number -** Enter the Dial Number provided by your ISP.
- **APN -** Enter the APN (Access Point Name) provided by your ISP.
- **Username/Password -** Enter the Username and Password provided by your ISP. These fields are case-sensitive.

Click the **Connect** button to connect to your 3G/4G network. Once the connection is successful, you will find the 3G/4G screen is similar to Figure 4-9. Click menu **Status** and you will see the 3G/4G status is similar to Figure 4-10.

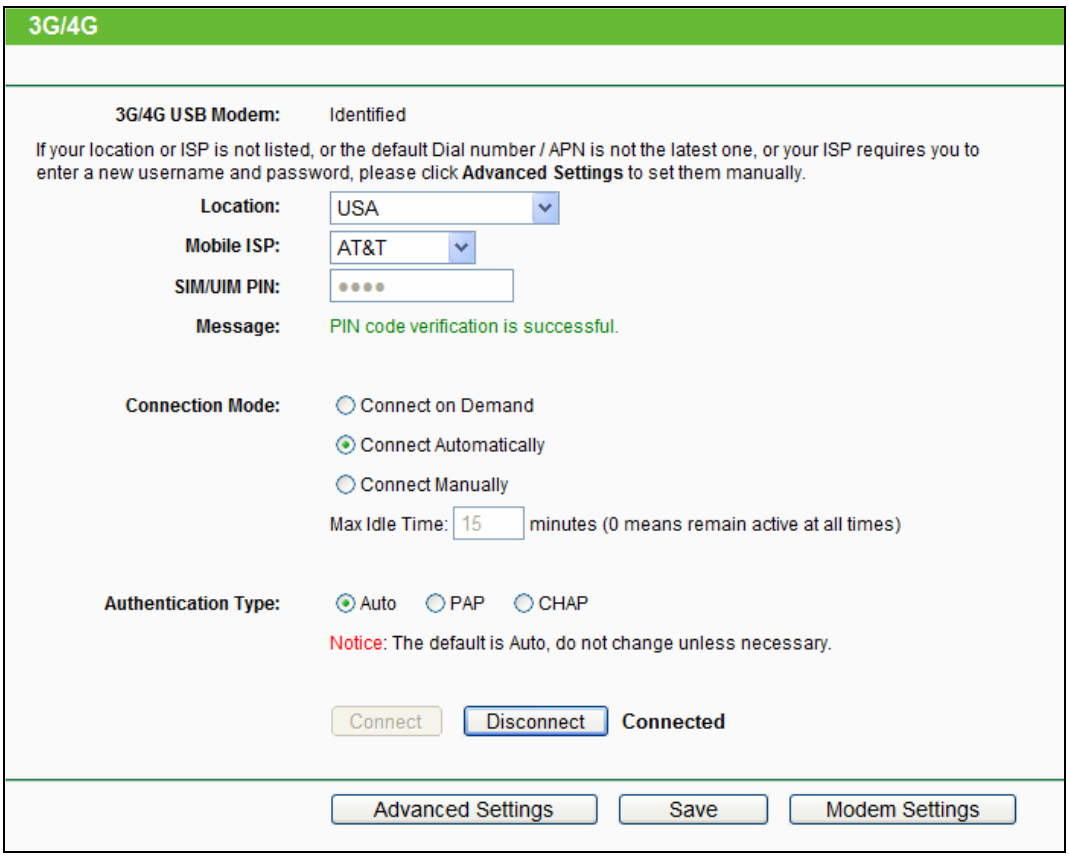


Figure 4-9

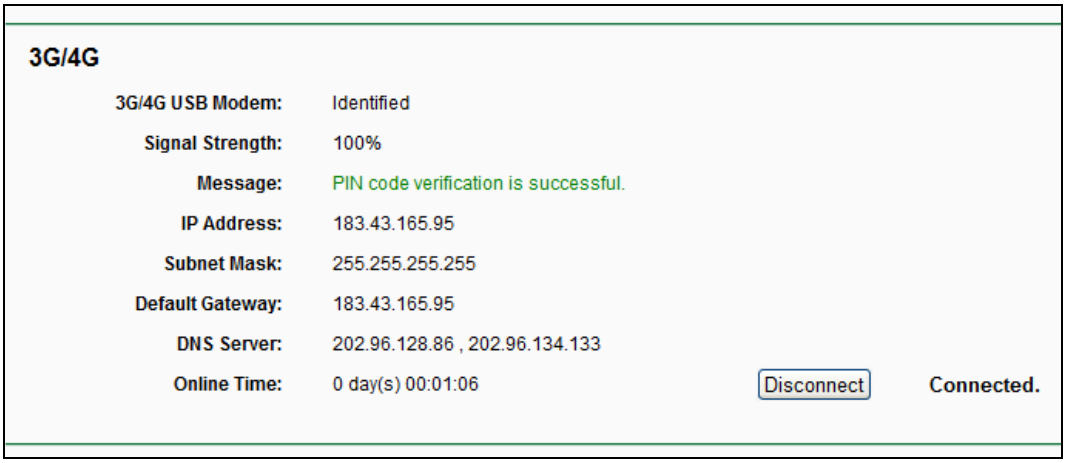


Figure 4-10

- **Connect on Demand -** You can configure the Router 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 Router to automatically re-establish your connection as soon as you attempt to access the Internet again. If you wish to activate **Connect on Demand**, click the radio button. If you want your Internet connection to remain active at all times, enter **0** in the **Max Idle Time** field. Otherwise, enter the number of minutes you want to have elapsed before your Internet connection terminates.

Note:

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

- **Connect Automatically -** Connect automatically after the Router is disconnected. To use this option, click the radio button.
- **Connect Manually -** You can configure the Router to make it connect or disconnect manually. After a specified period of inactivity (**Max Idle Time**), the Router will disconnect 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 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 requested.

Note:

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

- **Authentication Type -** Some ISPs need a specific authentication type, please confirm it with your ISP or keep it Auto.

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

Click the **Modem Settings** button if your 3G/4G USB Modem is not supported by the Router, and then you will see the screen as shown in Figure 4-11. Parameters of your USB modem can be configured on this page.

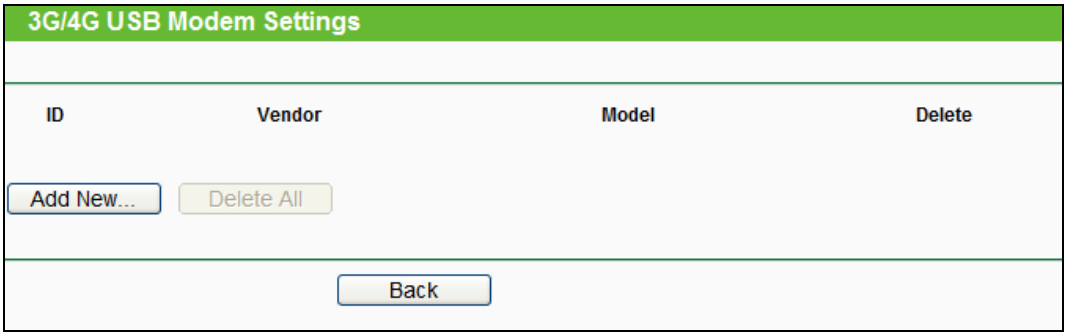


Figure 4-11 3G/4G USB Modem Settings

There are already much 3G/4G USB modem information embedded in the router. The USB modem parameters will be set automatically if the card is supported by the router. But when the router finds the card you just insert "unknown" to it, it will prompt you to set these parameters. The router can identify your "unknown" card if the correct parameters are in the list. We suggest you to do the “3G/4G USB Modem Setting” only in such circumstance.

To add 3G/4G USB Modem entries, follow the steps below.

1. Download a most recent 3G/4G USB modem configuration file from our website (http://www.tp-link.com).
2. Click the **Add New...** button in Figure 4-11, and then you will see Figure 4-12.
3. Click **Browse…** to select the path name where you save the downloaded file on the computer into the File blank.
4. Click the **Upload** button to upload the configuration.

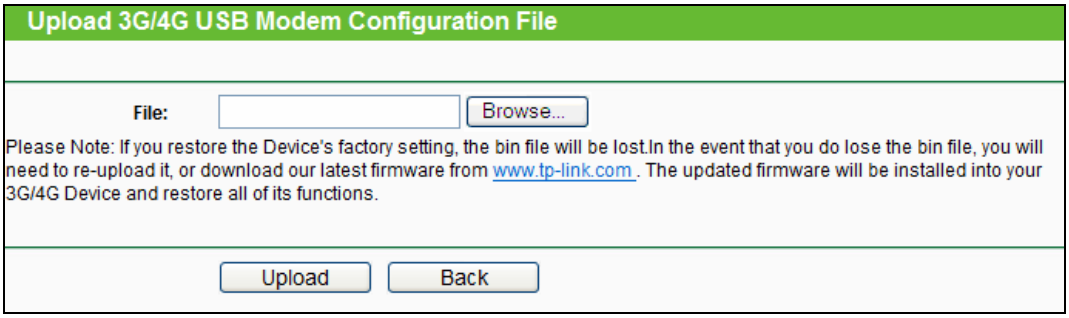


Figure 4-12 Add or Modify a 3G/4G USB Modem Entry

4.5.3 WAN

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

☞ **Note:**

WAN settings are unavailable when the Internet Access mode is set to 3G/4G Only mode. Please change settings on 4.5.1 Internet Access if you want to use WAN.

1. If your ISP provides the DHCP service, please choose **Dynamic IP** type, and the Router will automatically get IP parameters from your ISP. You can see the page as follows (Figure 4-13):

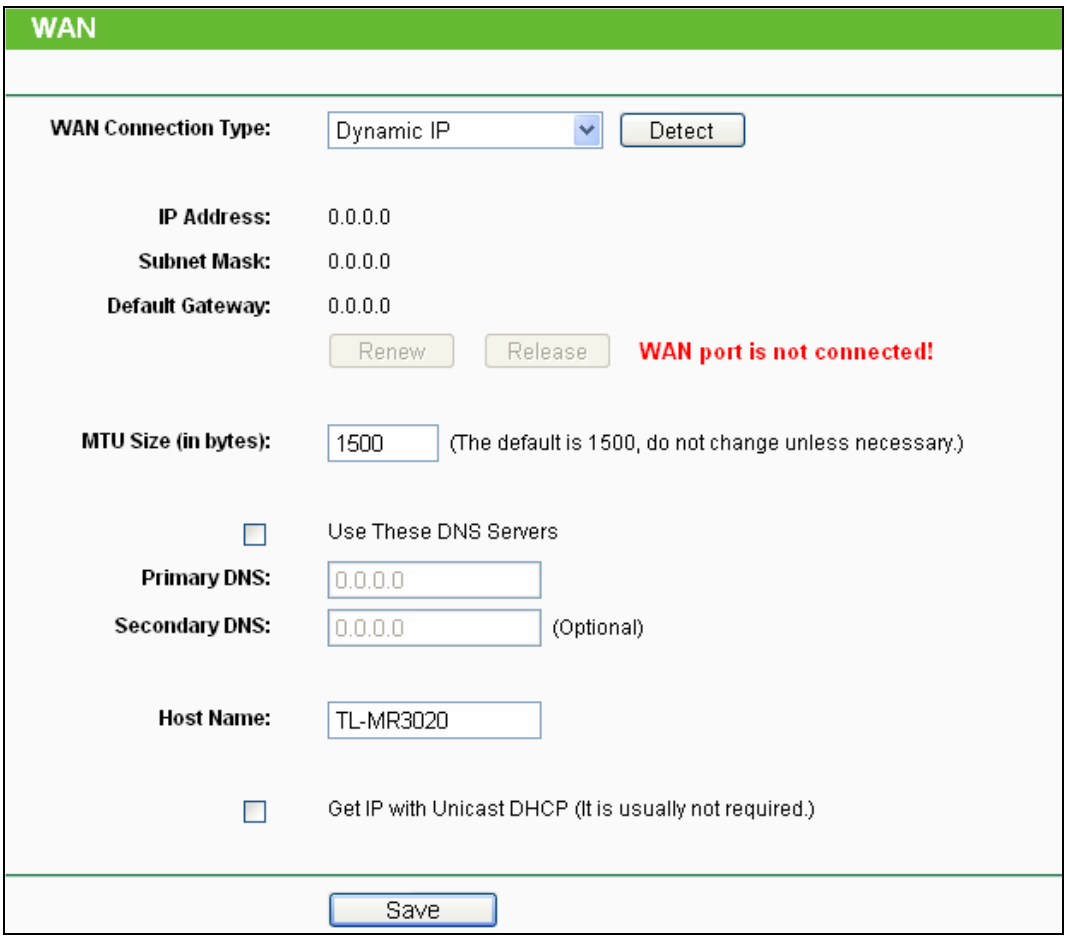


Figure 4-13 WAN - Dynamic IP

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

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

  ☞ **Note:**

  If you 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.

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

2. If your ISP provides a static or fixed IP Address, Subnet Mask, Gateway and DNS setting, select **Static IP**. The Static IP settings page will appear, shown in Figure 4-14.

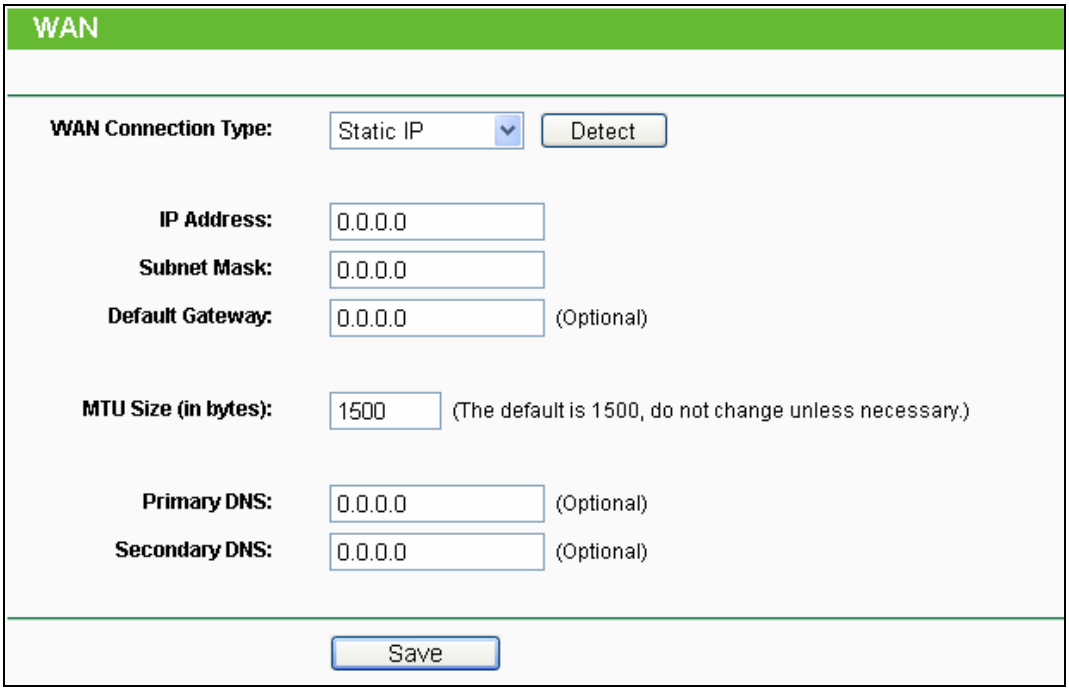


Figure 4-14 WAN - Static IP

- **IP Address -** Enter the IP address in dotted-decimal notation provided by your ISP.
- **Subnet Mask -** Enter the subnet Mask in dotted-decimal notation provided by your ISP, usually is 255.255.255.0.
- **Default Gateway -** (Optional) Enter the gateway IP address in dotted-decimal notation provided by your ISP.
- **MTU Size -** The normal **MTU** (Maximum Transmission Unit) value for most Ethernet networks is 1500 Bytes. It is not recommended that you change the default **MTU Size** unless required by your ISP.
- **Primary/Secondary DNS -** (Optional) Enter one or two DNS addresses in dotted-decimal notation provided by your ISP.

3. If your ISP provides a PPPoE connection, select **PPPoE/Russia PPPoE** option. You should enter the following parameters (Figure 4-15):

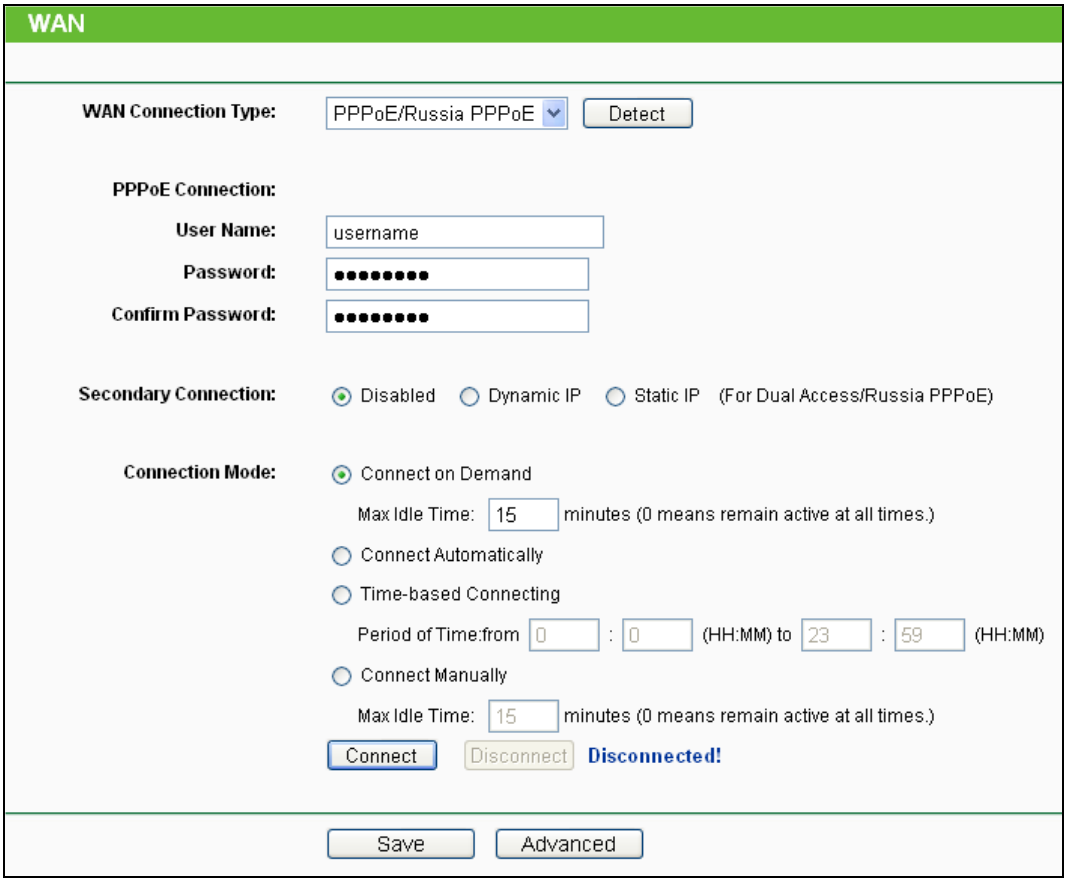


Figure 4-15 WAN - PPPoE

- **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 -** You can check this radio button to use Dynamic IP as the secondary connection to connect to the local area network provided by ISP.
  - **Static IP -** You can check this radio button to use Static IP as the secondary connection to connect to the local area network provided by 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.

- **Time-based Connecting -** The connection will only be established in the period from the start time to the end time (both are in HH:MM format).

  Note:

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

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

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

If you want to do some advanced configurations, please click the **Advanced** button, and the page shown in Figure 4-16 will then appear:

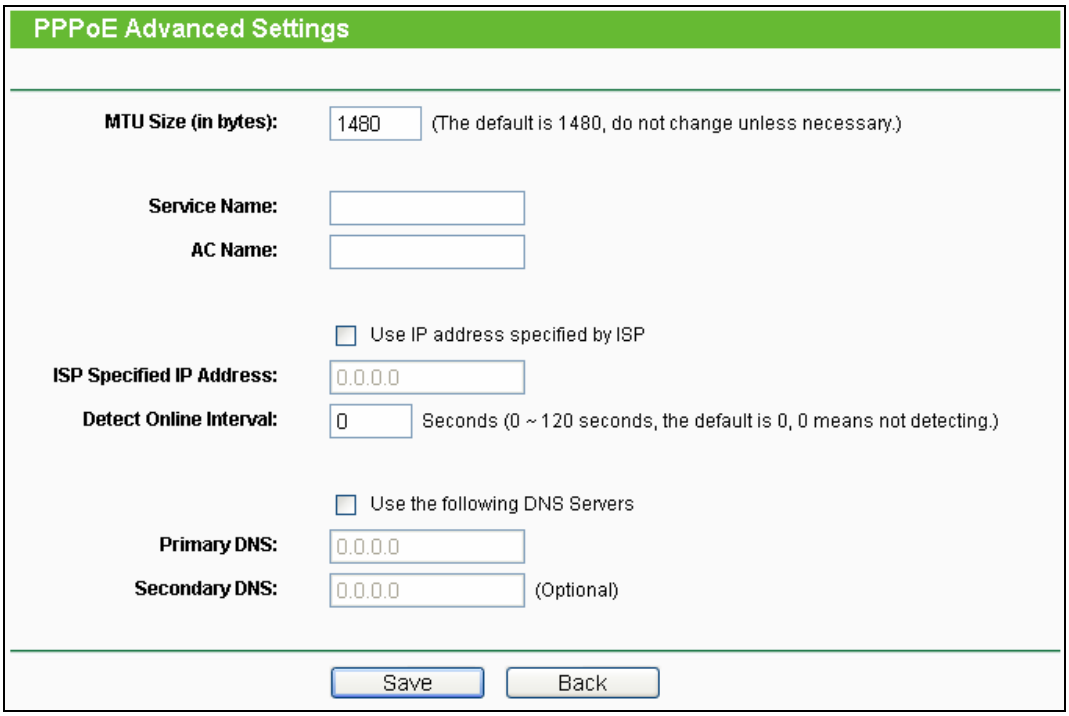


Figure 4-16 PPPoE Advanced Settings

- **MTU Size -** The default MTU size is "1480" bytes, which is usually fine. It is not recommended that you change the default **MTU Size** unless required by your ISP.

- **Service Name/AC Name -** The service name and AC (Access Concentrator) name, which should not be configured unless you are sure it is necessary for your ISP. In most cases, leaving these fields blank will work.

- **ISP Specified IP Address -** If your ISP does not automatically assign IP addresses to the Router during login, please click "**Use IP address specified by ISP**" check box and enter the IP address provided by your ISP in dotted-decimal notation.

- **Detect Online Interval -** The Router will detect Access Concentrator online at every interval. The default value is “0”. You can input the value between “0”and “120”. The value “0” means no detect.
- **DNS IP address -** If your ISP does not automatically assign DNS addresses to the Router during login, please click “**Use the following DNS servers**” check box and enter the IP address in dotted-decimal notation of your ISP’s primary DNS server. If a secondary DNS server address is available, enter it as well.

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

4. If your ISP provides BigPond Cable (or Heart Beat Signal) connection, please select **BigPond Cable**. And you should enter the following parameters (Figure 4-17):

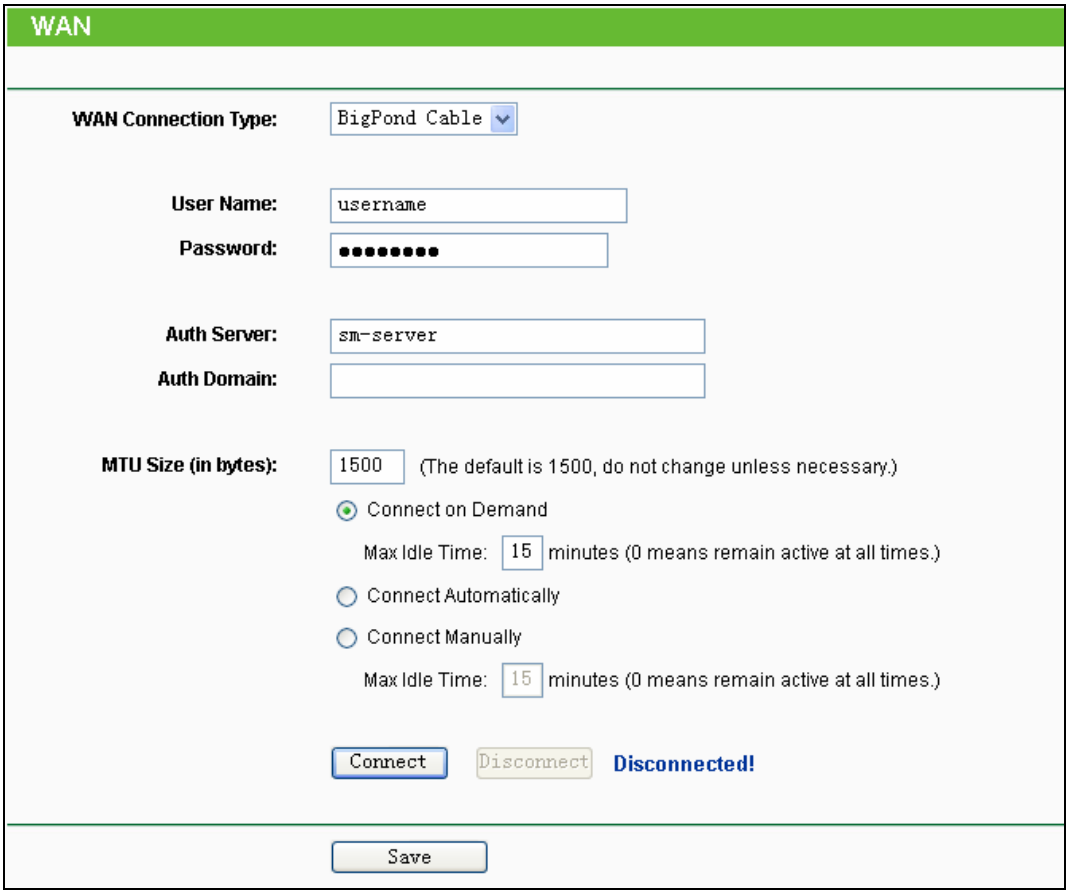


Figure 4-17 WAN – BigPond Cable

- **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.

e.g.

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.

Caution: 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. And you should enter the following parameters (Figure 4-18):

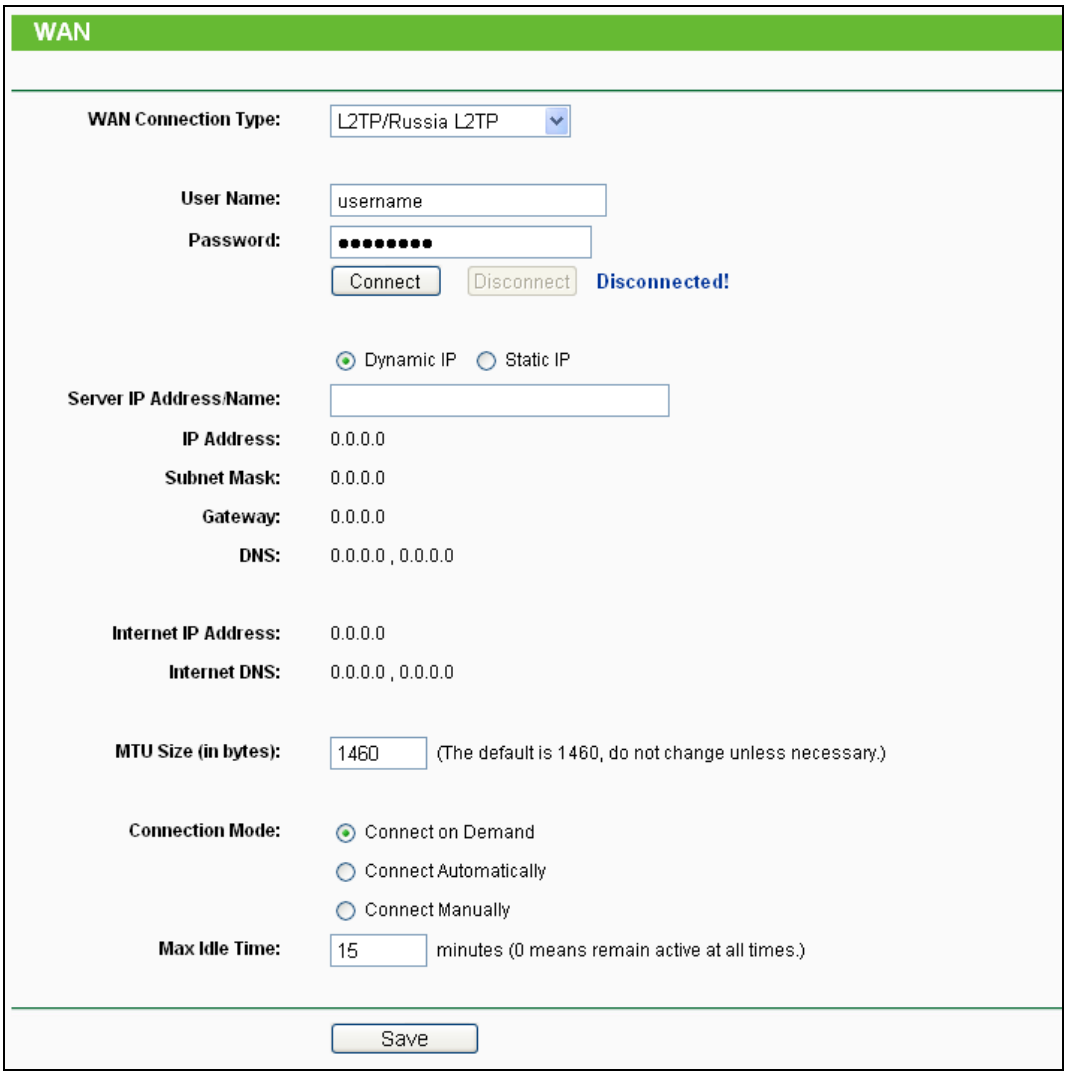


Figure 4-18 L2TP Settings

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

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

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

6. If your ISP provides PPTP connection, please select **PPTP/Russia PPTP** option. And you should enter the following parameters (Figure 4-19):

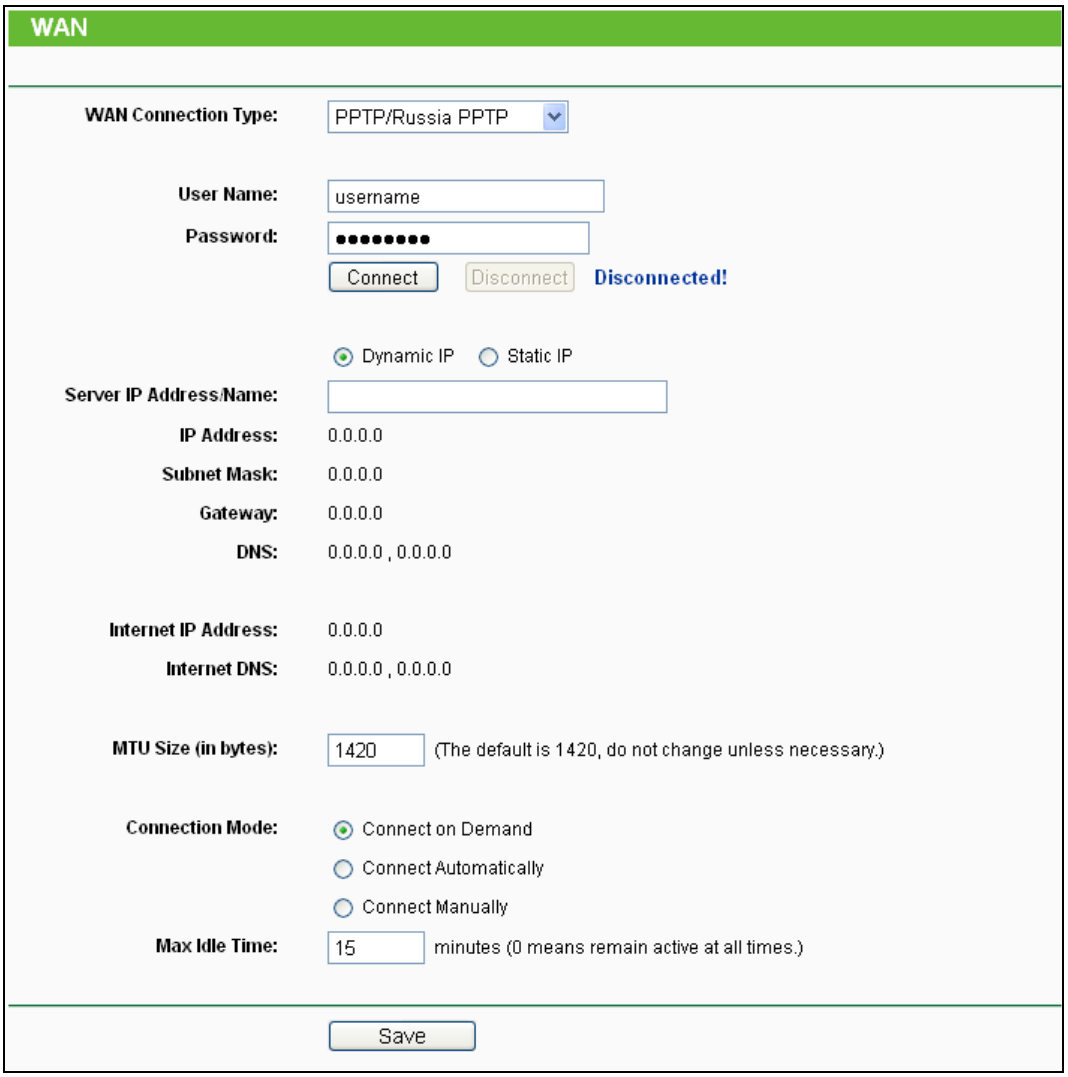


Figure 4-19 PPTP Settings

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

- **Dynamic IP/ Static IP -** Choose either as you are given by your ISP and enter the ISP's IP address or the domain name.

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

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

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

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

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

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

☞ **Note:**

If you don't know how to choose the appropriate connection type, click the **Detect** button to allow the Router to automatically search your Internet connection for servers and protocols. The connection type will be reported when an active Internet service is successfully detected by the Router. This report is for your reference only. To make sure the connection type your ISP provides, please refer to the ISP. The various types of Internet connections that the Router can detect are as follows:

- **PPPoE -** Connections which use PPPoE that requires a user name and password.
- **Dynamic IP -** Connections which use dynamic IP address assignment.
- **Static IP -** Connections which use static IP address assignment.

The Router can not detect PPTP/L2TP/BigPond connections with your ISP. If your ISP uses one of these protocols, then you must configure your connection manually.

4.5.4 MAC Clone

Choose menu "**Network→MAC Clone**", you can configure the MAC address of the WAN on the screen below, Figure 4-20:

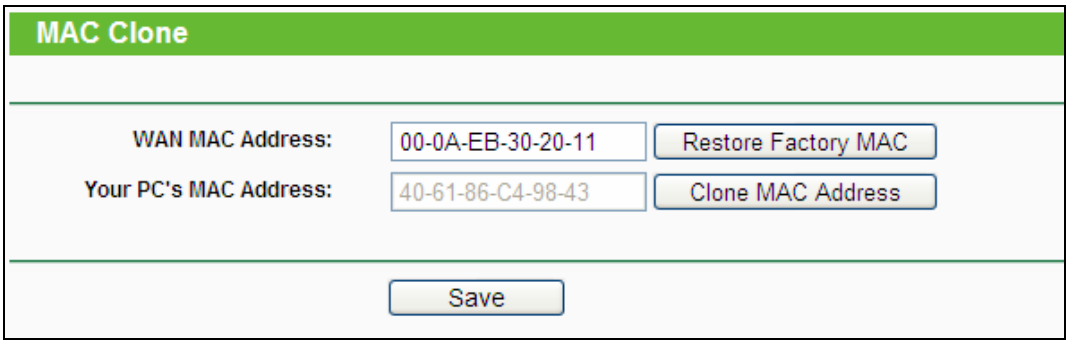


Figure 4-20 MAC Address Clone

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

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

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

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

☞ **Note:**

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

4.5.5 LAN

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

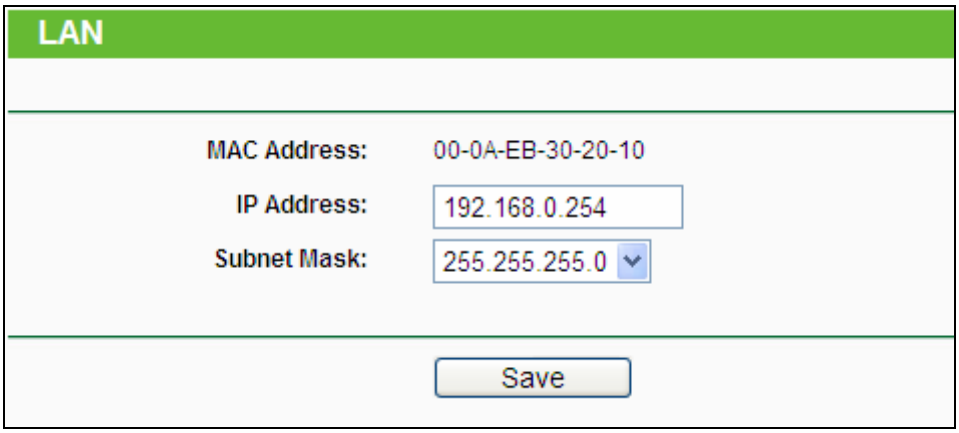


Figure 4-21 LAN

- **MAC Address -** The physical address of the Router, as seen from the LAN. The value can't be changed.
- **IP Address -** Enter the IP address of your Router or reset it in dotted-decimal notation (factory default: 192.168.0.254).
- **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 change accordingly at the same time，while the Virtual Server and DMZ Host will not take effect until they are re-configured.

4.6 Wireless

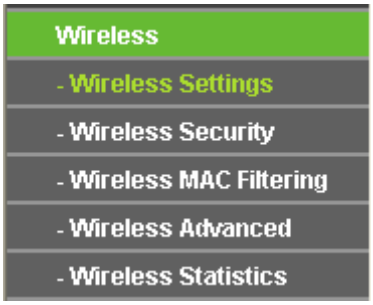


Figure 4-22 Wireless menu

There are five submenus under the Wireless menu (shown in Figure 4-22): **Wireless Settings**, **Wireless Security, Wireless MAC Filtering, Wireless Advanced** and **Wireless Statistics.** Click any of them, and you will be able to configure the corresponding function.

4.6.1 Wireless Settings

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

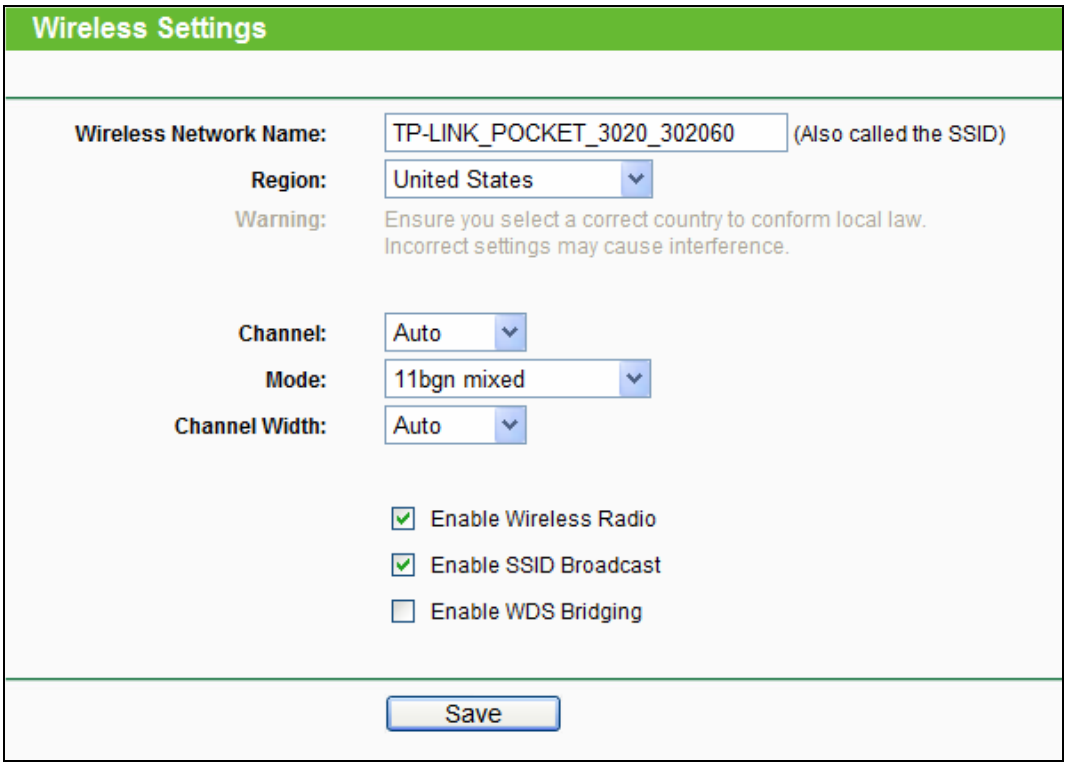


Figure 4-23 Wireless Settings

- **Wireless Network Name -** Enter a value of up to 32 characters. The same name of Wireless Network Name must be assigned to all wireless devices in your network. Considering your wireless network security, the default Wireless Network Name is set to be TP-LINK_POCKET_3020_XXXXXX (XXXXXX indicates the last six unique numbers of each Router's MAC address). 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 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.

Note:

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

- **Channel -** This field determines which operating frequency will be used. The default channel is set to **Auto**, so the Router will choose the best channel automatically. It is not necessary to change the wireless channel unless you notice interference problems with another nearby access point.

- **Mode -** Select the desired mode. The default setting is 11bgn mixed.

  11b only - Select if all of your wireless clients are 802.11b.

  11g only - Select if all of your wireless clients are 802.11g.

11n only - Select if all of your wireless clients are 802.11n.

11bg mixed - Select if you are using both 802.11b and 802.11g wireless clients.

11bgn mixed - Select if you are using a mix of 802.11b, 11g, and 11n wireless clients.

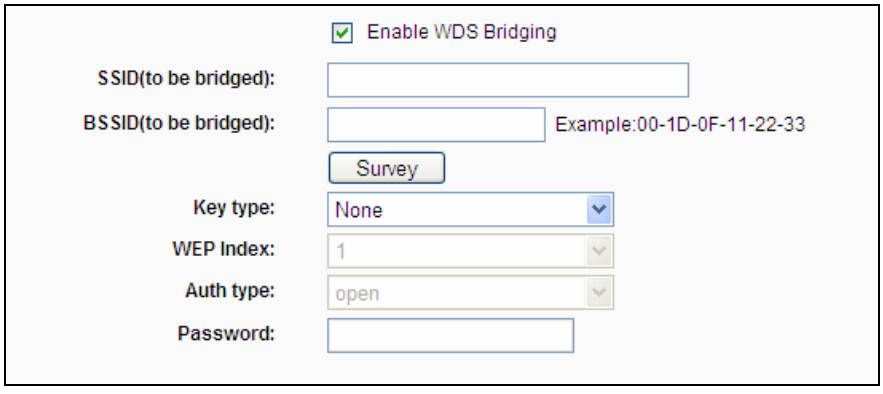
Select the desired wireless mode. When 802.11g mode is selected, only 802.11g wireless stations can connect to the Router. When 802.11n mode is selected, only 802.11n wireless stations can connect to the AP. It is strongly recommended that you set the Mode to **802.11b&g&n**, and all of 802.11b, 802.11g, and 802.11n wireless stations can connect to the Router.

- **Channel width -** Select any channel width from the pull-down list. The default setting is automatic, which can adjust the channel width for your clients automatically.

Note:

If **11b only**, **11g only**, or **11bg mixed** is selected in the **Mode** field, the **Channel Width** selecting field will turn grey and the value will become 20M, which is unable to be changed.

- **Max Tx Rate -** You can limit the maximum tx rate of the Router through this field.
- **Enable Wireless Router Radio -** The wireless radio of this Router can be enabled or disabled to allow wireless stations access.
- **Enable SSID Broadcast -** When wireless clients survey the local area for wireless networks to associate with, they will detect the SSID broadcast by the Router. If you select the **Enable SSID Broadcast** checkbox, the Wireless Router will broadcast its name (SSID) on the air.
- **Enable WDS Bridging -** Check this box to enable WDS Bridging. With this function, the Router can bridge two or more WLANs. If this checkbox is selected, you will have to set the following parameters as shown below. Make sure the following settings are correct



- **SSID(to be bridged)** - The SSID of the AP your Router is going to connect to as a client. You can also use the search function to select the SSID to join.
- **BSSID(to be bridged)** - The BSSID of the AP your Router 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.
- **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.

- **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.
- **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.
- **Password** - If the AP your Router is going to connect needs password, you need to fill the password in this blank.

4.6.2 Wireless Security

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

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

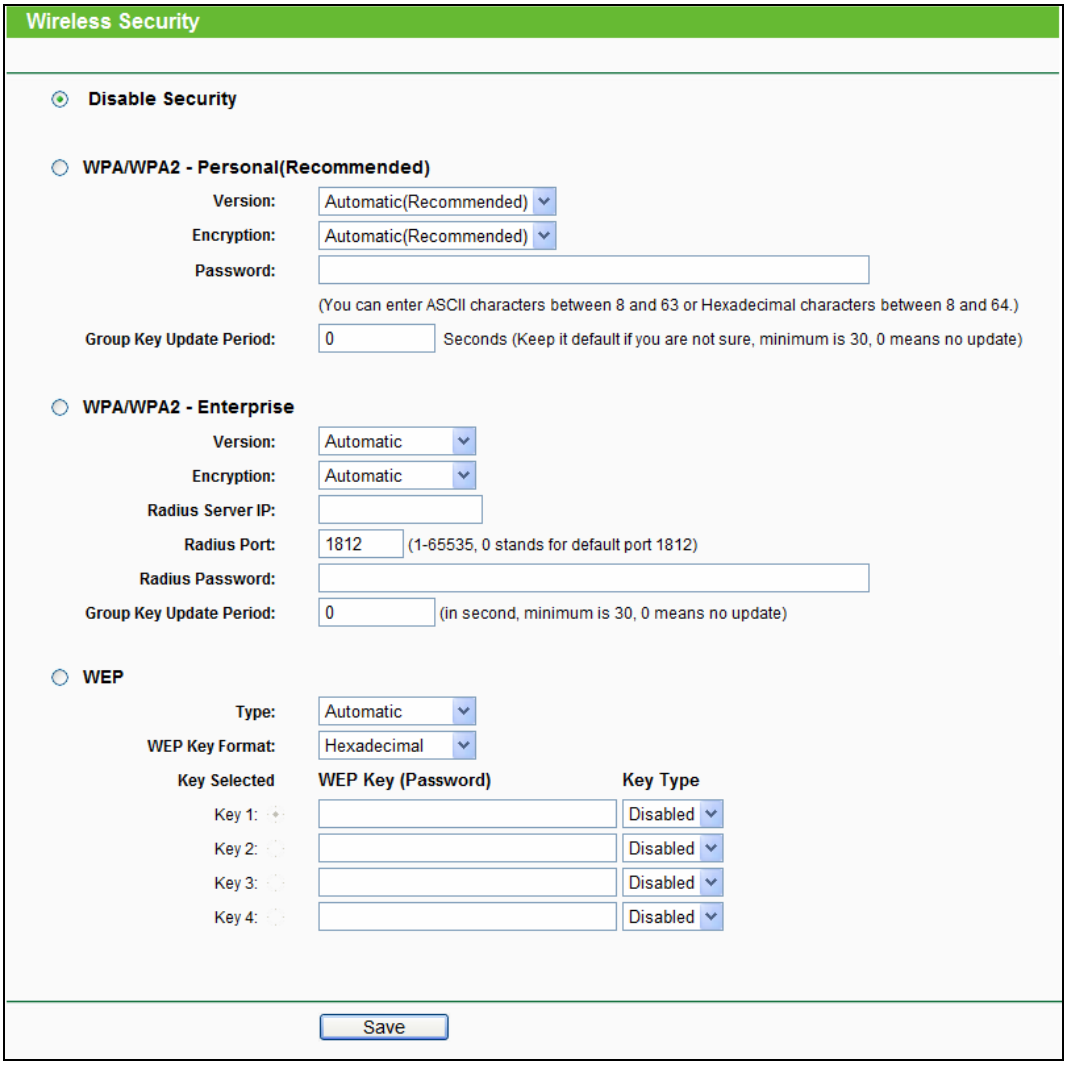


Figure 4-24

- **Disable Security -** If you do not want to use wireless security, select this check box, but it's strongly recommended to choose one of the following modes to enable security.

➢ **WPA/WPA2 – Personal (Recommended) -** It's the WPA/WPA2 authentication type based on pre-shared passphrase.

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

☞ **Note:**

If you check the **WPA/WPA2 – Personal (Recommended)** radio button and choose TKIP encryption, you will find a notice in red as shown in Figure 4-25.

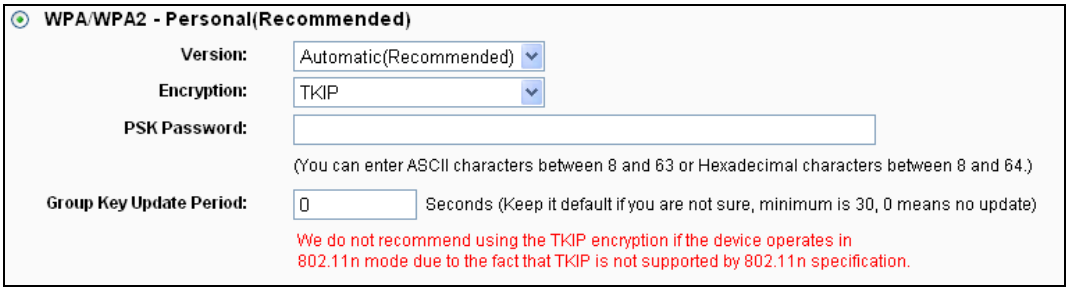


Figure 4-25

- **PSK Password -** You can enter ASCII characters between 8 and 63 characters or 8 to 64 Hexadecimal characters.
- **Group Key Update Period -** Specify the group key update interval in seconds. The value should be 30 or above. Enter 0 to disable the update.

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

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

- **Version -** you can choose the version of the WPA security on the pull-down list. The default setting is **Automatic**, which can select **WPA (**Wi-Fi Protected Access) or **WPA2 (**WPA version 2) automatically based on the wireless station's capability and request.
- **Encryption -** You can select either **Automatic**, or **TKIP** or **AES.**

☞ **Note:**

If you check the **WPA/WPA2 - Enterprise** radio button and choose TKIP encryption, you will find a notice in red as shown in Figure 4-26.

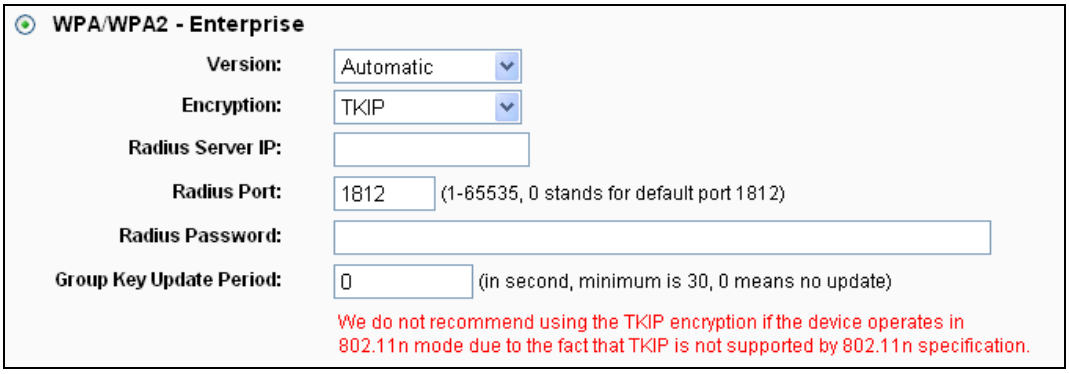


Figure 4-26

- **Radius Server IP -** Enter the IP address of the Radius Server.
- **Radius Port -** Enter the port that radius service used.
- **Radius Password -** Enter the password for the Radius Server.
- **Group Key Update Period -** Specify the group key update interval in seconds. The value should be 30 or above. Enter 0 to disable the update.

➢ **WEP -** It is based on the IEEE 802.11 standard. If you select this check box, you will find a notice in red as show in Figure 4-27.

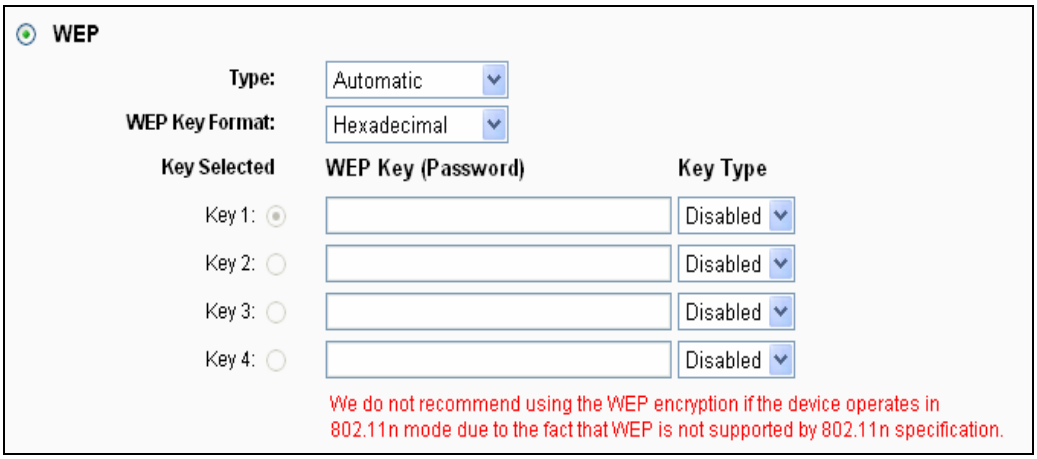


Figure 4-27

- **Type -** you can choose the type for the WEP security on the pull-down list. The default setting is **Automatic**, which can select **Open System** or **Shared Key** authentication type automatically based on the wireless station's capability and request.
- **WEP Key Format - Hexadecimal** and **ASCII** formats are provided. **Hexadecimal** format stands for any combination of hexadecimal digits (0-9, a-f, A-F) in the specified length. **ASCII** format stands for any combination of keyboard characters in the specified length.

- **WEP Key-** Select which of the four keys will be used and enter the matching WEP key that you create. Make sure these values are identical on all wireless stations in your network.

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

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

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

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

☞ **Note:**

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

4.6.3 Wireless MAC Filtering

Choose menu "**Wireless → Wireless MAC Filtering**", you can control the wireless access by configuring the Wireless MAC Address Filtering function, shown in Figure 4-28.

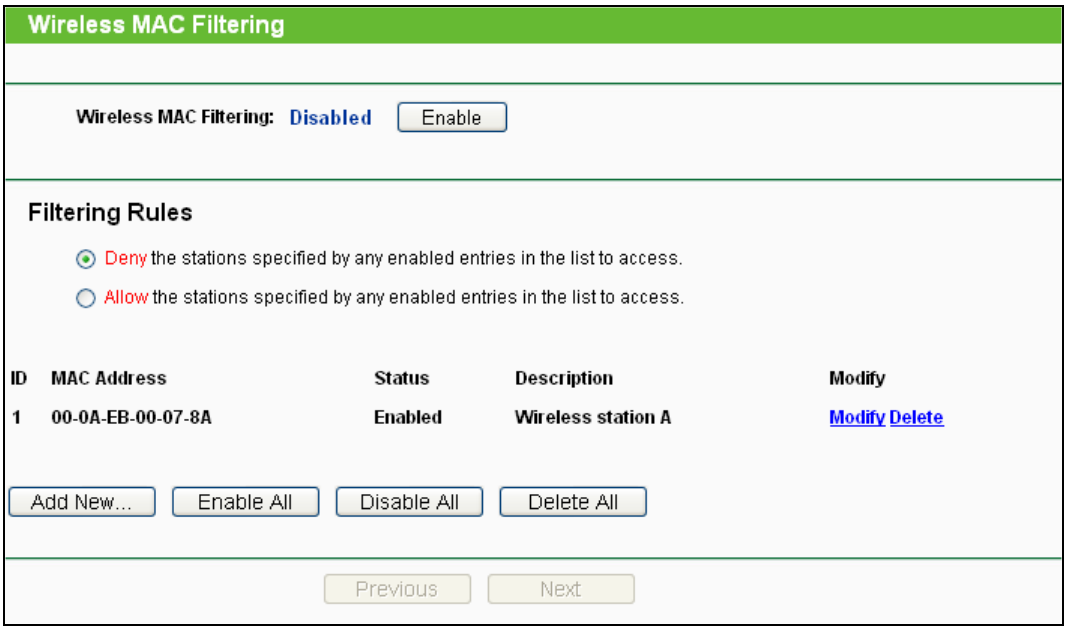


Figure 4-28 Wireless MAC address Filtering

To filter wireless users by MAC Address, click **Enable**. The default setting is **Disabled**.

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

To Add a Wireless MAC Address filtering entry, click the **Add New…** button. The "**Add or Modify Wireless MAC Address Filtering entry**" page will appear, shown in Figure 4-29:

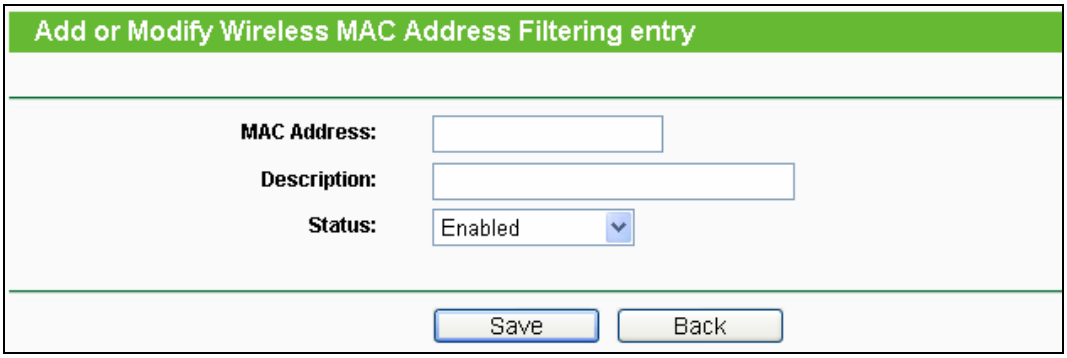


Figure 4-29 Add or Modify Wireless MAC Address Filtering entry

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

1. Enter the appropriate MAC Address into the **MAC Address** field. The format of the MAC Address is XX-XX-XX-XX-XX-XX (X is any hexadecimal digit). For example: 00-0A-EB-00-07-8A.
2. Enter a simple description of the wireless station in the **Description** field. For example: Wireless station A.
3. **Status -** Select **Enabled** or **Disabled** for this entry on the **Status** pull-down list.
4. Click the **Save** button to save this entry.

To modify or delete an existing entry:

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

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

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

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

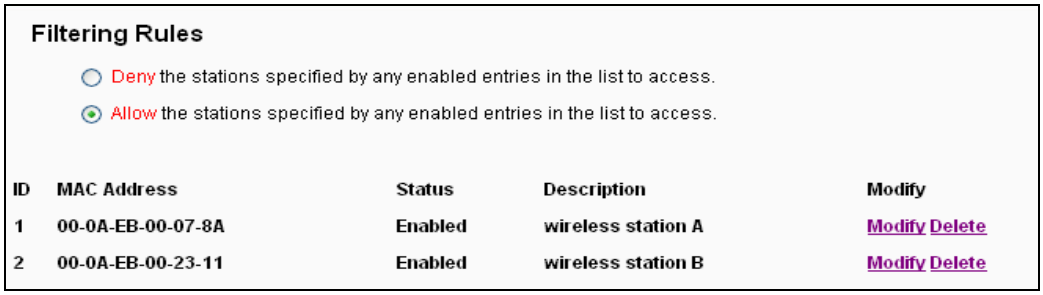
Click the **Next** button to go to the next page

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

For example: If you desire that the wireless station A with MAC address 00-0A-EB-00-07-8A and the wireless station B with MAC address 00-0A-EB-00-23-11 are able to access the Router, but all the other wireless stations cannot access the Router, you can configure the **Wireless MAC 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-00-07-8A /00-0A-EB-00-23-11 in the **MAC Address** field, then enter wireless station A/B in the **Description** field, while select **Enabled** in the **Status** pull-down list. Finally, click the **Save** and the **Back** button.

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



4.6.4 Wireless Advanced

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

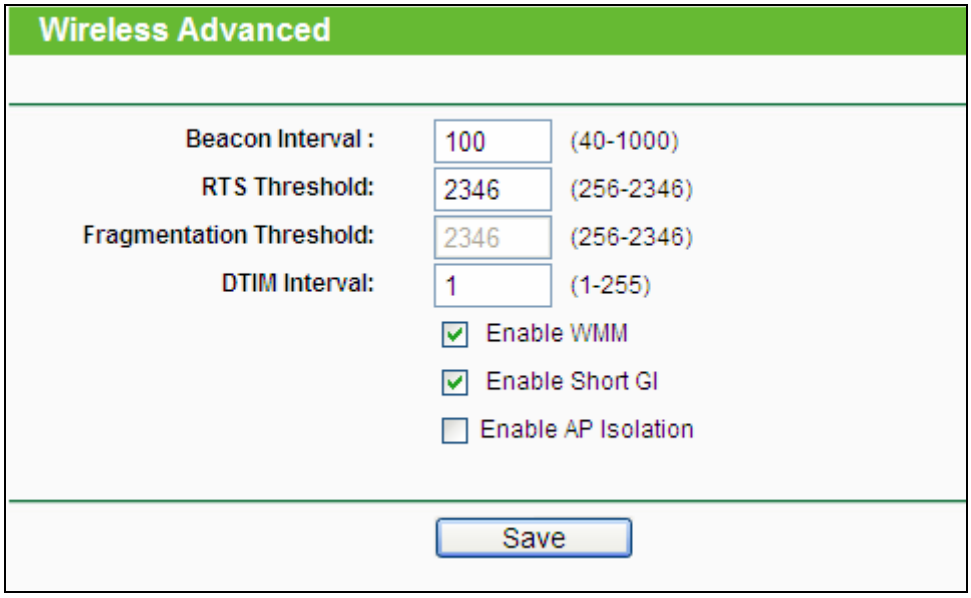


Figure 4-30 Wireless Advanced

- **Beacon Interval -** Enter a value between 40-1000 milliseconds for Beacon Interval here. The beacons are the packets sent by the router to synchronize a wireless network. Beacon Interval value determines the time interval of the beacons. The default value is 100.

- **RTS Threshold -** Here you can specify the RTS (Request to Send) Threshold. If the packet is larger than the specified RTS Threshold size, the router will send RTS frames to a particular receiving station and negotiate the sending of a data frame. The default value is 2346.
- **Fragmentation Threshold -** This value is the maximum size determining whether packets will be fragmented. Setting the Fragmentation Threshold too low may result in poor network performance since excessive packets. 2346 is the default setting and is recommended.
- **DTIM Interval -** This value determines the interval of the Delivery Traffic Indication Message (DTIM). A DTIM field is a countdown field informing clients of the next window for listening to broadcast and multicast messages. When the Router has buffered broadcast or multicast messages for associated clients, it sends the next DTIM with a DTIM Interval value. You can specify the value between 1-255 Beacon Intervals. The default value is 1, which indicates the DTIM Interval is the same as Beacon Interval.
- **Enable WMM - WMM** function can guarantee the packets with high- priority messages being transmitted preferentially. It is strongly recommended enabled.
- **Enable Short GI -** This function is recommended for it will increase the data capacity by reducing the guard interval time.
- **Enabled AP Isolation -** This function can isolate wireless stations on your network from each other. Wireless devices will be able to communicate with the Router but not with each other. To use this function, check this box. AP Isolation is disabled by default.

Note:

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

4.6.5 Wireless Statistics

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

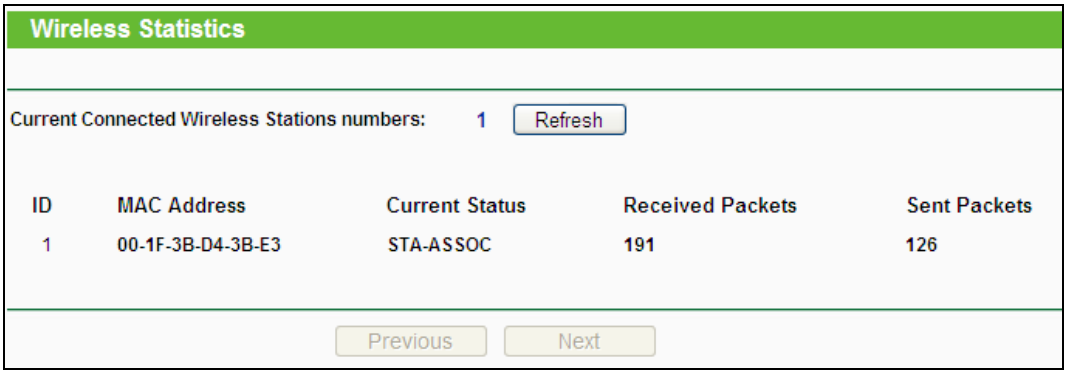


Figure 4-31 The Router attached wireless stations

- **MAC Address -** The connected wireless station's MAC address
- **Current Status -** The connected wireless station's running status, one of **STA-AUTH / STA-ASSOC / STA-JOINED / WPA / WPA-PSK / WPA2 / WPA2-PSK / AP-UP / AP-DOWN / Disconnected**
- **Received Packets -** Packets received by the station
- **Sent Packets -** Packets sent by the station

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

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

☞ **Note:**

This page will be refreshed automatically every 5 seconds.

4.7 DHCP

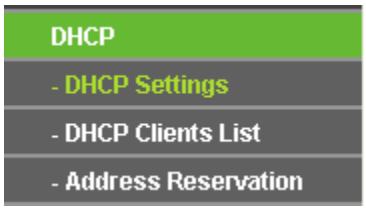


Figure 4-32 The DHCP menu

There are three submenus under the DHCP menu (shown in Figure 4-32): **DHCP Settings**, **DHCP Clients List** and **Address Reservation.** Click any of them, and you will be able to configure the corresponding function.

4.7.1 DHCP Settings

Choose menu "**DHCP→DHCP Settings**", you can configure the DHCP Server on the page (shown in Figure 4-33).The Router is set up by default as a DHCP (Dynamic Host Configuration Protocol) server, which provides the TCP/IP configuration for all the PC(s) that are connected to the Router on the LAN.

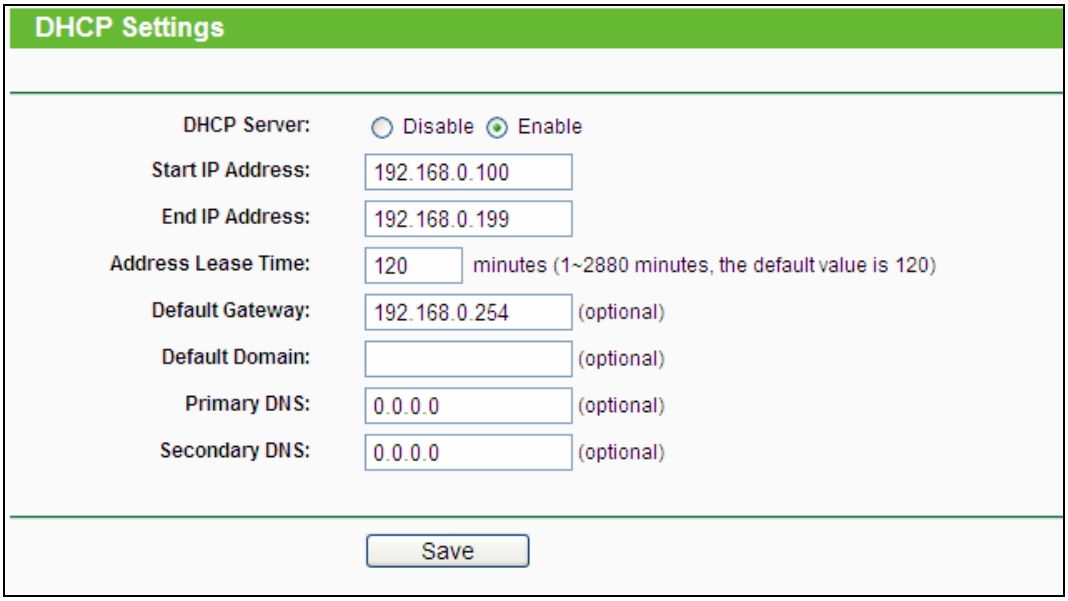


Figure 4-33 DHCP Settings

- **DHCP Server - Enable** or **Disable** the DHCP server. If you disable the Server, you must have another DHCP server within your network or else you must configure the computer manually.
- **Start IP Address -** Specify an IP address for the DHCP Server to start with when assigning IP addresses. 192.168.0.100 is the default start address.
- **End IP Address -** Specify an IP address for the DHCP Server to end with when assigning IP addresses. 192.168.0.199 is the default end address.
- **Address Lease Time -** The **Address Lease Time** is the amount of time a network user will be allowed connection to the Router with their current dynamic IP Address. Enter the amount of time in minutes and the user will be "leased" this dynamic IP Address. After the time is up, the user 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) Suggest to input the IP address of the LAN port of the Router, default value is 192.168.0.254.
- **Default Domain -** (Optional) Input the domain name of your network.
- **Primary DNS -** (Optional) Input the DNS IP address provided by your ISP. Or consult your ISP.
- **Secondary DNS -** (Optional) Input the IP address of another DNS server if your ISP provides two DNS servers.

Note:

To use the DHCP server function of the Router, you must configure all computers on the LAN as "Obtain an IP address automatically" mode.

4.7.2 DHCP Clients List

Choose menu "**DHCP→DHCP Clients List**", you can view the information about the clients attached to the Router in the next screen (shown in Figure 4-34).

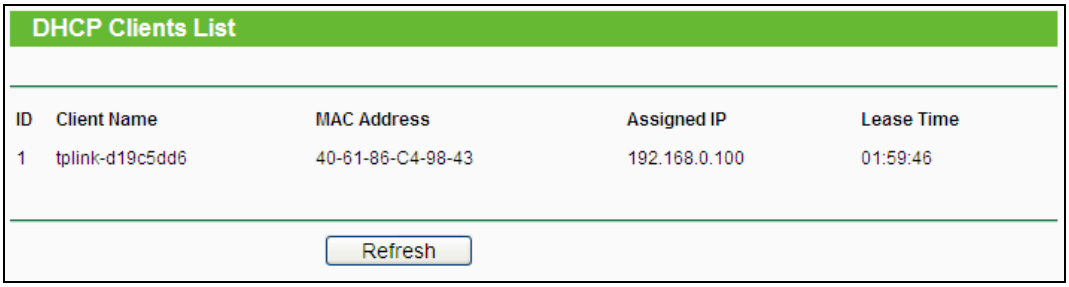


Figure 4-34 DHCP Clients List

- **ID -** The index of the DHCP Client
- **Client Name -** The name of the DHCP client
- **MAC Address -** The MAC address of the DHCP client
- **Assigned IP -** The IP address that the Router has allocated to the DHCP client.
- **Lease Time -** The time of the DHCP client leased. After the dynamic IP address has expired, a new dynamic IP address will be automatically assigned to the user.

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

4.7.3 Address Reservation

Choose menu "**DHCP→Address Reservation**", you can view and add a reserved addresses for clients via the next screen (shown in Figure 4-35).When you specify a reserved IP address for a PC on the LAN, that PC will always receive the same IP address each time when it accesses the DHCP server. Reserved IP addresses should be assigned to the servers that require permanent IP settings.

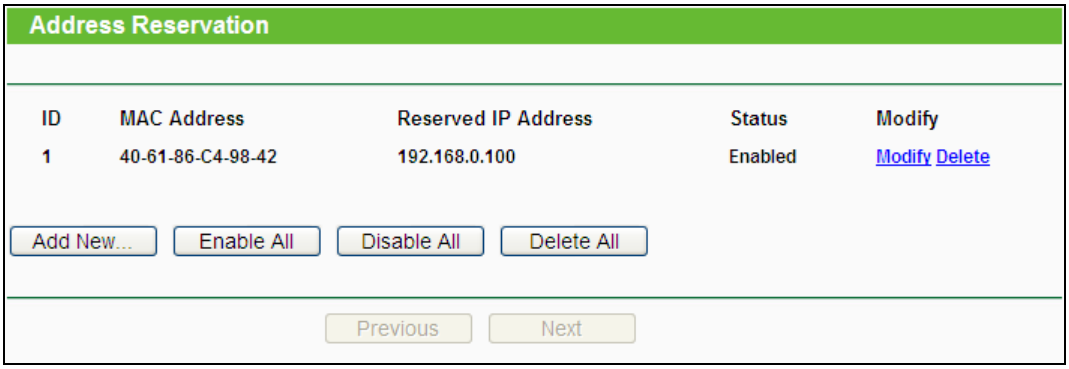


Figure 4-35 Address Reservation

- **MAC Address -** The MAC address of the PC for which you want to reserve IP address.
- **Assigned IP Address -** The IP address of the Router reserved.

- **Status -** The status of this entry either **Enabled** or **Disabled**.

To Reserve IP addresses:

1. Click the **Add New …** button. (Pop-up Figure 4-36)
2. Enter the MAC address (in XX-XX-XX-XX-XX-XX format.) and IP address in dotted-decimal notation of the computer you wish to add.
3. Click the **Save** button when finished.

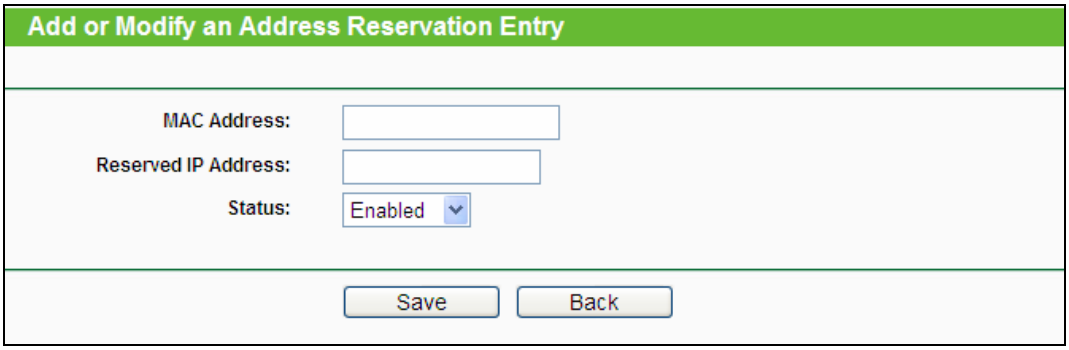


Figure 4-36 Add or Modify an Address Reservation Entry

To modify or delete an existing entry:

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

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

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

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

4.8 Forwarding

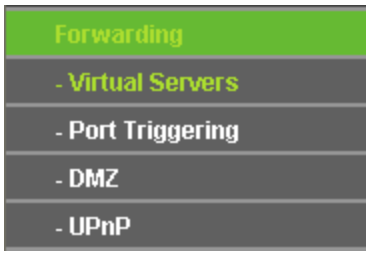


Figure 4-37 The Forwarding menu

There are four submenus under the Forwarding menu (shown in Figure 4-37): **Virtual Servers**, **Port Triggering**, **DMZ** and **UPnP**. Click any of them, and you will be able to configure the corresponding function.

4.8.1 Virtual Servers

Choose menu "**Forwarding→Virtual Servers**", you can view and add virtual servers in the next screen (shown in Figure 4-38). 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 be changed when using the DHCP function.

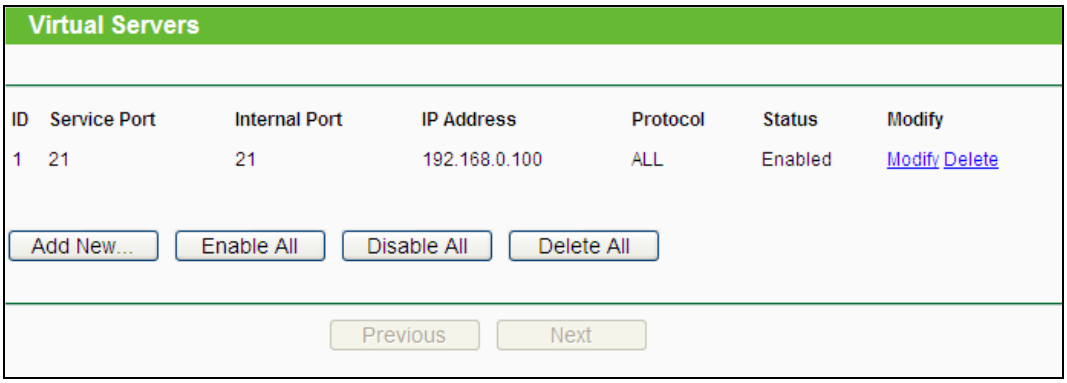


Figure 4-38 Virtual Servers

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

To setup a virtual server entry:

1. Click the **Add New…** button. (pop-up Figure 4-39)
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 **IP Address** box.
4. Select the protocol used for this application, either **TCP** or **UDP**, or **All**.
5. Select the **Enable** check box to enable the virtual server.
6. Click the **Save** button.

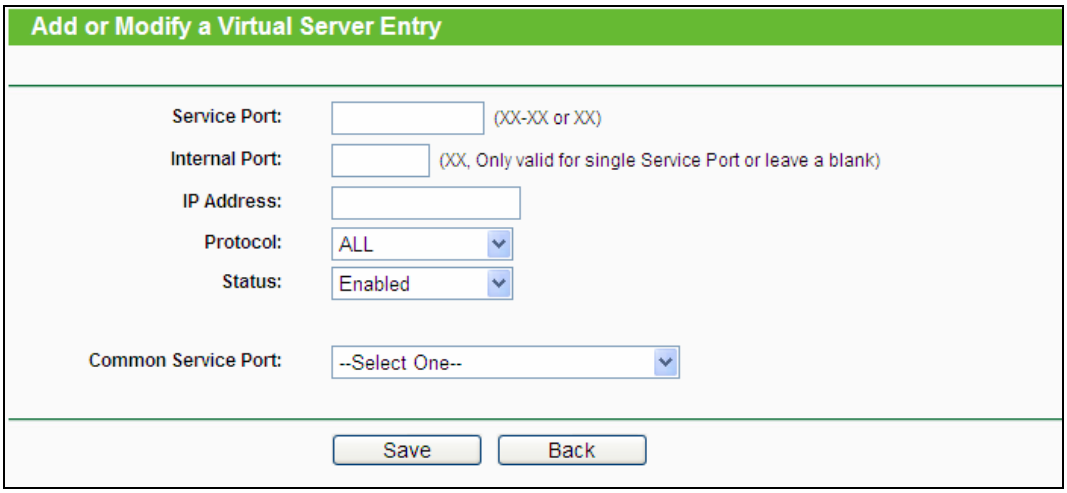


Figure 4-39 Add or Modify a Virtual Server Entry

Note:

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

To modify or delete an existing entry:

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

Click the **Enable/ Disable All** button to make all entries enabled/ disabled.
Click the **Delete All** button to delete all entries.
Click the **Next** button to go to the next page and click the **Previous** button to return the previous page.

Note:

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

4.8.2 Port Triggering

Choose menu "**Forwarding→Port Triggering**", you can view and add port triggering in the next screen (shown in Figure 4-40). Some applications require multiple connections, like Internet ames, video conferencing, Internet calling and so on. These applications cannot work with a pure NAT Router. Port Triggering is used for some of these applications that can work with an NAT Router.

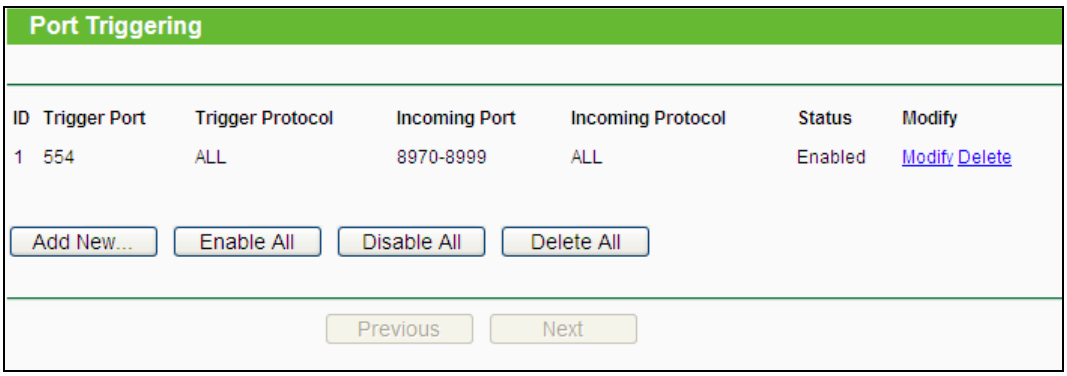


Figure 4-40 Port Triggering

Once the Router is configured, the operation is as follows:

1. A local host makes an outgoing connection using a destination port number defined in the Trigger Port field.
2. The Router records this connection, opens the incoming port or ports associated with this entry in the Port Triggering table, and associates them with the local host.
3. When necessary the external host will be able to connect to the local host using one of the ports defined in the **Incoming Ports** field.

- **Trigger Port -** The port for outgoing traffic. An outgoing connection using this port will "Trigger" this rule.
- **Trigger Protocol -** The protocol used for Trigger Ports, either **TCP**, **UDP**, or **All** (all protocols supported by the Router).
- **Incoming Port -** The port or port range used by the remote system when it responds to the outgoing request. A response using one of these ports will be forwarded to the PC that triggered this rule. You can input at most 5 groups of ports (or port section). Every group of ports must be set apart with ",". For example, 2000-2038, 2050-2051, 2085, 3010-3030.
- **Incoming Protocol -** The protocol used for Incoming Ports Range, either **TCP** or **UDP,** or **ALL** (all protocols supported by the Router).
- **Status -** The status of this entry either **Enabled** or **Disabled**.

To add a new rule, follow the steps below.

1. Click the **Add New…** button, the next screen will pop-up as shown in Figure 4-41.
2. Select a common application from the **Common Applications** drop-down list, then the **Trigger Port** field and the **Incoming Ports** field will be automatically filled. If the **Common Applications** do not have the application you need, enter the **Trigger Port** and the **Incoming Ports** manually.
3. Select the protocol used for Trigger Port from the **Trigger Protocol** drop-down list, either **TCP**, **UDP**, or **All**.
4. Select the protocol used for Incoming Ports from the **Incoming Protocol** drop-down list, either **TCP** or **UDP**, or **All.**
5. Select **Enable** in **Status** field.

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

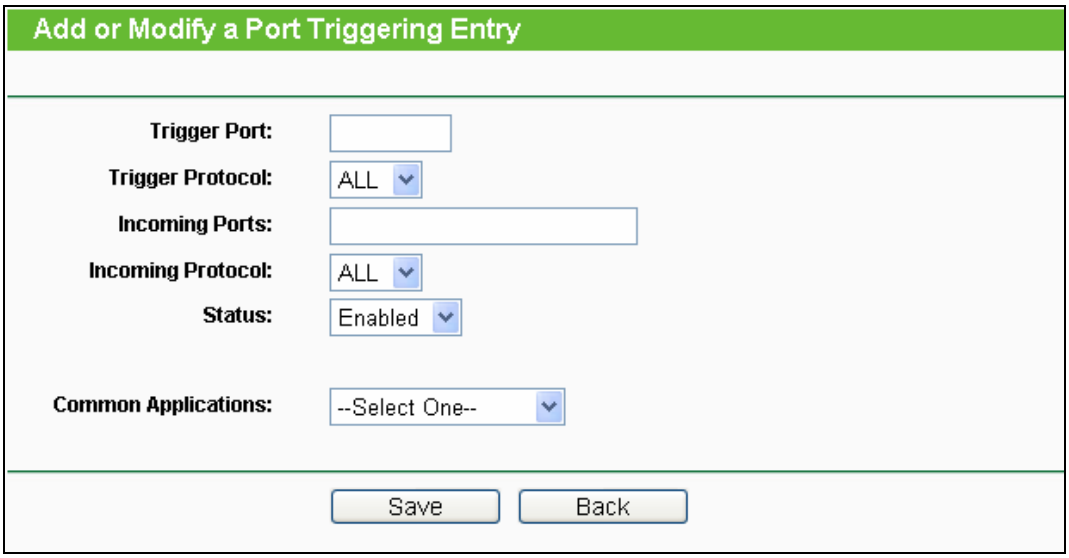


Figure 4-41 Add or Modify a Triggering Entry

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 **Disable All** button to make all entries disabled.

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

Note:

1) When the trigger connection is released, the according opening ports will be closed.
2) Each rule allowed to be used only by one host on LAN synchronously. The trigger connection of other hosts on LAN will be refused.
3) Incoming Port Range cannot overlap each other.

4.8.3 DMZ

Choose menu "**Forwarding→DMZ**", you can view and configure DMZ host in the screen (shown in Figure 4-42).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 be changed when using the DHCP function.

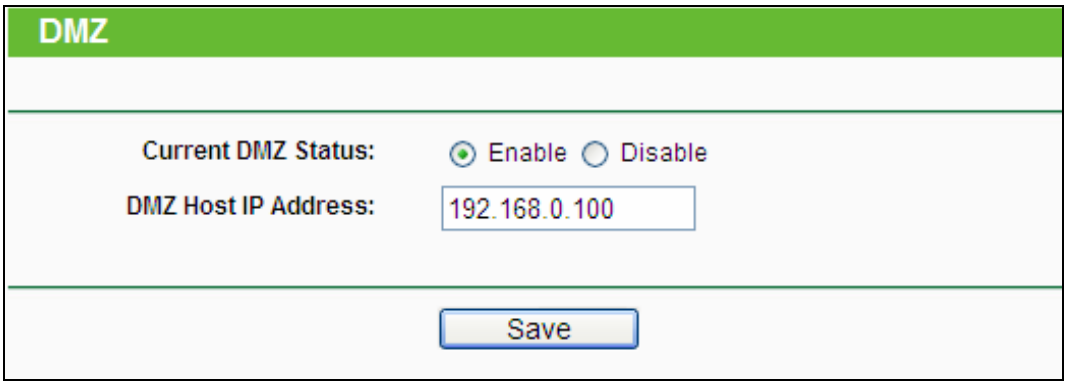


Figure 4-42 DMZ

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

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

Note:

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

4.8.4 UPnP

Choose menu "**Forwarding→UPnP**", you can view the information about **UPnP**(Universal Plug and Play) in the screen (shown in Figure 4-43).The UPnP feature allows the devices, such as Internet computers, to access the local host resources or devices as needed. UPnP devices can be automatically discovered by the UPnP service application on the LAN.

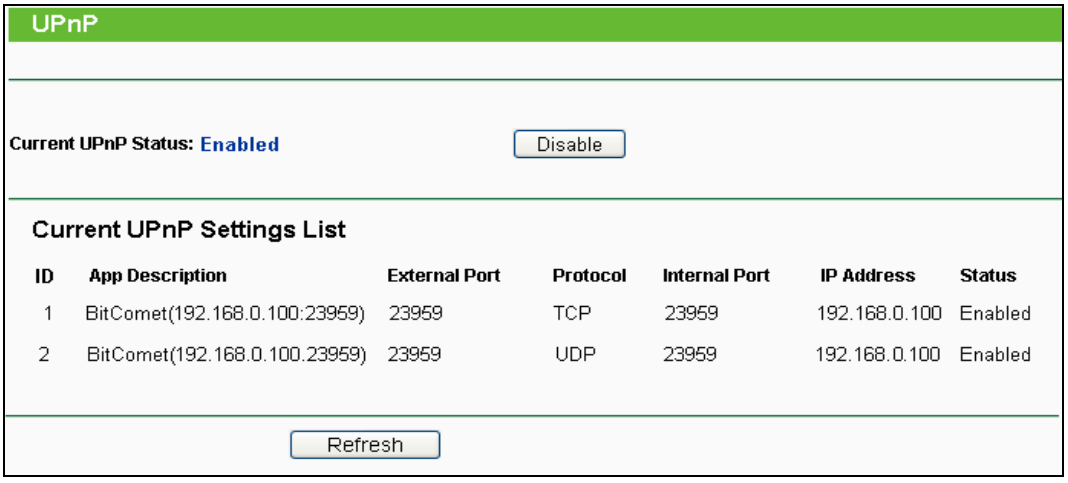


Figure 4-43 UPnP Setting

- **Current UPnP Status -** UPnP can be enabled or disabled by clicking the **Enable** or **Disable** button. As allowing this may present a risk to security, this feature is enabled by default.
- **Current UPnP Settings List -** This table displays the current UPnP information.

- **App Description -**The description provided by the application in the UPnP request
- **External Port -** External port, which the router opened for the application.
- **Protocol -** Shows which type of protocol is opened.
- **Internal Port -** Internal port, which the router opened for local host.
- **IP Address -** The UPnP device that is currently accessing the router.
- **Status -** The port's status displayed here. "Enabled" means that port is still active. Otherwise, the port is inactive.

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

4.9 Security

Figure 4-44 The Security menu

There are four submenus under the Security menu as shown in Figure 4-44: **Basic Security**, **Advanced Security**, **Local Management** and **Remote Management.** Click any of them, and you will be able to configure the corresponding function.

4.9.1 Basic Security

Choose menu "**Security → Basic Security**", you can configure the basic security in the screen as shown in Figure 4-45.

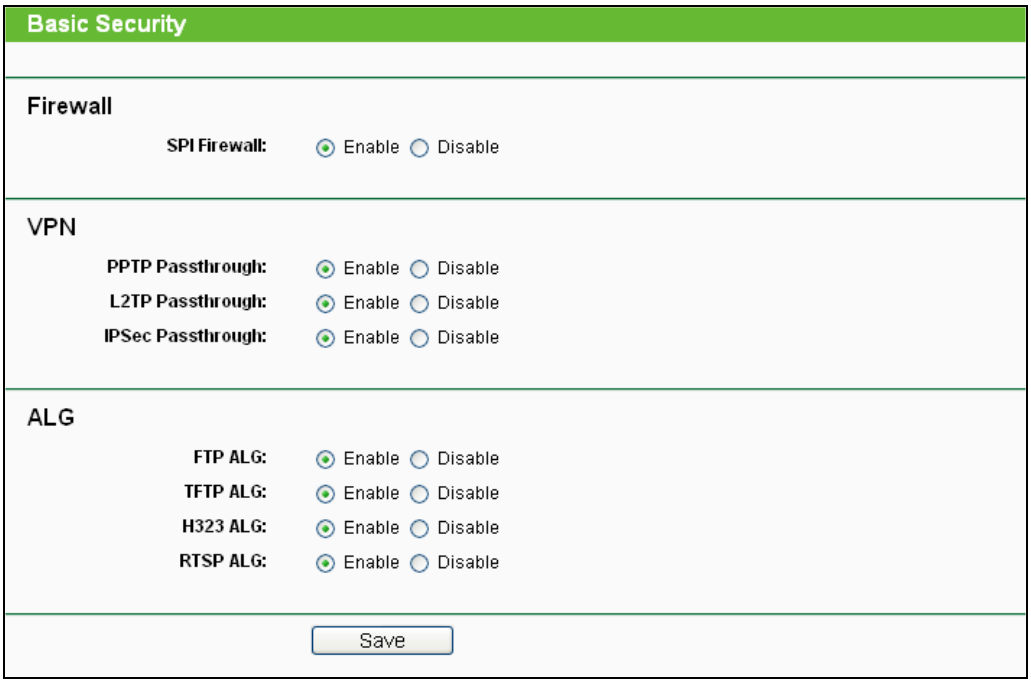


Figure 4-45 Basic Security

- **Firewall -** A firewall protects your network from the outside world. Here you can enable or disable the Router's firewall.
  - **SPI Firewall -** SPI (Stateful Packet Inspection, also known as dynamic packet filtering) 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 IPSec, PPTP, or L2TP protocols to pass through the Router's firewall.
  - **PPTP Passthrough -** Point-to-Point Tunneling Protocol (PPTP) allows the Point-to-Point Protocol (PPP) to be tunneled through an IP network. To allow PPTP tunnels to pass through the Router, keep the default, **Enable**.
  - **L2TP Passthrough -** Layer 2 Tunneling Protocol (L2TP) is the method used to enable Point-to-Point sessions via the Internet on the Layer 2 level. To allow L2TP tunnels to pass through the Router, keep the default, **Enable**.
  - **IPSec Passthrough -** Internet Protocol Security (IPSec) is a suite of protocols for ensuring private, secure communications over Internet Protocol (IP) networks, through the use of cryptographic security services. To allow IPSec tunnels to pass through the Router, keep the default, **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, RTSP etc.
  - **FTP ALG -** Select **Enable**, to allow FTP servers to operate properly.
  - **TFTP ALG -** Select **Enable**, to allow TFTP servers to operate properly.
  - **H323 ALG -** Select **Enable**, to allow H323 services to operate properly.
  - **RTSP ALG -** Select **Enable**, to allow RTSP services to operate properly.

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

4.9.2 Advanced Security

Choose menu "**Security → Advanced Security**", you can protect the Router from being attacked by TCP-SYN Flood, UDP Flood and ICMP-Flood in the screen as shown in Figure 4-46.

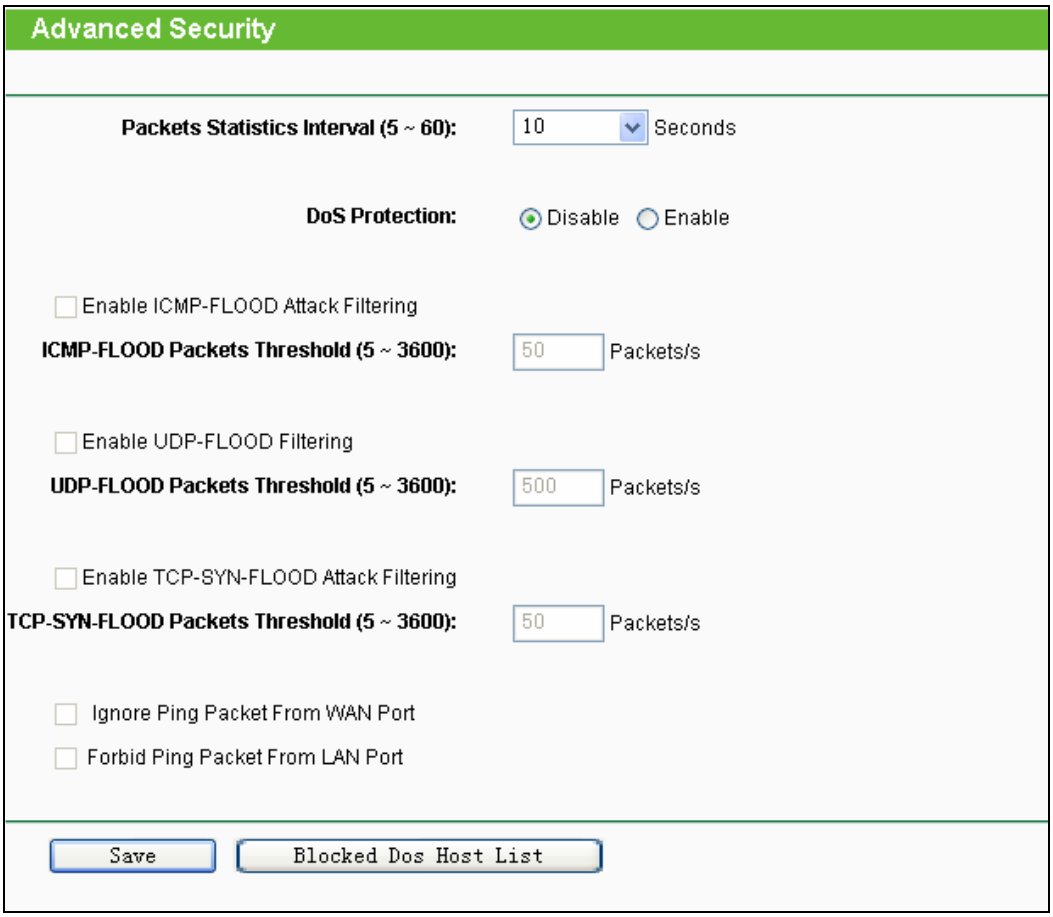


Figure 4-46 Advanced Security

- **Packets Statistics Interval (5~60) -** The default value is 10. Select a value between 5 and 60 seconds from the drop-down list. The Packets Statistics Interval value indicates the time section of the packets statistics. The result of the statistics is used for analysis by SYN Flood, UDP Flood and ICMP-Flood.
- **DoS Protection -** Denial of Service protection. Check the Enable or Disable button to 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 Router will startup 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 Router will startup 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 Router will startup 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 the Internet cannot access the Router.
- **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 Router. This function can be used to 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.

4.9.3 Local Management

Choose menu "**Security → Local Management**", you can configure the management rule in the screen as shown in Figure 4-47. The management feature allows you to deny computers in LAN from accessing the Router.

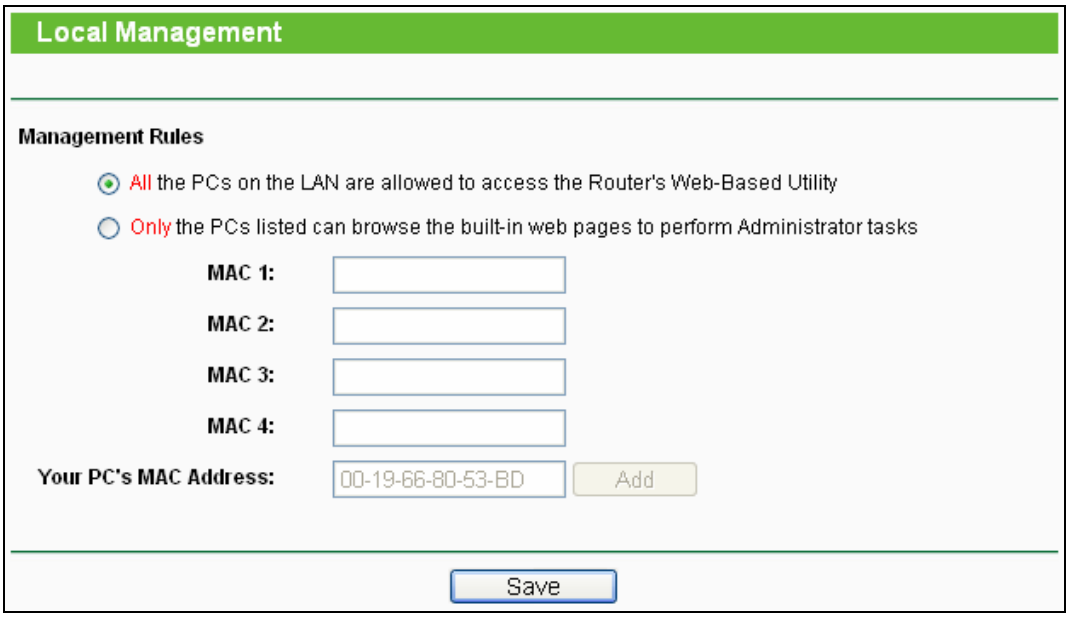


Figure 4-47 Local Management

By default, the radio button "**All the PCs on the LAN are allowed to access the Router's Web-Based Utility**" is checked. If you want to allow PCs with specific MAC Addresses to access the Setup page of the Router's Web-Based Utility locally from inside the network, check 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 MAC address listed can use the password to browse the built-in web pages to perform Administrator tasks while all the others will be blocked.

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

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

Note:

If your PC is blocked but you want to access the Router again, press and hold the **Reset Button** on the front panel for at least 10 seconds to reset the Router's factory defaults on the Router's Web-Based Utility.

4.9.4 Remote Management

Choose menu "**Security → Remote Management**", you can configure the Remote Management function in the screen as shown in Figure 4-48. This feature allows you to manage your Router from a remote location via the Internet.

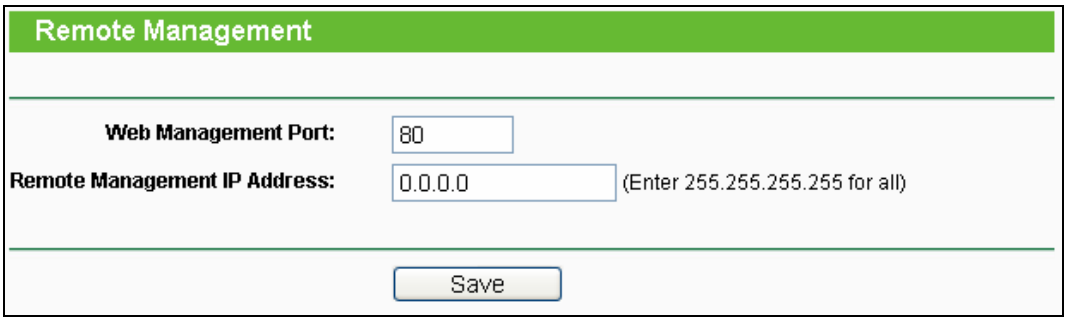


Figure 4-48 Remote Management

- **Web Management Port -** Web browser access normally uses the standard HTTP service port 80. This Router's default remote management web port number is 80. For greater security, you can change the remote management web port to a custom port by entering that number in the box provided. Choose a number between 1 and 65534 but do not use the number of any common service port.
- **Remote Management IP Address -** This is the current address you will use when accessing your Router from the Internet. This function is disabled when the IP address is set to the default value of 0.0.0.0. To enable this function change 0.0.0.0 to a valid IP address. If set to 255.255.255.255, then all the hosts can access the Router from internet.

Note:

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

2) Be sure to change the Router's default password to a very secure password.

4.10 Parental Control

Choose menu "**Parental Control**", and you can configure the parental control in the screen as shown in Figure 4-49. The Parental Control function can be used to control the internet activities of the child, limit the child to access certain websites and restrict the time of surfing.

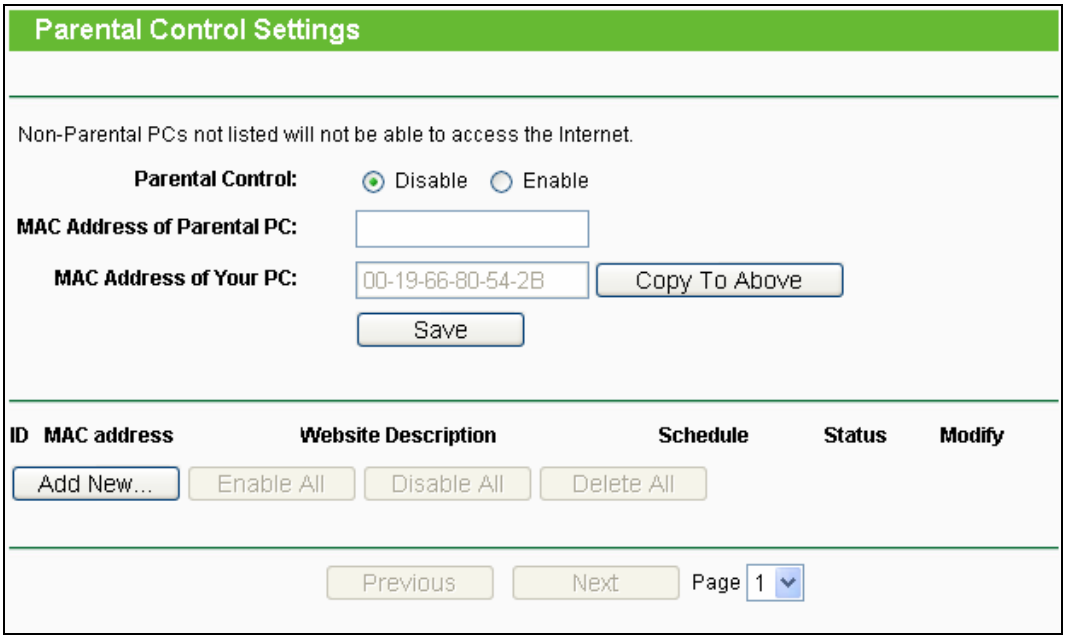


Figure 4-49 Parental Control Settings

- **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 Router. 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.

To add a new entry, please follow the steps below.

1. Click the **Add New…** button and the next screen will pop-up as shown in Figure 4-50.
2. Enter the MAC address of the PC (e.g. 00-11-22-33-44-AA) you'd like to control in the MAC Address of Child PC field. Or you can choose the MAC address from the All Address in Current LAN drop-down list.
3. Give a description (e.g. Allow Google) for the website allowed to be accessed in the Website Description field.

4. Enter the allowed domain name of the website, either the full name or the keywords (e.g. google) in the Allowed Domain Name field. Any domain name with keywords in it (www.google.com, www.google.com.hk) will be allowed.
5. Select from the Effective Time drop-down list the schedule (e.g. Schedule_1) you want the entry to take effect. If there are not suitable schedules for you, click the **Schedule** in red below to go to the Advance Schedule Settings page and create the schedule you need.
6. In the Status field, you can select **Enabled** or **Disabled** to enable or disable your entry.
7. Click the **Save** button.

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, or click the **Previous** button return to the previous page.

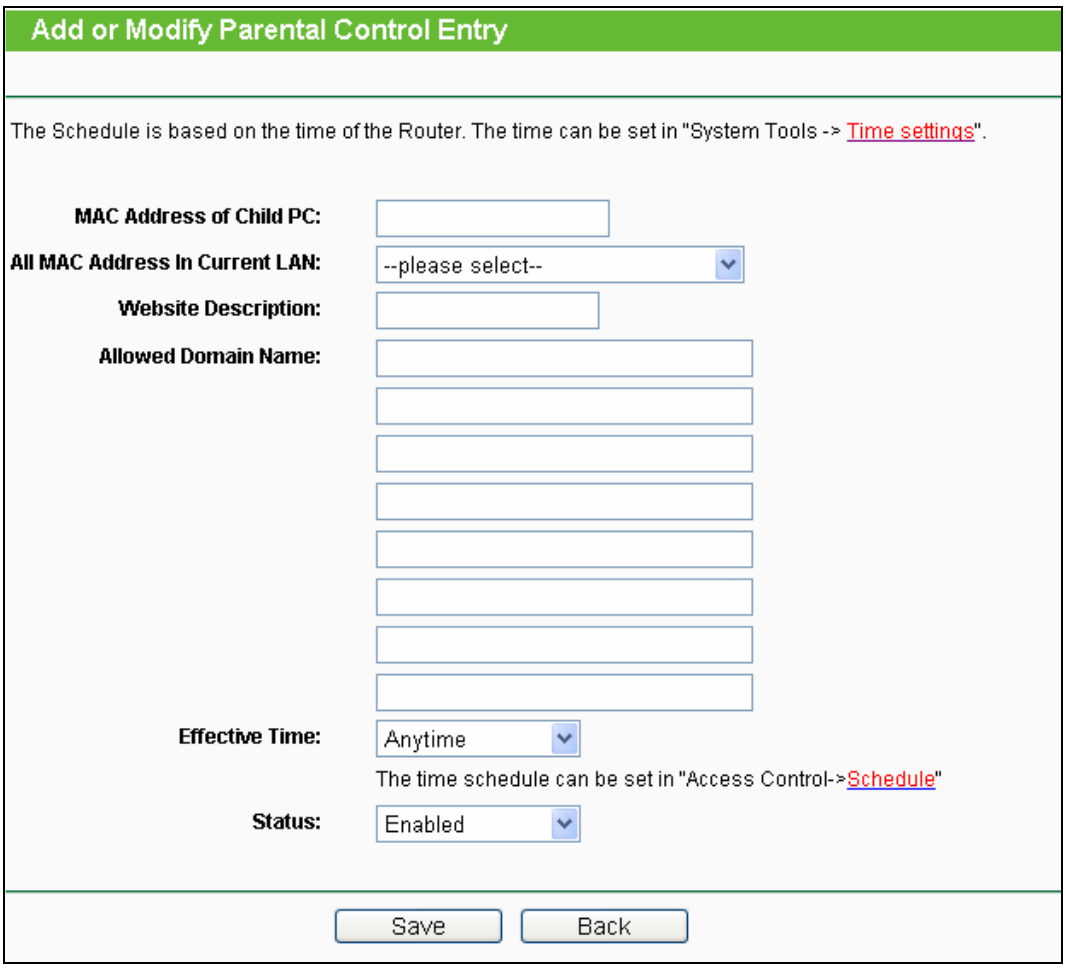


Figure 4-50 Add or Modify Parental Control Entry

For example: If you desire that the child 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 Add or Modify Parental Control Entry page:

   - Click **Add New...** button.
   - Enter 00-11-22-33-44-AA in the **MAC Address of Child PC** field.
   - Enter “Allow Google” in the **Website Description** field.
   - Enter “www.google.com” in the **Allowed Domain Name** field.
   - Select “Schedule_1” you create just now from the **Effective Time** drop-down list.
   - In **Status** field, select Enable.

4. Click **Save** to complete the settings.

   Then you will go back to the Parental Control Settings page and see the following list, as shown in Figure 4-51.

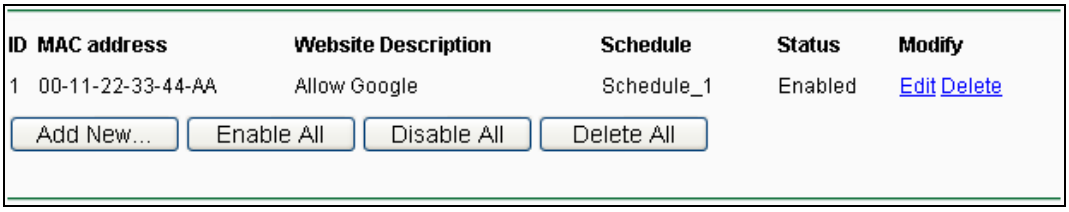


Figure 4-51 Parental Control Settings

4.11 Access Control

Figure 4-52 Access Control

There are four submenus under the Access Control menu as shown in Figure 4-52: **Rule**, **Host**, **Target** and **Schedule**. Click any of them, and you will be able to configure the corresponding function.

4.11.1 Rule

Choose menu “**Access Control** → **Rule**”, and then you can view and set Access Control rules in the screen as shown in Figure 5-47.

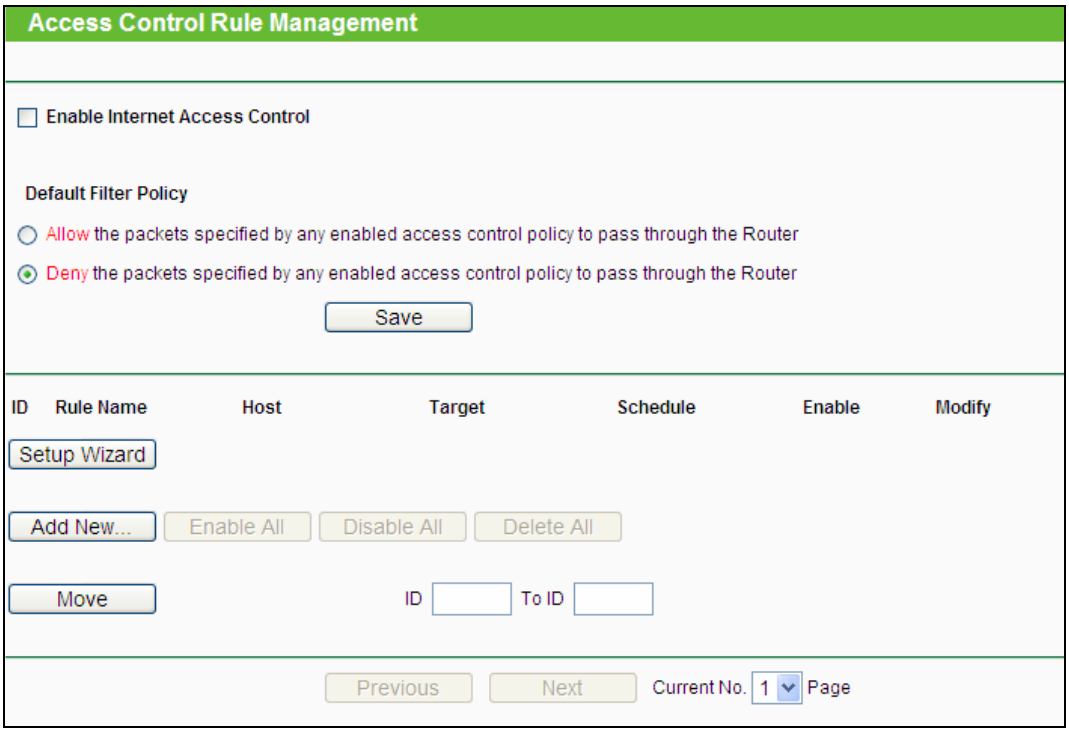


Figure 4-53 Access Control Rule Management

- **Enable Internet Access Control -** Select the check box to enable the Internet Access Control function, so 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.
- **Enable -** Here displays the status of the rule, enabled or not. Check this option to enable a specific entry.
- **Modify -** Here you can edit or delete an existing rule.
- **Setup Wizard -** Click the **Setup Wizard** button to create a new rule entry.
- **Add New... -** Click the **Add New...** button to add a new rule entry.
- **Enable All -** Click the **Enable All** button to enable all the rules in the list.
- **Disable All -** Click the **Disable All** button to disable all the rules in the list.
- **Delete All -** Click the **Delete All** button to delete all the entries in the table.
- **Move -** You can change the entry's order as desired. Enter in the first box the ID number of the entry you want to move and in the second box another ID number, and then click the **Move** button to change the entries' order.
- **Next -** Click the **Next** button to go to the next page.
- **Previous -** Click the **Previous** button to return to the previous page.

There are two methods to add a new rule.

Method One:

1. Click **Setup Wizard** button and the next screen will appear as shown in Figure 4-54.

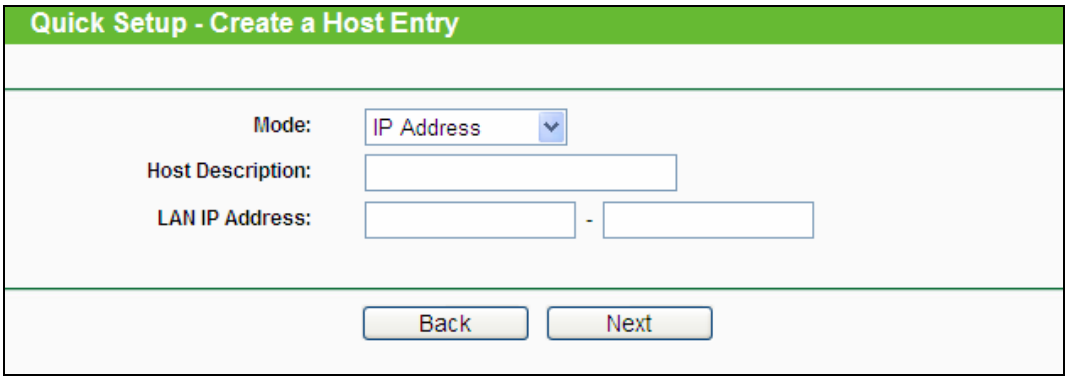


Figure 4-54 Quick Setup – Create a Host Entry

- **Host Description** - In this field, create a unique description for the host (e.g. Host_1).
- **Mode** - Here are two options, **IP Address** and **MAC Address**. You can select either of them from the drop-down list.

If the **IP Address** is selected, you can see the following item:

- **LAN IP Address** - Enter the IP address or address range of the host in dotted-decimal format (e.g. 192.168.0.23).

If the MAC Address is selected, you can see the following item:

- **MAC Address** - Enter the MAC address of the host in XX-XX-XX-XX-XX-XX format (e.g. 00-11-22-33-44-AA).

2. Click **Next** when finishing creating the host entry, and the next screen will appear as shown in Figure 4-55.

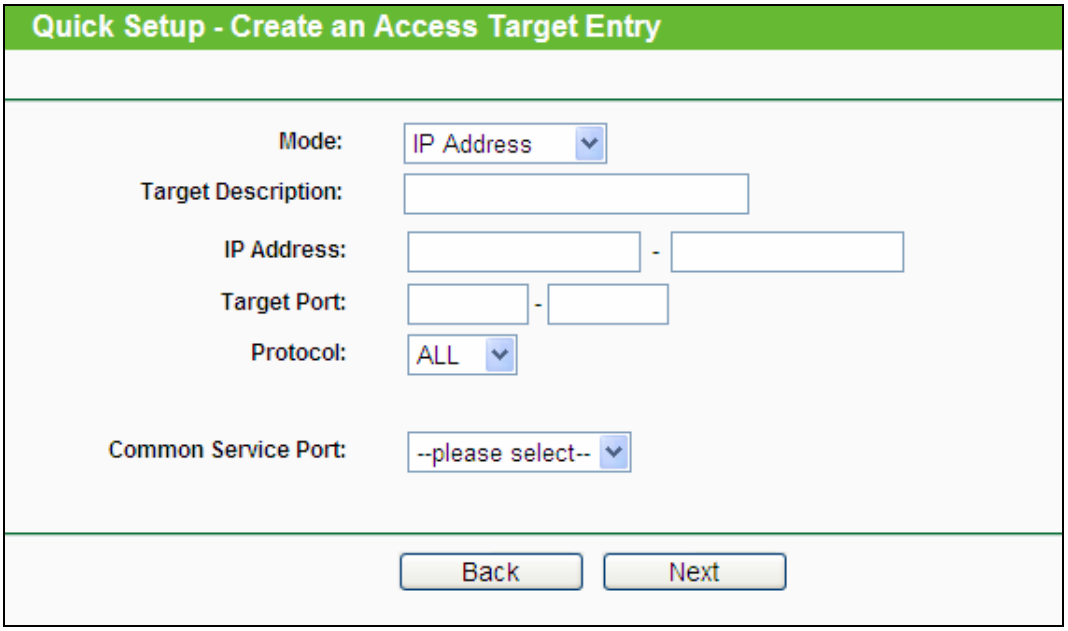


Figure 4-55 Quick Setup – Create an Access Target Entry

- **Target Description** - In this field, create a description for the target. Note that this description should be unique (e.g. Target_1).
- **Mode** - Here are two options, IP Address and Domain Name. You can choose either of them from the drop-down list.

If the **IP Address** is selected, you will see the following items:

- **IP Address** - Enter the IP address (or address range) of the target (targets) in dotted-decimal format (e.g. 192.168.0.23).
- **Target Port** - Specify the port or port range for the target. For some common service ports, you can make use of the Common Service Port item below.
- **Protocol** - Here are four options, All, TCP, UDP, and ICMP. Select one of them from the drop-down list for the target.
- **Common Service Port** - Here lists some common service ports. Select one from the drop-down list, and the corresponding port number will be filled in the Target Port field automatically. For example, if you select "FTP", "21" will be filled in the Target Port automatically.

If the **Domain Name** is selected, you will see the following items:

- **Domain Name** - Here you can enter 4 domain names, either the full name or the keywords (for example, google). Any domain name with keywords in it (www.google.com, www.google.cn) will be blocked or allowed.

3. Click **Next** when finishing creating the access target entry, and the next screen will appear as shown in Figure 4-56.

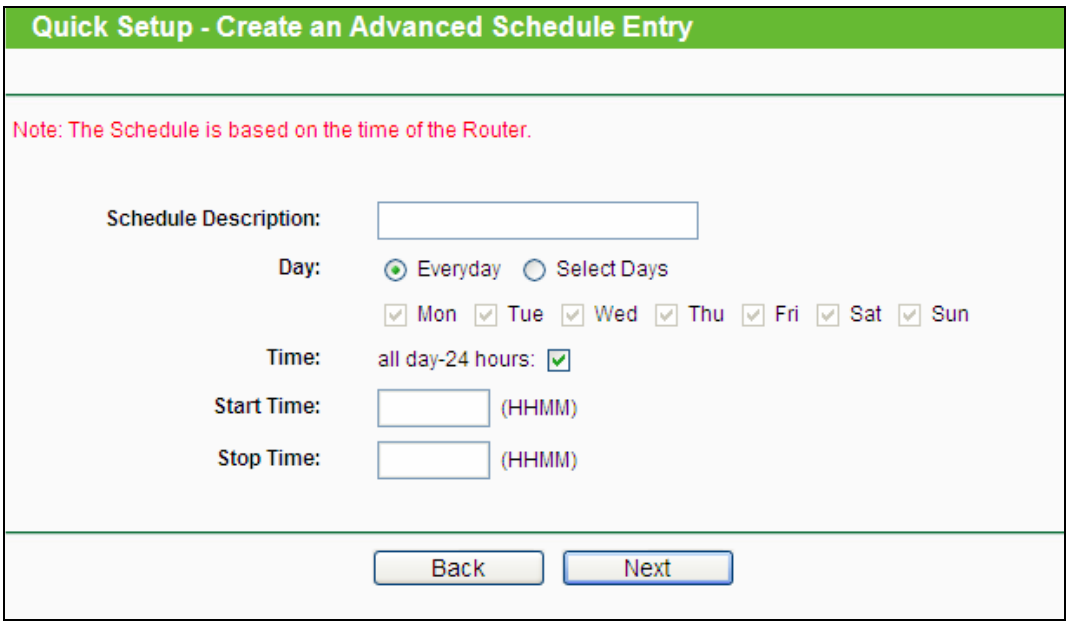


Figure 4-56 Quick Setup – Create an Advanced Schedule Entry

- **Schedule Description** - In this field, create a description for the schedule. Note that this description should be unique (e.g. Schedule_1).
- **Day** - Choose Select Days and select the certain day (days), or choose Everyday.
- **Time** - Select "24 hours", or specify the Start Time and Stop Time yourself.
- **Start Time** - Enter the start time in HHMM format (HHMM are 4 numbers). For example 0800 is 8:00.
- **Stop Time** - Enter the stop time in HHMM format (HHMM are 4 numbers). For example 2000 is 20:00.

4. Click **Next** when finishing creating the advanced schedule entry, and the next screen will appear as shown in Figure 4-57.

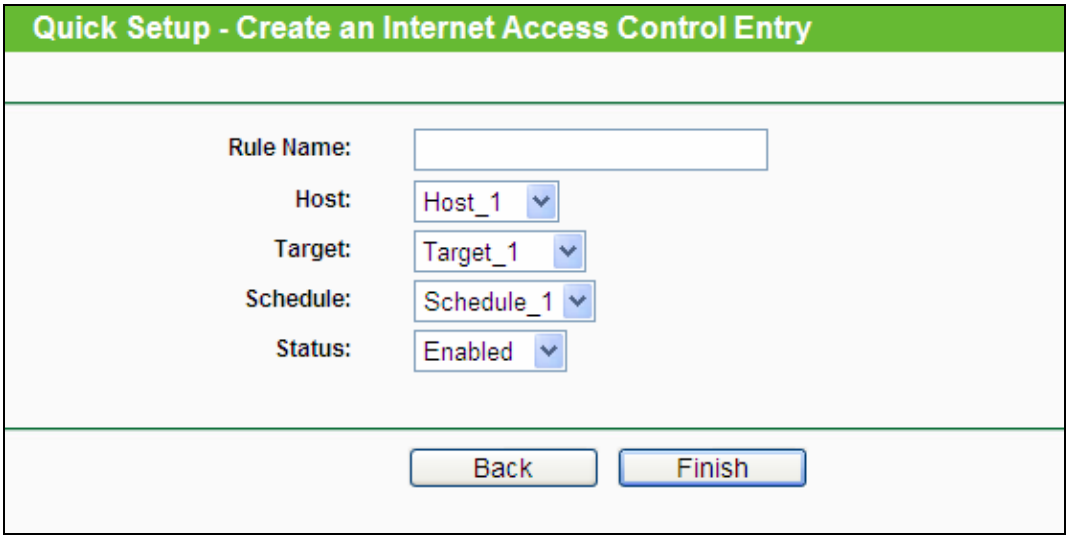


Figure 4-57 Quick Setup – Create an Internet Access Control Entry

- **Rule** - In this field, create a name for the rule. Note that this name should be unique (e.g. Rule_1).
- **Host** - In this field, select a host from the drop-down list for the rule. The default value is the **Host Description** you set just now.
- **Target** - In this filed, select a target from the drop-down list for the rule. The default value is the **Target Description** you set just now.
- **Schedule** - In this field, select a schedule from the drop-down list for the rule. The default value is the **Schedule Description** you set just now.
- **Status** - In this field, there are two options, **Enable** or **Disable**. Select **Enable** so that the rule will take effect. Select **Disable** so that the rule won't take effect.

5. Click **Finish** to complete adding a new rule.

Method Two:

1. Click the **Add New…** button and the next screen will pop up as shown in **Figure** 5-52.
2. Give a name (e.g. Rule_1) for the rule in the **Rule Name** field.
3. Select a host from the **Host** drop-down list or choose "**Click Here To Add New Host List**".
4. Select a target from the **Target** drop-sown list or choose "**Click Here To Add New Target List**".
5. Select a schedule from the **Schedule** drop-down list or choose "**Click Here To Add New Schedule**".
6. In the **Status** field, select **Enabled** or **Disabled** to enable or disable your entry.
7. Click the **Save** button.

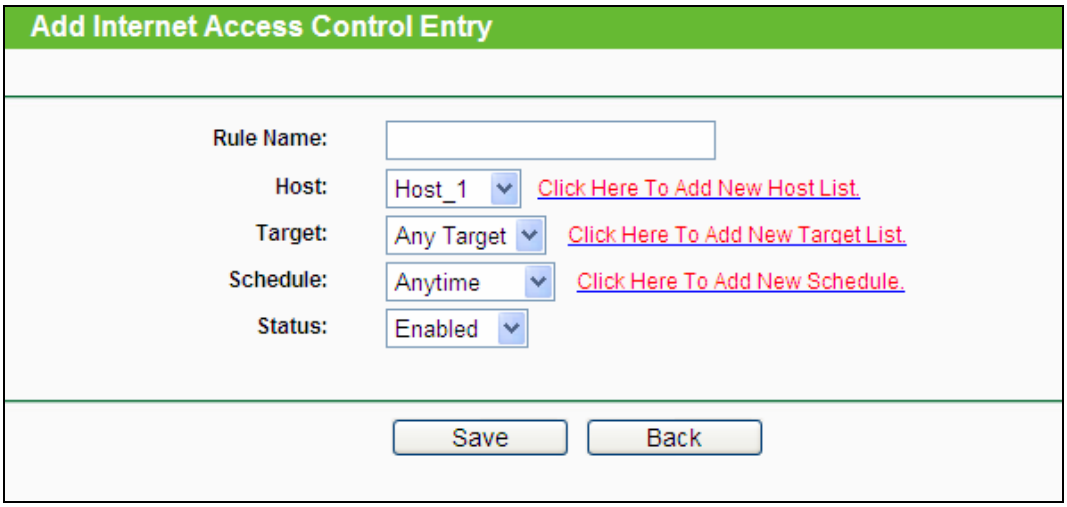


Figure 4-58 Add Internet Access Control Entry

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 Router".
2. We recommend that you click **Setup Wizard** button to finish all the following settings.
3. Click the submenu **Host of Access Control** in the left to enter the Host List page. Add a new entry with the Host Description is Host_1 and MAC Address is 00-11-22-33-44-AA.
4. Click the submenu **Target of Access Control** in the left to enter the Target List page. Add a new entry with the Target Description is Target_1 and Domain Name is www.google.com.
5. Click the submenu **Schedule of Access Control** in the left to enter the Schedule List page. Add a new entry with the Schedule Description is Schedule_1, Day is Sat and Sun, Start Time is 1800 and Stop Time is 2000.
6. Click the submenu **Rule of Access Control** in the left, Click **Add New...** button to add a new rule as follows:
   - In Rule Name field, create a name for the rule. Note that this name should be unique, for example Rule_1.
   - In Host field, select Host_1.
   - In Target field, select Target_1.
   - In Schedule field, select Schedule_1.
   - In Status field, select Enable.
   - Click Save to complete the settings.

Then you will go back to the Access Control Rule Management page and see the following list.

4.11.2 Host

Choose menu "**Access Control → Host**", you can view and set a Host list in the screen as shown in Figure 4-59. The host list is necessary for the Access Control Rule.

Figure 4-59 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.

To add a new entry, please follow the steps below.

1. Click the **Add New…** button.
2. In the **Mode** field, select IP Address or MAC Address.
   - If you select IP Address, the screen shown is Figure 4-60.
     1) In **Host Description** field, create a unique description for the host (e.g. Host_1).
     2) In **LAN IP Address** field, enter the IP address.
   - If you select MAC Address, the screen shown is Figure 4-61.
     1) In **Host Description** field, create a unique description for the host (e.g. Host_1).
     2) In **MAC Address** field, enter the MAC address.
3. Click the **Save** button to complete the settings.

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

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

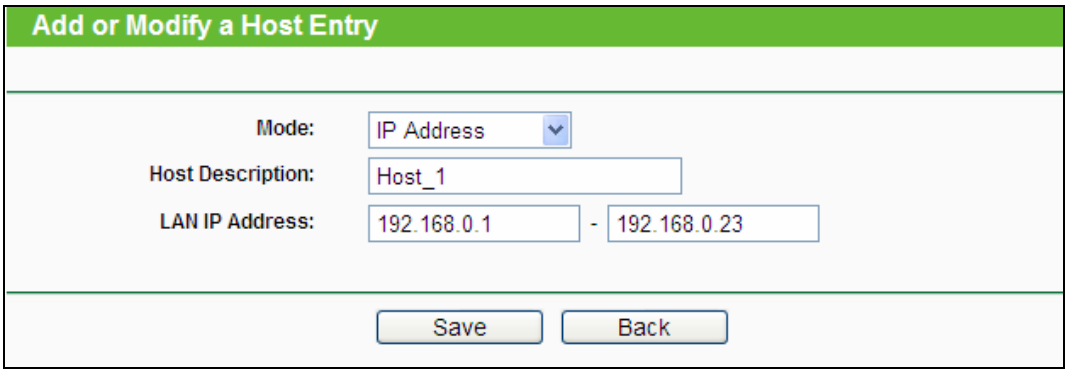


Figure 4-60 Add or Modify a Host Entry

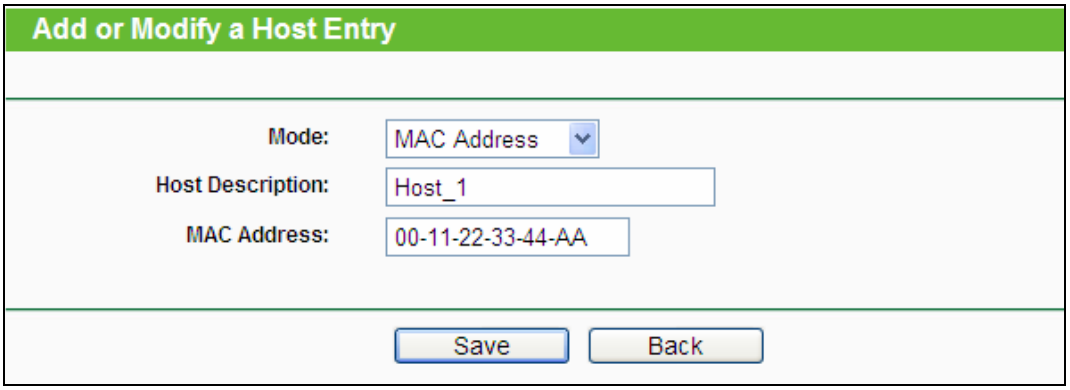


Figure 4-61 Add or Modify a Host Entry

For example: If you desire to restrict the internet activities of host with MAC address 00-11-22-33-44-AA, you should first follow the settings below:

1. Click **Add New...** button in Figure 4-59 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 Description** field, create a **unique** description for the host (e.g. Host_1).
4. In **MAC Address** field, enter 00-11-22-33-44-AA.
5. Click **Save** to complete the settings.

Then you will go back to the Host Settings page and see the following list.

ID	Host Description	Information	Modify
1	Host_1	MAC: 00-11-22-33-44-AA	Edit Delete

4.11.3 Target

Choose menu "**Access Control → Target**", you can view and set a Target list in the screen as shown in Figure 4-62. The target list is necessary for the Access Control Rule.

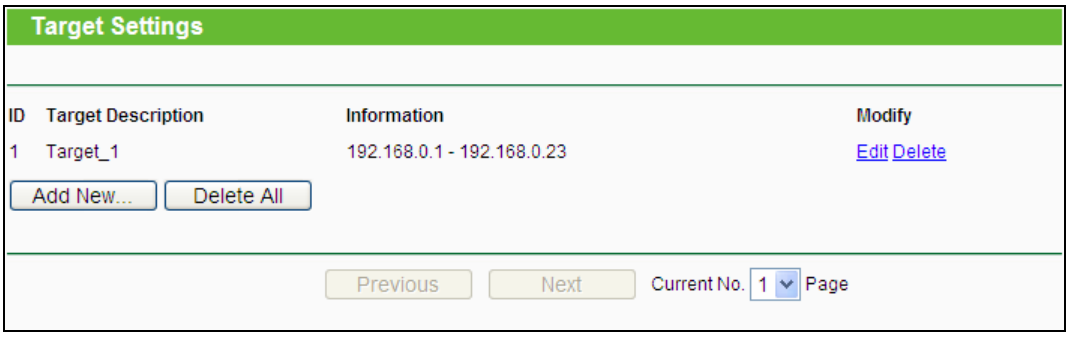


Figure 4-62 Target Settings

- **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.

To add a new entry, please follow the steps below.

1. Click the **Add New…** button.
2. In **Mode** field, select IP Address or Domain Name.
   - If you select **IP Address**, the screen shown is Figure 4-63.
     1) In **Target Description** field, create a unique description for the target (e.g. Target_1).
     2) In **IP Address** field, enter the IP address of the target.
     3) Select a common service from **Common Service Port** drop-down list, so that the **Target Port** will be automatically filled. If the **Common Service Port** drop-down list doesn't have the service you want, specify the **Target Port** manually.
     4) In **Protocol** field, select TCP, UDP, ICMP or ALL.
   - If you select **Domain Name**, the screen shown is Figure 4-64.
     1) In **Target Description** field, create a unique description for the target (e.g. Target_1).

2) In **Domain Name** field, enter the domain name, either the full name or the keywords (for example google) in the blank. Any domain name with keywords in it (www.google.com, www.google.hk) will be blocked or allowed. You can enter 4 domain names.

3. Click the **Save** button.

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

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

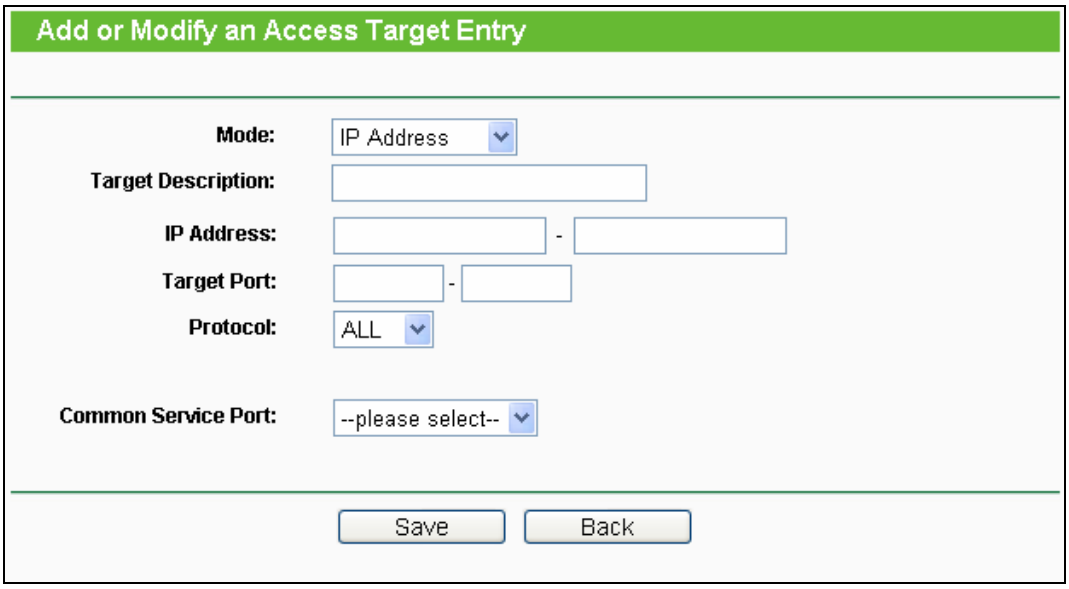


Figure 4-63 Add or Modify an Access Target Entry

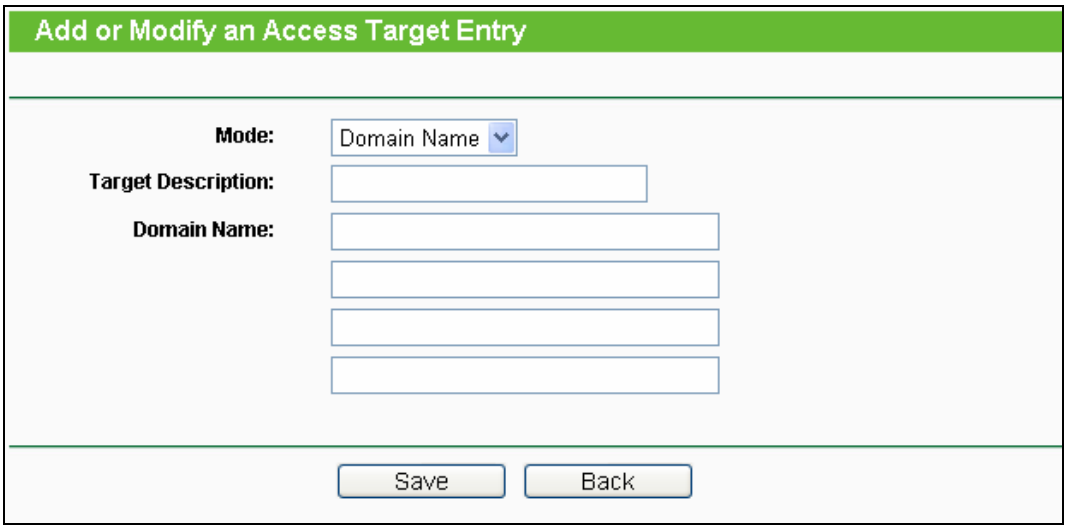


Figure 4-64 Add or Modify an Access Target Entry

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 in Figure 4-62 to enter the 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 (e.g. Target_1).
4. In **Domain Name** field, enter www.google.com.
5. Click **Save** to complete the settings.

Then you will go back to the Target Settings page and see the following list.

ID	Target Description	Information	Modify
1	Target_1	www.google.com	Edit Delete

4.11.4 Schedule

Choose menu "**Access Control → Schedule**", you can view and set a Schedule list in the next screen as shown in Figure 4-65. The Schedule list is necessary for the Access Control Rule.

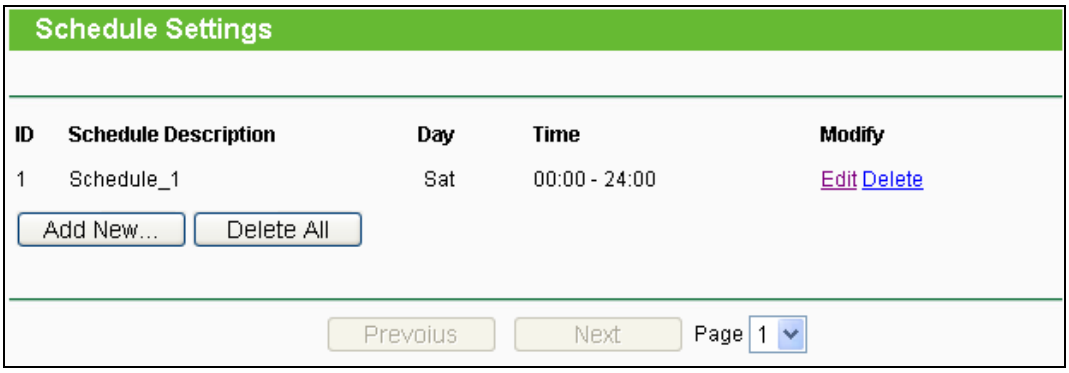


Figure 4-65 Schedule Settings

- **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.

To add a new schedule, follow the steps below.

1. Click **Add New...** button shown in Figure 4-65 and the next screen will pop-up as shown in Figure 4-66.
2. In **Schedule Description** field, create a unique description for the schedule (e.g. Schedule_1).
3. In **Day** field, select the day or days you need.
4. In **Time** field, you can select all day-24 hours or you may enter the Start Time and Stop Time in the corresponding field.
5. Click **Save** to complete the settings.

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

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

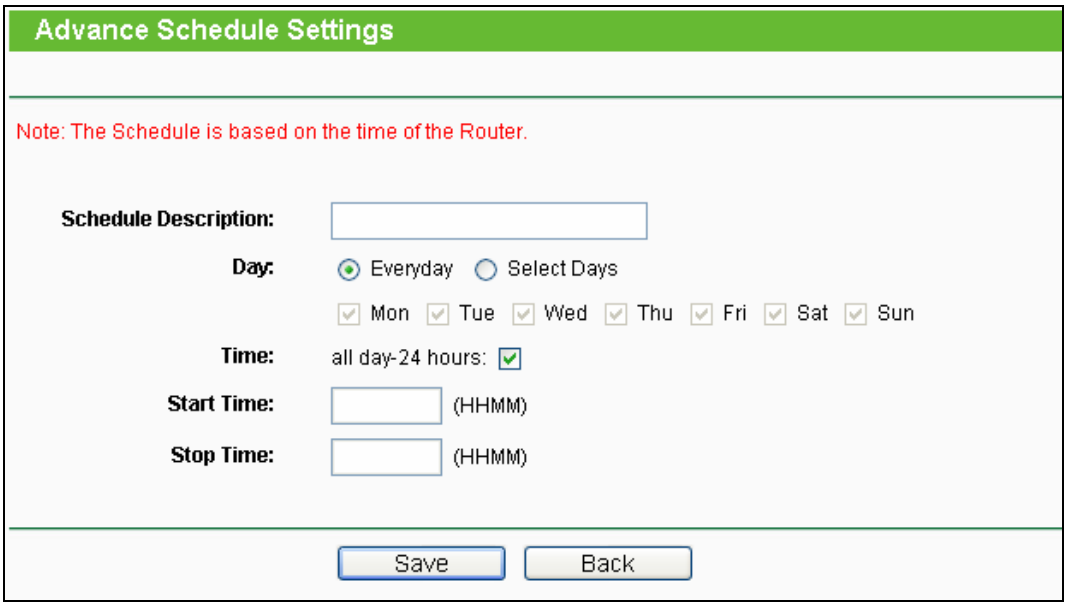


Figure 4-66 Advanced Schedule Settings

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 shown in Figure 4-65 to enter the Advanced Schedule Settings page.
2. In **Schedule Description** field, create a unique description for the schedule (e.g. Schedule_1).
3. In **Day** field, check the Select Days radio button and then select Sat and Sun.
4. In **Time** field, enter 1800 in Start Time field and 2000 in Stop Time field.
5. Click **Save** to complete the settings.

Then you will go back to the Schedule Settings page and see the following list.

ID	Schedule Description	Day	Time	Modify
1	Schedule_1	Sat Sun	18:00 - 20:00	Edit Delete

4.12 Advanced Routing

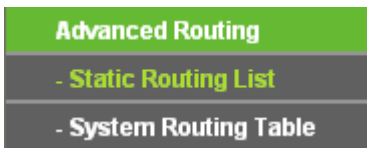


Figure 4-67 Advanced Routing

There are two submenus under the Advanced Routing menu as shown in Figure 4-67: **Static Routing List** and **System Routing Table**. Click any of them, and you will be able to configure the corresponding function.

4.12.1 Static Routing List

Choose menu "**Advanced Routing → Static Routing List**", you can configure the static route in the next screen (shown in Figure 4-68). A static route is a pre-determined path that network information must travel to reach a specific host or network.

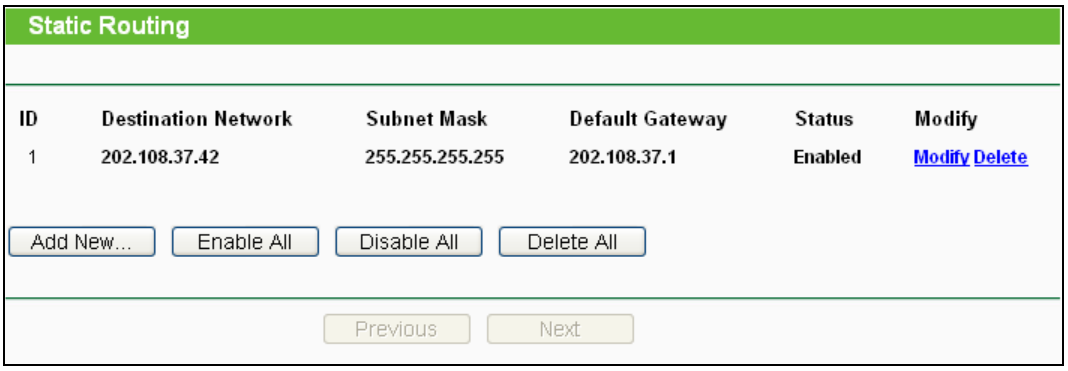


Figure 4-68 Static Routing

To add static routing entries:

1. Click **Add New…** shown in Figure 4-68, you will see the following screen.

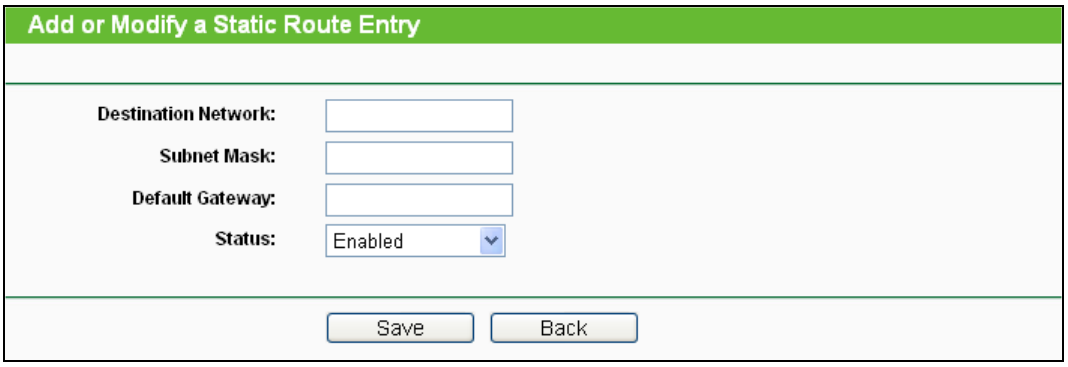


Figure 4-69 Add or Modify a Static Route Entry

2. Enter the following data:

   - **Destination Network -** The **Destination Network** is the address of the network or host that you want to assign to a static route.
   - **Subnet Mask -** The **Subnet Mask** determines which portion of an IP Address is the network portion, and which portion is the host portion.
   - **Gateway -** This is the IP Address of the gateway device that allows for contact between the Router and the network or host.

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

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

Other configurations for the entries:

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

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

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

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

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

4.12.2 System Routing Table

Choose menu "**Advanced Routing → System Routing Table**", you can configure the system routing table in the next screen (shown in Figure 4-70). System routing table views all of the valid route entries in use.

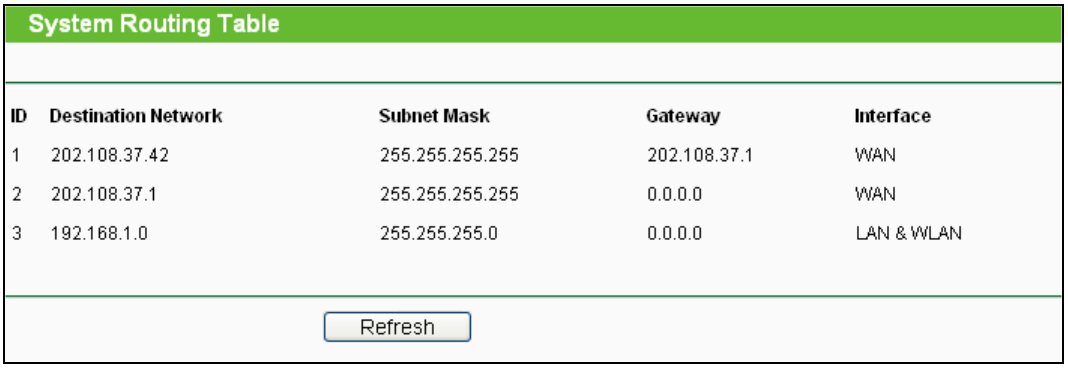


Figure 4-70 System Routing Table

- **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 Router 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).

4.13 Bandwidth Control

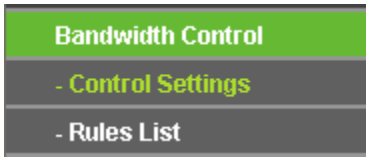


Figure 4-71 Bandwidth Control

There are two submenus under the Bandwidth Control menu as shown in Figure 4-71: **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.

4.13.1 Control Settings

Choose menu "**Bandwidth Control → Control Settings**", you can configure the Egress Bandwidth and Ingress Bandwidth in the next screen. Their values you configure should be less than 100000Kbps. For optimal control of the bandwidth, please select the right Line Type and ask your ISP for the total bandwidth of the egress and ingress.

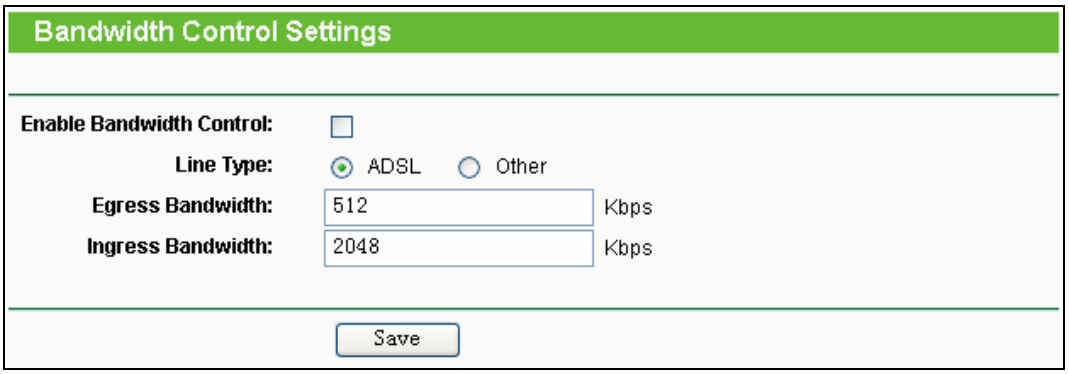


Figure 4-72 Bandwidth Control Settings

- **Enable Bandwidth Control -** Check this box so that the Bandwidth Control settings can take effect.
- **Line Type -** Select the right type for you network connection. If you don't know how to choose, please ask your ISP for the information.
- **Egress Bandwidth** - The upload speed through the WAN port.
- **Ingress Bandwidth -** The download speed through the WAN port.

4.13.2 Rules List

Choose menu "**Bandwidth Control → Rules List**", you can view and configure the Bandwidth Control rules in the Figure 4-73.

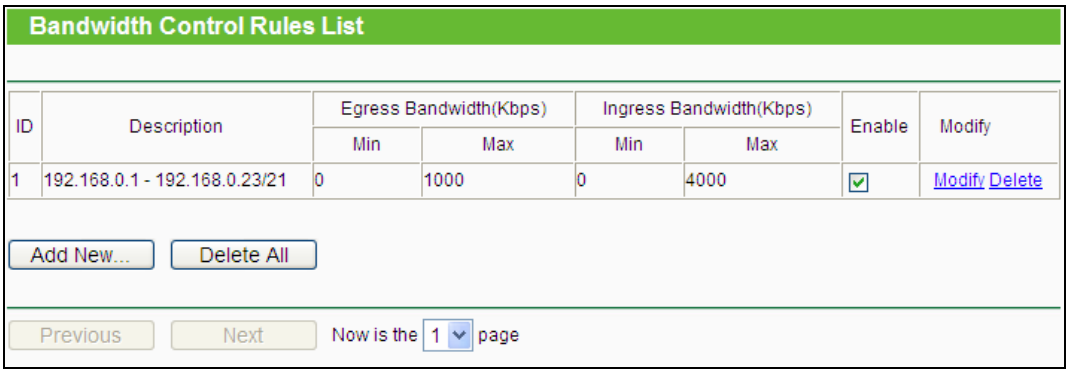


Figure 4-73 Bandwidth Control Rules List

- **Description -** This is the information about the rules such as address range.

- **Egress bandwidth -** This field displays the max and mix upload bandwidth through the WAN port. The default is 0.
- **Ingress bandwidth -** This field displays the max and mix download bandwidth through the WAN port. The default is 0.
- **Enable -** This displays the status of the rule.
- **Modify -** Click **Modify** to edit the rule. Click **Delete** to delete the rule.

To add a Bandwidth Control rule, follow the steps below.

Step 1: Click **Add New…** shown in Figure 4-73, you will see a new screen shown in Figure 4-74.

Step 2: Enter the information like the screen shown below.

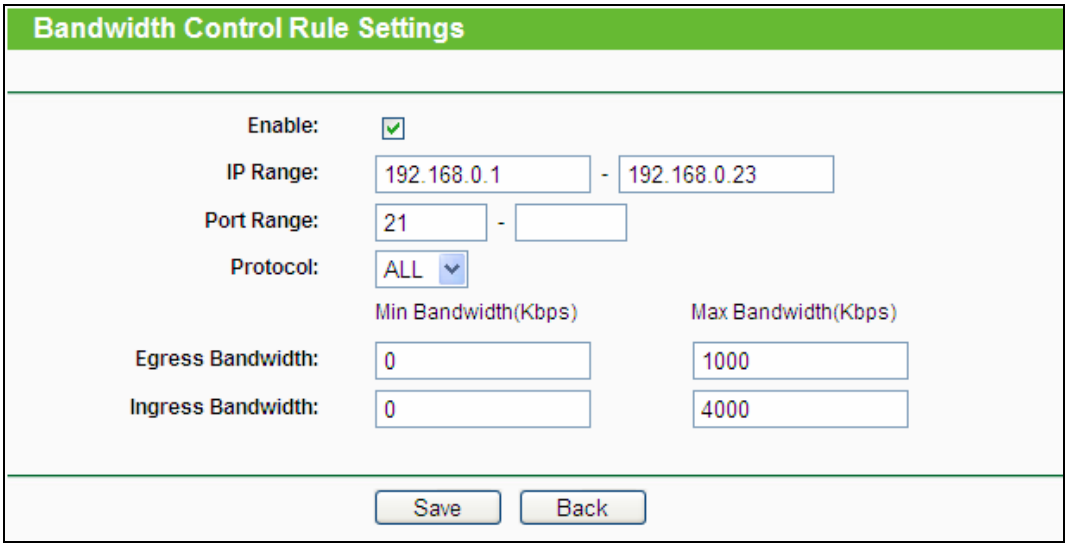


Figure 4-74 Bandwidth Control Rule Settings

Step 3: Click the **Save** button.

4.14 IP & MAC Binding

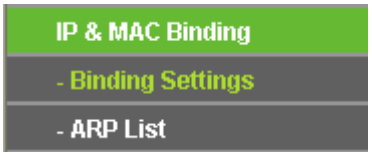


Figure 4-75 the IP & MAC Binding menu

There are two submenus under the IP &MAC Binding menu (shown in Figure 4-75): **Binding Settings** and **ARP List**. Click any of them, and you will be able to scan or configure the corresponding function. The detailed explanations for each submenu are provided below.

4.14.1 Binding Settings

This page displays the **Binding Settings** table; you can operate it in accord with your desire shown in Figure 4-76).

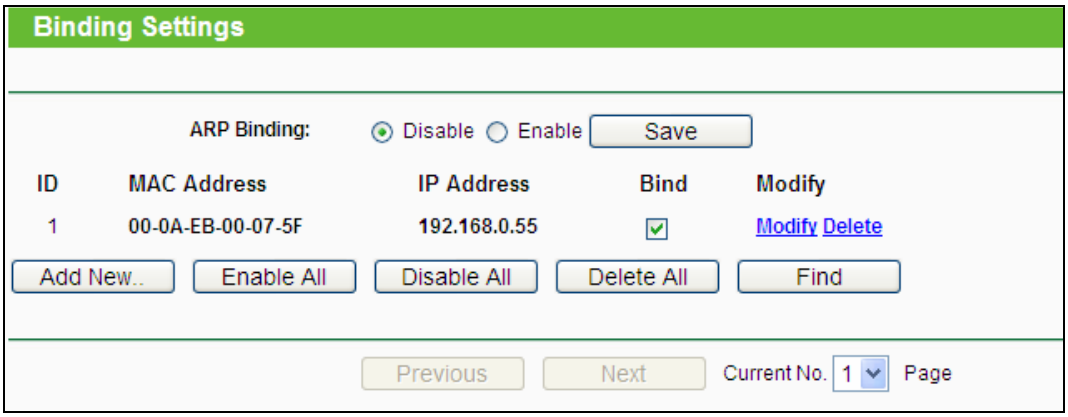


Figure 4-76 Binding Settings

- **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 4-77).

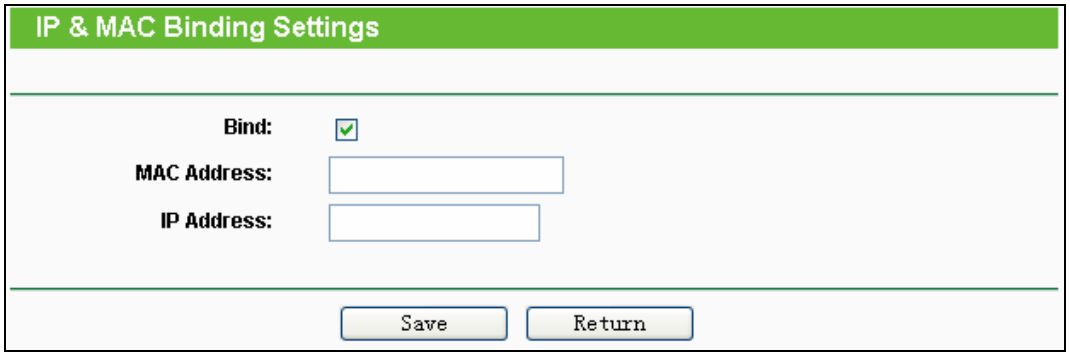


Figure 4-77 IP & MAC Binding Setting (Add & Modify)

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

1. Click the **Add New...** button as shown in Figure 4-76.
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 4-76.

2. Enter the MAC Address or IP Address.
3. Click the **Find** button in the page as shown in Figure 4-78.

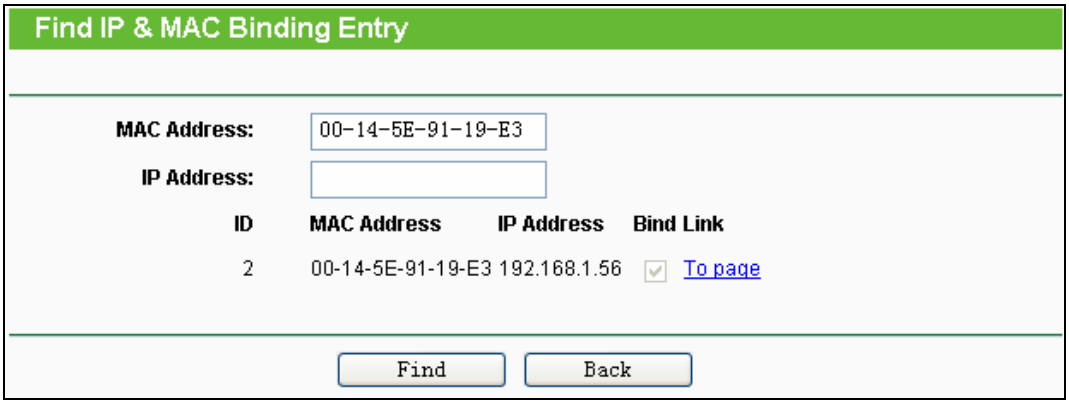


Figure 4-78 Find IP & MAC Binding Entry

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

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

4.14.2 ARP List

To manage the computer, you could 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 4-79).

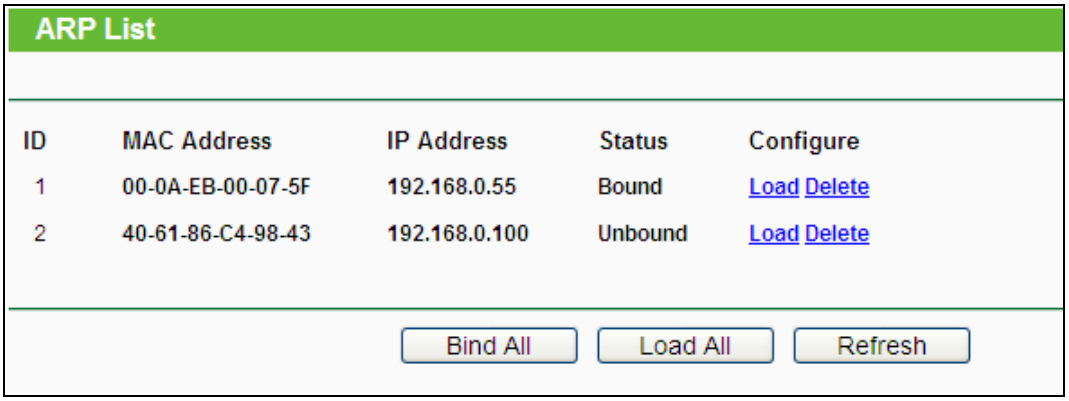


Figure 4-79 ARP List

- **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.

4.15 Dynamic DNS

Choose menu "**Dynamic DNS**", and you can configure the Dynamic DNS function.

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

4.15.1 Comexe.cn DDNS

If the dynamic DNS **Service Provider** you select is www.comexe.cn, the page will appear as shown in Figure 4-80.

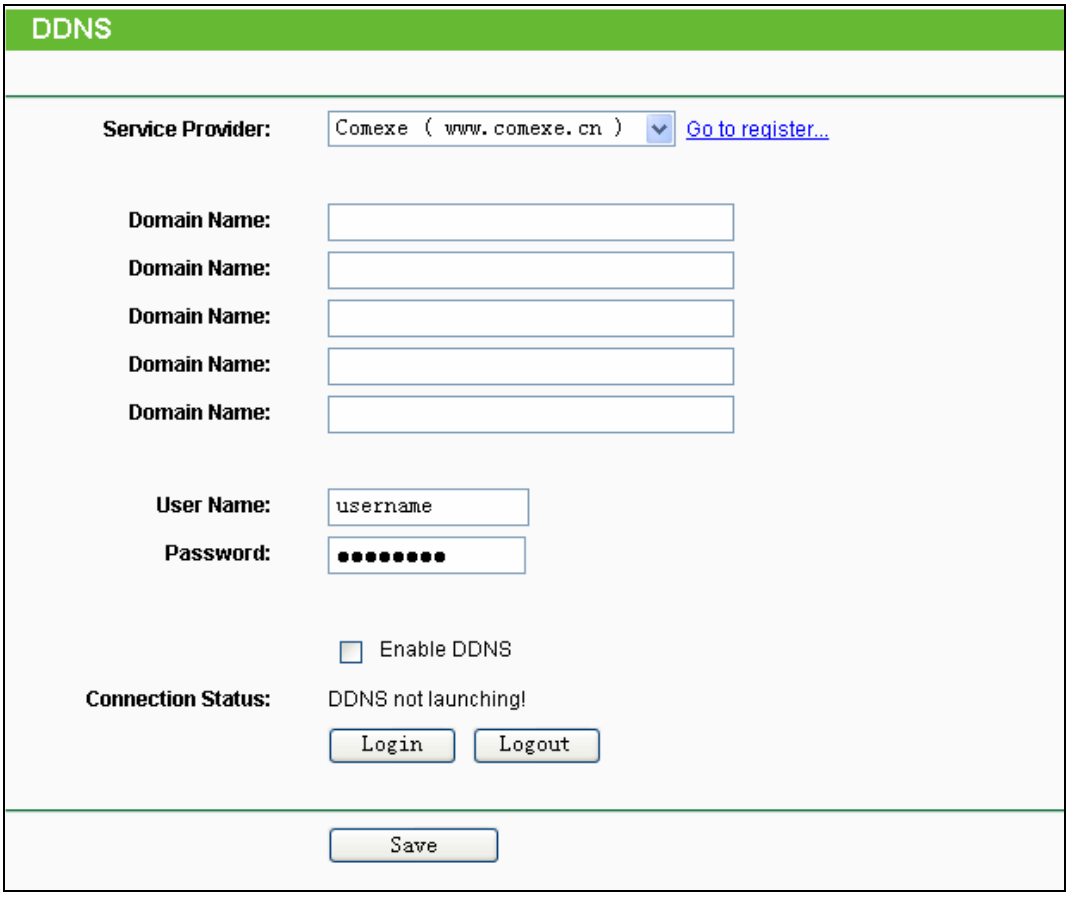


Figure 4-80 Comexe.cn DDNS Settings

To set up for DDNS, follow these instructions:

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

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

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

4.15.2 Dyndns.org DDNS

If the dynamic DNS **Service Provider** you select is www.dyndns.org, the page will appear as shown in Figure 4-81.

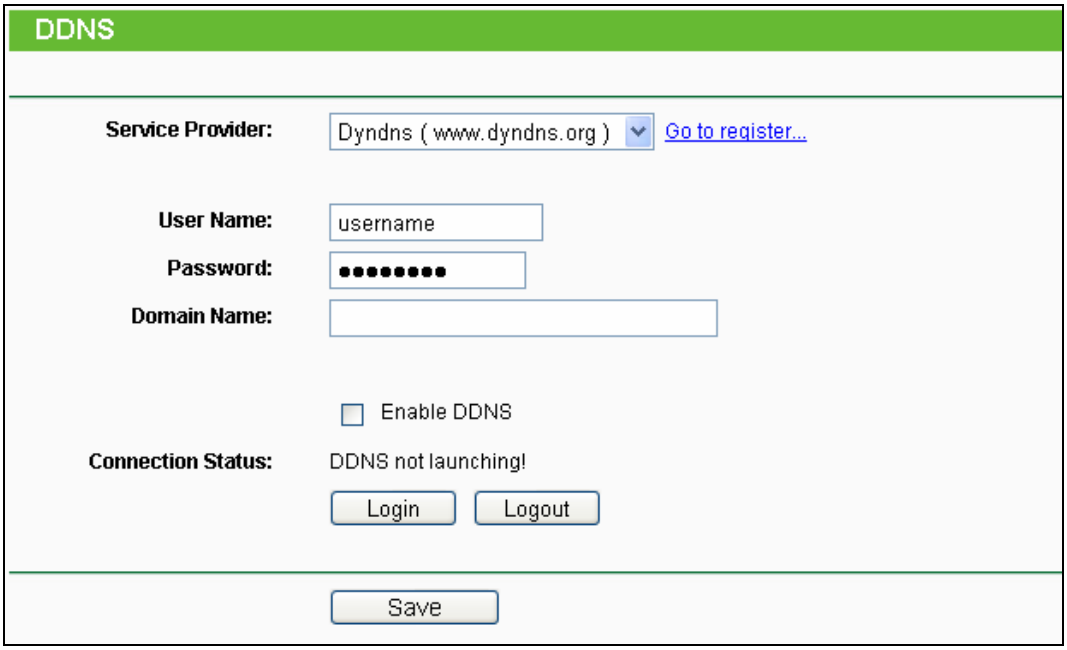


Figure 4-81 Dyndns.org DDNS Settings

To set up for DDNS, follow these instructions:

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

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

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

4.15.3 No-ip.com DDNS

If the dynamic DNS **Service Provider** you select is www.no-ip.com, the page will appear as shown in Figure 4-82.

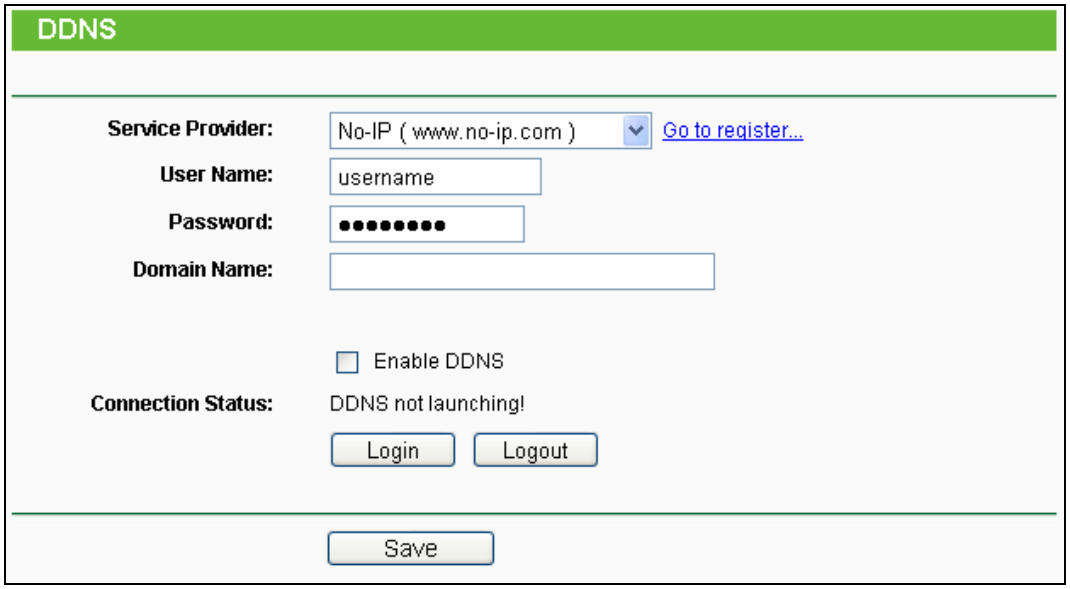


Figure 4-82 No-ip.com DDNS Settings

To set up for DDNS, follow these instructions:

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

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

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

4.16 System Tools

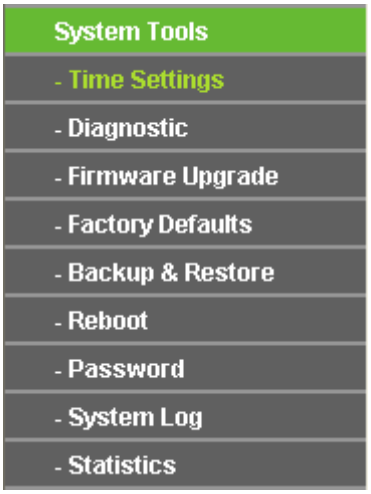


Figure 4-83 The System Tools menu

Choose menu "**System Tools**", and you can see the submenus under the main menu: **Time Settings**, **Diagnostic**, **Firmware Upgrade**, **Factory Defaults, Backup & Restore, Reboot,**

Password, System Log and **Statistics.** Click any of them, and you will be able to configure the corresponding function. The detailed explanations for each submenu are provided below.

4.16.1 Time Settings

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

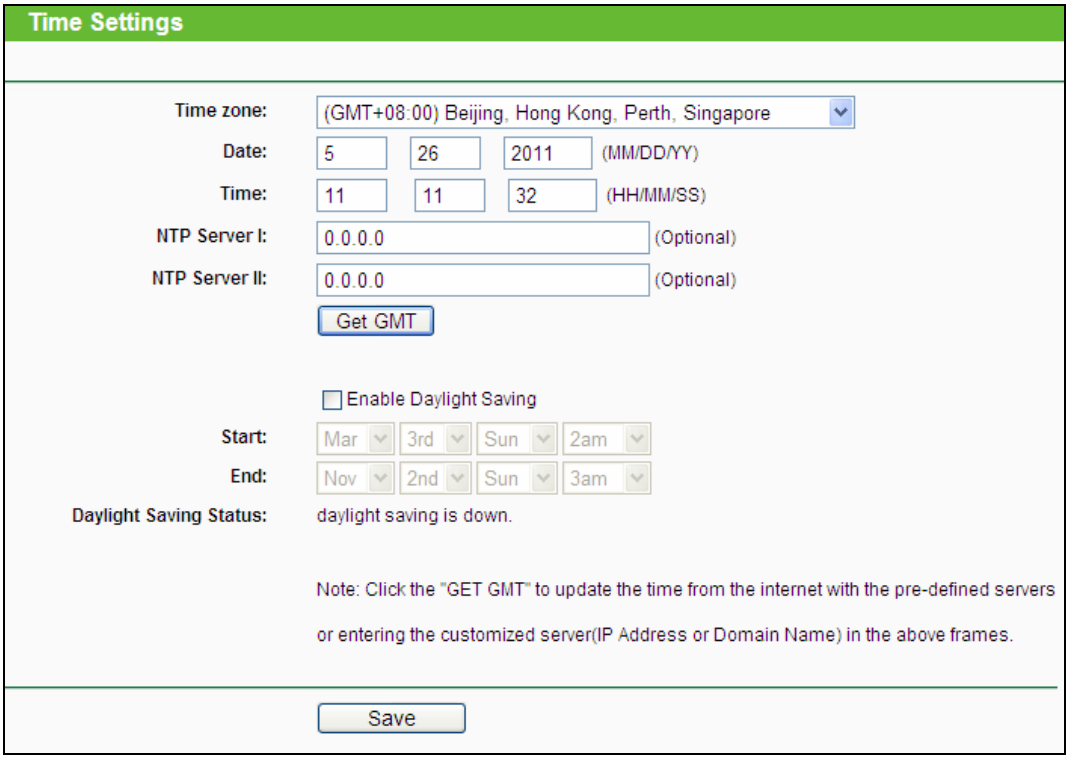


Figure 4-84 Time settings

- **Time Zone -** Select your local time zone from this pull down list.
- **Date -** Enter your local date in MM/DD/YY into the right blanks.
- **Time -** Enter your local time in HH/MM/SS into the right blanks.
- **NTP Server I / NTP Server II -** Enter the address or domain of the **NTP Server I** or **NTP Server II**, and then the Router will get the time from the NTP Server preferentially. In addition, the Router built-in some common NTP Servers, so it can get time automatically once it connects the Internet.
- **Enable Daylight Saving -** Check the box to enable the Daylight Saving function.
- **Start -** The time to start the Daylight Saving. Select the month in the first field, the week in the second field, the day in the third field and the time in the last field.
- **End -** The time to end the Daylight Saving. Select the month in the first field, the week in the second field, the day in the third field and the time in the last field.
- **Daylight Saving Status -** Displays the status whether the Daylight Saving is in use.

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**.

To set time automatically:

1. Select your local time zone.
2. Enter the address or domain of the **NTP Server I** or **NTP Server II**.
3. Click the **Get GMT** button to get system time from Internet if you have connected to the Internet.

To set Daylight Saving:

1. Check the box to enable Daylight Saving.
2. Select the start time from the drop-down lists in the **Start** field.
3. Select the end time from the drop-down lists in the **End** field.
4. Click the **Save** button to save the settings.

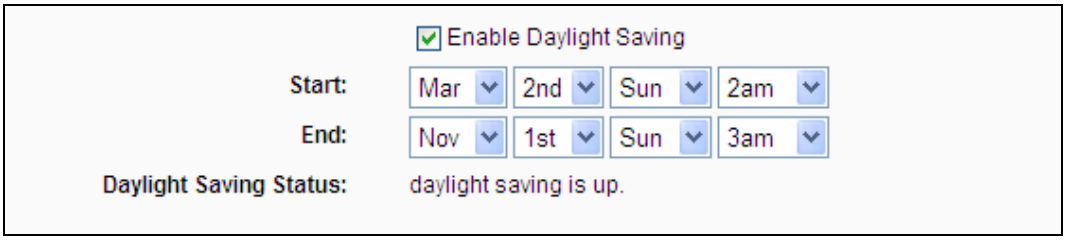


Figure 4-85 Time settings

Note:

1) This setting will be used for some time-based functions such as firewall. You must specify your time zone once you login to the router successfully, otherwise, these functions will not take effect.
2) The time will be lost if the router is turned off.
3) The Router will automatically obtain GMT from the Internet if it is configured accordingly.
4) The Daylight Saving will take effect one minute after the configurations are completed.

4.16.2 Diagnostic

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

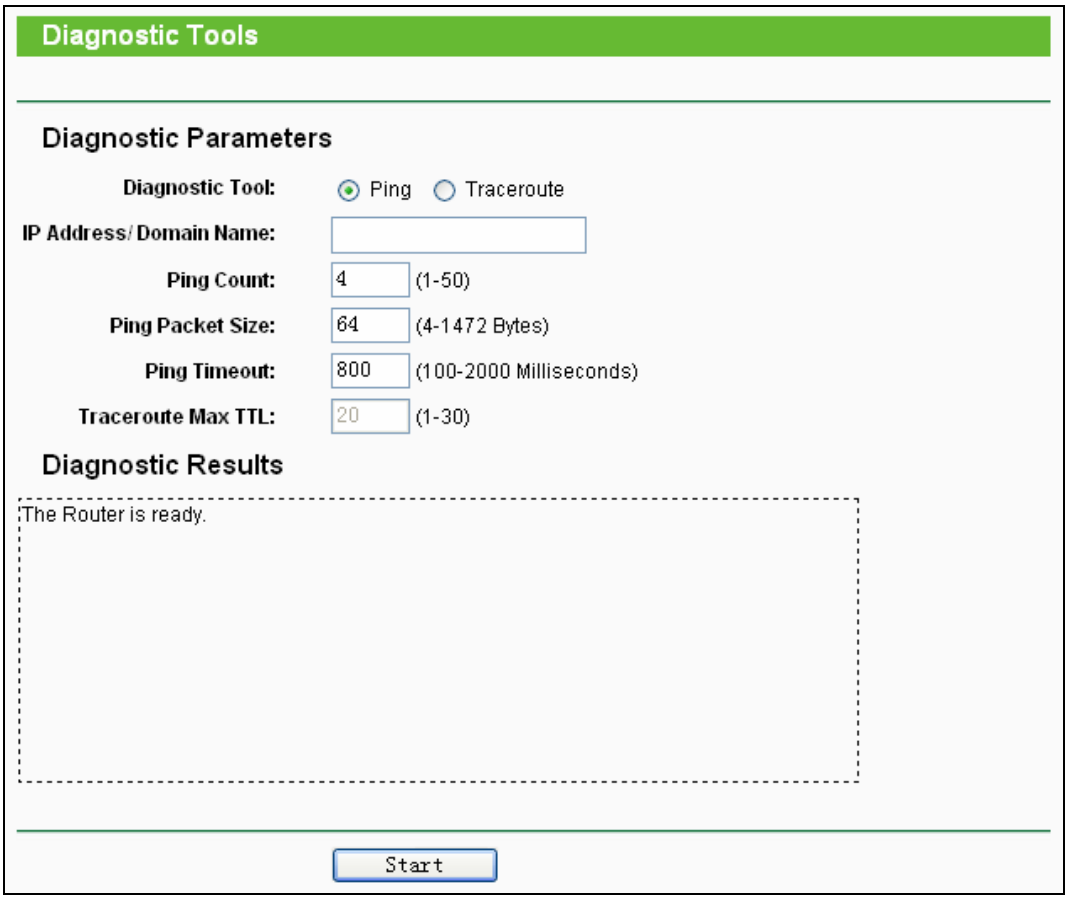


Figure 4-86 Diagnostic Tools

- **Diagnostic Tool -** Check the radio button to select one diagnostic too.
  - **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 - Type the destination IP address (such as 202.108.22.5) or Domain name (such as http://www.tp-link.com)

- **Pings Count -** The number of Ping packets for a Ping connection.
- **Ping Packet Size -** The size of Ping packet.
- **Ping Timeout -** Set the waiting time for the reply of each Ping packet. If there is no reply in the specified time, the connection is overtime.
- **Traceroute Max TTL -** The max number of hops for a Traceroute connection.

Click **Start** to check the connectivity of the Internet.

The **Diagnostic Results** page displays the result of diagnosis.

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

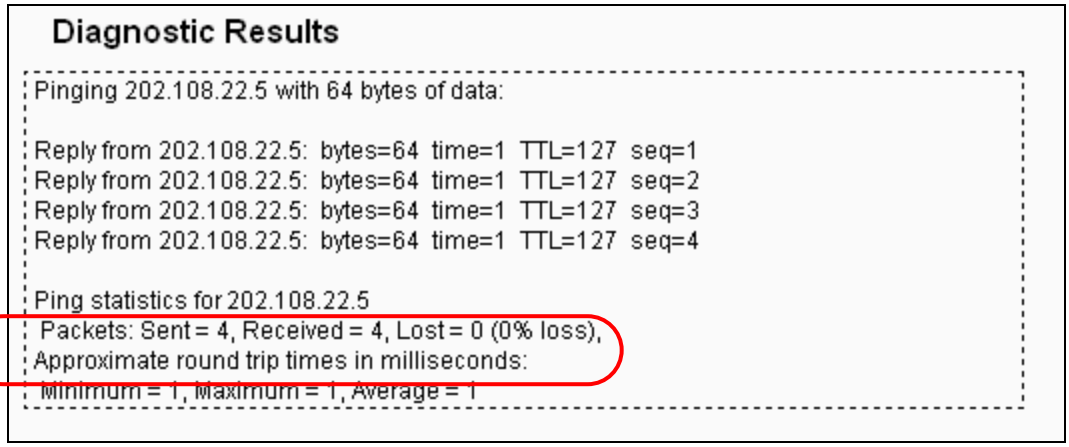


Figure 4-87 Diagnostic Results

Note:

Only one user can use this tool at one time. Options “Number of Pings”, “Ping Size” and “Ping Timeout” are used for **Ping** function. Option “Tracert Hops” are used for **Tracert** function.

4.16.3 Firmware Upgrade

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

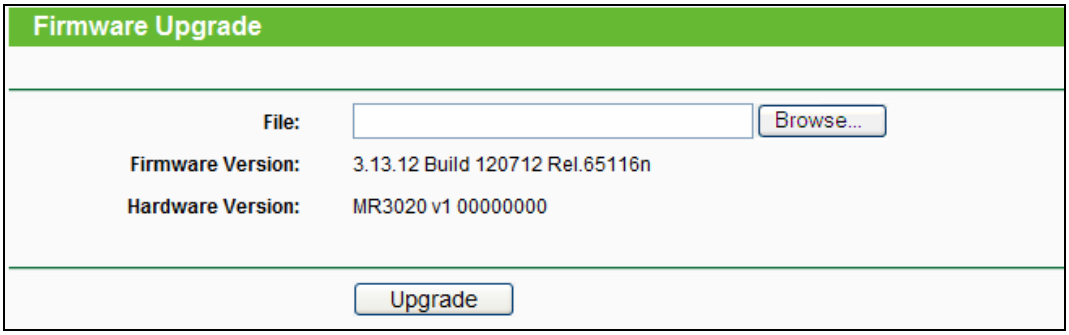


Figure 4-88 Firmware Upgrade

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

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

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

Note:

1) New firmware versions are posted at http://www.tp-link.com and can be downloaded for free. There is no need to upgrade the firmware unless the new firmware has a new feature you want to use. However, when experiencing problems caused by the Router rather than the configuration, you can try to upgrade the firmware.
2) When you upgrade the Router's firmware, you may lose its current configurations, so before upgrading the firmware please write down some of your customized settings to avoid losing important settings.
3) Do not turn off the Router or press the Reset button while the firmware is being upgraded, otherwise, the Router may be damaged.
4) The Router will reboot after the upgrading has been finished.

4.16.4 Factory Defaults

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

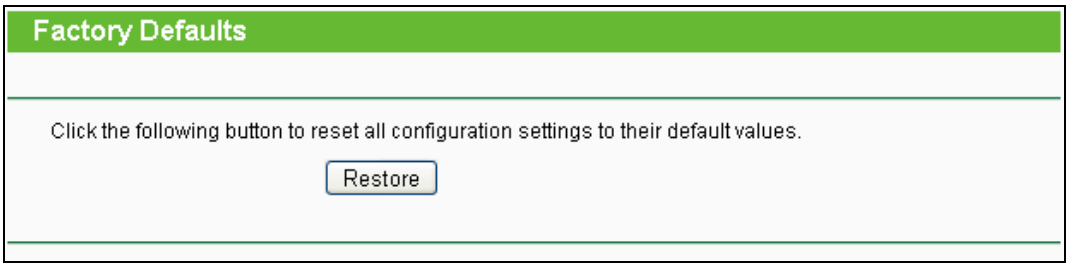


Figure 4-89 Restore Factory Default

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

- The default **User Name**: admin
- The default **Password**: admin
- The default **IP Address**: 192.168.0.254
- The default **Subnet Mask**: 255.255.255.0

Note:

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

4.16.5 Backup & Restore

Choose menu "**System Tools** → **Backup & Restore**", you can save the current configuration of the Router as a backup file and restore the configuration via a backup file as shown in Figure 4-90.

Figure 4-90 Backup & Restore Configuration

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

Note:

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

4.16.6 Reboot

Choose menu "**System Tools → Reboot**", you can click the **Reboot** button to reboot the Router.

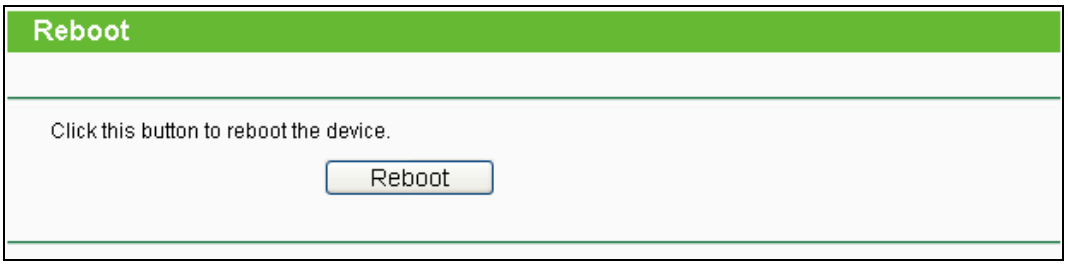


Figure 4-91 Reboot the Router

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

- 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 Router (system will reboot automatically).
- Restore the Router's settings to factory defaults (system will reboot automatically).
- Update the configuration with the file (system will reboot automatically.

4.16.7 Password

Choose menu "**System Tools** → **Password**", you can change the factory default user name and password of the Router in the next screen as shown in Figure 4-92.

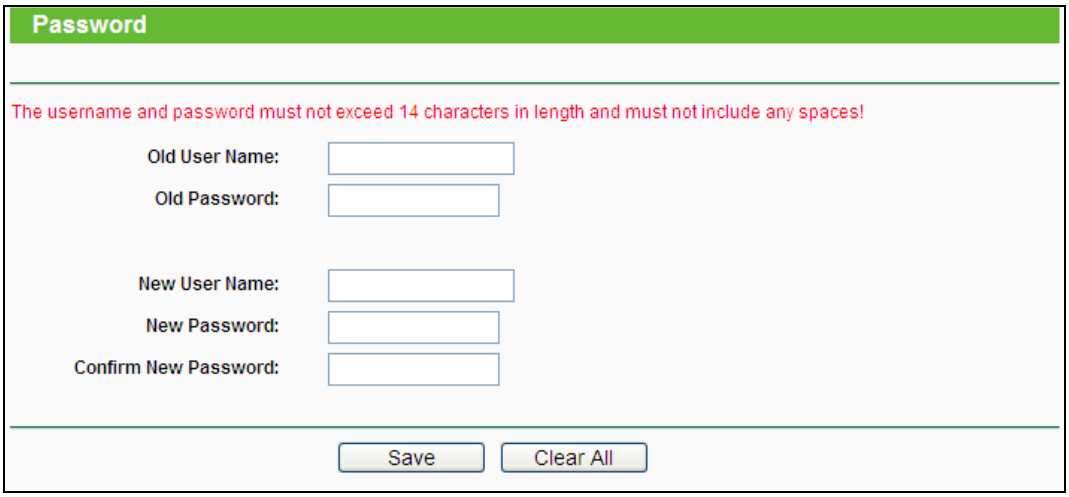


Figure 4-92 Password

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

☞ **Note:**

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

Click the **Save** button when finished.

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

4.16.8 System Log

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

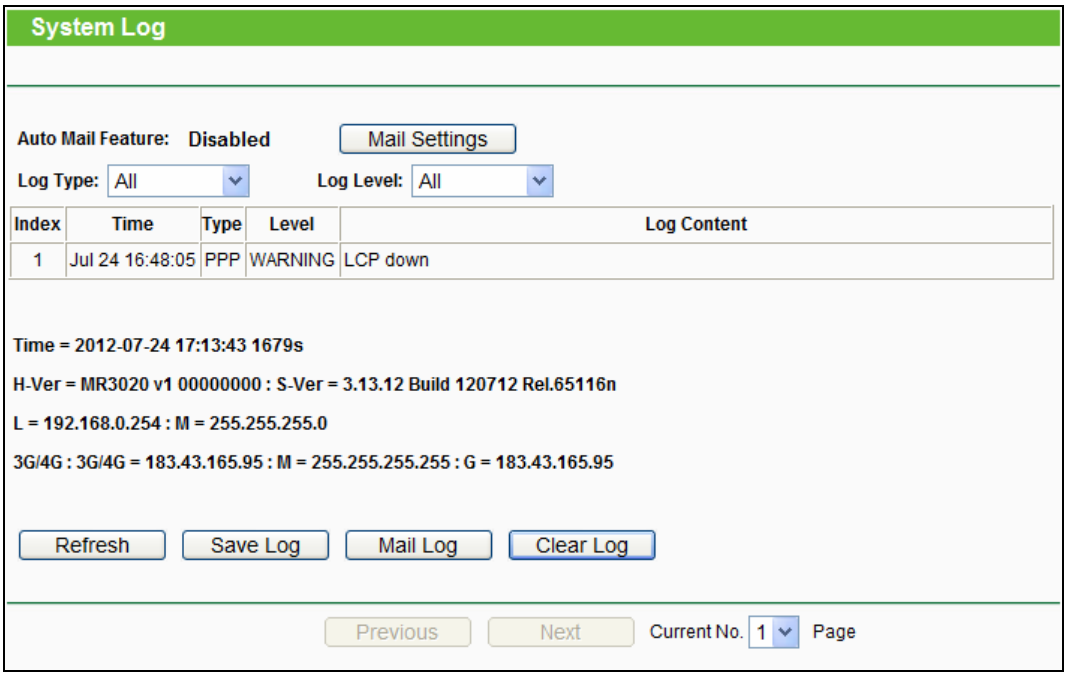


Figure 4-93 System Log

- **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.
- **Clear Log -** All the logs will be deleted from the Router permanently, not just from the page.

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

4.16.9 Working Mode

Choose menu "**System Tools** → **Working Mode**", and you can view the working mode of the Router.

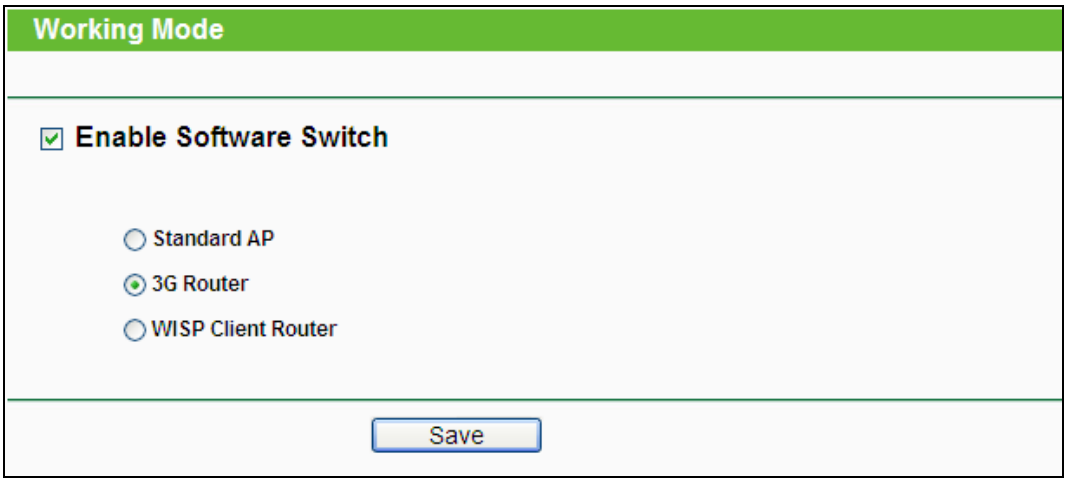


Figure 4-94 Working Mode

- **Standard AP -** In this mode, the device enables multiusers to access, and provides several wireless modes, such as AP, Client, Repeater and so on.
- **3G/4G Router -** In this mode, the device enables multiusers 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 3G/4G Router mode.
- **WISP Client Router -** In this mode, the device enables multiusers 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 WISP Client Router mode. The Ethernet port acts as a LAN port.

Note:

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

4.16.10 Statistics

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

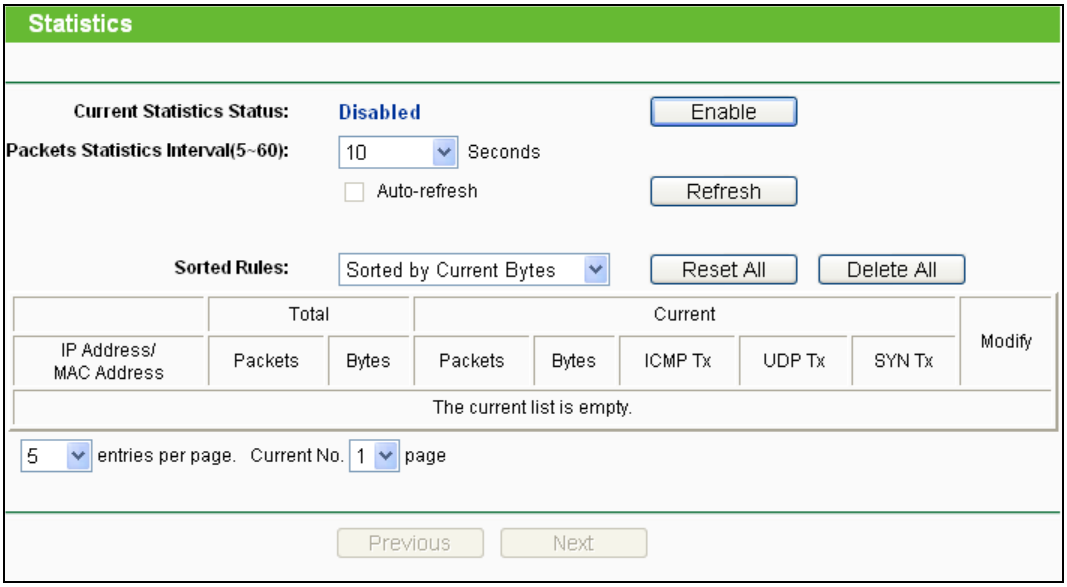


Figure 4-95 Statistics

- **Current Statistics Status -** Enable or Disable. The default value is disabled. To enable, click the **Enable** button. If disabled, the function of DoS protection in Security settings will disabled.
- **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 indicates the time section of the packets statistic.
- **Sorted Rules -** Choose how displayed statistics are sorted.

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

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

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

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

Statistics Table:

IP/MAC Address		The IP and MAC address are displayed with related statistics.
Total	**Packets**	The total number of packets received and transmitted by the Router.
	Bytes	The total number of bytes received and transmitted by the Router.
Current	**Packets**	The total number of packets received and transmitted in the last Packets Statistic interval seconds.
	Bytes	The total number of bytes received and transmitted in the last Packets Statistic interval seconds.
	ICMP Tx	The number of the ICMP packets transmitted to 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 value of he entry to zero.
	Delete	Delete the existing entry in the table.

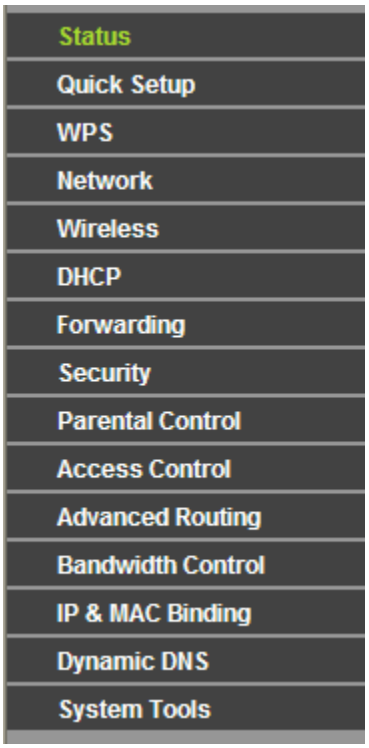
There would be 5 entries on each page. Click **Previous** to return to the previous page and **Next** to the next page.

Chapter 5. Router Configuration—WISP Mode

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

5.1 Login

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



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

5.2 Status

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

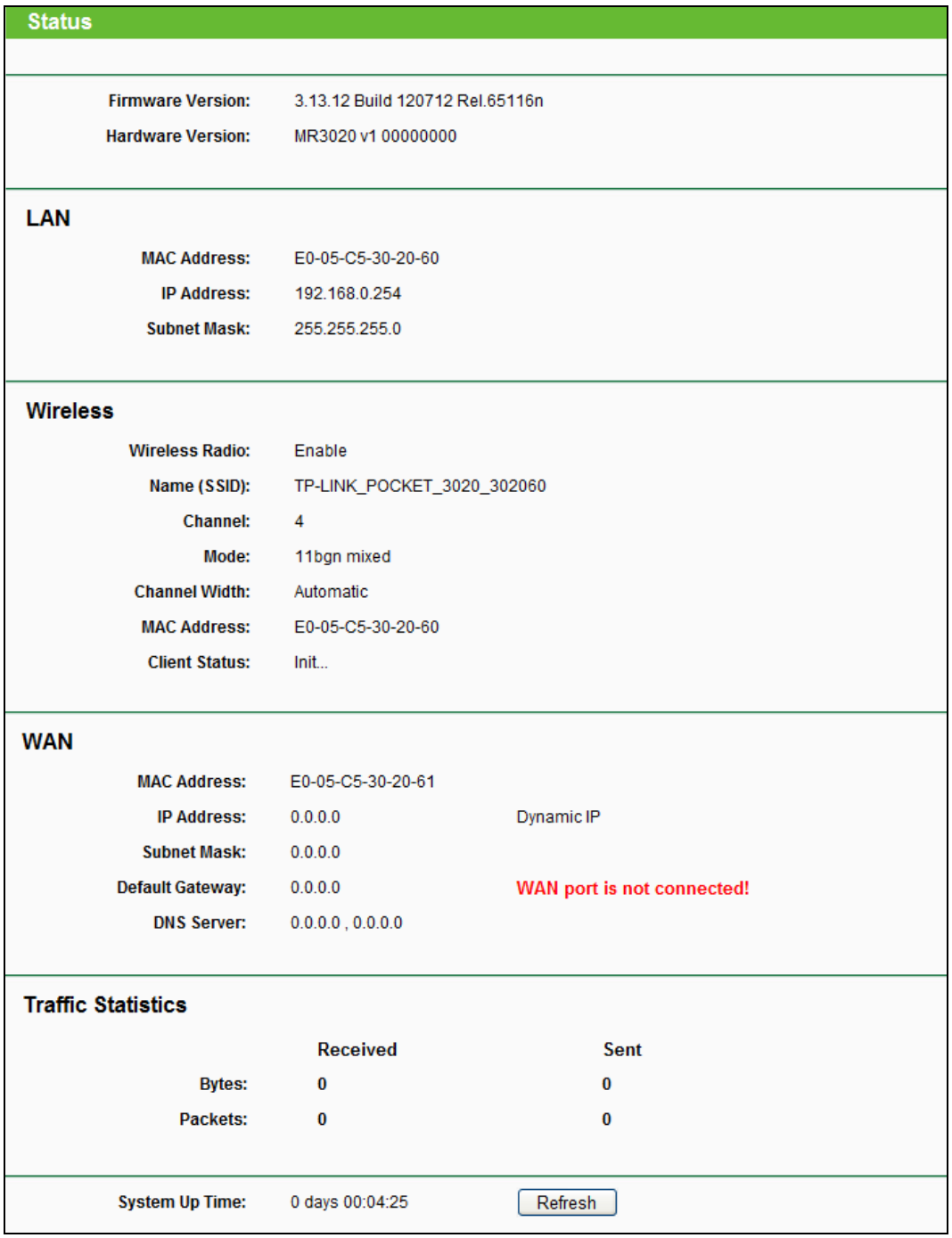


Figure 5-1 Router Status

5.3 Quick Setup

Please refer to Chapter 3: "Quick Installation Guide."

5.4 WPS

This section will guide you to add a new wireless device to an existing network quickly by **WPS (Wi-Fi Protected Setup)** function.

a). Choose menu "**WPS**", and you will see the next screen (shown in Figure 5-2).

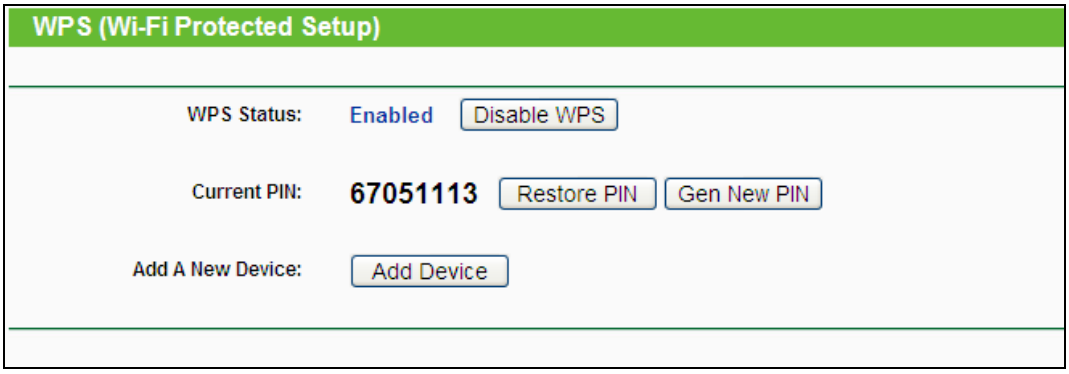


Figure 5-2 WPS

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

b). To add a new device:

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

Note:

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

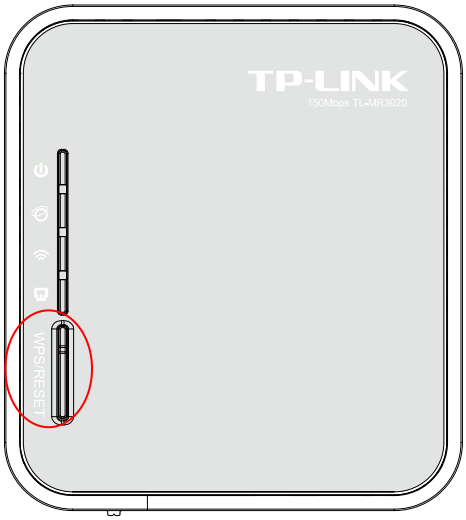
For the configuration of the new device, here takes the Wireless Adapter of our company for example.

I. By PBC

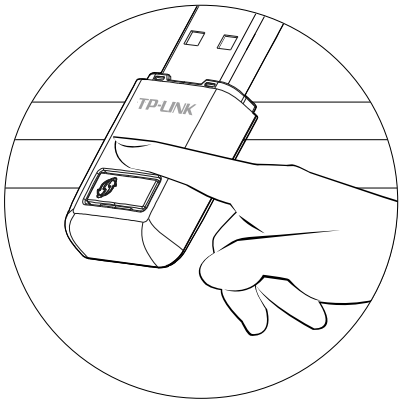
If the wireless adapter supports Wi-Fi Protected Setup and the Push Button Configuration (PBC) method, you can add it to the network by PBC with the following two methods.

Method One:

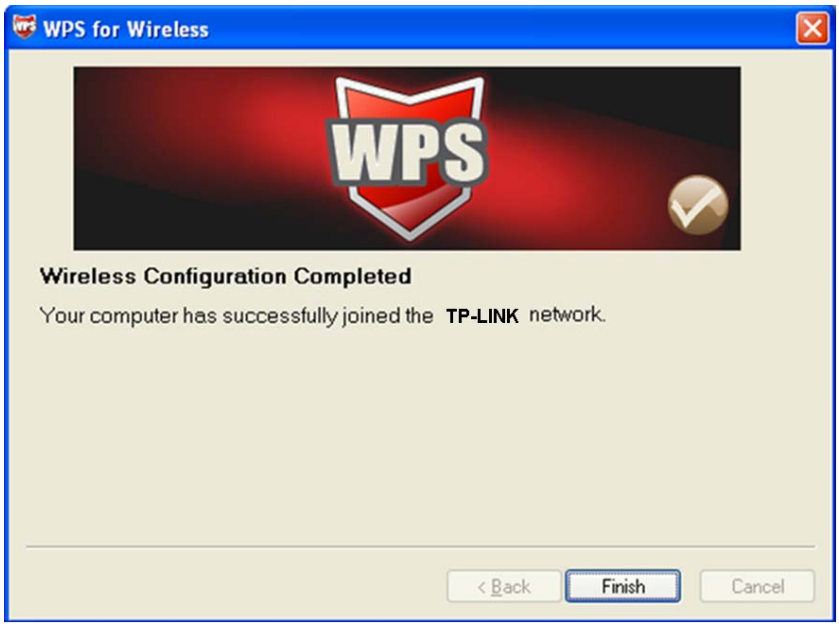
Step 1. Press the WPS/RESET button on the front panel of the Router for less than 5 seconds.



Step 2. Press and hold the WPS button of the adapter directly for 2 or 3 seconds.



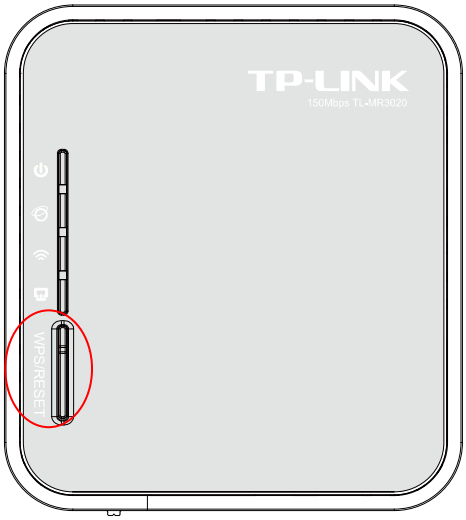
Step 3. Wait for a while until the next screen appears. Click **Finish** to complete the WPS configuration.



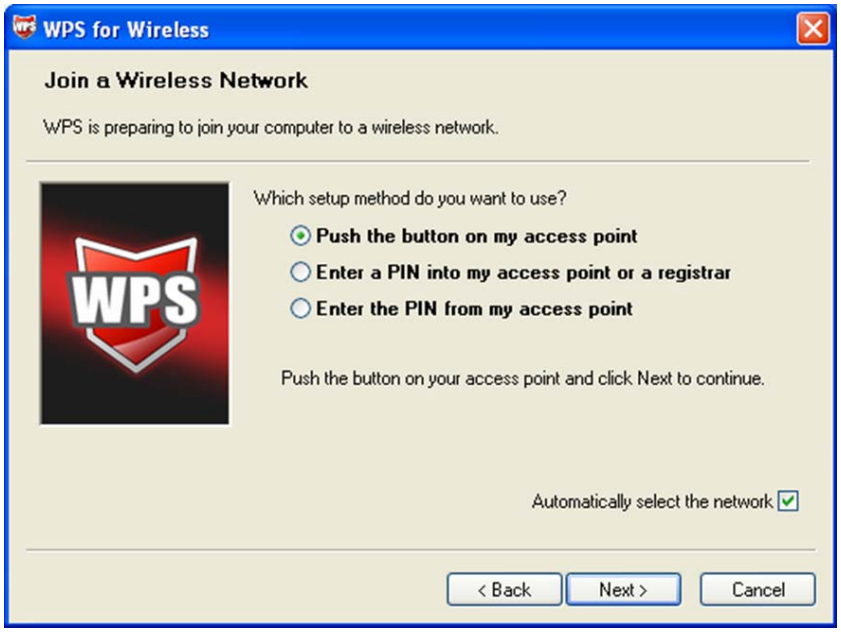
The WPS Configuration Screen of Wireless Adapter

Method Two:

Step 4. Press the WPS/RESET button on the front panel of the Router for less than 5 seconds.

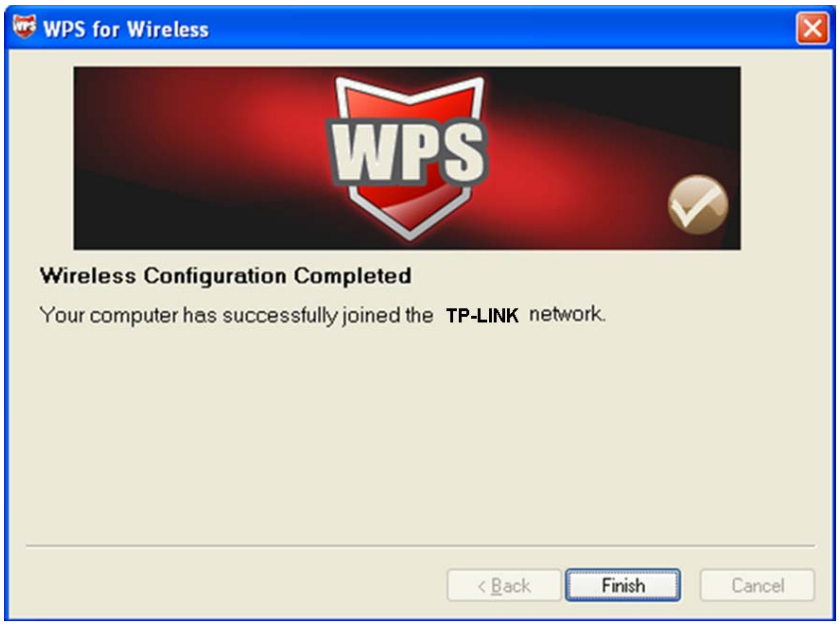


Step 5. For the configuration of the wireless adapter, please choose **Push the button on my access point** in the configuration utility of the WPS as below, and click **Next**.



The WPS Configuration Screen of Wireless Adapter

Step 6. Wait for a while until the next screen appears. Click **Finish** to complete the WPS configuration.



The WPS Configuration Screen of Wireless Adapter

Method Three:

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

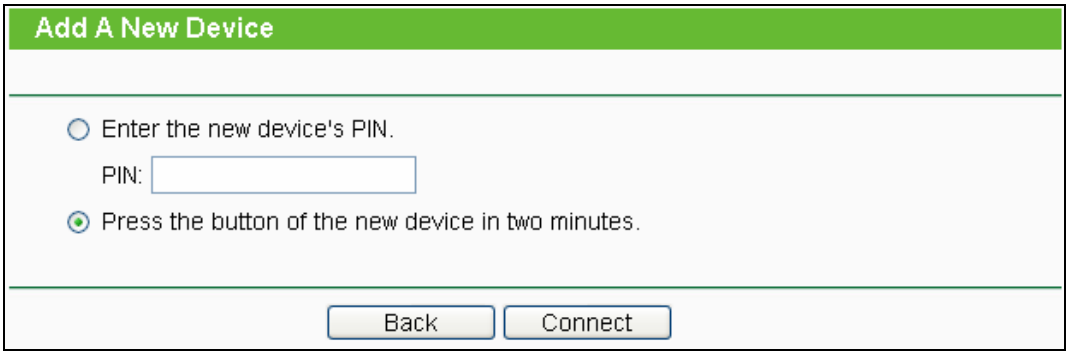
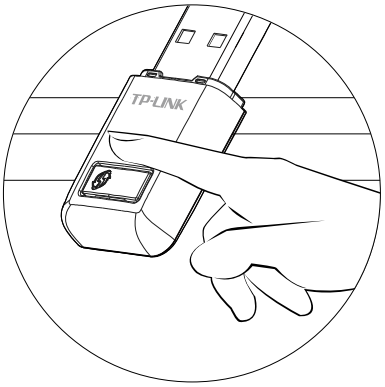


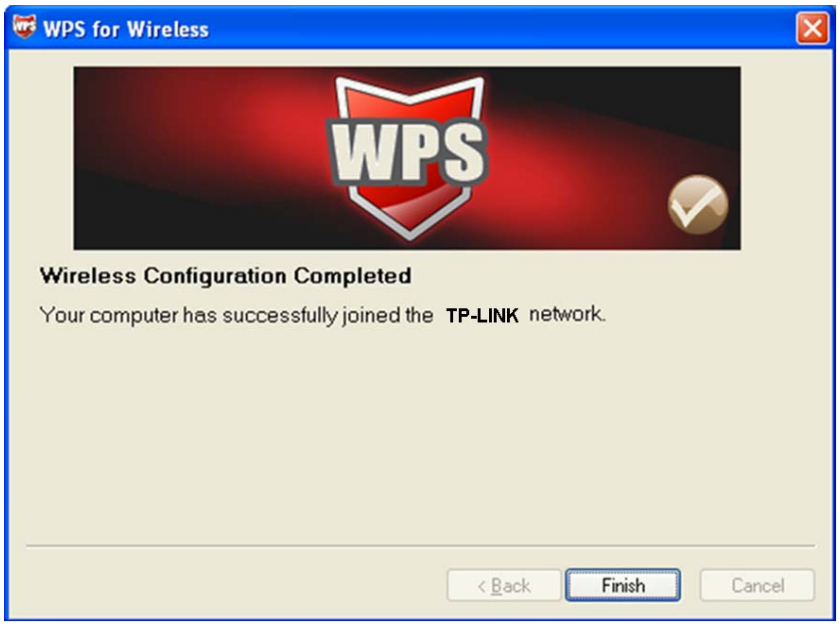
Figure 5-3 Add A New Device

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

Step 3. Press and hold the WPS button of the adapter directly for 2 or 3 seconds.



Step 4. Wait for a while until the next screen appears. Click **Finish** to complete the WPS configuration.



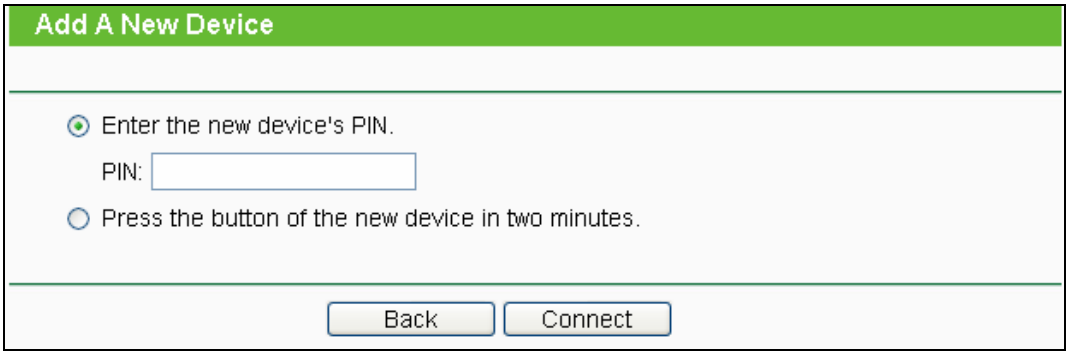
The WPS Configuration Screen of Wireless Adapter

II. By PIN

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

Method One: Enter the PIN into my Router

Step 1. Keep the default WPS Status as **Enabled** and click the **Add device** button in Figure 5-2, then the following screen will appear.

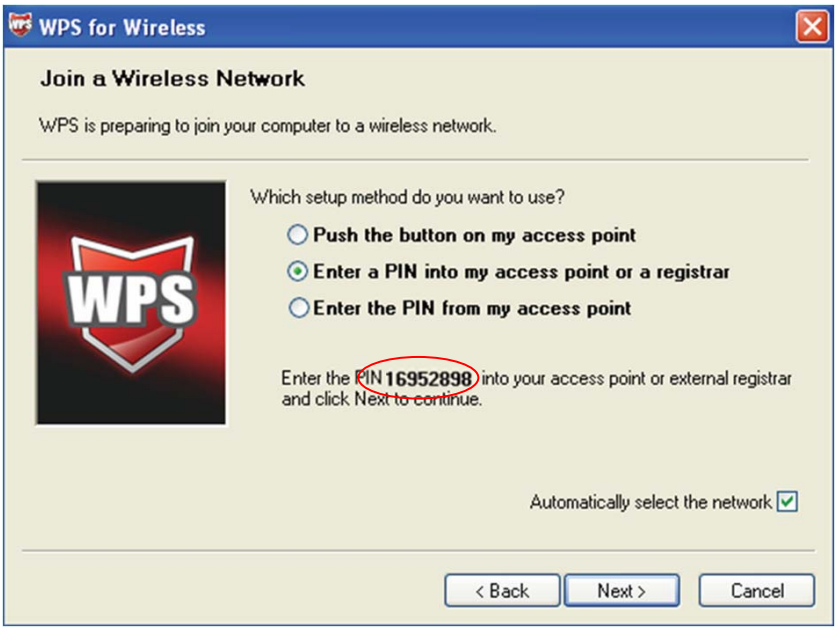


Step 2. Choose **Enter the new device's PIN** and enter the PIN code of the wireless adapter in the field behind PIN in the above figure. Then click **Connect**.

Note:

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

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



The WPS Configuration Screen of Wireless Adapter

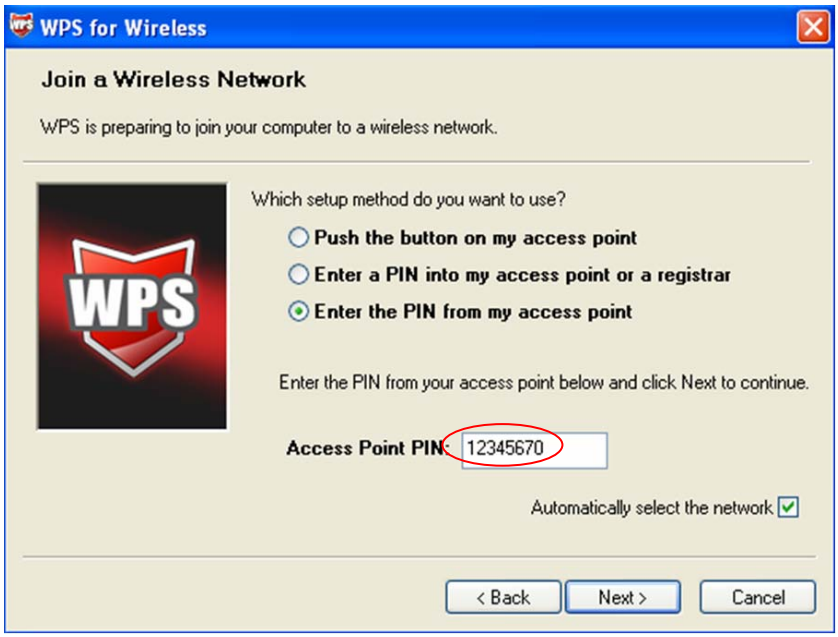
Note:

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

Method Two: Enter the PIN from my Router

Step 1. Get the Current PIN code of the Router in Figure 5-2 (each Router has its unique PIN code. Here takes the PIN code 12345670 of this Router for example).

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

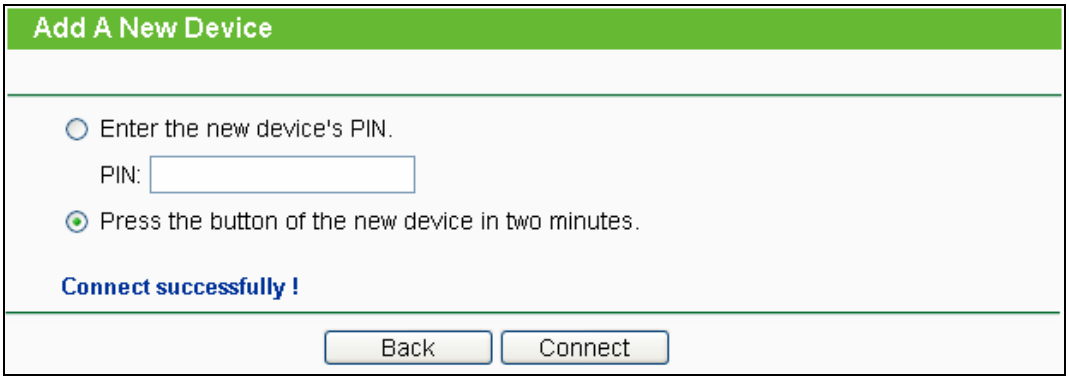


The WPS Configuration Screen of Wireless Adapter

Note:

The default PIN code of the Router can be found in its label or the WPS configuration screen as Figure 5-2.

Step 3. You will see the following screen when the new device successfully connected to the network.



Note:

1) The status LED on the Router will light green all the time if the device has been successfully added to the network.
2) The WPS function cannot be configured if the Wireless Function of the Router is disabled. Please make sure the Wireless Function is enabled before configuring the WPS.

5.5 Network

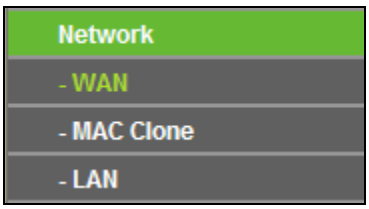


Figure 5-4 the Network menu

There are three submenus under the Network menu (shown in Figure 5-4): **WAN**, **MAC Clone** and **LAN.** Click any of them, and you will be able to configure the corresponding function.

5.5.1 WAN

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

1. If your ISP provides the DHCP service, please choose **Dynamic IP** type, and the Router will automatically get IP parameters from your ISP. You can see the page as follows (Figure 5-5):

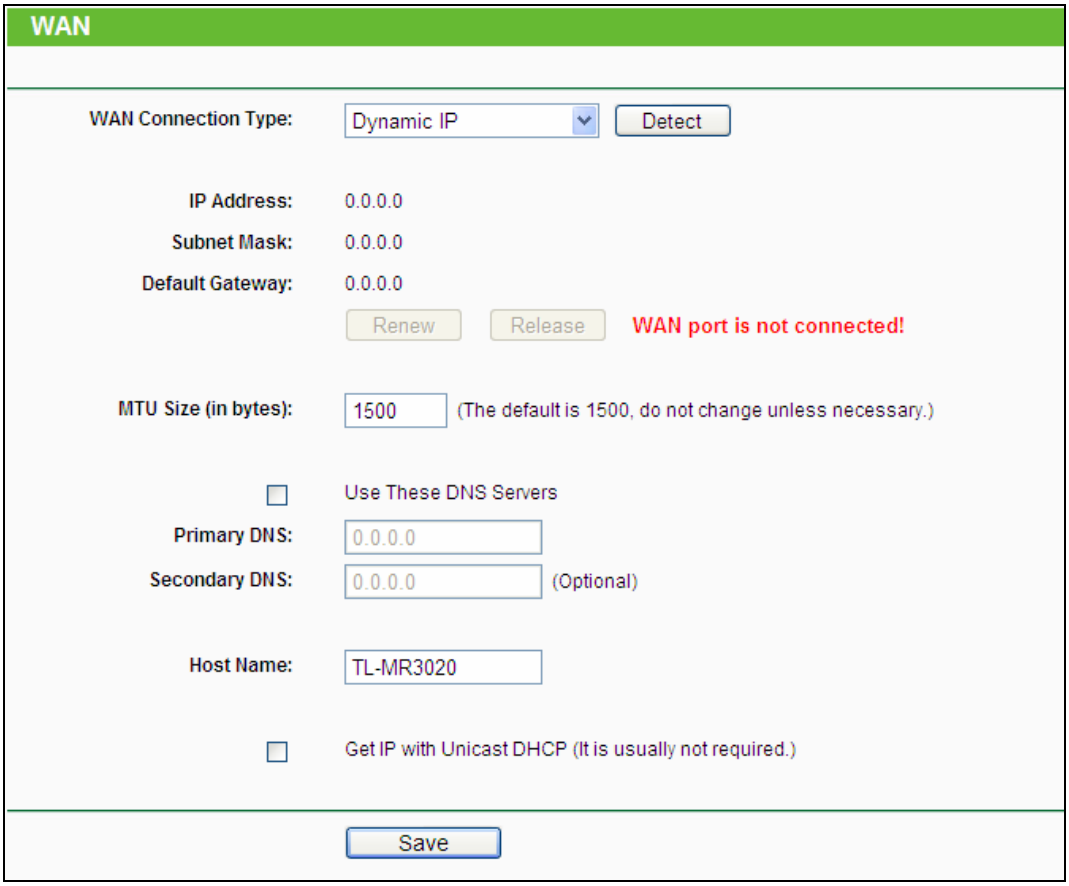


Figure 5-5 WAN - Dynamic IP

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

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

Note:

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

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

2. If your ISP provides a static or fixed IP Address, Subnet Mask, Gateway and DNS setting, select **Static IP**. The Static IP settings page will appear as shown in Figure 5-6.

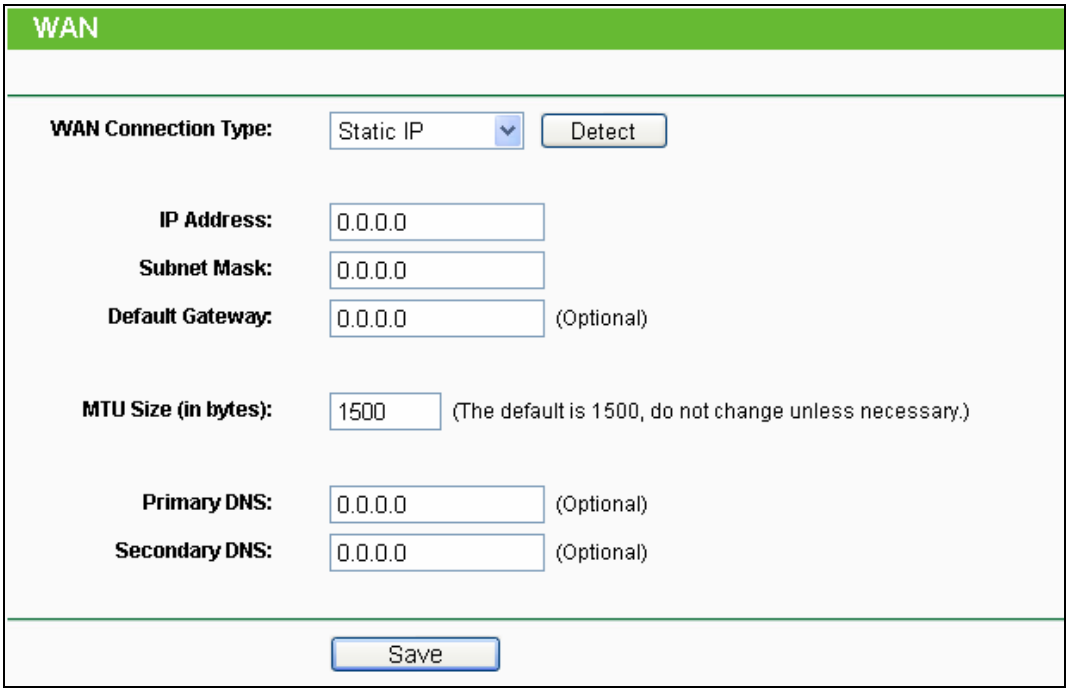


Figure 5-6 WAN - Static IP

- **IP Address -** Enter the IP address in dotted-decimal notation provided by your ISP.
- **Subnet Mask -** Enter the subnet Mask provided by your ISP in dotted-decimal notation. Usually, the Sub Mask is 255.255.255.0.
- **Default Gateway -** (Optional) Enter the gateway IP address provided by your ISP in dotted-decimal notation.
- **MTU Size -** The normal **MTU** (Maximum Transmission Unit) value for most Ethernet networks is 1500 Bytes. It is not recommended that you change the default **MTU Size** unless required by your ISP.
- **Primary/Secondary DNS -** (Optional) Enter one or two DNS addresses in dotted-decimal notation provided by your ISP.

3. If your ISP provides a PPPoE connection, select **PPPoE/Russia PPPoE** option. And you should enter the following parameters (Figure 5-7):

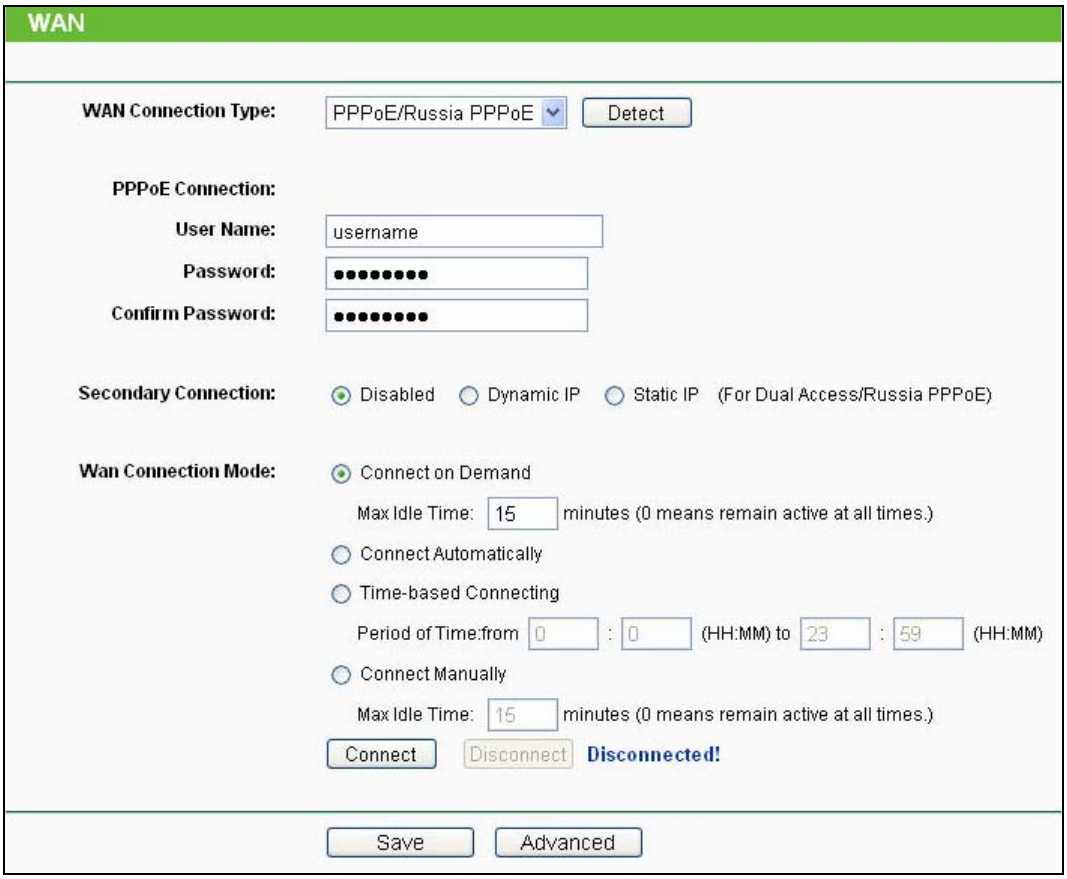


Figure 5-7 WAN - PPPoE

- **User Name/Password -** Enter the User Name and Password provided by your ISP. These fields are case-sensitive.
- **Confirm Password -** Re-enter the Password provided by your ISP to ensure the Password you entered is correct.
- **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 -** You can check this radio button to use Dynamic IP as the secondary connection to connect to the local area network provided by ISP.
  - **Static IP -** You can check this radio button to use Static IP as the secondary connection to connect to the local area network provided by 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.
- **Time-based Connecting -** The connection will only be established in the period from the start time to the end time (both are in HH:MM format).

Note:

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

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

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

If you want to do some advanced configurations, please click the **Advanced** button, and the page shown in Figure 5-8 will then appear:

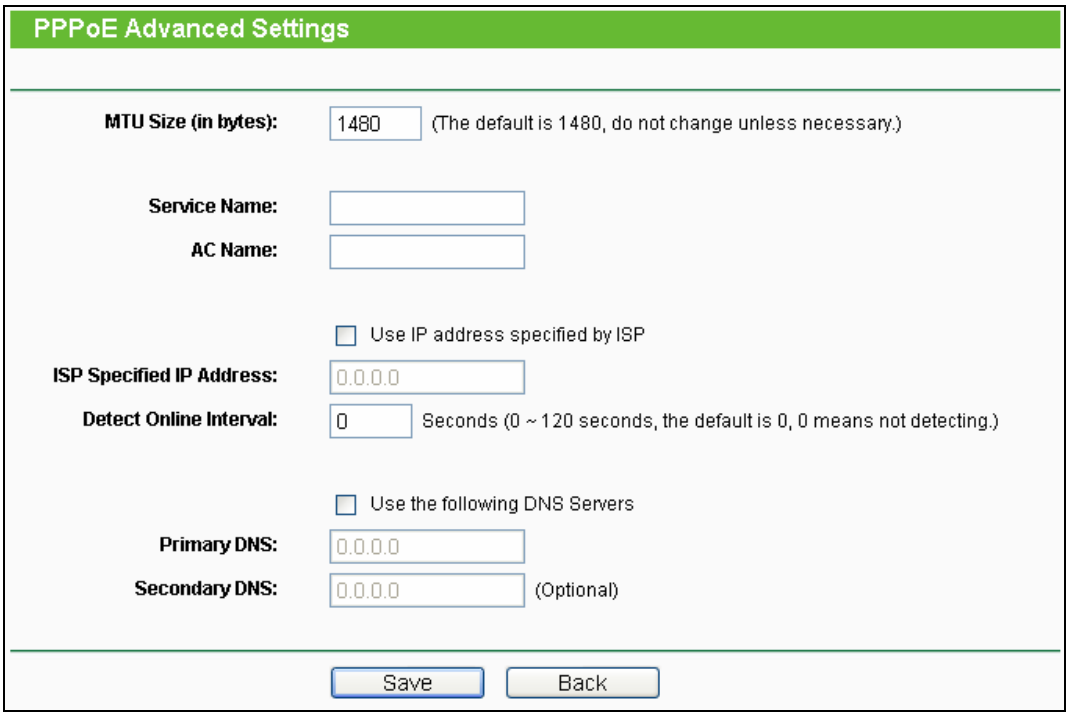


Figure 5-8 PPPoE Advanced Settings

- **MTU Size -** The default MTU size is “1480” bytes, which is usually fine. It is not recommended that you change the default **MTU Size** unless required by your ISP.
- **Service Name/AC Name -** The service name and AC (Access Concentrator) name, which should not be configured unless you are sure it is necessary for your ISP. In most cases, leaving these fields blank will work.

- **ISP Specified IP Address -** If your ISP does not automatically assign IP addresses to the Router during login, please click "**Use IP address specified by ISP**" check box and enter the IP address provided by your ISP in dotted-decimal notation.
- **Detect Online Interval -** The Router will detect Access Concentrator online at every interval. The default value is "0". You can input the value between "0"and "120". The value "0" means no detect.
- **DNS IP address -** If your ISP does not automatically assign DNS addresses to the Router during login, please click "**Use the following DNS servers**" check box and enter the IP address in dotted-decimal notation of your ISP's primary DNS server. If a secondary DNS server address is available, enter it as well.

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

4. If your ISP provides BigPond Cable (or Heart Beat Signal) connection, please select **BigPond Cable**. And you should enter the following parameters (Figure 5-9):

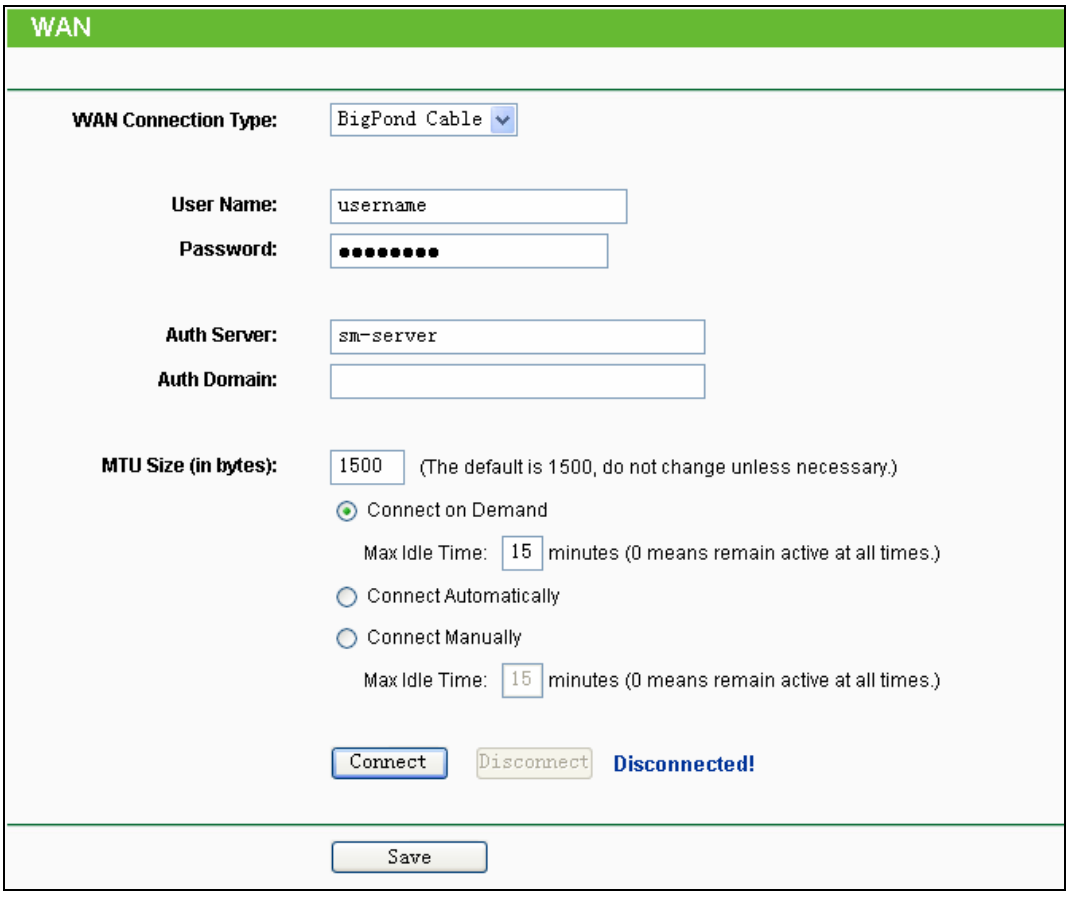


Figure 5-9 WAN – BigPond Cable

- **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.

e.g.

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.

Caution: 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. And you should enter the following parameters (Figure 5-10):

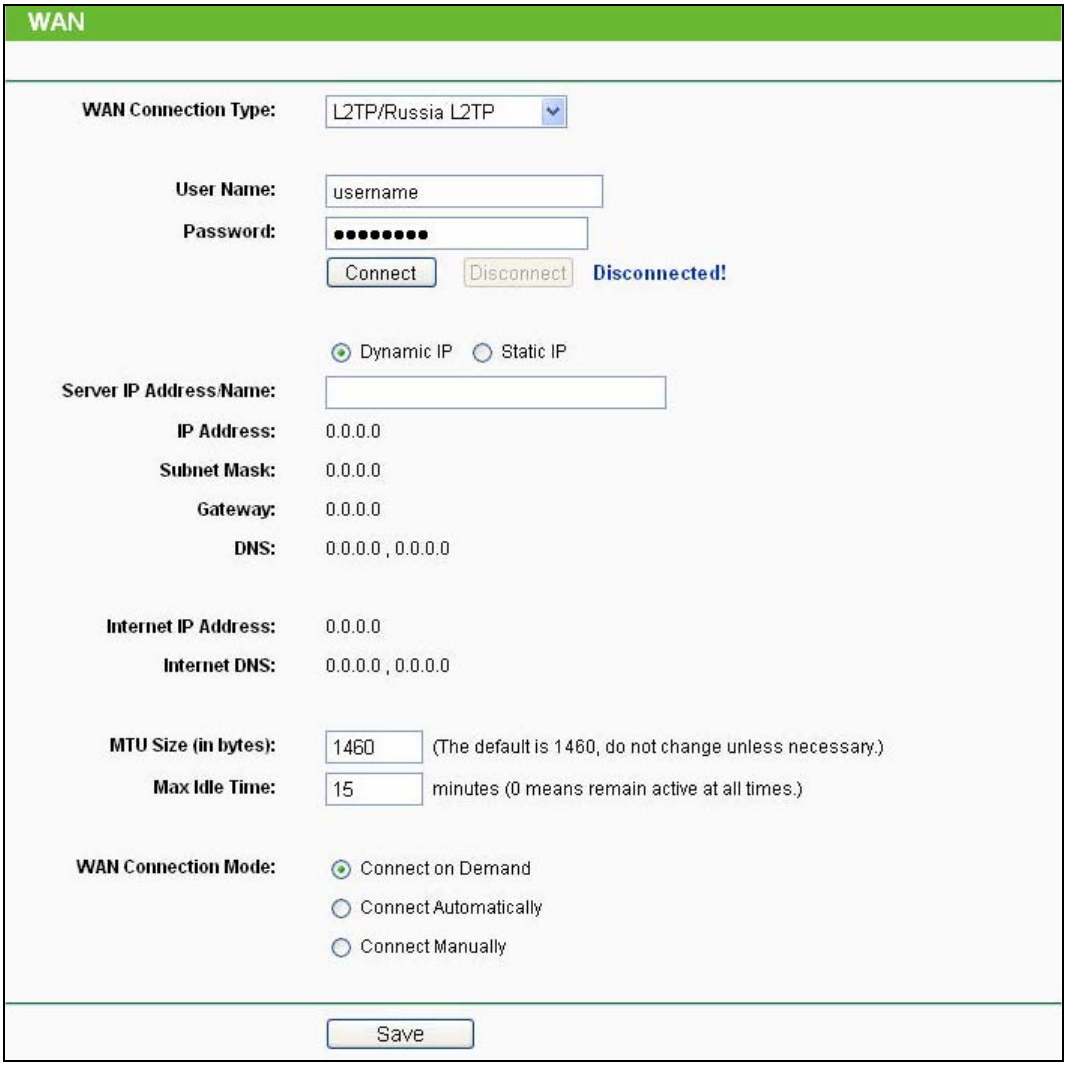


Figure 5-10 WAN –L2TP

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

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

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

6. If your ISP provides PPTP connection, please select **PPTP/Russia PPTP** option. And you should enter the following parameters (Figure 5-11):

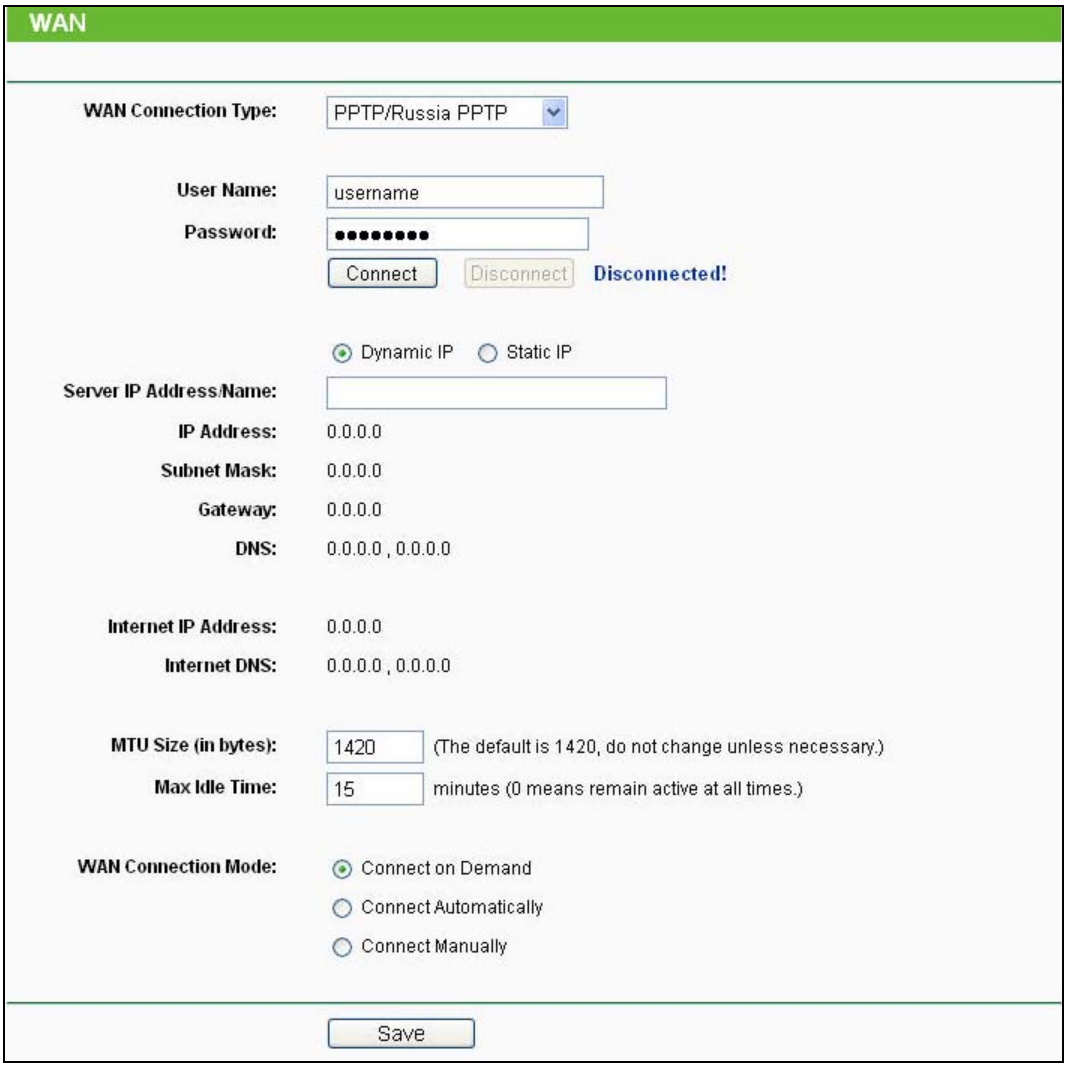


Figure 5-11 WAN –PPTP

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

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

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

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

Note:

If you don't know how to choose the appropriate connection type, click the **Detect** button to allow the Router to automatically search your Internet connection for servers and protocols. The connection type will be reported when an active Internet service is successfully detected by the Router. This report is for your reference only. To make sure the connection type your ISP provides, please refer to the ISP. The various types of Internet connections that the Router can detect are as follows:

- **PPPoE -** Connections which use PPPoE that requires a user name and password.
- **Dynamic IP -** Connections which use dynamic IP address assignment.
- **Static IP -** Connections which use static IP address assignment.

The Router can not detect PPTP/L2TP/BigPond connections with your ISP. If your ISP uses one of these protocols, then you must configure your connection manually.

5.5.2 MAC Clone

Choose menu "**Network→MAC Clone**", and then you can configure the MAC address of the WAN on the screen below, Figure 5-12:

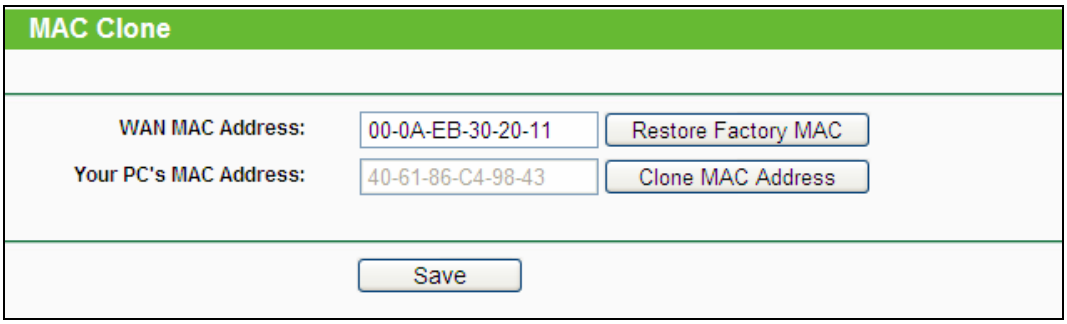


Figure 5-12 MAC Address Clone

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

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

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

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

Note:

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

5.5.3 LAN

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

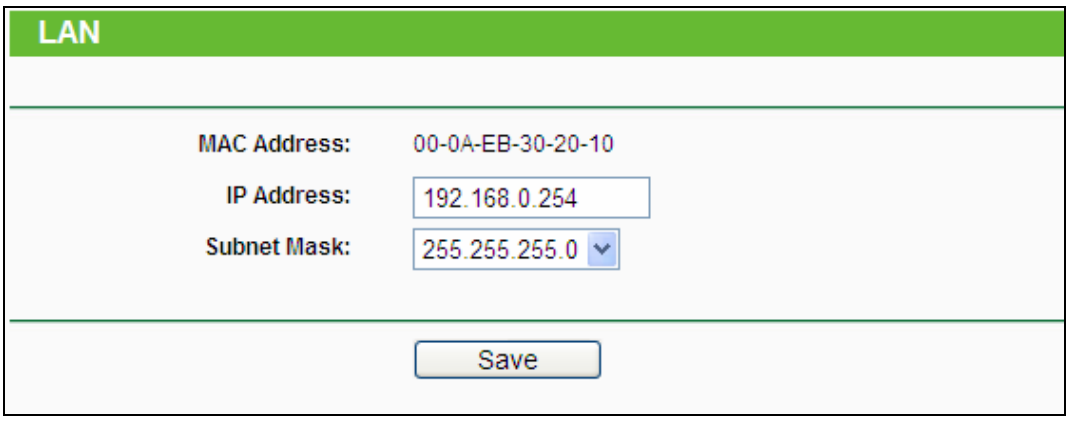


Figure 5-13 LAN

- **MAC Address -** The physical address of the Router, as seen from the LAN. The value can't be changed.
- **IP Address -** Enter the IP address of your Router or reset it in dotted-decimal notation (factory default: 192.168.0.254).
- **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 change accordingly at the same time，while the Virtual Server and DMZ Host will not take effect until they are re-configured.

5.6 Wireless

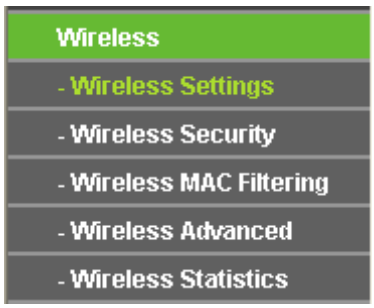


Figure 5-14 Wireless menu

There are five submenus under the Wireless menu (shown in Figure 5-14): **Wireless Settings**, **Wireless Security, Wireless MAC Filtering, Wireless Advanced** and **Wireless Statistics.** Click any of them, and you will be able to configure the corresponding function.

5.6.1 Wireless Settings

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

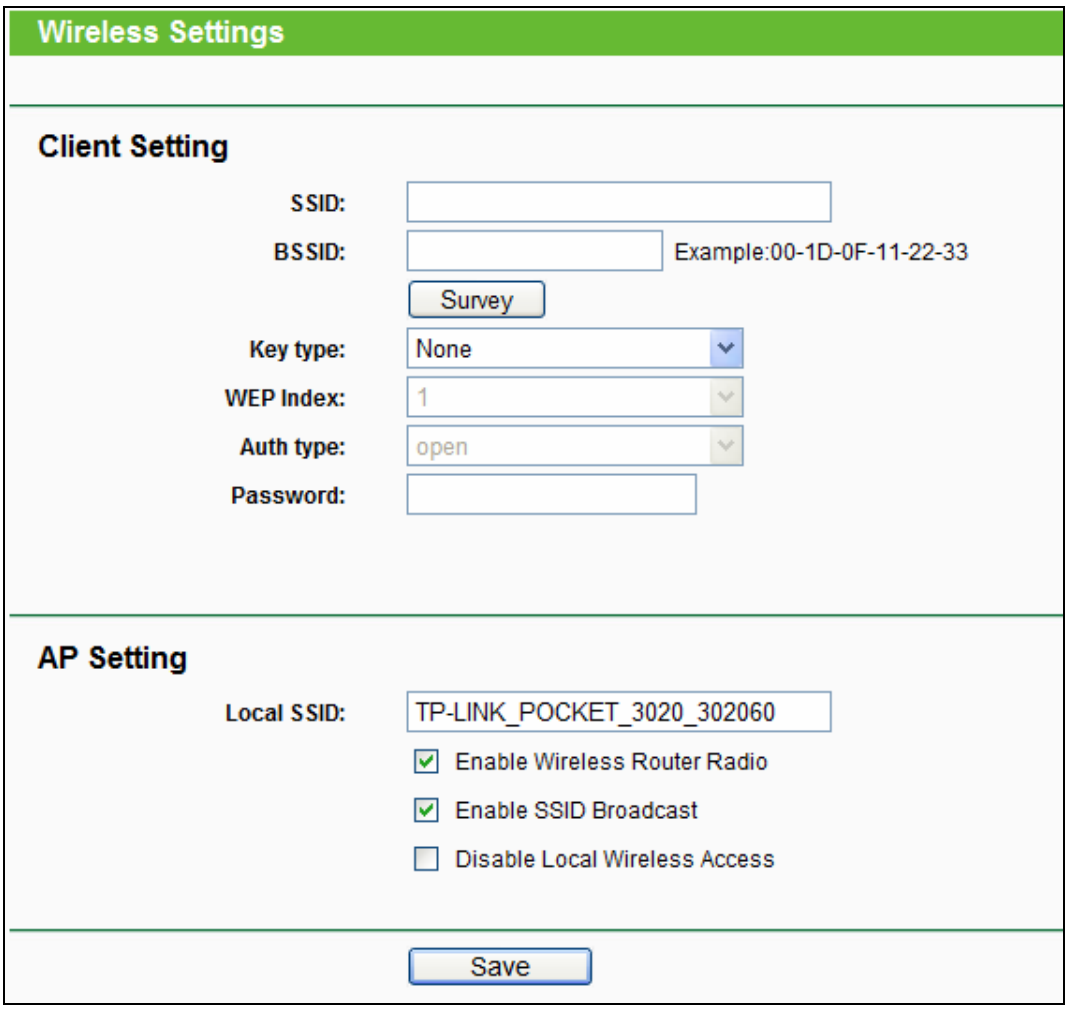


Figure 5-15 Wireless Settings

- **SSID -** The SSID of the AP your Router is going to connect to as a client. You can also use the search function to select the SSID to join.
- **BSSID -** The BSSID of the AP your Router 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 survey 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.
- **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.
- **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.
- **Password -** If the AP your Router is going to connect needs password, you need to fill the password in this blank.
- **Local SSID -** Enter a value of up to 32 characters. The same Name (SSID) must be assigned to all wireless devices in your network.

- **Enable Wireless Router Radio -** The wireless radio of the Router can be enabled or disabled to allow wireless stations access. If enabled, the wireless stations will be able to access the Router. Otherwise, wireless stations will not be able to access the Router.
- **Enable SSID Broadcast -** If you select the **Enable SSID Broadcast** checkbox, the wireless router will broadcast its name (SSID) on the air.
- **Disable Local Wireless Access -** If you select the **Disable Local Wireless Access** checkbox, the wireless router will disable local wireless access; other stations will not be able to access the Router by wireless.

Click **Survey** button on the Wireless page shown as Figure 5-15, and then AP List page will appear, as shown in Figure 5-16. 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 5-17.

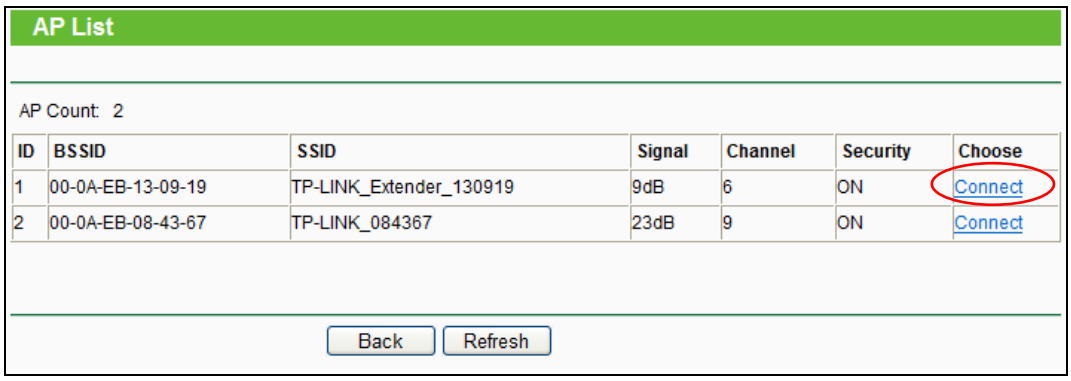


Figure 5-16 AP List

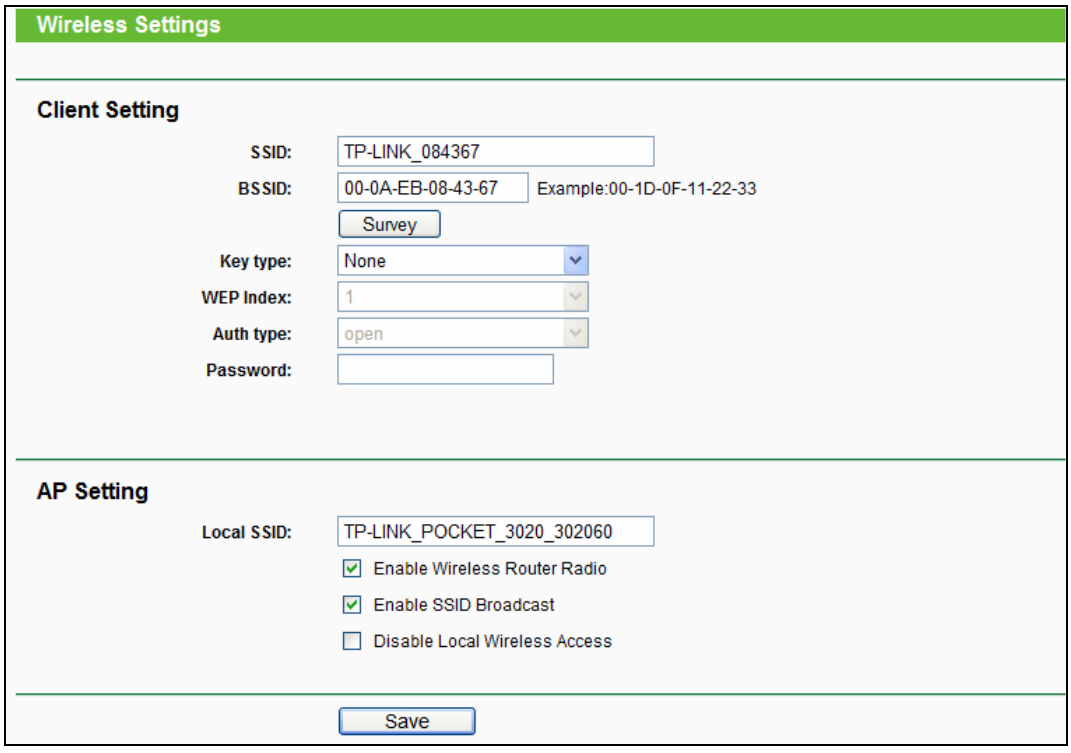


Figure 5-17

Note:

If you know the SSID of the desired AP, you can also input it into the field "SSID" manually.

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

Note:

1) The operating distance or range of your wireless connection varies significantly based on the physical placement of the Router. For best results, place your Router.
   - 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.
2) Failure to follow these guidelines can result in significant performance degradation or inability to wirelessly connect to the Router.

5.6.2 Wireless Security

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

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

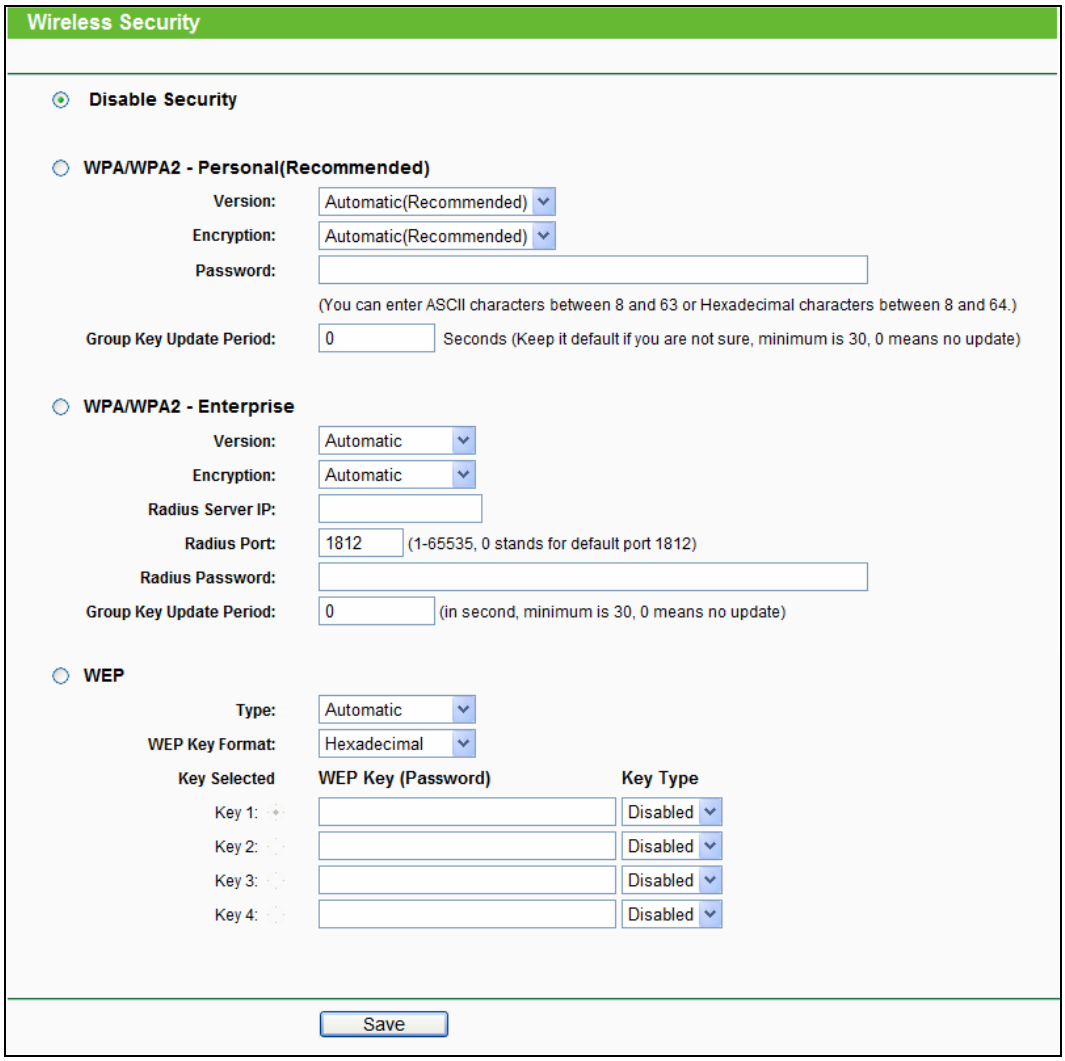


Figure 5-18

- **Disable Security -** If you do not want to use wireless security, select this check box, but it's strongly recommended to choose one of the following modes to enable security.
- **WPA/WPA2 – Personal (Recommended) -** It's the WPA/WPA2 authentication type based on pre-shared passphrase.
  - **Version -** you can choose the version of the WPA-PSK security on the drop-down list. The default setting is **Automatic**, which can select **WPA-PSK (**Pre-shared key of WPA) or **WPA2-PSK** (Pre-shared key of WPA) automatically based on the wireless station's capability and request.
  - **Encryption -** When **WPA-PSK** or **WPA** is set as the Authentication Type, you can select either **Automatic**, or **TKIP** or **AES** as Encryption.

☞ **Note:**

If you check the **WPA/WPA2 – Personal (Recommended)** radio button and choose TKIP encryption, you will find a notice in red as shown in Figure 5-19.

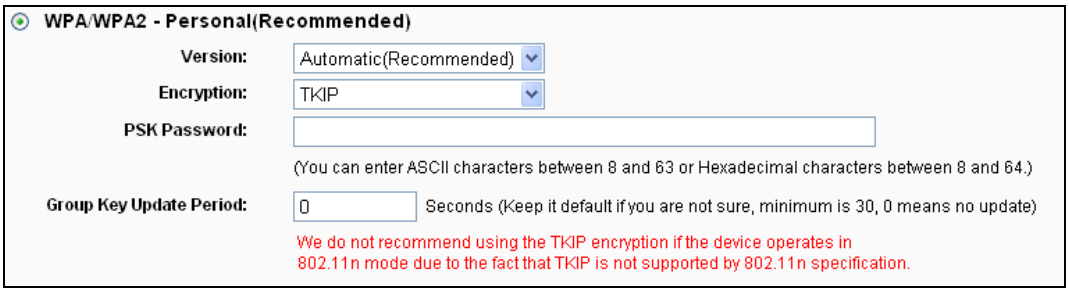


Figure 5-19

- **PSK Password -** You can enter ASCII characters between 8 and 63 characters or 8 to 64 Hexadecimal characters.
- **Group Key Update Period -** Specify the group key update interval in seconds. The value should be 30 or above. Enter 0 to disable the update.

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

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

- **Version -** you can choose the version of the WPA security on the pull-down list. The default setting is **Automatic**, which can select **WPA (**Wi-Fi Protected Access) or **WPA2 (**WPA version 2) automatically based on the wireless station's capability and request.
- **Encryption -** You can select either **Automatic**, or **TKIP** or **AES.**

Note:

If you check the **WPA/WPA2 - Enterprise** radio button and choose TKIP encryption, you will find a notice in red as shown in Figure 5-20.

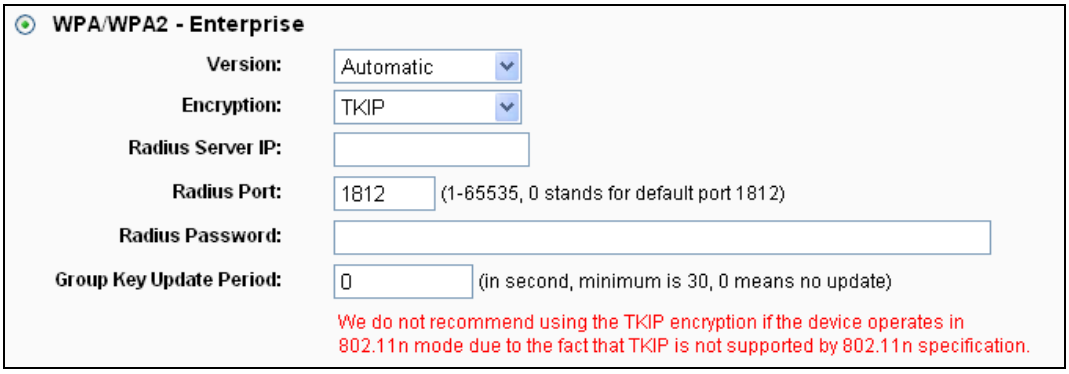


Figure 5-20

- **Radius Server IP -** Enter the IP address of the Radius Server.
- **Radius Port -** Enter the port that radius service used.
- **Radius Password -** Enter the password for the Radius Server.
- **Group Key Update Period -** Specify the group key update interval in seconds. The value should be 30 or above. Enter 0 to disable the update.

➢ **WEP -** It is based on the IEEE 802.11 standard. If you select this check box, you will find a notice in red as show in Figure 5-21.

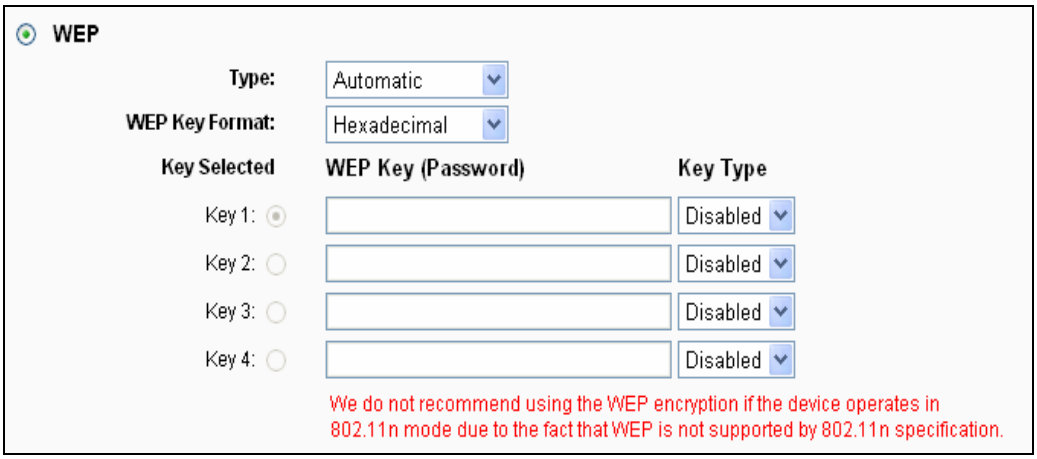


Figure 5-21

- **Type -** you can choose the type for the WEP security on the pull-down list. The default setting is **Automatic**, which can select **Open System** or **Shared Key** authentication type automatically based on the wireless station's capability and request.
- **WEP Key Format - Hexadecimal** and **ASCII** formats are provided. **Hexadecimal** format stands for any combination of hexadecimal digits (0-9, a-f, A-F) in the specified length. **ASCII** format stands for any combination of keyboard characters in the specified length.
- **WEP Key-** Select which of the four keys will be used and enter the matching WEP key that you create. Make sure these values are identical on all wireless stations in your network.
- **Key Type -** You can select the WEP key length (64-bit, or 128-bit, or 152-bit.) for encryption. "Disabled" means this WEP key entry is invalid.

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

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

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

☞ **Note:**

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

5.6.3 Wireless MAC Filtering

Choose menu "**Wireless→MAC Filtering**", and then you can control the wireless access by configuring the Wireless MAC Address Filtering function, shown in Figure 5-22.

Figure 5-22 Wireless MAC address Filtering

To filter wireless users by MAC Address, click **Enable**. The default setting is **Disable**.

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

To Add a Wireless MAC Address filtering entry, click the **Add New…** button. The "**Add or Modify Wireless MAC Address Filtering entry"** page will appear as shown in Figure 5-23:

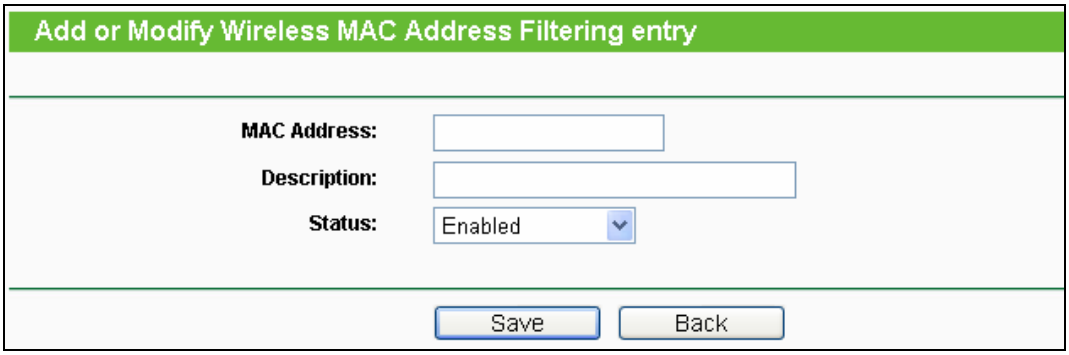


Figure 5-23 Add or Modify Wireless MAC Address Filtering entry

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

1. Enter the appropriate MAC Address into the **MAC Address** field. The format of the MAC Address is XX-XX-XX-XX-XX-XX (X is any hexadecimal digit). For example: 00-0A-EB-00-07-8A.
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** drop-down list.

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

To modify or delete an existing entry:

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

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

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

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

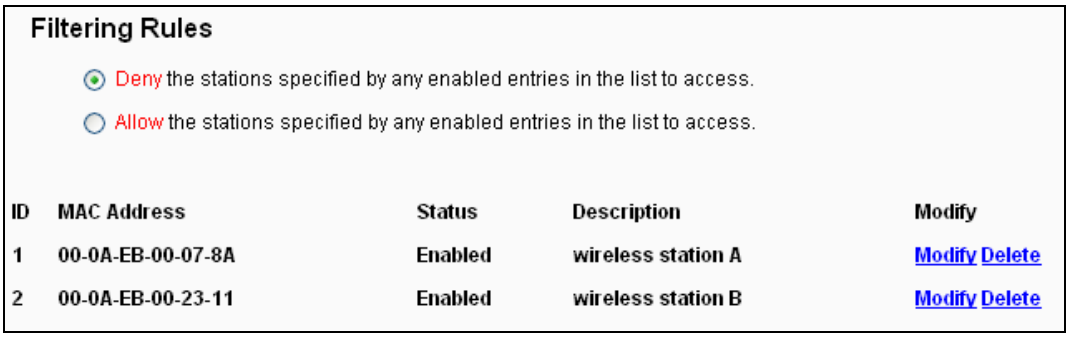
Click the **Next** button to go to the next page

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

For example: If you desire that the wireless station A with MAC address 00-0A-EB-00-07-8A and the wireless station B with MAC address 00-0A-EB-00-23-11 are able to access the Router, but all the other wireless stations cannot access the Router, you can configure the **Wireless MAC Address Filtering** list by following these steps:

1. Click the **Enable** button to enable this function.
2. Select the radio button: **Deny the stations not specified by any enabled entries in the list to access** for **Filtering Rules.**
3. Delete all or disable all entries if there are any entries already.
4. Click the **Add New...** button and enter the MAC address 00-0A-EB-00-07-8A /00-0A-EB-00-23-11 in the **MAC Address** field, then enter wireless station A/B in the **Description** field, while select **Enabled** in the **Status** drop-down list. Finally, click the **Save** and the **Back** button.

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



5.6.4 Wireless Advanced

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

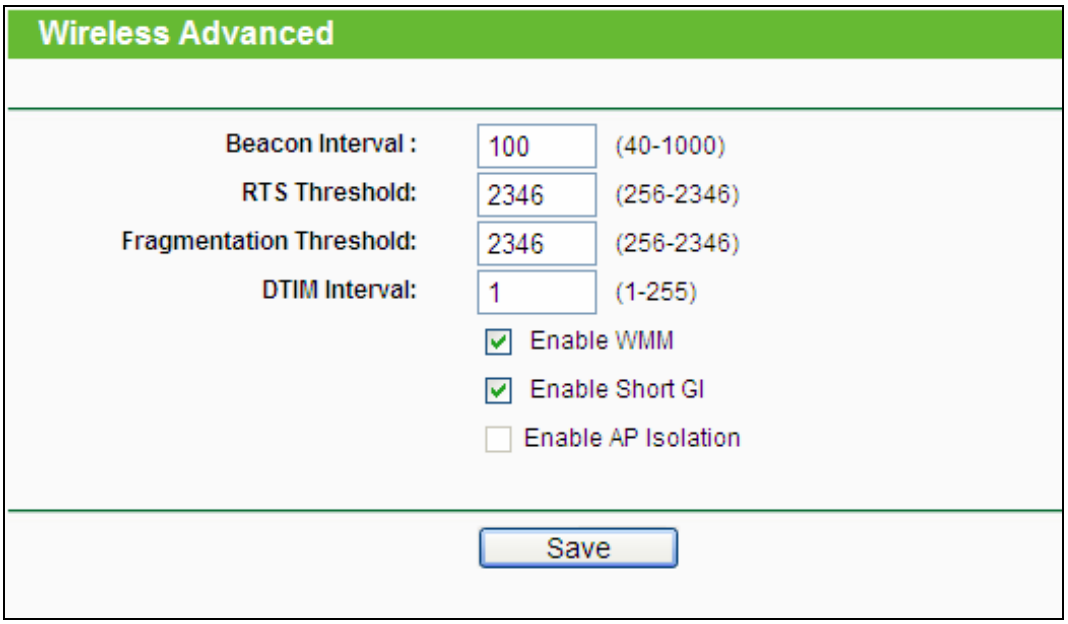


Figure 5-24 Wireless Advanced

- **Beacon Interval -** Enter a value between 40-1000 milliseconds for Beacon Interval here. The beacons are the packets sent by the router to synchronize a wireless network. Beacon Interval value determines the time interval of the beacons. The default value is 100.
- **RTS Threshold -** Here you can specify the RTS (Request to Send) Threshold. If the packet is larger than the specified RTS Threshold size, the router will send RTS frames to a particular receiving station and negotiate the sending of a data frame. The default value is 2346.
- **Fragmentation Threshold -** This value is the maximum size determining whether packets will be fragmented. Setting the Fragmentation Threshold too low may result in poor network performance since excessive packets. 2346 is the default setting and is recommended.
- **DTIM Interval -** This value determines the interval of the Delivery Traffic Indication Message (DTIM). A DTIM field is a countdown field informing clients of the next window for listening to broadcast and multicast messages. When the Router has buffered broadcast or multicast messages for associated clients, it sends the next DTIM with a DTIM Interval value. You can specify the value between 1-255 Beacon Intervals. The default value is 1, which indicates the DTIM Interval is the same as Beacon Interval.

- **Enable WMM - WMM** function can guarantee the packets with high- priority messages being transmitted preferentially. It is strongly recommended enabled.
- **Enable Short GI -** This function is recommended for it will increase the data capacity by reducing the guard interval time.
- **Enabled AP Isolation -** This function can isolate wireless stations on your network from each other. Wireless devices will be able to communicate with the Router but not with each other. To use this function, check this box. AP Isolation is disabled by default.

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.

5.6.5 Wireless Statistics

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

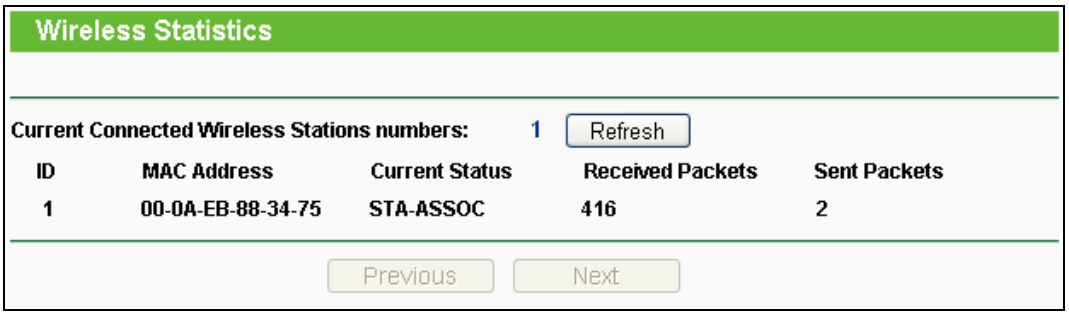


Figure 5-25 The Router attached wireless stations

- **MAC Address -** The connected wireless station's MAC address
- **Current Status -** The connected wireless station's running status, one of **STA-AUTH / STA-ASSOC / STA-JOINED / WPA / WPA-PSK / WPA2 / WPA2-PSK / AP-UP / AP-DOWN / Disconnected**.
- **Received Packets -** Packets received by the station
- **Sent Packets -** Packets sent by the station

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

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

Note:

This page will be refreshed automatically every 5 seconds.

5.7 DHCP

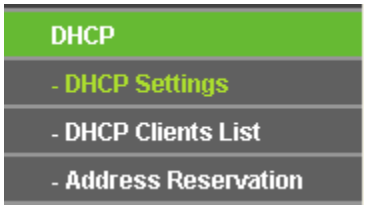


Figure 5-26 The DHCP menu

There are three submenus under the DHCP menu (shown in Figure 5-26): **DHCP Settings**, **DHCP Clients List** and **Address Reservation.** Click any of them, and you will be able to configure the corresponding function.

5.7.1 DHCP Settings

Choose menu "**DHCP→DHCP Settings**", and then you can configure the DHCP Server on the page (shown in Figure 5-27).The Router is set up by default as a DHCP (Dynamic Host Configuration Protocol) server, which provides the TCP/IP configuration for all the PC(s) that are connected to the Router on the LAN.

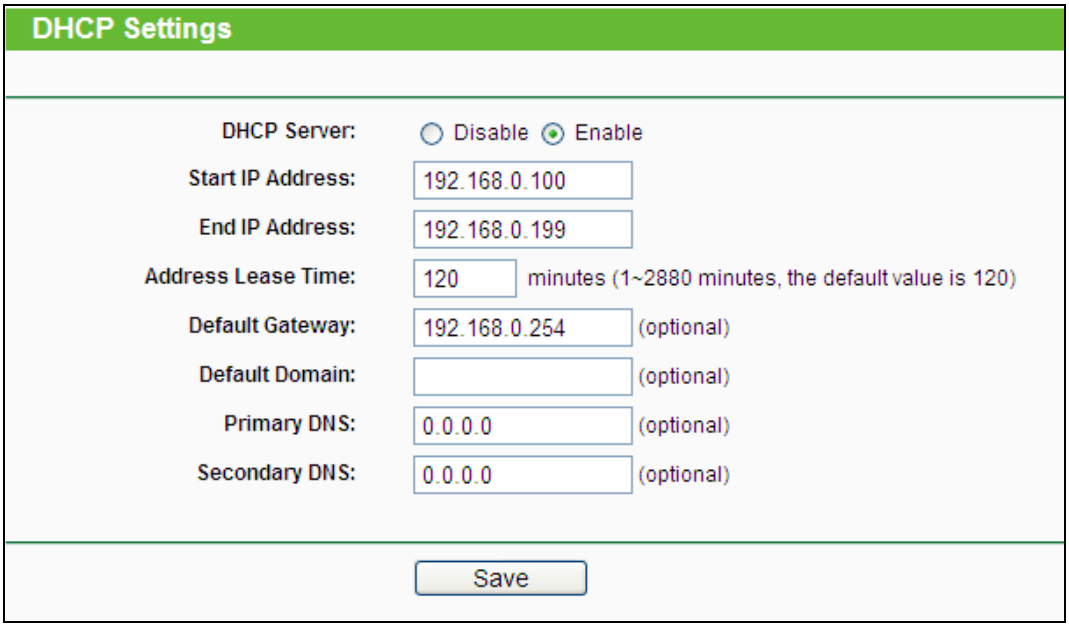


Figure 5-27 DHCP Settings

- **DHCP Server - Enable** or **Disable** the DHCP server. If you disable the Server, you must have another DHCP server within your network or else you must configure the computer manually.
- **Start IP Address -** Specify an IP address for the DHCP Server to start with when assigning IP addresses. 192.168.0.100 is the default start address.
- **End IP Address -** Specify an IP address for the DHCP Server to end with when assigning IP addresses. 192.168.0.199 is the default end address.

- **Address Lease Time -** The **Address Lease Time** is the amount of time a network user will be allowed connection to the Router with their current dynamic IP Address. Enter the amount of time in minutes and the user will be "leased" this dynamic IP Address. After the time is up, the user 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) Suggest to input the IP address of the LAN port of the Router, default value is 192.168.0.254.
- **Default Domain -** (Optional) Input the domain name of your network.
- **Primary DNS -** (Optional) Input the DNS IP address provided by your ISP. Or consult your ISP.
- **Secondary DNS -** (Optional) Input the IP address of another DNS server if your ISP provides two DNS servers.

Note:

To use the DHCP server function of the Router, you must configure all computers on the LAN as "Obtain an IP address automatically" mode.

5.7.2 DHCP Clients List

Choose menu "**DHCP→DHCP Clients List**", and then you can view the information about the clients attached to the Router in the next screen (shown in Figure 5-28).

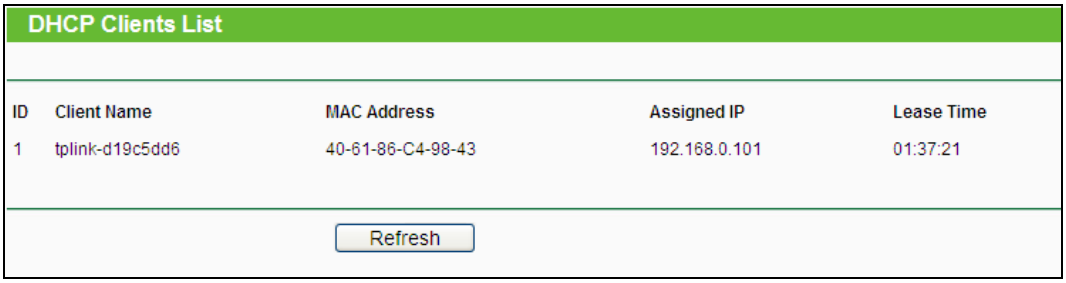


Figure 5-28 DHCP Clients List

- **ID -** The index of the DHCP Client.
- **Client Name -** The name of the DHCP client.
- **MAC Address -** The MAC address of the DHCP client.
- **Assigned IP -** The IP address that the Router has allocated to the DHCP client.
- **Lease Time -** The time of the DHCP client leased. After the dynamic IP address has expired, a new dynamic IP address will be automatically assigned to the user.

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

5.7.3 Address Reservation

Choose menu "**DHCP→Address Reservation**", and then you can view and add a reserved address for clients via the next screen (shown in Figure 5-29). When you specify a reserved IP address for a PC on the LAN, that PC will always receive the same IP address each time when it accesses the DHCP server. Reserved IP addresses should be assigned to the servers that require permanent IP settings.

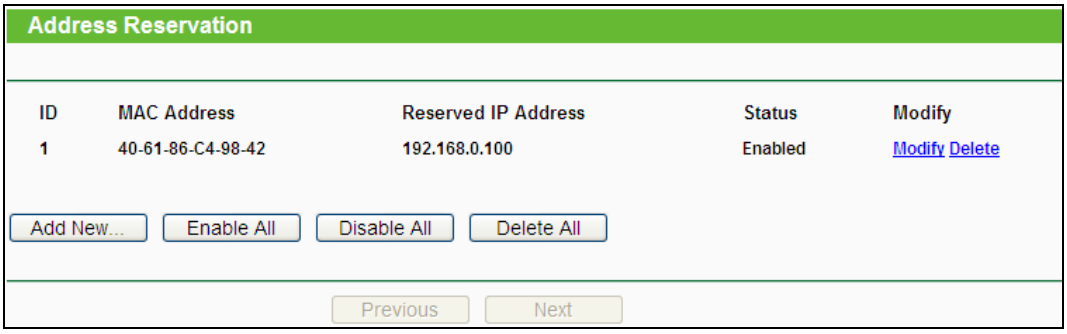


Figure 5-29 Address Reservation

- **MAC Address -** The MAC address of the PC for which you want to reserve IP address.
- **Assigned IP Address -** The IP address of the Router reserved.
- **Status -** The status of this entry, either **Enabled** or **Disabled**.

To Reserve IP addresses:

1. Click the **Add New …** button. (Pop-up Figure 5-30)
2. Enter the MAC address (in XX-XX-XX-XX-XX-XX format) and IP address of the computer you wish to add in dotted-decimal notation.
3. Click the **Save** button when finished.

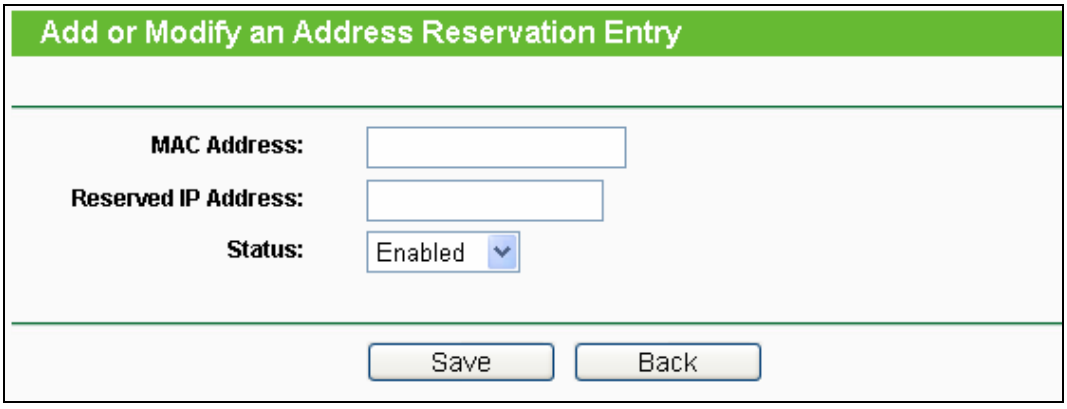


Figure 5-30 Add or Modify an Address Reservation Entry

To modify or delete an existing entry:

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

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

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

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

5.8 Forwarding

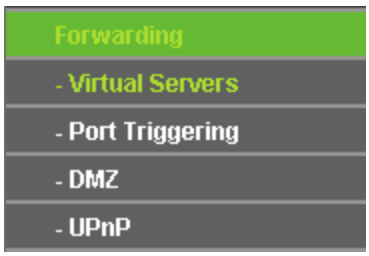


Figure 5-31 The Forwarding menu

There are four submenus under the Forwarding menu (shown in Figure 5-31): **Virtual Servers**, **Port Triggering**, **DMZ** and **UPnP**. Click any of them, and you will be able to configure the corresponding function.

5.8.1 Virtual Servers

Choose menu "**Forwarding→Virtual Servers**", and then you can view and add virtual servers in the next screen (shown in Figure 5-32). Virtual servers can be used for setting up public services on your LAN. A virtual server is defined as a service port, and all requests from Internet to this service port will be redirected to the computer specified by the server IP. Any PC that was used for a virtual server must have a static or reserved IP address because its IP address may change when using the DHCP function.

Figure 5-32 Virtual Servers

- **Service Port** - The numbers of External Service Ports. You can enter a service port or a range of service ports (the format is XXX – YYY; XXX is the Start port and 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 running 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, "Enabled" means the virtual server entry is enabled.
- **Common Service Port** - Some common services already exist in the drop-down list.
- **Modify** - To modify or delete an existing entry.

To setup a virtual server entry:

1. Click the **Add New...** button. (pop-up Figure 5-33)
2. Select the service you want to use from the **Common Service Port** list. If the **Common Service Port** menu does not list the service that you want to use, enter the number of the service port or service port range in the **Service Port** field.
3. Enter the IP address of the computer running the service application in the **IP Address** field.
4. Select the protocol used for this application in the **Protocol** drop-down list, either **TCP**, **UDP**, or **All**.
5. Select the **Enabled** option in the **Status** drop-down list.
6. Click the **Save** button.

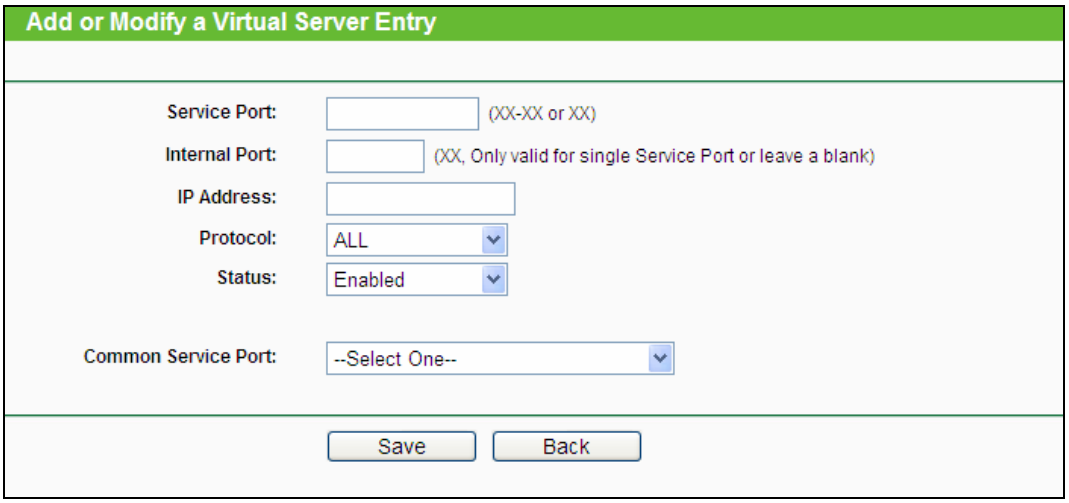


Figure 5-33 Add or Modify a Virtual Server Entry

Note:

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

To modify or delete an existing entry:

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

Click the **Enable/ Disable All** button to make all entries enabled/ disabled.
Click the **Delete All** button to delete all entries.
Click the **Next** button to go to the next page and click the **Previous** button to return to the previous page.

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

5.8.2 Port Triggering

Choose menu "**Forwarding→Port Triggering**", you can view and add port triggering in the next screen (shown in Figure 5-34). Some applications require multiple connections, like Internet games, video conferencing, Internet telephoning and so on. Port Triggering is used for some of these applications that cannot work with a pure NAT Router.

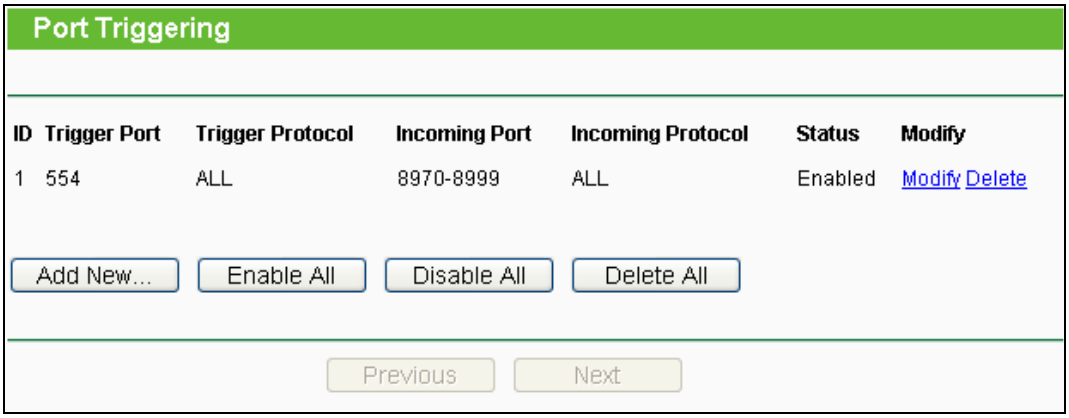


Figure 5-34 Port Triggering

To add a new rule, follow the steps below.

1. Click the **Add New…** button, the next screen will pop-up as shown in Figure 5-35.
2. Select a common application from the **Common Applications** drop-down list, then the **Trigger Port** field and the **Incoming Ports** field will be automatically filled. If the **Common Applications** do not have the application you need, enter the **Trigger Port** and the **Incoming Ports** manually.
3. Select the protocol used for Trigger Port from the **Trigger Protocol** drop-down list, either **TCP**, **UDP**, or **All**.
4. Select the protocol used for Incoming Ports from the **Incoming Protocol** drop-down list, either **TCP** or **UDP**, or **All.**

5. Select **Enable** in **Status** field.
6. Click the **Save** button to save the new rule.

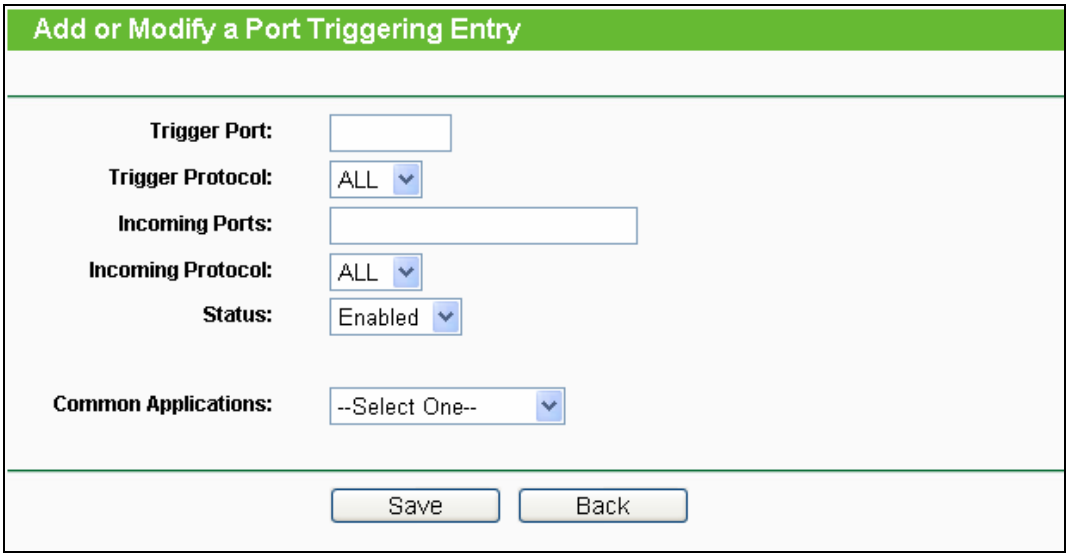


Figure 5-35 Add or Modify a Triggering Entry

- **Trigger Port** - The port for outgoing traffic. An outgoing connection using this port will trigger this rule.
- **Trigger Protocol** - The protocol used for Trigger Ports, either **TCP**, **UDP**, or **All** (all protocols supported by the Router).
- **Incoming Port** - 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 which triggered this rule. You can input at most 5 groups of ports (or port sections). Every group of ports must be separated with ",", for example, 2000-2038, 2046, 2050-2051, 2085, 3010-3030.
- **Incoming Protocol** - The protocol used for **Incoming Port**, either **TCP**, **UDP**, or **ALL** (all protocols supported by the Router).
- **Status** - The status of this entry, Enabled means the Port Triggering entry is enabled.
- **Modify** - To modify or delete an existing entry.
- **Common Applications** - Some popular applications already listed in the drop-down list of **Incoming Protocol**.

To modify or delete an existing entry:

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

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

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

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

Once the Router is configured, the 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.

Note:

1) When the trigger connection is released, the corresponding opened 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 Ports** ranges cannot overlap each other.

5.8.3 DMZ

Choose menu "**Forwarding→DMZ**", and then you can view and configure DMZ host in the screen (shown in Figure 5-36).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. The Router forwards packets of all services to the DMZ host. 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 be changed when using the DHCP function.

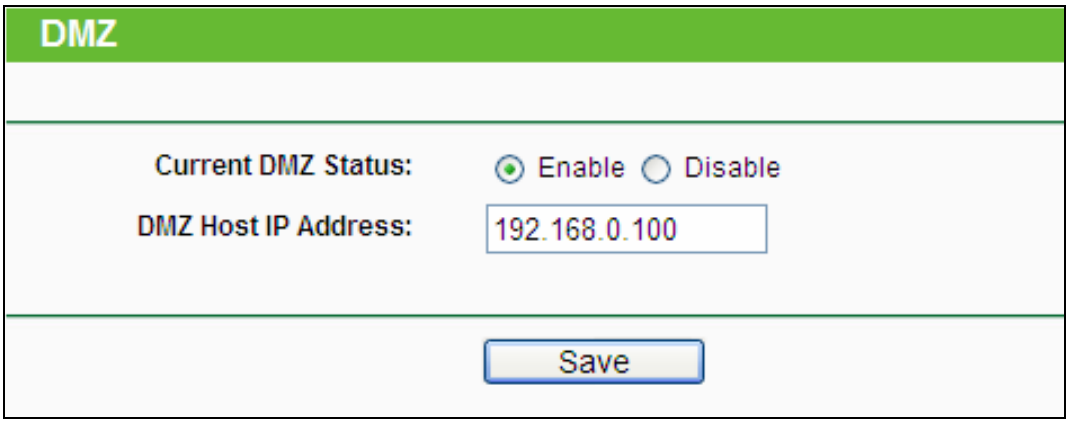


Figure 5-36 DMZ

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

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

5.8.4 UPnP

Choose menu "**Forwarding→UPnP**", and then you can view the information about **UPnP** in the screen (shown in Figure 5-37). 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.

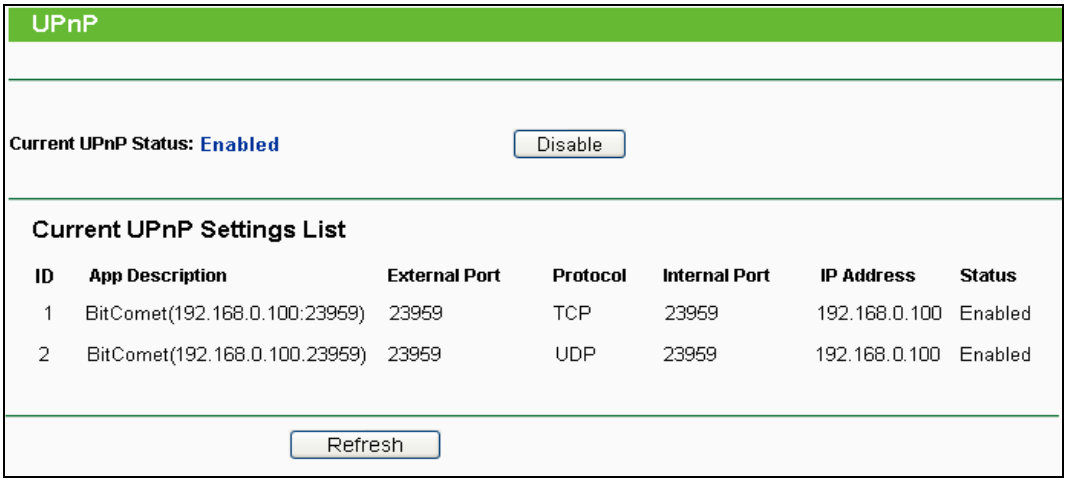


Figure 5-37 UPnP Setting

- **Current UPnP Status -** UPnP can be enabled or disabled by clicking the **Enable** or **Disable** button. This feature is enabled by default.
- **Current UPnP Settings List -** This table displays the current UPnP information.
  - **App Description** - The description about the application which initiates the UPnP request.
  - **External Port** - The port which the Router opened for the application.
  - **Protocol** - The type of protocol which is opened.
  - **Internal Port** - The 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 the port is still active; otherwise, the port is inactive.

Click the **Enable** button to enable UPnP.

Click the **Disable** button to disable UPnP.

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

5.9 Security

Figure 5-38 The Security menu

There are four submenus under the Security menu as shown in Figure 5-38: **Basic Security**, **Advanced Security**, **Local Management** and **Remote Management.** Click any of them, and you will be able to configure the corresponding function.

5.9.1 Basic Security

Choose menu "**Security → Basic Security**", and then you can configure the basic security in the screen as shown in Figure 5-39.

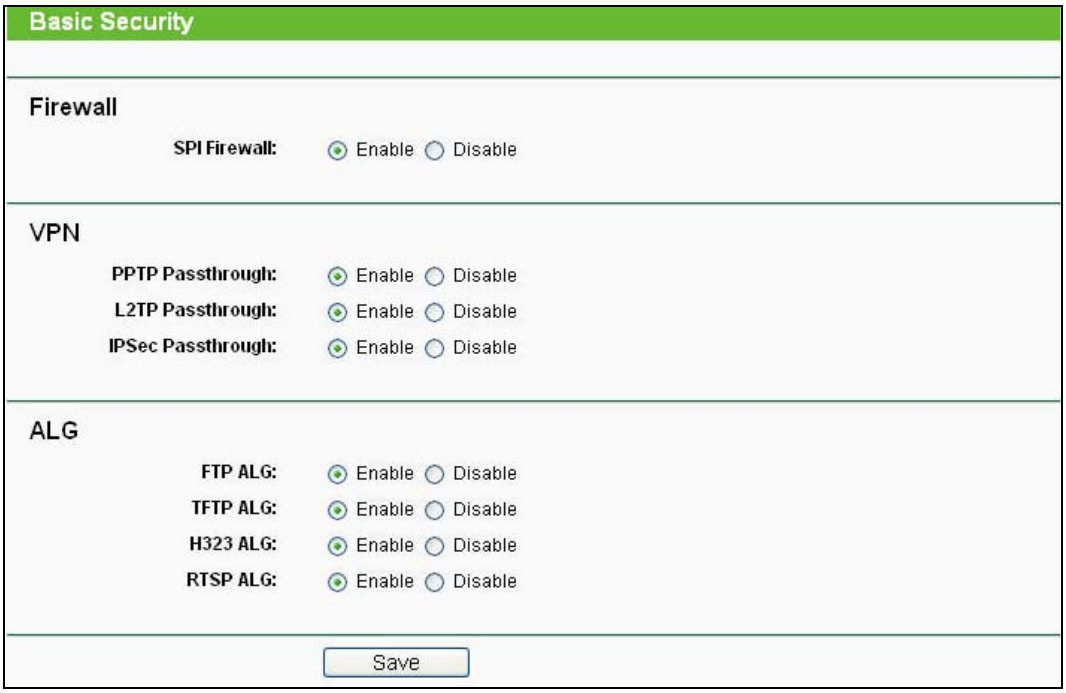


Figure 5-39 Basic Security

- **Firewall -** A firewall protects your network from the outside world. Here you can enable or disable the Router's firewall.

  - **SPI Firewall** - SPI (Stateful Packet Inspection, also known as dynamic packet filtering) 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 Router.

  - **PPTP Passthrough** - Point-to-Point Tunneling Protocol (PPTP) allows the Point-to-Point Protocol (PPP) to be tunneled through an IP network. To allow PPTP tunnels to pass through the Router, click **Enable**.
  - **L2TP Passthrough** - Layer Two Tunneling Protocol (L2TP) 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 Router, click **Enable**.
  - **IPSec Passthrough** - Internet Protocol security (IPSec) is a suite of protocols for ensuring private, secure communications over Internet Protocol (IP) networks, through the use of cryptographic security services. To allow IPSec tunnels to pass through the Router, 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**.
  - **RTSP ALG** - To allow some media player clients to communicate with some streaming media servers across NAT, click **Enable**.

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

5.9.2 Advanced Security

Choose menu "**Security → Advanced Security**", and then you can protect the Router from being attacked by TCP-SYN Flood, UDP Flood and ICMP-Flood in the screen as shown in Figure 5-40.

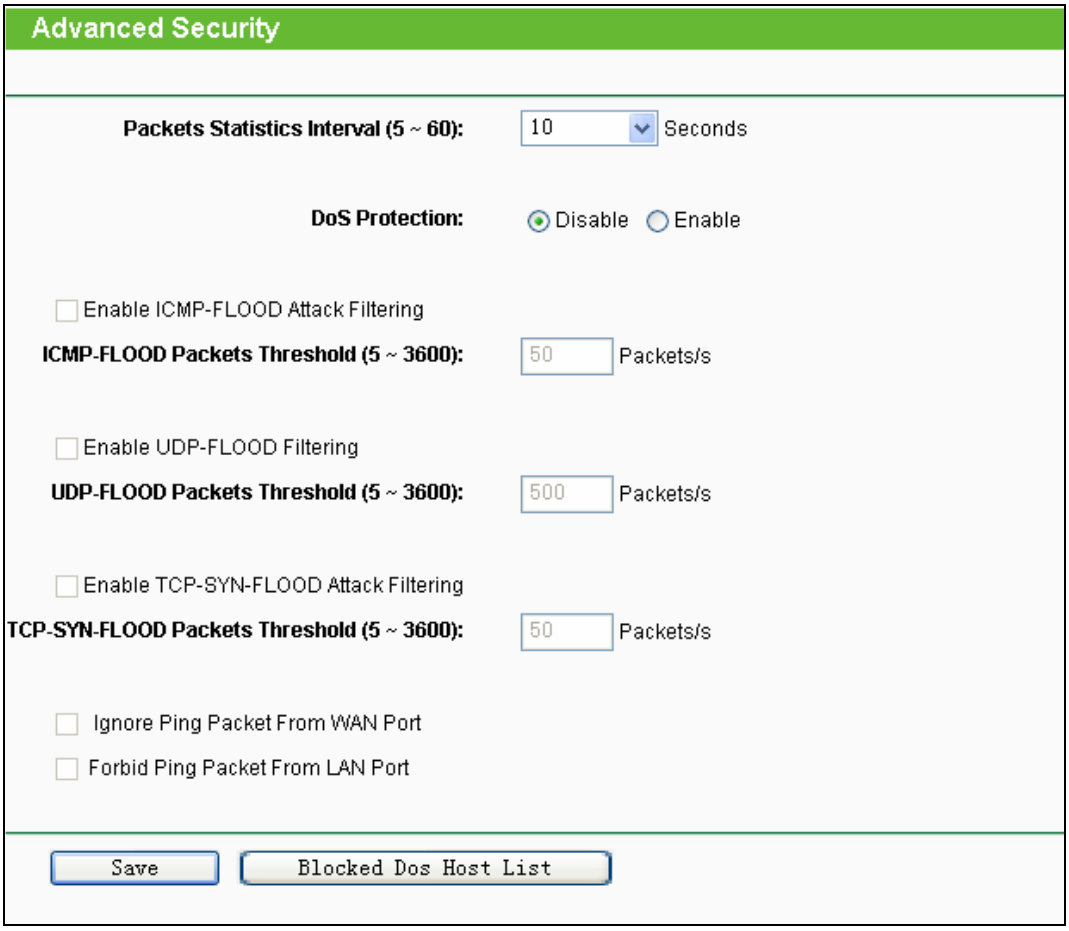


Figure 5-40 Advanced Security

- **Packets Statistics Interval (5~60) -** The default value is 10. Select a value between 5 and 60 seconds from the drop-down list. The Packets Statistics Interval value indicates the time section of the packets statistics. The result of the statistics is used for analysis by SYN Flood, UDP Flood and ICMP-Flood.
- **DoS Protection -** Denial of Service protection. Check the Enable or Disable button to enable or disable the DoS protection function. Only when it is enabled, will the flood filters be enabled.

Note:

Dos Protection will take effect only when the **Traffic Statistics** in "**System Tool → Traffic Statistics**" is 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 Router will startup 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 Router will startup 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 Router will startup 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 the Internet cannot access the Router.
- **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 Router. This function can be used to 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.

5.9.3 Local Management

Choose menu "**Security → Local Management**", and then you can configure the management rule in the screen as shown in Figure 5-41. The management feature allows you to deny computers in LAN from accessing the Router.

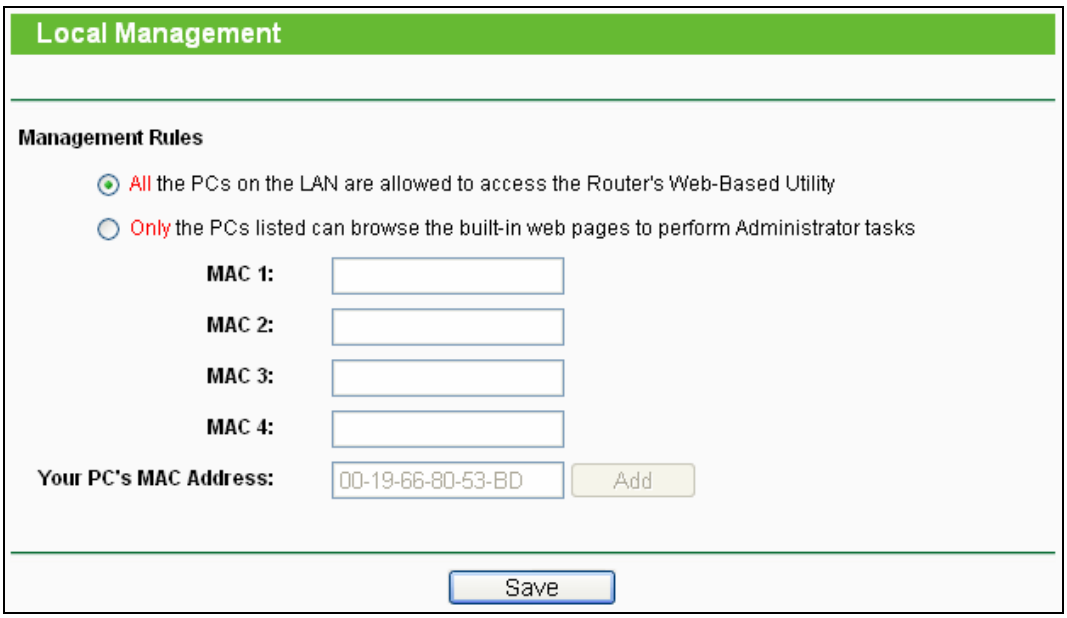


Figure 5-41 Local Management

By default, the radio button "**All the PCs on the LAN are allowed to access the Router's Web-Based Utility**" is checked. If you want to allow PCs with specific MAC Addresses to

access the Setup page of the Router's Web-Based Utility locally from inside the network, check 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 MAC address listed can use the password to browse the built-in web pages to perform Administrator tasks while all the others will be blocked.

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

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

☞ **Note:**

If your PC is blocked but you want to access the Router again, press and hold the **Reset Button** on the front panel for at least 10 seconds to reset the Router's factory defaults on the Router's Web-Based Utility.

5.9.4 Remote Management

Choose menu "**Security → Remote Management**", and then you can configure the Remote Management function in the screen as shown in Figure 5-42. This feature allows you to manage your Router from a remote location via the Internet.

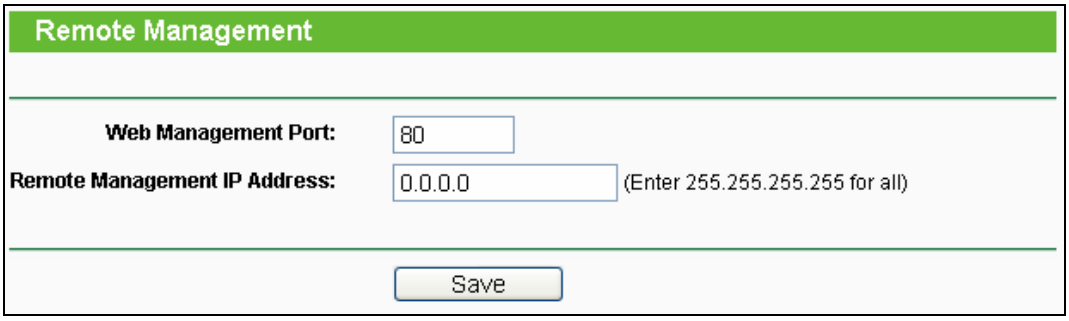


Figure 5-42 Remote Management

- **Web Management Port -** Web browser access normally uses the standard HTTP service port 80. This Router's default remote management web port number is 80. For greater security, you can change the remote management web port to a custom port by entering that number in the box provided. Choose a number between 1 and 65534 but do not use the number of any common service port.
- **Remote Management IP Address -** This is the current address you will use when accessing your Router from the Internet. This function is disabled when the IP address is set to the default value of 0.0.0.0. To enable this function change 0.0.0.0 to a valid IP address. If set to 255.255.255.255, then all the hosts can access the Router from internet.

☞ **Note:**

1) To access the Router, you should type your Router's WAN IP address into your browser's address (in IE) or Location (in Navigator) box, followed by a colon and the custom port number. For example, if your Router's WAN address is 202.96.12.8, and the port number

used is 8080, please enter http://202.96.12.8:8080 in your browser. Later, you may be asked for the Router's password. After successfully entering the username and password, you will be able to access the Router's web-based utility.

2) Be sure to change the Router's default password to a very secure password.

5.10 Parental Control

Choose menu "**Parental Control**", and then you can configure the parental control in the screen as shown in Figure 5-43. The Parental Control function can be used to control the internet activities of the child, limit the child to access certain websites and restrict the time of surfing.

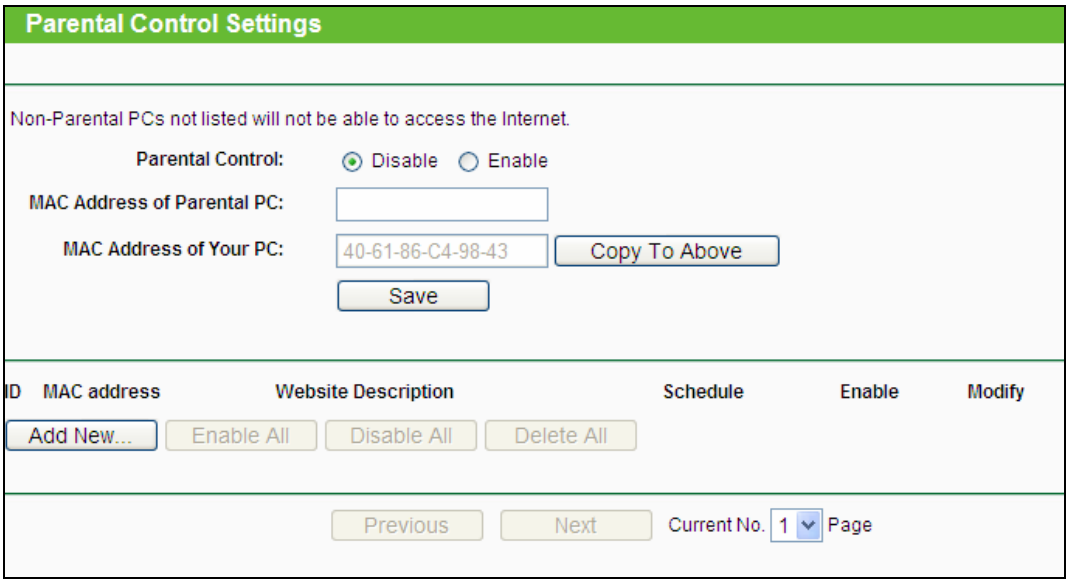


Figure 5-43 Parental Control Settings

To add a new entry, please follow the steps below.

1. Click the **Add New…** button and the next screen will pop-up as shown in Figure 5-44.

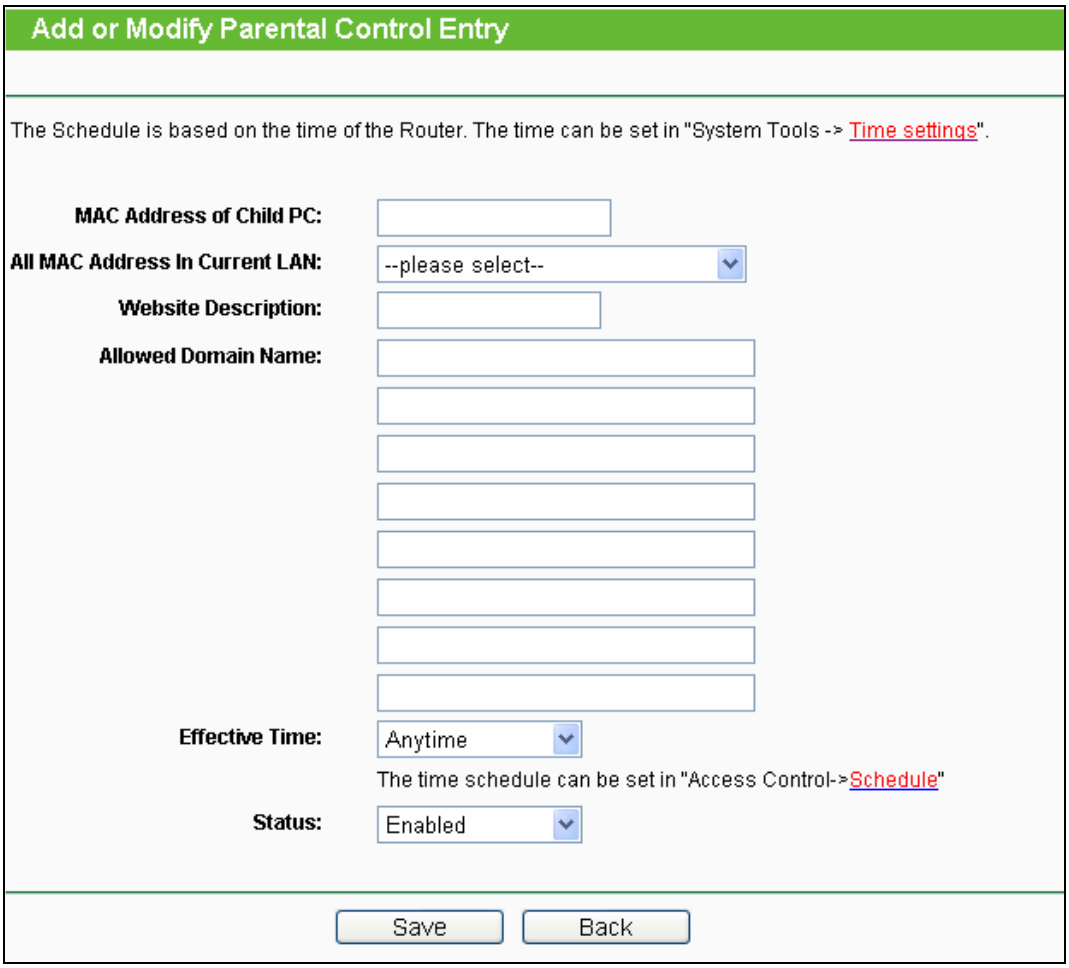


Figure 5-44 Add or Modify Parental Control Entry

- **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 Router. 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**".
- **Enable** - Check this option to enable a specific entry.
- **Modify -** Here you can edit or delete an existing entry.

2. Enter the MAC address of the PC (e.g. 00-11-22-33-44-AA) you'd like to control in the **MAC Address of Child PC** field, or you can choose the MAC address from the **All Address in Current LAN** drop-down list.
3. Give a description (e.g. Allow Google) for the website allowed to be accessed in the **Website Description** field.

4. Enter the allowed domain name of the website, either the full name or the keywords (e.g. google) in the **Allowed Domain Name** field. Any domain name with keywords in it (www.google.com, www.google.com.cn) will be allowed.
5. Select from the Effective Time drop-down list the schedule (e.g. Schedule_1) you want. If there are not suitable schedules for you, click the **Schedule** in red below to go to the Advance Schedule Settings page and create the schedule you need.
6. In the Status field, you can select **Enabled** or **Disabled** to enable or disable your entry.
7. Click the **Save** button.

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, or click the **Previous** button to return to the previous page.

For example: If you desire that the child 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 Add or Modify Parental Control Entry page:
   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.
4. Click **Save** to complete the settings.

   Then you will go back to the **Parental Control Settings** page and see the following list, as shown in Figure 5-45.

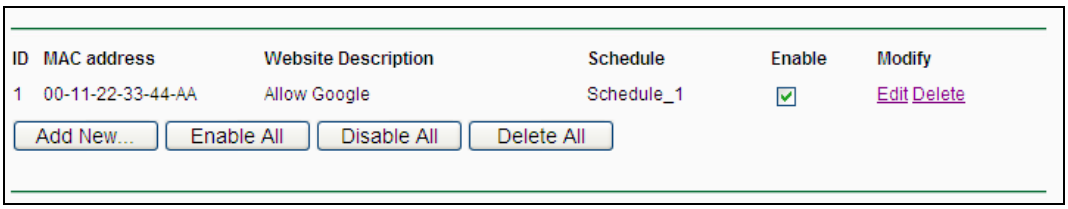


Figure 5-45 Parental Control Settings

5.11 Access Control

Figure 5-46 Access Control

There are four submenus under the Access Control menu as shown in Figure 5-46: **Rule**, **Host**, **Target** and **Schedule**. Click any of them, and you will be able to configure the corresponding function.

5.11.1 Rule

Choose menu "**Access Control** → **Rule**", and then you can view and set Access Control rules in the screen as shown in Figure 5-47.

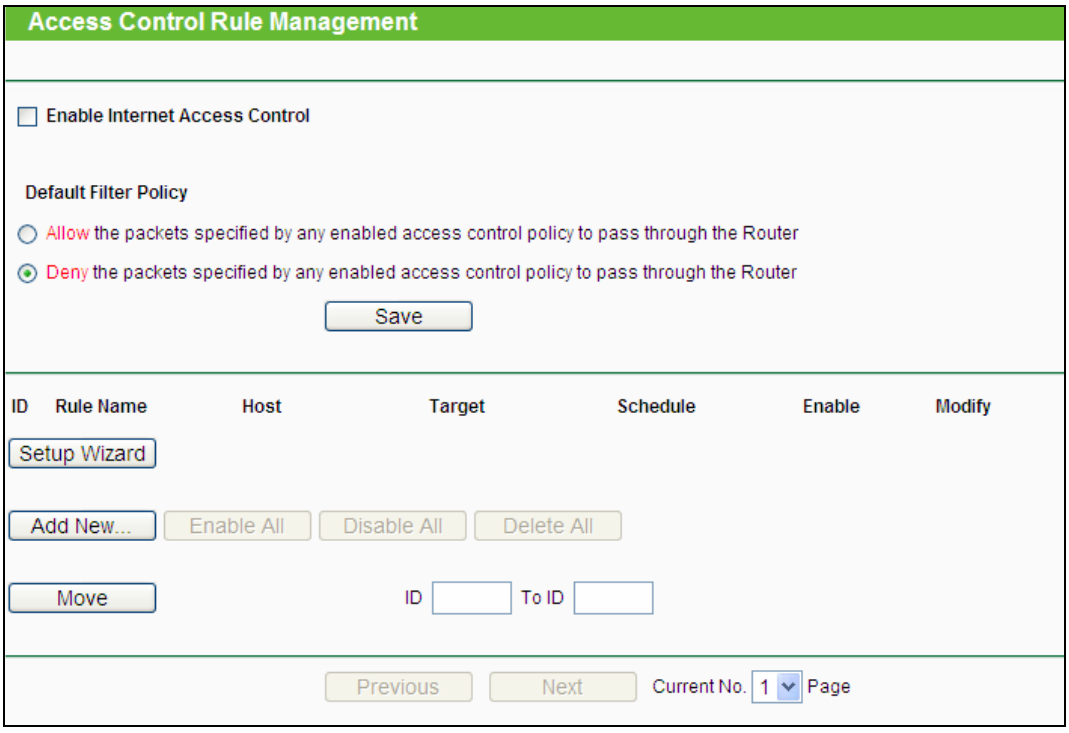


Figure 5-47 Access Control Rule Management

- **Enable Internet Access Control -** Select the check box to enable the Internet Access Control function, so 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.

- **Enable -** Here displays the status of the rule, enabled or not. Check this option to enable a specific entry.
- **Modify -** Here you can edit or delete an existing rule.
- **Setup Wizard -** Click the **Setup Wizard** button to create a new rule entry.
- **Add New... -** Click the **Add New...** button to add a new rule entry.
- **Enable All -** Click the **Enable All** button to enable all the rules in the list.
- **Disable All -** Click the **Disable All** button to disable all the rules in the list.
- **Delete All -** Click the **Delete All** button to delete all the entries in the table.
- **Move -** You can change the entry's order as desired. Enter in the first box the ID number of the entry you want to move and in the second box another ID number, and then click the **Move** button to change the entries' order.
- **Next -** Click the **Next** button to go to the next page.
- **Previous -** Click the **Previous** button to return to the previous page.

There are two methods to add a new rule.

Method One:

1. Click **Setup Wizard** button and the next screen will appear as shown in Figure 5-48.

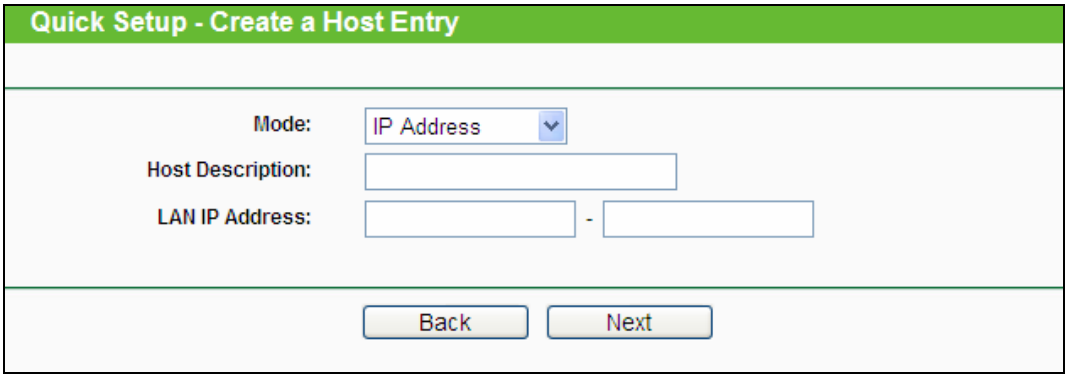


Figure 5-48 Quick Setup – Create a Host Entry

- **Host Description** - In this field, create a unique description for the host (e.g. Host_1).
- **Mode** - Here are two options, **IP Address** and **MAC Address**. You can select either of them from the drop-down list.

If the **IP Address** is selected, you can see the following item:

- **LAN IP Address** - Enter the IP address or address range of the host in dotted-decimal format (e.g. 192.168.0.23).

If the MAC Address is selected, you can see the following item:

- **MAC Address** - Enter the MAC address of the host in XX-XX-XX-XX-XX-XX format (e.g. 00-11-22-33-44-AA).

2. Click **Next** when finishing creating the host entry, and the next screen will appear as shown in Figure 5-49.

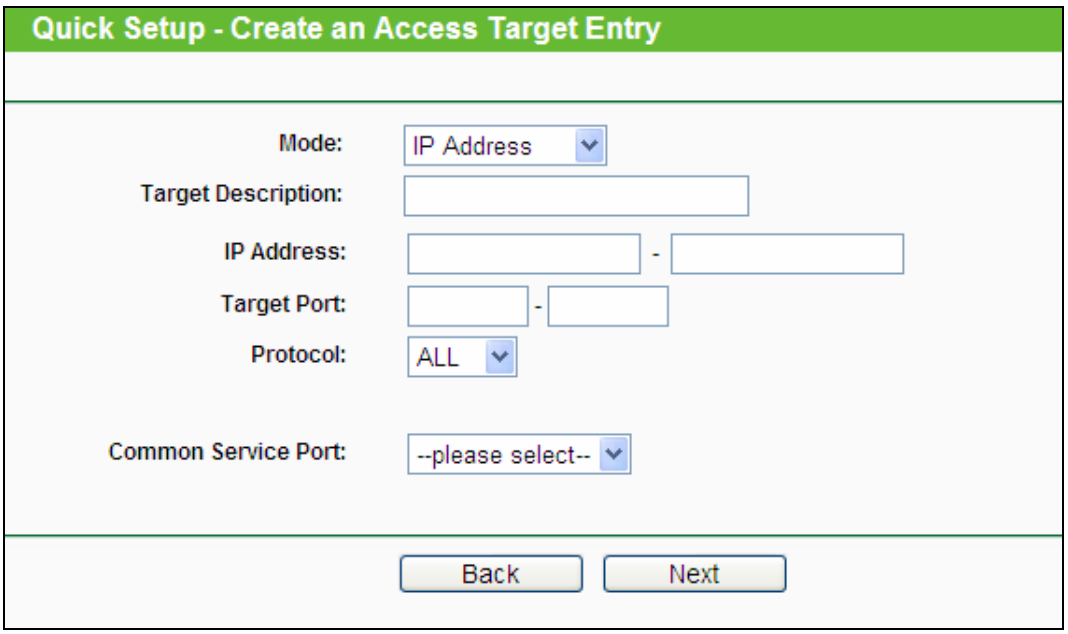


Figure 5-49 Quick Setup – Create an Access Target Entry

- **Target Description** - In this field, create a description for the target. Note that this description should be unique (e.g. Target_1).
- **Mode** - Here are two options, IP Address and Domain Name. You can choose either of them from the drop-down list.

If the **IP Address** is selected, you will see the following items:

- **IP Address** - Enter the IP address (or address range) of the target (targets) in dotted-decimal format (e.g. 192.168.0.23).
- **Target Port** - Specify the port or port range for the target. For some common service ports, you can make use of the Common Service Port item below.
- **Protocol** - Here are four options, All, TCP, UDP, and ICMP. Select one of them from the drop-down list for the target.
- **Common Service Port** - Here lists some common service ports. Select one from the drop-down list, and the corresponding port number will be filled in the Target Port field automatically. For example, if you select "FTP", "21" will be filled in the Target Port automatically.

If the **Domain Name** is selected, you will see the following items:

- **Domain Name** - Here you can enter 4 domain names, either the full name or the keywords (for example, google). Any domain name with keywords in it (www.google.com, www.google.hk) will be blocked or allowed.

3. Click **Next** when finishing creating the access target entry, and the next screen will appear as shown in Figure 4-51.

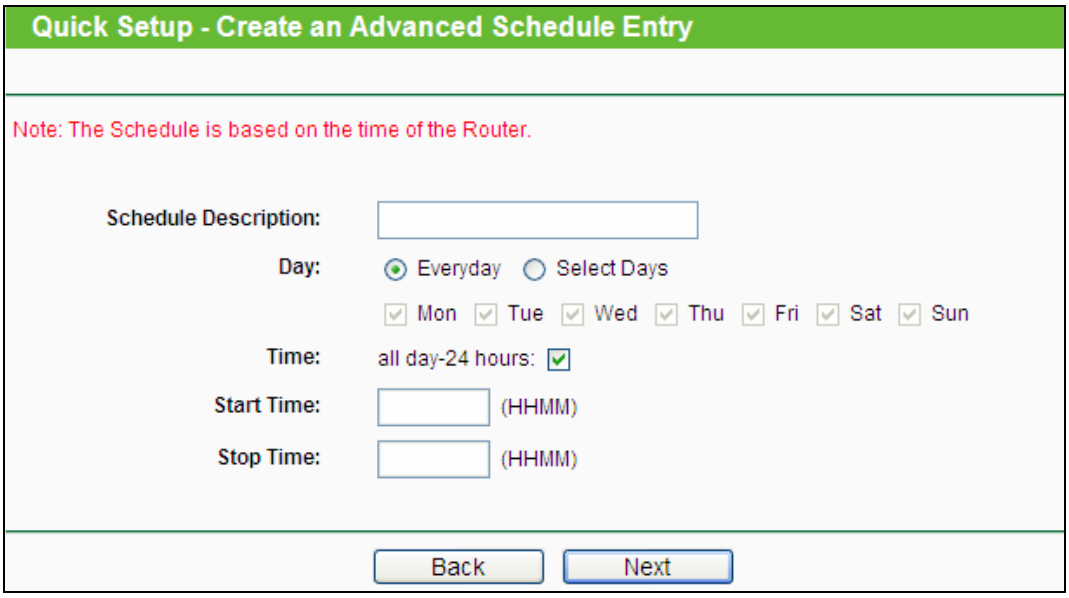


Figure 5-50 Quick Setup – Create an Advanced Schedule Entry

- **Schedule Description** - In this field, create a description for the schedule. Note that this description should be unique (e.g. Schedule_1).
- **Day** - Choose Select Days and select the certain day (days), or choose Everyday.
- **Time** - Select "24 hours", or specify the Start Time and Stop Time yourself.
- **Start Time** - Enter the start time in HHMM format (HHMM are 4 numbers). For example 0800 is 8:00.
- **Stop Time** - Enter the stop time in HHMM format (HHMM are 4 numbers). For example 2000 is 20:00.

4. Click **Next** when finishing creating the advanced schedule entry, and the next screen will appear as shown in Figure 4-52.

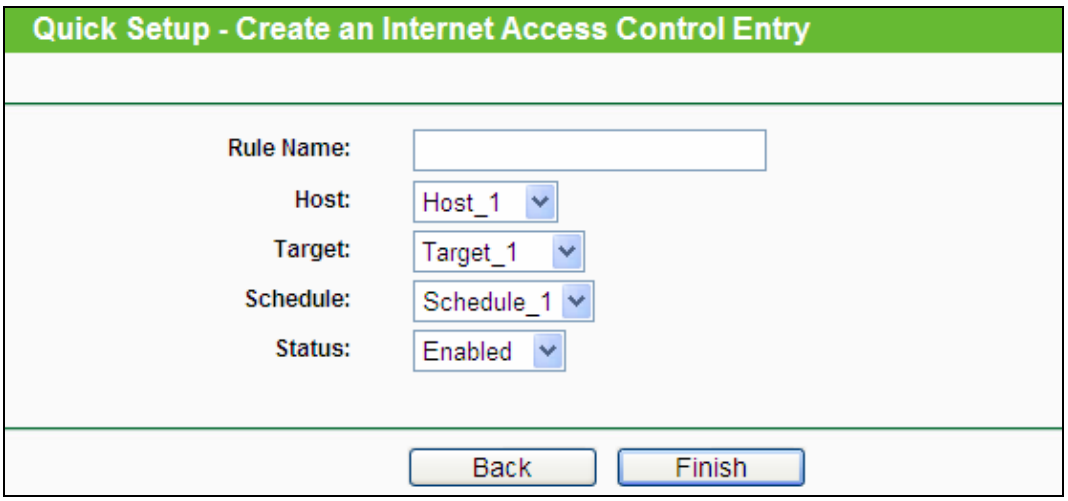


Figure 5-51 Quick Setup – Create an Internet Access Control Entry

- **Rule** - In this field, create a name for the rule. Note that this name should be unique (e.g. Rule_1).
- **Host** - In this field, select a host from the drop-down list for the rule. The default value is the **Host Description** you set just now.
- **Target** - In this filed, select a target from the drop-down list for the rule. The default value is the **Target Description** you set just now.
- **Schedule** - In this field, select a schedule from the drop-down list for the rule. The default value is the **Schedule Description** you set just now.
- **Status** - In this field, there are two options, **Enable** or **Disable**. Select **Enable** so that the rule will take effect. Select **Disable** so that the rule won't take effect.

5. Click **Finish** to complete adding a new rule.

Method Two:

1. Click the **Add New…** button and the next screen will pop up as shown in Figure 5-52.
2. Give a name (e.g. Rule_1) for the rule in the **Rule Name** field.
3. Select a host from the **Host** drop-down list or choose "**Click Here To Add New Host List**".
4. Select a target from the **Target** drop-sown list or choose "**Click Here To Add New Target List**".
5. Select a schedule from the **Schedule** drop-down list or choose "**Click Here To Add New Schedule**".
6. In the **Status** field, select **Enabled** or **Disabled** to enable or disable your entry.
7. Click the **Save** button.

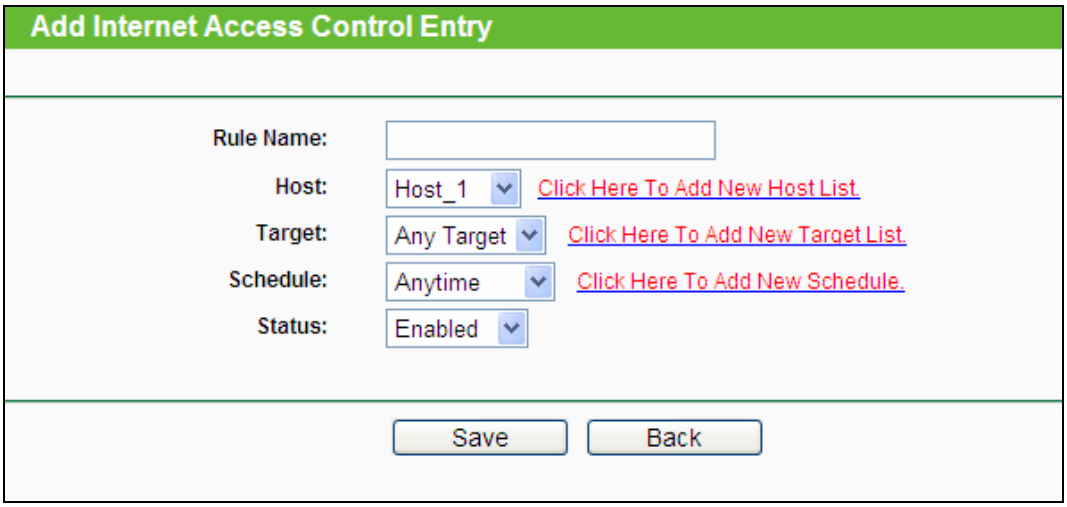


Figure 5-52 Add Internet Access Control Entry

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 Router".
2. We recommend that you click **Setup Wizard** button to finish all the following settings.
3. Click the submenu **Host of Access Control** in the left to enter the Host List page. Add a new entry with the Host Description is Host_1 and MAC Address is 00-11-22-33-44-AA.
4. Click the submenu **Target of Access Control** in the left to enter the Target List page. Add a new entry with the Target Description is Target_1 and Domain Name is www.google.com.
5. Click the submenu **Schedule of Access Control** in the left to enter the Schedule List page. Add a new entry with the Schedule Description is Schedule_1, Day is Sat and Sun, Start Time is 1800 and Stop Time is 2000.
6. Click the submenu **Rule of Access Control** in the left, Click **Add New...** button to add a new rule as follows:
   - In Rule Name field, create a name for the rule. Note that this name should be unique, for example Rule_1.
   - In Host field, select Host_1.
   - In Target field, select Target_1.
   - In Schedule field, select Schedule_1.
   - In Status field, select Enable.
   - Click Save to complete the settings.

Then you will go back to the Access Control Rule Management page and see the following list.

ID	Rule Name	Host	Target	Schedule	Enable	Modify
1	Rule_1	Host_1	Target_1	Schedule_1	☑	Edit Delete

5.11.2 Host

Choose menu "**Access Control → Host**", you can view and set a Host list in the screen as shown in Figure 5-53. The host list is necessary for the Access Control Rule.

Figure 5-53 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.

To add a new entry, please follow the steps below.

1. Click the **Add New…** button.
2. In the **Mode** field, select IP Address or MAC Address.
   - If you select IP Address, the screen shown is Figure 5-54.
     1) In **Host Description** field, create a unique description for the host (e.g. Host_1).
     2) In **LAN IP Address** field, enter the IP address.
   - If you select MAC Address, the screen shown is Figure 5-55.
     1) In **Host Description** field, create a unique description for the host (e.g. Host_1).
     2) In **MAC Address** field, enter the MAC address.
3. Click the **Save** button to complete the settings.

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

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

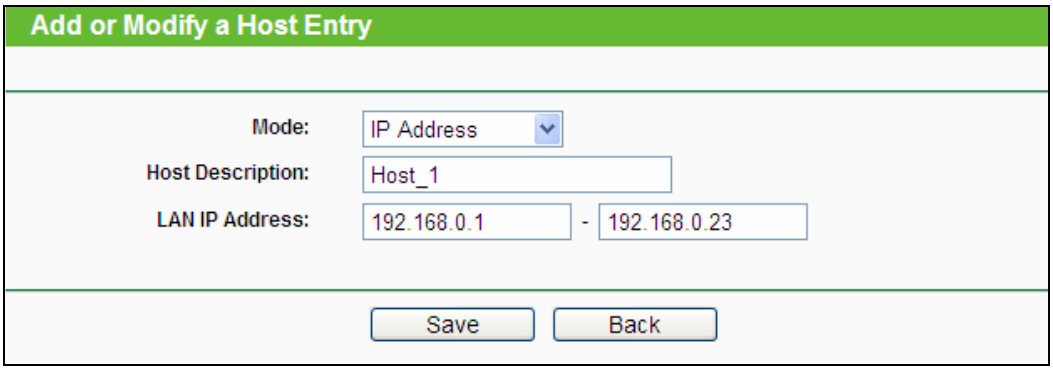


Figure 5-54 Add or Modify a Host Entry

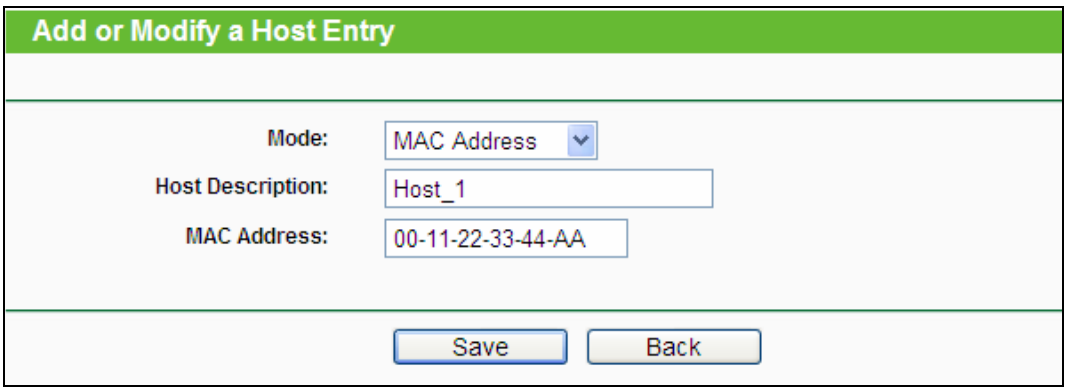


Figure 5-55 Add or Modify a Host Entry

For example: If you desire to restrict the internet activities of host with MAC address 00-11-22-33-44-AA, you should first follow the settings below:

1. Click **Add New...** button in Figure 5-53 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 Description** field, create a **unique** description for the host (e.g. Host_1).
4. In **MAC Address** field, enter 00-11-22-33-44-AA.

5. Click **Save** to complete the settings.

Then you will go back to the Host Settings page and see the following list.

ID	Host Description	Information	Modify
1	Host_1	MAC: 00-11-22-33-44-AA	Edit Delete

5.11.3 Target

Choose menu "**Access Control → Target**", you can view and set a Target list in the screen as shown in Figure 5-56. The target list is necessary for the Access Control Rule.

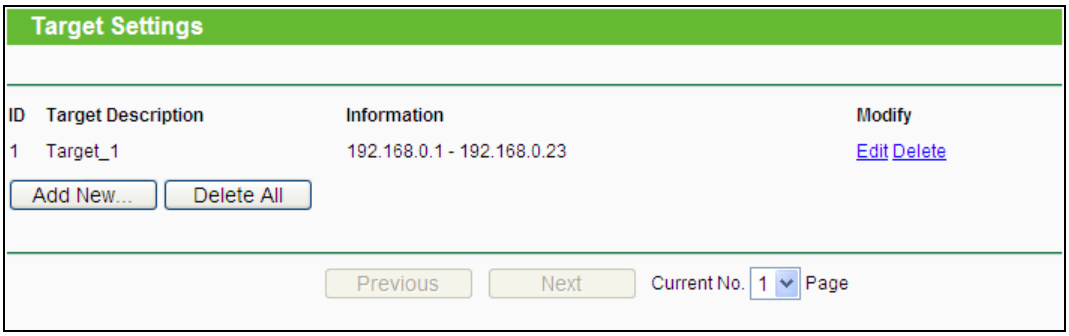


Figure 5-56 Target Settings

- **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.

To add a new entry, please follow the steps below.

1. Click the **Add New…** button.
2. In **Mode** field, select IP Address or Domain Name.
   - If you select **IP Address**, the screen shown is Figure 5-57.
     1) In **Target Description** field, create a unique description for the target (e.g. Target_1).
     2) In **IP Address** field, enter the IP address of the target.
     3) Select a common service from **Common Service Port** drop-down list, so that the **Target Port** will be automatically filled. If the **Common Service Port** drop-down list doesn't have the service you want, specify the **Target Port** manually.
     4) In **Protocol** field, select TCP, UDP, ICMP or ALL.
   - If you select **Domain Name**, the screen shown is Figure 5-58.
     1) In **Target Description** field, create a unique description for the target (e.g. Target_1).
     2) In **Domain Name** field, enter the domain name, either the full name or the keywords (for example google) in the blank. Any domain name with keywords in it (www.google.com, www.google.hk) will be blocked or allowed. You can enter 4 domain names.

3. Click the **Save** button.

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

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

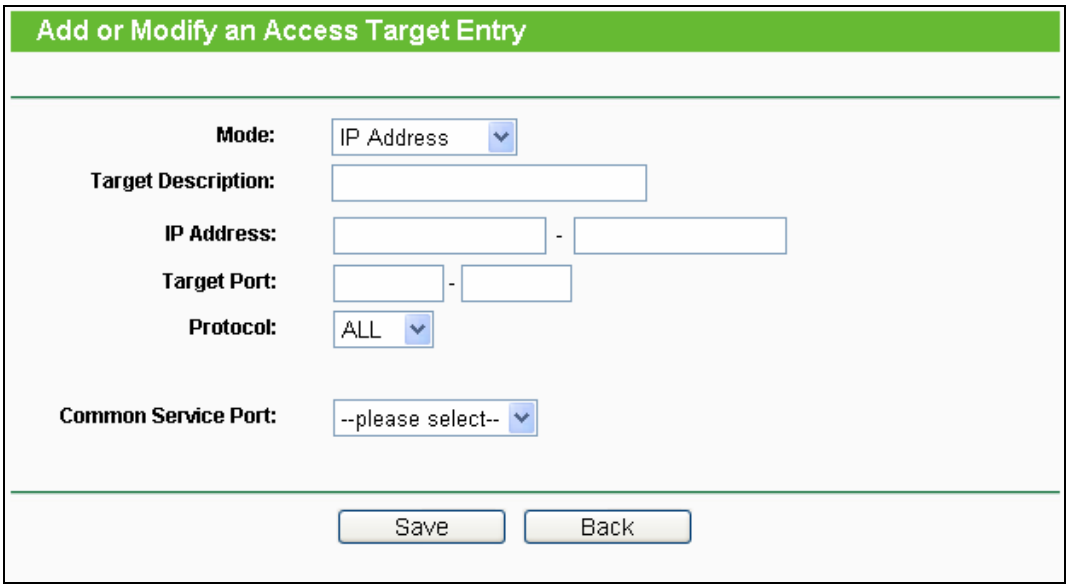


Figure 5-57 Add or Modify an Access Target Entry

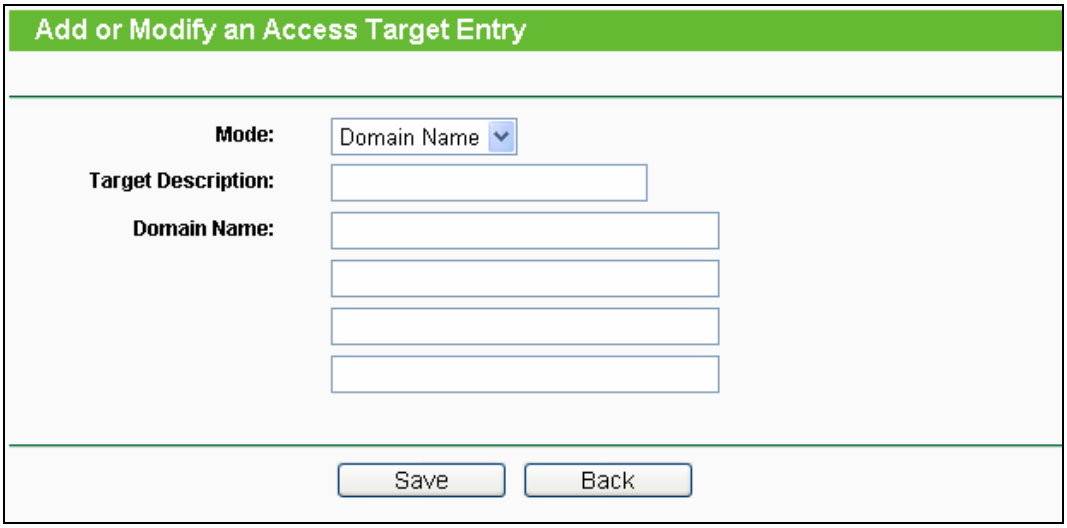


Figure 5-58 Add or Modify an Access Target Entry

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 in Figure 5-56 to enter the 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 (e.g. Target_1).
4. In **Domain Name** field, enter www.google.com.
5. Click **Save** to complete the settings.

Then you will go back to the Target Settings page and see the following list.

ID	Target Description	Information	Modify
1	Target_1	www.google.com	Edit Delete

5.11.4 Schedule

Choose menu "**Access Control → Schedule**", you can view and set a Schedule list in the next screen as shown in Figure 5-59. The Schedule list is necessary for the Access Control Rule.

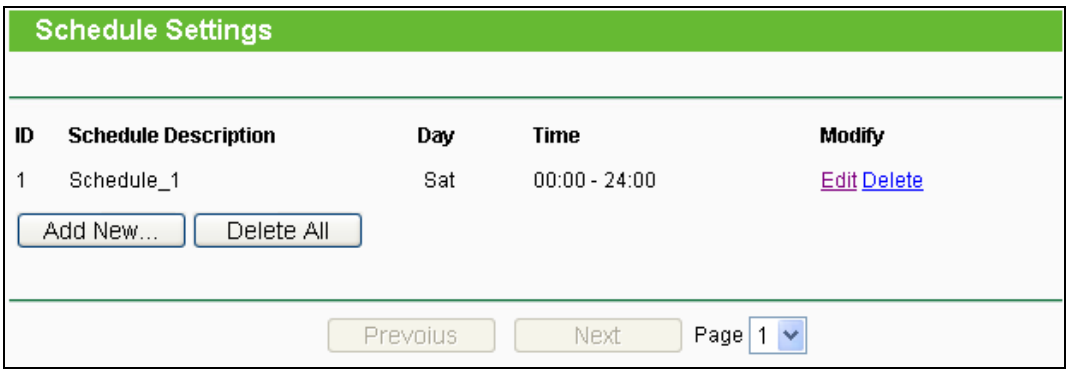


Figure 5-59 Schedule Settings

- **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.

To add a new schedule, follow the steps below.

1. Click **Add New...** button shown in Figure 5-59 and the next screen will pop-up as shown in Figure 5-60.
2. In **Schedule Description** field, create a unique description for the schedule (e.g. Schedule_1).
3. In **Day** field, select the day or days you need.
4. In **Time** field, you can select all day-24 hours or you may enter the Start Time and Stop Time in the corresponding field.
5. Click **Save** to complete the settings.

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

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

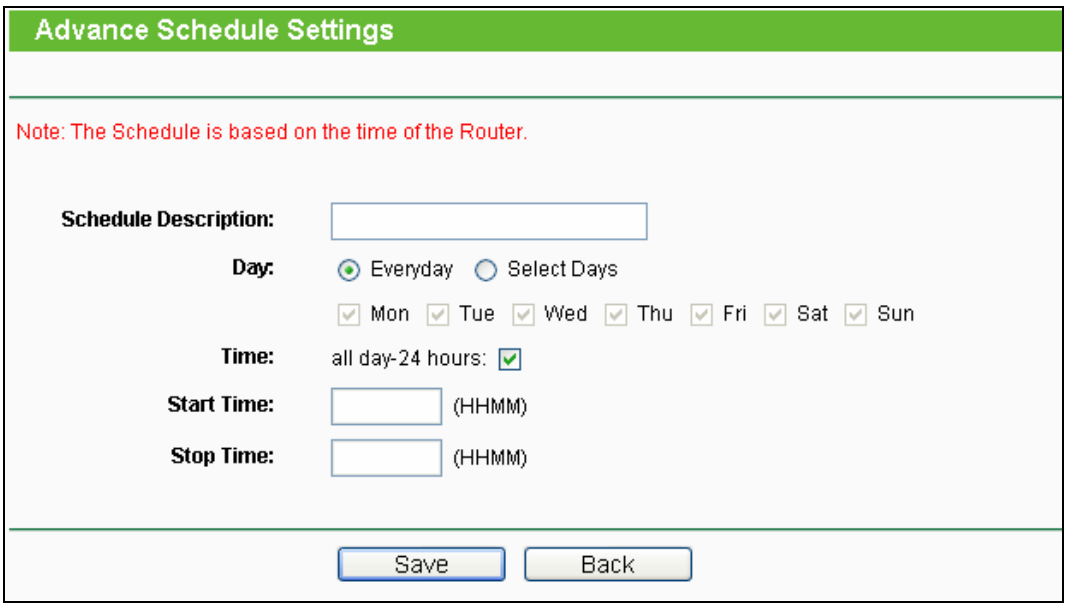


Figure 5-60 Advanced Schedule Settings

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 shown in Figure 5-59 to enter the Advanced Schedule Settings page.
2. In **Schedule Description** field, create a unique description for the schedule (e.g. Schedule_1).
3. In **Day** field, check the Select Days radio button and then select Sat and Sun.
4. In **Time** field, enter 1800 in Start Time field and 2000 in Stop Time field.
5. Click **Save** to complete the settings.

Then you will go back to the Schedule Settings page and see the following list.

ID	Schedule Description	Day	Time	Modify
1	Schedule_1	Sat Sun	18:00 - 20:00	Edit Delete

5.12 Advanced Routing

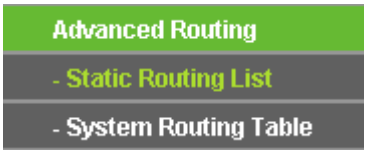


Figure 5-61 Advanced Routing

There are two submenus under the Advanced Routing menu as shown in Figure 5-61: **Static Routing List** and **System Routing Table**. Click any of them, and you will be able to configure the corresponding function.

5.12.1 Static Routing List

Choose menu "**Advanced Routing → Static Routing List**", and then you can configure the static route in the next screen (shown in Figure 5-62). A static route is a pre-determined path that network information must travel to reach a specific host or network.

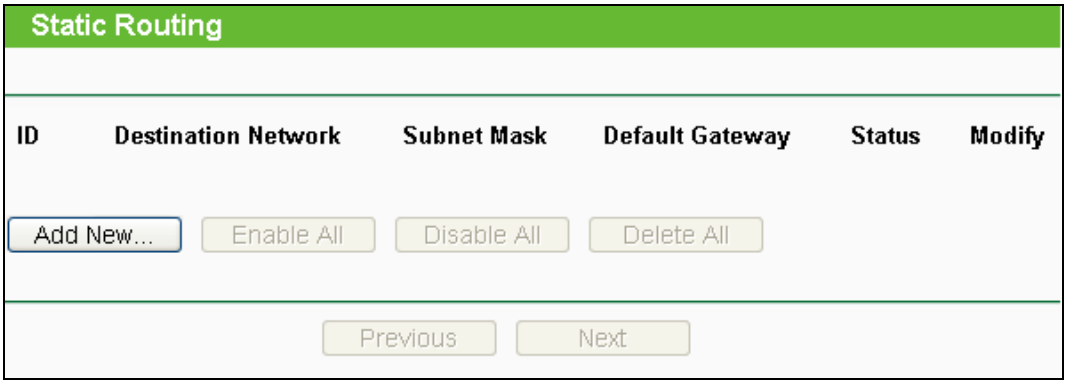


Figure 5-62 Static Routing

To add static routing entries:

1. Click **Add New…** shown in Figure 5-63, you will see the following screen.

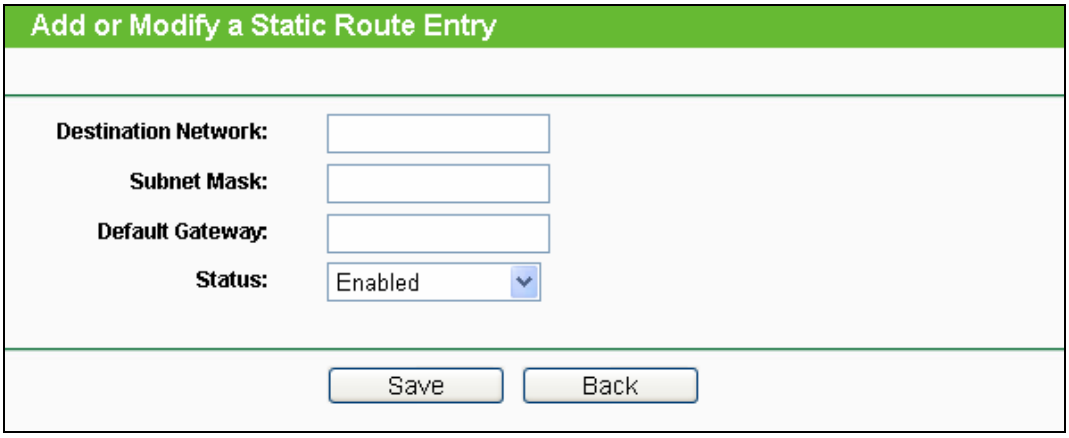


Figure 5-63 Add or Modify a Static Route Entry

2. Enter the following data:

   - **Destination Network** - The Destination Network is the address of the network or host that you want to assign to a static route.
   - **Subnet Mask -** The **Subnet Mask** determines which portion of an IP Address is the network portion, and which portion is the host portion.
   - **Default Gateway** - This is the IP Address of the gateway device that allows for contact between the Router and the network or host.

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

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

Other configurations for the entries:

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

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

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

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

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

5.12.2 System Routing Table

Choose menu "**Advanced Routing → System Routing Table**", and then you can view the System Routing Table in the next screen (shown in Figure 5-64). System routing table views all of the valid route entries in use. The Destination IP address, Subnet Mask, Gateway, and Interface will be displayed for each entry.

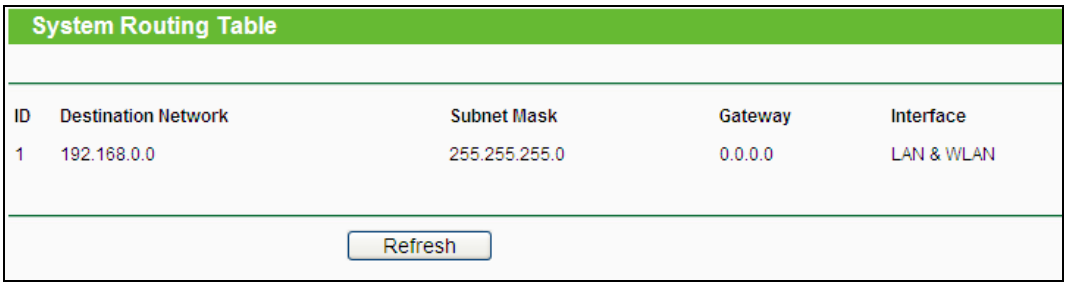


Figure 5-64 System Routing Table

- **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 Router and the network or host.
- **Interface** - This interface tells you either the Destination IP Address is on the **LAN & WLAN** (internal wired and wireless networks), or on the **WAN** (Internet).

5.13 Bandwidth Control

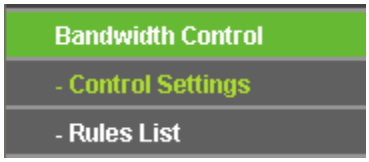


Figure 5-65 Bandwidth Control

There are two submenus under the Bandwidth Control menu as shown in Figure 5-65: **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.

5.13.1 Control Settings

Choose menu "**Bandwidth Control → Control Settings**", and then you can configure the Egress Bandwidth and Ingress Bandwidth in the next screen. Their values you configure should be less than 100000Kbps. For optimal control of the bandwidth, please select the right Line Type and ask your ISP for the total bandwidth of the egress and ingress.

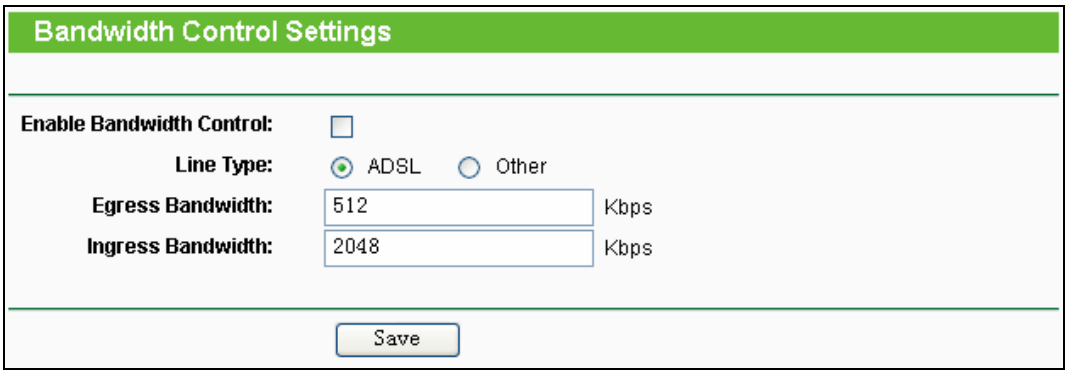


Figure 5-66 Bandwidth Control Settings

- **Enable Bandwidth Control -** Check this box so that the Bandwidth Control settings can take effect.
- **Line Type -** Select the right type for you network connection. If you don't know how to choose, please ask your ISP for the information.
- **Egress Bandwidth** - The upload speed through the WAN port.
- **Ingress Bandwidth -** The download speed through the WAN port.

5.13.2 Rules List

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

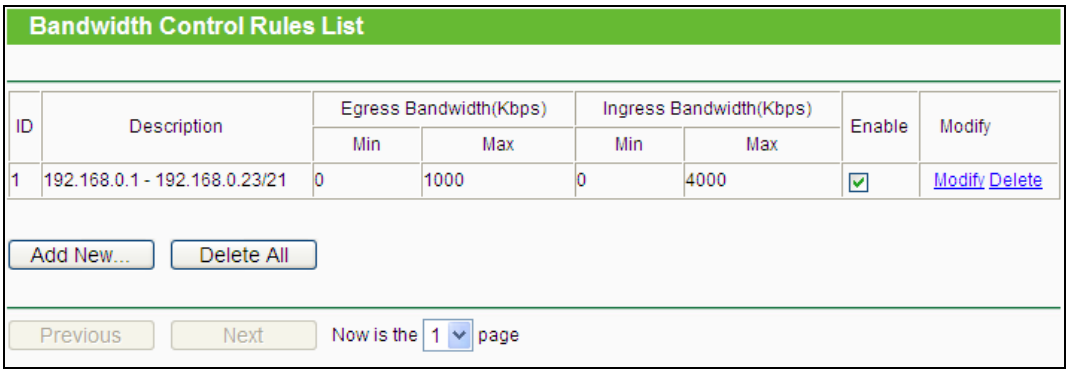


Figure 5-67 Bandwidth Control Rules List

- **Description -** This is the information about the rules such as address range.

- **Egress bandwidth -** This field displays the max and mix upload bandwidth through the WAN port, the default is 0.
- **Ingress bandwidth -** This field displays the max and mix download bandwidth through the WAN port, the default is 0.
- **Enable -** This displays the status of the rule.
- **Modify -** Click **Modify** to edit the rule. Click **Delete** to delete the rule.

To add/modify a Bandwidth Control rule, follow the steps below.

1. Click **Add New…** shown in Figure 5-67, you will see a new screen shown in Figure 5-68.
2. Enter the information like the screen shown below.

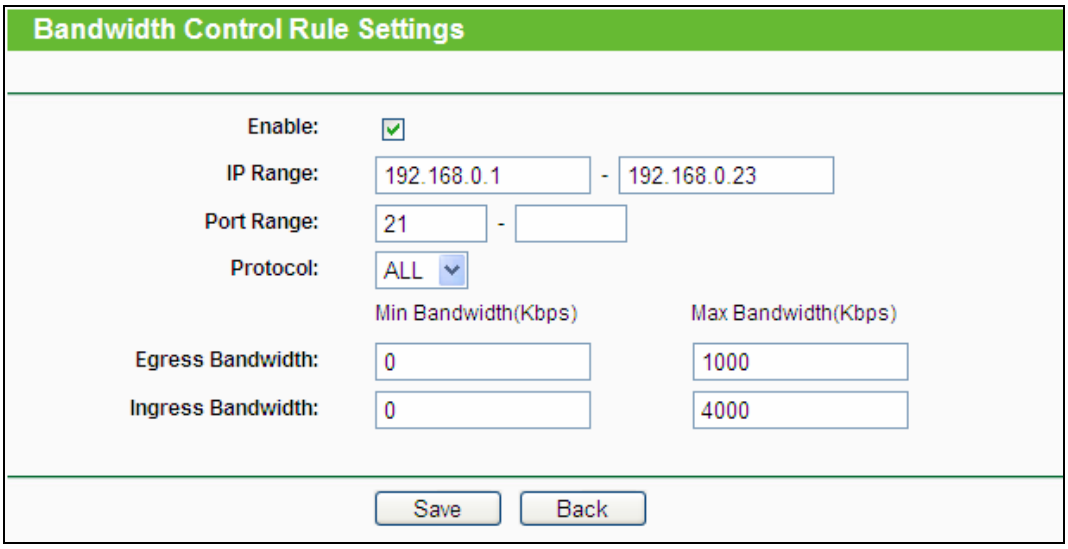


Figure 5-68 Bandwidth Control Rule Settings

3. Click the **Save** button.

5.14 IP & MAC Binding Setting

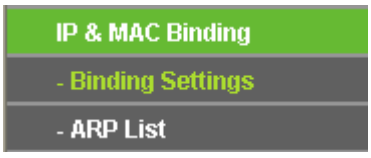


Figure 5-69 the IP & MAC Binding menu

There are two submenus under the IP &MAC Binding menu (shown in Figure 5-69): **Binding Settings** and **ARP List**. Click any of them, and you will be able to scan or configure the corresponding function. The detailed explanations for each submenu are provided below.

5.14.1 Binding Settings

This page displays the **IP & MAC Binding Setting** table; you can operate it in accord with your desire (shown in Figure 5-70).

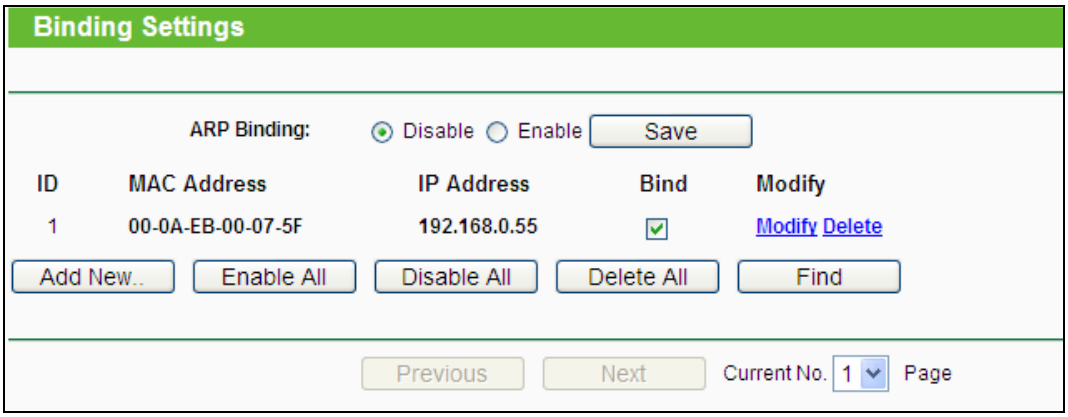


Figure 5-70 Binding Setting

- **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 5-71).

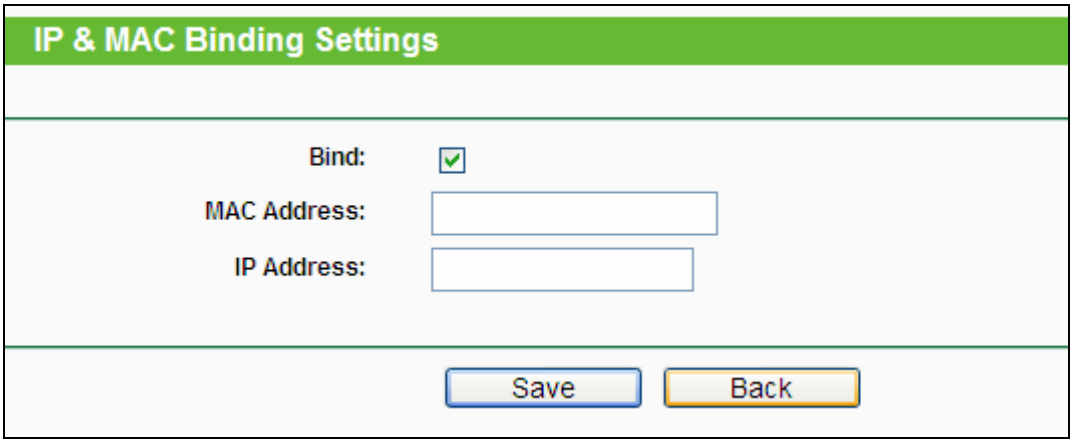


Figure 5-71 IP & MAC Binding Setting (Add & Modify)

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

1. Click the **Add New...** button as shown in Figure 5-70.
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 5-70.
2. Enter the MAC Address or IP Address.
3. Click the **Find** button in the page as shown in Figure 5-72.

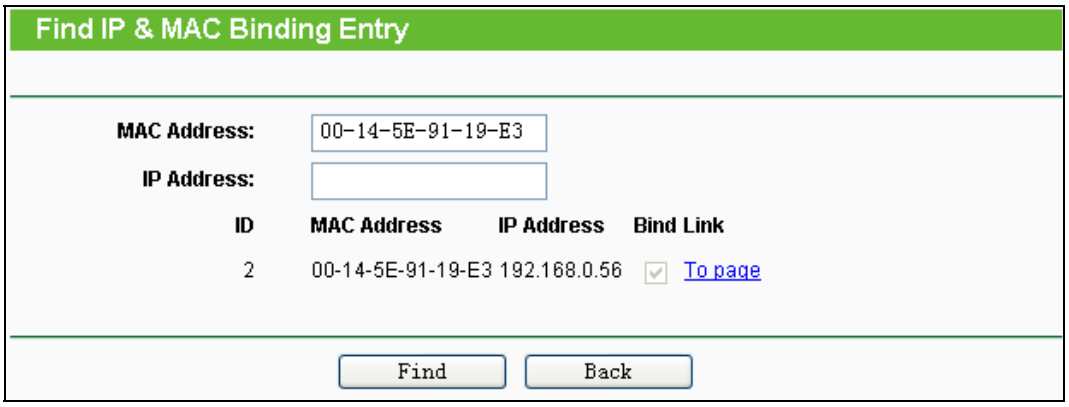


Figure 5-72 Find IP & MAC Binding Entry

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

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

5.14.2 ARP List

To manage the computer, you could observe the computers in the LAN by checking the relationship of MAC address and IP address on the ARP list, and you could also configure the items on the ARP list. This page displays the ARP List; it shows all the existing IP & MAC Binding entries (shown in Figure 5-73).

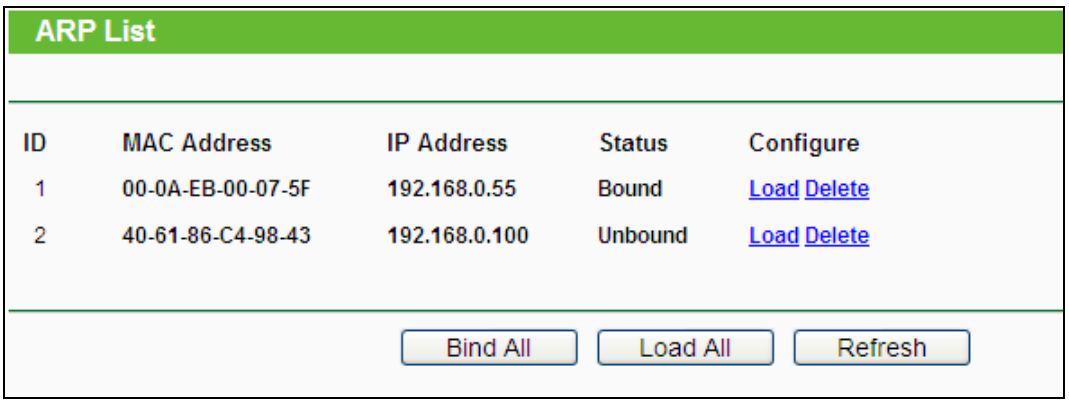


Figure 5-73 ARP List

1. **MAC Address -** The MAC address of the controlled computer in the LAN.
2. **IP Address -** The assigned IP address of the controlled computer in the LAN.
3. **Status -** Indicates whether or not the MAC and IP addresses are bound.
4. **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.

5.15 Dynamic DNS

Choose menu "**Dynamic DNS**", and you can configure the Dynamic DNS function.

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

5.15.1 Comexe.cn DDNS

If the dynamic DNS **Service Provider** you select is www.comexe.cn, the page will appear as shown in Figure 5-74.

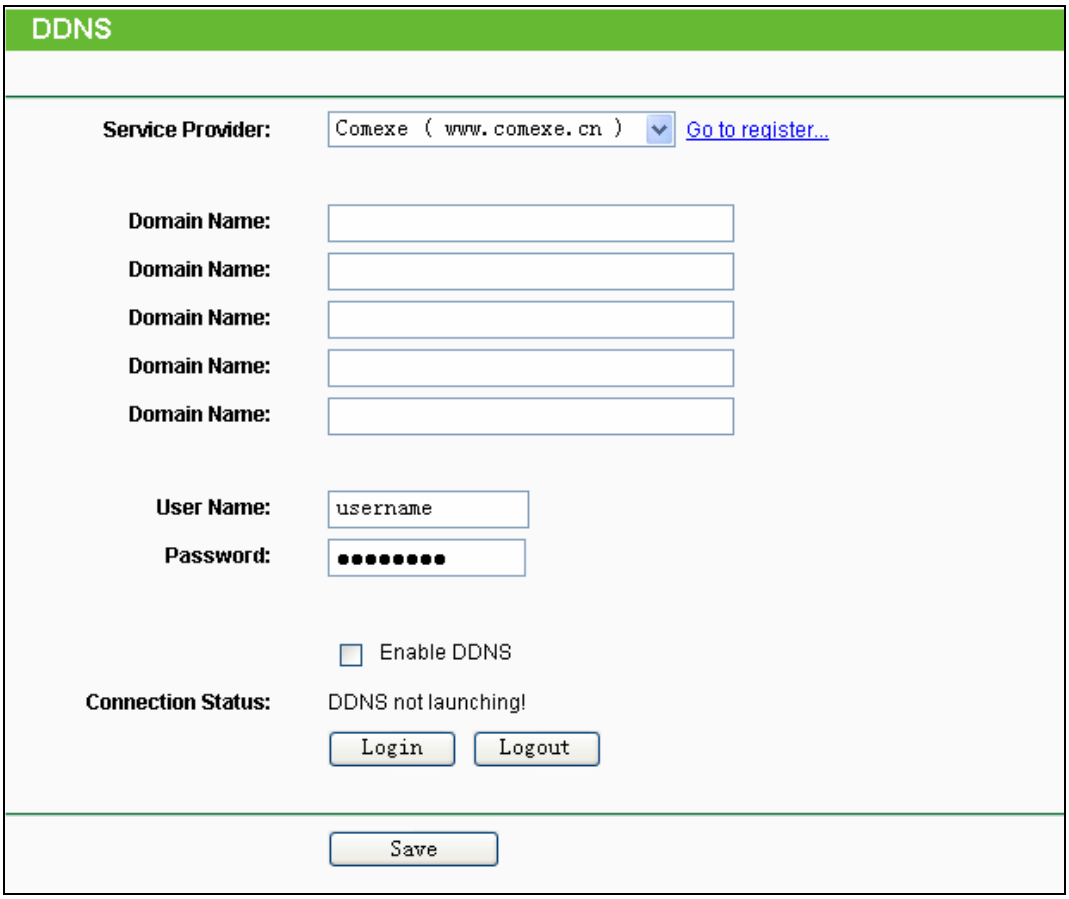


Figure 5-74 Comexe.cn DDNS Settings

To set up for DDNS, follow these instructions:

1. Enter the **Domain Name** 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 log out 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.

5.15.2 Dyndns.org DDNS

If the dynamic DNS **Service Provider** you select is www.dyndns.org, the page will appear as shown in Figure 5-75.

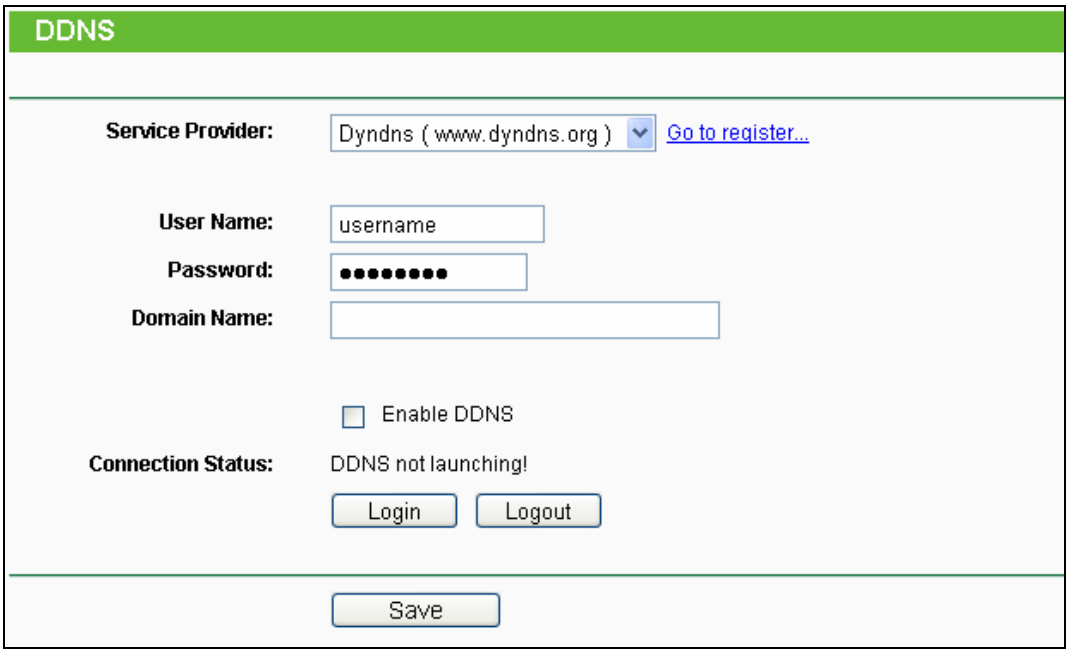


Figure 5-75 Dyndns.org DDNS Settings

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.

5.15.3 No-ip.com DDNS

If the dynamic DNS **Service Provider** you select is www.no-ip.com, the page will appear as shown in Figure 5-76.

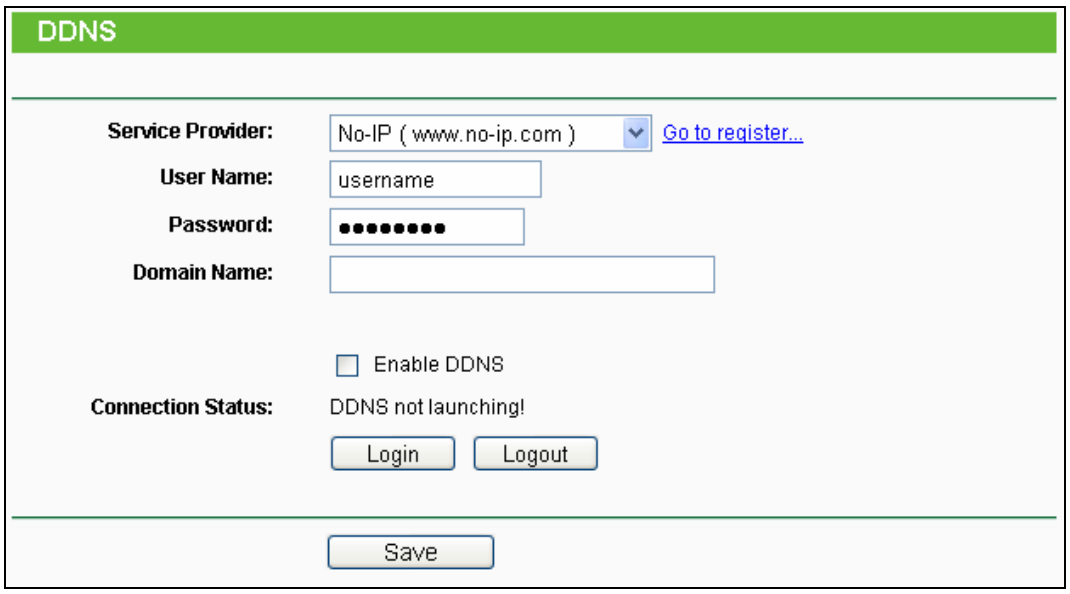


Figure 5-76 No-ip.com DDNS Settings

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 log out 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.

5.16 System Tools

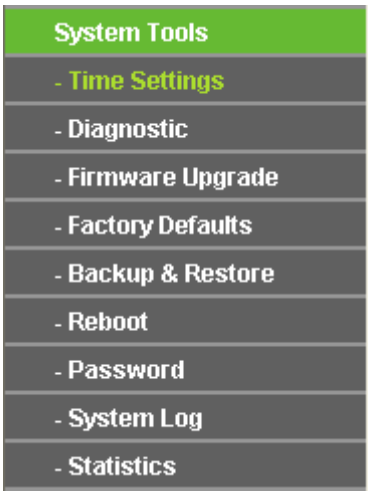


Figure 5-77 The System Tools menu

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

5.16.1 Time Setting

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

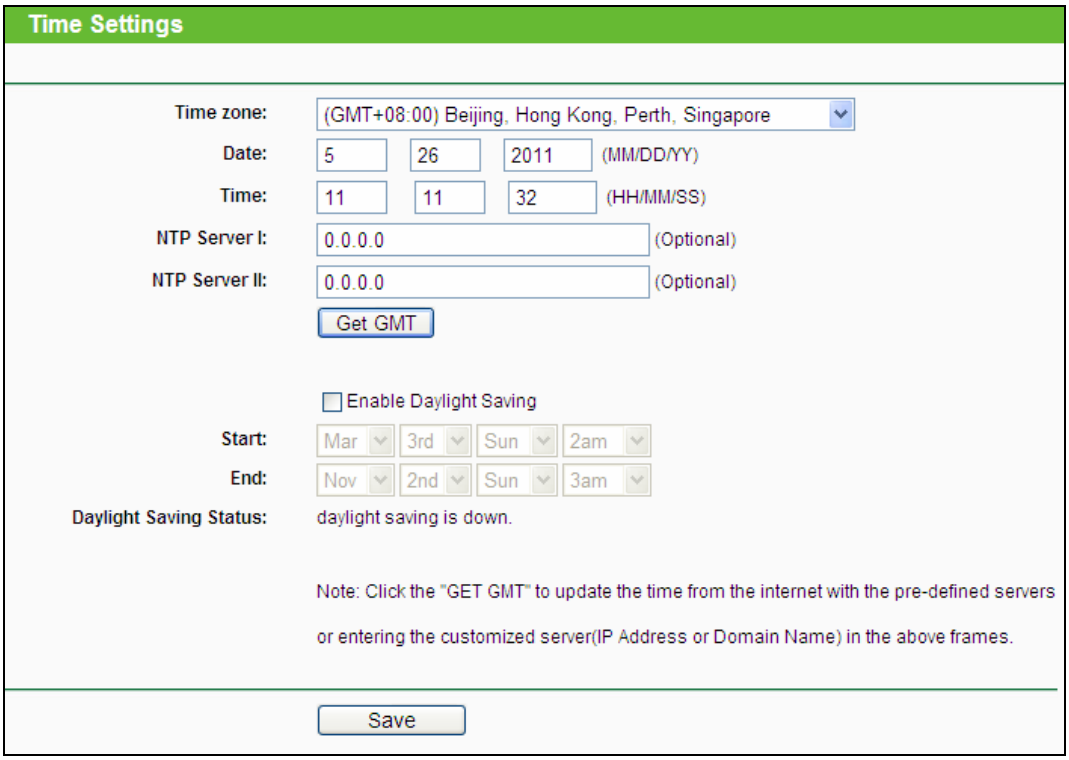


Figure 5-78 Time settings

- **Time Zone -** Select your local time zone from this pull down list.
- **Date -** Enter your local date in MM/DD/YY into the right blanks.
- **Time -** Enter your local time in HH/MM/SS into the right blanks.
- **NTP Server I / NTP Server II -** Enter the address or domain of the **NTP Server I** or **NTP Server II**, and then the Router will get the time from the NTP Server preferentially. In addition, the Router built-in some common NTP Servers, so it can get time automatically once it connects the Internet.
- **Enable Daylight Saving -** Check the box to enable the Daylight Saving function.
- **Start -** The time to start the Daylight Saving. Select the month in the first field, the week in the second field, the day in the third field and the time in the last field.

- **End -** The time to end the Daylight Saving. Select the month in the first field, the week in the second field, the day in the third field and the time in the last field.
- **Daylight Saving Status -** Displays the status whether the Daylight Saving is in use.

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**.

To set time automatically:

1. Select your local time zone.
2. Enter the address or domain of the **NTP Server I** or **NTP Server II**.
3. Click the **Get GMT** button to get system time from Internet if you have connected to the Internet.

To set Daylight Saving:

1. Check the box to enable Daylight Saving.
2. Select the start time from the drop-down lists in the **Start** field.
3. Select the end time from the drop-down lists in the **End** field.
4. Click the **Save** button to save the settings.

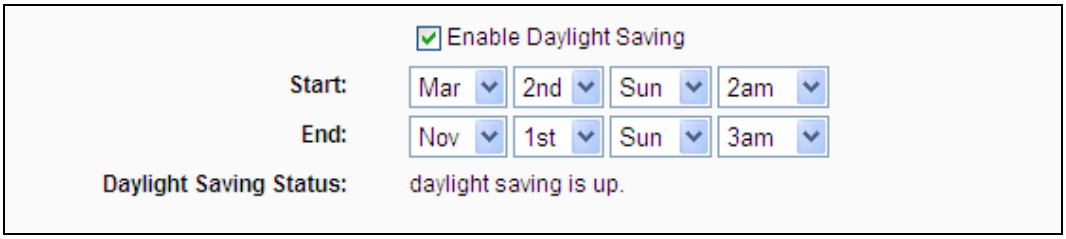


Figure 5-79 Time settings

Note:

1) This setting will be used for some time-based functions such as firewall. You must specify your time zone once you login to the router successfully, otherwise, these functions will not take effect.
2) The time will be lost if the router is turned off.
3) The Router will automatically obtain GMT from the Internet if it is configured accordingly.
4) The Daylight Saving will take effect one minute after the configurations are completed.

5.16.2 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.

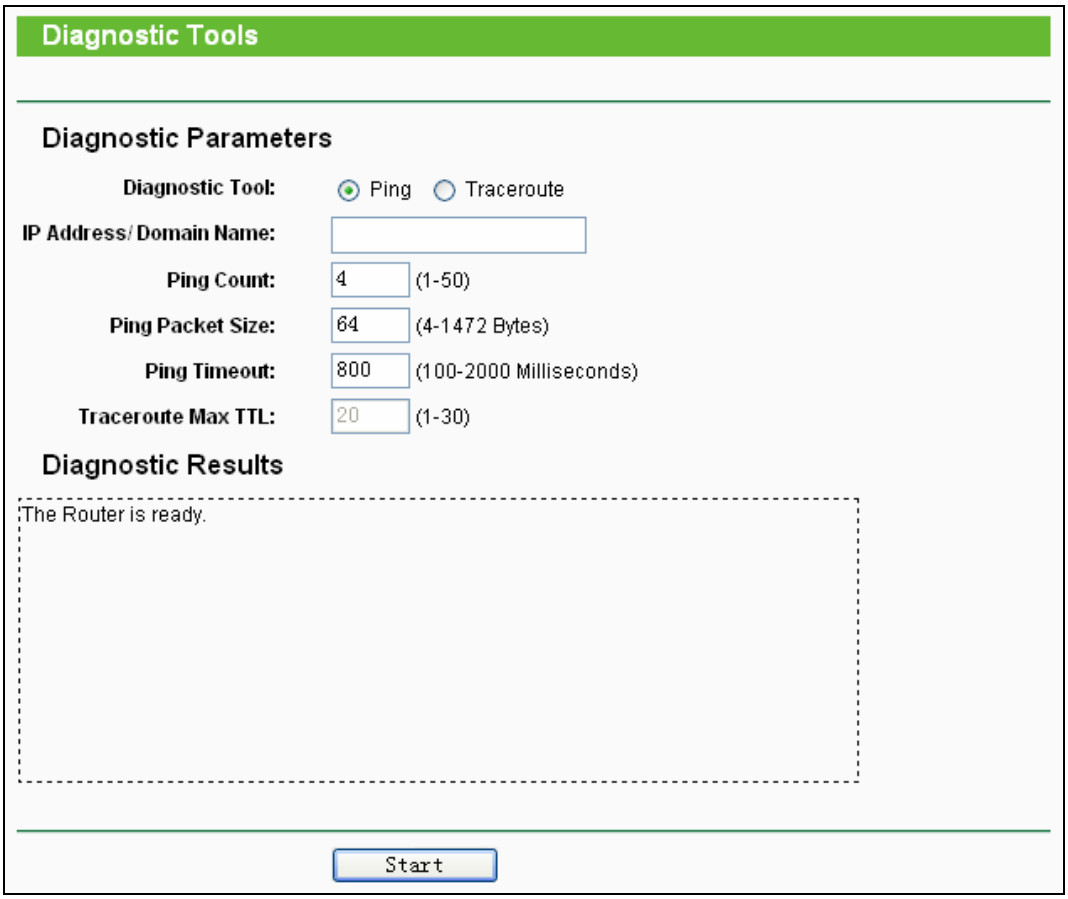


Figure 5-80 Diagnostic Tools

- **Diagnostic Tool** - Check the radio button to select one diagnostic too.
- **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.
- **Pings 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 **Start** to check the connectivity of the Internet.

The **Diagnostic Results** page displays the result of diagnosis.

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

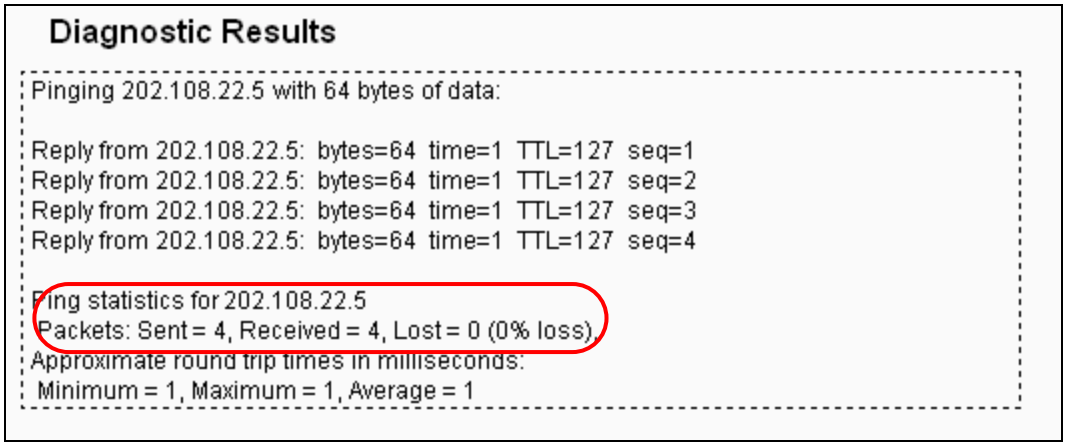


Figure 5-81 Diagnostic Results

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.

5.16.3 Firmware Upgrade

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

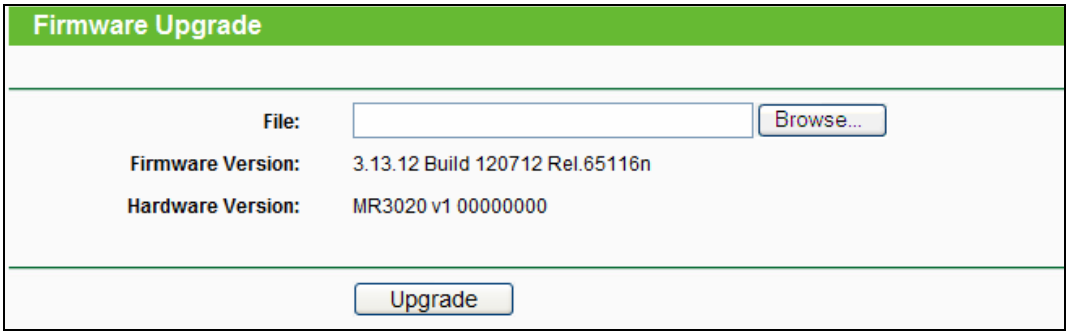


Figure 5-82 Firmware Upgrade

- **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 Router's current hardware version.

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

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 Router will reboot while the upgrading has been finished.

Note:

1) New firmware versions are posted at http://www.tp-link.com and can be downloaded for free. There is no need to upgrade the firmware unless the new firmware has a new feature you want to use. However, when experiencing problems caused by the Router rather than the configuration, you can try to upgrade the firmware.
2) When you upgrade the Router's firmware, you may lose its current configurations, so before upgrading the firmware please write down some of your customized settings to avoid losing important settings.
3) Do not turn off the Router or press the Reset button while the firmware is being upgraded. Loss of power during the upgrade could damage the Router.
4) The firmware version must correspond to the hardware.
5) The upgrade process takes a few moments and the Router restarts automatically when the upgrade is complete.

5.16.4 Factory Defaults

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

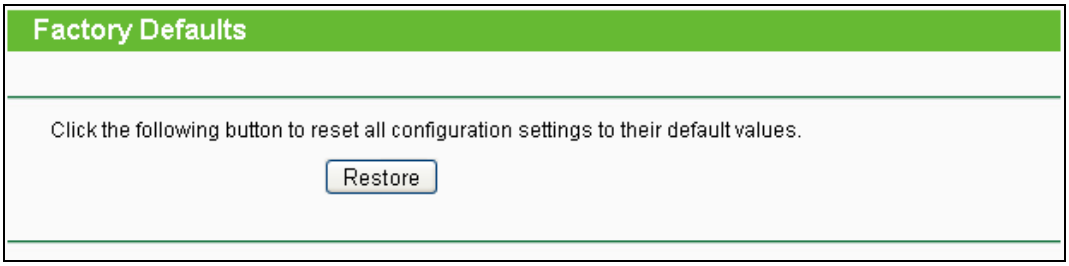


Figure 5-83 Restore Factory Default

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

- The default **User Name**: admin
- The default **Password**: admin
- The default **IP Address**: 192.168.0.254
- The default **Subnet Mask**: 255.255.255.0

Note:

All changed settings will be lost when defaults are restored.

5.16.5 Backup & Restore

Choose menu "**System Tools → Backup & Restore**", and then you can save the current configuration of the Router as a backup file and restore the configuration via a backup file as shown in Figure 5-84.

Figure 5-84 Backup & Restore Configuration

- Click the **Backup** button to save all configuration settings as a backup file in your local computer.
- To upgrade the Router's configuration, follow these instructions.
  - Click the **Browse** button to find the configuration file which you want to restore.
  - 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 Router will restart automatically then. Keep the power of the Router on during the process, in case of any damage.

5.16.6 Reboot

Choose menu "**System Tools** → **Reboot**", and then you can click the **Reboot** button to reboot the Router.

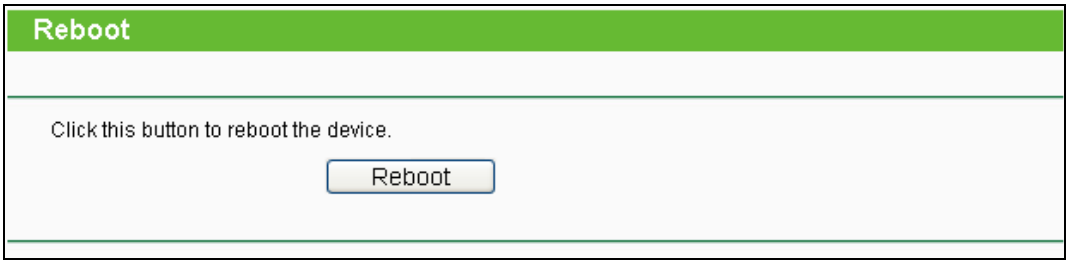


Figure 5-85 Reboot the Router

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

- 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 Router (system will reboot automatically).
- Restore the Router's settings to factory defaults (system will reboot automatically).
- Update the configuration with the file (system will reboot automatically.

5.16.7 Password

Choose menu "**System Tools** → **Password**", and then you can change the factory default user name and password of the Router in the next screen as shown in Figure 5-86.

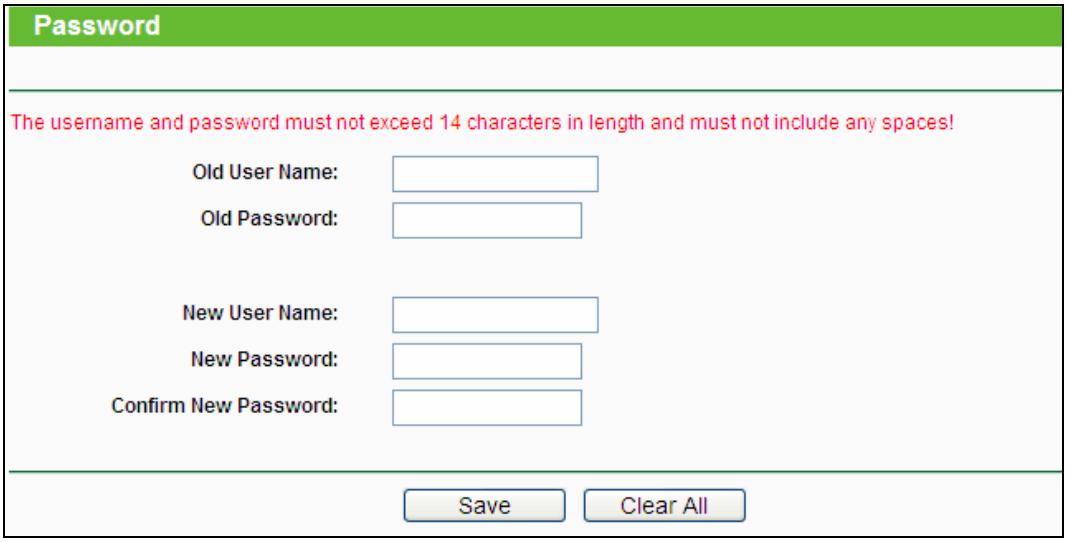


Figure 5-86 Password

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

Note:

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

Click the **Save** button when finished.

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

5.16.8 System Log

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

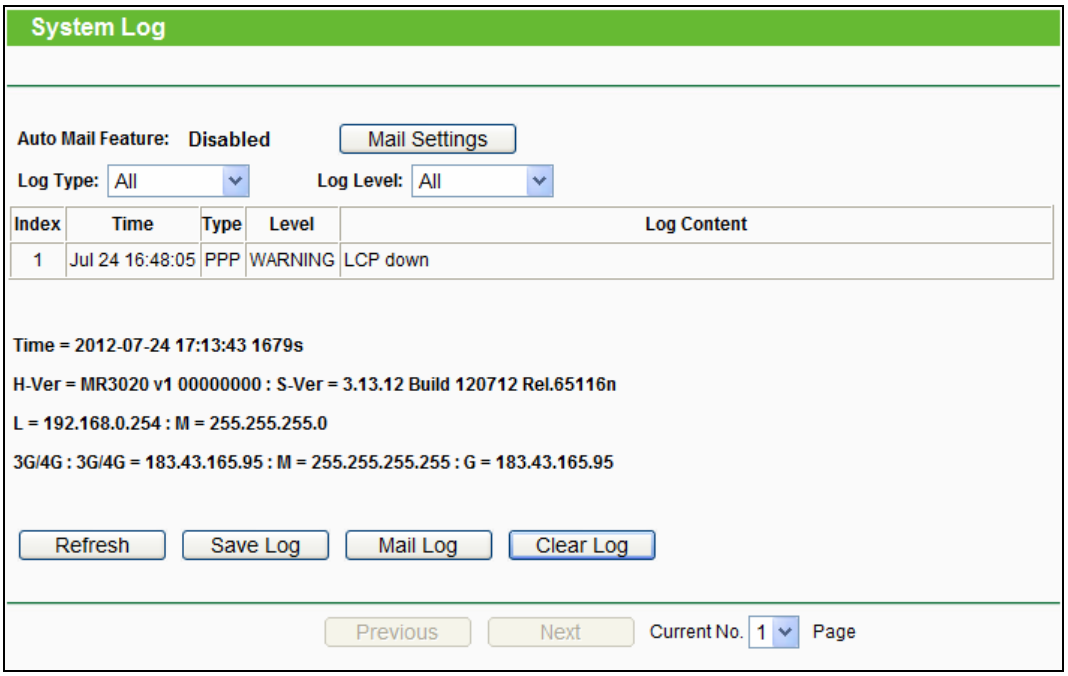


Figure 5-87 System Log

- **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.
- **Clear Log -** All the logs will be deleted from the Router permanently, not just from the page.

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

5.16.9 Working Mode

Choose menu "**System Tools** → **Working Mode**", and you can view the working mode of the Router.

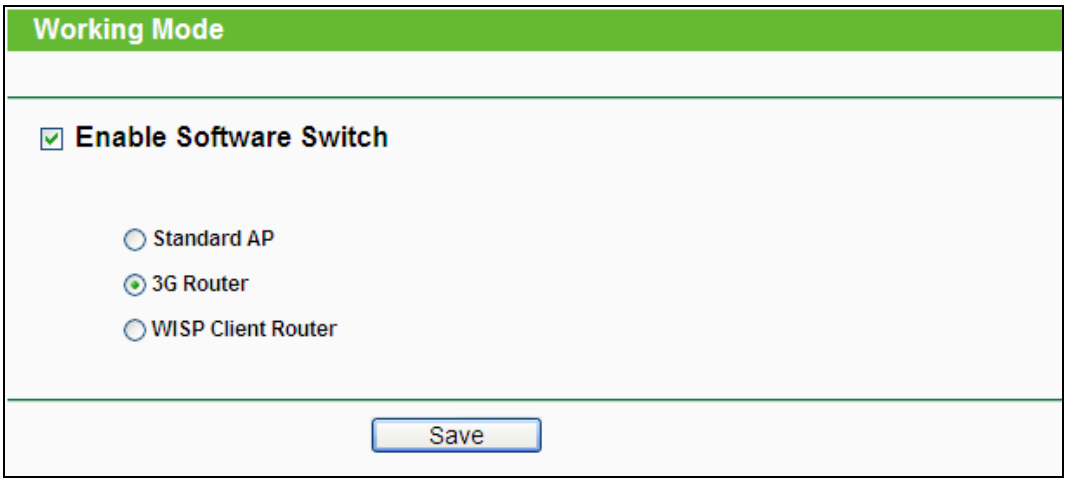


Figure 5-88 Working Mode

- **Standard AP -** In this mode, the device enables multiusers to access, and provides several wireless modes, such as AP, Client, Repeater and so on.
- **3G/4G Router -** In this mode, the device enables multiusers 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 3G/4G Router mode.
- **WISP Client Router -** In this mode, the device enables multiusers 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 WISP Client Router mode. The Ethernet port acts as a LAN port.

Note:

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

5.16.10 Statistics

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

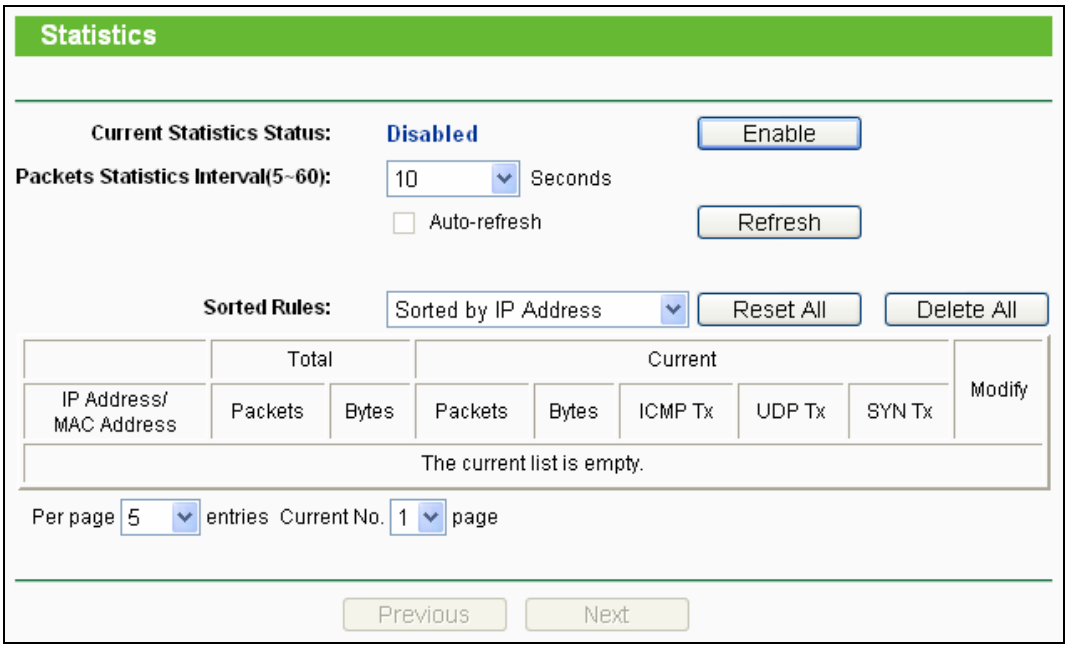


Figure 5-89 Statistics

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

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

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

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

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

Statistics Table:

IP/MAC Address		The IP and MAC address are displayed with related statistics.
Total	**Packets**	The total number of packets received and transmitted by the Router.
	Bytes	The total number of bytes received and transmitted by the Router.
Current	**Packets**	The total number of packets received and transmitted in the last Packets Statistic interval seconds.
	Bytes	The total number of bytes received and transmitted in the last Packets Statistic interval seconds.
	ICMP Tx	The number of the ICMP packets transmitted to 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 value of he entry to zero.
	Delete	Delete the existing entry in the table.

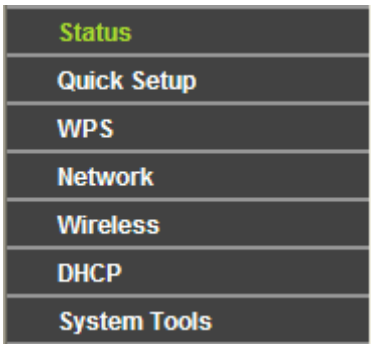
There would be 5 entries on each page. Click **Previous** to return to the previous page and **Next** to the next page.

Chapter 6. Router Configuration—AP Mode

This chapter will show each Web page's key functions and the configuration way on AP Mode. The Portable 3G/4G Wireless N Router is easy to configure and manage with the Web-based (Internet Explorer, Netscape® Navigator, Firefox, Safari, Opera or Chrome) management page, which can be launched on any windows, Macintosh or UNIX OS with a web browser.

6.1 Login

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



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

6.2 Status

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

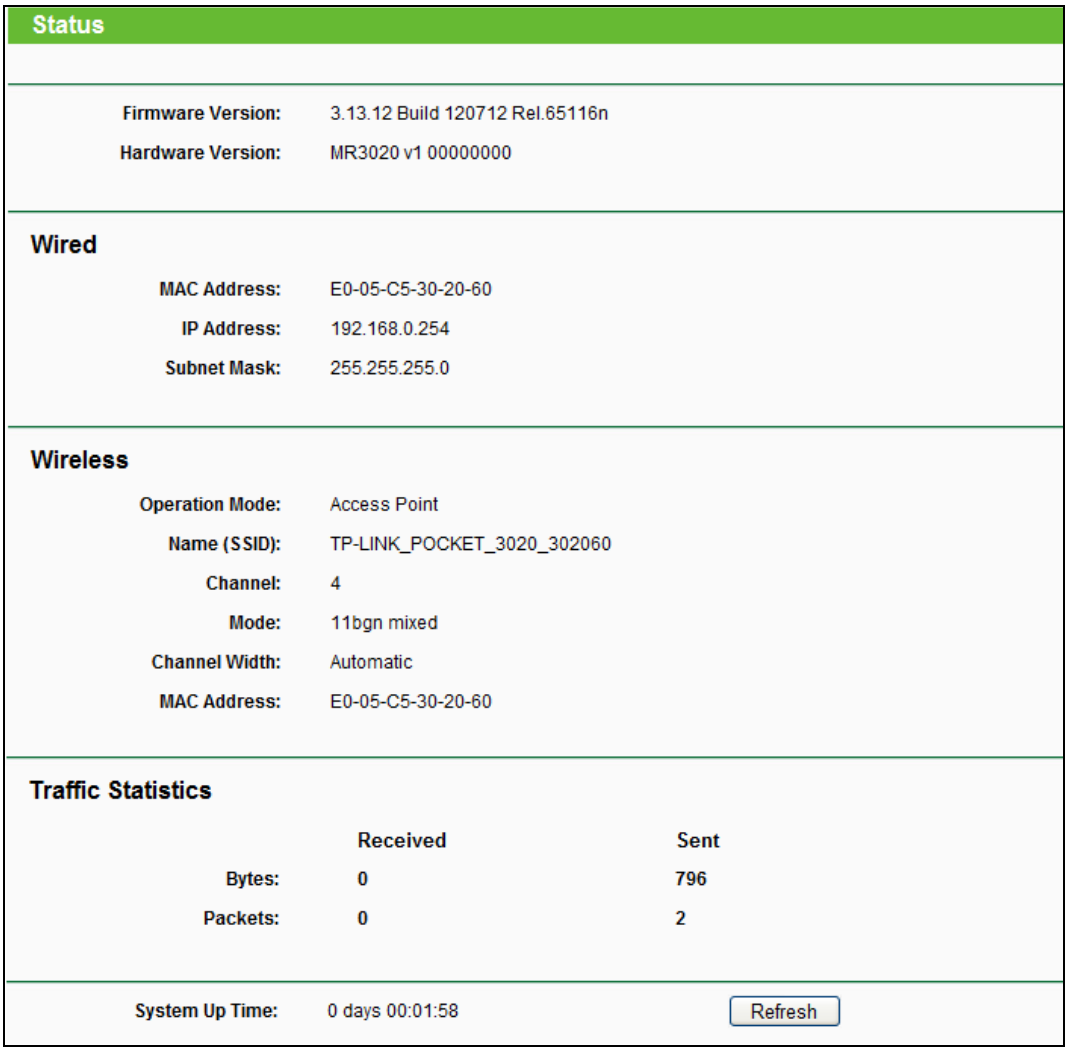
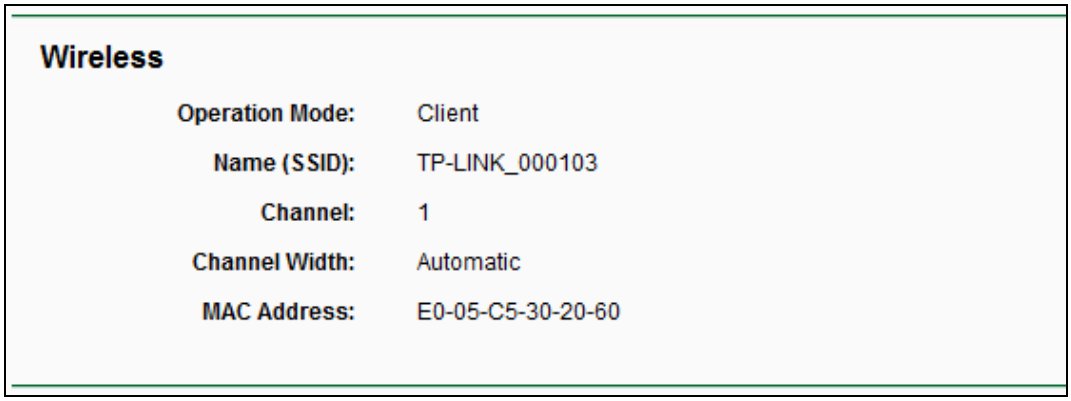


Figure 6-1 Device Status

- **Firmware Version -** This field displays the current firmware version of the AP.
- **Hardware Version -** This field displays the current hardware version of the AP
- **Wired -** This field displays the current settings or information for the Network, including the **MAC address**, **IP address** and **Subnet Mask**.
- **Wireless -** This field displays basic information or status for wireless function, including **Operating Mode, SSID, Channel, Mode, Channel Width, Max Tx Rate and MAC Address.**
- **Traffic Statistics -** This field displays the AP's traffic statistics.
- **System Up Time -** This filed displays the run time of the AP since it's powered on or reset.

Note:

If you select Client mode in Figure 6-8, the wireless status in Figure 6-1 will change, similar to the figure below:



6.3 Quick Setup

Please refer to Chapter 3: "Quick Installation Guide."

6.4 WPS

WPS (Wi-Fi Protected Setup) can help you to quickly and securely connect to a network. This section will guide you to add a new wireless device to an existing network quickly by function. The WPS function is only available when the Operation Mode is set to Access Point and Multi-SSID. Here we take the Access Point mode for example. Select menu "**WPS**", you will see the next screen shown in Figure 6-2.

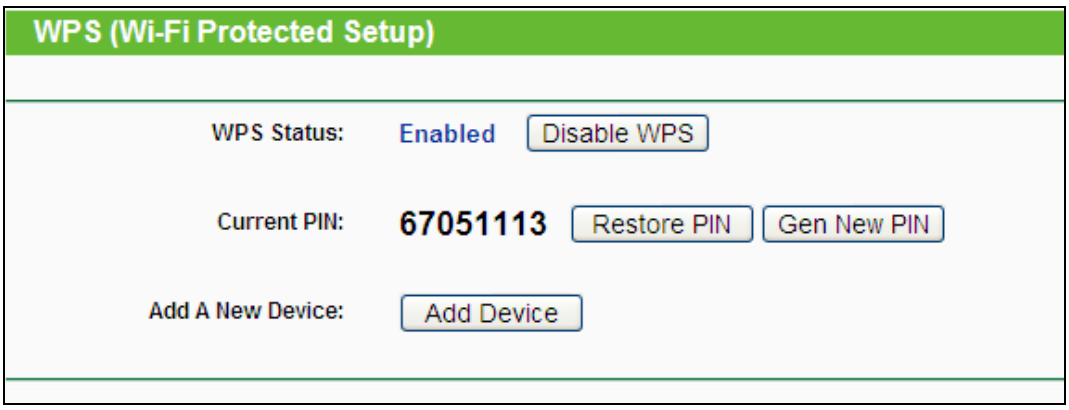


Figure 6-2 WPS

- **WPS Status -** To enable or disable the WPS function here.
- **Current PIN -** The current value of the device's PIN is 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 device -** You can add a new device to the existing network manually by clicking this button.

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 device using either Push Button Configuration (PBC) method or PIN method.

Note:

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

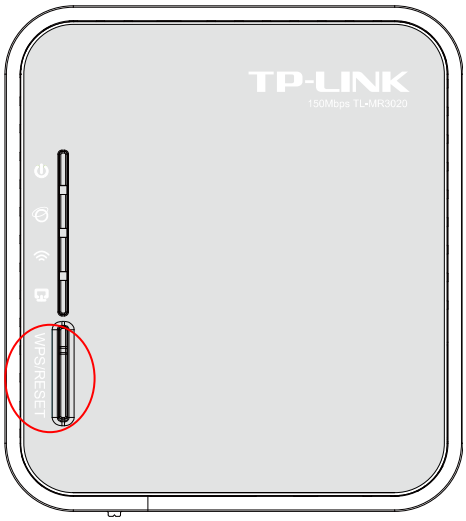
For the configuration of the new device, here takes the Wireless Adapter of our company for example.

I. By PBC

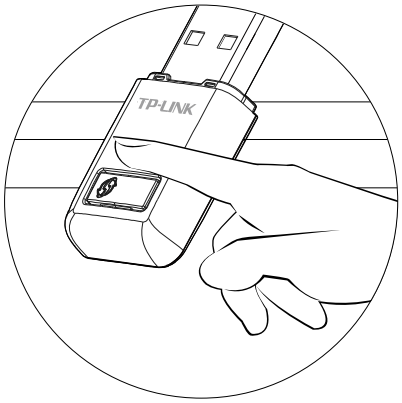
If the wireless adapter supports Wi-Fi Protected Setup and the Push Button Configuration (PBC) method, you can add it to the network by PBC with the following two methods.

Method One:

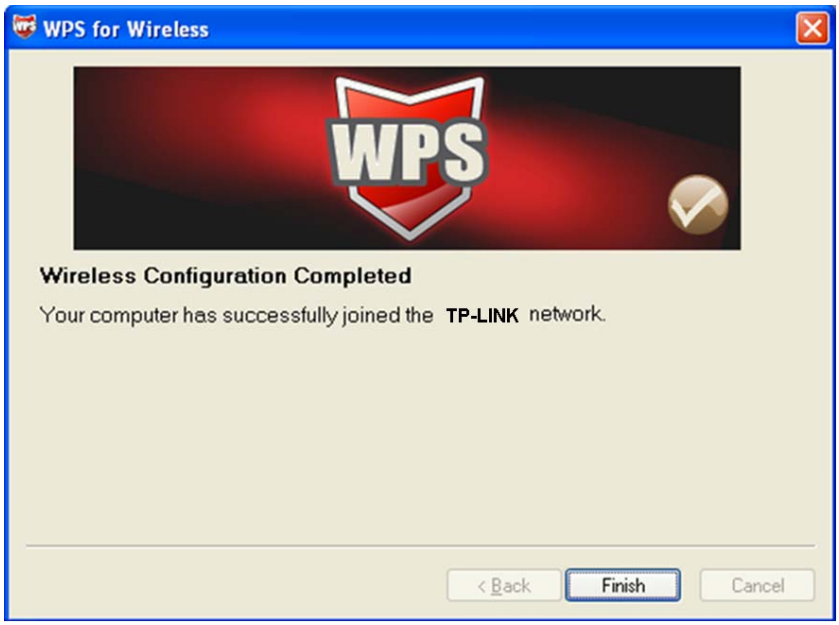
Step 1: Press the WPS/RESET button on the front panel of the Router for less than 5 seconds.



Step 2: Press and hold the WPS button of the adapter directly for 2 or 3 seconds.



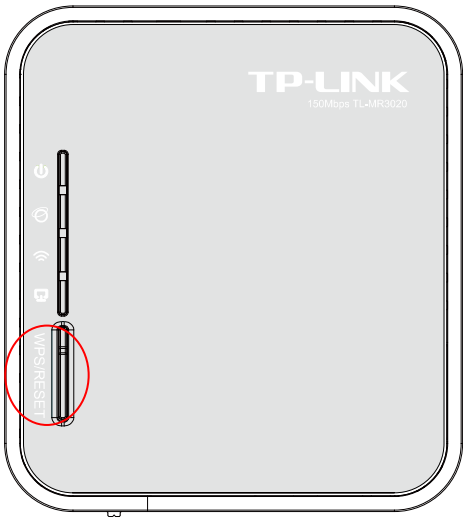
Step 3: Wait for a while until the next screen appears. Click **Finish** to complete the WPS configuration.



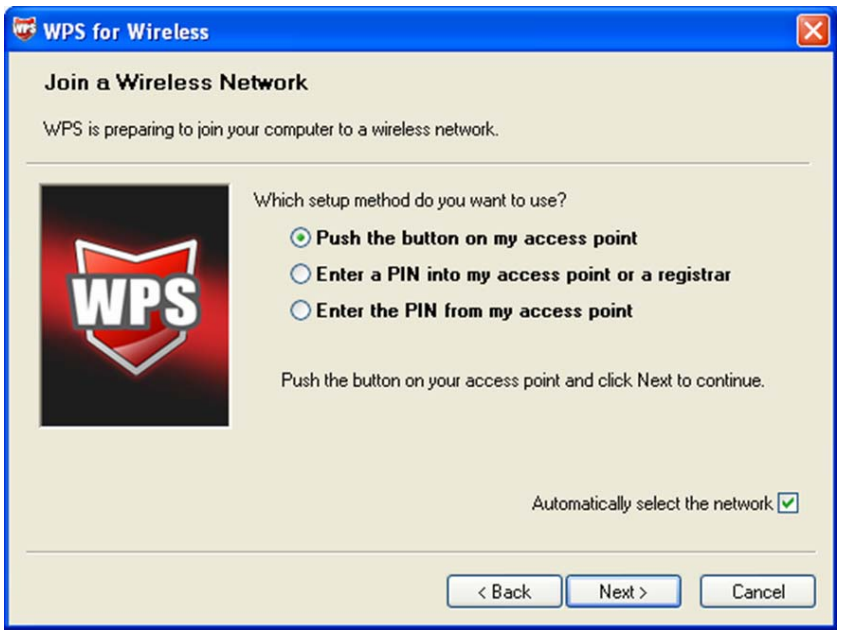
The WPS Configuration Screen of Wireless Adapter

Method Two:

Step 1: Press the WPS/RESET button on the front panel of the Router for less than 5 seconds.



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



The WPS Configuration Screen of Wireless Adapter

Step 3: Wait for a while until the next screen appears. Click **Finish** to complete the WPS configuration.

The WPS Configuration Screen of Wireless Adapter

Method Three:

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

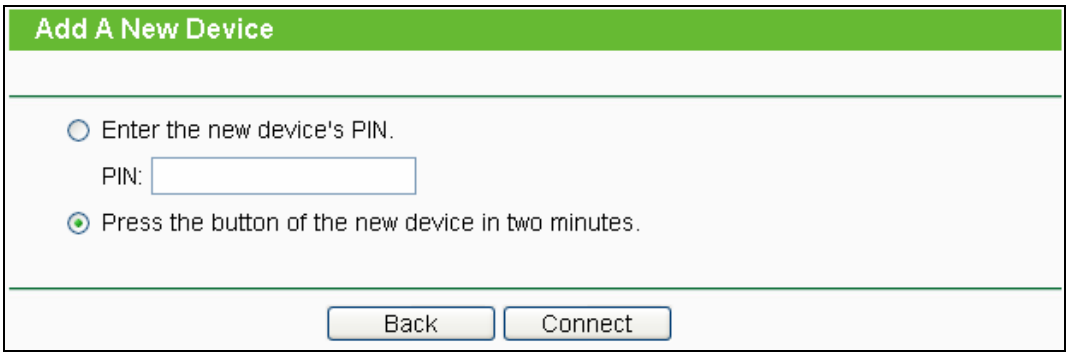
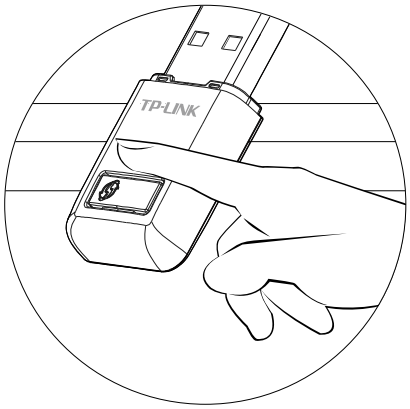


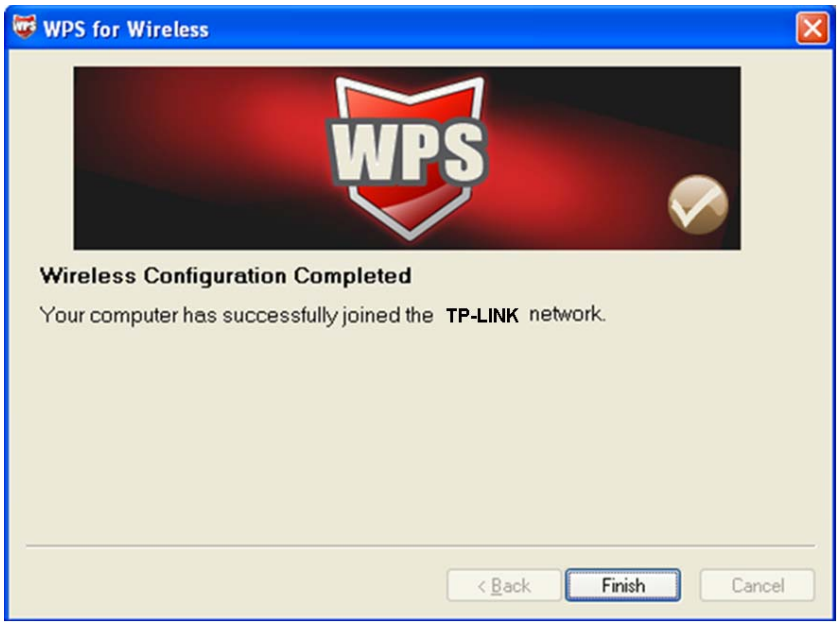
Figure 6-3 Add A New Device

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

Step 3. Press and hold the WPS button of the adapter directly for 2 or 3 seconds.



Step 4. Wait for a while until the next screen appears. Click **Finish** to complete the WPS configuration.



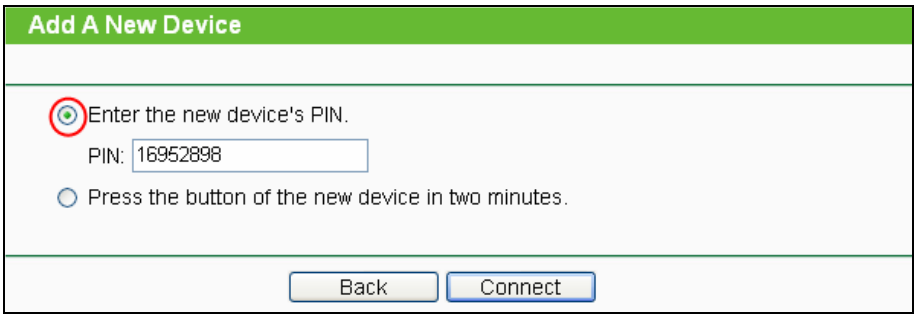
The WPS Configuration Screen of Wireless Adapter

II. By PIN

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

Method One: Enter the PIN into my AP

Step 1: Keep the default WPS Status as **Enabled** and click the **Add device** button in Figure 6-2, then the following screen will appear.

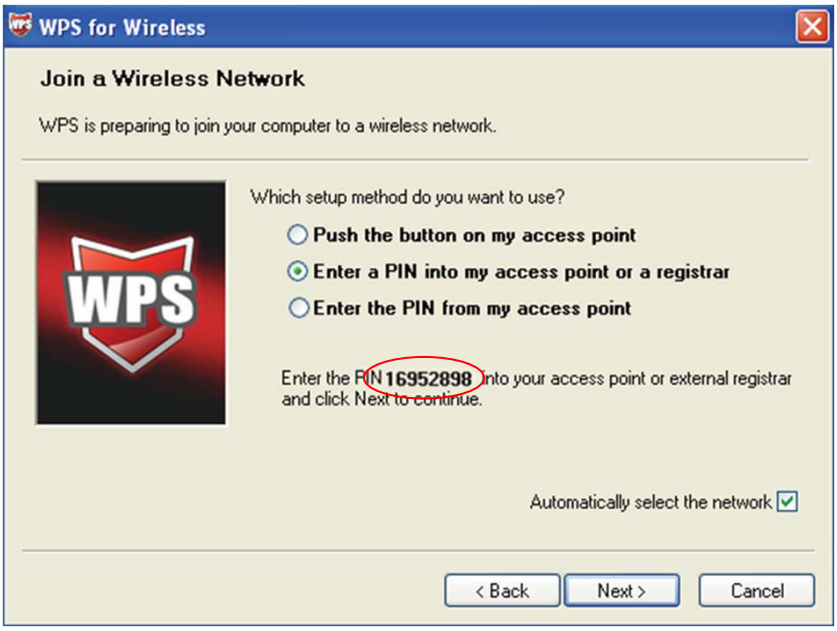


Step 2: Choose "**Enter the new device's PIN**" and enter the PIN code (take 16952898 for example) of the wireless adapter in the field as shown in the figure above. Then click **Connect.**

☞ **Note:**

The PIN code of the adapter is always displayed on the WPS configuration screen as shown in the following figure.

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



The WPS Configuration Screen of Wireless Adapter

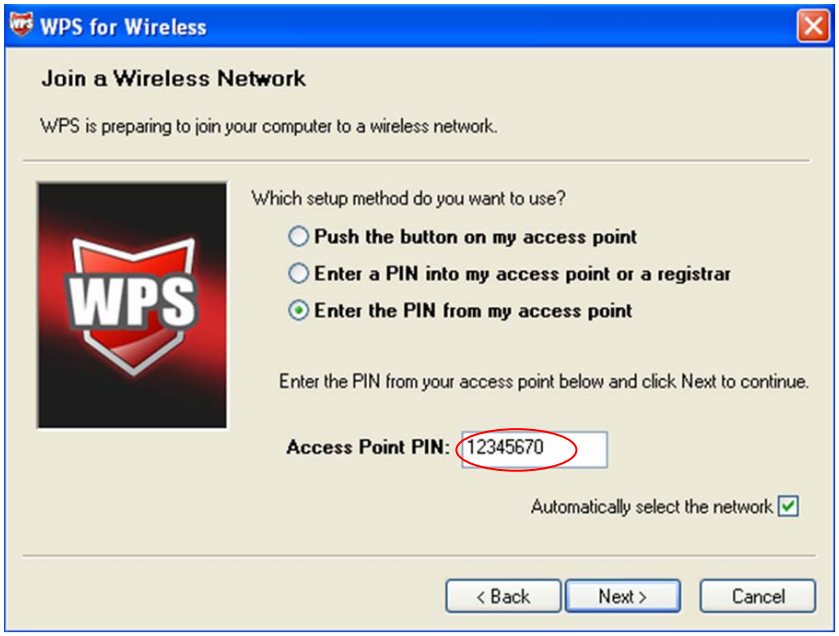
Note:

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

Method Two: Enter the PIN from my AP

Step 1: Get the Current PIN code of the AP in Figure 6-2 (each AP has its unique PIN code. Here takes the PIN code 12345670 of this AP for example).

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

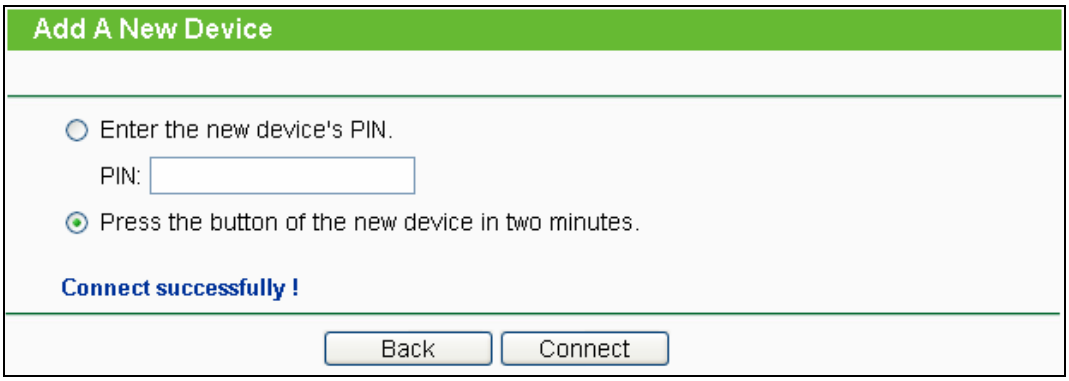


The WPS Configuration Screen of Wireless Adapter

Note:

The default PIN code of the AP can be found in its label or the WPS configuration screen as Figure 6-2.

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



Note:

1) The WPS LED on the AP will light green for five minutes if the device has been successfully added to the network.

2) The WPS function cannot be configured if the Wireless function of the AP is disabled. Please make sure the Wireless function is enabled before configuring the WPS.

6.5 Network

Figure 6-4 the Network menu

There is one submenu under the Network menu (shown in Figure 6-4): **LAN**. Click it and you will be able to configure the LAN function.

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

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

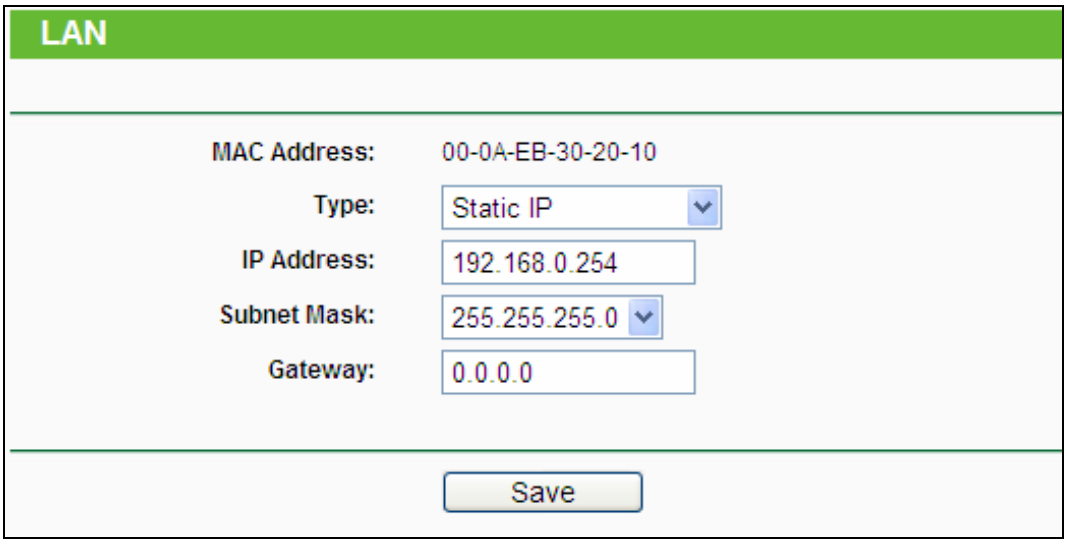


Figure 6-5 LAN

- **MAC Address -** The physical address of the AP. The value can't be changed.
- **Type -** Select **Dynamic IP** to get IP address from DHCP server or select **Static IP** to configure IP address manually from the drop-down list.
- **IP Address -** Enter the IP address of your AP in dotted-decimal notation (factory default setting is 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, you must use the new IP Address to log in the AP.

2) If the new LAN IP Address you set is not in the same subnet with the IP Address pool of DHCP sever, the IP Address pool will not take effect until it is re-configured accordingly.

6.6 Wireless

The **Wireless** option, improving functionality and performance for wireless network, can help you make the AP an ideal solution for your wireless network. Here you can create a wireless local area network just through a few settings. Wireless Settings is used for the configuration of some basic parameters of the AP. Wireless Security 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 Advanced allows you to configure some advanced parameters for the AP. Throughput Monitor helps to watch wireless throughput information Wireless statistics enables you to get detailed information about the current connected wireless stations.

There are six submenus under the Wireless menu (shown in Figure 6-6): **Wireless Settings**, **Wireless Security**, **Wireless MAC Filtering**, **Wireless Advanced** 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.

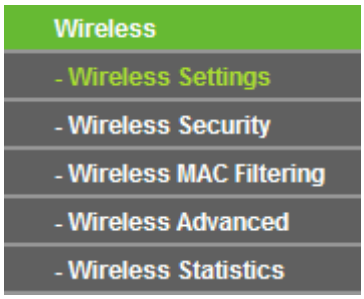


Figure 6-6 Wireless menu

6.6.1 Wireless Settings

Selecting **Wireless** > **Wireless Settings** will enable you to configure the basic settings for your wireless network on the screen below (Figure 6-7).This page allows you to configure the wireless mode for your device. Six operation modes are supported here, including **Access Point**, **Client**, **Repeater** and **Bridge with AP**. The available setting options for each operation mode are different from those of the other.

1) Access Point: This mode allows wireless stations to access this device.

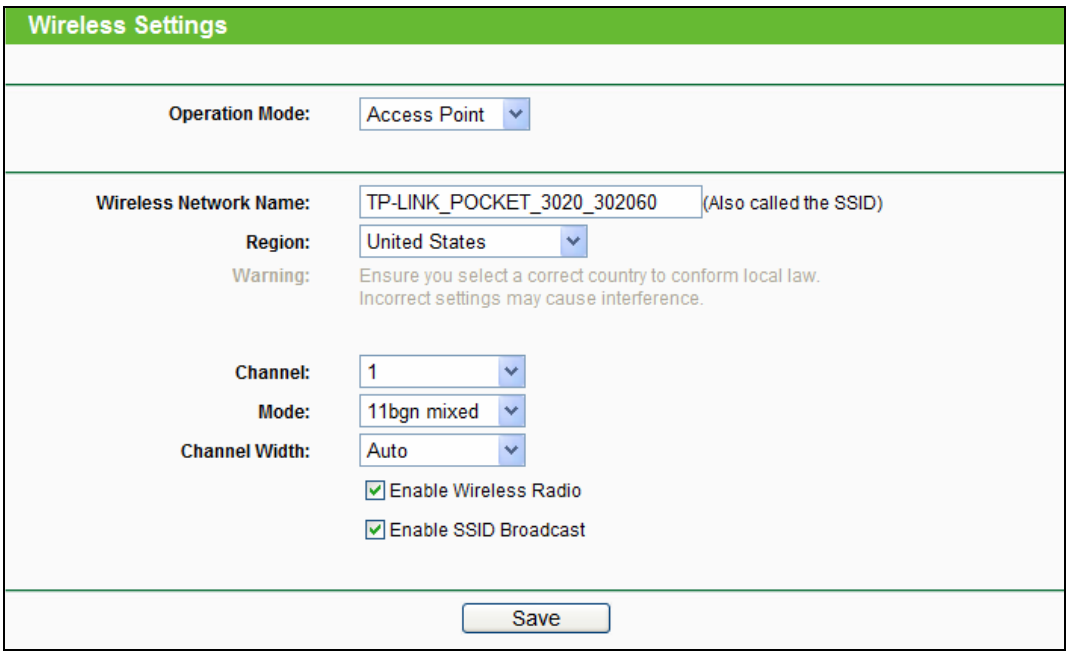
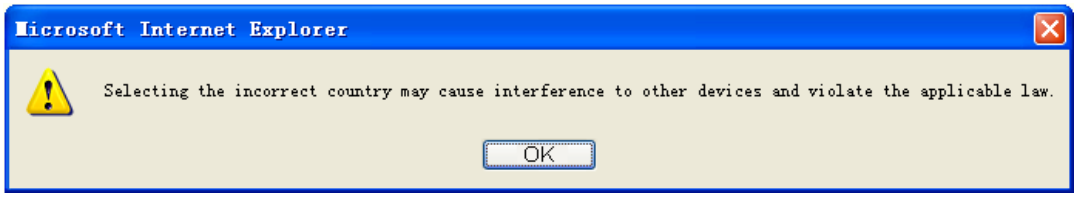


Figure 6-7 Wireless Settings in Access Point mode

- **Wireless Network Name (also called SSID) -** Identifies your wireless network name. Create a name up to 32 characters and make sure all wireless points in the wireless network with the same SSID. The default SSID is TP-LINK_POCKET_3020_XXXXXX (XXXXXX indicates the last unique six characters of each device's MAC address). This value is case-sensitive. For example, *TEST* is NOT the same as *test*.

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

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



Note Dialog

Note:

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

- **Channel -** Determines the operating frequency to be used. It is not necessary to change the wireless channel unless you notice interference problems with another nearby access point.
- **Mode -** Select the desired wireless mode. The options are:
  - **11b only -** Only 802.11b wireless stations can connect to the device.
  - **11g only -** Only 802.11g wireless stations can connect to the device.
  - **11n only -** Only 802.11n wireless stations can connect to the device.
  - **11bg mixed -** Both 802.11b and 802.11g wireless stations can connect to the device.
  - **11bgn mixed -** All 802.11b, 802.11g and 802.11n wireless stations can connect to the device.
- **Channel Width -** Determines the channel width to be used. It is unnecessary to change the default value unless required.
- **Max Tx Rate -** Specifies the maximum transmit rate of the device through this field.
- **Enable Wireless Radio -** Select or deselect this check box to allow or deny wireless stations to access the device.
- **Enable SSID Broadcast -** Select or deselect this check box to allow or deny the device to broadcast its name (SSID) on the air. If it's allowed, when wireless clients survey the local area for wireless networks to associate with, they will detect the SSID broadcast by the device.

Note:

To apply any settings you have altered on the page, please click the **Save** button, and then you will be reminded to reboot the device.

2) **Client:** This mode allows the device to act as a wireless station to enable wired host(s) to access an AP.

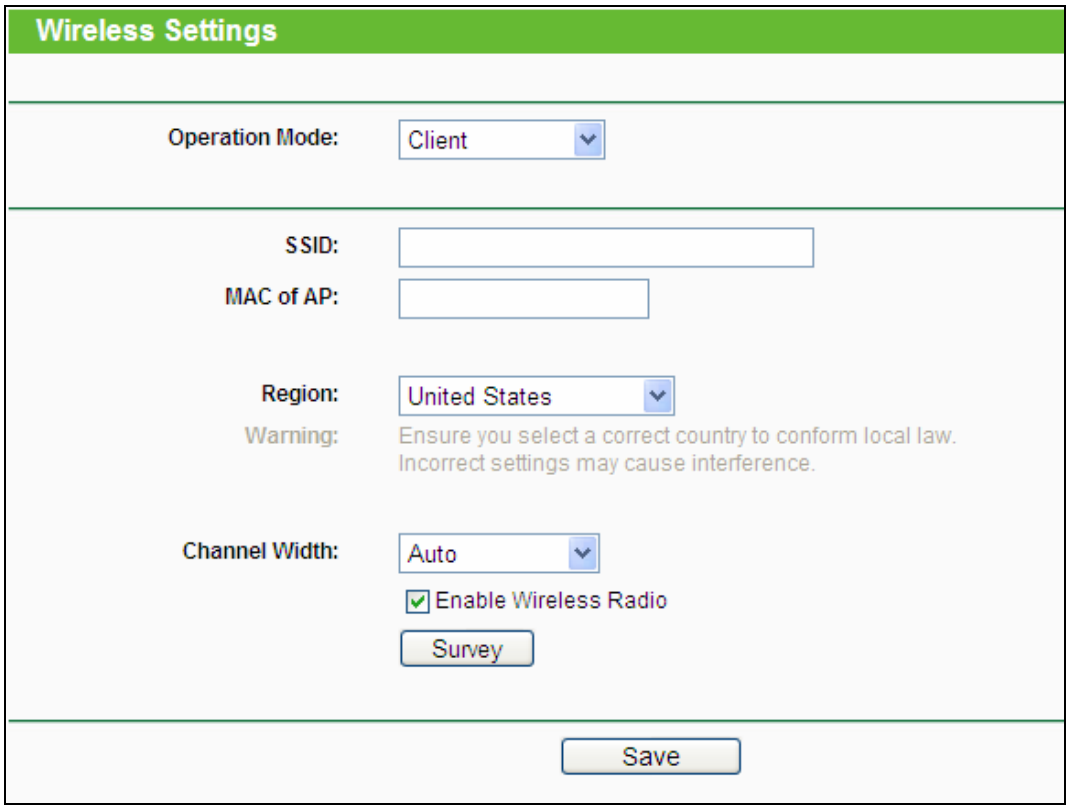


Figure 6-8 Wireless Settings in Client mode

- **SSID -** If you select the radio button before **SSID**, the AP client will connect to the AP according to SSID. Enter the SSID of AP that you want to access.
- **MAC of AP -** If you select the radio button before **MAC of AP**, the AP client will connect to the AP according MAC address. Enter the MAC address of AP that you want to access.
- **Region -** Select your region from the pull-down list. This field specifies the region where the wireless function of the device can be used. It may be illegal to use the wireless function of the device in a region other than one of those specified in this field. If your country or region is not listed, please contact your local government agency for assistance.

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

Note Dialog

Note:

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

- **Channel Width -** Determines the channel width to be used. It is unnecessary to change the default value unless required.
- **Enable Wireless Radio -** Select or deselect this check box to allow or deny wireless stations to access the device.

Click the **Survey** button to detect the SSIDs in the local area.

Note:

To apply any settings you have altered on the page, please click the **Save** button, and then you will be reminded to reboot the device.

3) Repeater: This mode allows the AP with its own BSS to relay data to a root AP to which it is associated with WDS enabled. The wireless repeater relays signal between its stations and the root AP for greater wireless range.

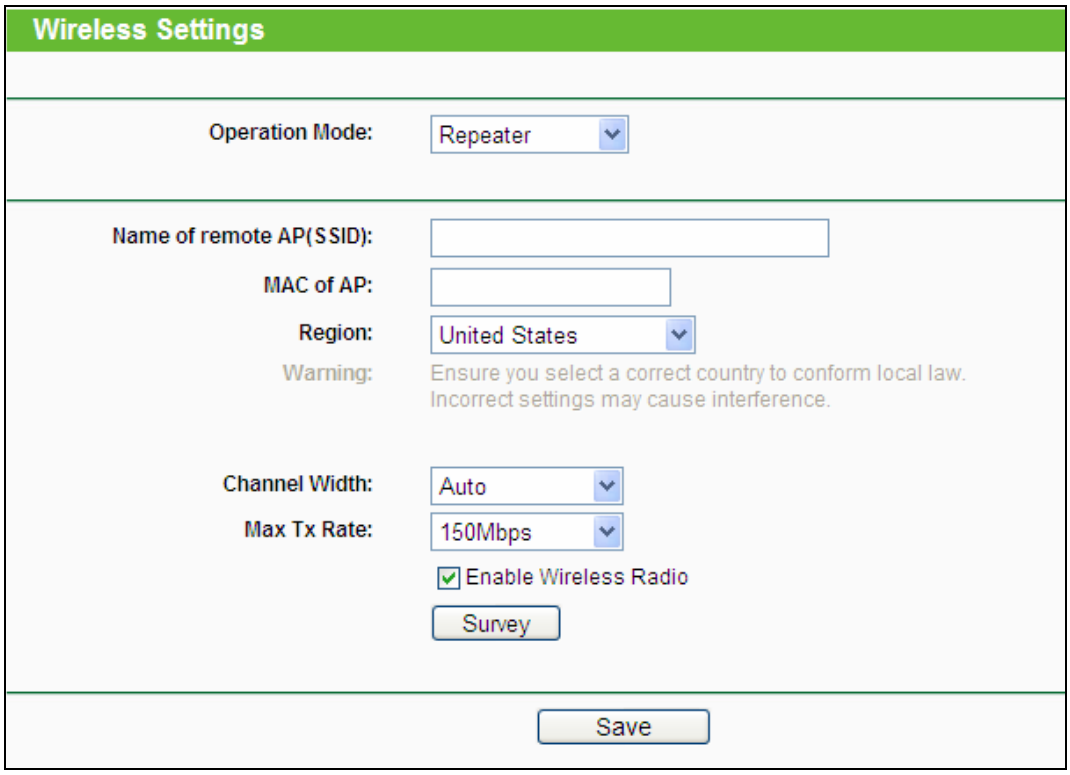


Figure 6-9 Wireless Settings in Repeater mode

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

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

Note Dialog

Note:

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

- **Channel Width -** Determines the channel width to be used. It is unnecessary to change the default value unless required.

- **Max Tx Rate -** Specifies the maximum transmit rate of the device through this field.
- **Enable Wireless Radio -** Select or deselect this check box to allow or deny wireless stations to access the device.

Click the **Survey** button to detect the SSIDs in the local area.

Note:

To apply any settings you have altered on the page, please click the **Save** button, and then you will be reminded to reboot the device.

4) Bridge with AP: This mode can bridge the AP and up to 4 APs also in bridge mode to connect two or more wired LANs.

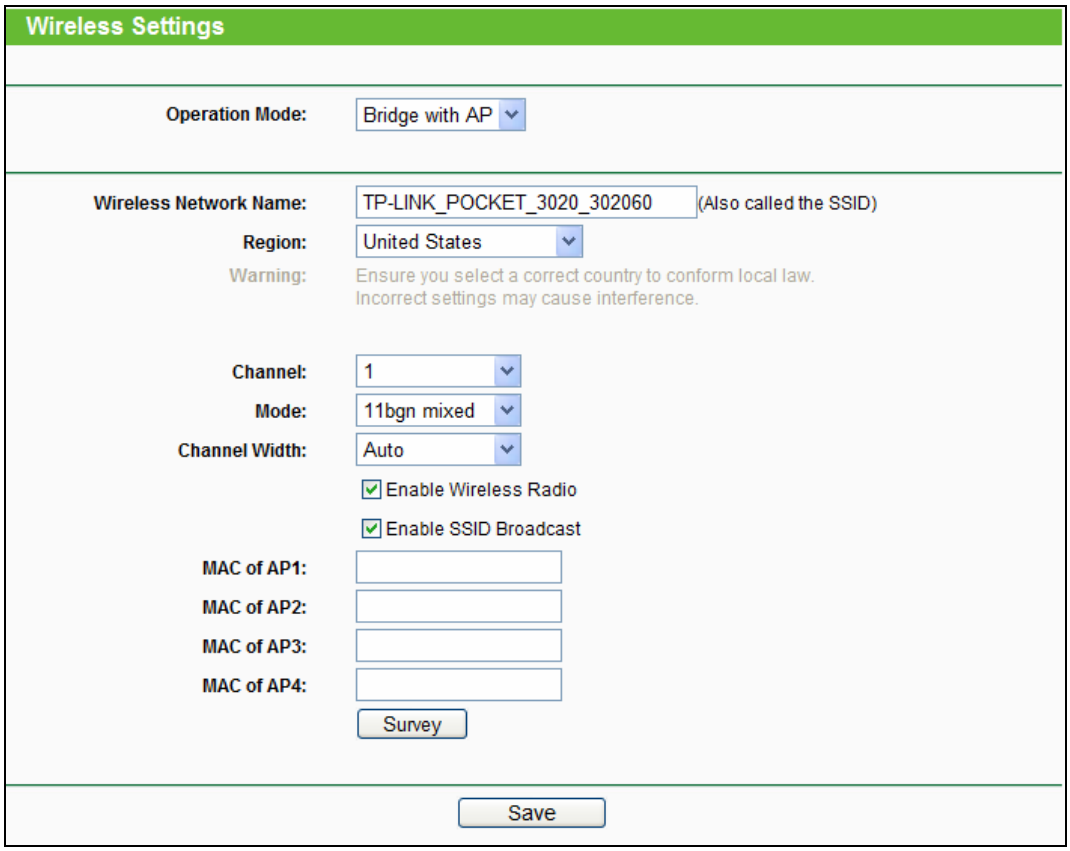


Figure 6-10 Wireless Settings in Bridge with AP mode

- **Wireless Network Name (also called SSID) -** Identifies your wireless network name. Create a name up to 32 characters and make sure all wireless points in the wireless network with the same SSID. The default SSID is TP-LINK_POCKET_3020_XXXXXX (XXXXXX indicates the last unique six characters of each device's MAC address). This value is case-sensitive. For example, *TEST* is NOT the same as *test*.
- **Region -** Select your region from the pull-down list. This field specifies the region where the wireless function of the device can be used. It may be illegal to use the wireless function of the device in a region other than one of those specified in this field. If your

country or region is not listed, please contact your local government agency for assistance.

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

Note Dialog

Note:

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

- **Channel -** Determines the operating frequency to 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 device works on.
  - **11b only -** Only 802.11b wireless stations can connect to the device.
  - **11g only -** Only 802.11g wireless stations can connect to the device.
  - **11n only -** Only 802.11n wireless stations can connect to the device.
  - **11bg mixed -** Both 802.11b and 802.11g wireless stations can connect to the device.
  - **11bgn mixed -** All 802.11b, 802.11g and 802.11n wireless stations can connect to the device.
- **Channel Width -** Determines the channel width to be used. It is unnecessary to change the default value unless required.
- **Max Tx Rate -** Specifies the maximum transmit rate of the device through this field.
- **Enable Wireless Radio -** Select or deselect this check box to allow or deny wireless stations to access the device.
- **Enable SSID Broadcast -** Select or deselect this check box to allow or deny the device to broadcast its name (SSID) on the air. If it's allowed, when wireless clients survey the local area for wireless networks to associate with, they will detect the SSID broadcast by the device.
- **MAC of AP (1-4) -** Enter the MAC address of other AP(s).

Click the **Survey** button to detect the SSIDs in the local area.

Note:

To apply any settings you have altered on the page, please click the **Save** button, and then you will be reminded to reboot the device.

6.6.2 Wireless Security

Selecting **Wireless** > **Wireless Security** will enable you to configure wireless security for your wireless network to protect your data from intruders. The AP provides three security types: WEP, WPA/WPA2 and WPA-PSK/WPA2-PSK. Wireless security can be set on the following screen shown as Figure 6-11. The security options are different for different operation mode.

1) Access Point

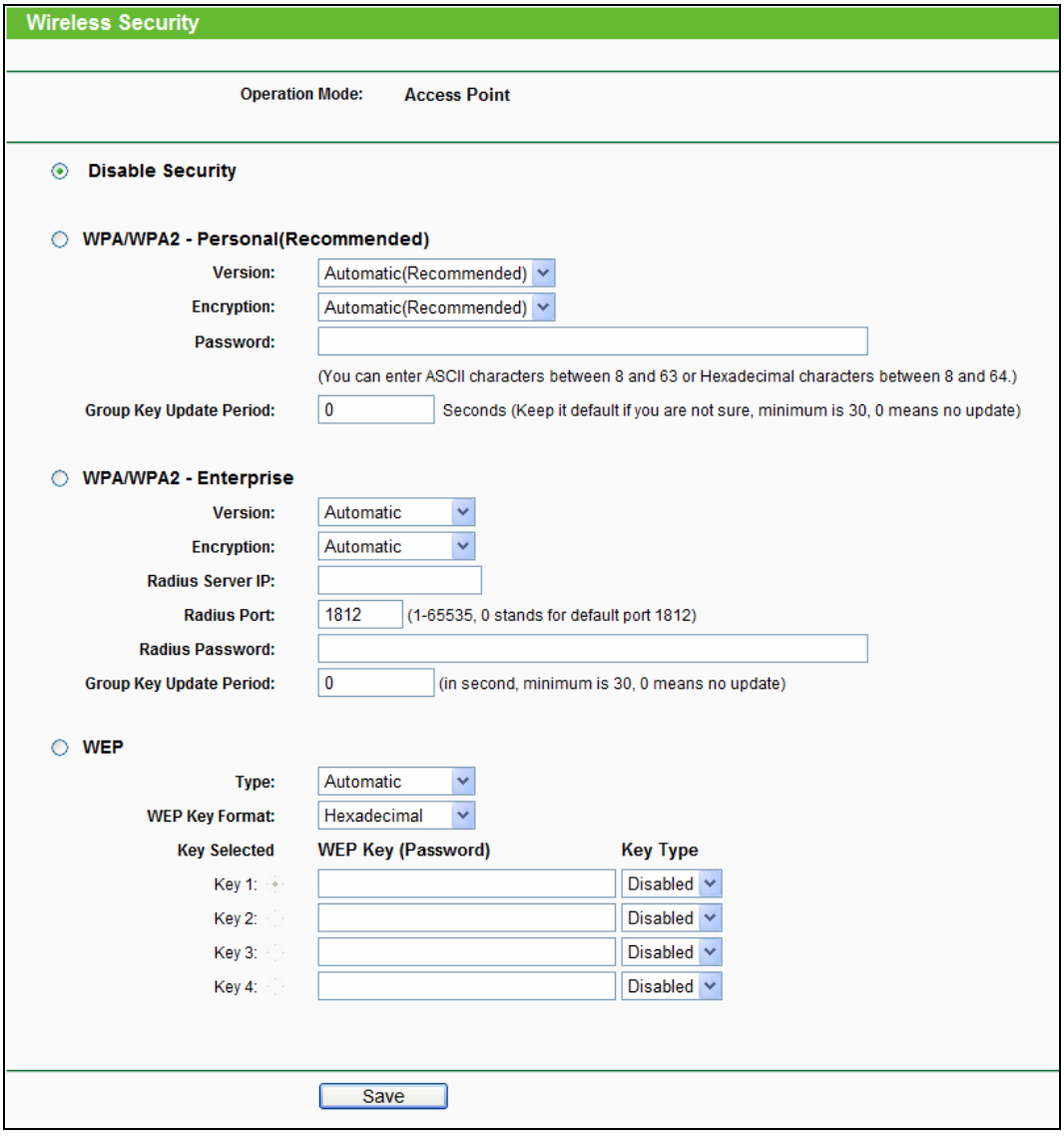


Figure 6-11 Wireless Security - Access Point

- **Operation Mode -** Shows the current operation mode.

- **Disable Security -** Check this box radio button to disable wireless security. If disabled, the wireless stations will be able to connect this device without encryption. It is strongly recommended that you choose one of the security types to enable security.
- **WPA/WPA2 – Personal (Recommended) -** Select WPA based on pre-shared key.
  - **Version -** You can select one of following versions.
    1) **Automatic (Recommended)** - Select **WPA-PSK** or **WPA2-PSK** automatically based on the wireless station's capability and request.
    2) **WPA-Personal -** Pre-shared key of WPA.
    3) **WPA2-Personal -** Pre-shared key of WPA2.
  - **Encryption** - When you select **WPA-Personal** or **WPA2-Personal** for **Authentication Type**, you can select either **Automatic (Recommended)**, **TKIP** or **AES** as **Encryption**.
  - **PSK Passphrase** - Enter a passphrase here.
  - **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 -** Select WPA/WPA2 based on Radius Server.
  - **Version -** You can select one of following versions.
    1) **Automatic -** Select **WPA** or **WPA2** automatically based on the wireless station's capability and request.
    2) **WPA -** Wi-Fi Protected Access.
    3) **WPA2 -** WPA version 2.
  - **Encryption** - You can select either **Automatic**, **TKIP** or **AES**.
  - **Radius Server IP** - Enter the IP address of the Radius Server.
  - **Radius Port** - Enter the port used by radius service.
  - **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 -** Select 802.11 WEP security.
  - **Type** - You can select one of following types.
    1) **Automatic** - Select **Shared Key** or **Open System** authentication type automatically based on the wireless station's capability and request.
    2) **Shared Key** - Select 802.11 **Shared Key** authentication type.
    3) **Open System** - Select 802.11 **Open System** authentication.

- **WEP Key Format** - You can select **ASCII** or **Hexadecimal** format. ASCII format stands for any combination of keyboard characters in the specified length. Hexadecimal format stands for any combination of hexadecimal digits (0-9, a-f, A-F) in the specified length.
- **WEP Key** - Select which of the four keys will be used and enter the matching WEP key information for your network in the selected key radio button. These values must be identical on all wireless stations in your network.
- **Key Type** - You can select the WEP key length (**64-bit**, or **128-bit**, or **152-bit**.) for encryption. "Disabled" means this WEP key entry is invalid.
    1) For **64-bit** encryption **-** You can enter 10 hexadecimal digits (any combination of 0-9, a-f, A-F, zero key is not permitted) or 5 ASCII characters.
    2) For **128-bit** encryption **-** You can enter 26 hexadecimal digits (any combination of 0-9, a-f, A-F, zero key is not permitted) or 13 ASCII characters.
    3) For **152-bit** encryption **-** You can enter 32 hexadecimal digits (any combination of 0-9, a-f, A-F, zero key is not permitted) or 16 ASCII characters.

☞ **Note:**

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

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

☞ **Note:**

You will be reminded to reboot the device after clicking the **Save** button.

2) Client

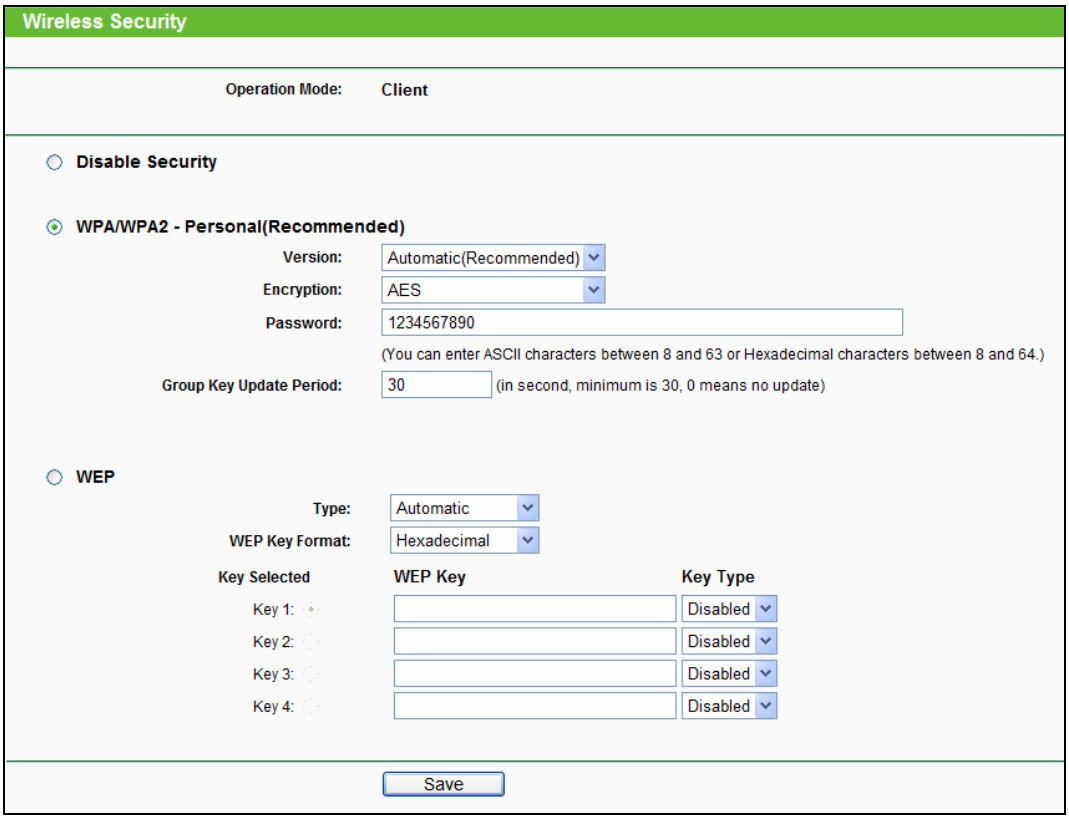


Figure 6-12 Wireless Security – Client

- **Operation Mode -** Shows the current operation mode.
- **Disable Security -** Check this box radio button to disable wireless security. If disabled, the wireless stations will be able to connect this device without encryption. It is strongly recommended that you choose one of the security types to enable security.
- **WPA/WPA2 – Personal (Recommended) -** Select WPA based on pre-shared key.
  - **Version -** You can select one of following versions.
    1) **Automatic (Recommended)** - Select **WPA-PSK** or **WPA2-PSK** automatically based on the wireless station's capability and request.
    2) **WPA-Personal -** Pre-shared key of WPA.
    3) **WPA2-Personal -** Pre-shared key of WPA2.
  - **Encryption** - When you select **WPA-Personal** or **WPA2-Personal** for **Authentication Type**, you can select either **Automatic (Recommended)**, **TKIP** or **AES** as **Encryption**.
  - **PSK Passphrase** - Enter a passphrase here.
  - **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 -** Select 802.11 WEP security.

- **Type** - You can select one of following types.
  1) **Automatic** - Select **Shared Key** or **Open System** authentication type automatically based on the wireless station's capability and request.
  2) **Shared Key** - Select 802.11 **Shared Key** authentication type.
  3) **Open System** - Select 802.11 **Open System** authentication.
- **WEP Key Format** - You can select **ASCII** or **Hexadecimal** format. ASCII format stands for any combination of keyboard characters in the specified length. Hexadecimal format stands for any combination of hexadecimal digits (0-9, a-f, A-F) in the specified length.
- **WEP Key** - Select which of the four keys will be used and enter the matching WEP key information for your network in the selected key radio button. These values must be identical on all wireless stations in your network.
- **Key Type** - You can select the WEP key length (**64-bit**, or **128-bit**, or **152-bit**.) for encryption. "Disabled" means this WEP key entry is invalid.
  1) For **64-bit** encryption **-** You can enter 10 hexadecimal digits (any combination of 0-9, a-f, A-F, zero key is not permitted) or 5 ASCII characters.
  2) For **128-bit** encryption **-** You can enter 26 hexadecimal digits (any combination of 0-9, a-f, A-F, zero key is not permitted) or 13 ASCII characters.
  3) For **152-bit** encryption **-** You can enter 32 hexadecimal digits (any combination of 0-9, a-f, A-F, zero key is not permitted) or 16 ASCII characters.

☞ **Note:**

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

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

☞ **Note:**

You will be reminded to reboot the device after clicking the **Save** button.

3) Repeater

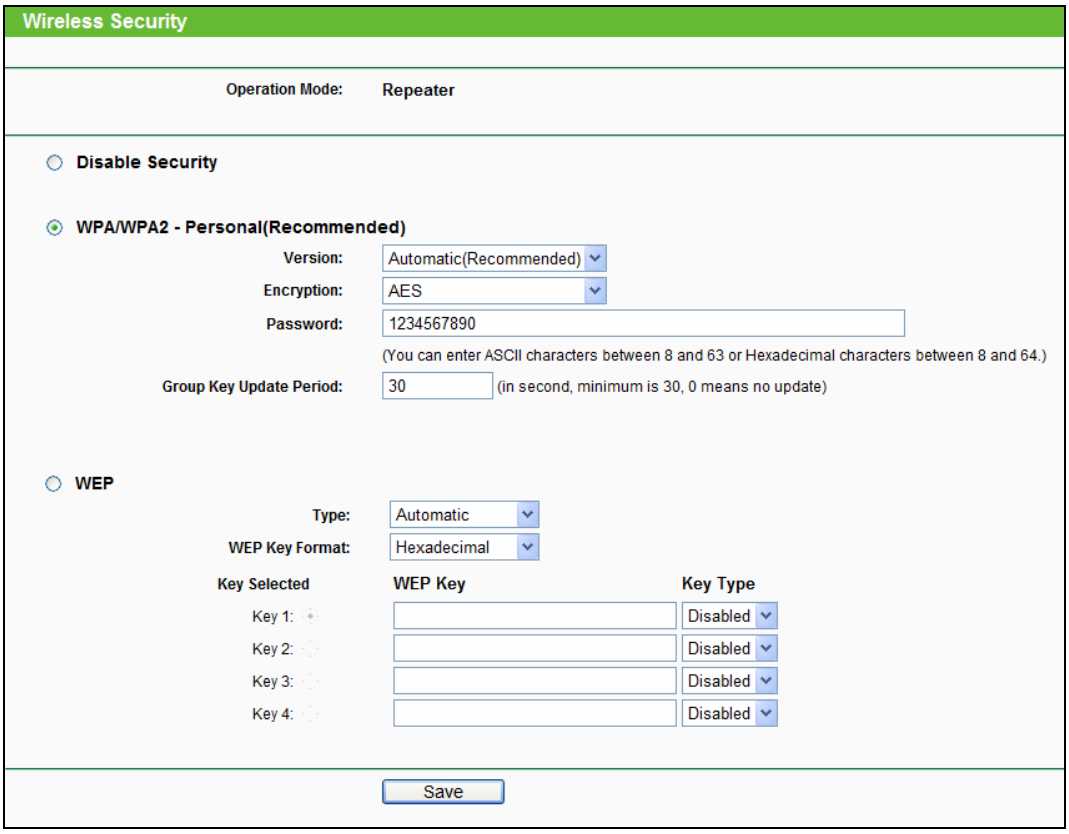


Figure 6-13 Wireless Security – Repeater

- **Operation Mode -** Shows the current operation mode.
- **Disable Security -** Check this box radio button to disable wireless security. If disabled, the wireless stations will be able to connect this device without encryption. It is strongly recommended that you choose one of the security types to enable security.
- **WPA/WPA2 – Personal (Recommended) -** Select WPA based on pre-shared key.
  - **Version** - You can select one of following versions.
    1) **Automatic (Recommended)** - Select **WPA-Personal** or **WPA2-Personal** automatically based on the wireless station's capability and request.
    2) **WPA-Personal** - Pre-shared key of WPA.
    3) **WPA2-Personal** - Pre-shared key of WPA2.
  - **Encryption** - When you select **WPA-Personal** or **WPA2-Personal** for **Authentication Type**, you can select either **Automatic (Recommended)**, **TKIP** or **AES** as **Encryption**.
  - **PSK Passphrase** - Enter a passphrase here.
  - **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 -** Select 802.11 WEP security.

- **Type** - You can select one of following types.
  1) **Automatic** - Select **Shared Key** or **Open System** authentication type automatically based on the wireless station's capability and request.
  2) **Shared Key** - Select 802.11 **Shared Key** authentication type.
  3) **Open System** - Select 802.11 Open System authentication.
- **WEP Key Format** - You can select **ASCII** or **Hexadecimal** format. ASCII format stands for any combination of keyboard characters in the specified length. Hexadecimal format stands for any combination of hexadecimal digits (0-9, a-f, A-F) in the specified length.
- **WEP Key** - Select which of the four keys will be used and enter the matching WEP key information for your network in the selected key radio button. These values must be identical on all wireless stations in your network.
- **Key Type** - You can select the WEP key length (**64-bit**, or **128-bit**, or **152-bit**.) for encryption. "Disabled" means this WEP key entry is invalid.
  1) For **64-bit** encryption **-** You can enter 10 hexadecimal digits (any combination of 0-9, a-f, A-F, zero key is not permitted) or 5 ASCII characters.
  2) For **128-bit** encryption **-** You can enter 26 hexadecimal digits (any combination of 0-9, a-f, A-F, zero key is not permitted) or 13 ASCII characters.
  3) For **152-bit** encryption **-** You can enter 32 hexadecimal digits (any combination of 0-9, a-f, A-F, zero key is not permitted) or 16 ASCII characters.

☞ **Note:**

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

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

☞ **Note:**

You will be reminded to reboot the device after clicking the **Save** button.

4) Bridge with AP

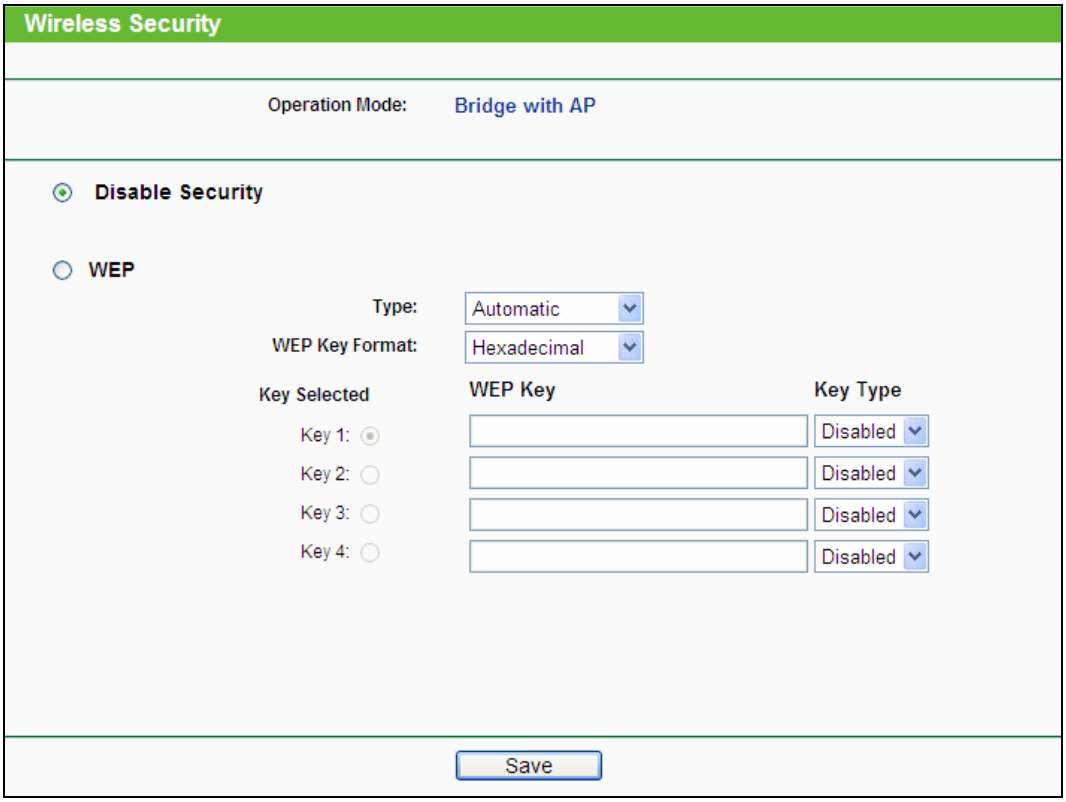


Figure 6-14 Wireless Security – Bridge with AP

- **Operation Mode -** Shows the current operation mode.
- **Disable Security -** Check this box radio button to disable wireless security. If disabled, the wireless stations will be able to connect this device without encryption. It is strongly recommended that you choose one of the security types to enable security.
- **WEP -** Select 802.11 WEP security.
  - **Type** - You can select one of following types.
    1) **Automatic** - Select **Shared Key** or **Open System** authentication type automatically based on the wireless station's capability and request.
    2) **Shared Key** - Select 802.11 **Shared Key** authentication type.
    3) **Open System** - Select 802.11 Open System authentication.
  - **WEP Key Format** - You can select **ASCII** or **Hexadecimal** format. ASCII format stands for any combination of keyboard characters in the specified length. Hexadecimal format stands for any combination of hexadecimal digits (0-9, a-f, A-F) in the specified length.
  - **WEP Key** - Select which of the four keys will be used and enter the matching WEP key information for your network in the selected key radio button. These values must be identical on all wireless stations in your network.

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

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

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

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

☞ **Note:**

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

2) You will be reminded to reboot the device after clicking the **Save** button.

6.6.3 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 6-15. This function is not available when the operation is set to Client. As the configuration is the same in each operation mode, here we just take the Access Point for example.

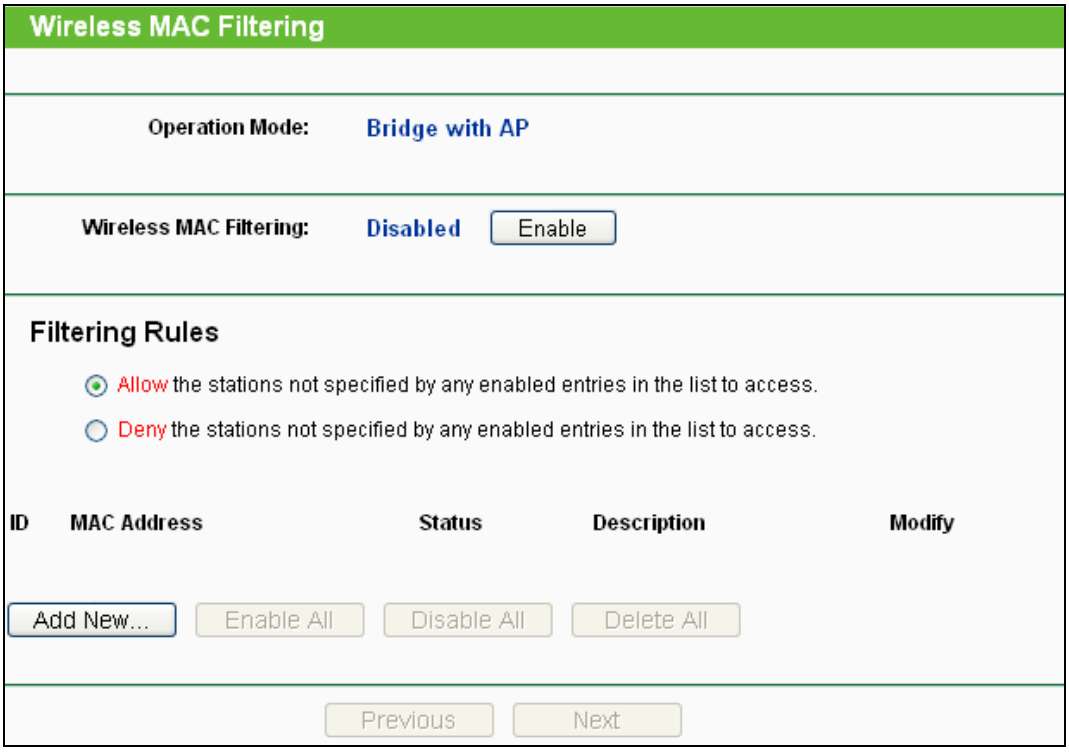


Figure 6-15 Wireless MAC address Filtering

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

- **Operation Mode -** Shows the current operation mode.
- **Wireless MAC Filtering -** Click the **Enable** button to enable the Wireless MAC Address Filtering. The default setting is disabled.

To Add a Wireless MAC Address filtering entry, click the **Add New…** button. The “Add or Modify Wireless MAC Address Filtering entry" page will appear, shown in Figure 6-16

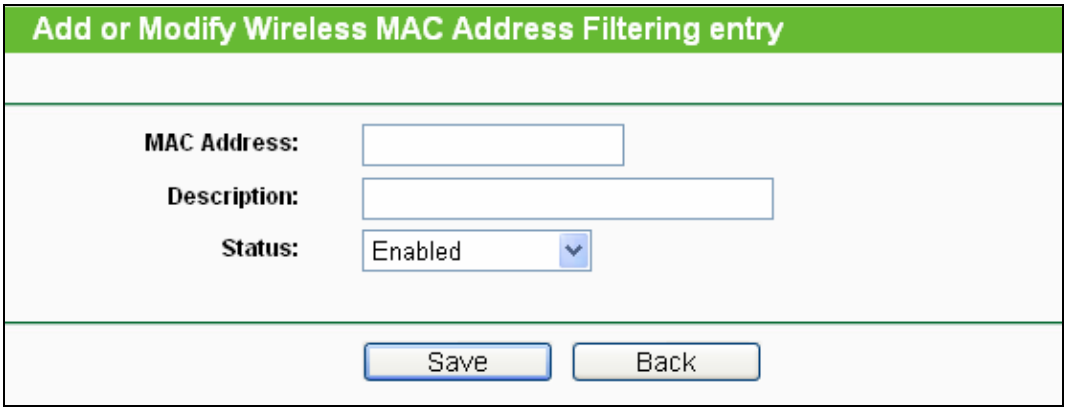


Figure 6-16 Add or Modify Wireless MAC Address Filtering entry

- **MAC Address -** Enter the wireless station's MAC address that you want to control.
- **Description -** Give a simple description of the wireless station.
- **Status -** Select a status for this entry, either **Enabled** or **Disabled**.

To set up an entry, follow these instructions:

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

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

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

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

To add additional entries, repeat steps 1-4.

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 **Disable All** button to make all entries disabled.

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

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

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

1. Click the **Enable** button to enable this function.
2. Select the radio button: **Deny the stations not specified by any enabled entries in the list to access** for **Filtering Rules.**
3. Delete all or disable all entries if there are any entries already.
4. Click the **Add New...** button and enter the MAC address 00-0A-EB-00-07-BE in the **MAC Address** field, enter Wireless Station A in the **Description** field and select **Enabled** 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

☞ **Note:**

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

6.6.4 Wireless Advanced

Selecting **Wireless** > **Wireless Advanced** will allow you to do some advanced settings for the device in the following screen shown in Figure 6-17. As the configuration for each operation mode is almost the same, we take Access Point mode for example here.

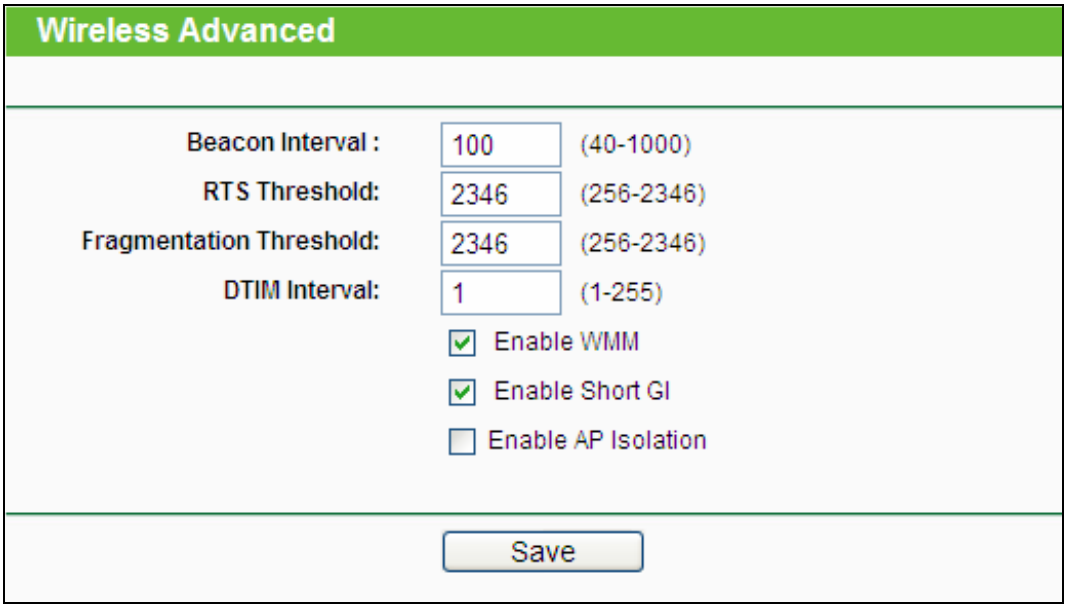


Figure 6-17 Wireless Advanced

- **Beacon Interval -** Specifies a value between 20-1000 milliseconds. The beacons are the packets sent by the device to synchronize a wireless network. Beacon Interval value determines the time interval of the beacons. The default value is 100.
- **RTS Threshold -** Specifies 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 -** 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 -** Isolates all connected wireless stations so that wireless stations cannot access each other through WLAN. This function will be disabled if WDS/Bridge is enabled.

6.6.5 Wireless Statistics

Selecting **Wireless** > **Wireless Statistics** will allow you to see the wireless transmission information in the following screen shown in Figure 6-18.

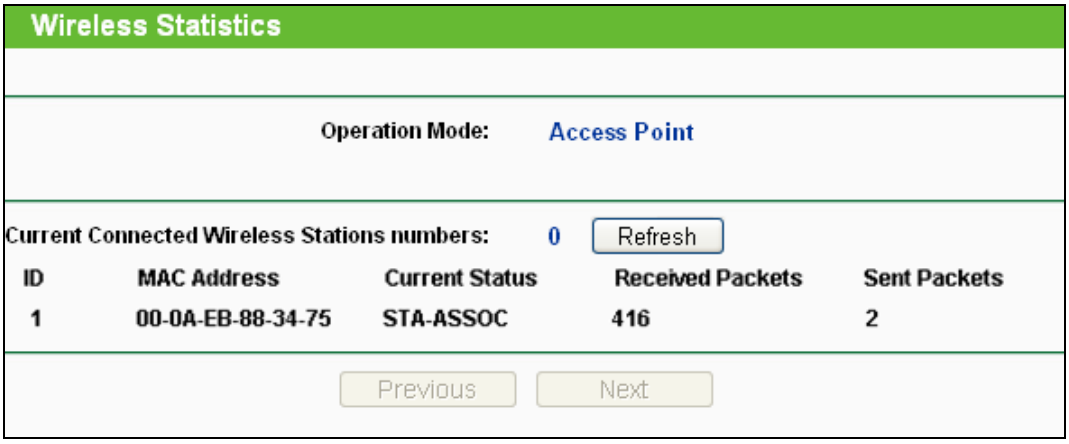


Figure 6-18 Statistics of the device attached wireless stations

- **Operation Mode -** Shows the current operation mode. If Multi-SSID is selected, all connected wireless stations will be shown here
- **MAC Address -** Shows the connected wireless station's MAC address
- **Current Status -** The connected wireless station's running status, one of STA-AUTH / STA-ASSOC / STA-JOINED / WPA / WPA-PSK / WPA2 / WPA2-PSK / AP-UP / AP-DOWN / Disconnected
- **Received Packets -** packets received by the station
- **Sent Packets -** packets sent by the station

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

6.7 DHCP

DHCP stands for Dynamic Host Configuration Protocol. The DHCP Server will automatically assign dynamic IP addresses to the computers on the network. This protocol simplifies network

management and allows new wireless devices to receive IP addresses automatically without the need to manually assign new IP addresses.

There are three submenus under the DHCP menu (shown as Figure 6-19): **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.

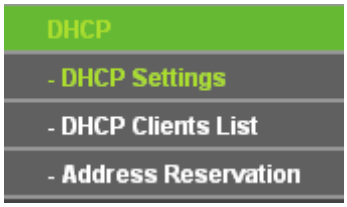


Figure 6-19 The DHCP menu

6.7.1 DHCP Settings

Selecting **DHCP** > **DHCP Settings** will enable you to set up the AP as a DHCP (Dynamic Host Configuration Protocol) server, which provides the TCP/IP configuration for all the PCs that are connected to the system on the LAN. The DHCP Server can be configured on the page (shown as Figure 6-20):

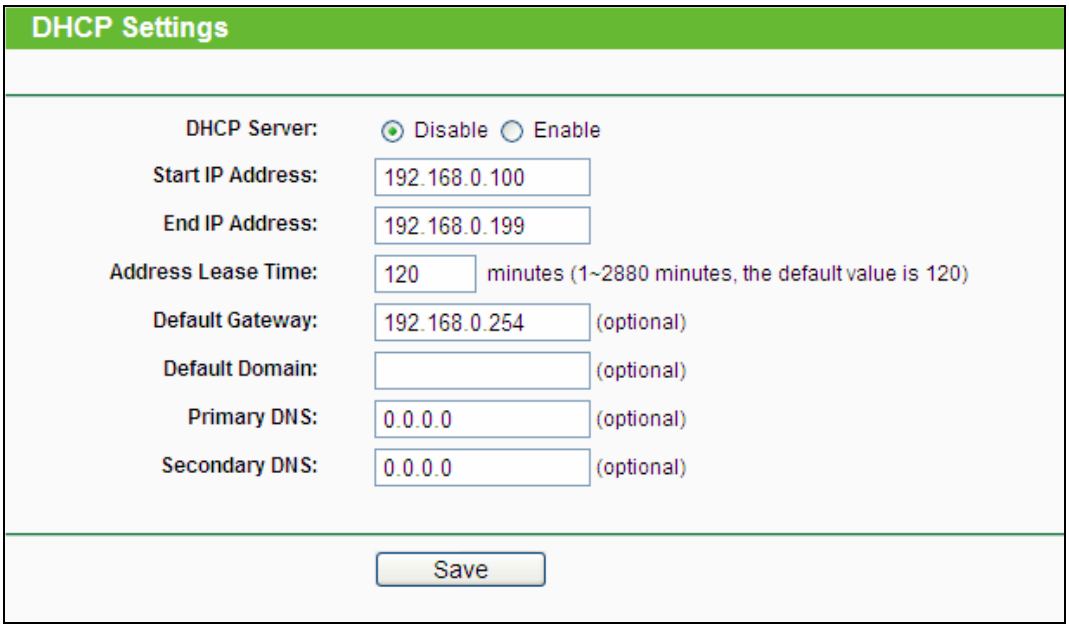


Figure 6-20 DHCP Settings

- **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 192.168.0.254.
- **Default Domain (optional) -** Enter the domain name of 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:**

1) When the device is working on Dynamic IP mode, the DHCP Server function will be disabled.
2) 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.

6.7.2 DHCP Clients List

Selecting **DHCP** > **DHCP Clients List** will enable you to view the Client Name, MAC Address, Assigned IP and Lease Time for each DHCP Client attached to the device (Figure 6-21).

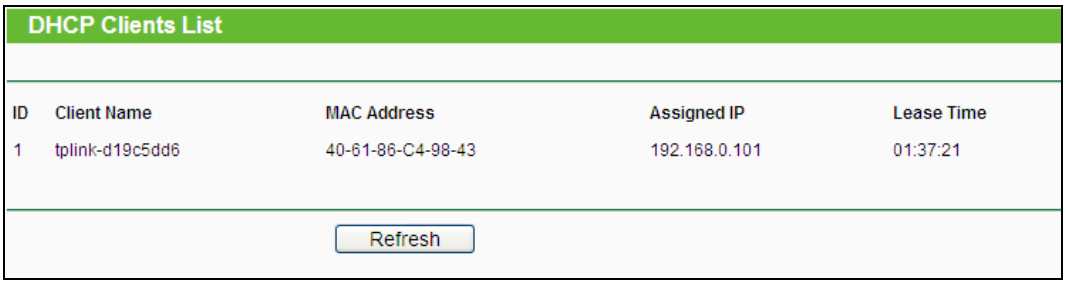


Figure 6-21 DHCP Clients List

- **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.

6.7.3 Address Reservation

Selecting **DHCP** > **Address Reservation** will enable you to specify a reserved IP address for a PC on the LAN, so the PC will always obtain the same IP address each time when it accesses the AP. Reserved IP addresses should be assigned to servers that require permanent IP settings. The screen below is used for address reservation (shown in Figure 6-22).

Figure 6-22 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 to add a new Address Reservation entry.
2. Enter the MAC address in XX-XX-XX-XX-XX-XX format and IP address in dotted-decimal notation of the computer you wish to add.
3. Click **Save** when finished.

To modify A Reserved IP address:

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

To delete all Reserved IP addresses:

1. Click **Clear All**.

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

Note:

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

6.8 System Tools

System Tools option helps you to optimize the configuration of your device. SNMP can help you to manage the device locally or remotely with specified software. The diagnostic tools (Ping and Traceroute) allow you to check the connections of your network components. 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. 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 ten submenus under the **System Tools** menu (shown as Figure 6-23): **Time Settings**, **Diagnostic**, **Firmware Upgrade**, **Factory Defaults**, **Backup & Restore**, **Reboot**, **Password**, **System Log**, **Working Mode** and **Statistics**. Clicking any of them will enable you to configure the corresponding function. The detailed explanations for each submenu are provided below.

Figure 6-23 The System Tools menu

6.8.1 Time Setting

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

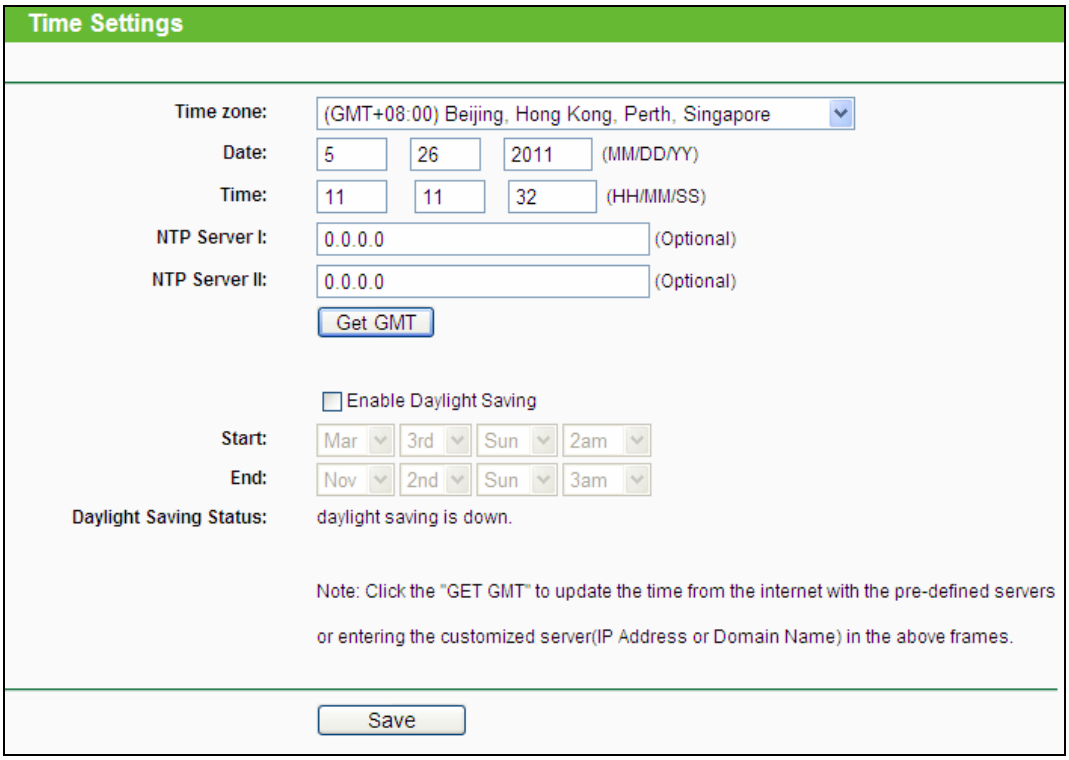


Figure 6-24 Time settings

- **Time Zone -** Select your local time zone from this pull down list.
- **Date -** Enter your local date in MM/DD/YY into the right blanks.
- **Time -** Enter your local time in HH/MM/SS into the right blanks.
- **NTP Server I / NTP Server II -** Enter the address or domain of the **NTP Server I** or **NTP Server II**, and then the Router will get the time from the NTP Server preferentially. In addition, the Router built-in some common NTP Servers, so it can get time automatically once it connects the Internet.
- **Enable Daylight Saving -** Check the box to enable the Daylight Saving function.
- **Start -** The time to start the Daylight Saving. Select the month in the first field, the week in the second field, the day in the third field and the time in the last field.
- **End -** The time to end the Daylight Saving. Select the month in the first field, the week in the second field, the day in the third field and the time in the last field.
- **Daylight Saving Status -** Displays the status whether the Daylight Saving is in use.

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**.

To set time automatically:

1. Select your local time zone.
2. Enter the address or domain of the **NTP Server I** or **NTP Server II**.
3. Click the **Get GMT** button to get system time from Internet if you have connected to the Internet.

To set Daylight Saving:

1. Check the box to enable Daylight Saving.
2. Select the start time from the drop-down lists in the **Start** field.
3. Select the end time from the drop-down lists in the **End** field.
4. Click the **Save** button to save the settings.

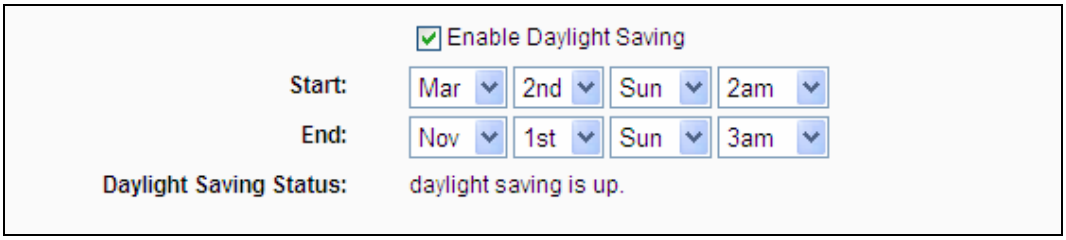


Figure 6-25 Time settings

Note:

1) This setting will be used for some time-based functions such as firewall. You must specify your time zone once you login to the router successfully, otherwise, these functions will not take effect.
2) The time will be lost if the router is turned off.
3) The Router will automatically obtain GMT from the Internet if it is configured accordingly.
4) The Daylight Saving will take effect one minute after the configurations are completed.

6.8.2 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.

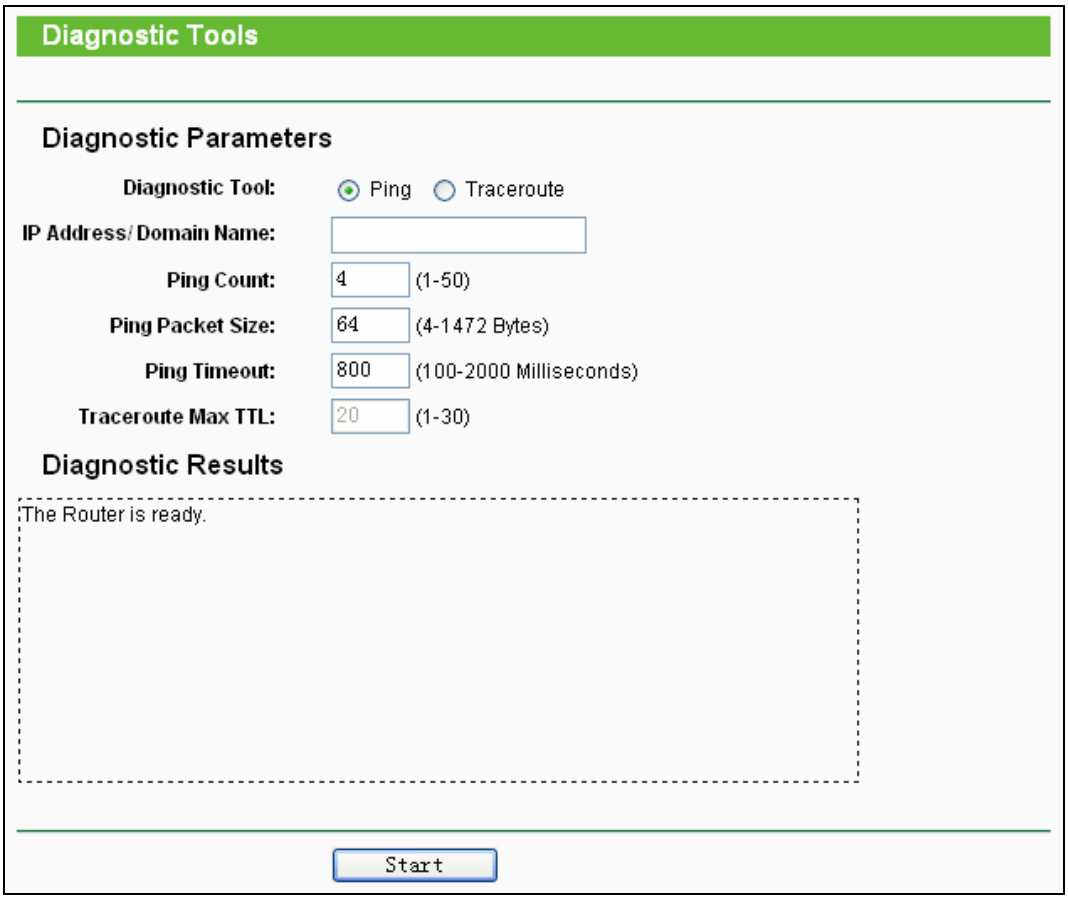


Figure 6-26 Diagnostic Tools

- **Diagnostic Tool** - Check the radio button to select one diagnostic too.
- **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.
- **Pings 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 **Start** to check the connectivity of the Internet.

The **Diagnostic Results** page displays the result of diagnosis.

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

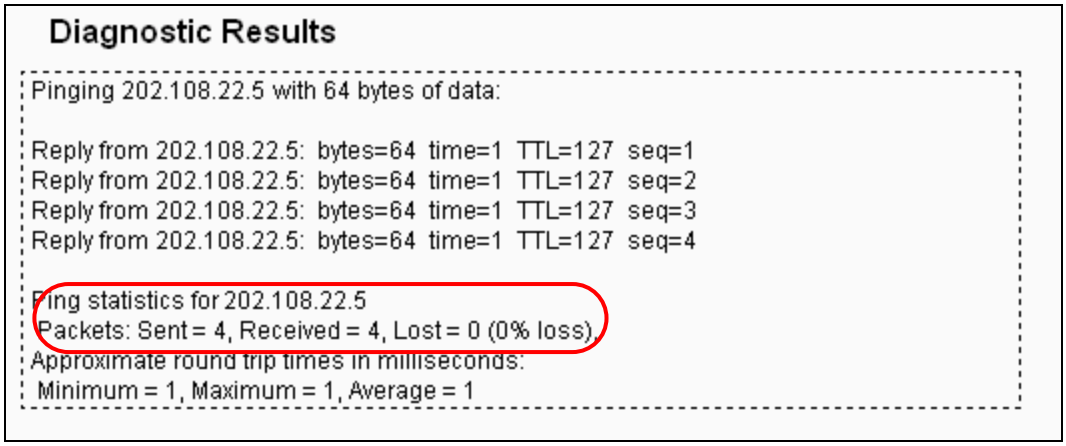


Figure 6-27 Diagnostic Results

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.

6.8.3 Firmware Upgrade

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

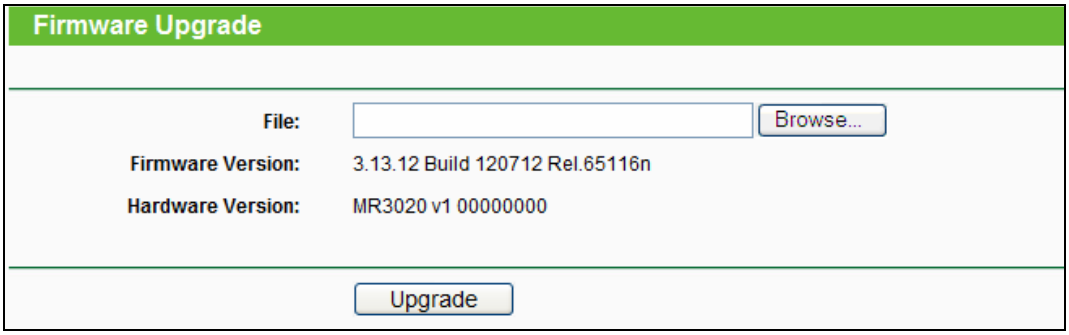


Figure 6-28 Firmware Upgrade

- **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 Router's current hardware version.

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

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 Router will reboot while the upgrading has been finished.

Note:

1) New firmware versions are posted at http://www.tp-link.com and can be downloaded for free. There is no need to upgrade the firmware unless the new firmware has a new feature you want to use. However, when experiencing problems caused by the Router rather than the configuration, you can try to upgrade the firmware.
2) When you upgrade the Router's firmware, you may lose its current configurations, so before upgrading the firmware please write down some of your customized settings to avoid losing important settings.
3) Do not turn off the Router or press the Reset button while the firmware is being upgraded. Loss of power during the upgrade could damage the Router.
4) The firmware version must correspond to the hardware.
5) The upgrade process takes a few moments and the Router restarts automatically when the upgrade is complete.

6.8.4 Factory Defaults

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

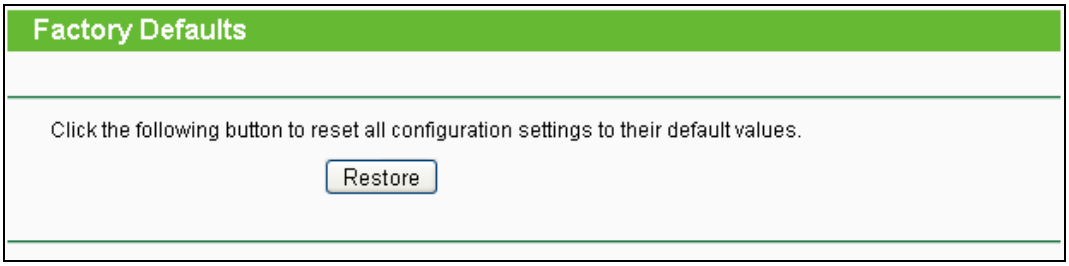


Figure 6-29 Restore Factory Default

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

- The default **User Name**: admin
- The default **Password**: admin
- The default **IP Address**: 192.168.0.254
- The default **Subnet Mask**: 255.255.255.0

Note:

All changed settings will be lost when defaults are restored.

6.8.5 Backup & Restore

Choose menu "**System Tools → Backup & Restore**", and then you can save the current configuration of the Router as a backup file and restore the configuration via a backup file as shown in Figure 6-30.

Figure 6-30 Backup & Restore Configuration

- Click the **Backup** button to save all configuration settings as a backup file in your local computer.
- To upgrade the Router's configuration, follow these instructions.
  - Click the **Browse** button to find the configuration file which you want to restore.
  - 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 Router will restart automatically then. Keep the power of the Router on during the process, in case of any damage.

6.8.6 Reboot

Choose menu "**System Tools** → **Reboot**", and then you can click the **Reboot** button to reboot the Router.

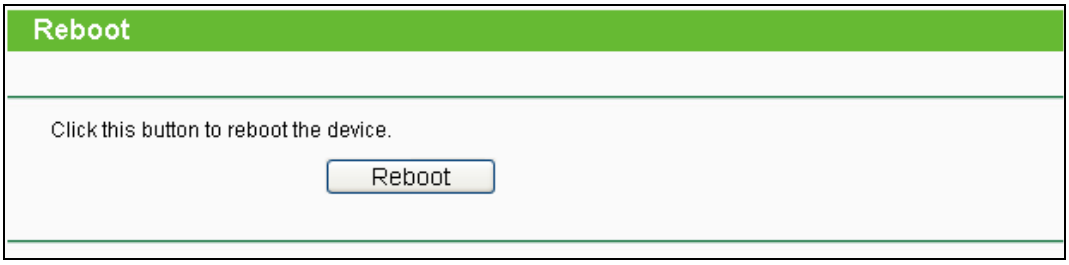


Figure 6-31 Reboot the Router

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

- 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 Router (system will reboot automatically).
- Restore the Router's settings to factory defaults (system will reboot automatically).
- Update the configuration with the file (system will reboot automatically.

6.8.7 Password

Choose menu "**System Tools** → **Password**", and then you can change the factory default user name and password of the Router in the next screen as shown in Figure 6-32.

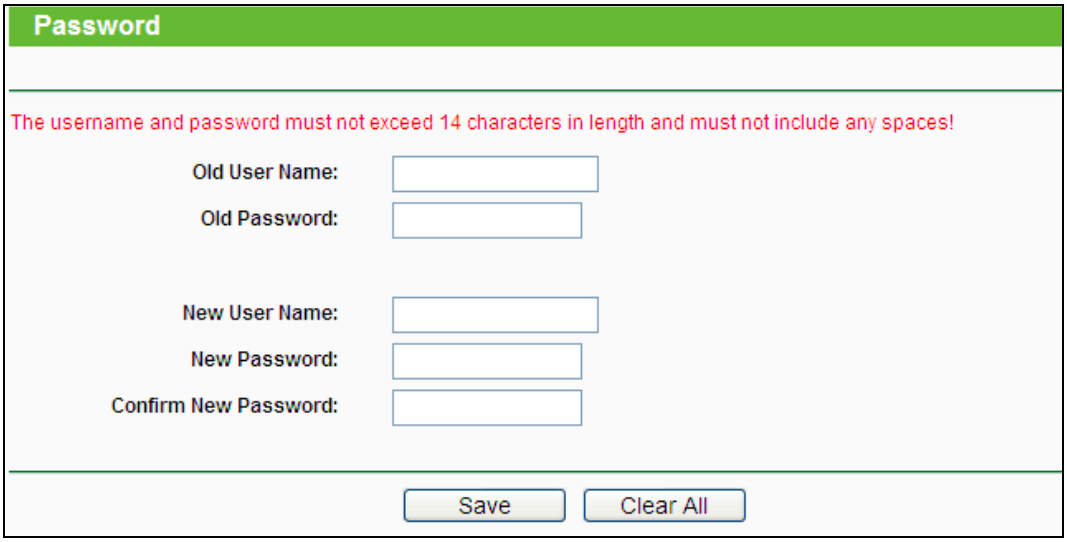


Figure 6-32 Password

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

Note:

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

Click the **Save** button when finished.

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

6.8.8 System Log

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

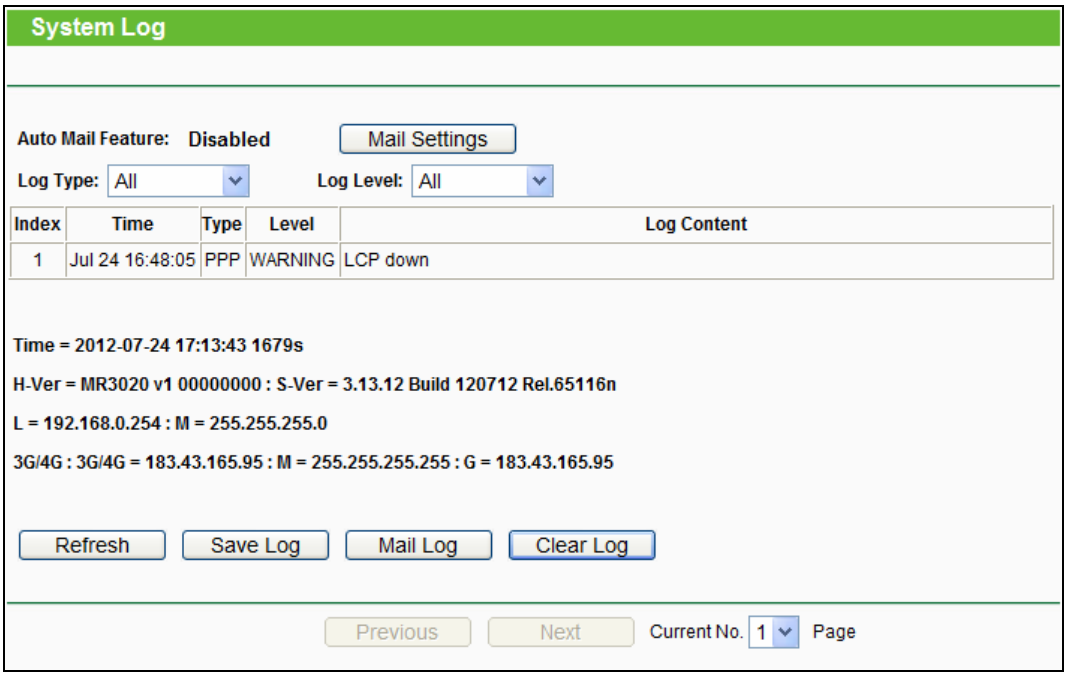


Figure 6-33 System Log

- **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.
- **Clear Log -** All the logs will be deleted from the Router permanently, not just from the page.

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

6.8.9 Working Mode

Choose menu "**System Tools** → **Working Mode**", and you can view the working mode of the Router.

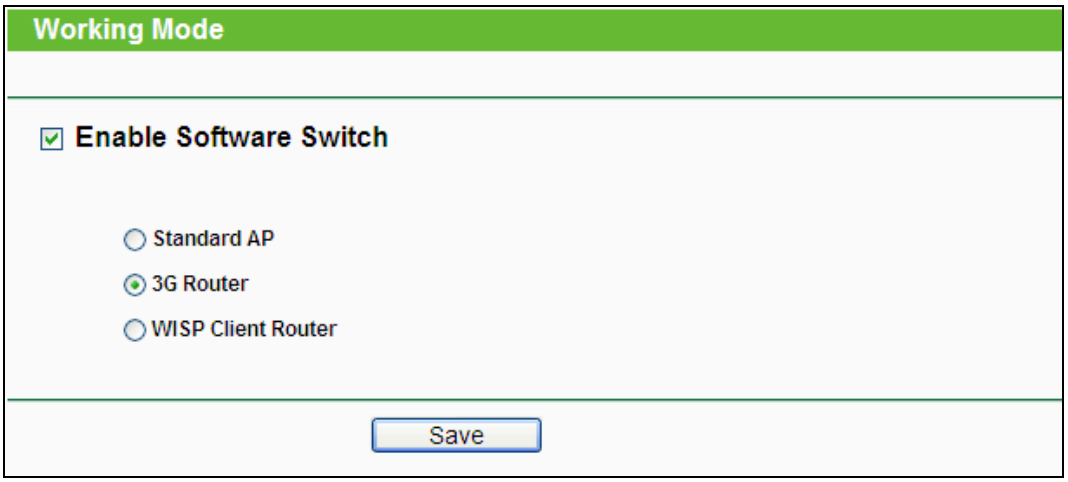


Figure 6-34 Working Mode

- **Standard AP -** In this mode, the device enables multiusers to access, and provides several wireless modes, such as AP, Client, Repeater and so on.
- **3G/4G Router -** In this mode, the device enables multiusers 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 3G/4G Router mode.
- **WISP Client Router -** In this mode, the device enables multiusers 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 WISP Client Router mode. The Ethernet port acts as a LAN port.

Note:

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

6.8.10 Statistics

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

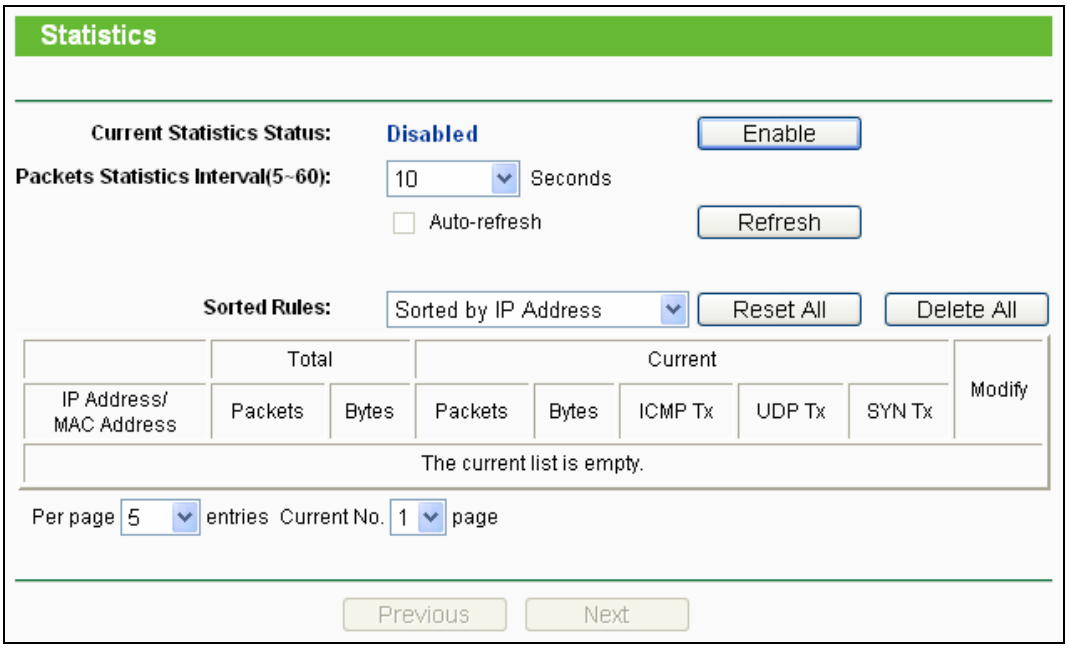


Figure 6-35 Statistics

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

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

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

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

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

Statistics Table:

IP/MAC Address		The IP and MAC address are displayed with related statistics.
Total	**Packets**	The total number of packets received and transmitted by the Router.
	Bytes	The total number of bytes received and transmitted by the Router.
Current	**Packets**	The total number of packets received and transmitted in the last Packets Statistic interval seconds.
	Bytes	The total number of bytes received and transmitted in the last Packets Statistic interval seconds.
	ICMP Tx	The number of the ICMP packets transmitted to 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 value of he entry to zero.
	Delete	Delete the existing entry in the table.

There would be 5 entries on each page. Click **Previous** to return to the previous page and **Next** to the next page.

Appendix A: FAQ

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

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

2) Connect the Ethernet cable from your ADSL Modem to the WAN port on the Router. The telephone cord plugs into the Line port of the ADSL Modem.

3) Login to the Router, click the “Network” menu on the left of your browser, and click "WAN" submenu. On the WAN page, select “PPPoE/Russia PPPoE” for WAN Connection Type. Type user name in the “User Name” field and password in the “Password” field, finish by clicking “Connect”.

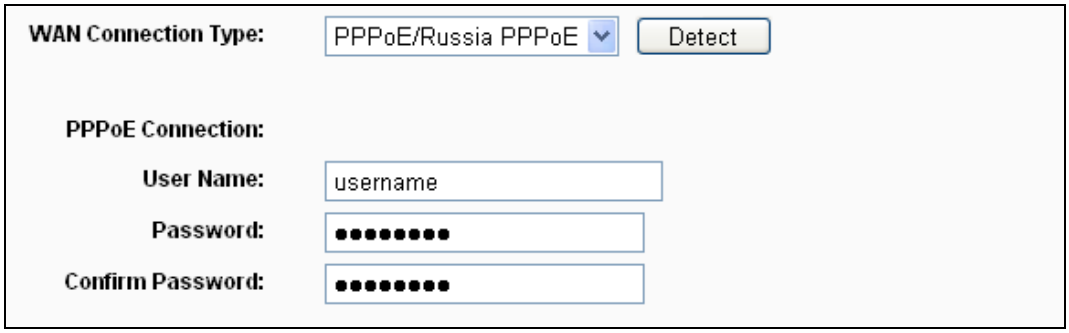


Figure A-1 PPPoE Connection Type

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

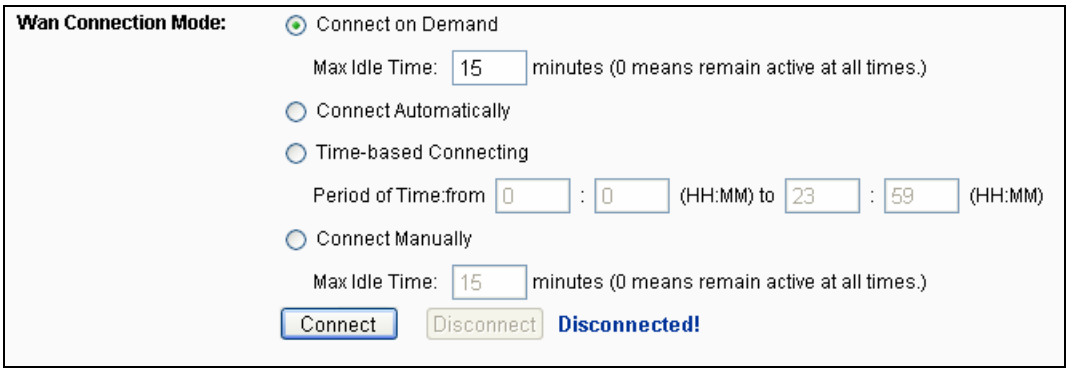


Figure A-2 PPPoE Connection Mode

Note:

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 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.

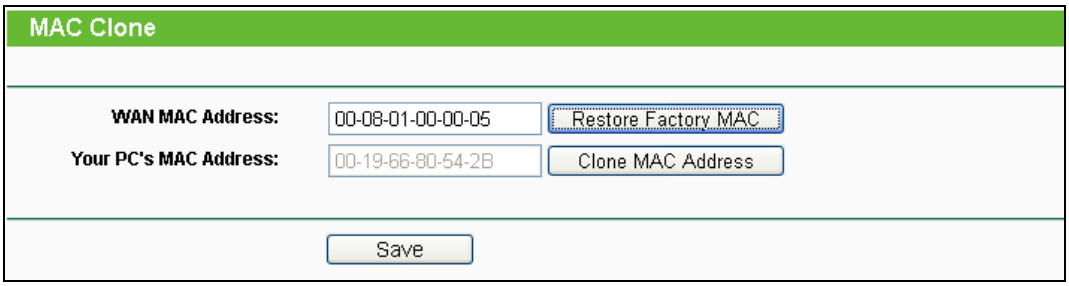


Figure A-3 MAC Clone

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

1) If you start Netmeeting as a host, 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 and make sure the H323 ALG is enabled.

3) How to configure Virtual Server: Log in to the Router, click the “**Forwarding**” menu on the left of your browser, and click "**Virtual Servers**" submenu. On the "**Virtual Servers**" page, click **Add New…**. Then on the “**Add or Modify a Virtual Server Entry**” page, enter “1720” for the “Service Port” blank, and your IP address for the “IP Address” blank, taking 192.168.0.169 for an example, remember to **Enable** and **Save**.

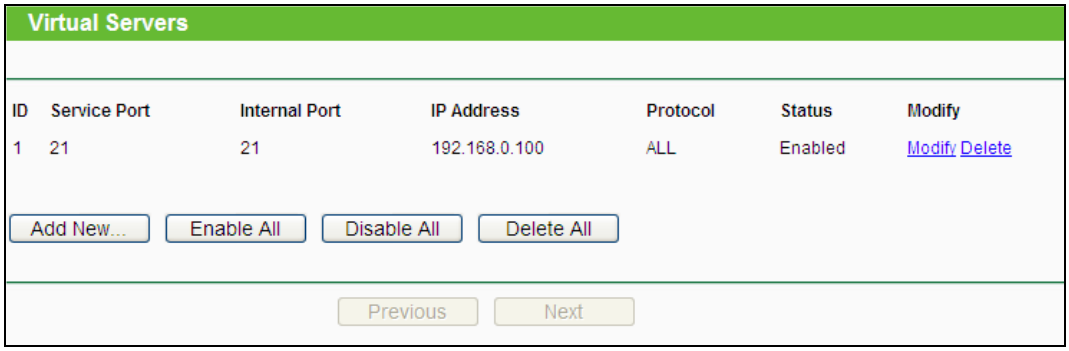


Figure A-4 Virtual Servers

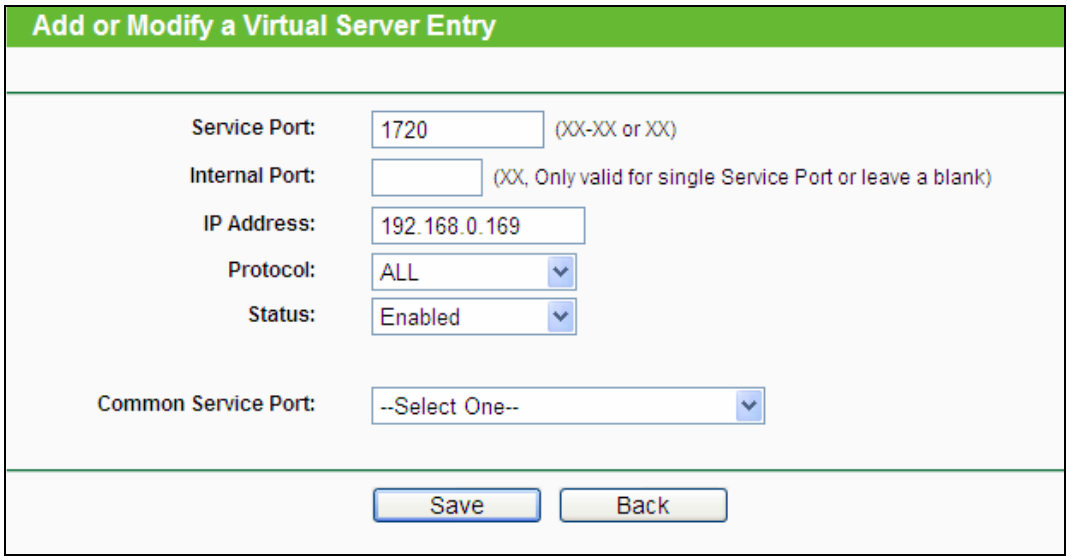


Figure A-5 Add or Modify a Virtual server Entry

Note:

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

4) How to enable DMZ Host: Log in to the Router, click the “**Forwarding**” menu on the left of your browser, and click "**DMZ**" submenu. On the "DMZ" page, click **Enable** radio button 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.

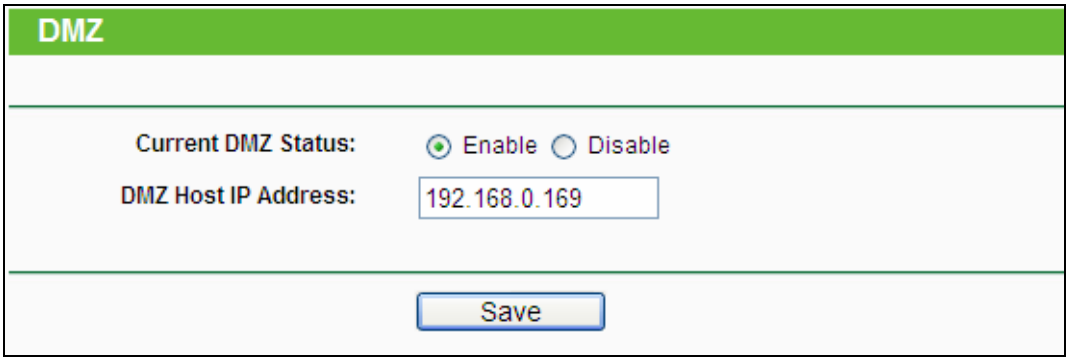


Figure A-6 DMZ

5) How to enable H323 ALG: Log in to the Router, click the "**Security**" menu on the left of your browser, and click "**Basic Security**" submenu. On the "**Basic Security**" page, check the **Enable** radio button next to **H323 ALG**. Remember to click the **Save** button.

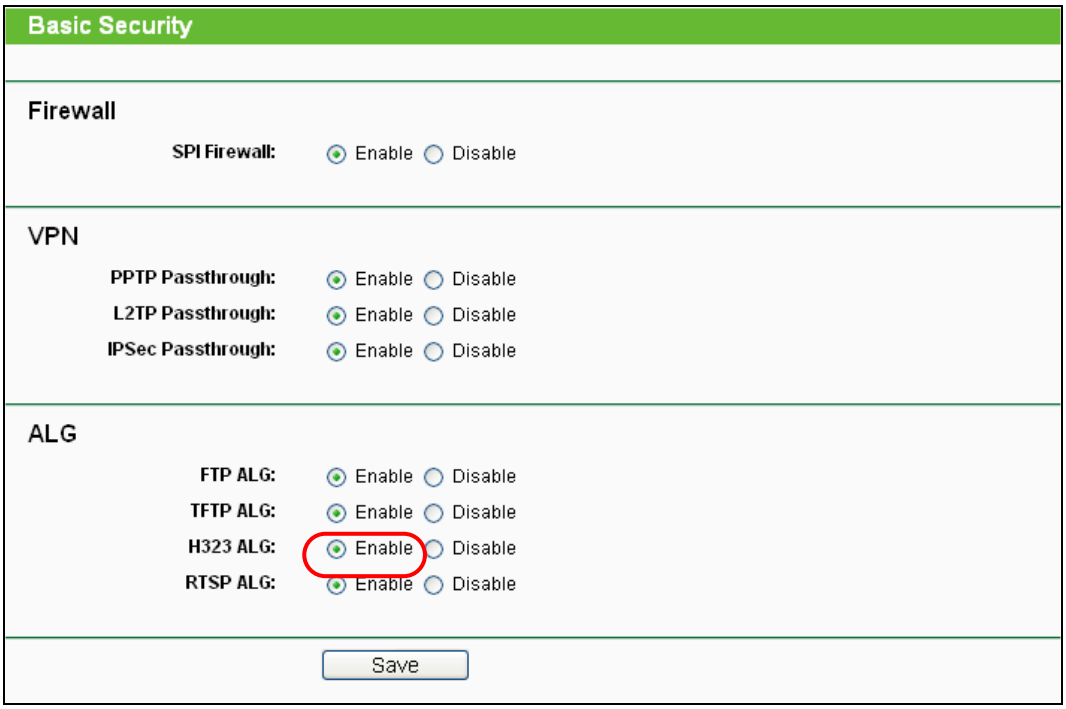


Figure A-7 Basic Security

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: Log in 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.

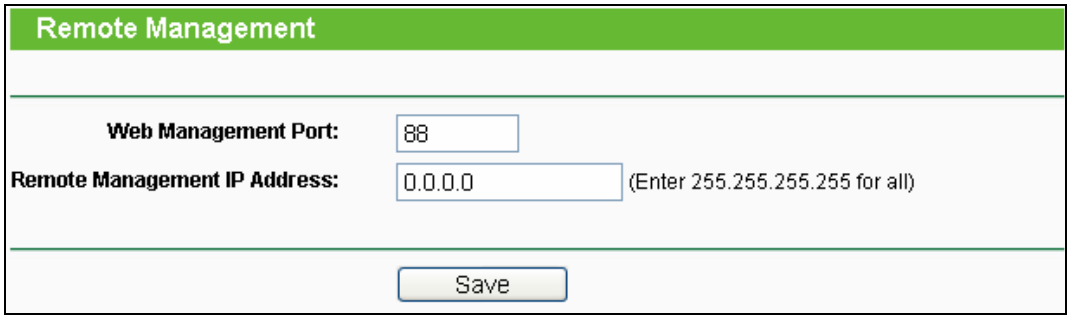


Figure A-8 Remote Management

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) Log in to the Router, click the "**Forwarding**" menu on the left of your browser, and click the "**Virtual Servers**" submenu. On the "**Virtual Servers**" page, click **Add New…**, then on the "**Add or Modify a Virtual Server**" page, enter "80" into the blank next to the "**Service Port**", and your IP address next to the "**IP Address**", assuming 192.168.0.188 for an example, remember to **Enable** and **Save**.

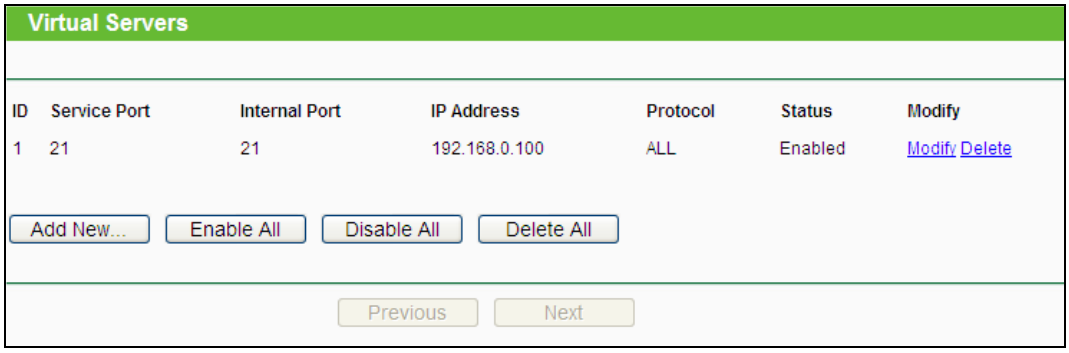


Figure A-9 Virtual Servers

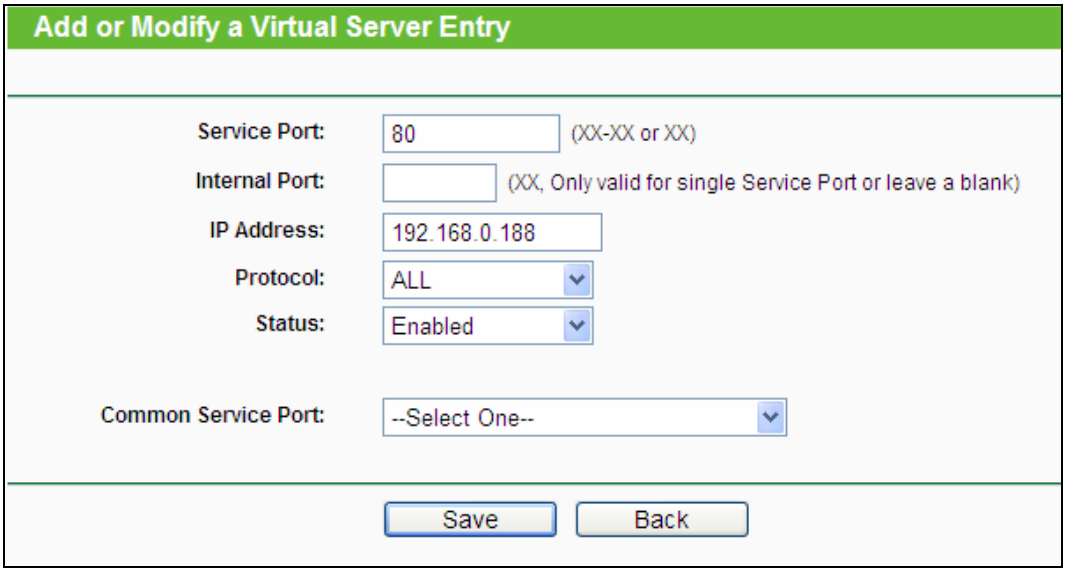


Figure A-10 Add or Modify a Virtual server Entry

5. The wireless stations cannot connect to the Router.

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

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

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

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

Appendix B: Configuring the PCs

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

1. Install TCP/IP component

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

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

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

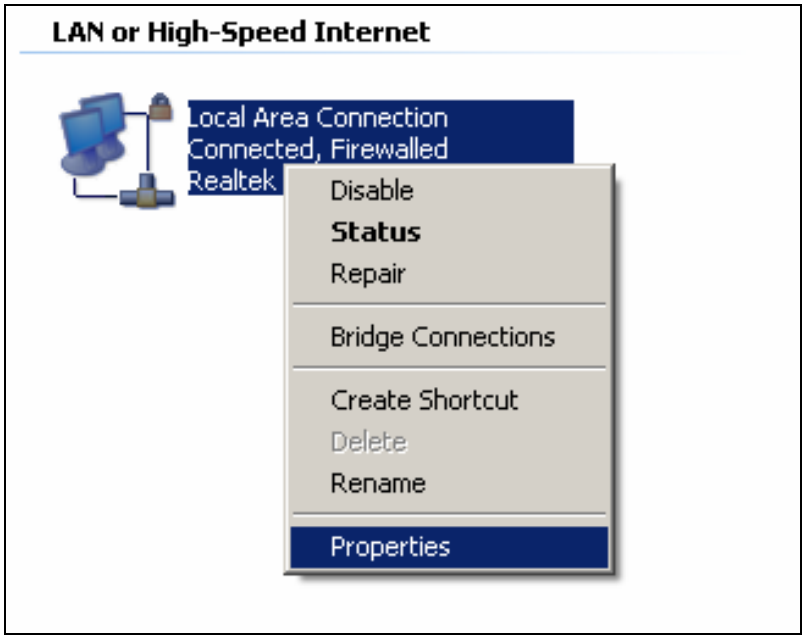


Figure B-0-1

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

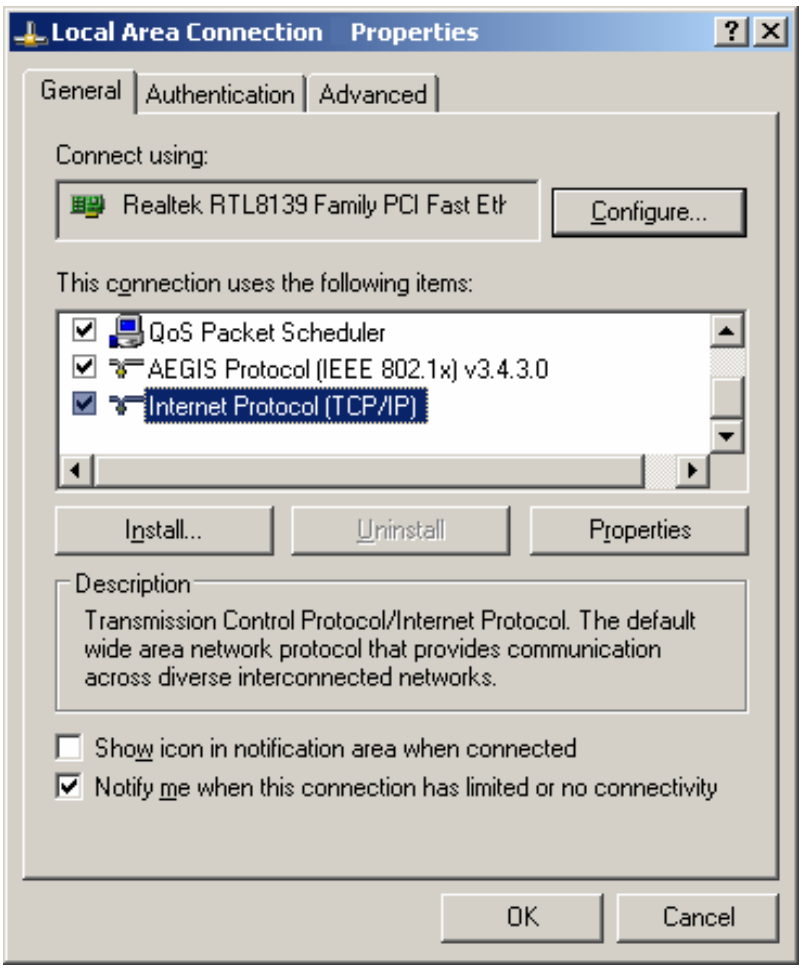


Figure B-0-2

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

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

➢ **Setting IP address automatically**

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

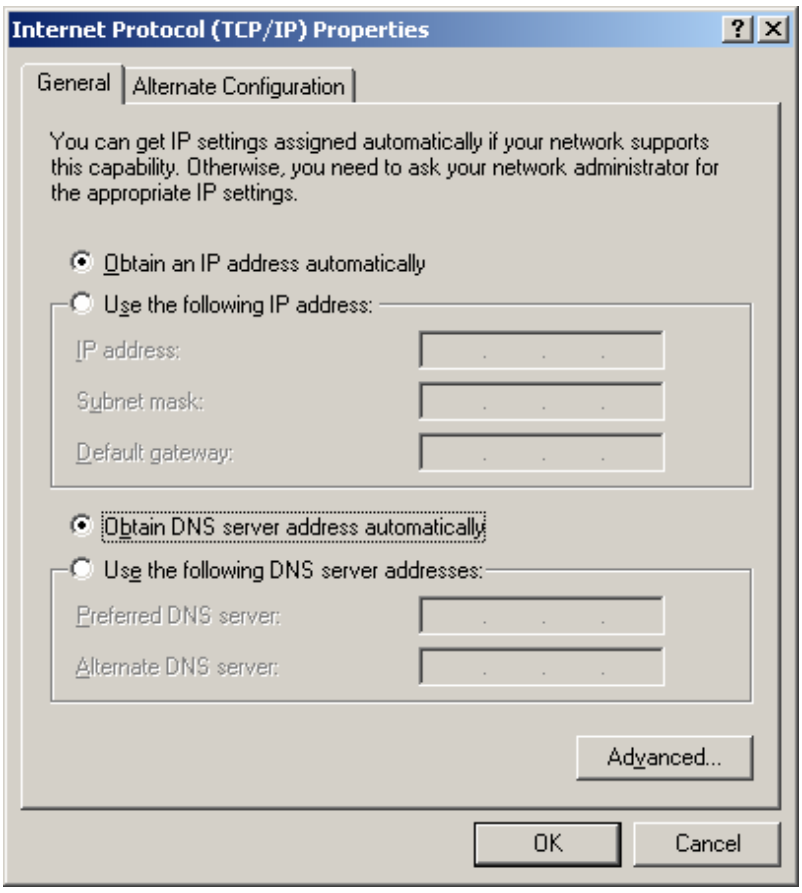


Figure B-0-3

➢ **Setting IP address manually**

1 Select **Use the following IP address** radio button, and the following items are available. If the Router's LAN IP address is 192.168.0.254, type 192.168.0.x (x is from 1 to 253) into the IP address field and 255.255.255.0 into the Subnet mask field.

2 Type the Router's LAN IP address (the default IP is 192.168.0.254) into the **Default gateway** field.

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

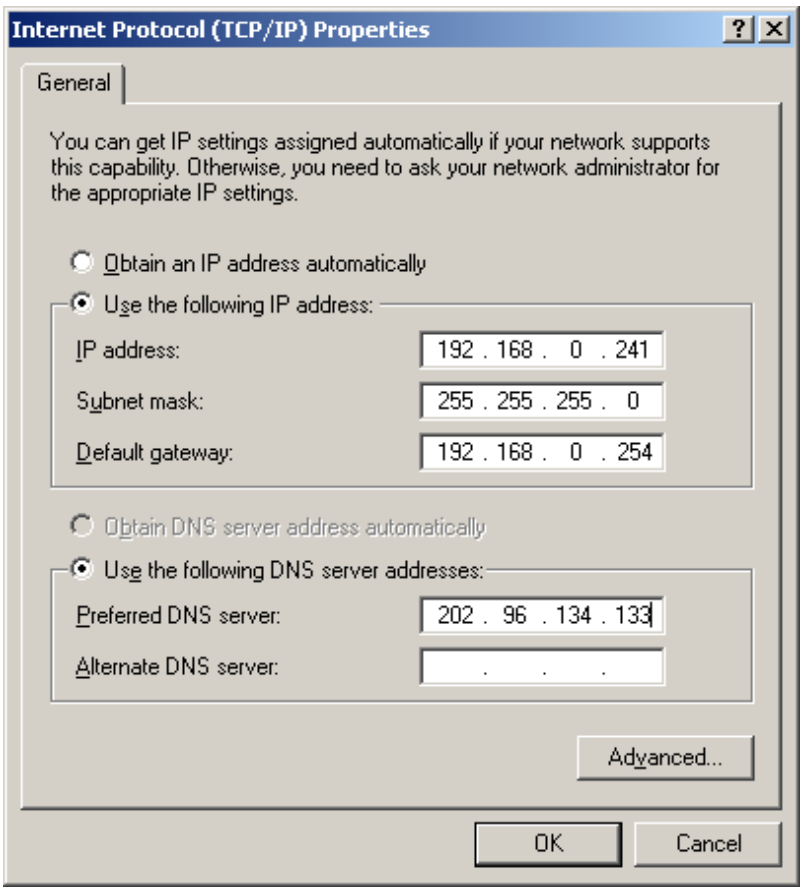


Figure B-0-4

Now click **OK** to keep your settings.

Appendix C: Specifications

General	
Standards	IEEE 802.3, 802.3u, 802.11b, 802.11g and 802.11n
Protocols	TCP/IP, PPPoE, DHCP, ICMP, NAT, SNTP
Ports	One 10/100M Auto-Negotiation LAN/WAN RJ45 port
Cabling Type	10BASE-T: UTP category 3, 4, 5 cable (maximum 100m) EIA/TIA-568 100Ω STP (maximum 100m)
	100BASE-TX: UTP category 5, 5e cable (maximum 100m) EIA/TIA-568 100Ω STP (maximum 100m)
LEDs	PWR, Internet, WLAN, Ethernet, WPS
Safety & Emissions	FCC, CE
Wireless	
Frequency Band	2.4~2.4835GHz
Radio Data Rate	11n：up to 150Mbps（Automatic） 11g：54/48/36/24/18/12/9/6M（Automatic） 11b：11/5.5/2/1M（Automatic）
Frequency Expansion	DSSS (Direct Sequence Spread Spectrum)
Modulation	DBPSK, DQPSK, CCK, OFDM, 16-QAM, 64-QAM
Security	WEP/WPA/WPA2/WPA2-PSK/WPA-PSK
Sensitivity @PER	130M: -68dBm@10% PER 108M: -68dBm@10% PER; 54M: -68dBm@10% PER 11M: -85dBm@8% PER; 6M: -88dBm@10% PER 1M: -90dBm@8% PER
Antenna Gain	5dBi
Environmental and Physical	
Temperature.	Operating : 0℃~40℃ (32℉~104℉)
	Storage: -40℃~70℃(-40℉~158℉)
Humidity	Operating: 10% ~ 90% RH, Non-condensing
	Storage: 5% ~ 90% RH, Non-condensing

Appendix D: Glossary

- **802.11n -** 802.11n builds upon previous 802.11 standards by adding MIMO (multiple-input multiple-output). MIMO uses multiple transmitter and receiver antennas to allow for increased data throughput via spatial multiplexing and increased range by exploiting the spatial diversity, perhaps through coding schemes like Alamouti coding. The Enhanced Wireless Consortium (EWC) [3] was formed to help accelerate the IEEE 802.11n development process and promote a technology specification for interoperability of next-generation wireless local area networking (WLAN) products.
- **802.11b -** The 802.11b standard specifies a wireless networking at 11 Mbps using direct-sequence spread-spectrum (DSSS) technology and operating in the unlicensed radio spectrum at 2.4GHz, and WEP encryption for security. 802.11b networks are also referred to as Wi-Fi networks.
- **802.11g -** specification for wireless networking at 54 Mbps using direct-sequence spread-spectrum (DSSS) technology, using OFDM modulation and operating in the unlicensed radio spectrum at 2.4GHz, and backward compatibility with IEEE 802.11b devices, and WEP encryption for security.
- **DDNS** (**D**ynamic **D**omain **N**ame **S**ystem) **-** The capability of assigning a fixed host and domain name to a dynamic Internet IP Address.
- **DHCP** (**D**ynamic **H**ost **C**onfiguration **P**rotocol) **-** A protocol that automatically configure the TCP/IP parameters for the all the PC(s) that are connected to a DHCP server.
- **DMZ** (**De**m**i**litarized **Z**one) **-** A Demilitarized Zone allows one local host to be exposed to the Internet for a special-purpose service such as Internet gaming or videoconferencing.
- **DNS** (**D**omain **N**ame **S**ystem) **-** An Internet Service that translates the names of websites into IP addresses.
- **Domain Name -** A descriptive name for an address or group of addresses on the Internet.
- **DSL** (**D**igital **S**ubscriber **L**ine) **-** A technology that allows data to be sent or received over existing traditional phone lines.
- **ISP** (**I**nternet **S**ervice **P**rovider) **-** A company that provides access to the Internet.
- **MTU** (**Maximum Transmission Unit**) **-** The size in bytes of the largest packet that can be transmitted.
- **NAT** (**N**etwork **A**ddress **T**ranslation) **-** NAT technology translates IP addresses of a local area network to a different IP address for the Internet.
- **PPPoE** (**P**oint to **P**oint **P**rotocol **o**ver **E**thernet) **-** PPPoE is a protocol for connecting remote hosts to the Internet over an always-on connection by simulating a dial-up connection.

- **SSID -** A **S**ervice **S**et **Id**entification is a thirty-two character (maximum) alphanumeric key identifying a wireless local area network. For the wireless devices in a network to communicate with each other, all devices must be configured with the same SSID. This is typically the configuration parameter for a wireless PC card. It corresponds to the ESSID in the wireless Access Point and to the wireless network name.
- **WEP** (**W**ired **E**quivalent **P**rivacy) **-** A data privacy mechanism based on a 64-bit or 128-bit or 152-bit shared key algorithm, as described in the IEEE 802.11 standard.
- **Wi-Fi -** A trade name for the 802.11b wireless networking standard, given by the Wireless Ethernet Compatibility Alliance (WECA, see http://www.wi-fi.net), an industry standards group promoting interoperability among 802.11b devices.
- **WLAN** (**W**ireless **L**ocal **A**rea **N**etwork) **-** A group of computers and associated devices communicate with each other wirelessly, which network serving users are limited in a local area.

Appendix E: Compatible 3G/4G USB Modem

The UMTS/HSPA/EVDO USB modems we've tested in the field are listed below. You can find the latest compatibility list in our website: http://www.tp-link.com.

Compatible 3G/4G USB Modem (Tested in the field)

HUAWEI	E122, E1262, E1550, E1552, E156, E156B, E156C, E156G, E160, E160E, E160G, E169, E1692, E169G, E173, E1750, E1752, E1756, E1762, E1782, E180, E1800, E1820, E182E, E220, E226, E230, E270, E272, E870, EC122, EC1260, EC1261, EC169, K3520, K3565, K3715, K3765, K4505, UMG1691 E398 (4G), E392 (4G)
ZTE	AC2726, AC2726i, AC2736, AC2766, AC581, K3565-Z, K3765-Z, K4505-Z, MF100, MF102, MF110, MF112, MF160, MF161, MF180, MF190, MF626, MF627, MF636, MF637, MF637U, MF645, MF668, MF668+, MU351, MF820(4G), MF821 (4G)
NOVATEL	U760, USB551L (4G)
NOKIA	CS-10, CS-12, CS-15
ONDA	MSA501HS, MT833UP, MW100HS, MW833UP
ALCATEL	X060S, X070S, X080S
4G SYSTEM	XSStick W12
CSL	U1-TF, U1
SAMSUNG	SGH-H128
BANDRICH	BANDLUXE C321, C120
BLUE CUBE	H01
Blue-Link	BL-HD72A
BM	WM78
CENTENNIAL	FlyingAngel HSUPA
DLINK	DWM-151, DWM-152, DWM-156, DWM-652

E-TOUCH	WM78
GLBETRTTER	GI0452
HAIER	CE100, OLIVE VME110, WM200
HSDC	Hsdc-03
MWALKER	MBD-100HU
MYWAVE	FW2012T
OPTION	iCon 401
PANTECH	PX500
QISDA	H21
SIERRA WIRELESS	AC306, AirCard 881U, Compass 885U, Compass 889, AirCard313U (4G)
SPRINT	U600
TELSEY	EVERYWEB HSUPA
T-MOBILE	USB STICK 120
VENUS	VT18
VIRGIN	MC760
LG	VL600 (4G)
Pantech	UML290 (4G)
Yota One	LU150 (4G)