TP-LINK®

User Guide

TL-WR902AC

AC750 Wireless Travel Router

Rev: 1.0.0
1910011679

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 © 2016 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."

This device is restricted in indoor environment only.

CE Mark Warning

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

RF Exposure Information

This device meets the EU requirements (1999/5/EC Article 3.1a) on the limitation of exposure of the general public to electromagnetic fields by way of health protection.

The device complies with RF specifications when the device used at 20 cm form your body.

National restrictions

Restricted to indoor use.

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.

Le présent appareil est conforme aux CNR d'Industrie Canada applicables aux appareils radio exempts de licence. L'exploitation est autorisée aux deux conditions suivantes :

1） l'appareil ne doit pas produire de brouillage;

2） l'utilisateur de l'appareil doit accepter tout brouillage radioélectrique subi, meme si le brouillage est susceptible d'en compromettre le fonctionnement.

Caution:

1） The device for operation in the band 5150–5250 MHz is only for indoor use to reduce the potential for harmful interference to co-channel mobile satellite systems;

2） For devices with detachable antenna(s), the maximum antenna gain permitted for devices in the band 5725-5850 MHz shall be such that the equipment still complies with the e.i.r.p. limits specified for point-to-point and non-point-to-point operation as appropriate.

Avertissement:

1） Le dispositif fonctionnant dans la bande 5150-5250 MHz est réservé uniquement pour une utilisation à l'intérieur afin de réduire les risques de brouillage préjudiciable aux systèmes de satellites mobiles utilisant les mêmes canaux;

2） Le gain maximal d'antenne permis pour les dispositifs avec antenne(s) amovible(s) utilisant la bande 5725-5850 MHz doit se conformer à la limitation P.I.R.E spécifiée pour l'exploitation point à point et non point à point, selon le cas.

Radiation Exposure Statement:

This equipment complies with IC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 20cm between the radiator & your body.

Déclaration d'exposition aux radiations:

Cet équipement est conforme aux limites d'exposition aux rayonnements IC établies pour un environnement non contrôlé. Cet équipement doit être installé et utilisé avec un minimum de 20 cm de distance entre la source de rayonnement et votre corps.

Industry Canada Statement

CAN ICES-3 (B)/NMB-3(B)

Korea Warning Statements

당해 무선설비는 운용중 전파혼신 가능성이 있음.

NCC 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。

減少電磁波影響，請妥適使用。

電磁波曝露量 MPE 標準值 1mW/cm2，本產品使用時建議應距離人體 20cm。

BSMI Notice

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.
- Adapter shall be installed near the equipment and shall be easily accessible.
- The plug considered as disconnect device of adapter.
- Use only power supplies which are provided by manufacturer and in the original packing of this product. If you have any questions, please don't hesitate to contact us.

For EU/EFTA, this product can be used in the following countries:

AT	BE	BG	CH	CY	CZ	DE	DK
EE	ES	FI	FR	GB	GR	HR	HU
IE	IS	IT	LI	LT	LU	LV	MT
NL	NO	PL	PT	RO	SE	SI	SK

Explanation of the symbols on the product label

Symbol	Explanation
⎓	DC voltage
	RECYCLING This product bears the selective sorting symbol for Waste electrical and electronic equipment (WEEE). This means that this product must be handled pursuant to European directive 2012/19/EU in order to be recycled or dismantled to minimize its impact on the environment. User has the choice to give his product to a competent recycling organization or to the retailer when he buys a new electrical or electronic equipment.

CONTENTS

Package Contents **1**

Chapter 1. Introduction **2**

1.1 Overview of the Router 2

1.2 Conventions 3

1.3 Main Features 3

1.4 Panel Layout 3

Chapter 2. Connecting the Router **5**

2.1 System Requirements 5

2.2 Installation Environment Requirements 5

2.3 Connecting the Router 5

2.3.1 Wireless Router Mode 5

2.3.2 Hotspot Mode 6

2.3.3 Access Point Mode 6

2.3.4 Range Extender Mode 7

2.3.5 Client Mode 7

Chapter 3. Quick Installation Guide **9**

3.1 TCP/IP Configuration 9

3.2 Quick Installation Guide 11

3.2.1 Wireless Router Mode 12

3.2.2 Hotspot Mode 16

3.2.3 Access Point Mode 19

3.2.4 Range Extender Mode 22

3.2.5 Client Mode 25

Chapter 4. Configuration for Wireless Router Mode **29**

4.1 Login 29

4.2 Status 30

4.3 Network 32

4.3.1 WAN 32

4.3.2 MAC Clone 41

4.3.3 LAN 42

4.4 Wireless 2.4GHz/5GHz 43

4.4.1 Wireless Settings 43

4.4.2 WPS....44
4.4.3 Wireless Security....48
4.4.4 Wireless MAC Filtering....51
4.4.5 Wireless Advanced....53
4.4.6 Wireless Statistics....54
4.5 DHCP....55
4.5.1 DHCP Settings....56
4.5.2 DHCP Client List....57
4.5.3 Address Reservation....57
4.6 Forwarding....58
4.6.1 Virtual Servers....59
4.6.2 Port Triggering....60
4.6.3 DMZ....62
4.6.4 UPnP....63
4.7 Security....64
4.7.1 Basic Security....64
4.7.2 Advanced Security....66
4.7.3 Local Management....68
4.7.4 Remote Management....69
4.8 Parental Control....70
4.9 Access Control....73
4.9.1 Rule....73
4.9.2 Host....76
4.9.3 Target....78
4.9.4 Schedule....80
4.10 Advanced Routing....82
4.10.1 Static Routing List....82
4.10.2 System Routing Table....83
4.11 Bandwidth Control....84
4.11.1 Control Settings....84
4.11.2 Rule List....84

4.12 IP & MAC Binding 86
4.12.1 Binding Setting 86
4.12.2 ARP List 88
4.13 Dynamic DNS 89
4.13.1 No-IP DDNS 89
4.13.2 Comexe.cn DDNS 90
4.13.3 Dyndns DDNS 91
4.14 System Tools 92
4.14.1 Working Mode 92
4.14.2 Time Settings 93
4.14.3 Diagnostic 94
4.14.4 Firmware Upgrade 95
4.14.5 Factory Defaults 96
4.14.6 Backup & Restore 97
4.14.7 Reboot 97
4.14.8 Password 98
4.14.9 System Log 98
4.14.10 Statistics 99
4.15 Logout 100
Chapter 5. Configuration for Access Point Mode 101
5.1 Login 101
5.2 Status 101
5.3 Operation Mode 103
5.4 Network 104
5.4.1 LAN 104
5.5 Wireless 2.4GHz/5GHz 105
5.5.1 Wireless Settings 105
5.5.2 WPS 106
5.5.3 Wireless Security 111
5.5.4 Wireless MAC Filtering 113
5.5.5 Wireless Advanced 115
5.5.6 Wireless Statistics 116

5.6 DHCP 117
5.6.1 DHCP Settings 118
5.6.2 DHCP Client List 119
5.6.3 Address Reservation 120
5.7 System Tools 121
5.7.1 Working Mode 121
5.7.2 Diagnostic 122
5.7.3 Firmware Upgrade 123
5.7.4 Factory Defaults 124
5.7.5 Backup & Restore 125
5.7.6 Reboot 125
5.7.7 Password 126
5.7.8 System Log 127
5.8 Logout 127
Chapter 6. Configuration for Range Extender Mode 128
6.1 Login 128
6.2 Status 128
6.3 Operation Mode 130
6.4 Network 131
6.4.1 LAN 131
6.5 Wireless 2.4GHz/5GHz 132
6.5.1 Wireless Settings 132
6.5.2 Wireless Security 134
6.5.3 Wireless MAC Filtering 136
6.5.4 Wireless Advanced 138
6.5.5 Wireless Statistics 139
6.6 DHCP 140
6.6.1 DHCP Settings 141
6.6.2 DHCP Client List 142
6.6.3 Address Reservation 143
6.7 System Tools 144
6.7.1 Working Mode 144

6.7.2 Diagnostic 145
6.7.3 Firmware Upgrade 146
6.7.4 Factory Defaults 147
6.7.5 Backup & Restore 148
6.7.6 Reboot 148
6.7.7 Password 149
6.7.8 System Log 150
6.8 Logout 150
Chapter 7. Configuration for Client Mode 151
7.1 Login 151
7.2 Status 151
7.3 Operation Mode 153
7.4 Network 154
7.4.1 LAN 154
7.5 Wireless 2.4GHz/5GHz 155
7.5.1 Wireless Settings 155
7.5.2 Wireless Security 156
7.5.3 Wireless Advanced 158
7.5.4 Wireless Statistics 159
7.6 DHCP 160
7.6.1 DHCP Settings 160
7.6.2 DHCP Client List 162
7.6.3 Address Reservation 162
7.7 System Tools 164
7.7.1 Working Mode 164
7.7.2 Diagnostic 165
7.7.3 Firmware Upgrade 166
7.7.4 Factory Defaults 167
7.7.5 Backup & Restore 168
7.7.6 Reboot 168
7.7.7 Password 169
7.7.8 System Log 170

7.8 Logout 170
Chapter 8. Configuration for Hotspot Mode 171
8.1 Login 171
8.2 Status 172
8.3 Network 174
8.3.1 WAN 174
8.3.2 MAC Clone 183
8.3.3 LAN 184
8.4 Wireless 2.4GHz/5GHz 185
8.4.1 Wireless Settings 185
8.4.2 WPS 186
8.4.3 Wireless Security 191
8.4.4 Wireless MAC Filtering 193
8.4.5 Wireless Advanced 195
8.4.6 Wireless Statistics 196
8.5 DHCP 197
8.5.1 DHCP Settings 198
8.5.2 DHCP Client List 199
8.5.3 Address Reservation 199
8.6 Forwarding 200
8.6.1 Virtual Servers 201
8.6.2 Port Triggering 202
8.6.3 DMZ 204
8.6.4 UPnP 205
8.7 Security 206
8.7.1 Basic Security 206
8.7.2 Advanced Security 208
8.7.3 Local Management 210
8.7.4 Remote Management 211
8.8 Parental Control 212
8.9 Access Control 215
8.9.1 Rule 215

8.9.2 Host 218
8.9.3 Target 220
8.9.4 Schedule 222
8.10 Advanced Routing 224
8.10.1 Static Routing List 224
8.10.2 System Routing Table 225
8.11 Bandwidth Control 226
8.11.1 Control Settings 226
8.11.2 Rule List 226
8.12 IP & MAC Binding 228
8.12.1 Binding Setting 228
8.12.2 ARP List 230
8.13 Dynamic DNS 231
8.13.1 No-IP DDNS 231
8.13.2 Comexe.cn DDNS 232
8.13.3 Dyndns DDNS 233
8.14 System Tools 234
8.14.1 Working Mode 234
8.14.2 Time Settings 235
8.14.3 Diagnostic 236
8.14.4 Firmware Upgrade 237
8.14.5 Factory Defaults 238
8.14.6 Backup & Restore 239
8.14.7 Reboot 239
8.14.8 Password 240
8.14.9 System Log 241
8.14.10 Statistics 241
8.15 Logout 243
Appendix A: FAQ 244
Appendix B: Configuring the PC 249
Appendix C: Specifications 252
Appendix D: Glossary 254

Package Contents

The following items should be found in your package:

- One TL-WR902AC AC750 Wireless Travel Router
- Quick Installation Guide
- One RJ-45 Ethernet Cable
- One USB Cable
- One Power Adapter

Note:

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

Chapter 1. Introduction

1.1 Overview of the Router

Small enough to fit in the average pocket, the TL-WR902AC AC750 Wireless Travel Router is uniquely suited to provide robust wireless networking to travelers, students, or anyone else for work or play.

Incredible Speed

TL-WR902AC supports the newest 802.11ac standards, and provides backward compatibility with older 802.11b/g standards as well. The up-to-750Mbps wireless speed makes it ideal for handling multiple data streams at the same time, which ensures your network stable and smooth.

Multiple Operation Modes

The TL-WR902AC AC750 Wireless Travel Router supports five operation modes. Wireless Router mode creates an instant private wireless network and share Internet to multiple Wi-Fi devices, which is suitable for most hotel and home network. Hotspot mode accesses the Internet wirelessly in areas with no wired ISP infrastructure. AP mode includes three sub modes: Access Point, Ranger Extender and Client. Access Point mode creates a wireless network for Wi-Fi devices. The wireless devices are exposed to the wired network. Range Extender mode extends your home wireless range by copying the same wireless name and password. Client mode works as a wireless adapter for any Ethernet-enabled devices, such as Smart TV, Game Console and PC.

Reliable Security Protections

With multiple protection measures, including SSID broadcast control and WiFi protected Access (WPA2-PSK, WPA-PSK), advanced Firewall protections encryption, as well as wireless LAN 64/128/152-bit WEP, the TL-WR902AC AC750 Wireless Travel Router provides complete data privacy.

Flexible Access Control

The TL-WR902AC AC750 Wireless Travel Router supports Virtual Server and DMZ host for Port Triggering, and then the network administrators can manage and monitor the network in real time with the remote management function.

Since the router is compatible with virtually all the major operating systems, it is very easy to manage. Quick Setup Wizard is supported and detailed instructions are provided step by step in

this user guide. Before installing the Router, please look through this guide to know all the Router's functions.

1.2 Conventions

The Router or TL-WR902AC mentioned in this guide stands for TL-WR902AC AC750 Wireless Travel Router without any explanation.

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

You can set the parameters according to your demand.

1.3 Main Features

- Complies with IEEE 802.11ac
- Wireless speed up to 750Mbps
- Powered by external power adapter or USB connection to computer
- Travel size design, ideal for home or travel use
- Compact and portable, powerful wireless signal as well
- Perfectly compatible with almost all the 2.4GHz and 5GHz Wi-Fi devices
- Supports AP, Router, Range Extender, Hotspot, and Client modes
- Supports WPA/WPA2, WPA-PSK/WPA2-PSK, WEP encryptions

1.4 Panel Layout

- **LED**

LED	Status	Indication
Power	On	The router is on.
	Blinking	The router is initializing or being upgraded.
Internet	On	The Internet is available.
	Off	The Internet is unavailable.
Wireless	On	The wireless network is enabled.
	Blinking	The router fails to connect to the host network when in Repeater or Client Mode.
	Off	The wireless network is disabled.
USB	On	A USB device is connected.
	Off	No USB device is connected.
WPS	On	The LED light stays for 5 minutes when a WPS connection is established, then goes off.
	Blinking	WPS connection is in progress.
	Off	No WPS connection is established.

- **Mode Switch:** This button is used to switch the working mode of the router.
- **LAN/WAN:** Functions as the LAN port in Hotspot, Range Extender, and Access Point mode. Functions as the WAN port in Wireless Router mode. As LAN, it connects the Router to the local PC; as WAN, it enables you connect the DSL/cable Modem, or Ethernet.
- **Power:** It is used to connect the provided power adapter.
- **Reset：** It is used to reset the Router to its factory defaults. With the Router powered on, use a pin to press and hold the **Reset** button (about 5 seconds) until the LED becomes quick-flash from slow-flash. And then release the button and wait the Router to reboot to its factory default settings.
- **3G/4G USB:** It is used to plug a 3G/4G modem.

Chapter 2. Connecting the Router

2.1 System Requirements

- Each PC in the LAN needs a working Ethernet Adapter
- TCP/IP protocol must be installed on each PC
- Web browser, such as Microsoft Internet Explorer 5.0 or later, Mozilla Firefox, Apple Safari
- If the device is configured to Wireless Router/Access Point mode, you also need Broadband Internet Access Service (DSL/Cable/Ethernet)
- One DSL/Cable Modem that has an RJ45 connector (which is not necessary if the Router is connected directly to the Ethernet.)

2.2 Installation Environment Requirements

- Place the Router in a well-ventilated place far from any heater or heating vent
- Place the Router in a location where it can be connected to the various devices as well as to a power source
- 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

Before installing the Router, please make sure your broadband service provided by your ISP is available. If there is any problem, please contact with your ISP.

Please choose the operation mode you need and carry out the corresponding steps. There are five operation modes supported by this router: **Wireless Router, Hotspot, Access Point, Range Extender** and **Client**.

2.3.1 Wireless Router Mode

As a wireless router, TL-WR902AC enables multi-user to share a wired (Ethernet) connection to wireless devices, such as in a hotel room, small office, etc.

The default mode of TL-WR902AC is Wireless Router. On this mode, the wired port LAN/WAN works as WAN, it can be connected to DSL Modem or directly connected to a wired network with

an Ethernet cable. And you can plug in a 3G/4G USB modem to obtain a continuous network. Devices could connect to the router wirelessly.

1. Switch the mode of the router on Share ETH.
2. Connect the router according to the steps A to E in the diagram above.

   Tips: Plug in a 3G/4G USB modem with a SIM/UIM card as you need.

2.3.2 Hotspot Mode

In Hotspot mode, TL-WR902AC enables user to create your personal Wi-Fi Hotspot from a public Wi-Fi network such as in a hotel room, trade show, etc.

On this mode, the LAN port devices share the same IP from public Wi-Fi through Wireless port. While connecting to public Wi-Fi, the Wireless port works as a WAN port. The LAN/WAN port acts as a LAN port.

1. Switch the mode of the router on Share Hotspot.
2. Connect the router according to the steps A to C in the diagram above.

2.3.3 Access Point Mode

As the supplement of wired LAN, TL-WR902AC enables the wired LAN to connect to the Internet wirelessly.

Connect TL-WR902AC to the power and connect the Ethernet cable correctly, you can surf the Internet by connecting your PC(s) to the router wirelessly.

On this mode, the wired port LAN/WAN works as LAN. The Pre-encryption function is opened by default and the default password is the last unique eight numbers of each Router's MAC address.

1. Switch the mode of the router on AP/Rng Ext/Client.
2. Connect the router according to the steps A to E in the diagram above.

2.3.4 Range Extender Mode

TL-WR902AC is used to extend the range of wireless signal of the existing AP or wireless router.

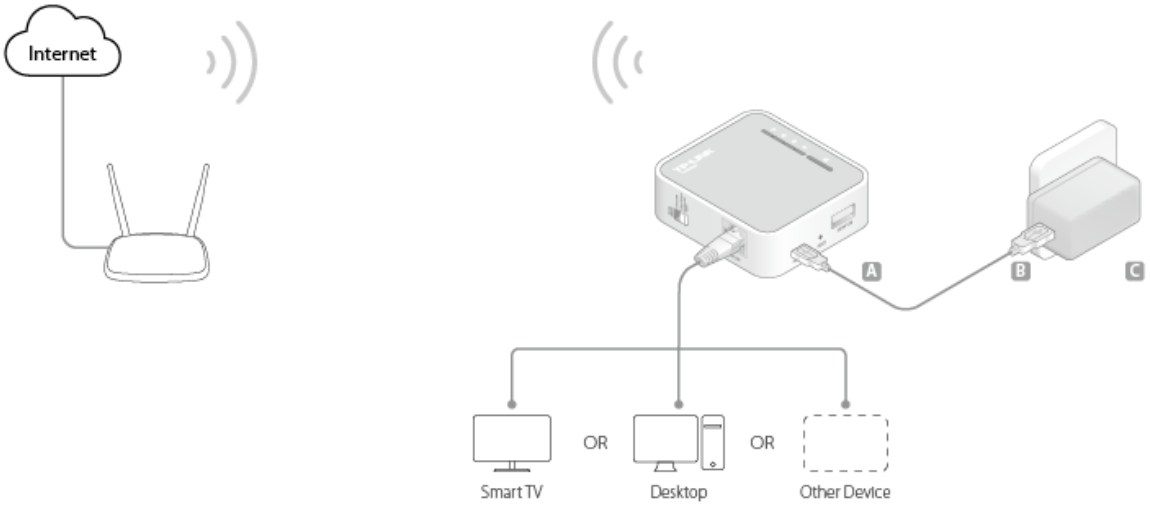
On this mode, the wired port LAN/WAN works as LAN. Computer could connect to the device by either wired or wireless way.

1. Switch the mode of the router on AP/Rng Ext/Client.
2. Connect the router according to the steps A to C in the diagram above.

2.3.5 Client Mode

TL-WR902AC is used as a wireless network card to connect the wireless network signal or wireless router.

On this mode, the wired port LAN/WAN works as LAN.



1. Switch the mode of the router on AP/Rng Ext/Client.
2. Connect the router according to the steps A to C in the diagram above.

Chapter 3. Quick Installation Guide

This chapter will show you how to configure the basic functions of your TL-WR902AC AC750 Wireless Travel Router using **Quick Setup Wizard** within minutes.

3.1 TCP/IP Configuration

The default IP addresses of the TL-WR902AC have two: 192.168.0.254 for AP mode, Range Extender mode and Client mode, and 192.168.0.1 for Wireless Router mode and HOTSPOT mode. And the default Subnet Mask is 255.255.255.0. These values can be changed as you desire. In this guide, we use all the default values for description. Here we take “192.168.0.254” as an example.

Connect the local PC to the LAN port of the Router. And then you can configure the IP address for your PC as the following steps:

1) Set up the TCP/IP Protocol in **"Obtain an IP address automatically"** mode on your PC. If you need instructions as to how to do this, please refer to Appendix B: "Configuring the PC”.

2) Then the built-in DHCP server will assign IP address for the PC.

Then connect to the Router through wireless connection following the steps below:

1) Click the icon at the bottom of your desktop. Click refresh button, and then select the default SSID of the Router. Click **Connect**.

2) Enter the **Security key**. Click **OK**.

3) If you can see **Connected** after the default SSID, you've successfully connected to the wireless network.

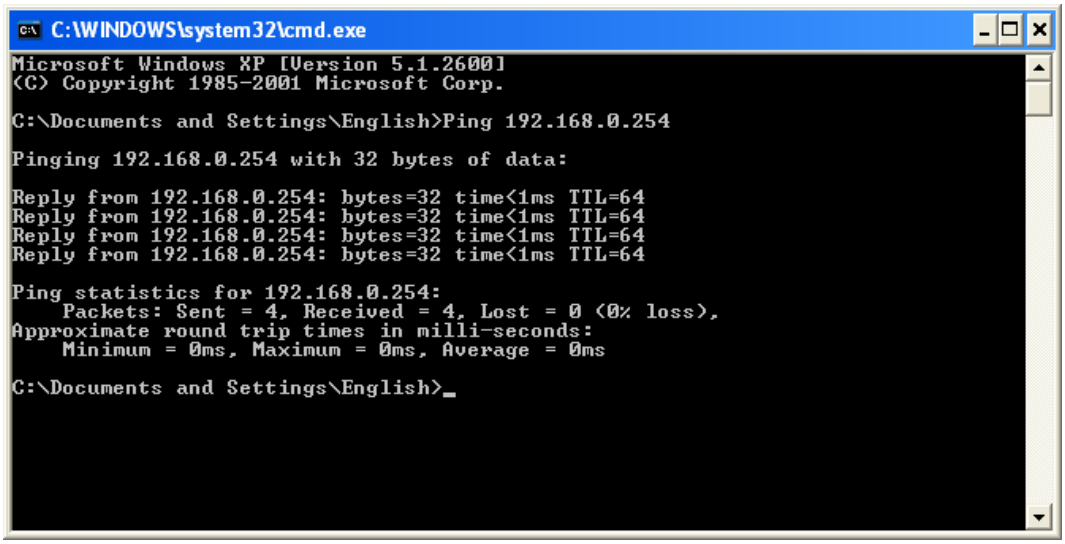
Note:

1. The default **SSID** and **Password** of your Router are on the Wi-Fi Info Card. Both are case-sensitive.
2. The pre-encryption function is enabled by default and the default **Network key**/**Security key** is the **Password** on the label.

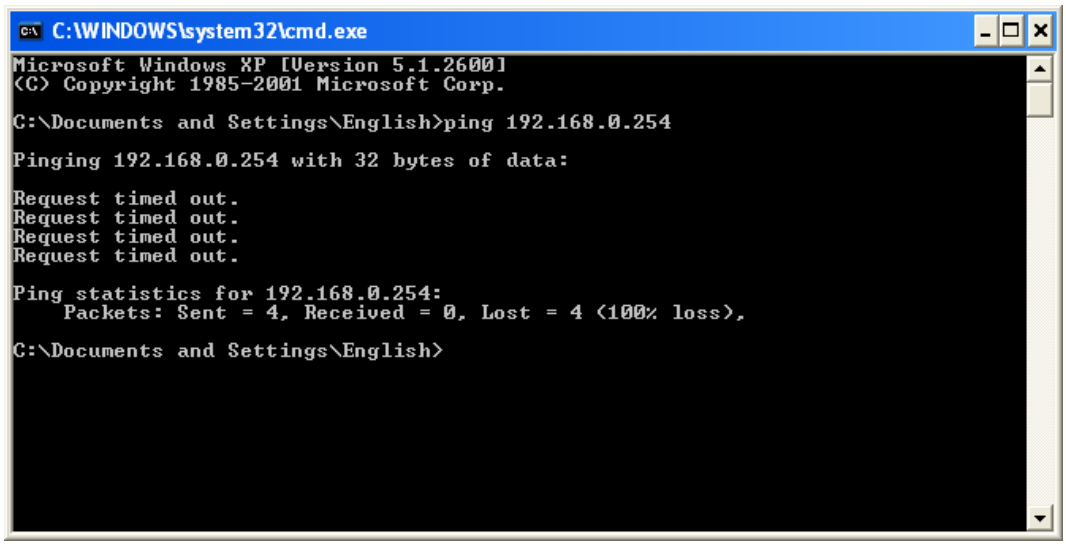
Now, you can run the Ping command in the **command prompt** to verify the network connection between your PC and the Router.

Open a command prompt, and type *ping 192.168.0.254*, and then press **Enter**.

- If the result displayed is similar to the figure below, it means the connection between your PC and the Router has been established well.



- If the result displayed is similar to the figure below, it means the connection between your PC and the Router has failed.



Please check the connection following these steps:

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

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

☞ **Note:**

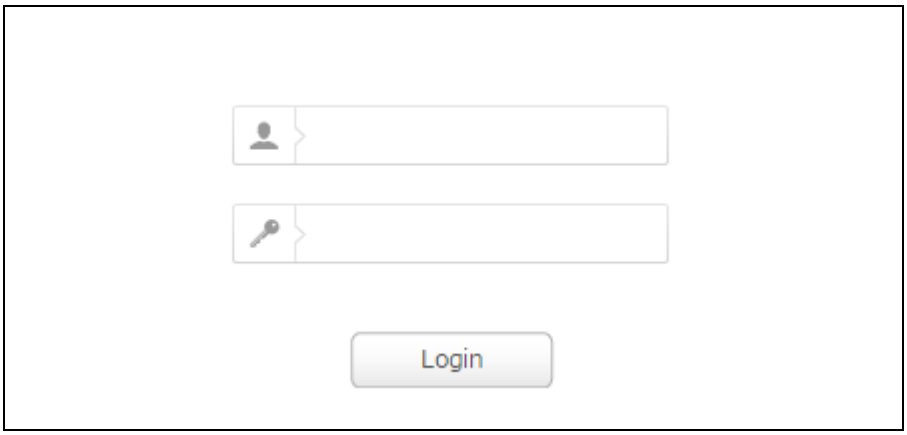
If the Router's IP address is 192.168.0.254, your PC's IP address must be within the range of 192.168.0.1 ~ 192.168.0.253.

3.2 Quick Installation Guide

With a Web-based utility, it is easy to configure and manage the TL-WR902AC. The Web-based utility can be used on any Windows, Macintosh or UNIX OS with a Web browser, such as Microsoft Internet Explorer, Mozilla Firefox or Apple Safari.

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

   After a moment, a login window will appear. Enter **admin** for the User Name and Password, both in lower case letters. Then click the **Login** button or press the **Enter** key.



Note:

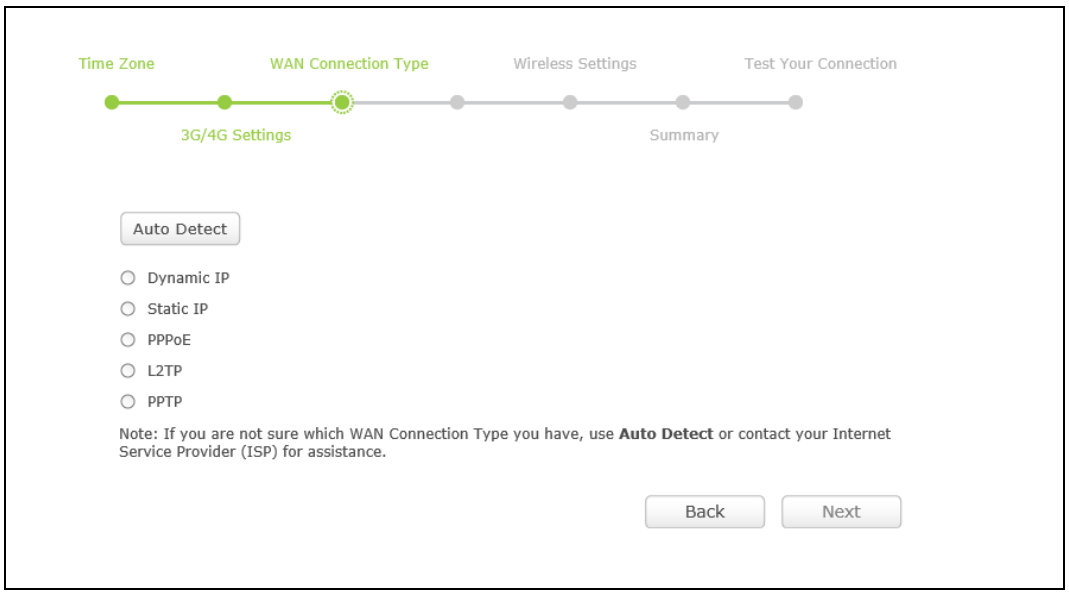
If the above screen does not pop-up, it means that your Web-browser has been set to a proxy. Go to Tools menu>Internet Options>Connections>LAN Settings, in the screen that appears, cancel the Using Proxy checkbox, and click **OK** to finish it.

2. After a successful login, you can click the **Quick Setup** menu to quickly configure your Router.

3.2.1 Wireless Router Mode

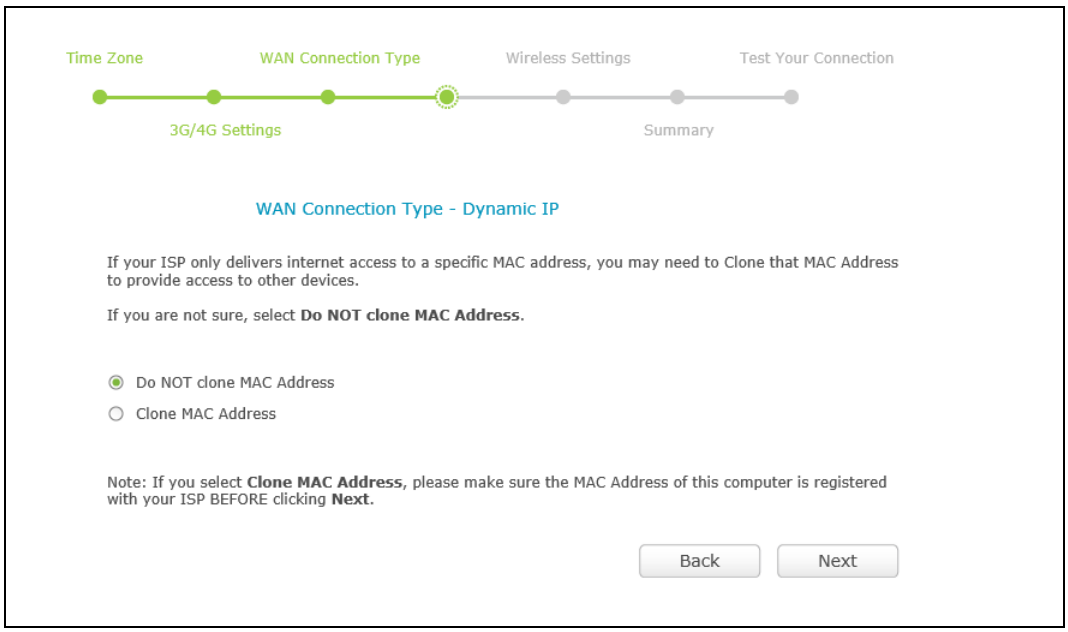
When you have switched the mode of the router on Share ETH, take the following steps:

1. Click **Next** and then **WAN Connection Type** page will appear as shown below.

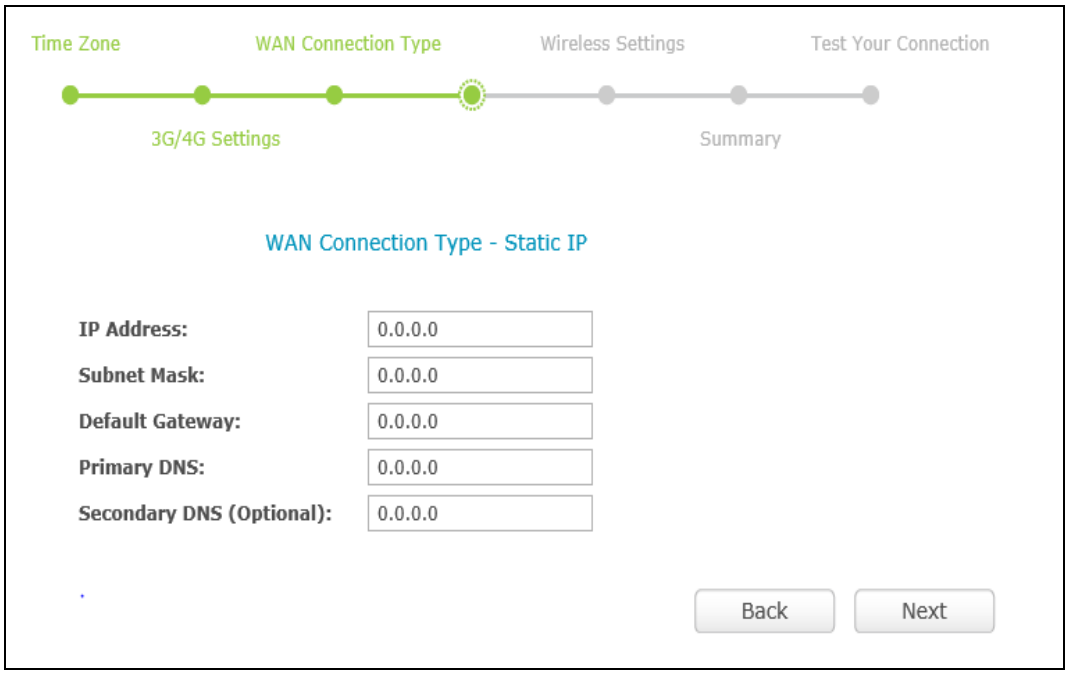


The Router supports five popular ways **Dynamic IP**, **Static IP**, **PPPoE/Russian PPPoE**, **L2TP/Russian L2TP** and **PPTP/Russian PPTP** to connect to the Internet. To make sure the connection type your ISP provides, please refer to the ISP. Make sure the cable is securely plugged into the WAN port before detection.

- **Auto Detect -** If you don't know the connection type your ISP provides, use this option to allow the Quick Setup to search your Internet connection for servers and protocols and determine your ISP configuration.
- **Dynamic IP -** Your ISP uses a DHCP service to assign your Router an IP address for connecting to the Internet. When the Router connects to a DHCP server, or the ISP supplies you with DHCP connection, please choose this type. If you choose this type of connection, you can click **Next** to continue.

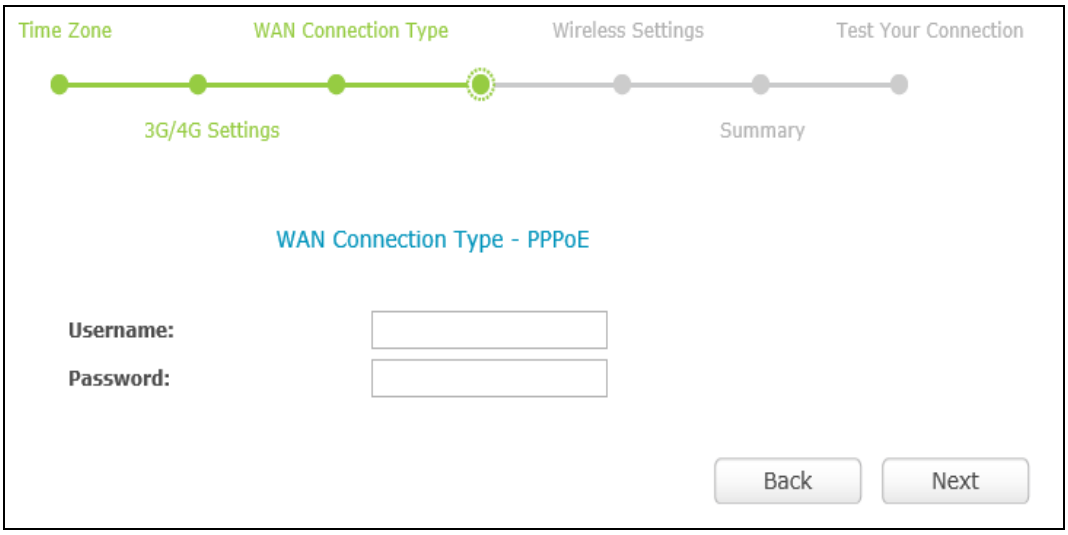


- **Static IP -** This type of connection uses a permanent, fixed (static) IP address that your ISP assigned. In this type, you should fill in the IP address, Subnet Mask, Default Gateway, and DNS IP address manually, which are specified by your ISP. Then click **Next** to continue.



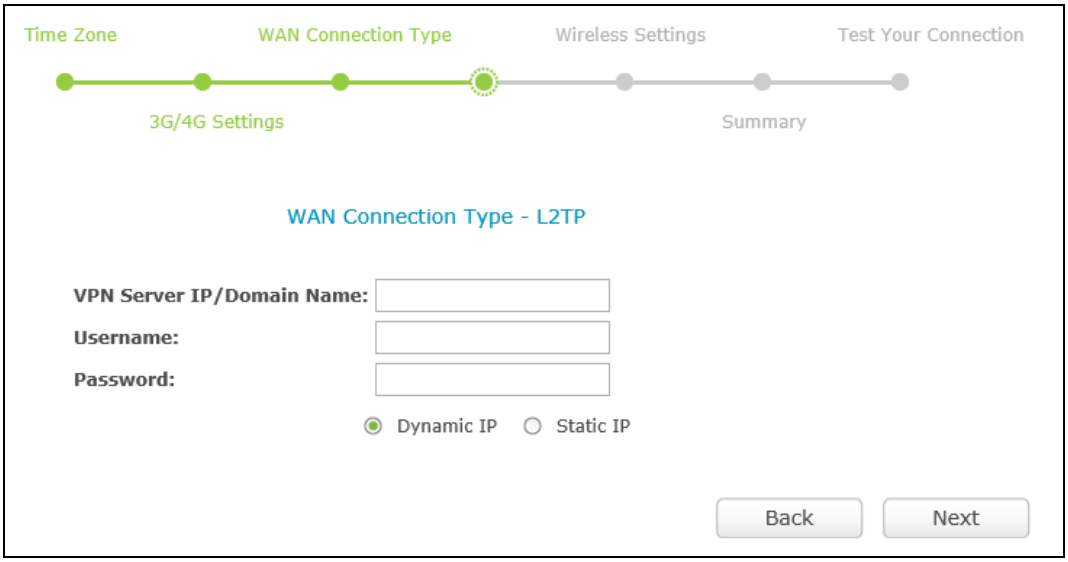
- **PPPoE/Russian PPPoE -** For this connection, you will need your account name and password from your ISP.

  If you have applied ADSL to realize Dial-up service, you should choose this type. Under this condition, you should fill in both the User Name and Password that the ISP supplied. Please note that these fields are case-sensitive.



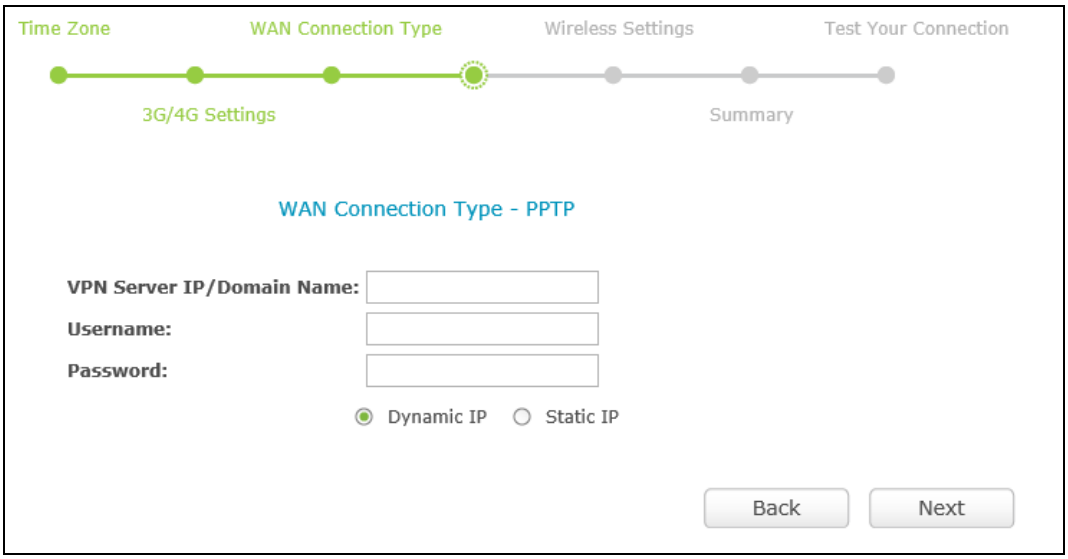
- **L2TP/Russian L2TP -** For this connection, you will need your account name and password from your ISP.

  If you have applied ADSL to realize Dial-up service, you should choose this type. Under this condition, you should fill in both the User Name and Password that the ISP supplied. Please note that these fields are case-sensitive.

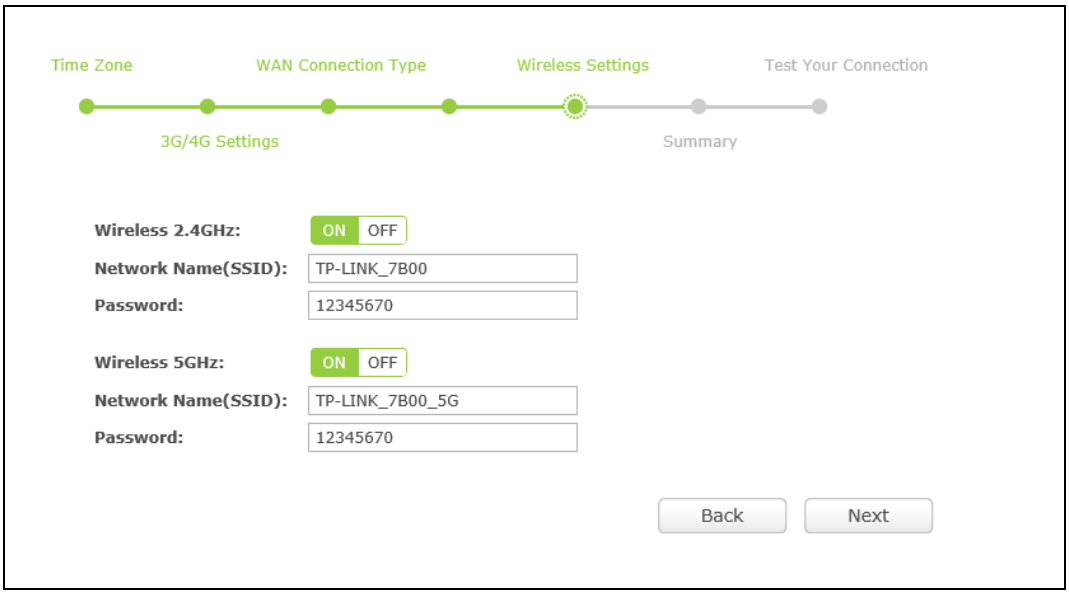


- **PPTP/Russian PPTP -** For this connection, you will need your account name and password from your ISP.

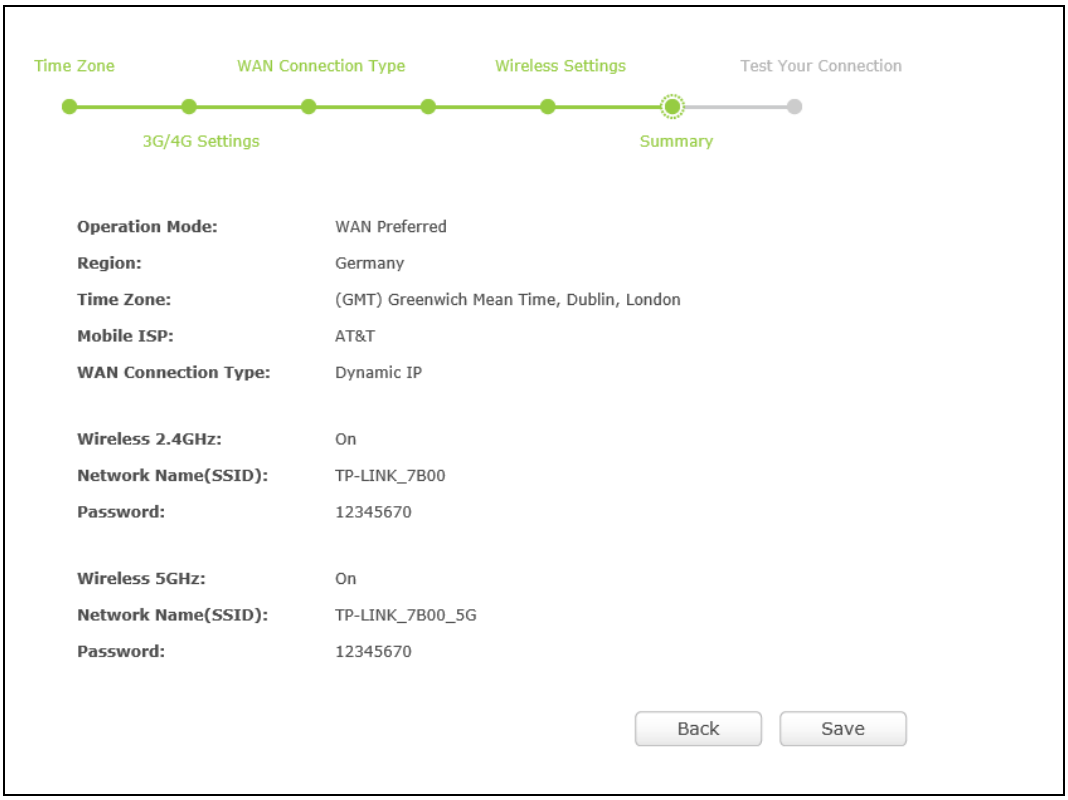
  If you have applied ADSL to realize Dial-up service, you should choose this type. Under this condition, you should fill in both the User Name and Password that the ISP supplied. Please note that these fields are case-sensitive.



2. Then, the **Wireless Settings** page will appear as shown below. You are recommended to change the Network Name (SSID) and Password. Then click **Next**.



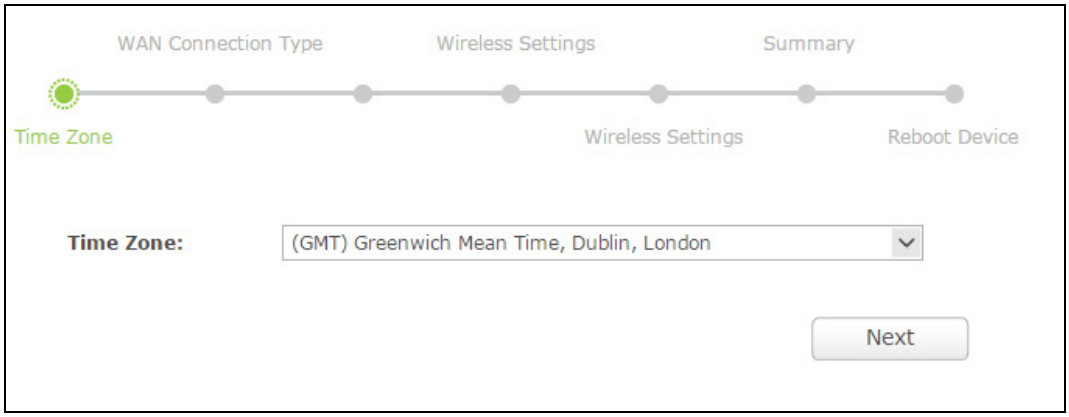
3. The **Summary** page is shown below. Click the **Save** button to make your wireless configuration take effect and finish the **Quick Setup**.



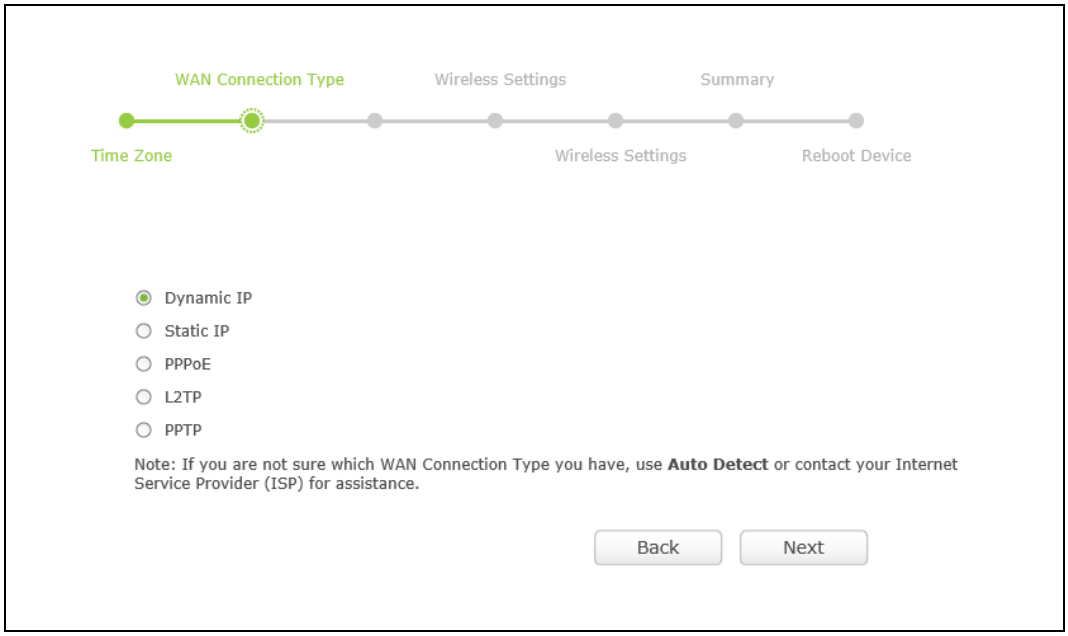
3.2.2 Hotspot Mode

When you have switched the mode of the router on Share Hotspot**,** take the following steps:

1. Select your Time Zone, and click **Next**.



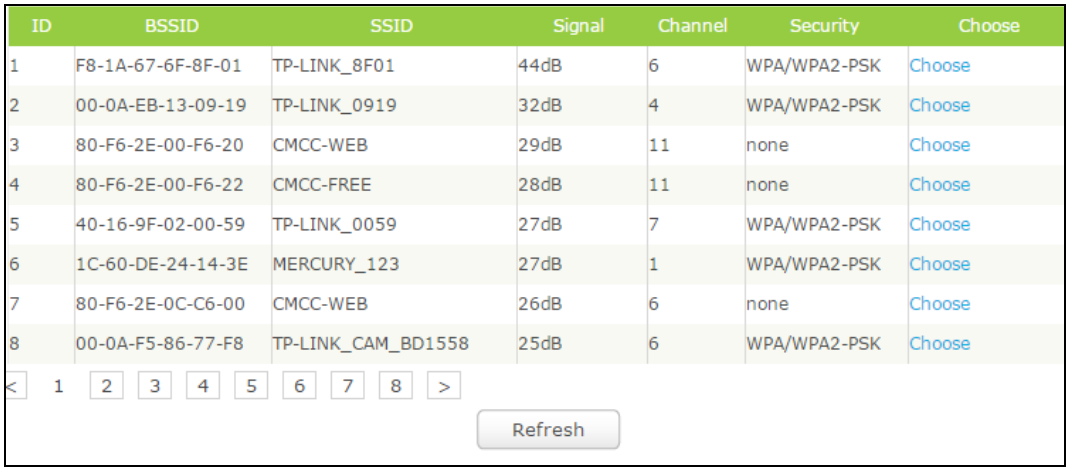
2. Select the **WAN Connection Type** and click **Next**.



In most case, select **Dynamic IP**.

- **Dynamic IP -** Your ISP uses a DHCP service to assign your Router an IP address for connecting to the Internet. When the Router connects to a DHCP server, or the ISP supplies you with DHCP connection, please choose this type.

3. Click Survey to find all available 2.4GHz/5GHz networks, choose the ones you want to access and click **Next**.

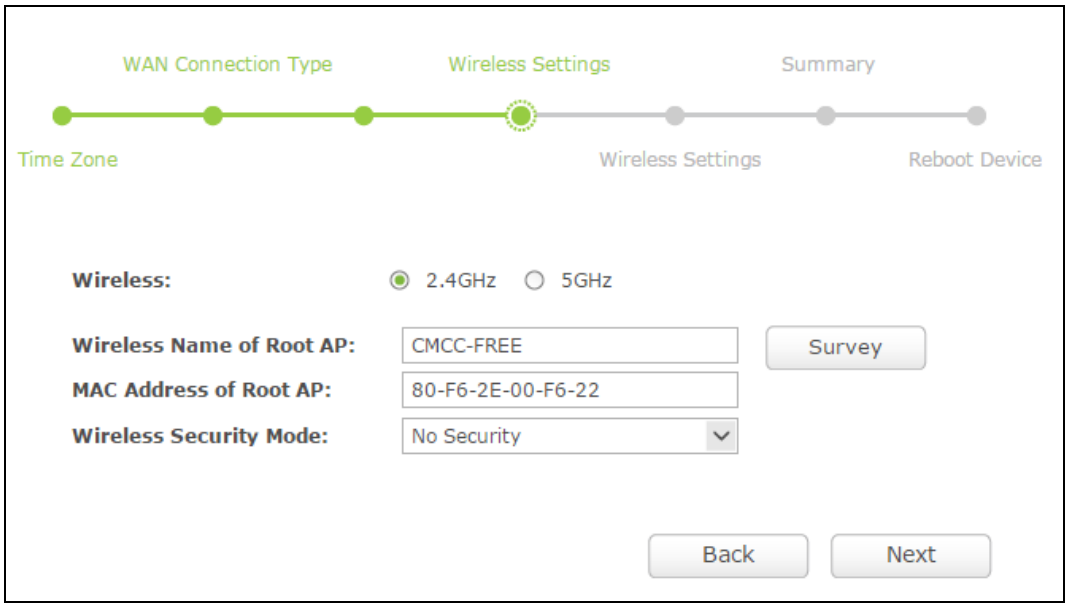


ID	BSSID	SSID	Signal	Channel	Security	Choose
1	F8-1A-67-6F-8F-01	TP-LINK_8F01	44dB	6	WPA/WPA2-PSK	Choose
2	00-0A-EB-13-09-19	TP-LINK_0919	32dB	4	WPA/WPA2-PSK	Choose
3	80-F6-2E-00-F6-20	CMCC-WEB	29dB	11	none	Choose
4	80-F6-2E-00-F6-22	CMCC-FREE	28dB	11	none	Choose
5	40-16-9F-02-00-59	TP-LINK_0059	27dB	7	WPA/WPA2-PSK	Choose
6	1C-60-DE-24-14-3E	MERCURY_123	27dB	1	WPA/WPA2-PSK	Choose
7	80-F6-2E-0C-C6-00	CMCC-WEB	26dB	6	none	Choose
8	00-0A-F5-86-77-F8	TP-LINK_CAM_BD1558	25dB	6	WPA/WPA2-PSK	Choose

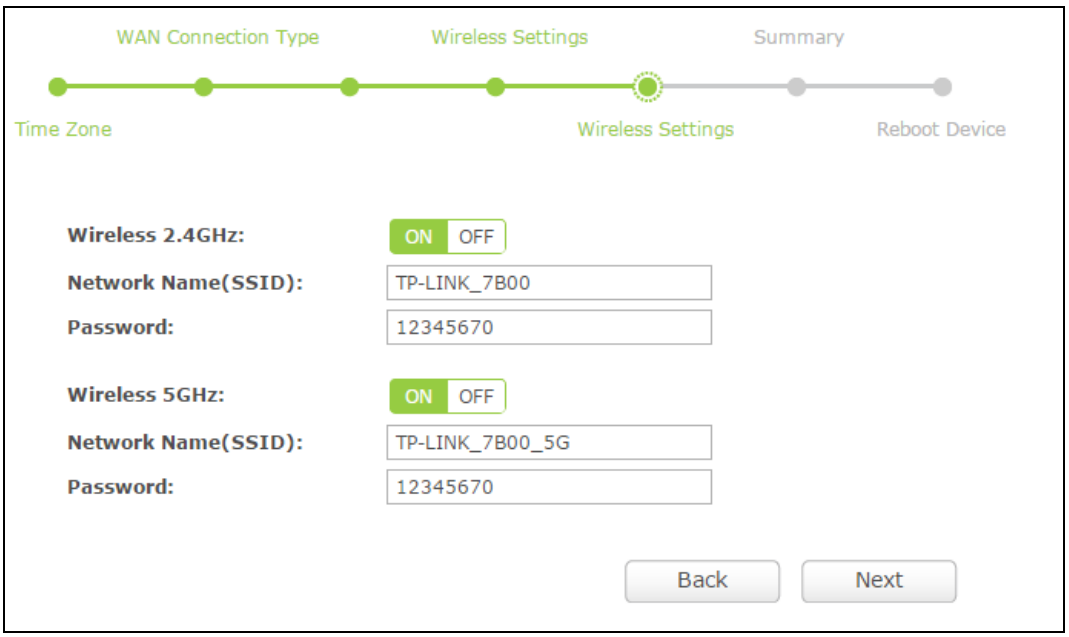
< 1 2 3 4 5 6 7 8 >

Refresh

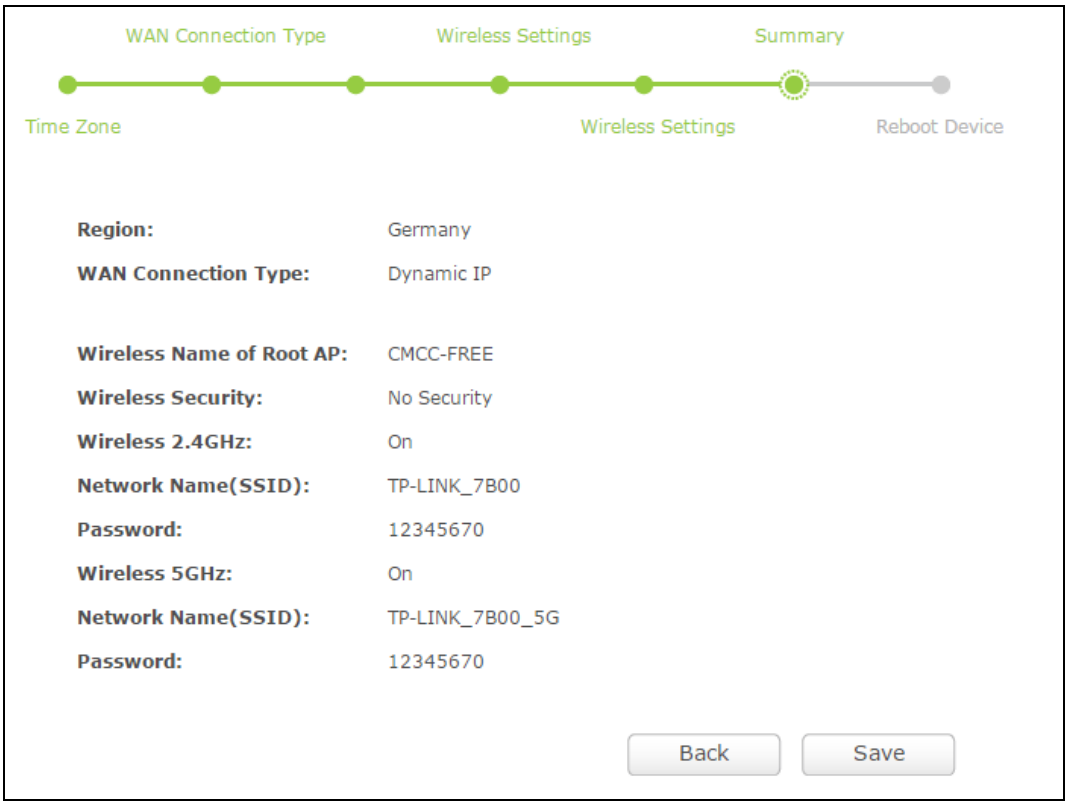
4. **Wireless Settings** page will appear as shown below.



5. You can configure the basic settings for your wireless network on this page.



4. The **Summary** page is shown below. Click **Save** and the router will reboot to apply the settings.



Note:

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.

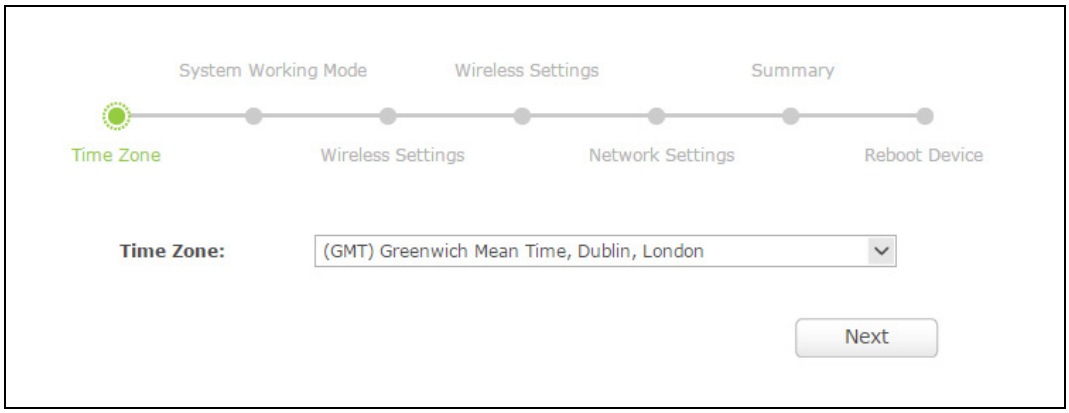
- Near the center of the area in which your wireless stations will operate.
- In an elevated location such as a high shelf.
- Away from the potential sources of interference, such as PCs, microwaves, and cordless phones.
- Away from large metal surfaces.

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

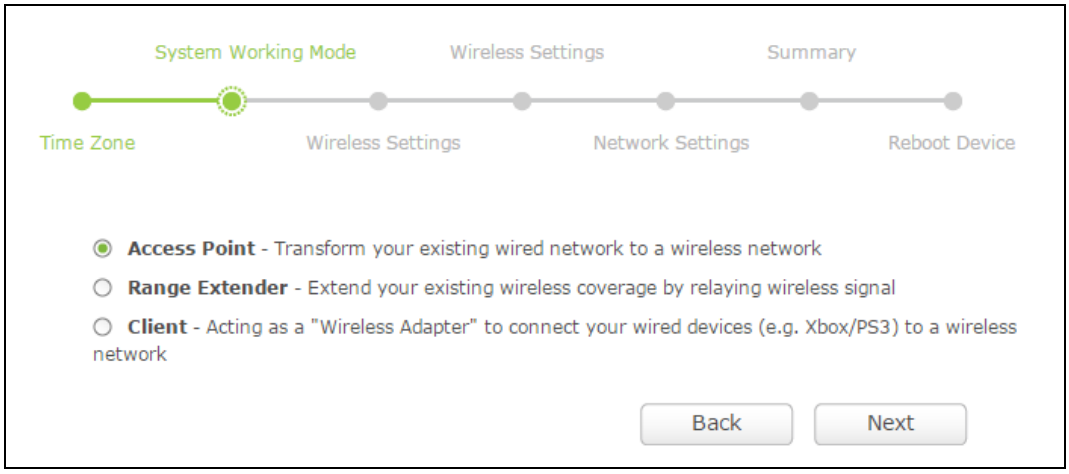
3.2.3 Access Point Mode

When you have switched the mode of the router on AP/Rng Ext/Client, take the following steps:

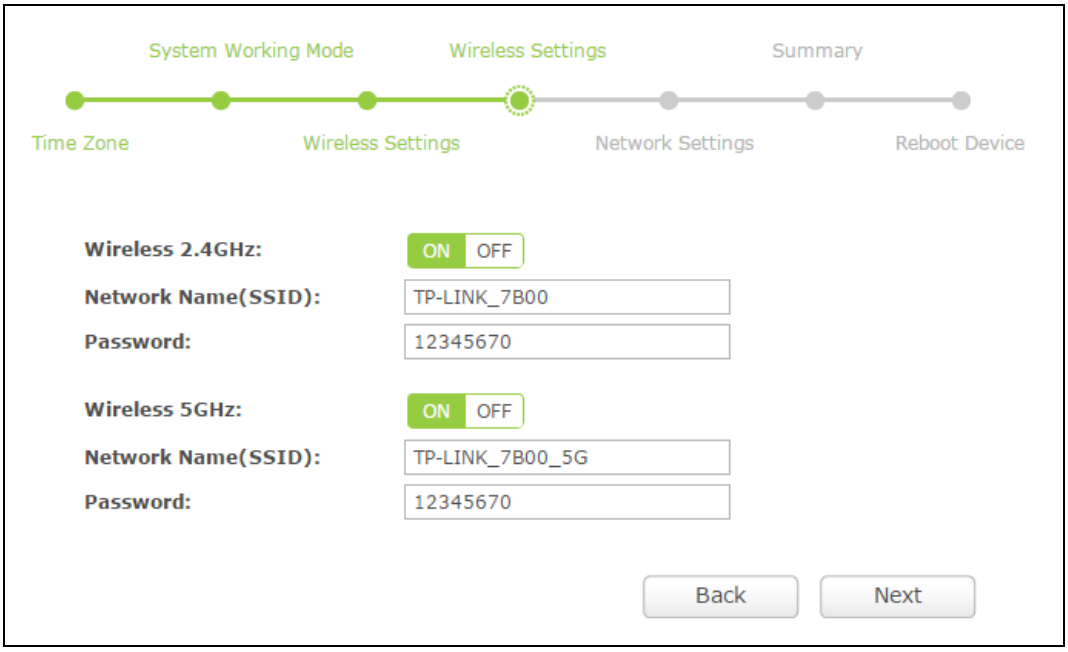
1. Select your Time Zone, and click **Next**.



2. Select **Access Point** for the System Working Mode, and click **Next**.



3. You are recommended to change the default Network Name (SSID) and password for your router. Once done, you have to reconnect to the network with the new SSID and password.

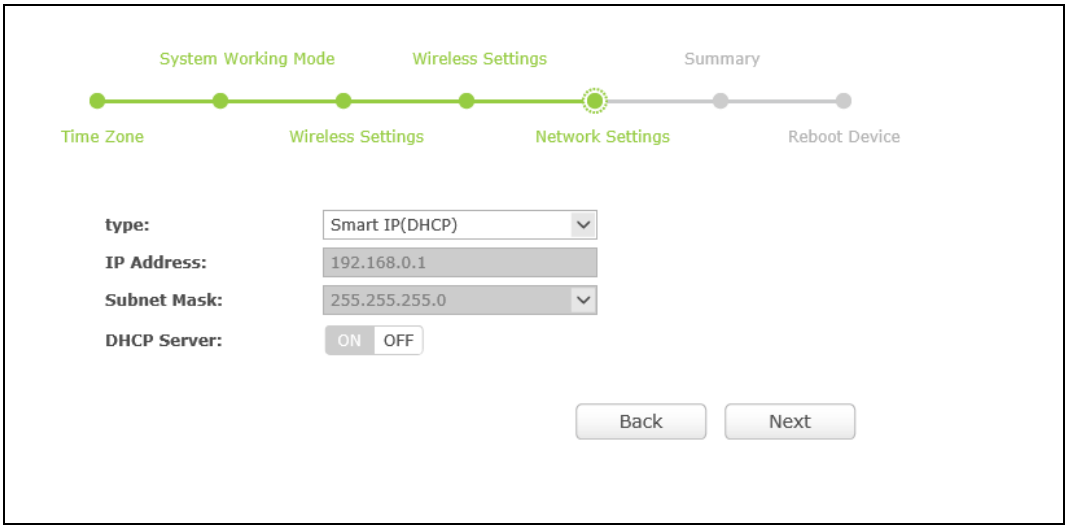


- **Wireless Network Name (SSID) -** Enter a string of up to 32 characters. The same name of SSID (Service Set Identification) must be assigned to all wireless devices in your network. The default SSID is set to be TP-LINK_XXXX (XXXX indicates the last

unique four numbers of each Router's MAC address). But it is recommended strongly that you change your networks name (SSID) to a different value. This value is case-sensitive. For example, *TEST* is NOT the same as *test*.

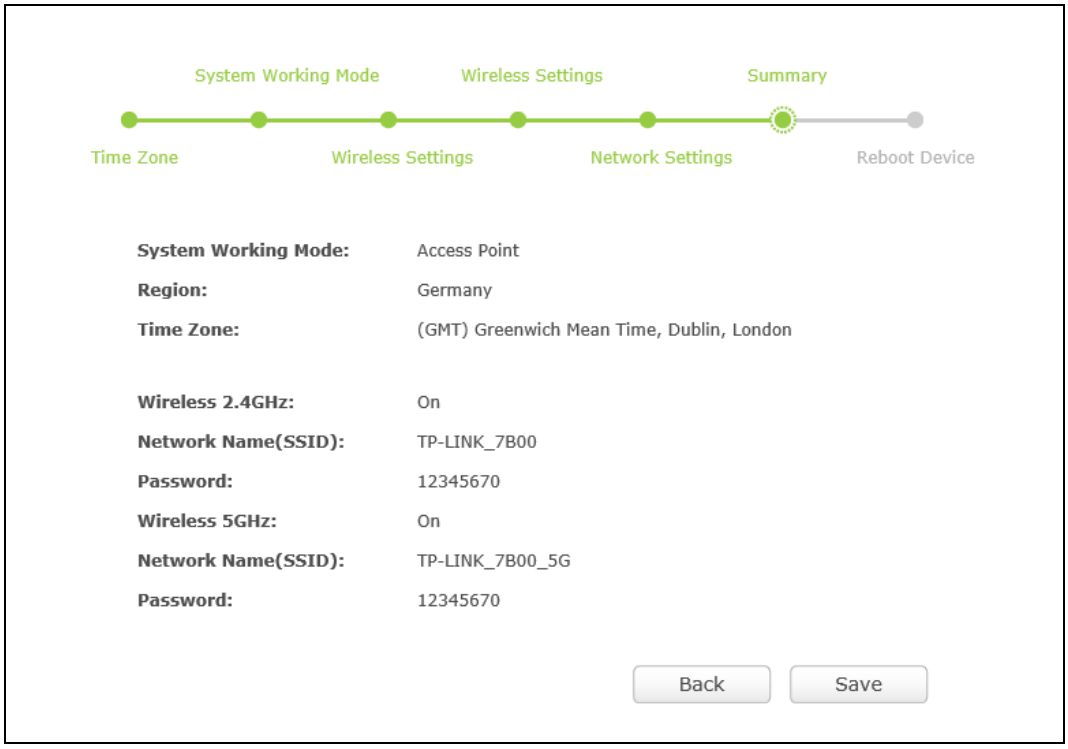
- **Password -** Input the password of your broadcast SSID.

4. You can configure the IP parameters of LAN on this page. But if you are not familiar with the setting items in this page, you're strongly recommended to keep the provided default values.



- **Type -** Choosing SmartDHCP to get IP address from remoter DHCP server, or choosing static IP to config IP address manually.
- **IP Address -** Enter the IP address of your system in dotted-decimal notation (factory default: 192.168.0.1).
- **Subnet Mask -** An address code that determines the size of the network. Normally 255.255.255.0 is used as the subnet mask.

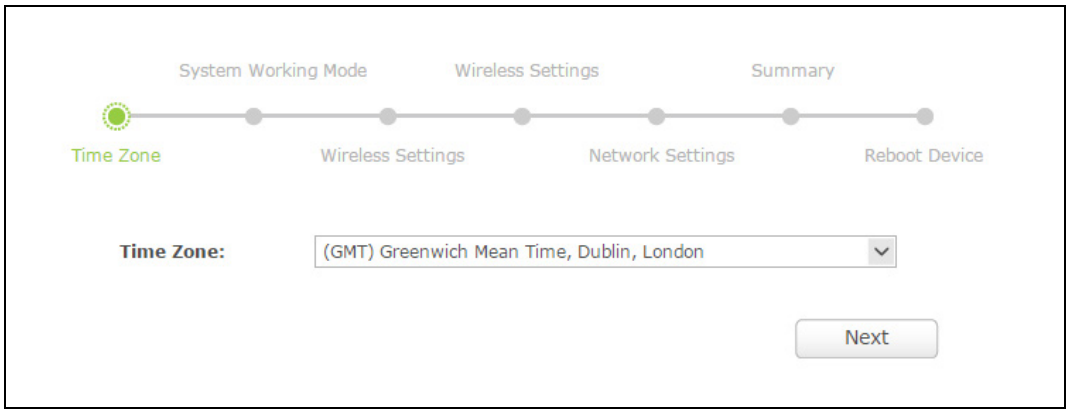
5. You will then see the **Summary** page. Click **Save** and the router will reboot to apply the settings.



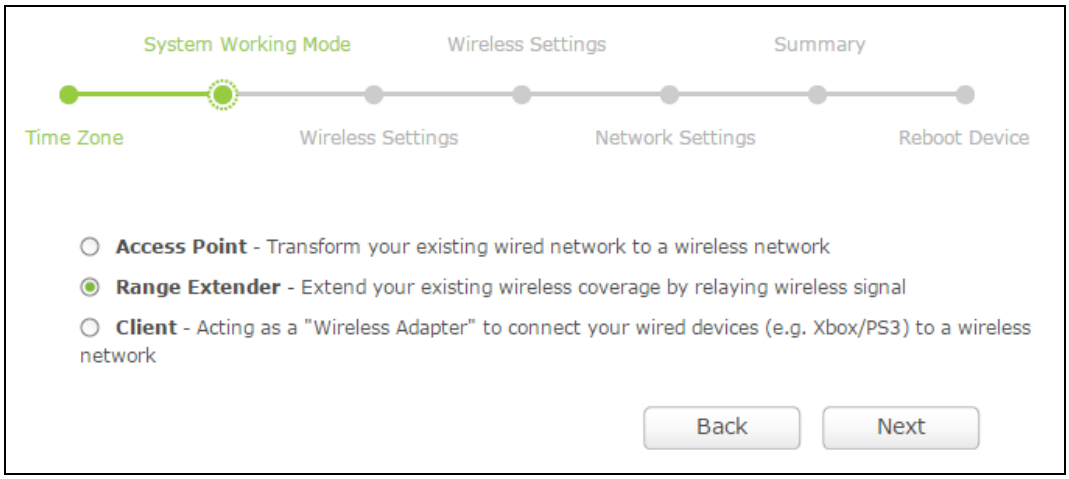
3.2.4 Range Extender Mode

When you have switched the mode of the router on AP/Rng Ext/Client, take the following steps:

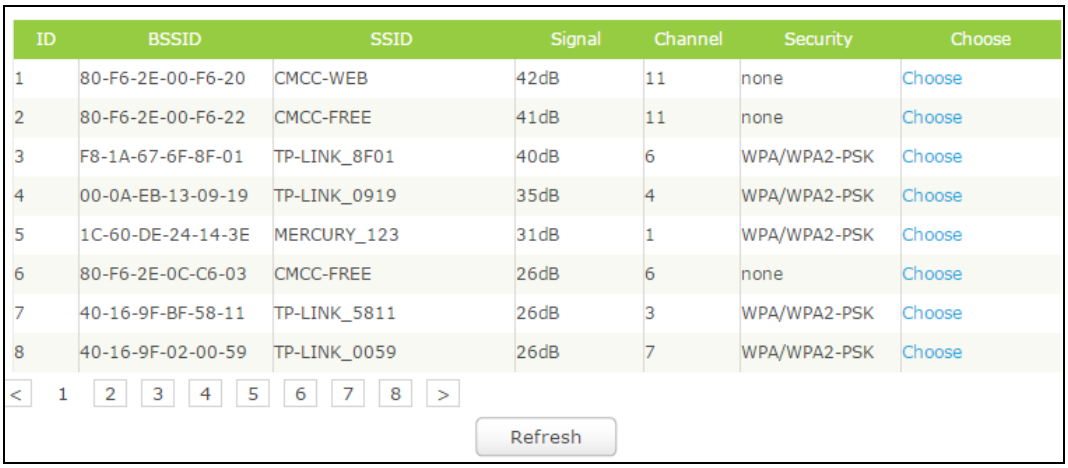
1. Select your Time Zone, and click **Next**.



2. Select **Range Extender** for the System Working Mode, and click **Next**.

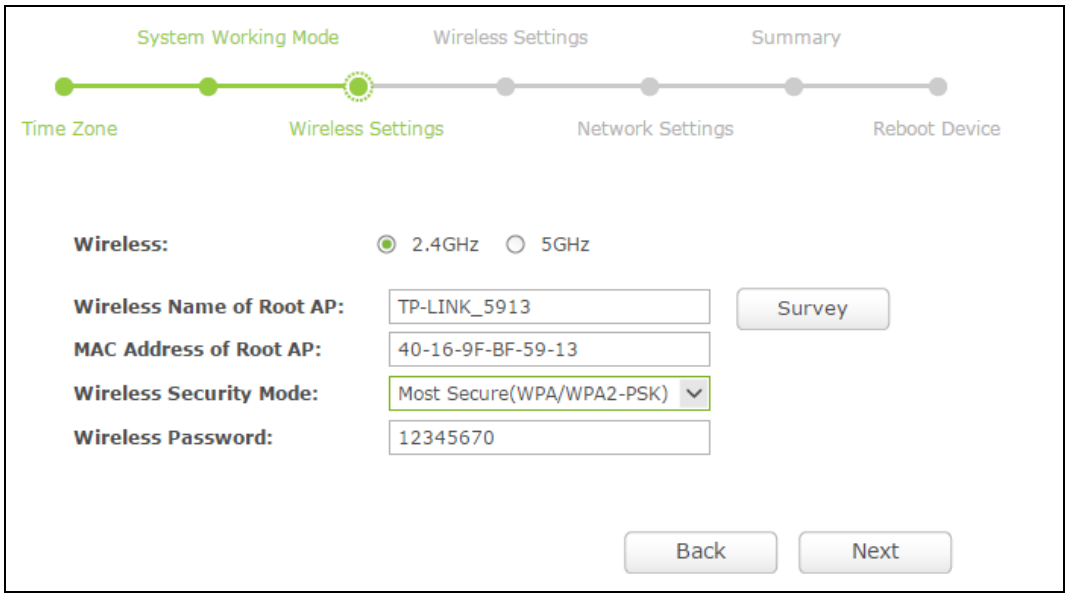


3. Click **Survey** to find all available 2.4GHz/5GHz networks and choose the ones you want to extend.



ID	BSSID	SSID	Signal	Channel	Security	Choose
1	80-F6-2E-00-F6-20	CMCC-WEB	42dB	11	none	Choose
2	80-F6-2E-00-F6-22	CMCC-FREE	41dB	11	none	Choose
3	F8-1A-67-6F-8F-01	TP-LINK_8F01	40dB	6	WPA/WPA2-PSK	Choose
4	00-0A-EB-13-09-19	TP-LINK_0919	35dB	4	WPA/WPA2-PSK	Choose
5	1C-60-DE-24-14-3E	MERCURY_123	31dB	1	WPA/WPA2-PSK	Choose
6	80-F6-2E-0C-C6-03	CMCC-FREE	26dB	6	none	Choose
7	40-16-9F-BF-58-11	TP-LINK_5811	26dB	3	WPA/WPA2-PSK	Choose
8	40-16-9F-02-00-59	TP-LINK_0059	26dB	7	WPA/WPA2-PSK	Choose

4. **Wireless Setting** page will appear as shown below.



- **Wireless Name of Root AP -** The SSID of AP that you want to access.
- **MAC Address of Root AP -** The MAC address of AP that you want to access.

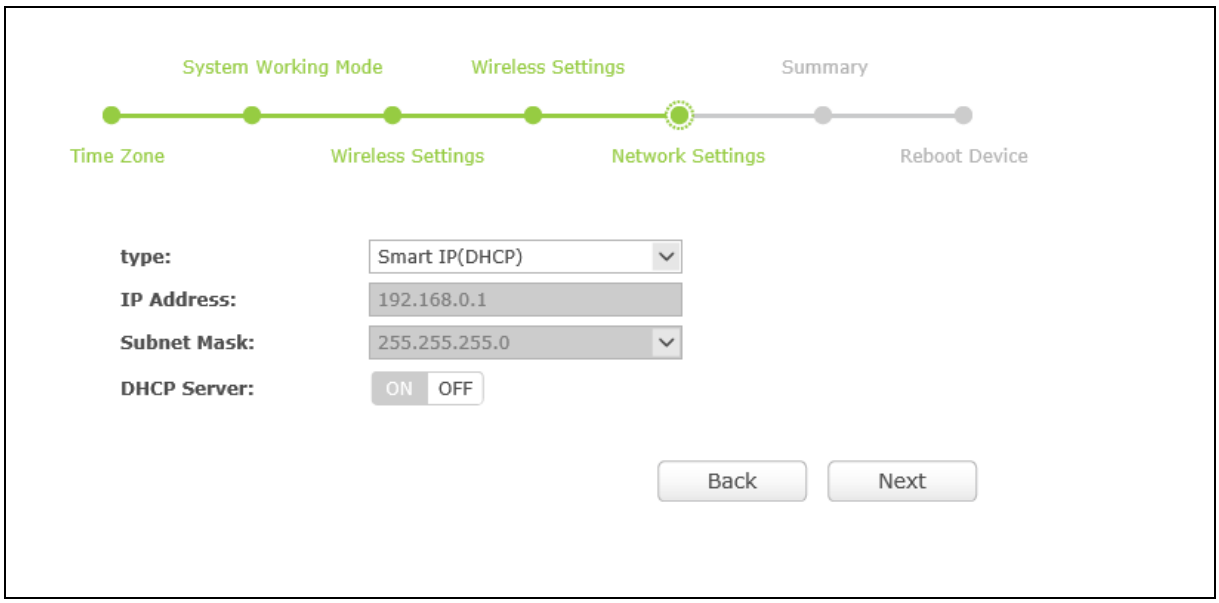
- **Wireless Security Mode -** This option should be chosen according to the security configuration of the AP you want to access. It is recommended that the security type is the same as your AP's security type.
- **Wireless Password -** If the AP your router is going to connect needs password, you need to fill the password in this blank.

Note:

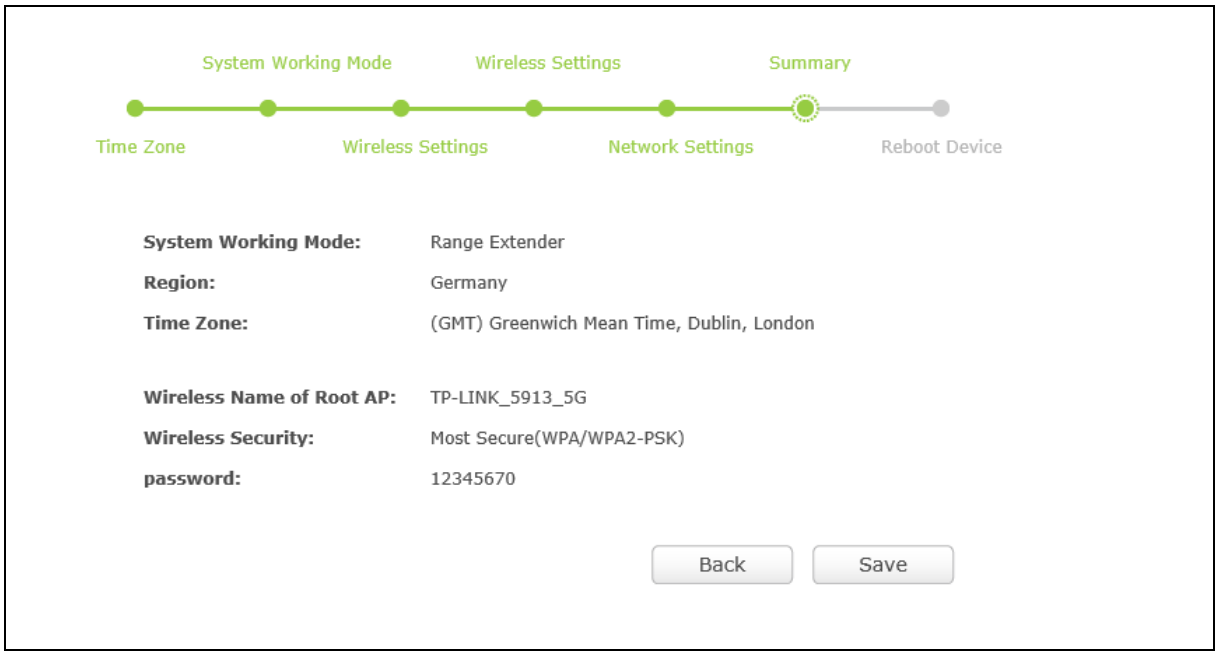
If you know the SSID of the desired AP, you can also input it into the field "SSID" manually.

5. Click the **Next** button. You can configure the IP parameters of LAN on this page.

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



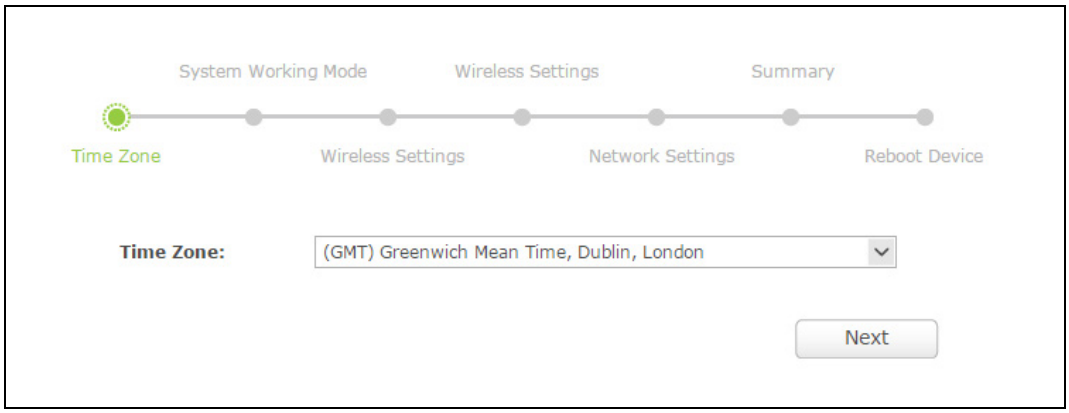
6. Click the **Next** button. You will then see the **Summary** page and click **Save** to apply your settings.



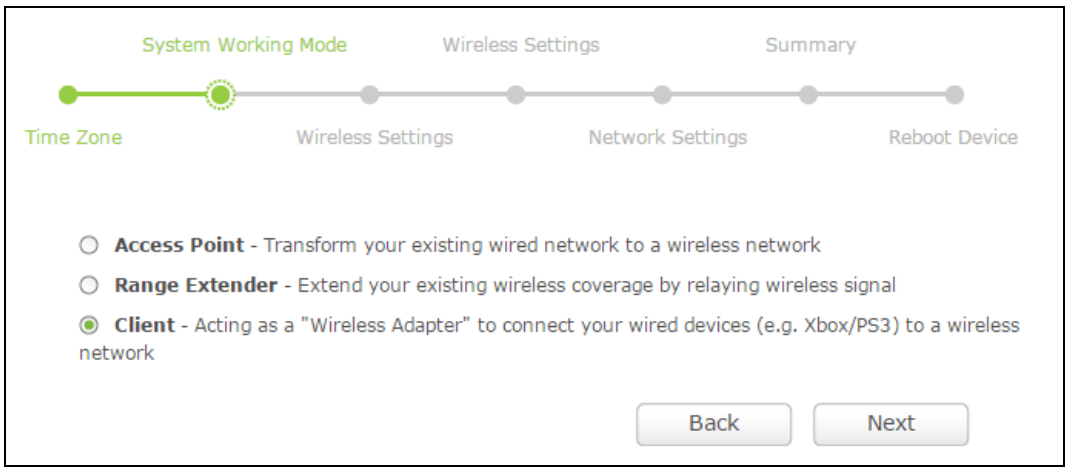
3.2.5 Client Mode

When you have switched the mode of the router on AP/Rng Ext/Client , take the following steps:

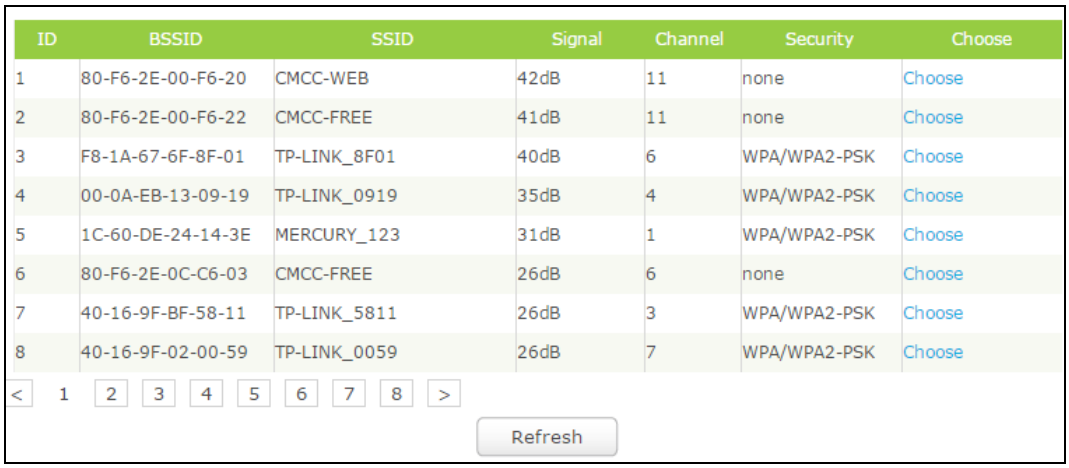
1. Select your Time Zone, and click **Next**.



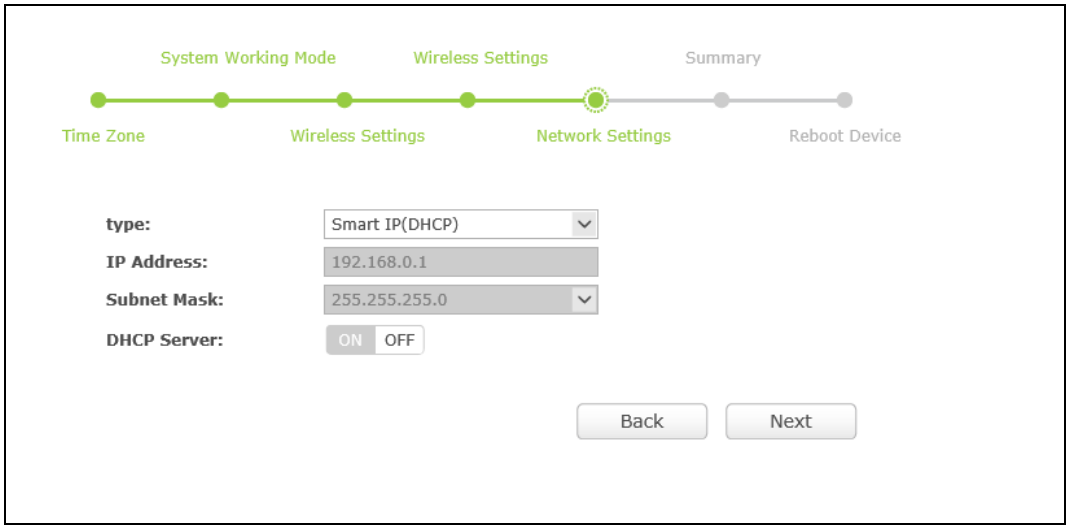
2. Select **Client** for the System Working Mode, and click **Next**.



3. Click **Survey** to find all available 2.4GHz/5GHz networks and choose the ones you want to access.

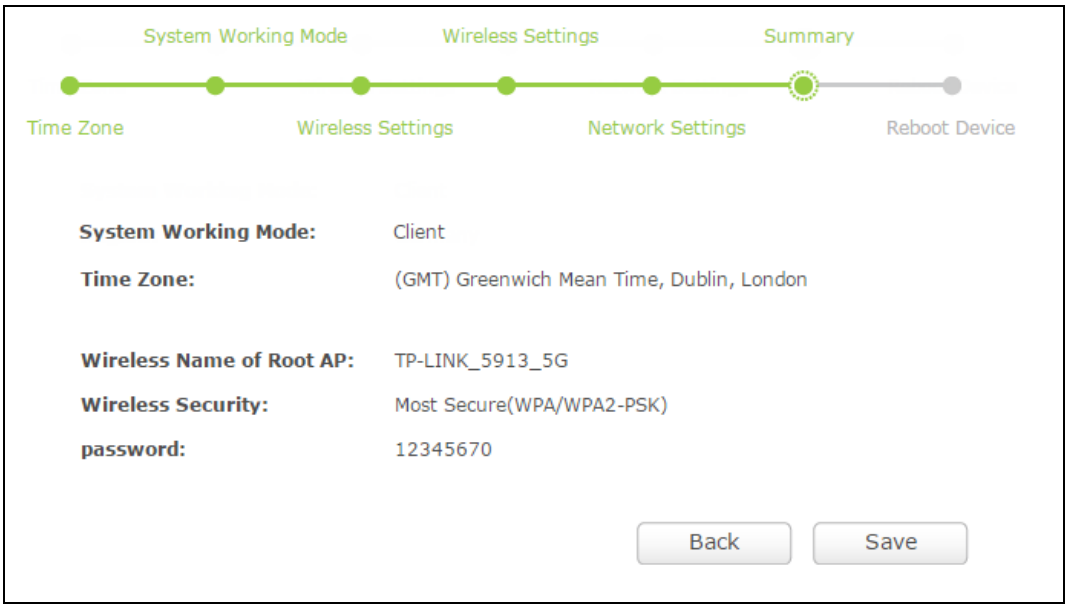


4. You can configure the IP parameters of LAN on this page. But if you are not familiar with the setting items in this page, you're strongly recommended to keep the provided default values.



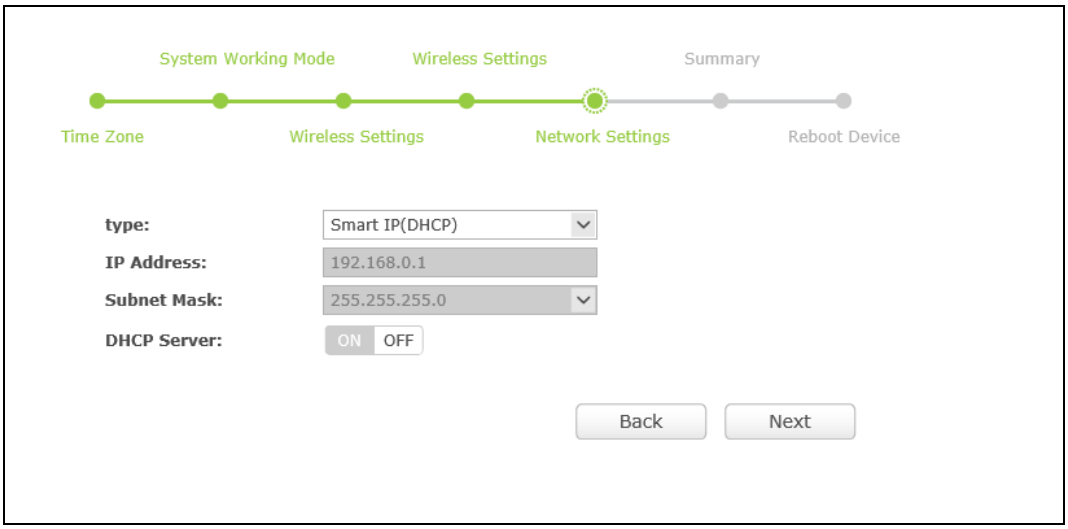
- **Type -** Choosing SmartDHCP to get IP address from remoter DHCP server, or choosing static IP to config IP address manually.
- **IP Address -** Enter the IP address of your system in dotted-decimal notation (factory default: 192.168.0.1).
- **Subnet Mask -** An address code that determines the size of the network. Normally 255.255.255.0 is used as the subnet mask.

5. Click **Next**, and then **Wireless Setting** page will appear as shown below.

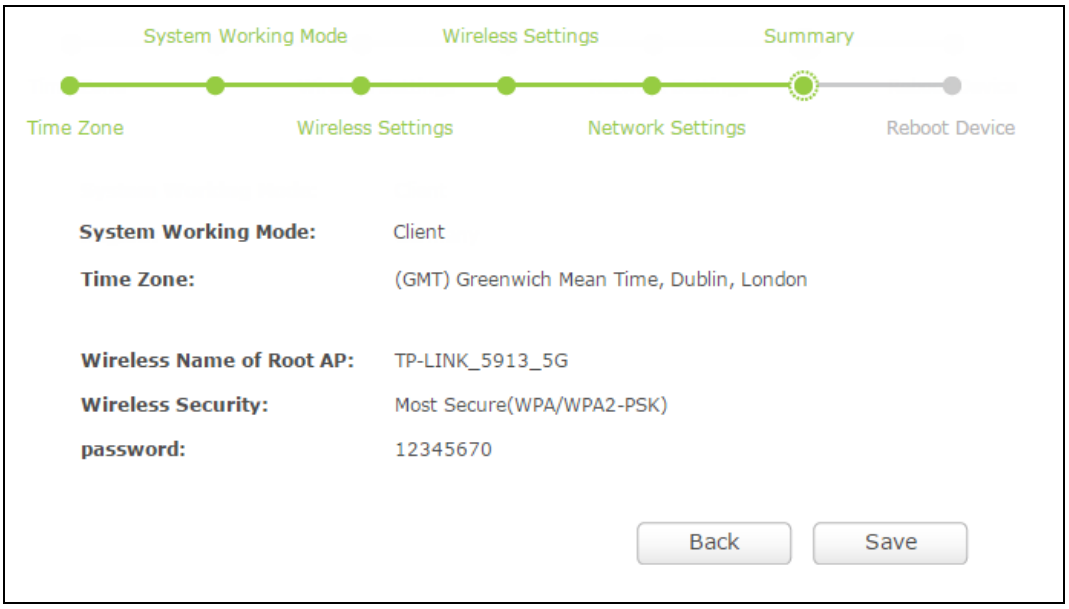


- **Wireless Name of Root AP -** Enter the SSID that you want to access.
- **MAC Address of Root AP -** Enter the MAC address of AP that you want to access.
- **Wireless Security Mode -** This option should be chosen according to the security configuration of the AP you want to access. It is recommended that the security type is the same as your AP's security type.
- **Root AP Wireless Password -** If the AP your router is going to connect need password, you need to fill the password in this blank.

6. Click the **Next** button. You can configure the IP parameters of LAN on this page. 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 low wireless network performance.



3. You will then see the **Summary** page. Click the **Save** and the router will reboot to apply the settings.

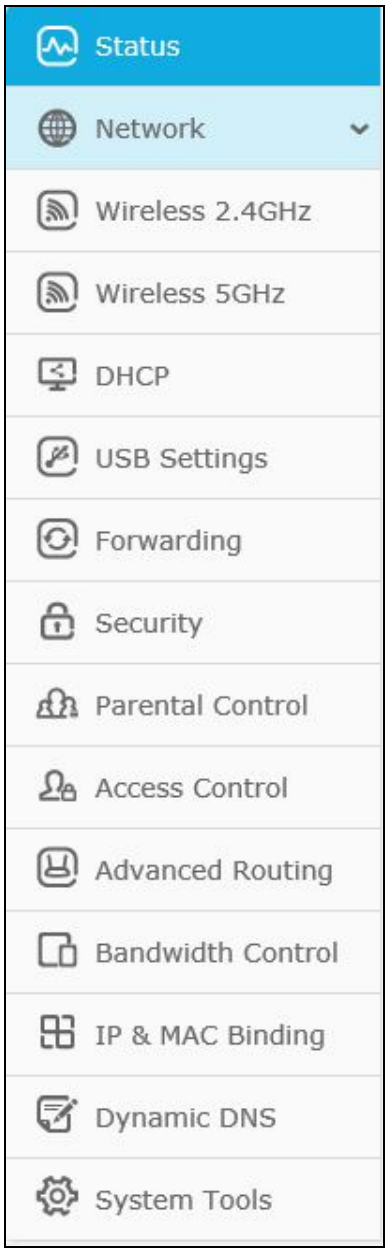

System Working Mode
Wireless Settings
Summary
Time Zone
Wireless Settings
Network Settings
Reboot Device
System Working Mode: Client
Time Zone: (GMT) Greenwich Mean Time, Dublin, London
Wireless Name of Root AP: TP-LINK_5913_5G
Wireless Security: Most Secure(WPA/WPA2-PSK)
password: 12345670
Back
Save

Chapter 4. Configuration for Wireless Router Mode

This chapter will show each Web page's key functions and the configuration way for Wireless Router Mode of TL-WR902AC.

4.1 Login

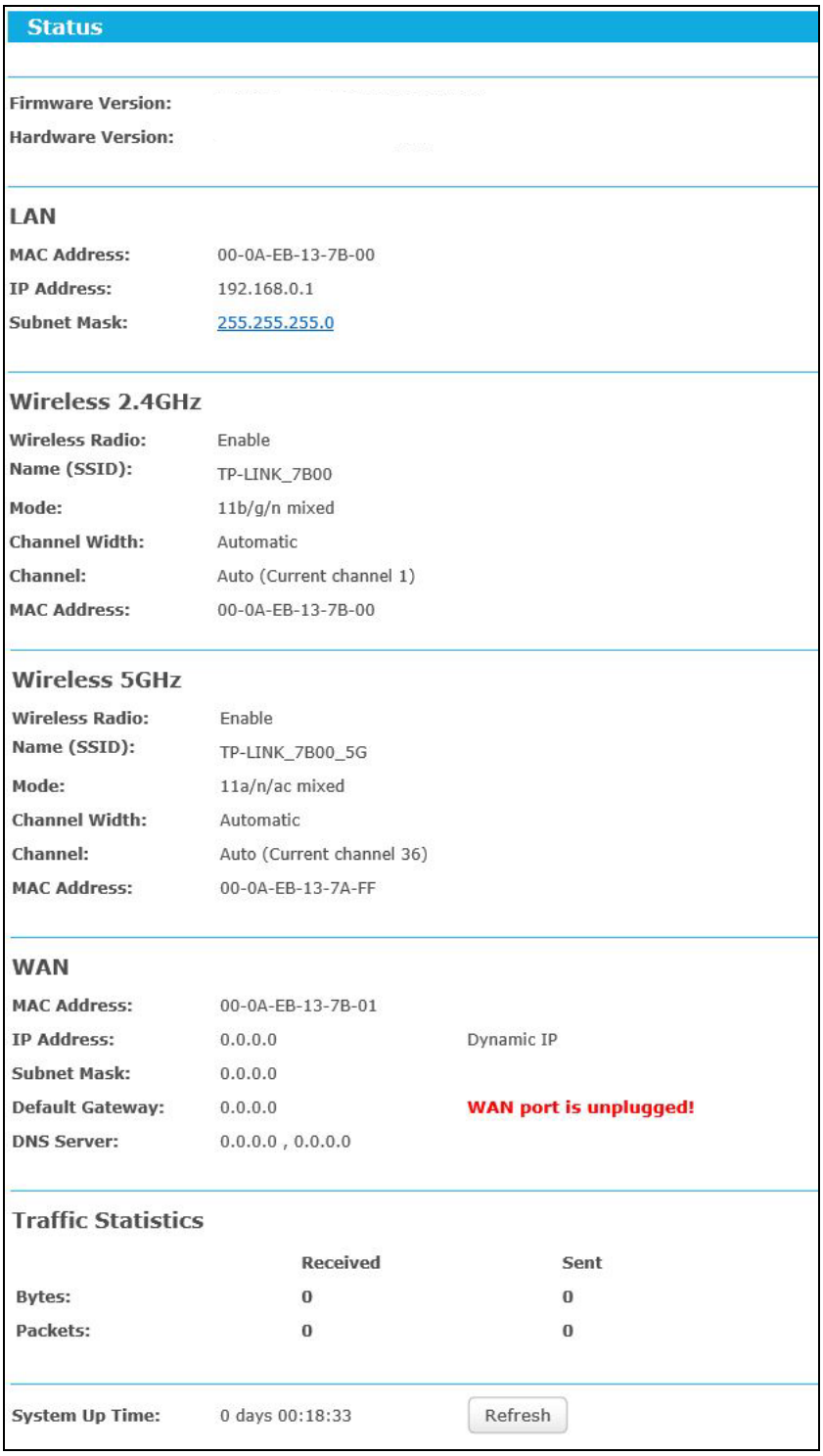
After your successful login, you can configure and manage the device. There are main menus on the left of the web-based utility. Submenus will be available after you click one of the main menus. On the right, there are the corresponding explanations and instructions.



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 on Wireless Router Mode. All information is read-only.



- **Firmware Version -** The version information of the Router's firmware.
- **Hardware Version -** The version information of the Router's hardware.

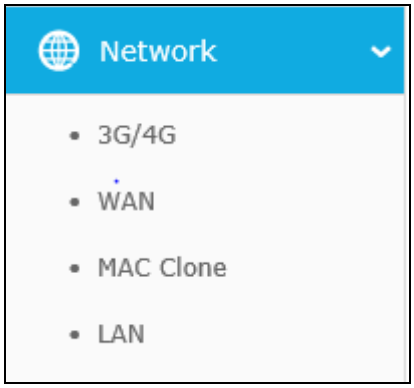
- **LAN -** This field displays the current settings or information for the LAN, you can configure them in the **Network > LAN** page.
  - **MAC Address -** The physical address of the Router, as seen from the LAN.
  - **IP Address -** The LAN IP address of the Router.
  - **Subnet Mask -** The subnet mask associated with LAN IP address.
- **Wireless -** This field displays basic information or status for wireless function, you can configure them in the **Wireless > Wireless Settings** page.
  - **Operation Mode -** The current wireless working mode in use.
  - **Wireless Radio -** Indicates whether the wireless radio feature of the AP is enabled or disabled.
  - **Name (SSID) -** The SSID of the Router.
  - **Mode -** The current wireless mode which the Router works on.
  - **Channel Width -** The current wireless channel width in use.
  - **Channel -** The current wireless channel in use.
  - **MAC Address -** The physical address of the Router, as seen from the WLAN.
  - **WDS Status -** The status of WDS connection.
- **WAN -** This field displays the current settings or information for the WAN, you can configure them in the **Network > WAN** page.
  - **MAC Address -** The physical address of the WAN port, as seen from the Internet.
  - **IP Address -** The current WAN (Internet) IP Address. This field will be blank or 0.0.0.0 if the IP Address is assigned dynamically and there is no connection to the Internet.
  - **Subnet Mask -** The subnet mask associated with the WAN IP Address.
  - **Default Gateway -** The Gateway currently used by the Router is shown here. When you use **Dynamic IP** as the connection Internet type, the **Renew** button will be displayed here. Click the **Renew** Button to obtain new IP parameters dynamically from the ISP. And if you have got an IP address, **Release** button will be displayed here. Click the **Release** button to release the IP address the Router has obtained from the ISP.
- **DNS Server -** The DNS (Domain Name System) server IP addresses currently used by the Router.
- **Traffic Statistics -** The Router's traffic statistics.
  - **Received (Bytes) -** Traffic that counted in bytes has been received out from the WAN port.
  - **Received (Packets) -** Traffic that counted in packets has been received out from the WAN port.
  - **Sent (Bytes) -** Traffic that counted in bytes has been sent out from the WAN port.

- **Sent (Packets) -** Traffic that counted in packets has been sent out from the WAN port.

➢ **System Up Time -** The length of the time since the Router was last powered on or reset.

Click the **Refresh** button to get the latest status and settings of the Router.

4.3 Network

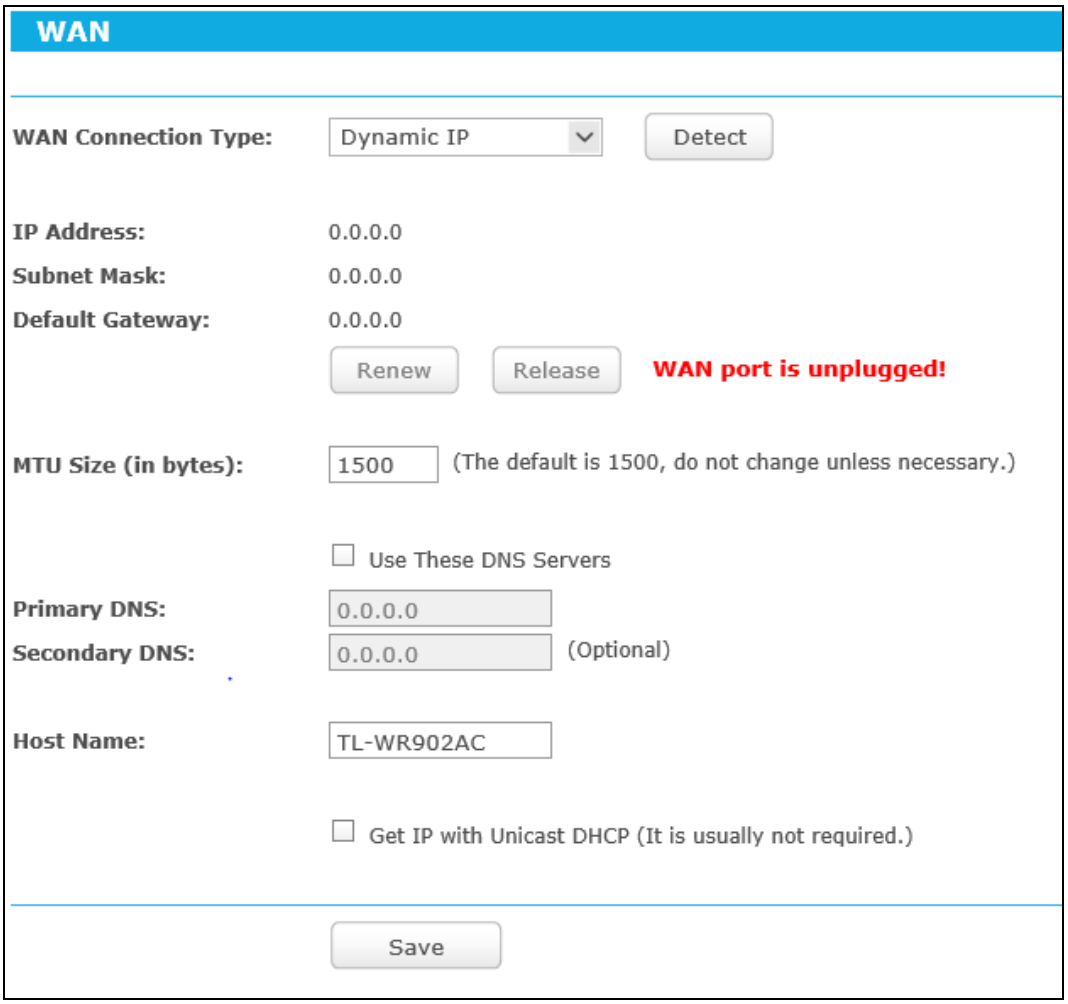


There are three submenus under the Network menu: **3G/4G**, **WAN**, **MAC Clone** and **LAN.** Click any of them, and you will be able to configure the corresponding function.

4.3.1 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 follow:



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.

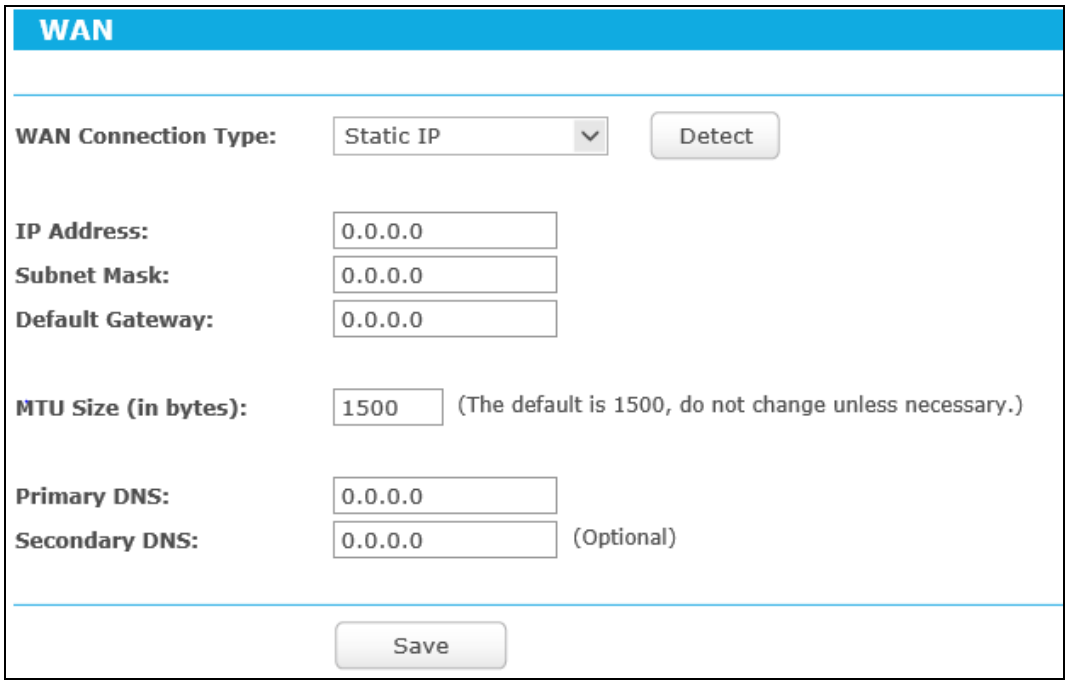
Note:

If you find error when you go to a website 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.

- **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.)

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

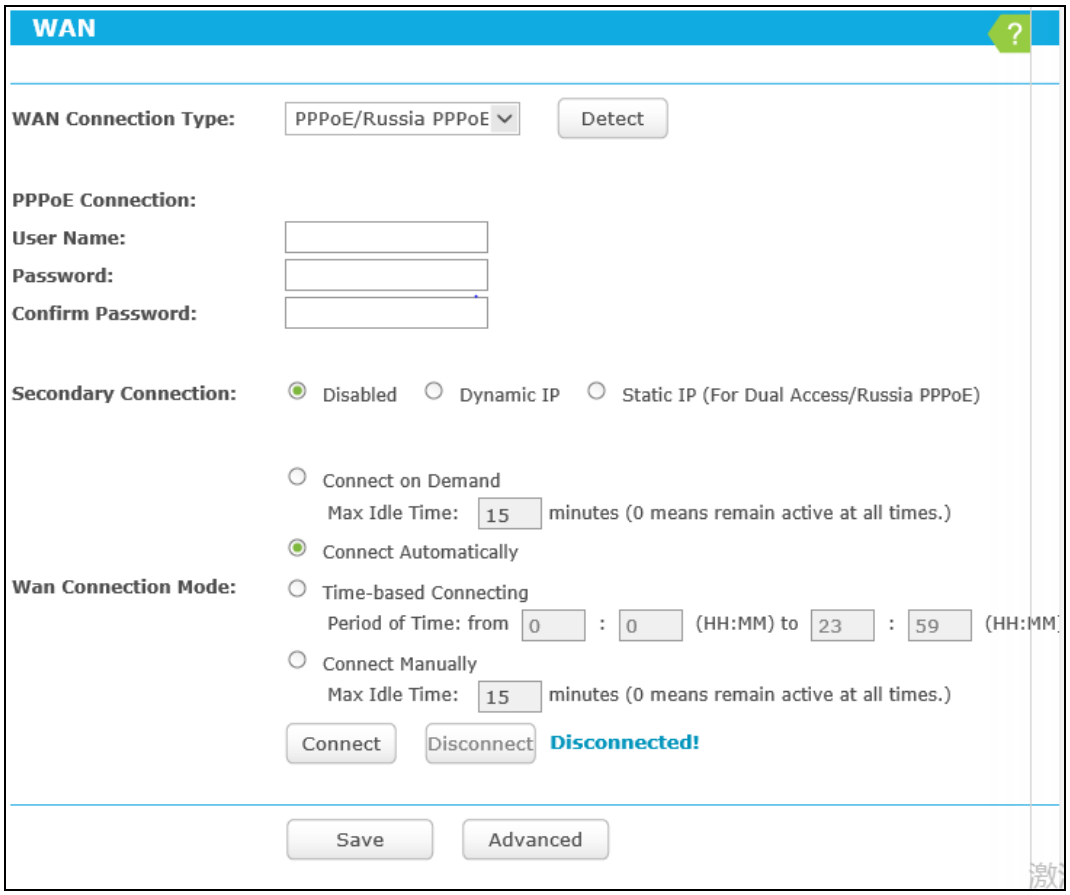
2. If your ISP provides a static or fixed **IP Address**, **Subnet Mask**, **Default Gateway** and **DNS** setting, select **Static IP**. The Static IP settings page will appear as shown below.



- **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 -** 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.

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

3. If your ISP provides a PPPoE connection, select **PPPoE/Russia PPPoE** option. Then you should enter the following parameters:



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

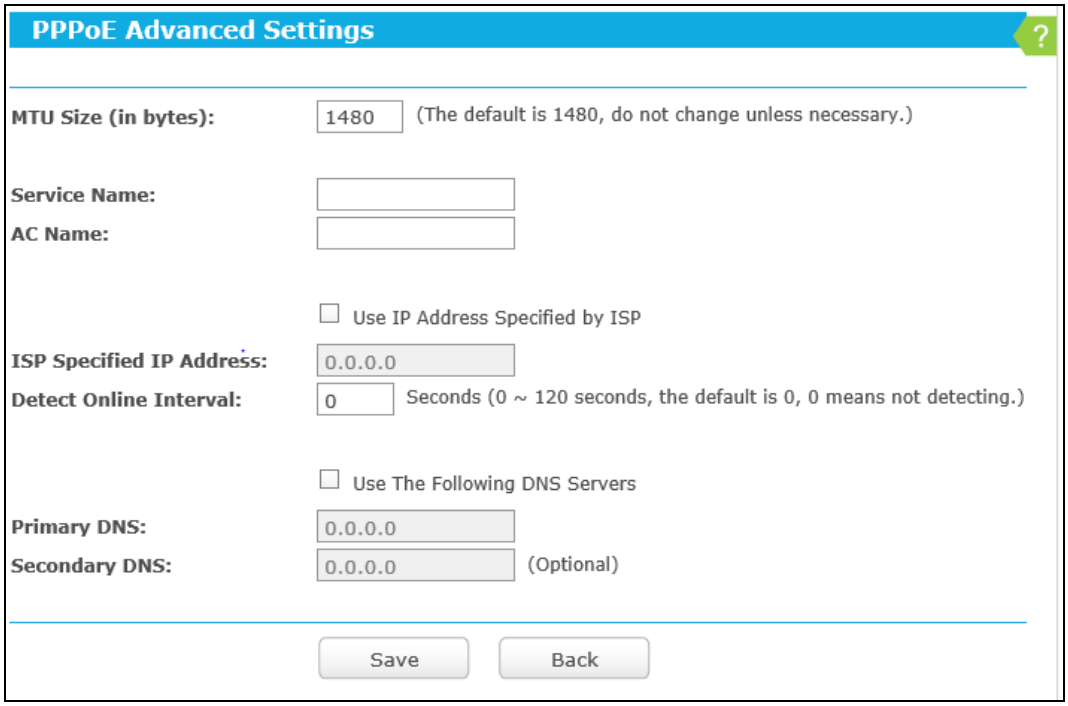
Only when you have configured the system time on "**System Tools** → **Time**" page, will the **Time-based Connecting** function can take effect.

- **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.

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.

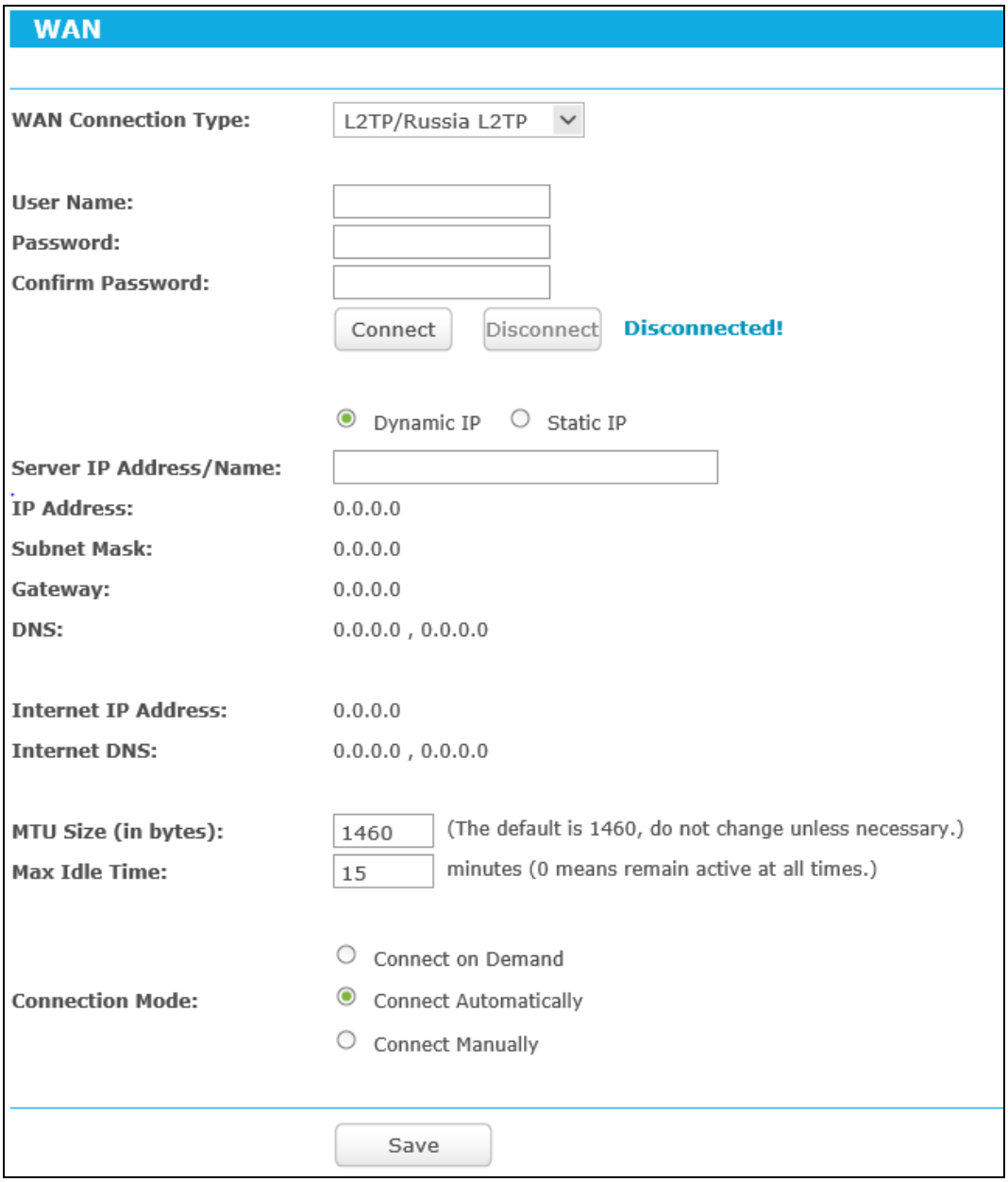
If you want to do some advanced configurations, please click the **Advanced** button, and the page shown will then appear:



- **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 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.
- **Primary DNS/Secondary DNS -** 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 L2TP connection, please select **L2TP/Russia L2TP** option. Then you should enter the following parameters:



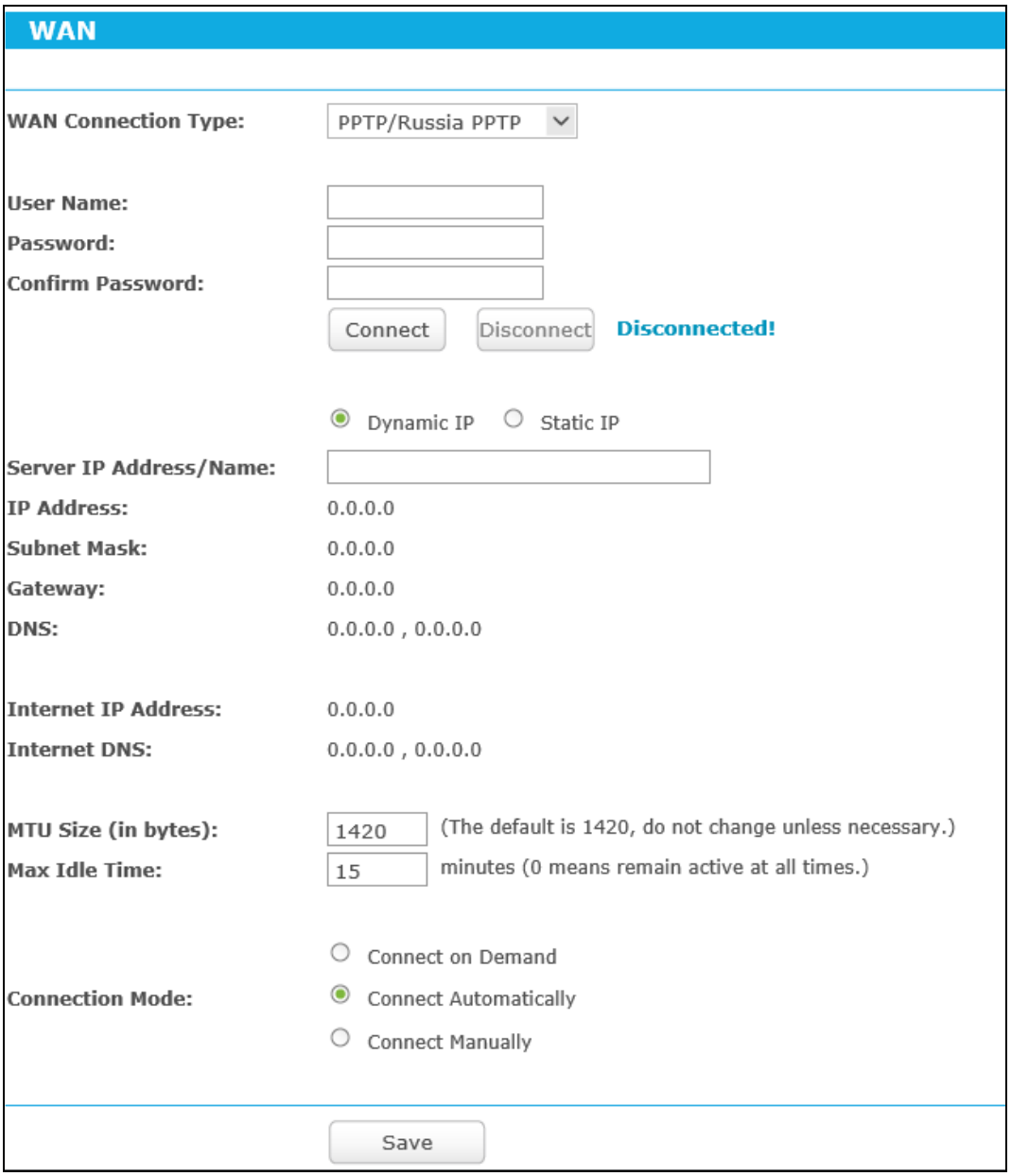
- **User Name/Password -** Enter the User Name and Password provided by your ISP. These fields are case-sensitive.
- **Dynamic IP/ Static IP -** Choose either as you are given by your ISP. Click the **Connect** button to connect immediately. Click the **Disconnect** button to disconnect immediately.
- **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**, check the radio button. If you want your Internet connection to remain active at all times, enter 0 in the **Max Idle Time** field. Otherwise, enter the number of minutes you want to have elapsed before your Internet connection terminates.

- **Connect Automatically -** Connect automatically after the Router is disconnected. To use this option, check 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, check the radio button. If you want your Internet connection to remain active at all times, enter "0" in the **Max Idle Time** field. Otherwise, enter the number of minutes 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**, because some applications are visiting the Internet continually in the background.

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

5. If your ISP provides PPTP connection, please select **PPTP/Russia PPTP** option. And you should enter the following parameters:



- **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**, check the radio button. If you want your Internet connection to remain active at all times, enter “0” in the **Max Idle Time** field. Otherwise, enter the number of minutes you want to have elapsed before your Internet connection terminates.

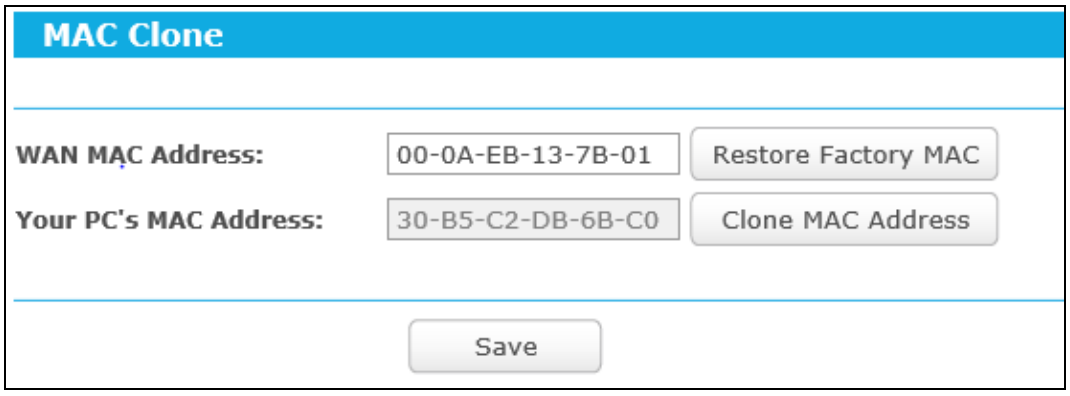
- **Connect Automatically -** Connect automatically after the Router is disconnected. To use this option, check the radio button.
- **Connect Manually -** You can configure the Router to make it connect or disconnect manually. After a specified period of inactivity (**Max Idle Time**), the Router will 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** because some applications are visiting the Internet continually in the background.

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

4.3.2 MAC Clone

Choose menu “**Network → MAC Clone**”, and then you can configure the WAN MAC address on the screen below, as shown below:



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.

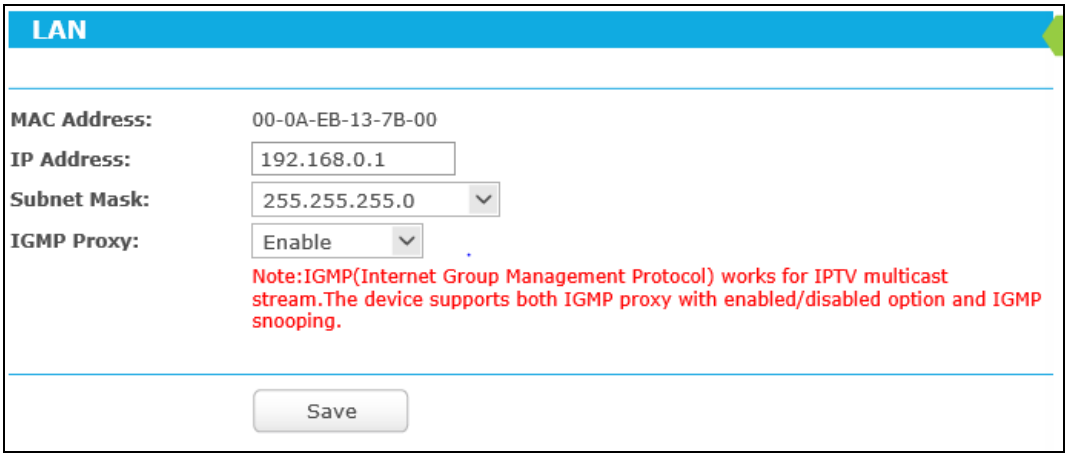
Click the **Save** button to save your settings.

Note:

1. Only the PC on your LAN can use the **MAC Address Clone** function.
2. If you change WAN MAC Address when the WAN connection is PPPoE, it will not take effect until the connection is re-established.

4.3.3 LAN

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

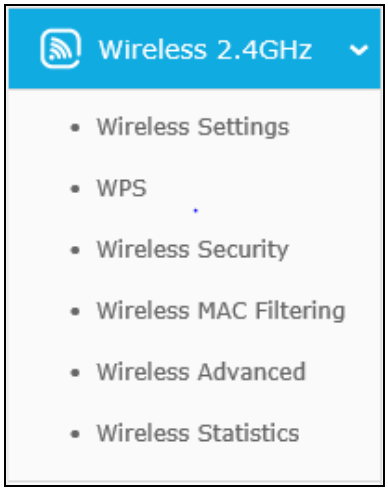


- **MAC Address -** The physical address of the LAN ports, as seen from the LAN. The value can't be changed.
- **IP Address -** Enter the IP address of your Router in dotted-decimal notation (factory default: 192.168.0.1).
- **Subnet Mask -** An address code that determines the size of the network. Normally use 255.255.255.0 as the subnet mask.
- **IGMP Proxy** - The Internet Group Management Protocol (IGMP) feature allows your devices in LAN can watch TV.

Note:

1. If you change the IP Address of LAN, you must use the new IP Address to login to the Router.
2. If the new LAN IP Address you set is not in the same subnet with the previous one, the IP Address pool in the DHCP server will be configured automatically，while the Virtual Server and DMZ Host will not take effect until they are re-configured.

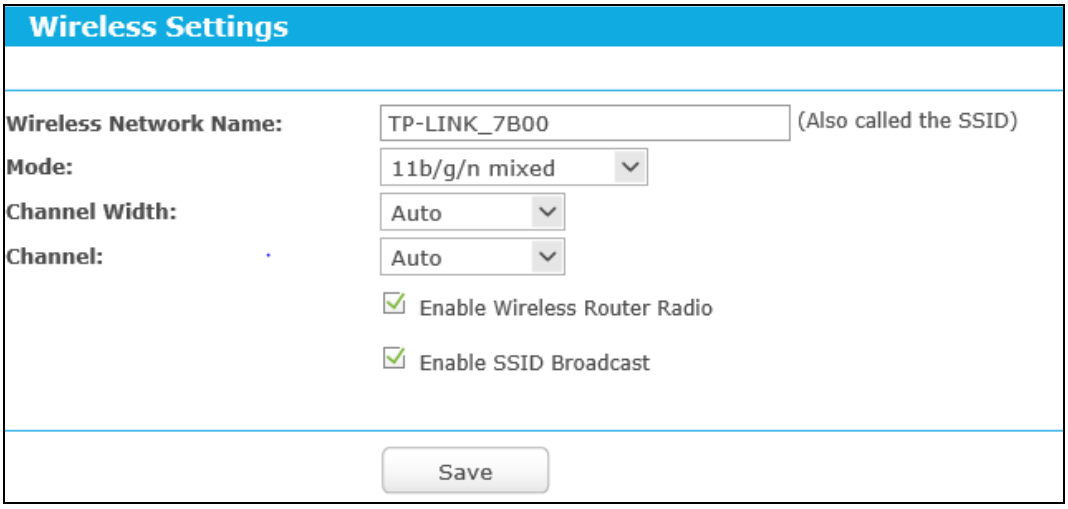
4.4 Wireless 2.4GHz/5GHz



There are five submenus under the Wireless menu: **Wireless Settings**, **WPS**, **Wireless Security, Wireless MAC Filtering, Wireless Advanced** and **Wireless Statistics**. Click any of them, and you will be able to configure the corresponding function.

4.4.1 Wireless Settings

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



- **Wireless Network Name -** Enter a string of up to 32 characters. The same name of SSID (Service Set Identification) must be assigned to all wireless devices in your network. The default SSID is set to be TP-LINK_XXXX (XXXX indicates the last unique four numbers of each Router's MAC address). But it is recommended strongly that you change your networks name (SSID) to a different value. This value is case-sensitive. For example, *TEST* is NOT the same as *test*.
- **Mode -** Select the desired mode. The default setting is 11bgn mixed.
  - **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.

  When 11bg mixed mode is selected, only 11bg mixed wireless stations can connect to the Router. It is strongly recommended that you set the Mode to 11bgn mixed, and all of 802.11b/g/n wireless stations can connect to the Router.

  ☞ **Note:**

  If **11bg mixed mode** 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.

- **Channel Width -** Select any channel width from the pull-down list. The default setting is automatic, which can automatically adjust the channel width for your clients.
- **Channel -** This field determines which operating frequency will be used. The default channel is set to **Auto**. It is not necessary to change the wireless channel unless you notice interference problems with another nearby access point.
- **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.

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

4.4.2 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. Select menu "**WPS**", you will see the next screen shown below.

- **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.
- **Disable PIN of this Device -** WPS external registrar of entering the device's PIN can be disabled or enabled manually. If the device receives multiple failed attempts to authenticate an external Registrar, this function will be disabled automatically.
- **Add Device -** You can add 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.

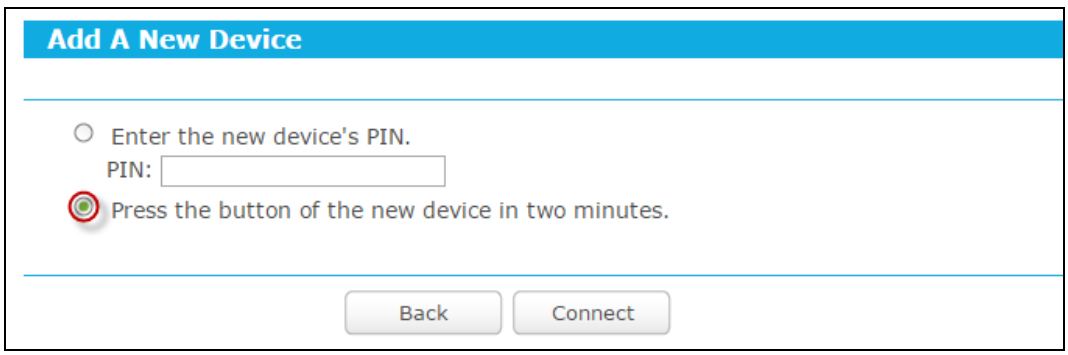
For the configuration of the new device, here takes the Wireless Adapter of our company for example.

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: Keep the WPS Status as **Enabled** and click the **Add Device** button, then the following screen will appear.



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

Step 3: For the configuration of the wireless adapter, please choose "**Push the button on my access point or wireless router**" in the configuration utility of the WPS as below, and click **Connect**.

The WPS Configuration Screen of Wireless Adapter

Step 1: Wait for a while until the next screen appears. Click **OK** to complete the WPS configuration.

The WPS Configuration Screen of Wireless Adapter

Method Two: Enter the PIN into my AP

Step 1: For the configuration of the wireless adapter, please choose "**Enter the PIN of this device into my access point or wireless router**" in the configuration utility of the WPS as below, and click **Connect**.

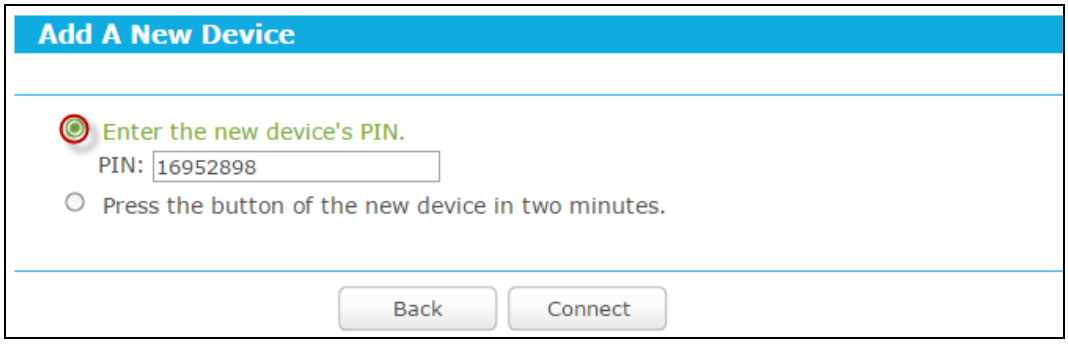
The WPS Configuration Screen of Wireless Adapter

Note:

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

Step 2: Keep the WPS Status as **Enabled** and click the **Add Device** button.

Step 3: Choose "**Enter the new device's PIN**" and enter the PIN code （take 16952898 for example） of the wireless adapter in the field after **PIN** as shown in the figure below. Then click **Connect**.



Method Three: Enter the PIN from my AP.

Step 1: Get the Current PIN code of the AP (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 the PIN of my access point or wireless router**" 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 **Connect**.

The WPS Configuration Screen of Wireless Adapter

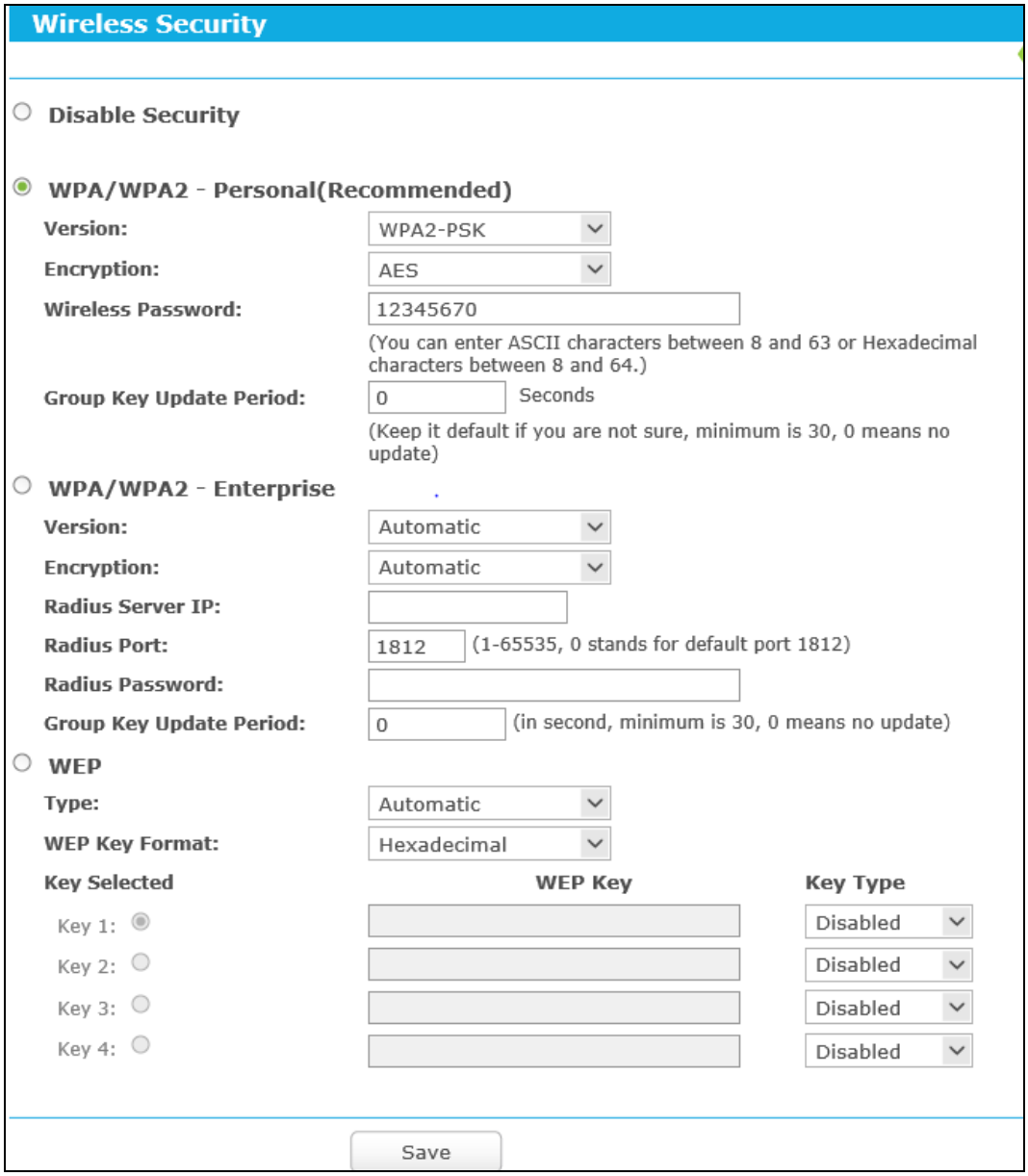
Note:

The default PIN code of the AP can be found in its label or the WPS configuration screen.

4.4.3 Wireless Security

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

There are three wireless security modes supported by the Router: WPA/WPA2-Personal, WPA/WPA2-Enterprise and WEP (Wired Equivalent Privacy).



- **Disable Security -** The wireless security function can be enabled or disabled. If disabled, the wireless stations will be able to connect the Router without encryption. But it's strongly recommended to choose one of the following modes to enable security.

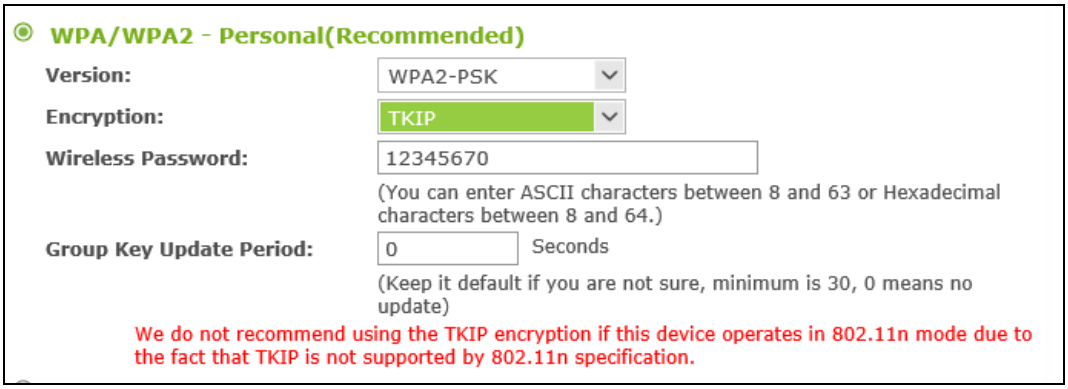
- **WPA-PSK/WPA2-Personal -** It's the WPA/WPA2 authentication type based on pre-shared passphrase.

  - **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-PSK/WPA2-PSK** radio button and choose TKIP encryption, you will find a notice in red as shown below.



- **WPA /WPA2-Enterprise -** It's based on Radius Server.
  - **Version -** you can choose the version of the WPA security from 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 **Automatic**, **TKIP** or **AES.**
  - **Radius Server IP -** Enter the IP address of the Radius server.
  - **Radius Port -** Enter the port that Radius server 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.
  - **Type -** you can choose the type for the WEP security on the pull-down list. The default setting is **Automatic**, which can select **Shared Key** or **Open System** authentication type automatically based on the wireless station's capability and request.
  - **WEP Key Format - Hexadecimal** and **ASCII** formats are provided here. **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 (Password) -** 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.

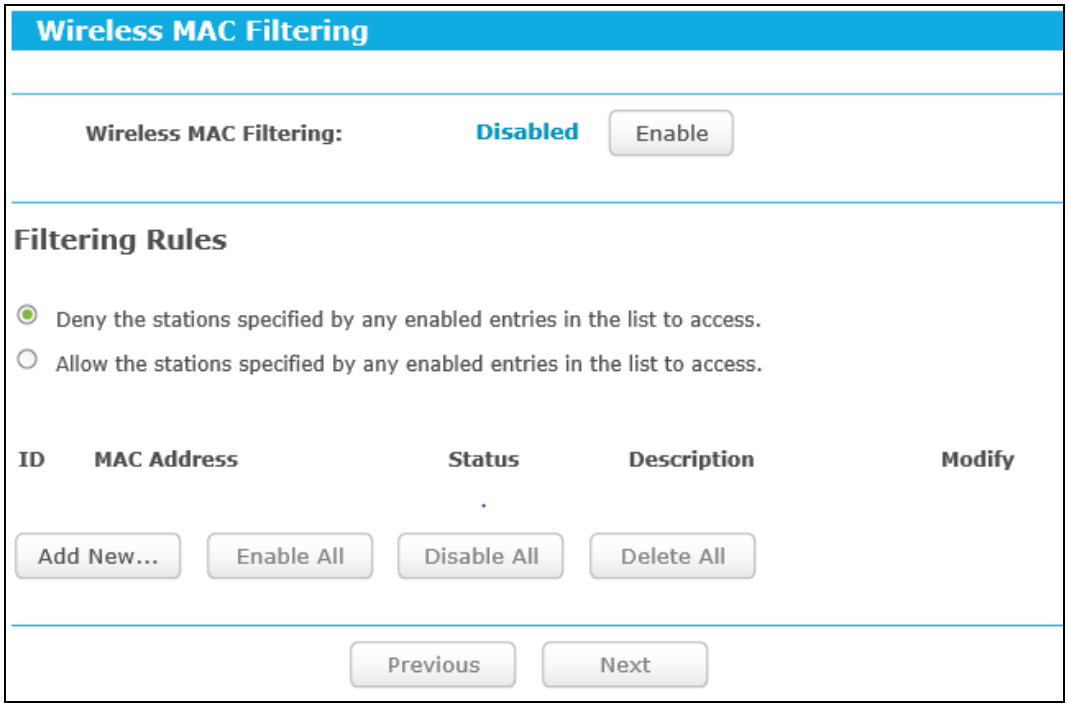
Note:

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

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

4.4.4 Wireless MAC Filtering

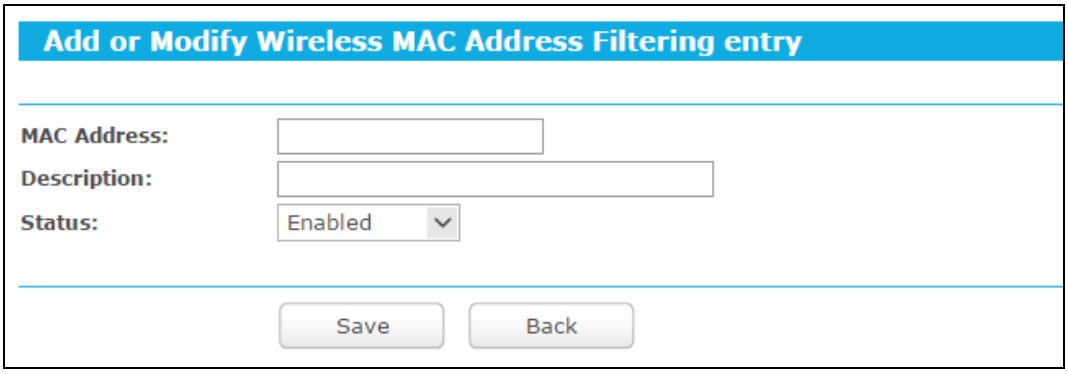
Choose menu "**Wireless → Wireless MAC Filtering**", and then you can control the wireless access by configuring the **Wireless MAC Filtering** function, as shown below.



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 access.
- **Status -** The status of this entry, either **Enabled** or **Disable**.
- **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 appea:



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

1. Enter the appropriate MAC Address into the **MAC Address** field. The format of the MAC Address is XX-XX-XX-XX-XX-XX (X is any hexadecimal digit). For example: 00-0A-EB-B0-00-0B.
2. Give a simple description for 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 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.

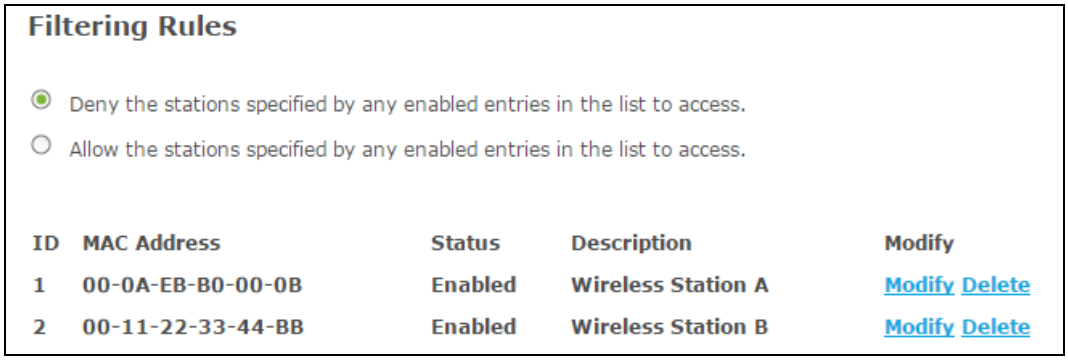
For example: If you desire that the wireless station A with MAC address 00-0A-EB-B0-00-0B and the wireless station B with MAC address 00-0A-EB-00-07-5F are able to access the Router, but all the other wireless stations cannot access the Router, you can configure the **Wireless MAC Address Filtering** list by following these steps:

1. Click the **Enabled** 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.

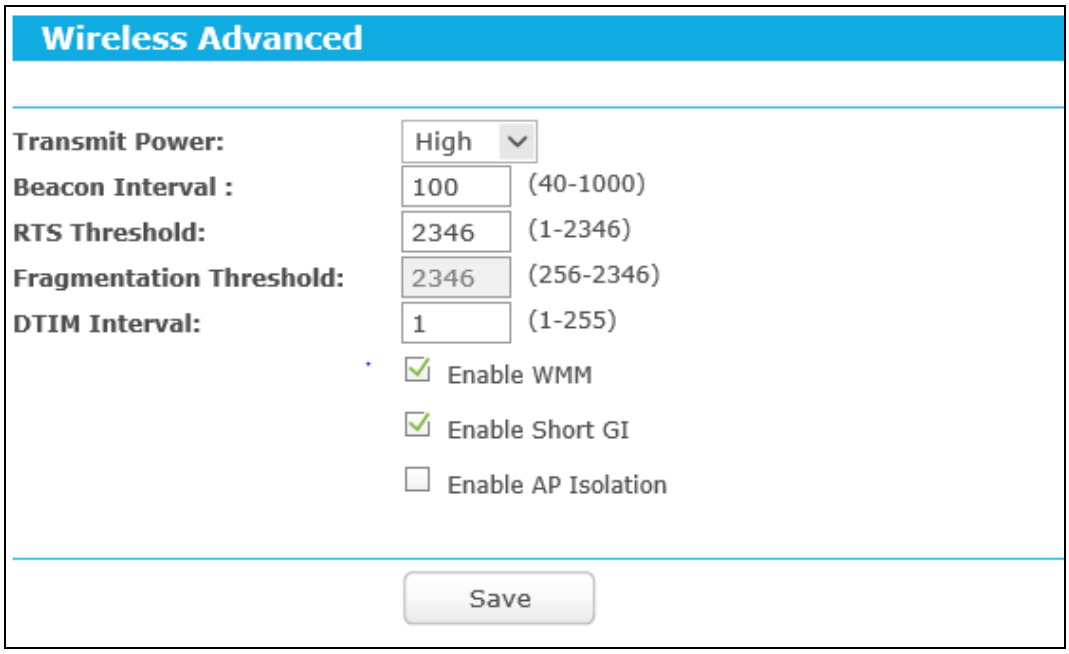
   1) Enter the MAC address 00-0A-EB-B0-00-0B/00-0A-EB-00-07-5F in the **MAC Address** field.
   2) Enter wireless station A/B in the **Description** field.
   3) Select **Enabled** in the **Status** pull-down list.
   4) Click the **Save** button.
   5) Click the **Back** button.

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



4.4.5 Wireless Advanced

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



- **Transmit Power -** Here you can specify the transmit power of Router. You can select High, Middle or Low which you would like. High is the default setting and is recommended.
- **Beacon Interval -** Enter a value between 20-1000 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.

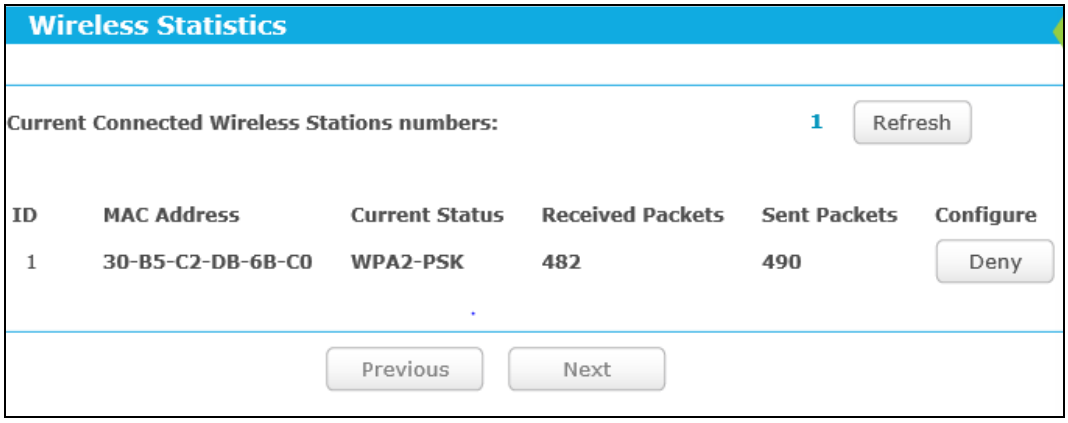
- **RTS Threshold -** Here you can specify the RTS (Request to Send) Threshold. If the packet is larger than the specified RTS Threshold size, the Router will send RTS frames to a particular receiving station and negotiate the sending of a data frame. The default value is 2346.
- **Fragmentation Threshold -** This value is the maximum size determining whether packets will be fragmented. Setting the Fragmentation Threshold too low may result in poor network performance because of 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.
- **Enable AP Isolation -** This function isolate all connected wireless stations so that wireless stations cannot access each other through WLAN. This function will be disabled if WDS/Bridge is enabled.

Note:

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

4.4.6 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.



- **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.
- **Configure -** The button is used for loading the item to the **Wireless MAC Filtering** list.
  - **Allow -** If the **Wireless MAC Filtering** function enable, allow the station to access.
  - **Deny -** If the **Wireless MAC Filtering** function enable, deny the station to access.

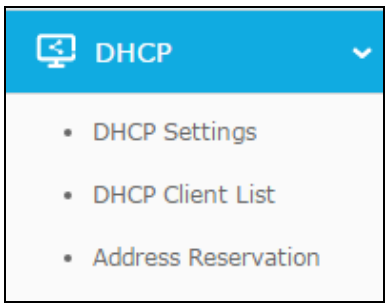
You cannot change any of the values on this page. To update this page and to show the current connected wireless stations, click on the **Refresh** button.

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.

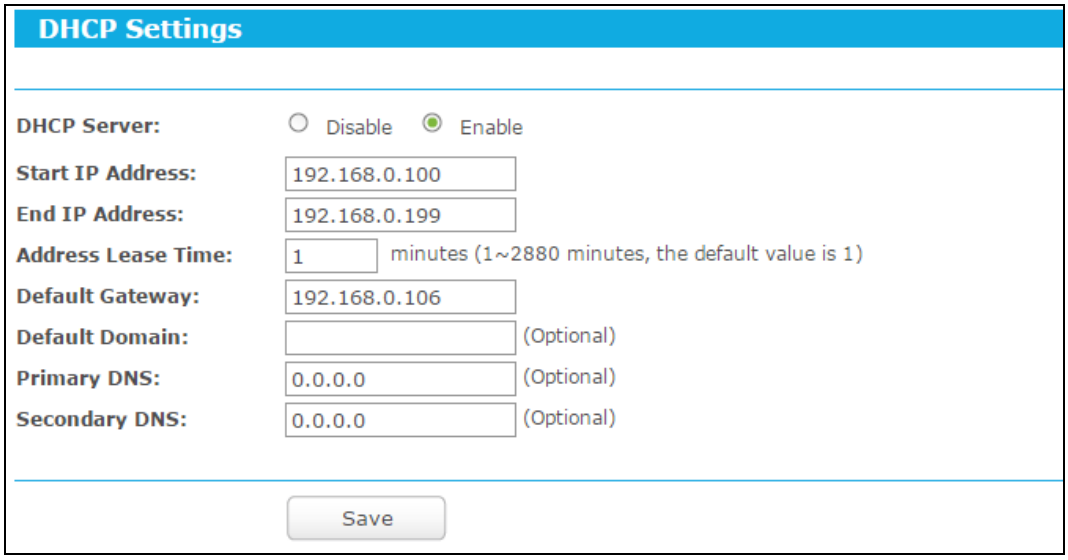
4.5 DHCP



There are three submenus under the DHCP menu, **DHCP Settings**, **DHCP Clients List** and **Address Reservation.** Click any of them, and you will be able to configure the corresponding function.

4.5.1 DHCP Settings

Choose menu "**DHCP → DHCP Settings**", and then you can configure the DHCP Server on the page as shown below. 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.



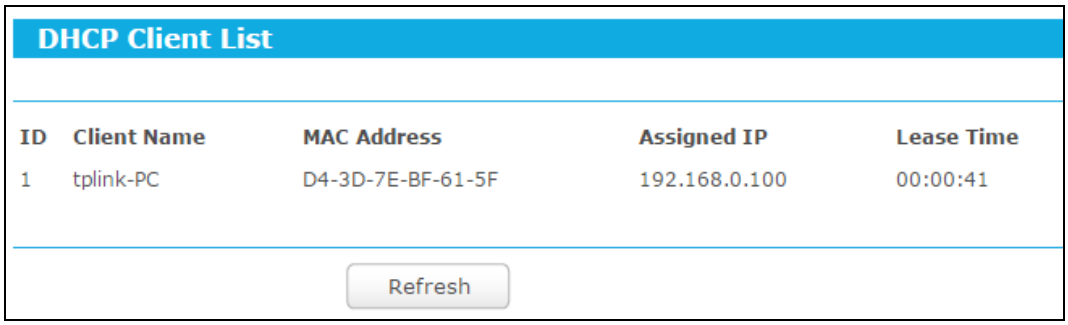
- **DHCP Server - Enable** or **Disable** the DHCP server. If you disable the Server, you must have another DHCP server within your network or else you must configure the computer manually.
- **Start IP Address -** Specify an IP address for the DHCP Server to start with when assigning IP addresses. 192.168.0.100 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) **-** It is suggested to input the IP address of the LAN port of the Router. The default value is 192.168.0.1.
- **Default Domain** (Optional) **-** Input the domain name of your network.
- **Primary DNS -** (Optional) Input the DNS IP address provided by your ISP or consult your ISP. 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".

4.5.2 DHCP Client List

Choose menu "**DHCP → DHCP Client List**", and then you can view the information about the clients attached to the Router in the screen as shown below.

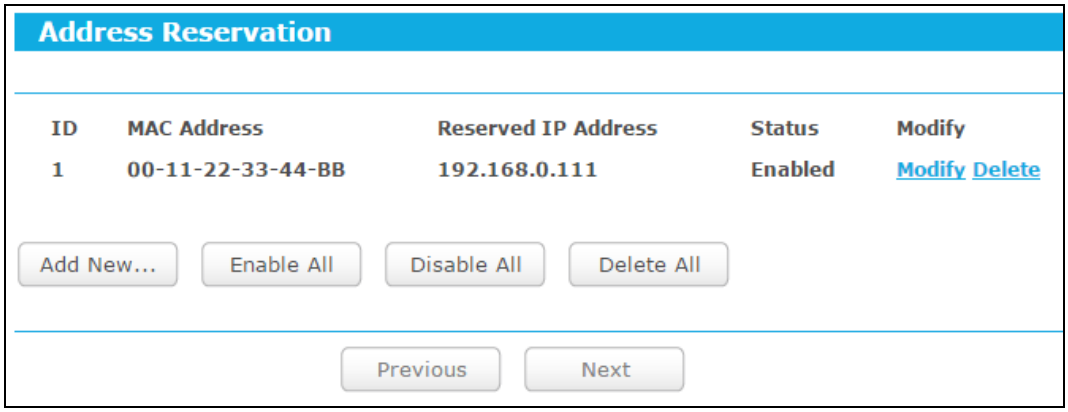


- **Client Name -** The name of the DHCP client
- **MAC Address -** The MAC address of the DHCP client
- **Assigned IP -** The IP address that the Router has allocated to the DHCP client
- **Lease Time -** The time of the DHCP client leased. After the dynamic IP address has expired, a new dynamic IP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

4.5.3 Address Reservation

Choose menu "**DHCP → Address Reservation**", and then you can view and add a reserved address for clients via the next screen. 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.

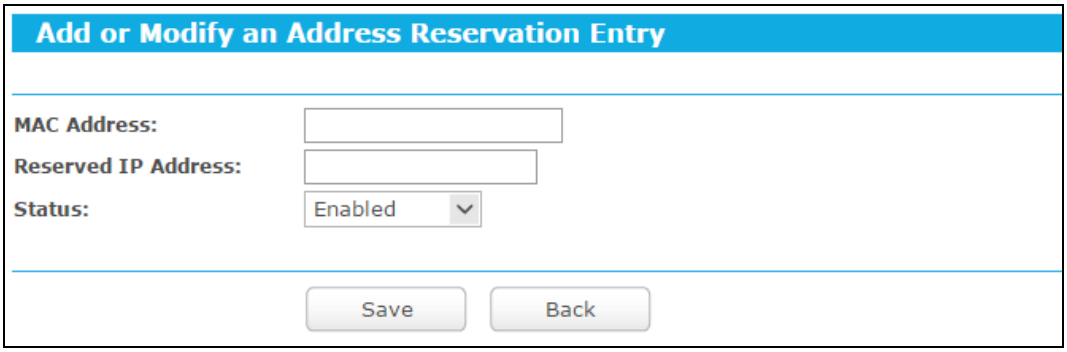


- **MAC Address -** The MAC address of the PC for which you want to reserve an IP address.

- **Reserved IP Address -** The IP address reserved for the PC by the Router.
- **Status -** The status of this entry, either **Enabled** or **Disabled**.
- **Modify -** To modify or delete an existing entry.

To Reserve an IP address:

1. Click the **Add New…** button. Then will pop-up.
2. Enter the MAC address (in XX-XX-XX-XX-XX-XX format.) and IP address (in dotted-decimal notation) of the computer for which you want to reserve an IP address.
3. Click the **Save** button.



To modify or delete an existing entry:

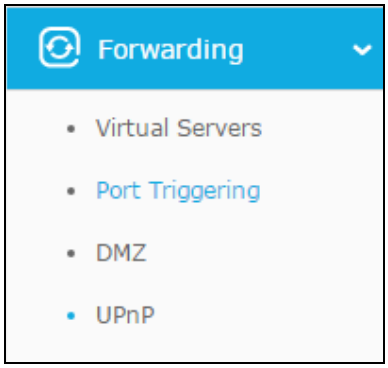
1. Click the **Modify** in the entry you want to modify. If you want to delete the entry, click the **Delete**.
2. Modify the information.
3. Click the **Save** button.

Click the **Enable/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.

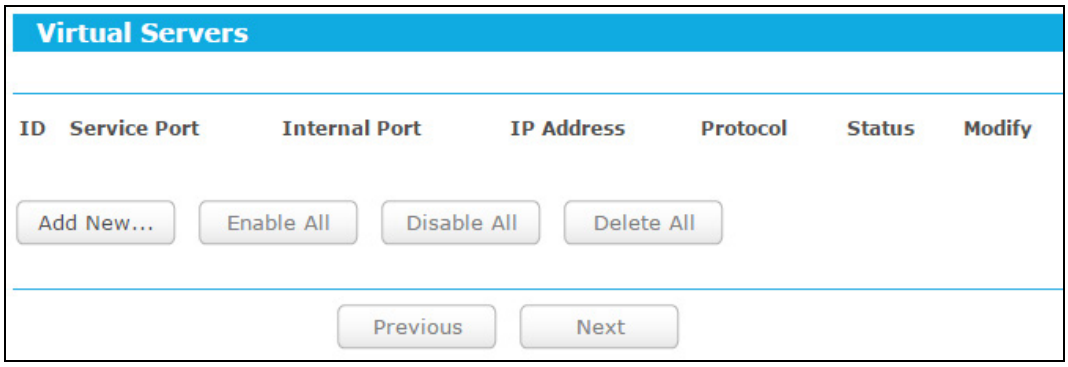
4.6 Forwarding



There are four submenus under the Forwarding menu: **Virtual Servers**, **Port Triggering**, **DMZ** and **UPnP**. Click any of them, and you will be able to configure the corresponding function.

4.6.1 Virtual Servers

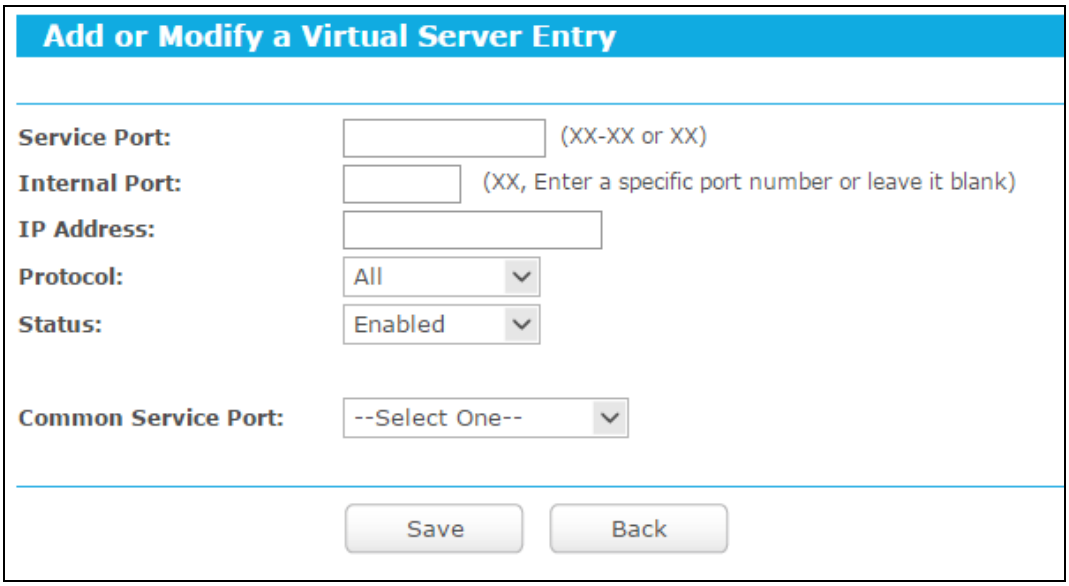
Choose menu "**Forwarding → Virtual Servers**", and then you can view and add virtual servers in the screen as shown below. Virtual servers can be used for setting up public services on your LAN, such as DNS, Email and FTP. A virtual server is defined as a service port, and all requests from the Internet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



- **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**.
- **Modify -** To modify or delete an existing entry.

To setup a virtual server entry:

1. Click the **Add New…** button, the next screen will pop-up as shown below.
2. Select the service port 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 service port number 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**, **UDP**, or **All**.
5. Select the **Enabled** to enable the virtual server.
6. Click the **Save** button.



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.

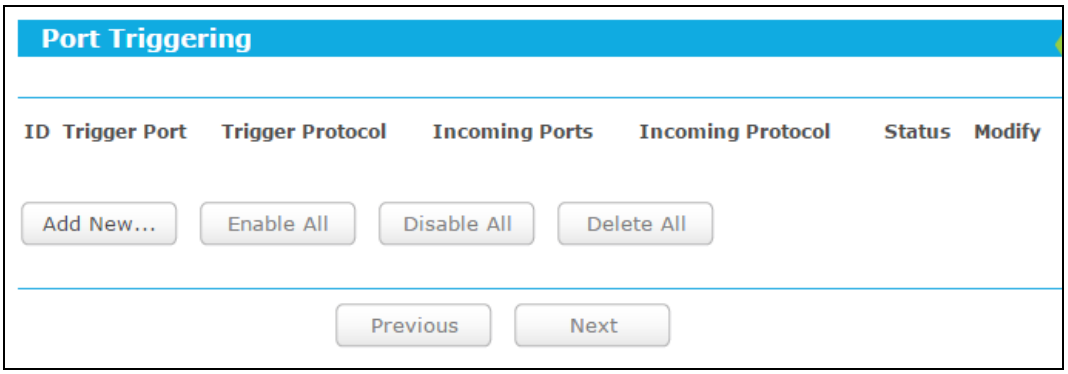
Click the **Next** button to go to the next page and click the **Previous** button to return the previous page.

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.

4.6.2 Port Triggering

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



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

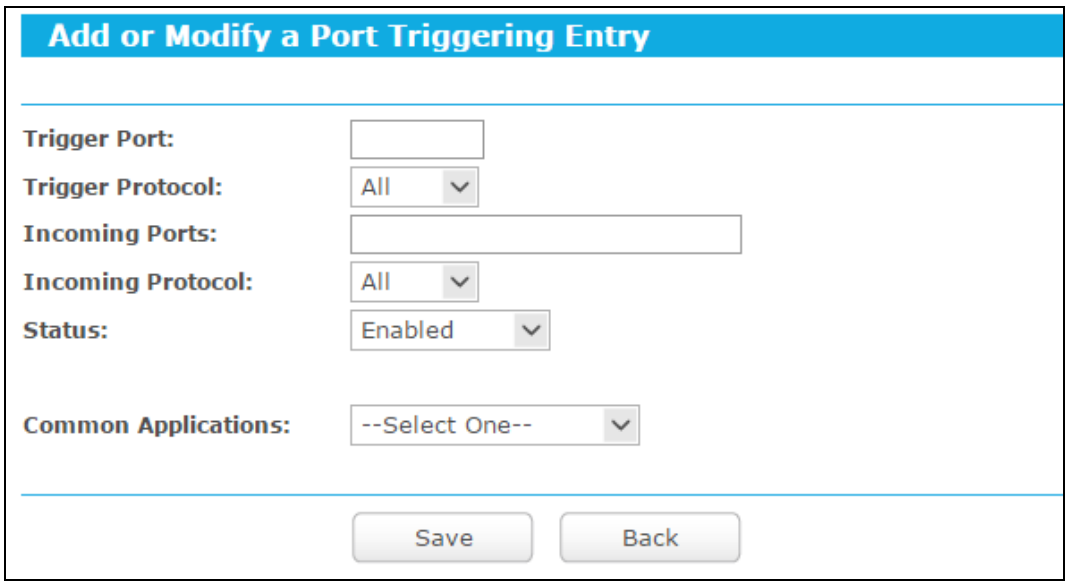
1. A local host makes an outgoing connection using a destination port number defined in the Trigger Port field.
2. The Router records this connection, opens the incoming port or ports associated with this entry in the Port Triggering table, and associates them with the local host.
3. When necessary， 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 Ports -** 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 sections). 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**.
- **Modify -** To modify or delete an existing entry.

To add a new rule, follow the steps below:

1. Click the **Add New…** button, the next screen will pop-up as shown below.
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 **Enabled** in **Status** field.
6. Click the **Save** button to save the new rule.



To modify or delete an existing entry:

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

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

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

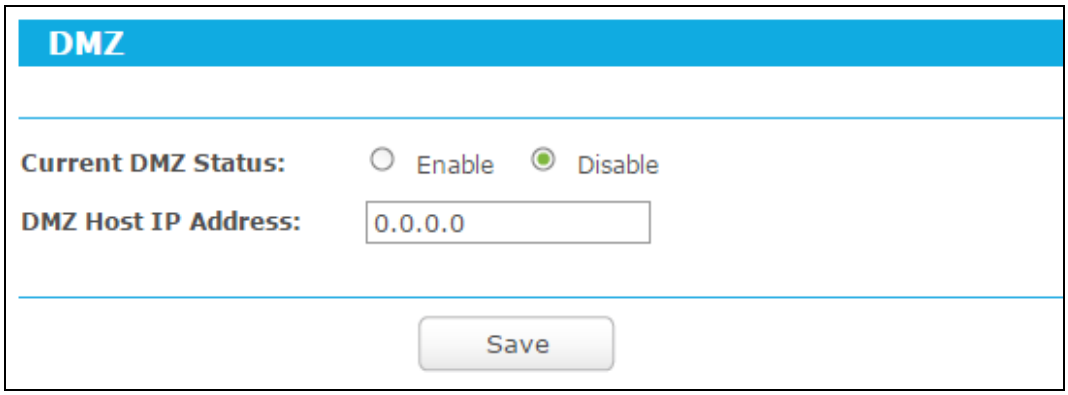
Click the **Delete All** button to delete all entries.

☞ **Note:**

1. When the trigger connection is released, the corresponding opening ports will be closed.
2. Each rule is 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.

4.6.3 DMZ

Choose menu "**Forwarding → DMZ**", and then you can view and configure DMZ host in the screen as shown below. 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.



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

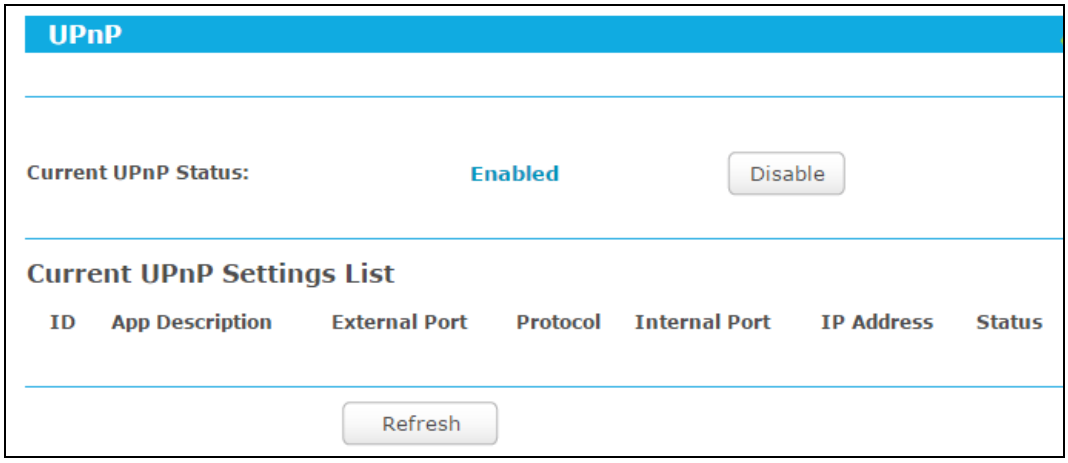
1. Check the **Enable** radio button.
2. Enter the IP Address of a local host in the **DMZ Host IP Address** field.
3. Click the **Save** button.

Note:

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

4.6.4 UPnP

Choose menu "**Forwarding** → **UPnP**", and then you can view the information about **UPnP** (Universal Plug and Play) in the screen as shown below. 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.

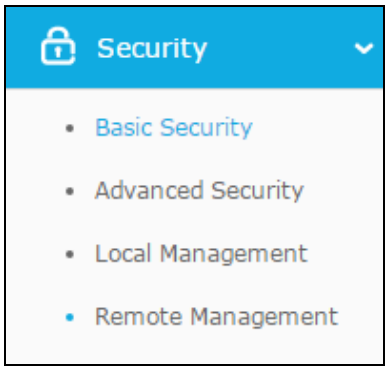


- **Current UPnP Status -** UPnP can be enabled or disabled by clicking the **Enable** or **Disable** button.
- **Current UPnP Settings List -** This table displays the current UPnP information.
  - **App Description -** The description provided by the application in the UPnP request.
  - **External Port -** The external port the Router opens for the application.
  - **Protocol -** The type of protocol the Router opens for the application.
  - **Internal Port -** The Internal port the Router opens for local host.

- **IP Address -** The IP address of the UPnP device that is currently accessing the Router.
- **Status -** The status of the port is displayed here. “Enabled” means that the port is still active. Otherwise, the port is inactive.

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

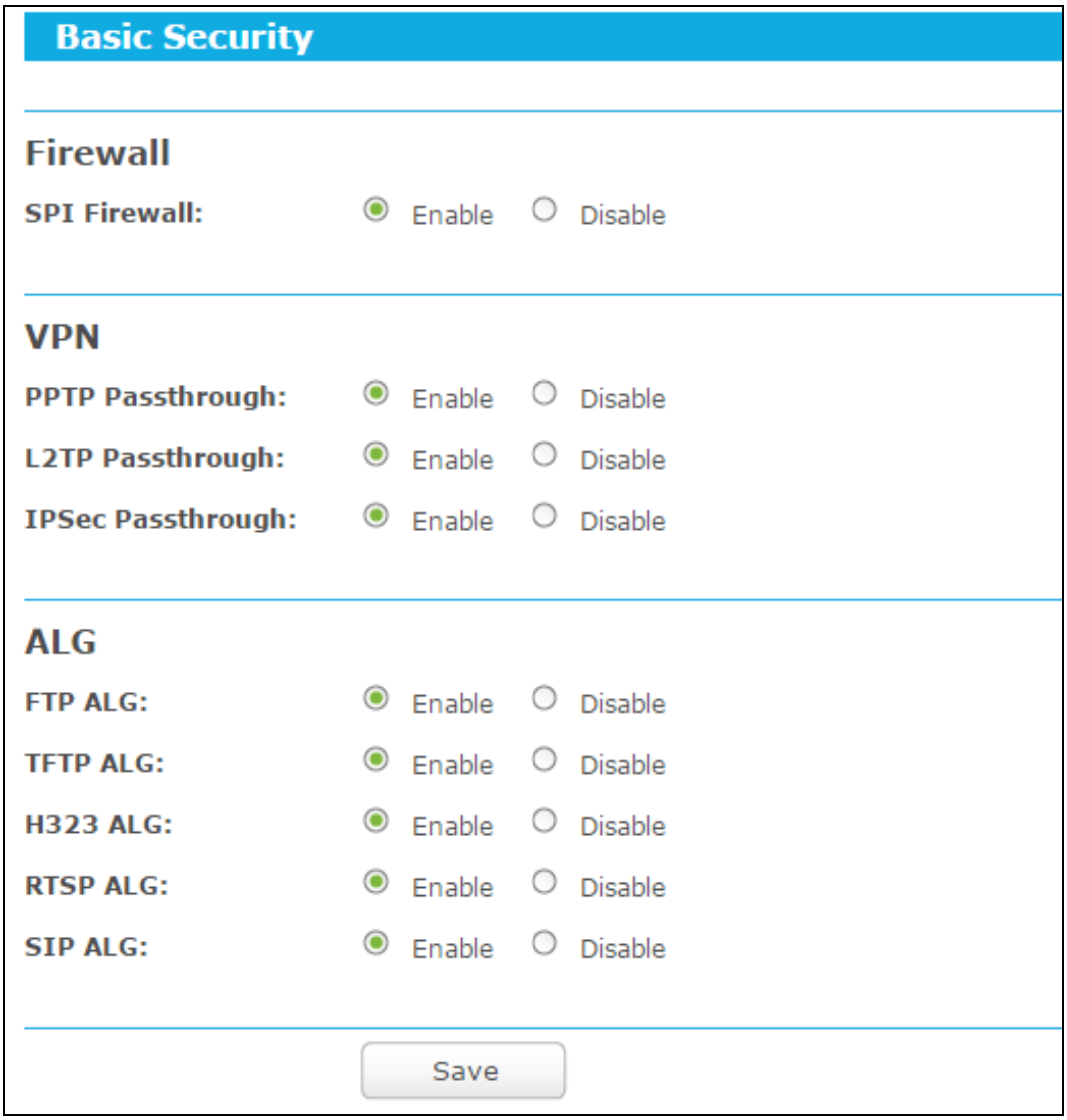
4.7 Security



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

4.7.1 Basic Security

Choose menu “**Security → Basic Security**”, you can configure the basic security in the screen as shown below.



- **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**.

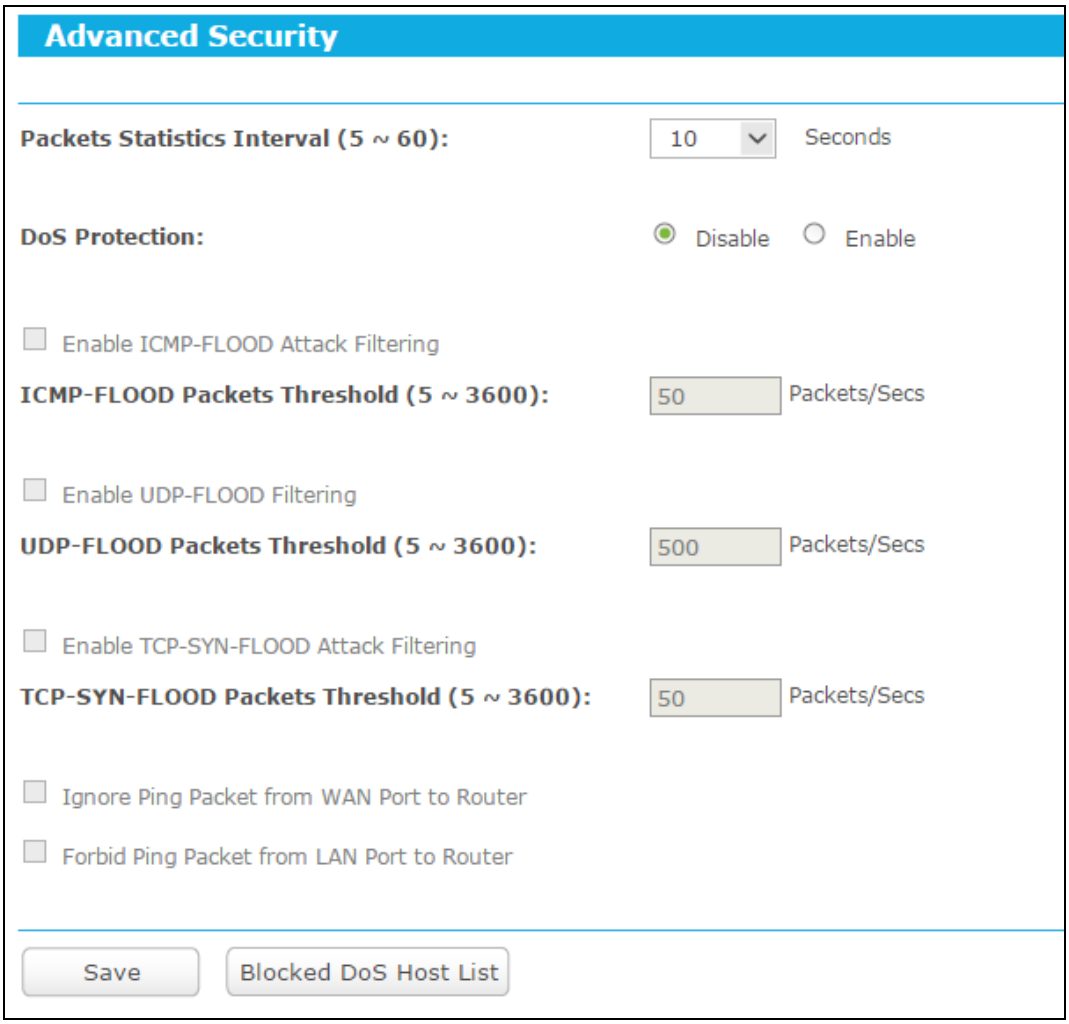
➢ **ALG -** It is recommended to enable Application Layer Gateway (ALG) because ALG allows customized Network Address Translation (NAT) traversal filters to be plugged into the gateway to support address and port translation for certain application layer "control/data" protocols such as FTP, TFTP, H323 etc.

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

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

4.7.2 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 below.



- **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.

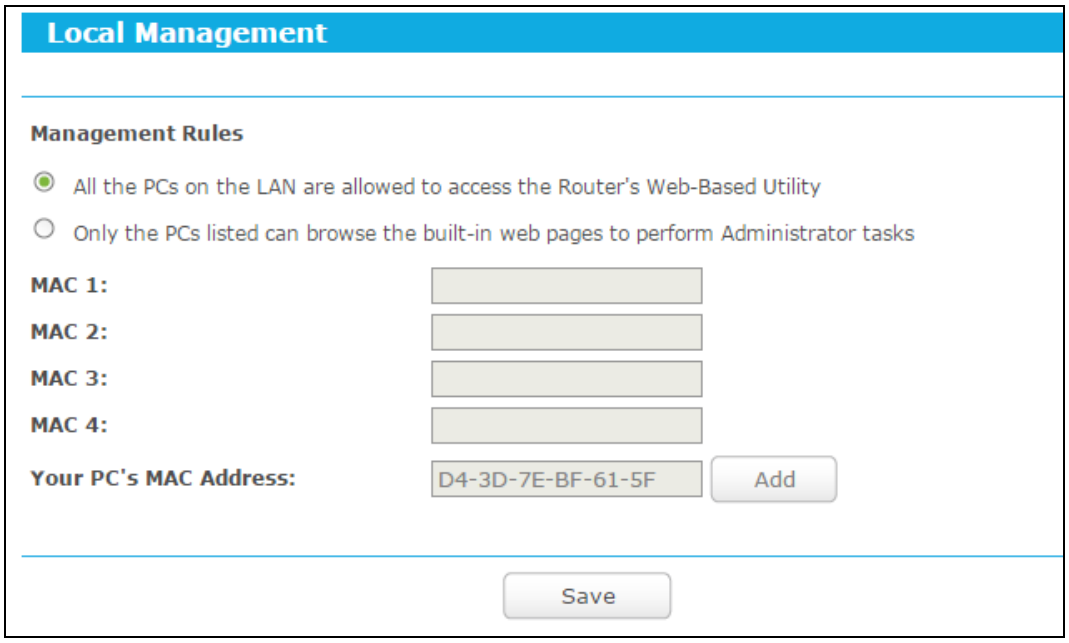
- **Enable UDP-FLOOD Filtering -** Enable or Disable the UDP-FLOOD Filtering.
- **UDP-FLOOD Packets Threshold (5~3600) -** The default value is 500. Enter a value between 5 ~ 3600. When the current UPD-FLOOD Packets number is beyond the set value, the Router will startup the blocking function immediately.
- **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.

4.7.3 Local Management

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



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.

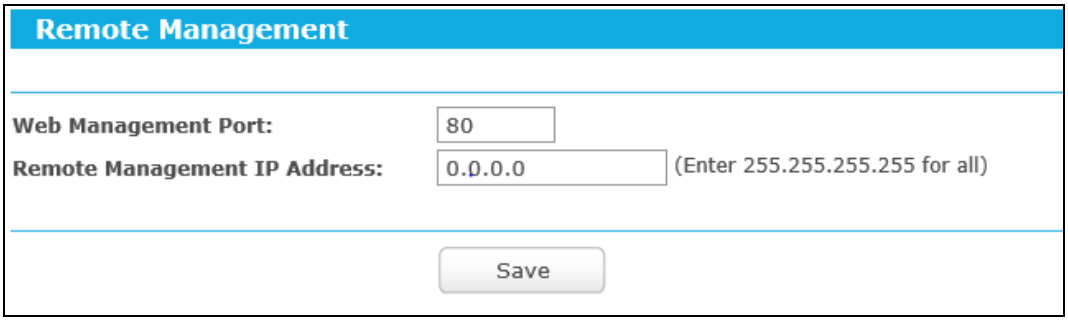
Click the **Save** button to save your settings.

Note:

If your PC is blocked but you want to access the Router again, press and hold the WPS button for more than 5 seconds to reset the Router to factory defaults.

4.7.4 Remote Management

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



- **Web Management Port -** Web browser access normally uses the standard HTTP service port 80. This router's default remote management Web port number is 80. For greater security, you can change the remote management Web interface to a custom port by entering that number in this box provided. Choose a number between 1024 and 65535, but do not use the number of any common service port.
- **Remote Management IP Address -** This is the current address you will use when accessing your router from the Internet. The default IP Address is 0.0.0.0. It means this function is disabled. To enable this function, change the default IP Address to another IP Address as desired.

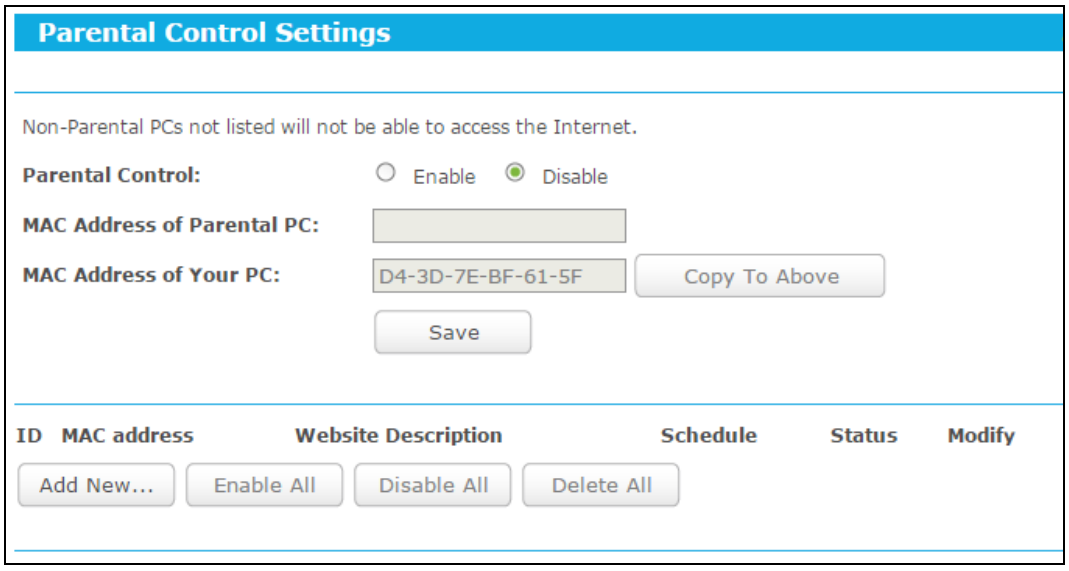
To access the router, you will type your router's WAN IP Address into your browser's Address (in IE) or Location (in Navigator) box, followed by a colon and the custom port number. For example, if your Router's WAN address is 202.96.12.8 and you use port number 8080, enter in your browser: http://202.96.12.8:8080.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

☞ **Note:**

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

4.8 Parental Control

Choose menu "**Parental Control**", and you can configure the parental control in the screen as shown below. 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.



- **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 below.
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 TP-LINK) 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. tp-link) in the Allowed Domain Name field. Any domain name with keywords in it (e.g. www.tp-link.com) 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.

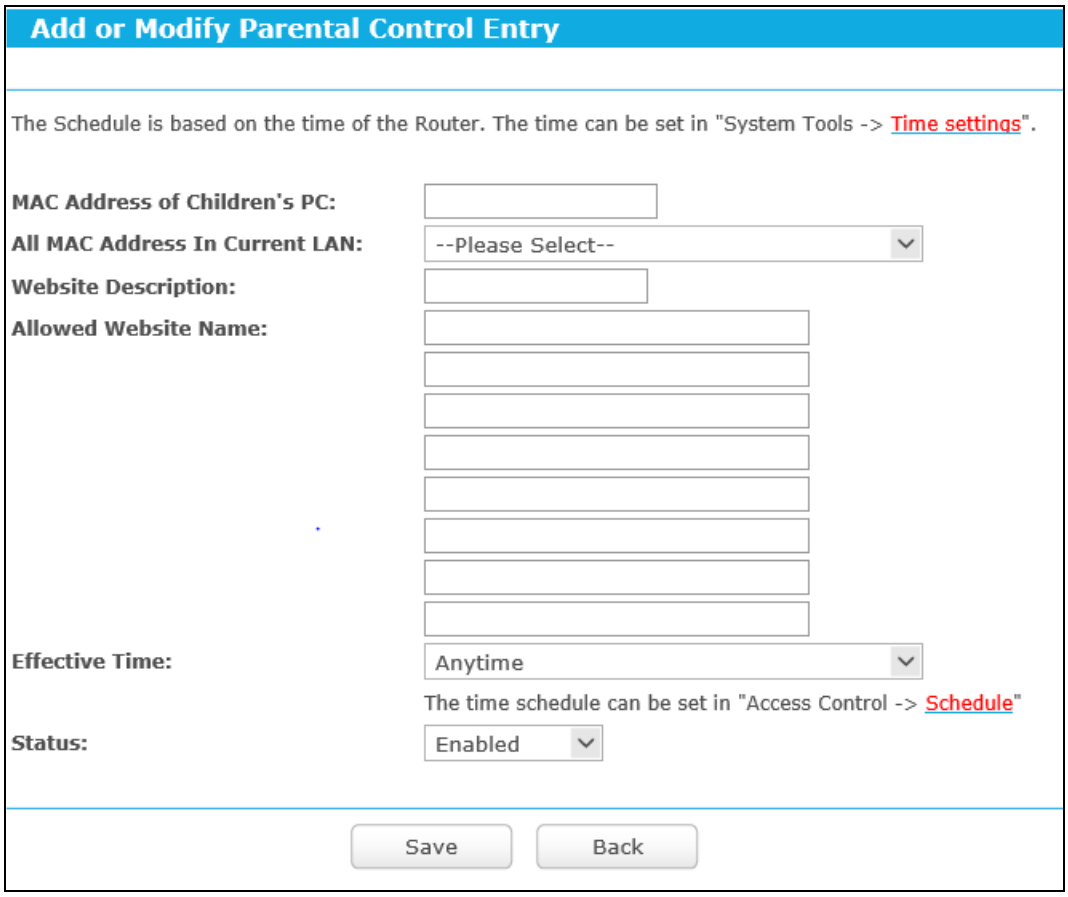
7. Click the **Save** button.

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.



For example: If you desire that the child PC with MAC address 00-11-22-33-44-AA can access www.tp-link.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.

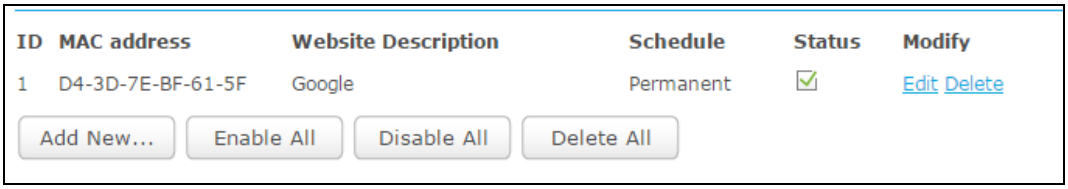
2. Click "**Access Restriction** → **Schedule**" on the left to enter the Schedule Settings page. Click **Add New...** button to create a new schedule with Schedule Description is Schedule_1, Day is Sat and Time is all day-24 hours.

3. Click "**Parental Control**" menu on the left to go back to the Add or Modify Parental Control Entry page:

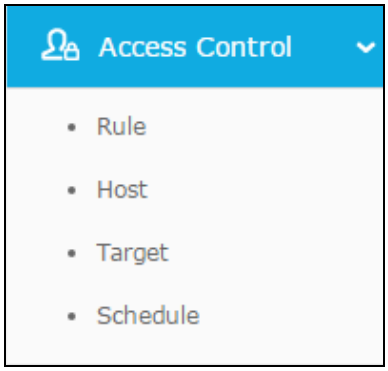
- Click **Add New...** button.
- Enter 00-11-22-33-44-AA in the **MAC Address of Child PC** field.
- Enter “Allow TP-LINK” in the **Website Description** field.
- Enter “www.tp-link.com” in the **Allowed Domain Name** field.
- Select “Schedule_1” you create just now from the **Effective Time** drop-down 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 below.



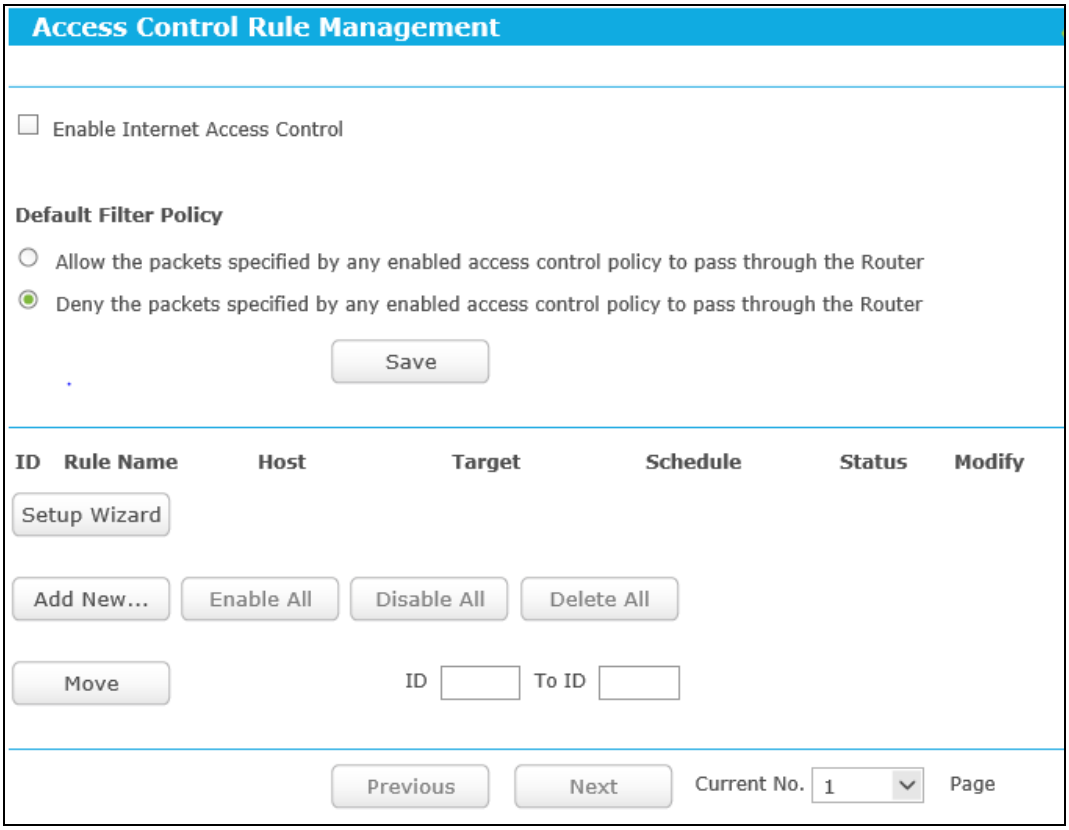
4.9 Access Control



There are four submenus under the Access Restriction menu: **Rule**, **Host**, **Target** and **Schedule**. Click any of them, and you will be able to configure the corresponding function.

4.9.1 Rule

Choose menu “**Access Control→ Rule**”, you can view and set Access Restriction rules in the screen as shown below.



- **Enable Internet Access Control -** Select the check box to enable the Internet Access Restriction 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.
- **Action -** Here displays the action the Router takes to deal with the packets. It could be **Allow** or **Deny**. **Allow** means that the Router permits the packets to go through the Router. **Deny** means that the Router rejects the packets to go through the Router.
- **Status -** This field displays the status of the rule. **Enabled** means the rule will take effect, **Disabled** means the rule will not take effect.
- **Modify -** Here you can edit or delete an existing rule.

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

1. Click the **Add New…** button and the next screen will pop-up as shown below.
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 **Action** field, select **Deny** or **Allow**.
7. In the **Status** field, select **Enabled** or **Disabled** to enable or disable your entry.
8. Click the **Save** button.

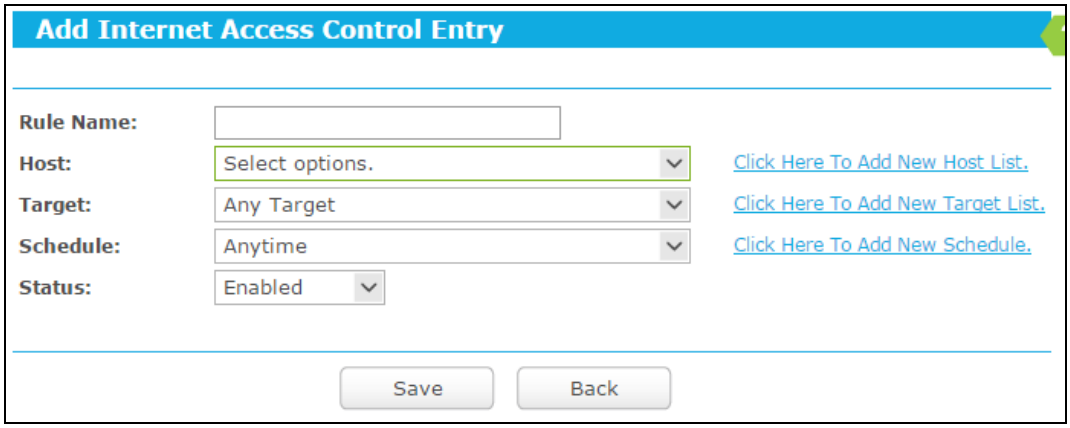
   Click the **Enable All** button to enable all the rules in the list.

   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.

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

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



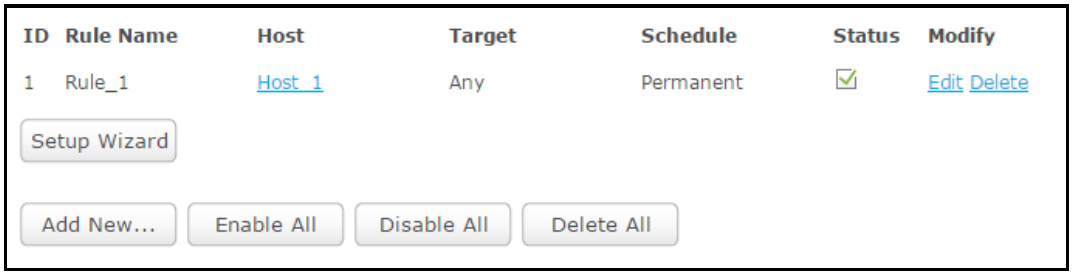
For example: If you desire to allow the host with MAC address 00-11-22-33-44-AA to access **www.tp-link.com** only from **18:00** to **20:00** on **Saturday and Sunday**, and forbid other hosts in the LAN to access the Internet, you should follow the settings below:

1. Click "**Access Control** → **Host**" in the left to enter the Host Settings page. Add a new entry with the Host Description is Host_1 and MAC Address is 00-11-22-33-44-AA.
2. Click "**Access Control** → **Target**" in the left to enter the Target Settings page. Add a new entry with the Target Description is Target_1 and Domain Name is www.tp-link.com.
3. Click "**Access Control** → **Schedule**" in the left to enter the Schedule Settings 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.
4. Click "**Access Control** → **Rule**" in the left to return to the Access Restriction Rule Management page. Select "**Enable Internet Access Restriction**" and choose "Deny the packets not specified by any access Restriction policy to pass through the Router".

5. Click **Add New...** button to add a new rule as follows:

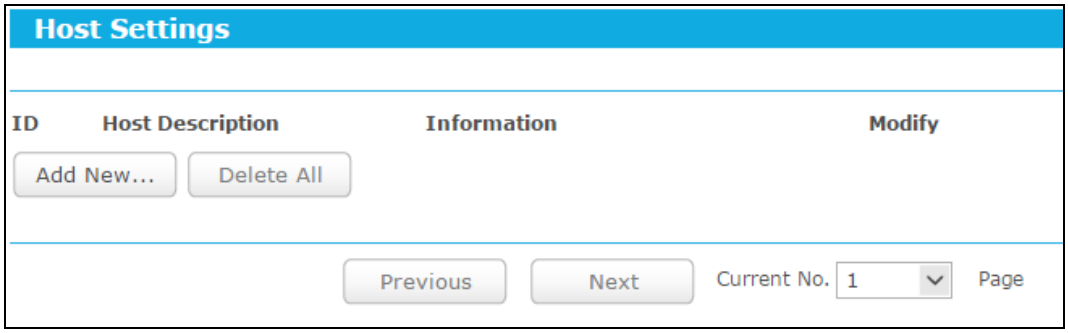
   - In **Rule Name** field, create a name for the rule. Note that this name should be unique, for example Rule_1.
   - In **Host** field, select Host_1.
   - In **Target** field, select Target_1.
   - In **Schedule** field, select Schedule_1.
   - In **Action** field, select Allow.
   - In **Status** field, select Enabled.
   - Click **Save** to complete the settings.

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



4.9.2 Host

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



- **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:
     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:.

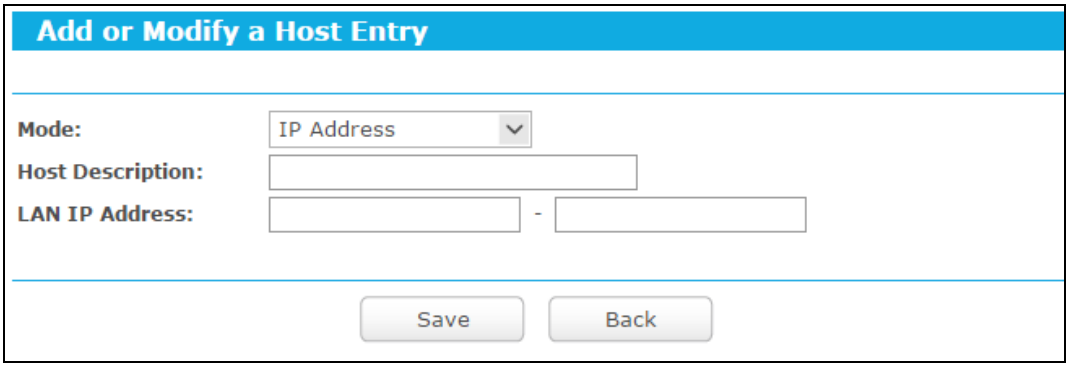
1) In **Host Description** field, create a unique description for the host (e.g. Host_1).

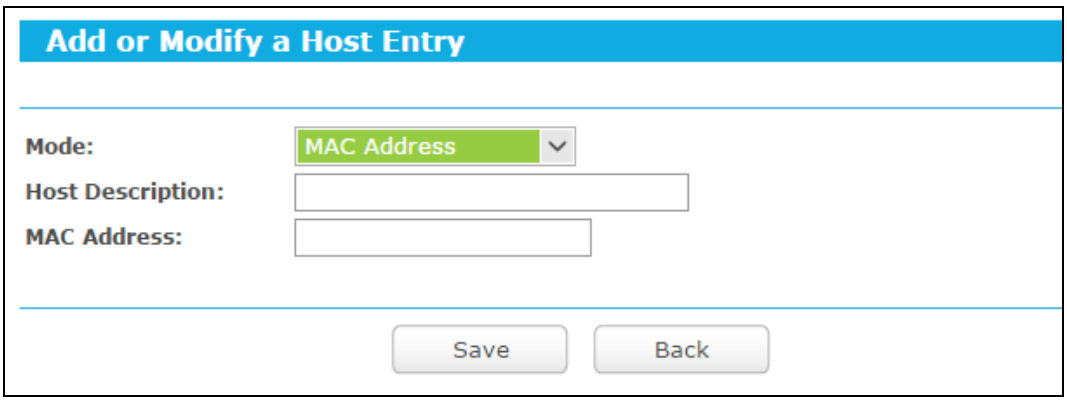
2) In **MAC Address** field, enter the MAC address.

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.

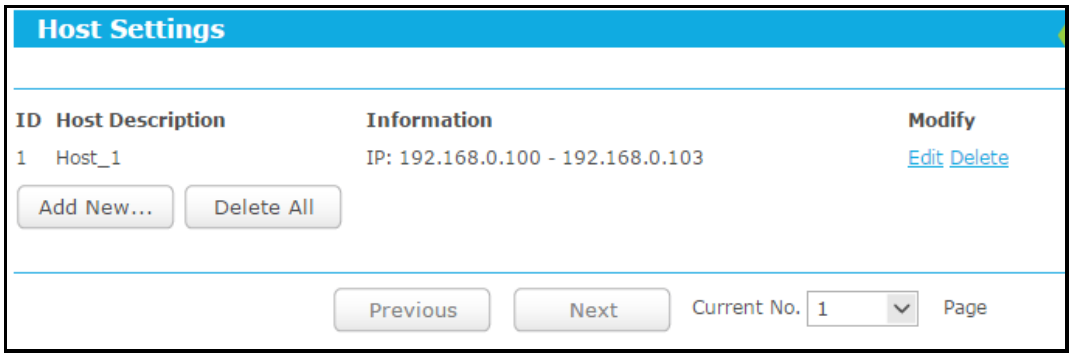




For example: If you desire to restrict the internet activities of host with MAC address 00-11-22-33-44-AA, you should first follow the settings below:

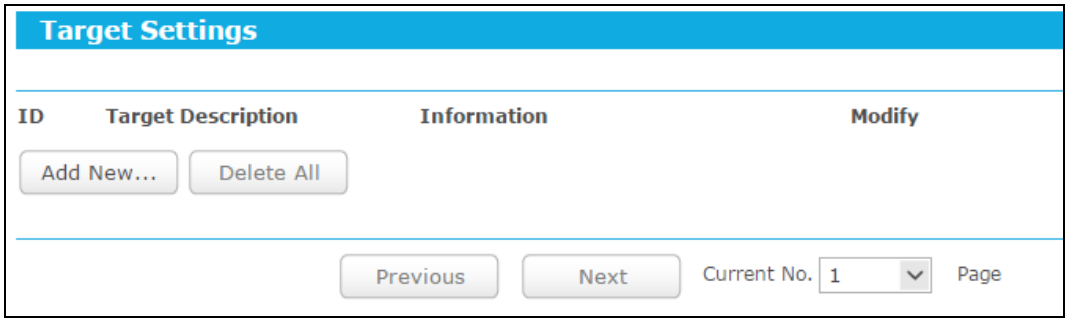
1. Click **Add New...** button to enter the Add or Modify a Host Entry page.
2. In **Mode** field, select MAC Address from the drop-down list.
3. In **Host Description** field, create a **unique** description for the host (e.g. Host_1).
4. In **MAC Address** field, enter 00-11-22-33-44-AA.
5. Click **Save** to complete the settings.

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



4.9.3 Target

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



- **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.

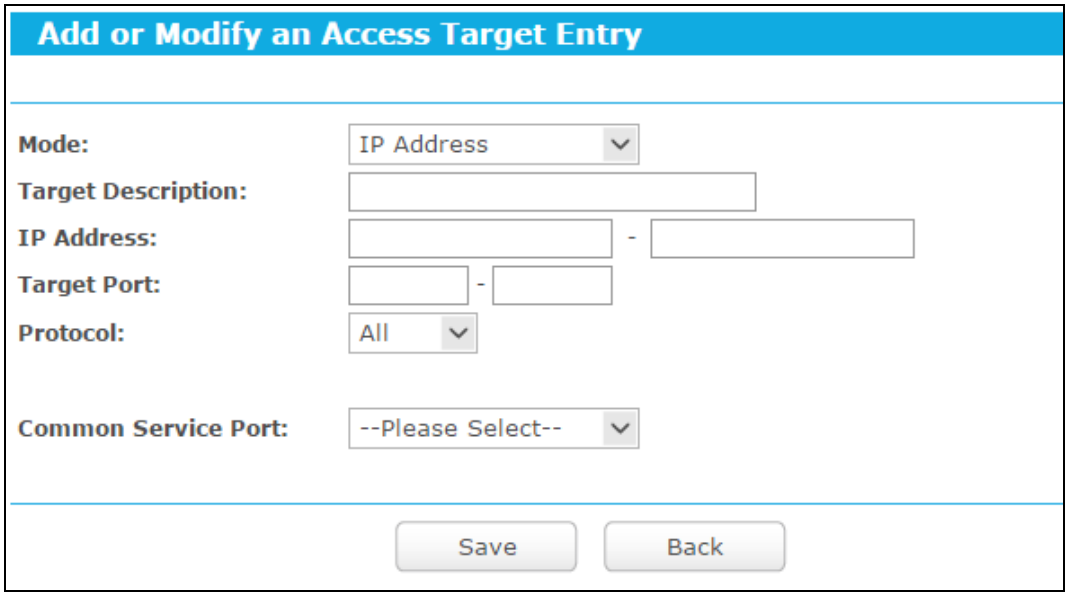
1. Click the **Add New…** button.
2. In **Mode** field, select IP Address or Domain Name.
   - If you select **IP Address**:
     1) In **Target Description** field, create a unique description for the target (e.g. Target_1).
     2) In **IP Address** field, enter the IP address of the target.
     3) 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**:
     1) In **Target Description** field, create a unique description for the target (e.g. Target_1).

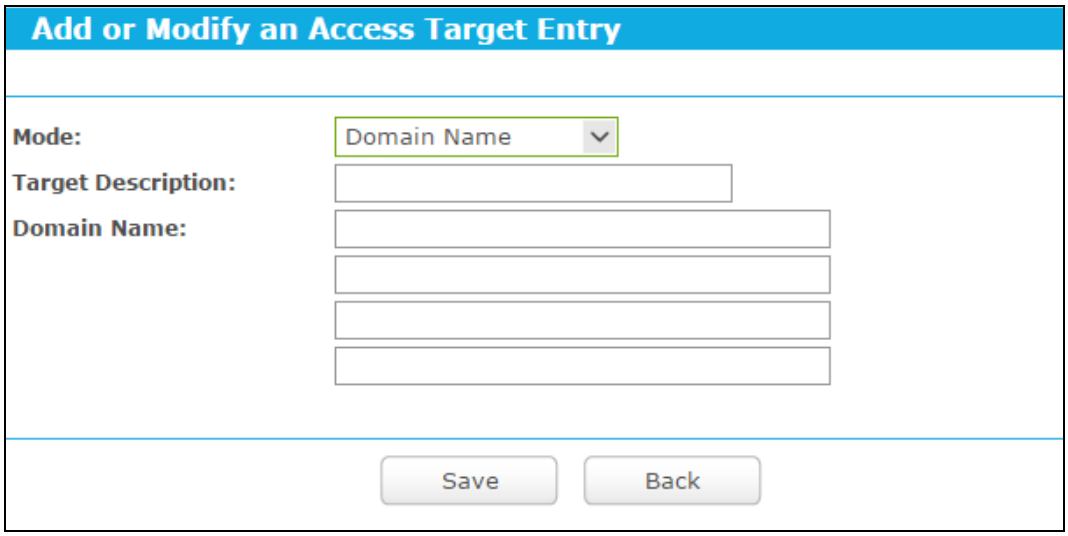
2) In **Domain Name** field, enter the domain name, either the full name or the keywords (for example TP-LINK) in the blank. Any domain name with keywords in it (e.g. www.tp-link.com) will be blocked or allowed. You can enter 4 domain names.

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.



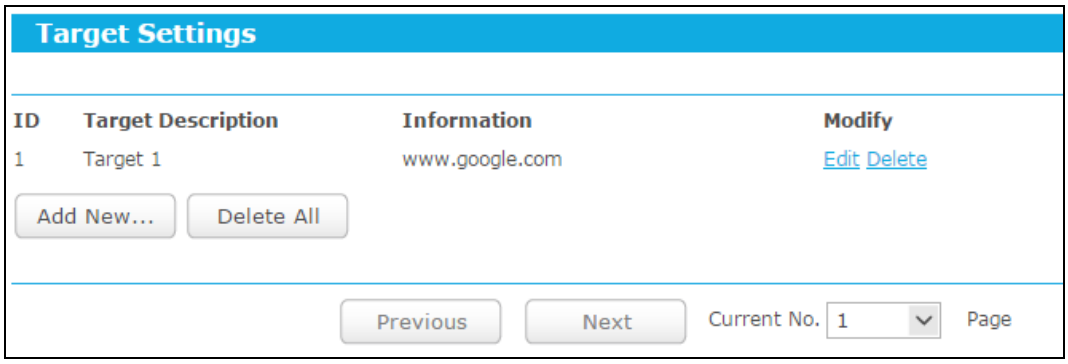


For example: If you desire to restrict the internet activities of host with MAC address 00-11-22-33-44-AA in the LAN to access **www.tp-link.com** only, you should first follow the settings below:

1. Click **Add New…**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.tp-link.com.

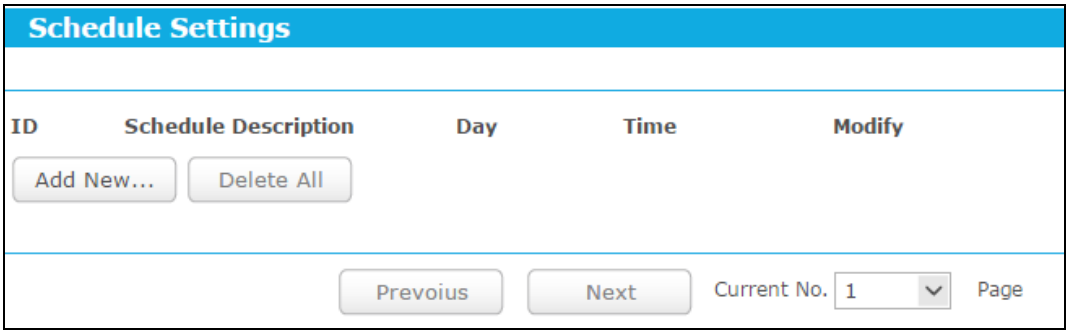
5. Click **Save** to complete the settings.

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



4.9.4 Schedule

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



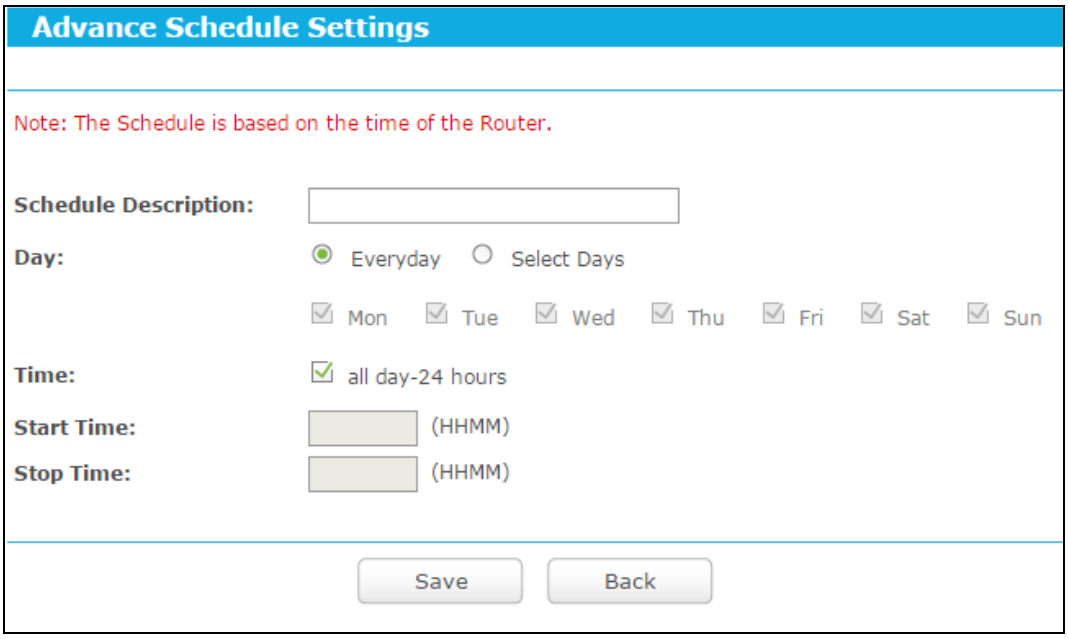
- **Schedule Description -** Here displays the description of the schedule and this description is unique.
- **Day -** Here displays the day(s) in a week.
- **Time -** Here displays the time period in a day.
- **Modify -** Here you can edit or delete an existing schedule.

To add a new schedule, follow the steps below.

1. Click **Add New...** button shown and the next screen will pop-up as shown below.
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.

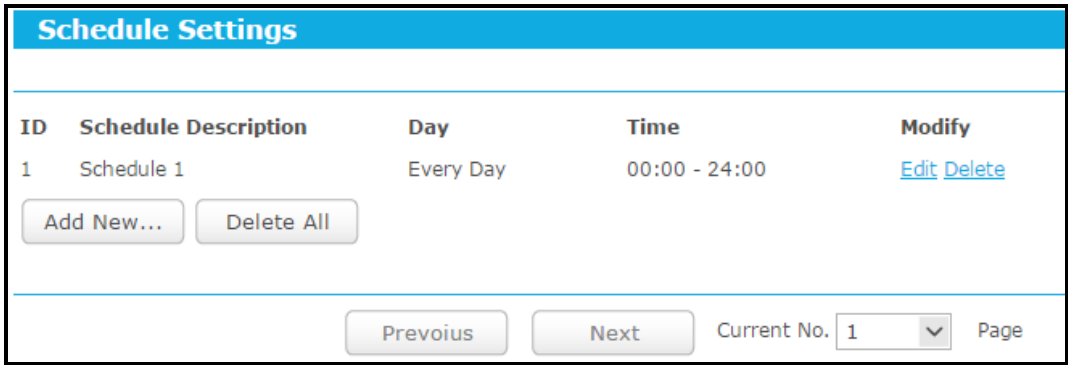
Click the **Next** button to go to the next page, or click the **Previous** button return to the previous page.



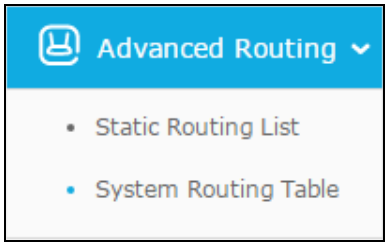
For example: If you desire to restrict the internet activities of host with MAC address 00-11-22-33-44-AA to access www.tp-link.com only from **18:00 to 20:00** on **Saturday** and **Sunday**, you should first follow the settings below:

1. Click **Add New...** 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.



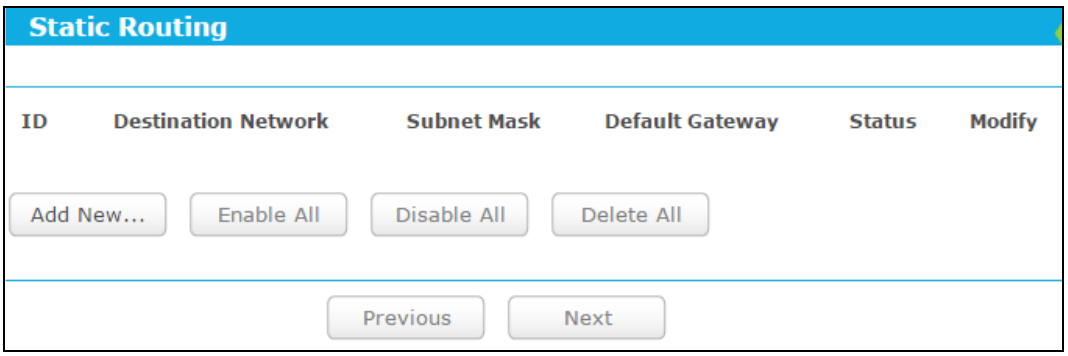
4.10 Advanced Routing



There are two submenus under the Network menu: **Static Routing List** and **System Routing Table**. Click any of them, and you will be able to configure the corresponding function.

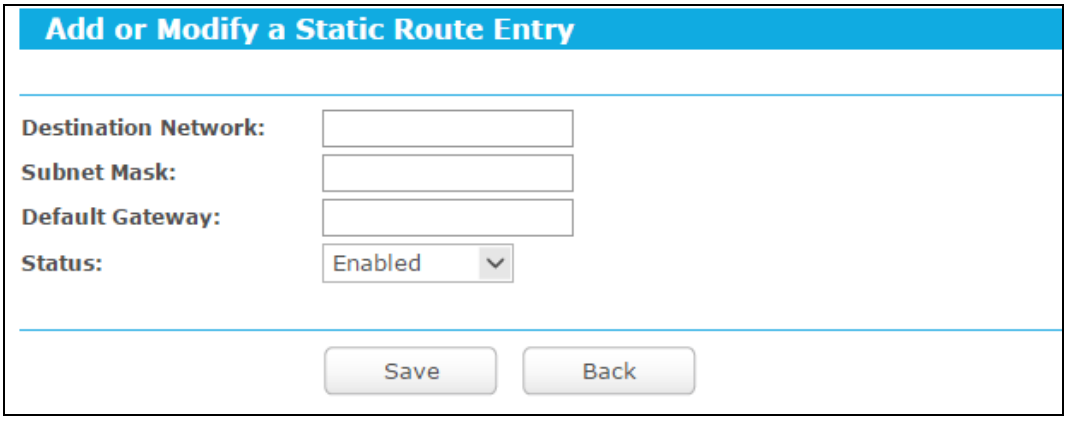
4.10.1 Static Routing List

Choose menu **"Static Routing"**, and you can configure the static route in the next screen. A static route is a pre-determined path that network information must travel to reach a specific host or network.



To add static routing entries, follow the steps below.

1. Click **Add New…**, and you will see the following screen.



2. Enter the following data.

- **Destination Network -** The **Destination IP Address** is the address of the network or host that you want to assign to a static route.
- **Subnet Mask -** The **Subnet Mask** determines which portion of an IP Address is the network portion, and which portion is the host portion.

- **Default Gateway -** This is the IP Address of the gateway device that allows for contact between the Router and the network or host.

3. Select **Enabled** or **Disabled** for this entry on the **Status** drop-down list.
4. Click the **Save** button to make the entry take effect.

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

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

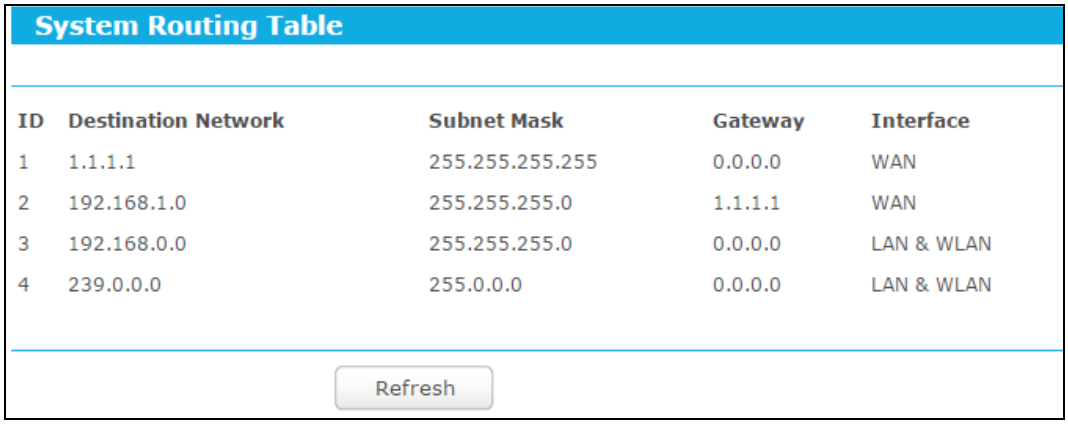
   Click the **Disable All** button to disable all the entries.

   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.

4.10.2 System Routing Table

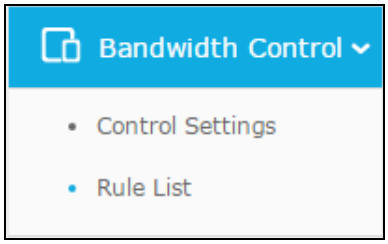
Choose menu "**Advanced Routing → System Routing Table**", and you can views all of the valid route entries in use. The Destination IP address, Subnet Mask, Gateway, and Interface will be displayed for each entry.



- **Destination Network -** The Destination IP Address 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)**.

Click the **Refresh** button to refresh the data displayed.

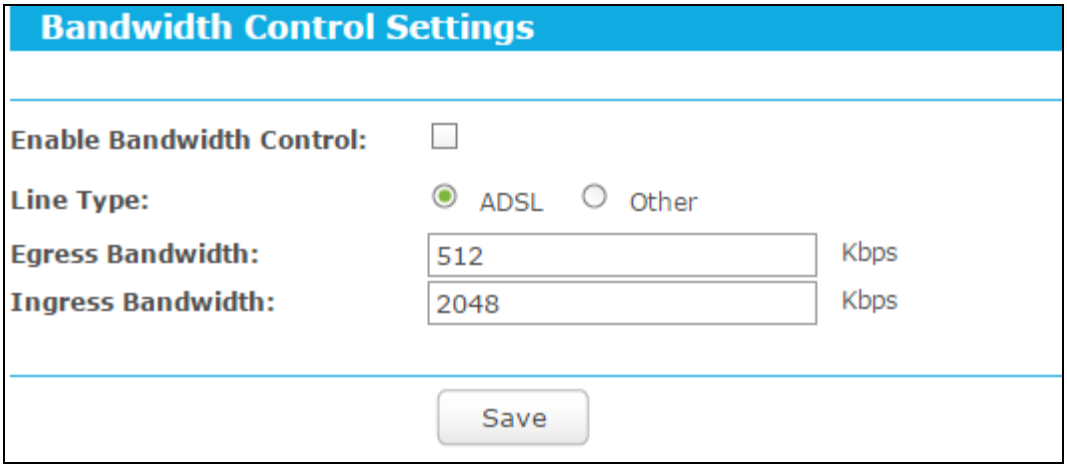
4.11 Bandwidth Control



There are two submenus under the Bandwidth Control menu as shown. Click any of them, and you will be able to configure the corresponding function. The detailed explanations for each submenu are provided below.

4.11.1 Control Settings

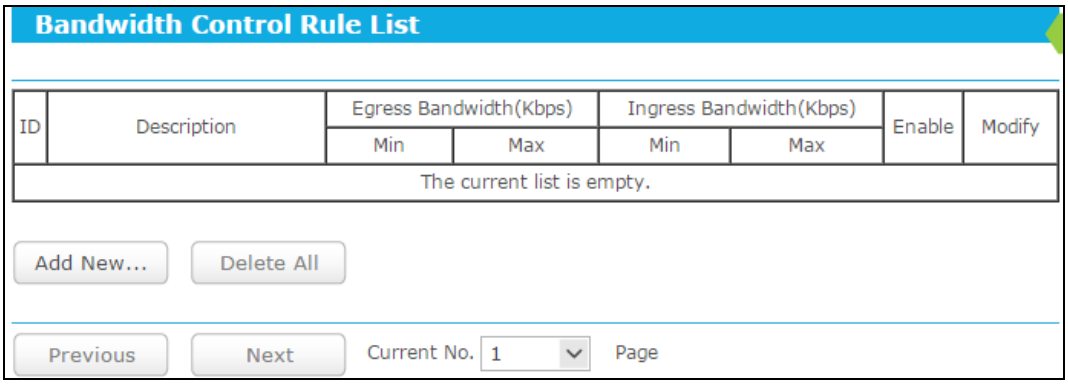
Choose menu "**Bandwidth Control → Control Settings**", you can configure the Egress Bandwidth and Ingress Bandwidth in the next screen. Their values you configure should be less than 100000Kbps. For optimal control of the bandwidth, please select the right Line Type and ask your ISP for the total bandwidth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



- **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.

4.11.2 Rule List

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

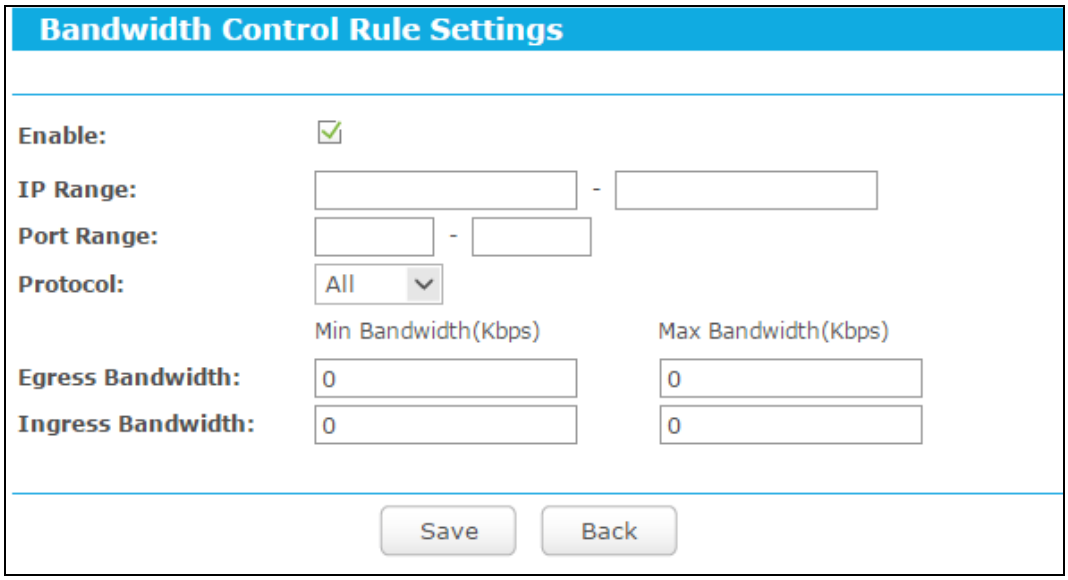


- **Description -** This is the information about the rules such as address range.
- **Egress Bandwidth -** This field displays the max and mix upload bandwidth through the WAN port, the default is 0.
- **Ingress Bandwidth -** This field displays the max and mix download bandwidth through the WAN port, 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.

Step 1: Click **Add New…**, you will see a new screen shown below.

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

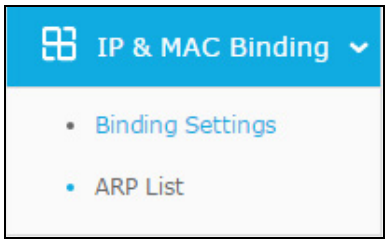


- **Enable** - Enable or disable the rule.
- **IP Range** - Interior PC address range. If both are blank (or 0.0.0.0), the domain is no effective.
- **Port Range** - The port range which the Interior PC access the outside PC. If all are blank (or 0), the domain is no effective.

- **Protocol** - Transport layer protocol, here there are All, TCP, UDP.
- **Egress Bandwidth** - The max and the min upload speed which through the WAN port, default number is 0.
- **Ingress Bandwidth** - The max and the min download speed through the WAN port, default number is 0.

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

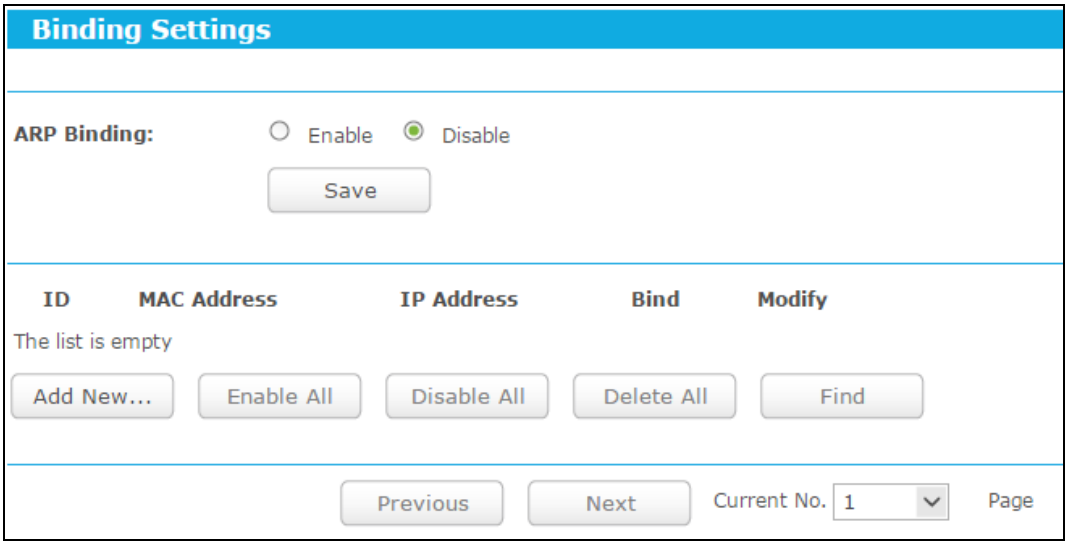
4.12 IP & MAC Binding



There are two submenus under the IP & MAC Binding menu: **Binding Setting** 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.

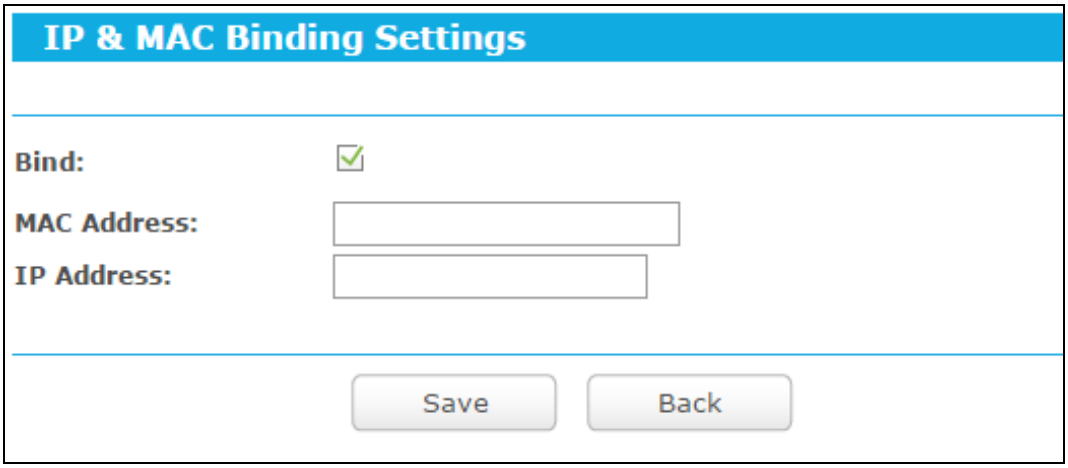
4.12.1 Binding Setting

This page displays the IP & MAC Binding Setting table; you can operate it in accord with your desire.



- **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 -** Whether or not enable the ARP binding.
- **Modify -** Edit or delete item.

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.



To add IP & MAC Binding entries:

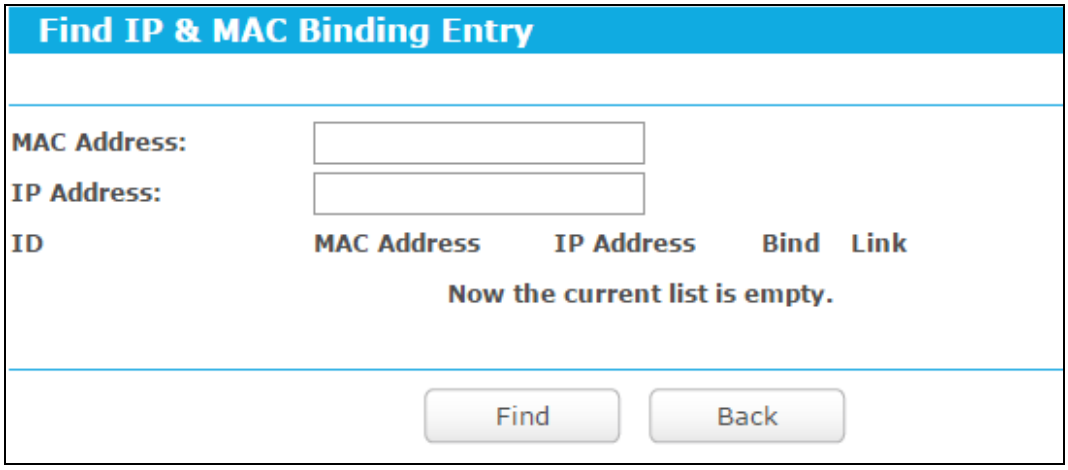
1. Click the **Add New…** button.
2. Enter the MAC Address and IP Address.
3. Select the Bind checkbox.
4. Click the **Save** button to save it.

To modify or delete an existing entry:

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

To find an existing entry:

1. Click the **Find** button.
2. Enter the MAC Address or IP Address.
3. Enter the **Find** button in the next page.

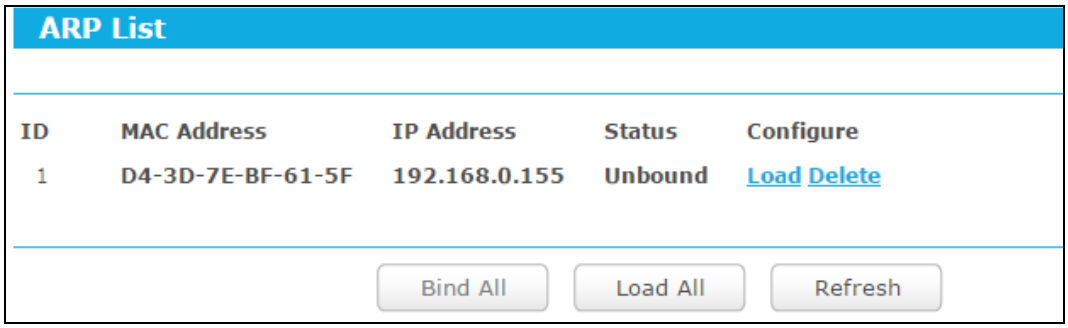


Click the **Enable All** button to make all entries enabled.

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

4.12.2 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.



- **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 -** Enabled or Disabled of the MAC address and IP address binding.
- **Configure -** Load or delete 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:

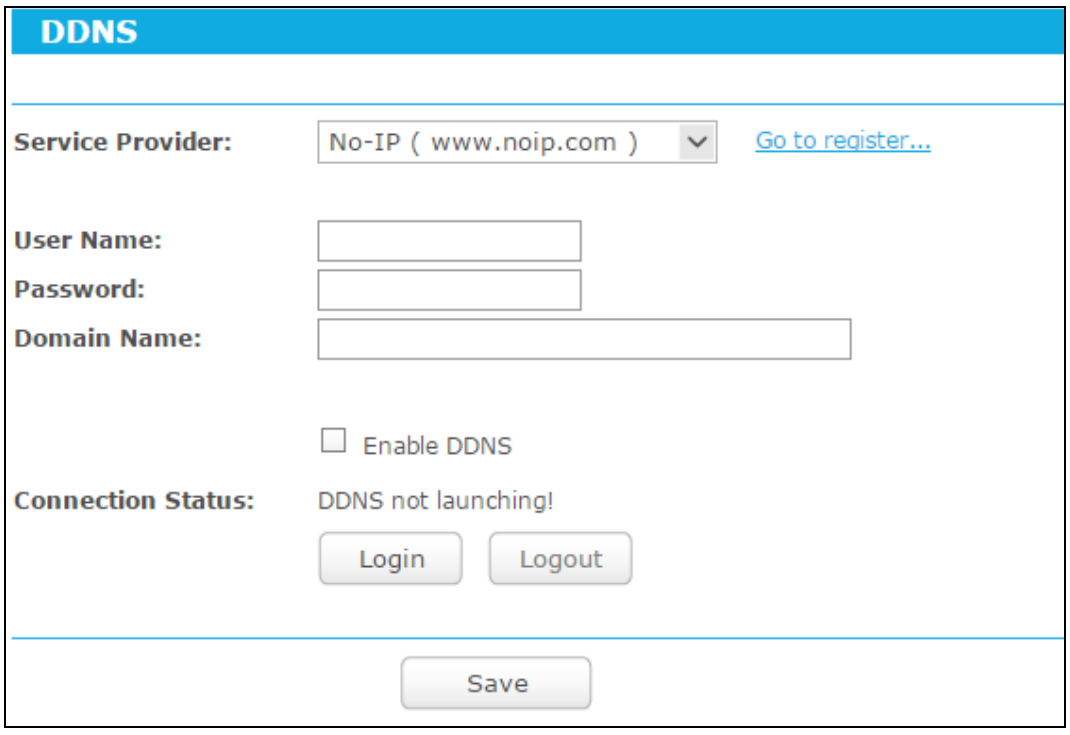
An item could not be loaded to the IP & MAC Binding list if the IP address of the item has been loaded before. Error warning will prompt as well. Likewise, "Load All" only loads the items without interference to the IP & MAC Binding list.

4.13 Dynamic DNS

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.noip.com, www.comexe.cn, or www.dyn.com. The Dynamic DNS client service provider will give you a password or key.

4.13.1 No-IP DDNS

If the dynamic DNS **Service Provider** you select is www.noip.com, the page will appear as shown below.



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.

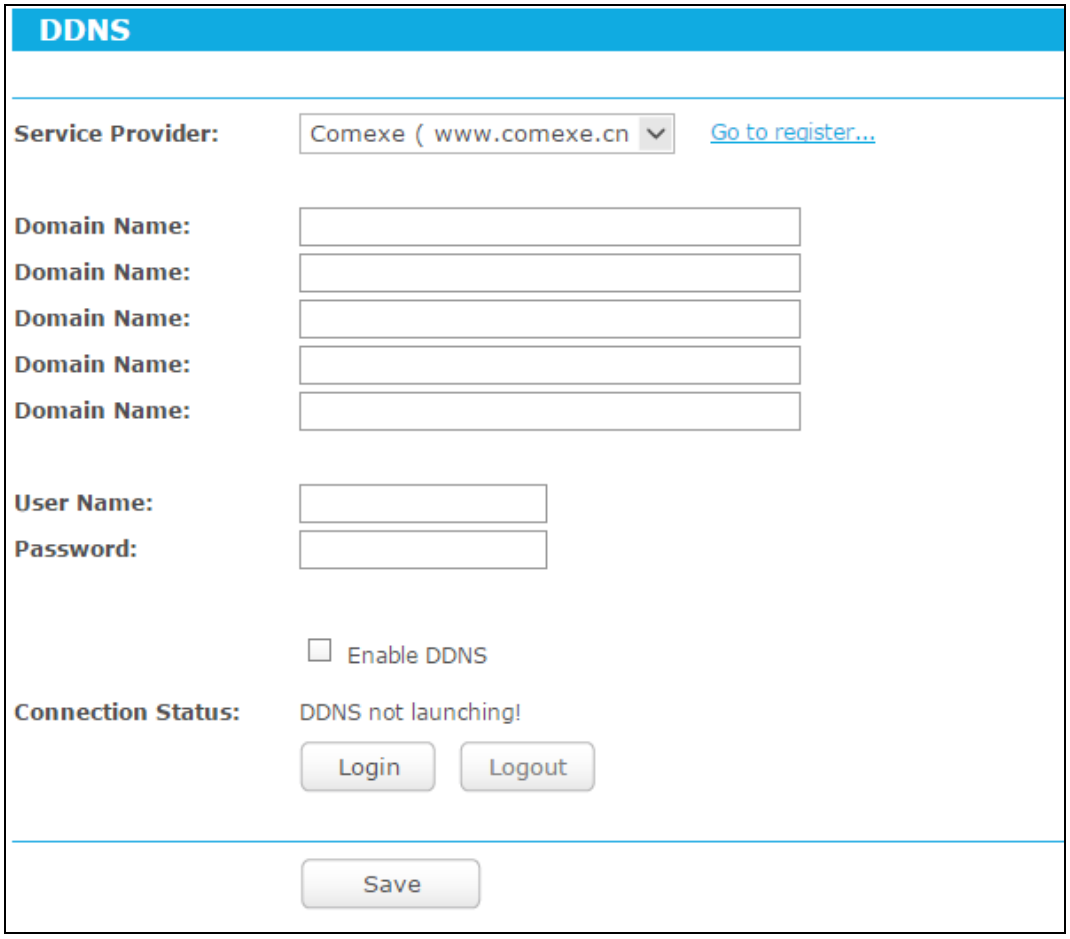
Click **Logout** to log out the DDNS service.

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.

4.13.2 Comexe.cn DDNS

If the dynamic DNS **Service Provider** you select is www.comexe.cn, the page will appear as shown below.



To set up for DDNS, follow these instructions:

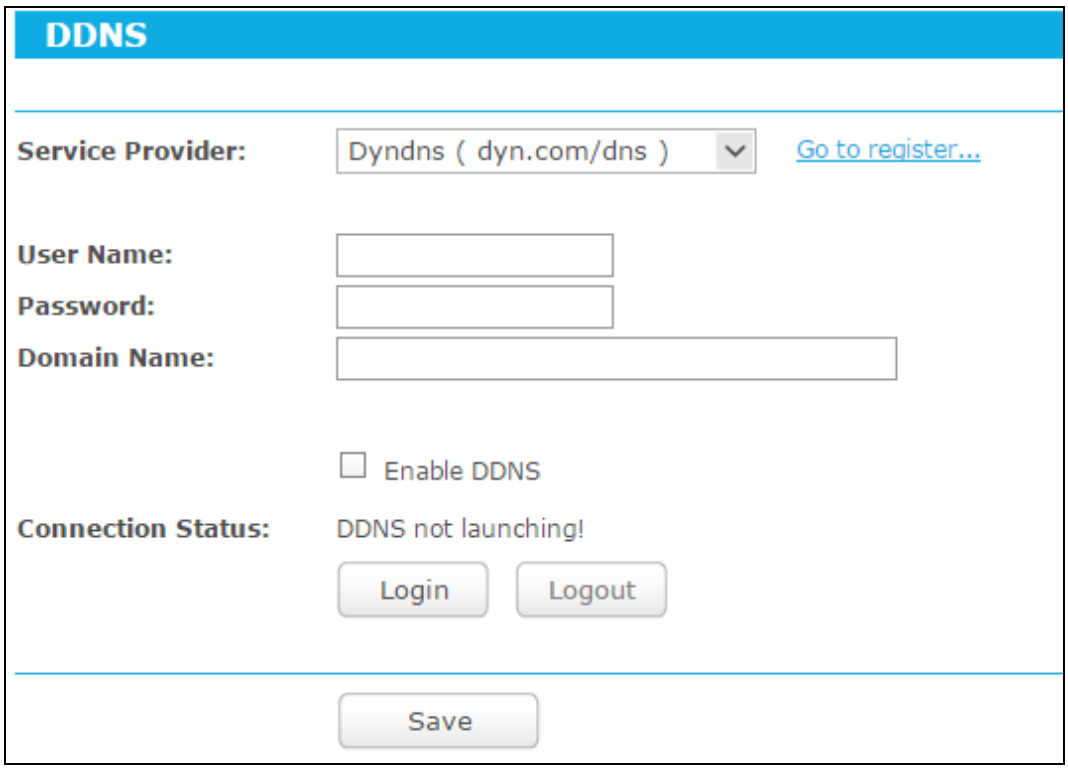
1. Type the **Domain Name** received from your dynamic DNS service provider.
2. Type the **User Name** for your DDNS account.
3. Type the **Password** for your DDNS account.
4. Click the **Login** button to log in to the DDNS service.

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

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

4.13.3 Dyndns DDNS

If the dynamic DNS **Service Provider** you select is www.dyndns.com, the page will appear as shown below.



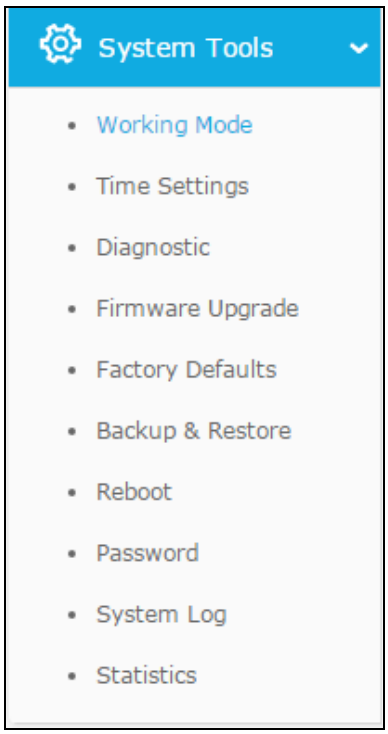
To set up for DDNS, follow these instructions:

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.

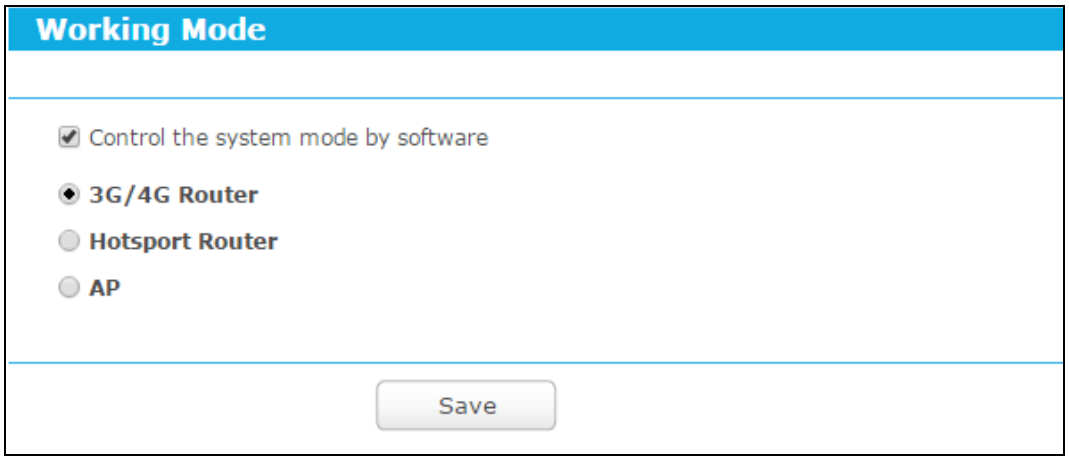
4.14 System Tools



There are nine submenus under the System Tools menu: **SNMP**, **Time Settings**, **Diagnostic**, **Firmware Upgrade**, **Factory Defaults**, **Backup and 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.

4.14.1 Working Mode

Choose menu "**System Tools** → **Working Mode**", check **Control the system mode by software** and then you can see the following screen.



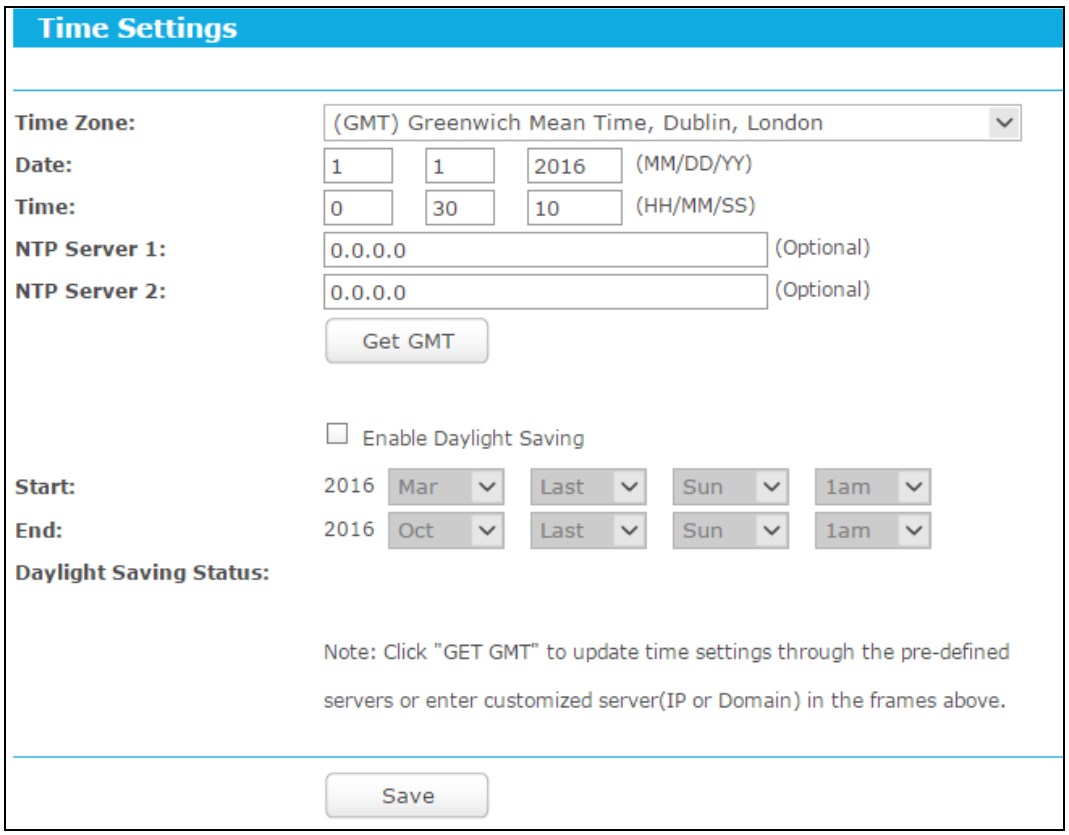
- **3G/4G Router -** This mode stands for Wireless Router Mode. It functions as a standard wireless router and you can also plug in a 3G/4G USB modem if you need.

- **Hotspot Router -** It functions as a hotspot router.
- **AP -** This mode stands for Access Point Mode, Repeater Mode and Client Mode. When selected, you have to go to the **Quick Setup** to specify the mode you need.

  Note: If **Control the system mode by software** is checked, the operation mode switch of the router will be disabled.

4.14.2 Time Settings

You can set time manually or get GMT from the Internet for the router on this page:



- **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.

To set time manually, follow the steps below:

1. Select your local time zone.
2. Enter the **Date** in Month/Day/Year format.
3. Enter the **Time** in Hour/Minute/Second format.
4. Click **Save**.

For automatic time synchronization:

1. Enter the address of the **NTP Server 1** or **NTP Server 2**.
2. Click the **Get GMT** button to get GMT time from Internet if you have connected to Internet.

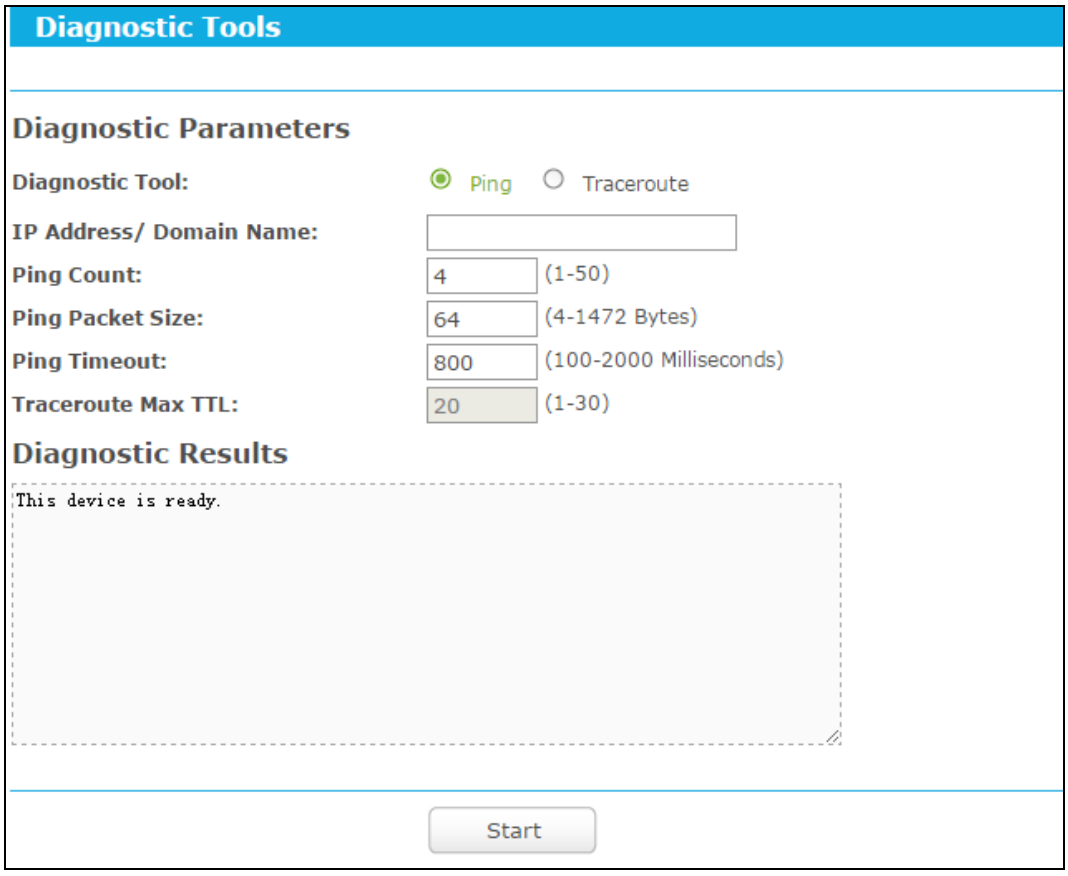
Note:

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

- The time will be lost if the router is turned off.
- The router will obtain GMT automatically from Internet if it has already connected to Internet.

4.14.3 Diagnostic

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



- **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

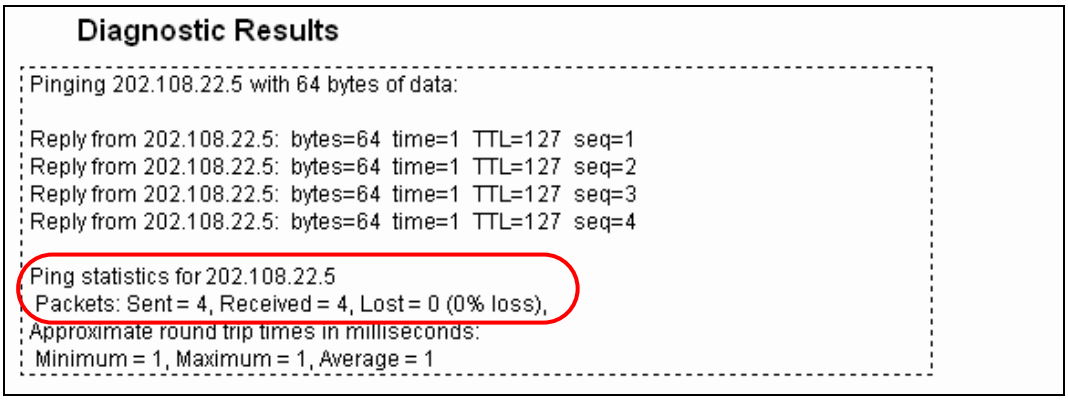
specifying can be resolved by using Domain Name System (DNS) queries.

- **IP Address/Domain Name -** Type the destination IP address (such as 202.108.22.5) or Domain name (such as www.baidu.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.

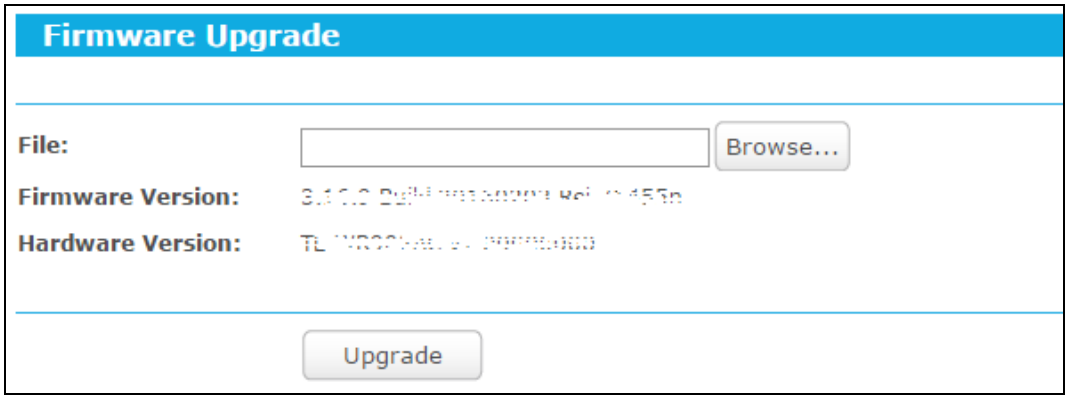


Note:

Only one user can use this tool at one time. "Ping Count", "Ping Packet Size" and "Ping Timeout" are Ping Parameters. "Traceroute Max TTL" is Traceroute Parameter.

4.14.4 Firmware Upgrade

The page allows you to upgrade the latest version firmware to keep your router up-to-date.



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

Note:

1. When you upgrade the router's firmware, you will lose current configuration settings, so make sure you backup the router's settings before you upgrade its firmware.
2. Make sure that your computer is connected to the Internet through the cable when you upgrade the firmware. To upgrade through wireless connection is not allowed.
3. Set your IP address as static IP before upgrading.

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

1. Download the latest firmware upgrade file from our website http://www.tp-link.com.
2. Enter or select the path name where you save the downloaded file on the computer into the **File** blank.
3. Click the **Upgrade** button.

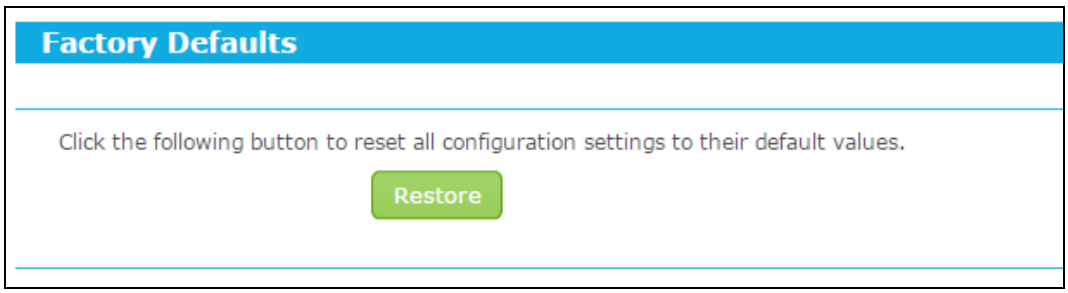
- **Firmware Version -** Displays the current firmware version.
- **Hardware Version -** Displays the current hardware version. The hardware version of the upgrade file must accord with the current hardware version.

Note:

The firmware version must correspond to the hardware. The upgrade process takes a few minutes and the Router will restart automatically when the upgrade is completed. It is important to keep power on during the entire process. Loss of power during the upgrade could damage the Router.

4.14.5 Factory Defaults

This page allows you to restore the factory default settings for the router.



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

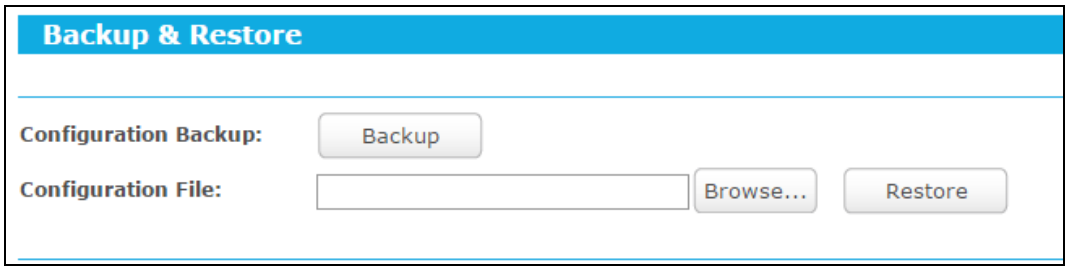
- The default User Name: admin
- The default Password: admin
- The default access: tplinkwifi.net

Note:

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

4.14.6 Backup & Restore

This page allows you to save current configuration of router as backup or restore the configuration file you saved before.



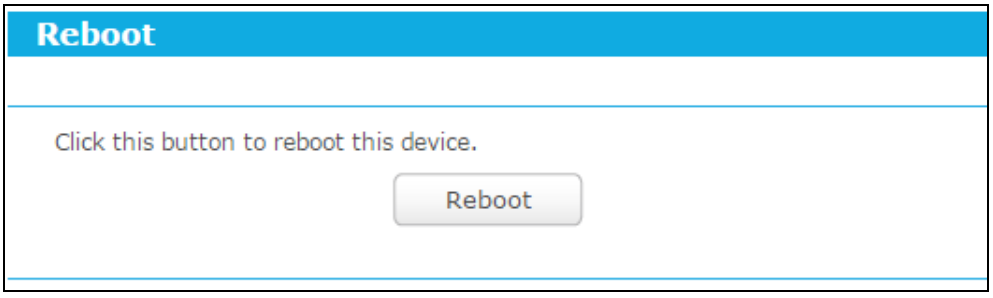
- Click the **Backup** button to save all configuration settings as a backup file in your local computer.
- To restore the router's configuration, follow these instructions:
  - Click the **Browse** button to select the backup file which you want to restore.
  - Click the **Restore** button.

Note:

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

4.14.7 Reboot

This page allows you to reboot the router.



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

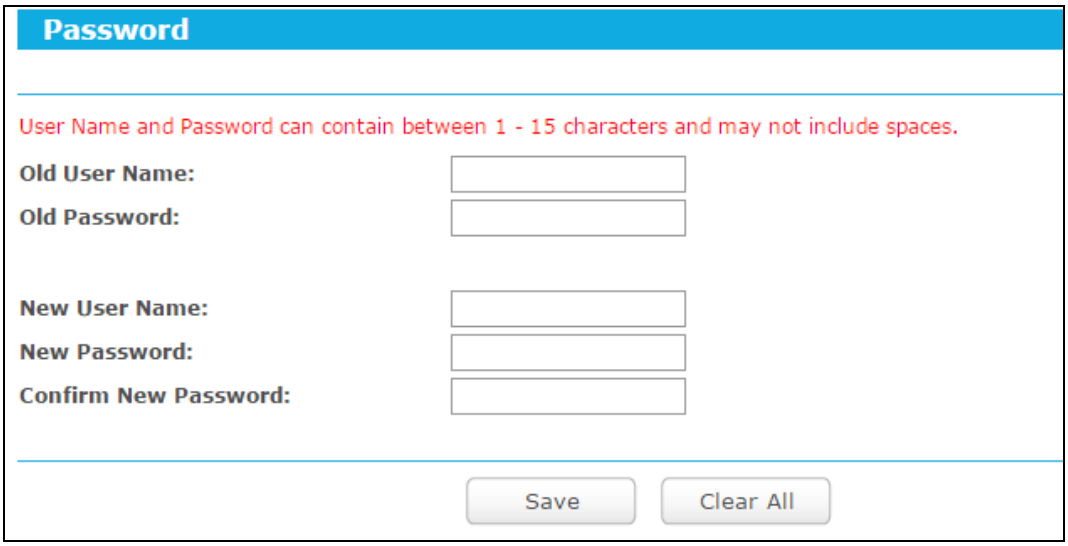
Some settings of the router will take effect only after rebooting, which include:

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

- Web Service Port of the router.
- Upgrade the firmware of the router (system will reboot automatically).
- Restore the router's settings to factory default (system will reboot automatically).

4.14.8 Password

This page allows you to change the factory default user name and password of the router.



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

Note:

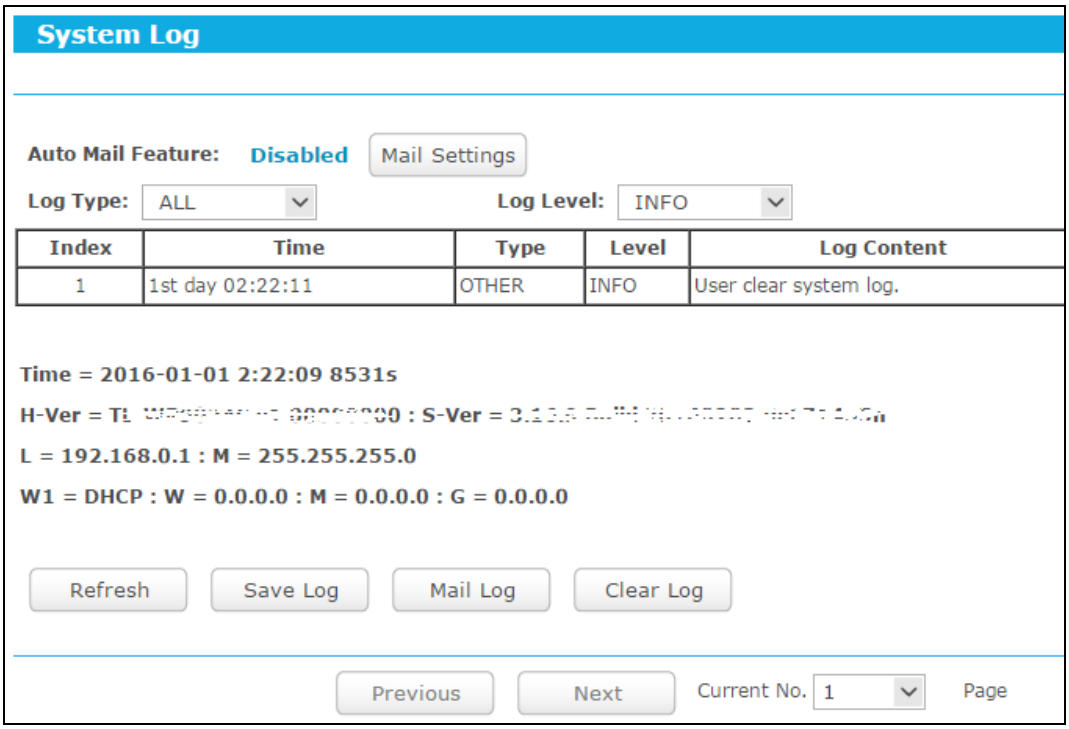
The new user name and password must not exceed 14 characters in length and must not include any spaces. Enter the new Password twice to confirm it.

Click the **Save** button when finished.

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

4.14.9 System Log

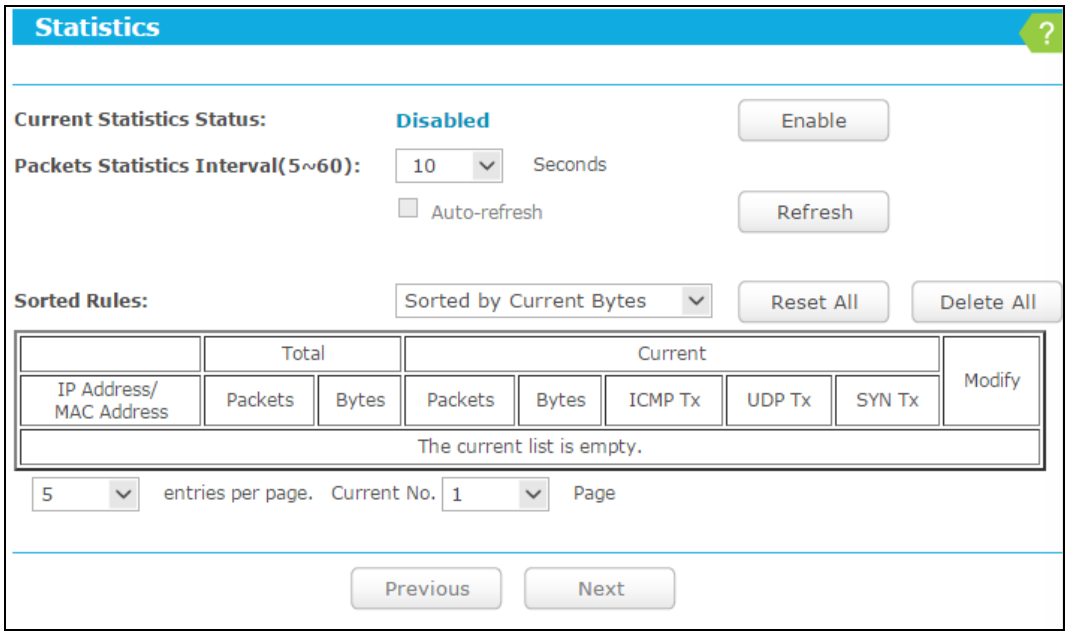
This page allows you to query the logs of the router.



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

4.14.10 Statistics

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



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

Statistics Table:

IP Address		The IP Address displayed with statistics
Total	**Packets**	The total amount of packets received and transmitted by the router.
	Bytes	The total amount of bytes received and transmitted by the router.
Current	**Packets**	The total amount of packets received and transmitted in the last **Packets Statistic interval** seconds.
	Bytes	The total amount of bytes received and transmitted in the last **Packets Statistic interval** seconds.
	ICMP Tx	The total amount of the ICMP packets transmitted to WAN in the last **Packets Statistic interval** seconds.
	UDP Tx	The total amount of the UDP packets transmitted to WAN in the last **Packets Statistic interval** seconds.
	TCP SYN Tx	The total amount of the TCP SYN packets transmitted to WAN in the last **Packets Statistic interval** seconds.

Click the **Save** button to save the **Packets Statistic interval** value.

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

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

4.15 Logout

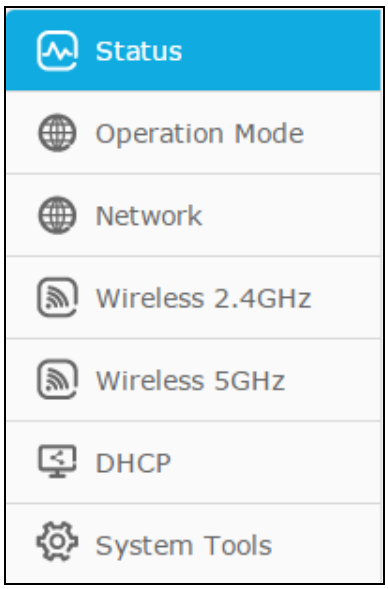
Click the **Logout** tab at the bottom of the main menu, and then the web-page will be logged out and return to the login window.

Chapter 5. Configuration for Access Point Mode

This chapter will show each Web page's key functions and the configuration way for Access Point Mode of TL-WR902AC.

5.1 Login

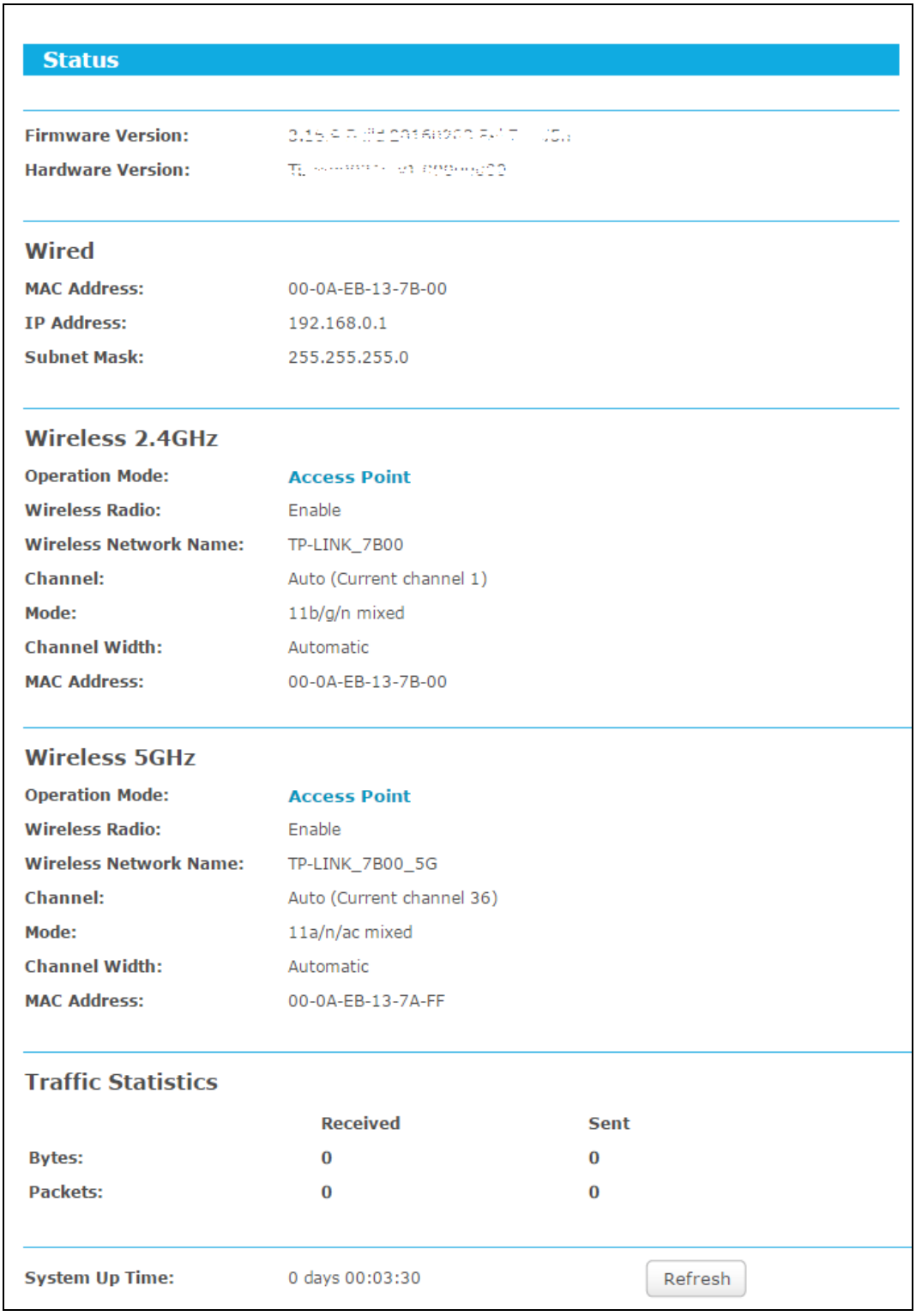
After your successful login, you can configure and manage the device. There are main menus on the left of the web-based utility. Submenus will be available after you click one of the main menus. On the right, there are the corresponding explanations and instructions.



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 on Access Point Mode. All information is read-only.



- **Firmware Version -** The version information of the Router's firmware.
- **Hardware Version -** The version information of the Router's hardware.
- **Wired -** This field displays the current settings or information for the LAN, you can configure them in the **Network > LAN** page.
  - **MAC address -** The physical address of the Router, as seen from the LAN.

- **IP address -** The LAN IP address of the Router.
- **Subnet Mask -** The subnet mask associated with LAN IP address.

➢ **Wireless -** This field displays basic information or status for wireless function, you can configure them in the **Wireless > Wireless Settings** page.

- **Operation Mode -** The current wireless working mode in use.
- **Wireless Network Name -** The SSID of the AP.
- **Channel -** The current wireless channel in use.
- **Mode -** The current wireless mode which the Router works on.
- **Channel Width -** The current wireless channel width in use.
- **MAC Address -** The physical address of the Router, as seen from the WLAN.

➢ **Traffic Statistics -** The Router's traffic statistics.

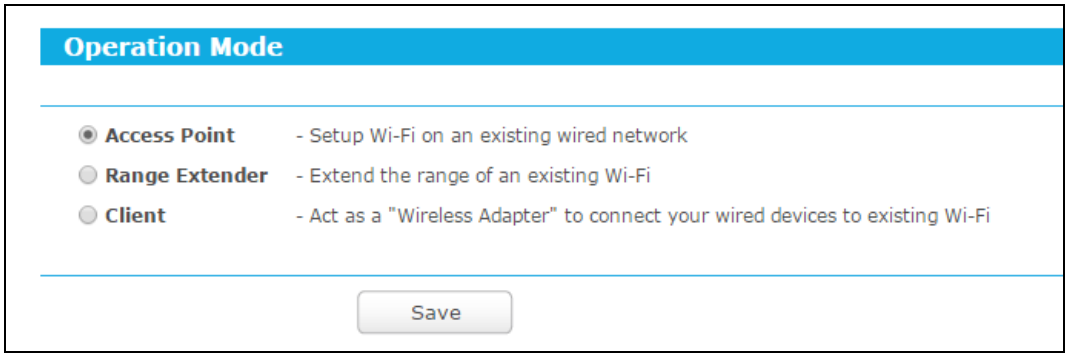
- **Received (Bytes) -** Traffic that counted in bytes has been received out from the WAN port.
- **Received (Packets) -** Traffic that counted in packets has been received out from the WAN port.
- **Sent (Bytes) -** Traffic that counted in bytes has been sent out from the WAN port.
- **Sent (Packets) -** Traffic that counted in packets has been sent out from the WAN port.

➢ **System Up Time -** The length of the time since the Router was last powered on or reset.

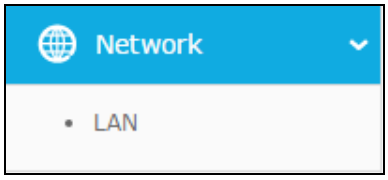
Click the **Refresh** button to get the latest status and settings of the Router.

5.3 Operation Mode

The Router supports five operation mode types: **Wireless Router**, **Access Point, Range Extender, Client** and **Hotspot**. Please select one you need. Click **Save** to save your choice, which is shown as below.



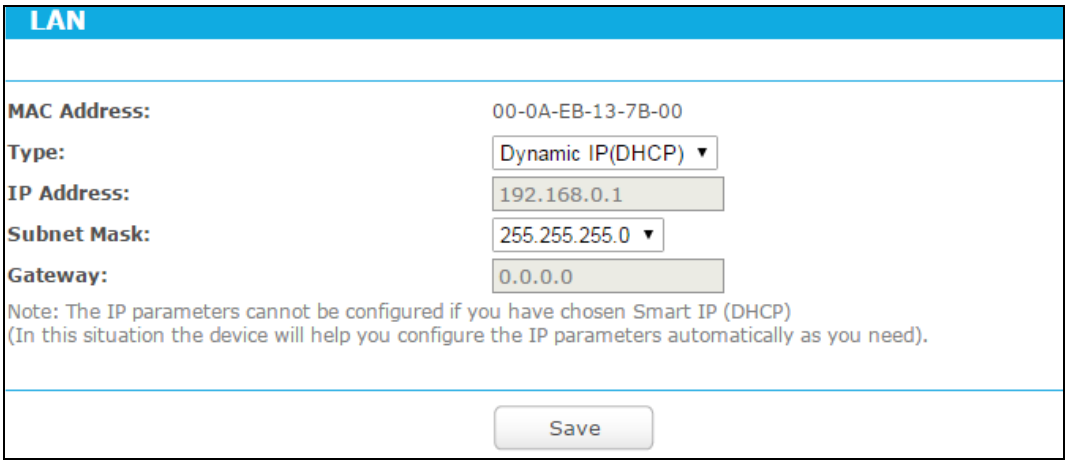
5.4 Network



There is only one submenu under the Network menu: **LAN**.

5.4.1 LAN

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

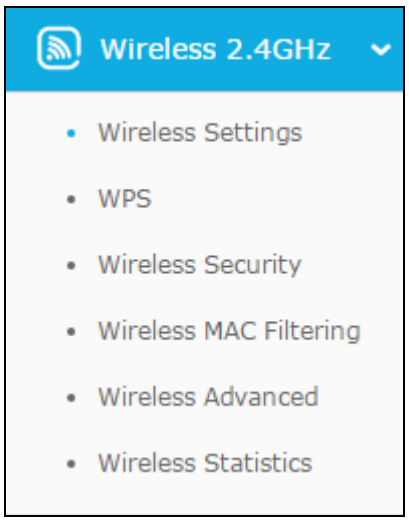


- **MAC Address** - The physical address of the LAN ports, as seen from the LAN. The value cannot be changed.
- **Type** - Choosing Smart IP (DHCP) to get IP address from DHCP server, or choosing static IP to config IP address manually.
- **IP Address** - Enter the IP address of your system in dotted-decimal notation (factory default - 192.168.0.254).
- **Subnet Mask** - An address code that determines the size of the network. Normally 255.255.255.0 is used as the subnet mask.

☞ **Note:**

1. If you change the IP Address of LAN, you must use the new IP Address to login to the Router.
2. If the new LAN IP Address you set is not in the same subnet with the previous one, the IP Address pool in the DHCP server will be configured automatically，while the Virtual Server and DMZ Host will not take effect until they are re-configured.
3. When you choose the **Smart IP(DHCP)** mode, the DHCP Server function will be disabled.

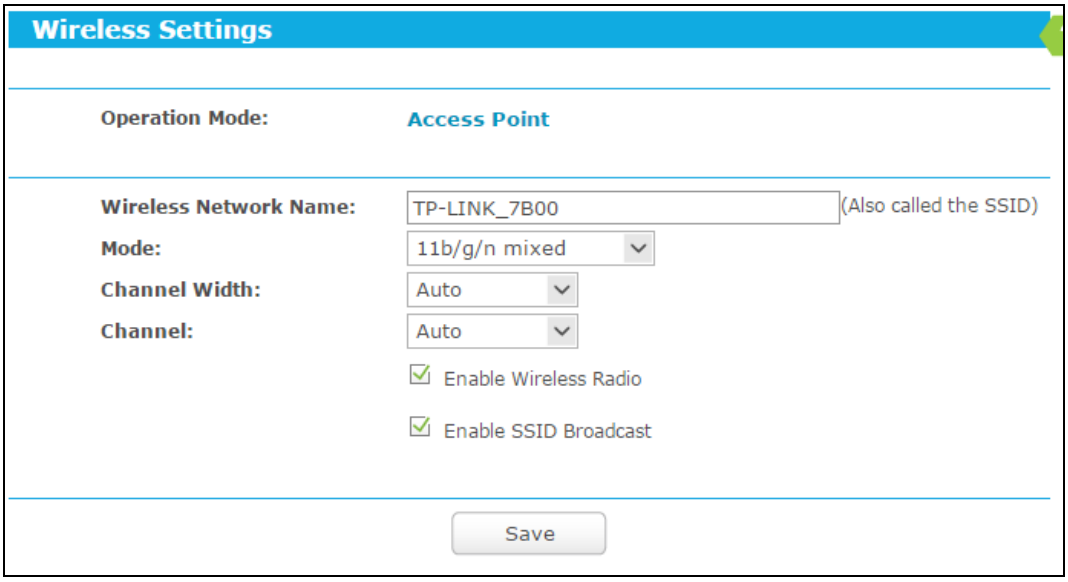
5.5 Wireless 2.4GHz/5GHz



There are six submenus under the Wireless menu: **Wireless Settings**, **WPS, Wireless Security, Wireless MAC Filtering, Wireless Advanced, and Wireless Statistics**. Click any of them, and you will be able to configure the corresponding function.

5.5.1 Wireless Settings

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



- **Wireless Network Name -** Enter a string of up to 32 characters. The same name of SSID (Service Set Identification) must be assigned to all wireless devices in your network. The default SSID is set to be TP-LINK_XXXX (XXXX indicates the last unique four numbers of each Router's MAC address). But it is recommended strongly that you change your networks name (SSID) to a different value. This value is case-sensitive. For example, *TEST* is NOT the same as *test*.
- **Mode -** Select the desired mode. The default setting is 11bgn mixed.

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

It is strongly recommended that you set the Mode to 11bgn mixed, and all of 802.11b/g/n wireless stations can connect to the Router.

- **Channel -** This field determines which operating frequency will be used. The default channel is set to **Auto**. It is not necessary to change the wireless channel unless you notice interference problems with another nearby access point.
- **Channel Width -** Select any channel width from the pull-down list. The default setting is automatic, which can automatically adjust the channel width for your clients.
- **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.

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.
   - 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.

5.5.2 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. Select menu "**WPS**", you will see the next screen shown below.

- **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.
- **Disable PIN of this Device -** WPS external registrar of entering the device's PIN can be disabled or enabled manually. If the device receives multiple failed attempts to authenticate an external Registrar, this function will be disabled automatically.
- **Add Device -** You can add 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.

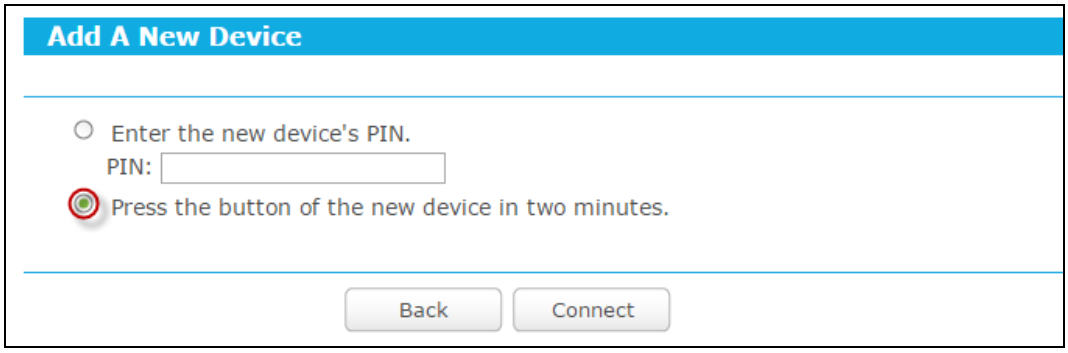
For the configuration of the new device, here takes the Wireless Adapter of our company for example.

II. 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: Keep the WPS Status as **Enabled** and click the **Add Device** button, then the following screen will appear.



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

Step 3: For the configuration of the wireless adapter, please choose "**Push the button on my access point or wireless router**" in the configuration utility of the WPS as below, and click **Connect**.

The WPS Configuration Screen of Wireless Adapter

Step 2: Wait for a while until the next screen appears. Click **OK** to complete the WPS configuration.

The WPS Configuration Screen of Wireless Adapter

Method Two: Enter the PIN into my AP

Step 1: For the configuration of the wireless adapter, please choose "**Enter the PIN of this device into my access point or wireless router**" in the configuration utility of the WPS as below, and click **Connect**.

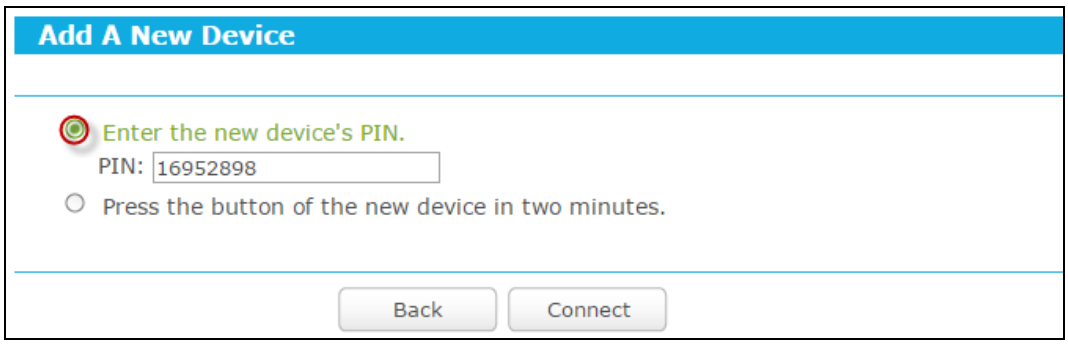
The WPS Configuration Screen of Wireless Adapter

Note:

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

Step 2: Keep the WPS Status as **Enabled** and click the **Add Device** button.

Step 3: Choose "**Enter the new device's PIN**" and enter the PIN code (take 16952898 for example) of the wireless adapter in the field after **PIN** as shown in the figure below. Then click **Connect**.



Method Three: Enter the PIN from my AP.

Step 1: Get the Current PIN code of the AP (each AP has its unique PIN code. Here take the PIN code 12345670 of this AP for example).

Step 2: For the configuration of the wireless adapter, please choose "**Enter the PIN of my access point or wireless router**" 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 **Connect**.

The WPS Configuration Screen of Wireless Adapter

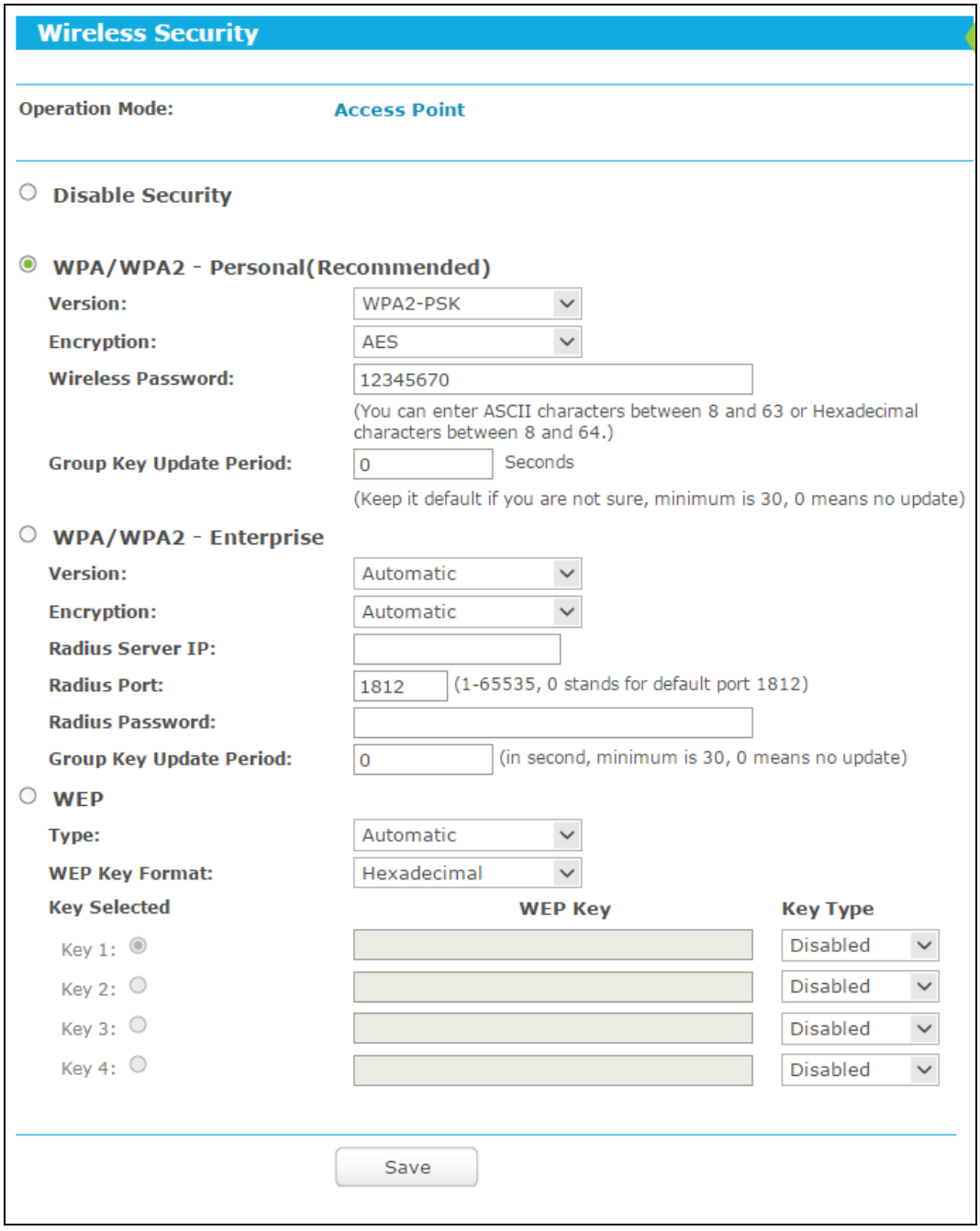
Note:

The default PIN code of the AP can be found in its label or the WPS configuration screen.

5.5.3 Wireless Security

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

There are three wireless security modes supported by the Router: WPA/WPA2-Personal, WPA/WPA2-Enterprise and WEP (Wired Equivalent Privacy).

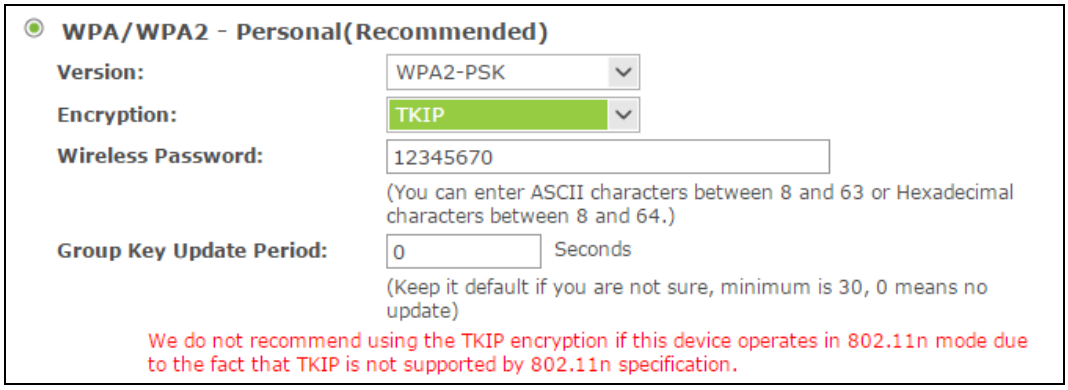


- **Disable Security -** The wireless security function can be enabled or disabled. If disabled, the wireless stations will be able to connect the Router without encryption. But it's strongly recommended to choose one of the following modes to enable security.

- **WPA-PSK/WPA2-Personal -** 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** radio button and choose TKIP encryption, you will find a notice in red as shown below.



- **WPA /WPA2-Enterprise -** It's based on Radius Server.
  - **Version -** you can choose the version of the WPA security from 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 **Automatic**, **TKIP** or **AES.**
  - **Radius Server IP -** Enter the IP address of the Radius server.
  - **Radius Port -** Enter the port that Radius server 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.
  - **Type -** you can choose the type for the WEP security on the pull-down list. The default setting is **Automatic**, which can select **Shared Key** or **Open System** authentication type automatically based on the wireless station's capability and request.

- **WEP Key Format - Hexadecimal** and **ASCII** formats are provided here. **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 (Password) -** 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.

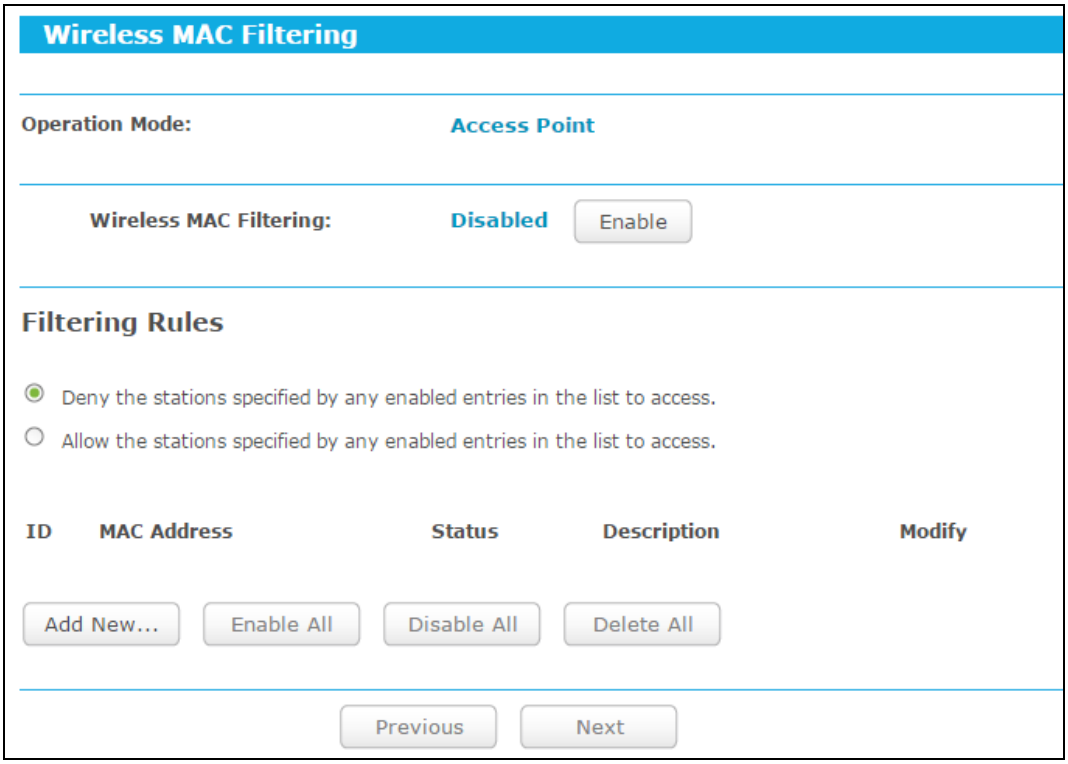
  152-bit - You can enter 32 hexadecimal digits (any combination of 0-9, a-f, A-F, zero key is not promoted) or 16 ASCII characters.

☞ **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.

5.5.4 Wireless MAC Filtering

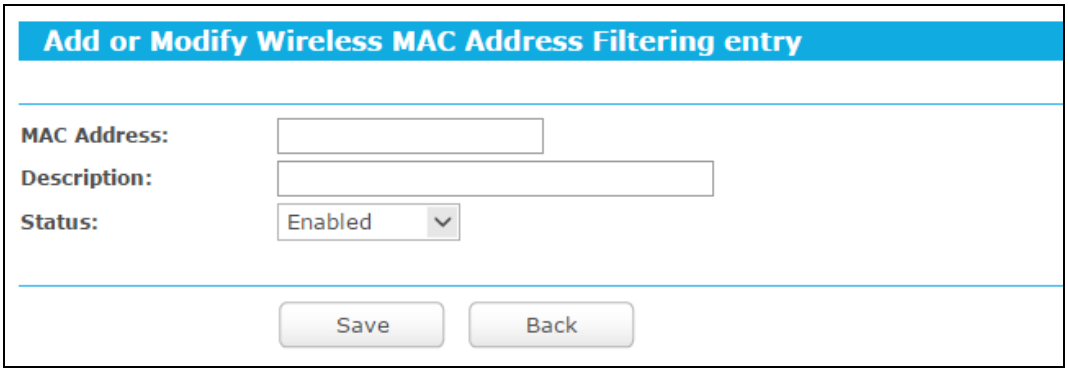
Choose menu "**Wireless → Wireless MAC Filtering**", and then you can control the wireless access by configuring the **Wireless MAC Filtering** function, as shown below.



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

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

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:



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

1. Enter the appropriate MAC Address into the **MAC Address** field. The format of the MAC Address is XX-XX-XX-XX-XX-XX (X is any hexadecimal digit). For example: 00-0A-EB-B0-00-0B.
2. Give a simple description for 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 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.

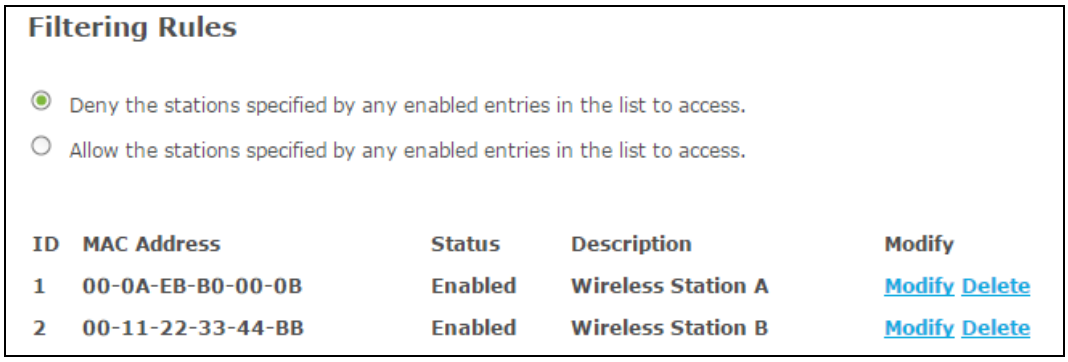
Click the **Previous** button to return to the previous page.

For example: If you desire that the wireless station A with MAC address 00-0A-EB-B0-00-0B and the wireless station B with MAC address 00-0A-EB-00-07-5F 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:

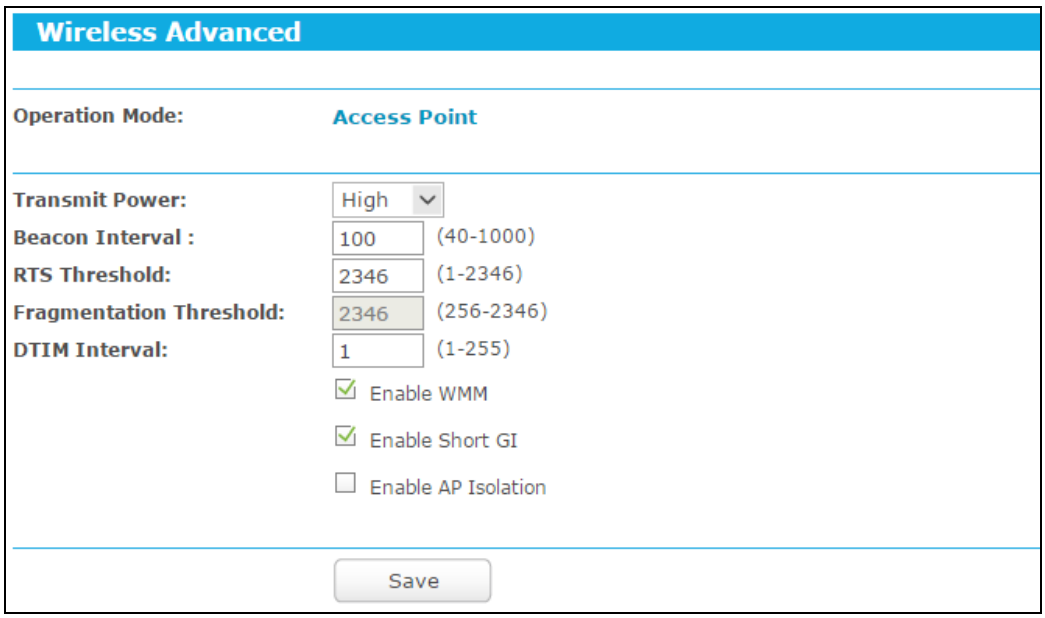
1. Click the **Enable** button to enable this function.
2. Select the radio button "Allow the stations specified by any enabled entries in the list to access" for **Filtering Rules**.
3. Delete all or disable all entries if there are any entries already.
4. Click the **Add New...** button.
   - Enter the MAC address 00-0A-EB-B0-00-0B/00-0A-EB-00-07-5F in the **MAC Address** field.
   - Enter wireless station A/B in the **Description** field.
   - Select **Enabled** in the **Status** pull-down list.
   - Click the **Save** button.
   - Click the **Back** button.

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



5.5.5 Wireless Advanced

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



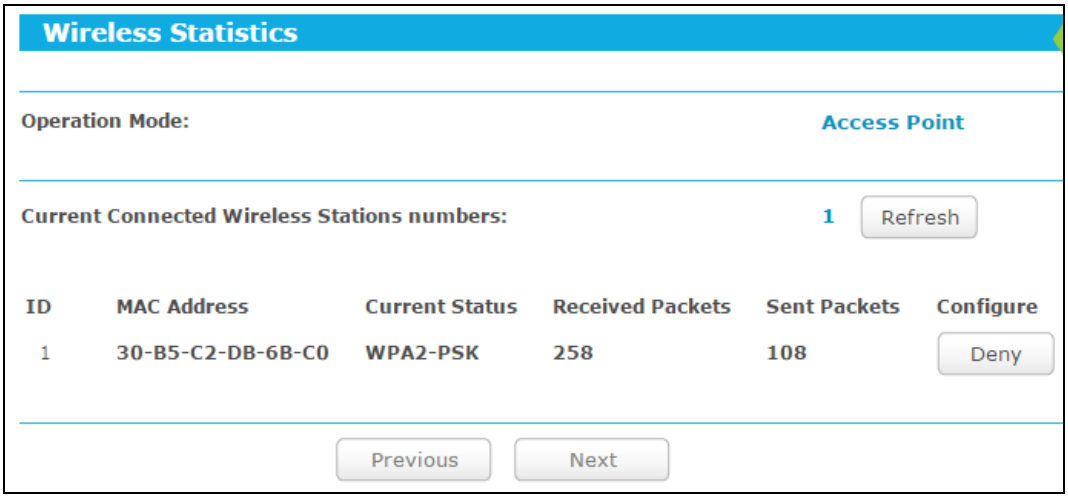
- **Transmit Power -** Here you can specify the transmit power of Router. You can select High, Middle or Low which you would like. High is the default setting and is recommended.
- **Beacon Interval -** Enter a value between 20-1000 milliseconds for Beacon Interval here. The beacons are the packets sent 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 because of 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.
- **Enable AP Isolation -** This function isolate all connected wireless stations so that wireless stations cannot access each other through WLAN. This function will be disabled if WDS/Bridge is enabled.

☞ **Note:**

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

5.5.6 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.



- **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.
- **Configure -** The button is used for loading the item to the **Wireless MAC Filtering** list.

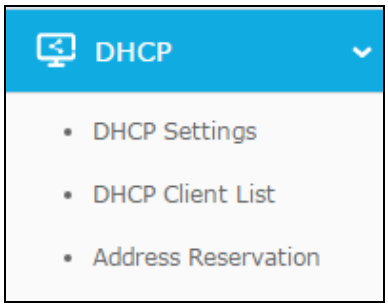
You cannot change any of the values on this page. To update this page and to show the current connected wireless stations, click on the **Refresh** button.

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

Note:

This page will be refreshed automatically every 5 seconds.

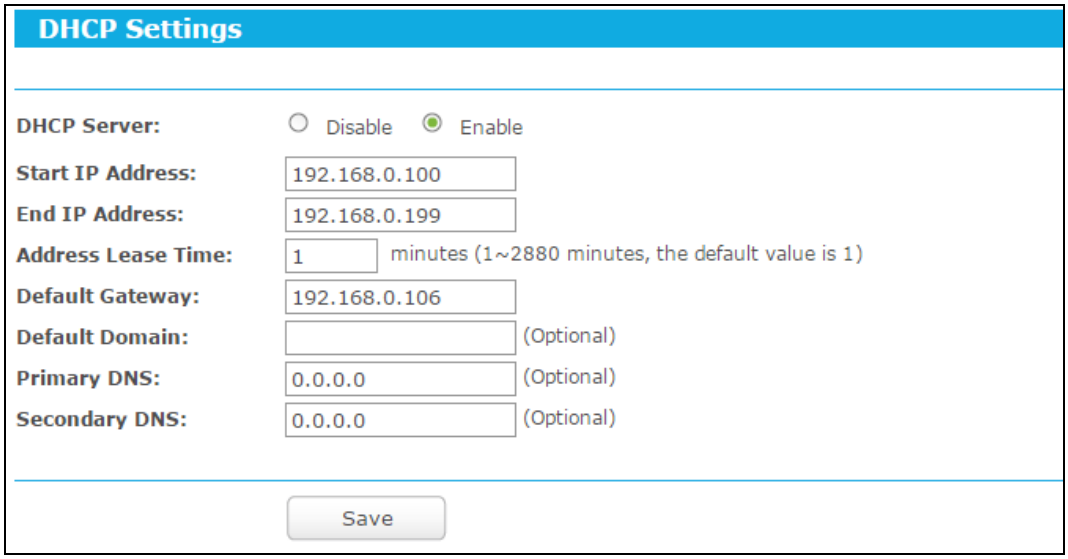
5.6 DHCP



There are three submenus under the DHCP menu, **DHCP Settings**, **DHCP Client List** and **Address Reservation**. Click any of them, and you will be able to configure the corresponding function.

5.6.1 DHCP Settings

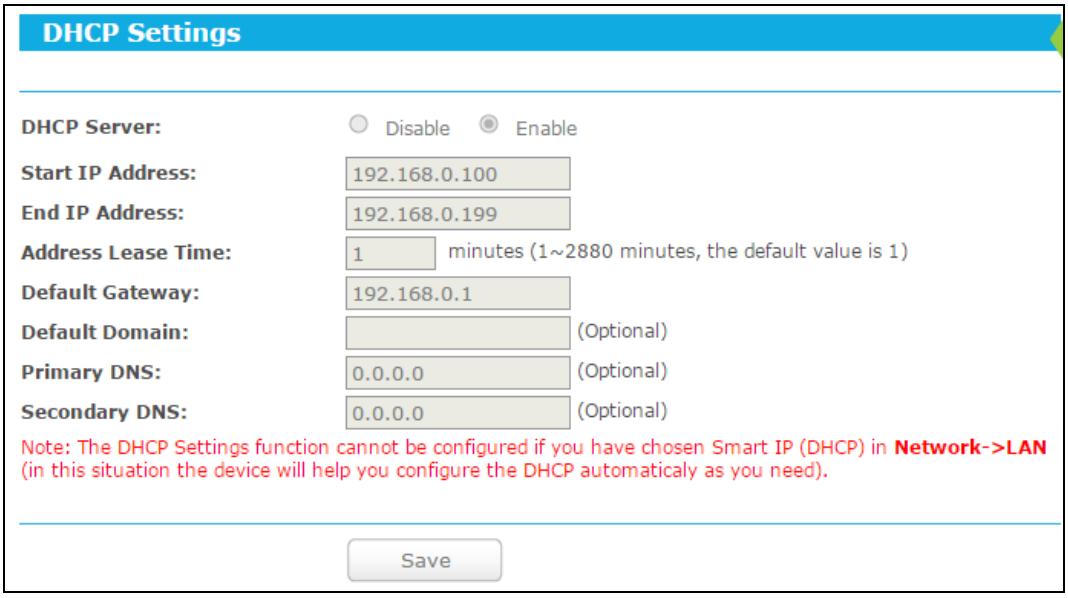
Choose menu "**DHCP → DHCP Settings**", and then you can configure the DHCP Server on the page as shown below. The Router is set up by default as a DHCP (Dynamic Host Configuration Protocol) server, which provides the TCP/IP configuration for all the PC(s) that are connected to the Router in the LAN.



- **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) **-** It is suggested to input the IP address of the LAN port of the Router. The 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.

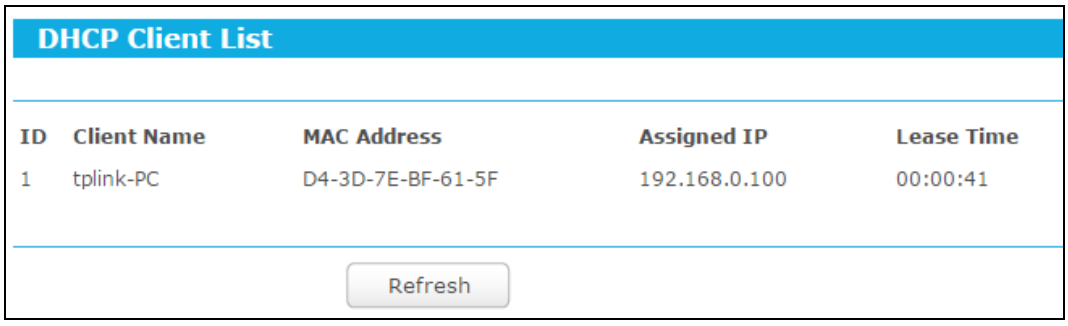
Note:

1. To use the DHCP server function of the Router, you must configure all computers on the LAN as "Obtain an IP Address automatically".
2. When you choose the **Smart IP (DHCP)** mode in **Network → LAN**, the DHCP Server function will be disabled. You will see the page as below.



5.6.2 DHCP Client List

Choose menu "**DHCP → DHCP Clients List**", and then you can view the information about the clients attached to the Router in the screen as shown below.

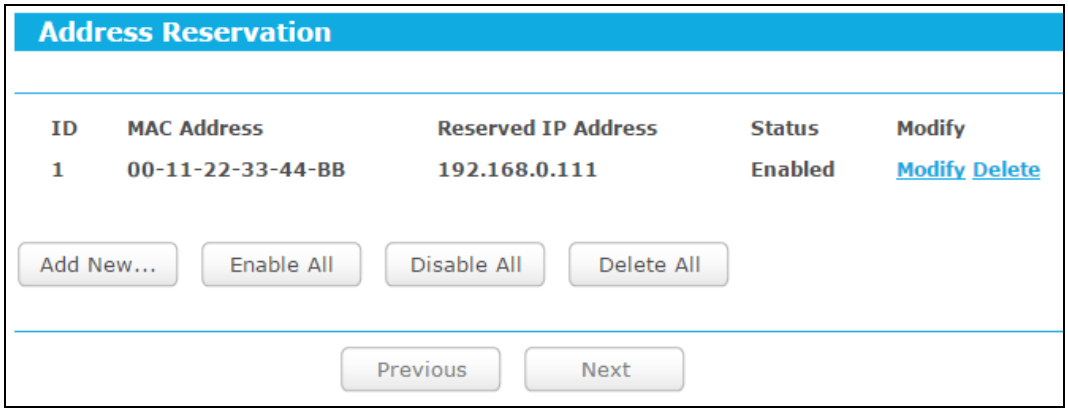


- **Client Name -** The name of the DHCP client.
- **MAC Address -** The MAC address of the DHCP client.
- **Assigned IP -** The IP address that the Router has allocated to the DHCP client.
- **Lease Time -** The time of the DHCP client leased. After the dynamic IP address has expired, a new dynamic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

5.6.3 Address Reservation

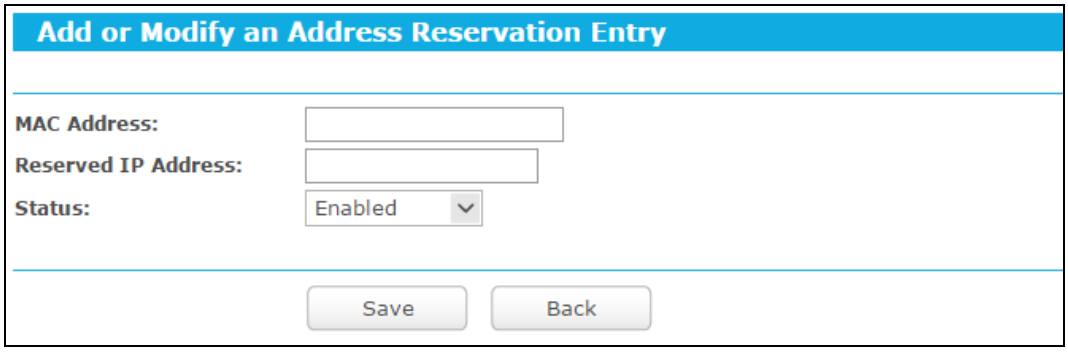
Choose menu "**DHCP → Address Reservation**", and then you can view and add a reserved address for clients via the next screen. When you specify a reserved IP address for a PC on the LAN, that PC will always receive the same IP address each time when it accesses the DHCP server. Reserved IP addresses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



- **MAC Address -** The MAC address of the PC for which you want to reserve an IP address.
- **Reserved IP Address -** The IP address reserved for the PC by the Router.
- **Status -** The status of this entry either **Enabled** or **Disabled**.
- **Modify -** To modify or delete an existing entry.

To Reserve an IP address:

1. Click the **Add New…** button.
2. Enter the MAC address (in XX-XX-XX-XX-XX-XX format.) and IP address (in dotted-decimal notation) of the computer for which you want to reserve an IP address.
3. Click the **Save** button.



To modify or delete an existing entry:

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

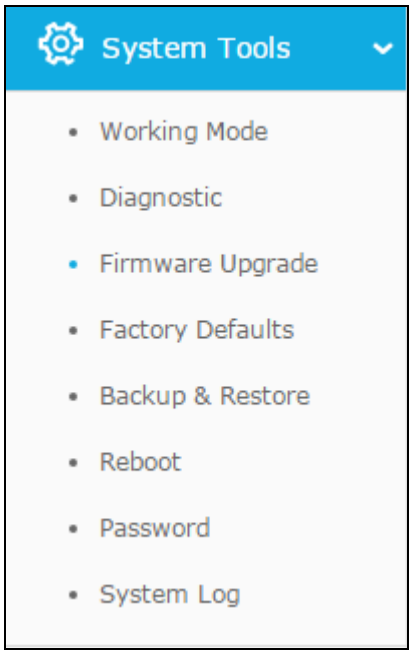
3. Click the **Save** button.

   Click the **Enable/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.

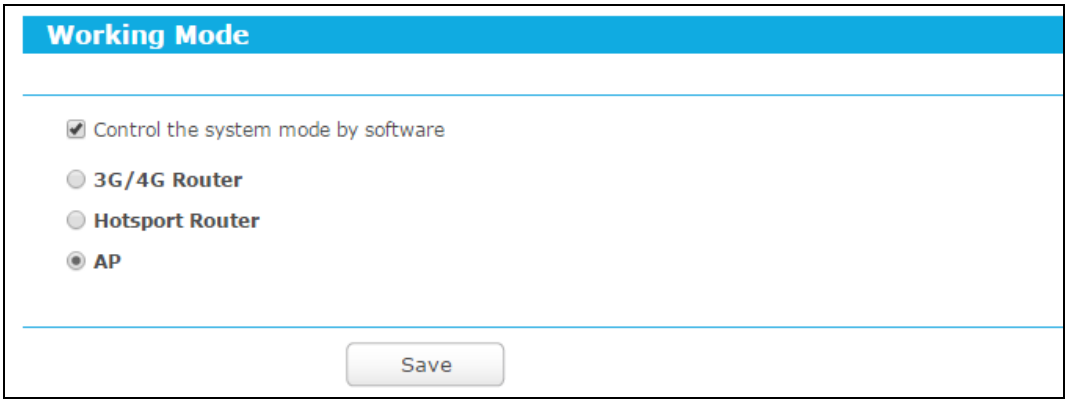
5.7 System Tools



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

5.7.1 Working Mode

Choose menu "**System Tools** → **Working Mode**", check **Control the system mode by software** and then you can see the following screen.

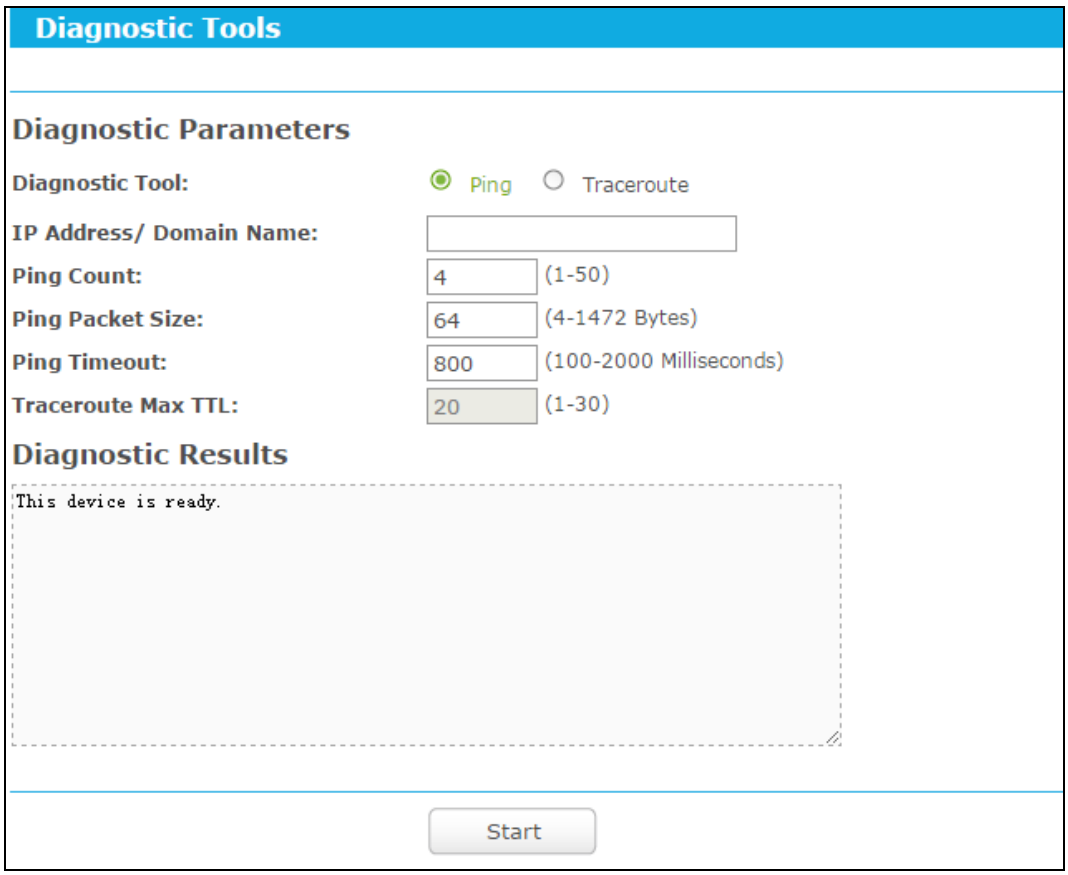


- **3G/4G Router -** This mode stands for Wireless Router Mode. It functions as a standard wireless router and you can also plug in a 3G/4G USB modem if you need.
- **Hotspot Router -** It functions as a hotspot router.
- **AP –** This mode stands for Access Point Mode, Repeater Mode and Client Mode. When selected, you have to go to the **Quick Setup** to specify the mode you need.

  Note: If **Control the system mode by software** is checked, the operation mode switch of the router will be disabled.

5.7.2 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.



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

Note:

You can use ping/traceroute to test both numeric IP address or domain name. If pinging/tracerouting the IP address is successful, but pinging/tracerouting the domain name is not,

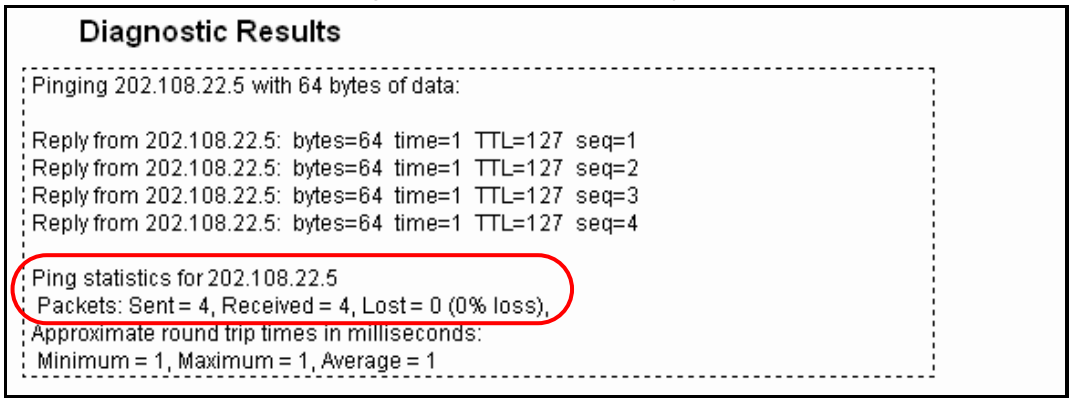
you might have a name resolution problem. In this case, ensure that the domain name you are specifying can be resolved by using Domain Name System (DNS) queries.

- **IP Address/Domain Name -** Type the destination IP address (e.g. 202.108.22.5) or Domain name (e.g. http://www.tp-link.com).
- **Pings Count -** The number of Ping packets for a Ping connection. The default is 4.
- **Ping Packet Size -** The size of Ping packet. The default is 64.
- **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. The default is 800.
- **Traceroute Max TTL -** The max number of hops for a Traceroute connection. 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.

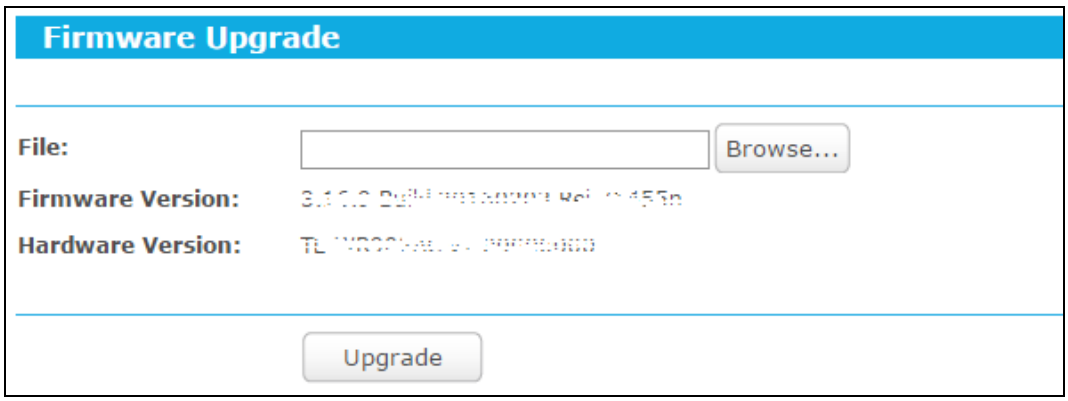


Note:

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.

5.7.3 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.



- **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:

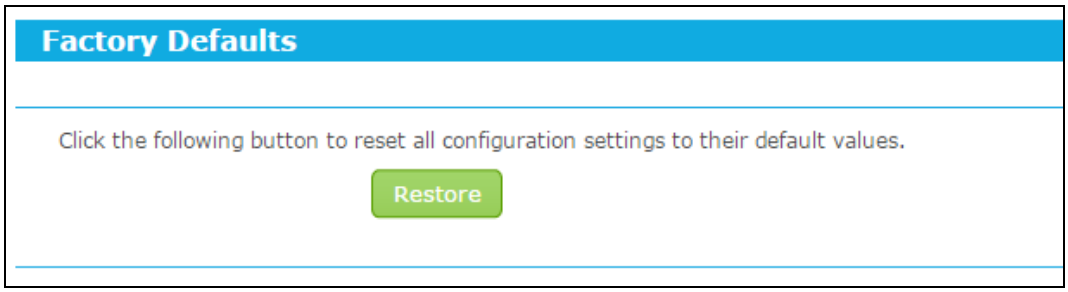
1. Download a more recent firmware upgrade file from the TP-LINK website (http://www.tp-link.com).
2. Type the path and file name of the update file into the **File** field, or click the **Browse** button to locate the update file.
3. Click the **Upgrade** button.

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.

5.7.4 Factory Defaults

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



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

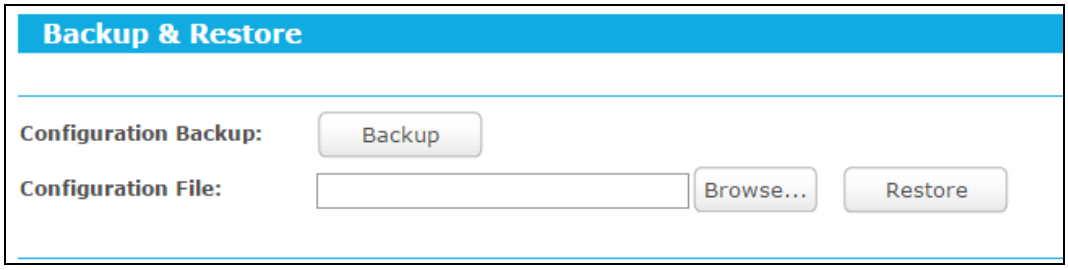
- The default User Name: admin
- The default Password: admin
- The default access: tplinkwifi.net

Note:

All changed settings will be lost when defaults are restored.

5.7.5 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 below.



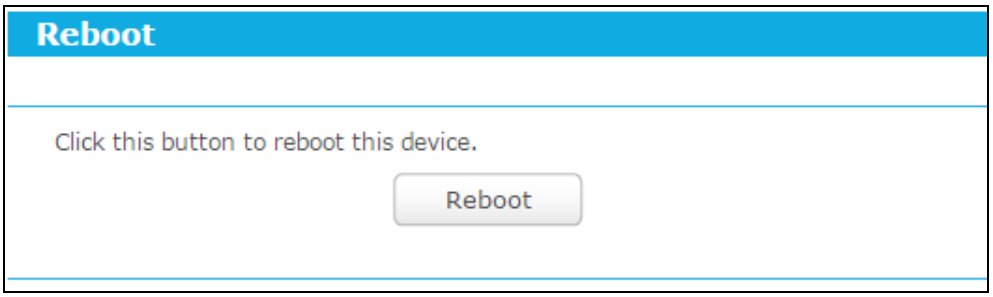
- Click the **Backup** button to save all configuration settings as a backup file in your local computer.
- To upgrade the Router's configuration, follow these instructions.
  - Click the **Browse…** button to locate the update file for the Router, or enter the exact path to the Setting file in the text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

5.7.6 Reboot

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



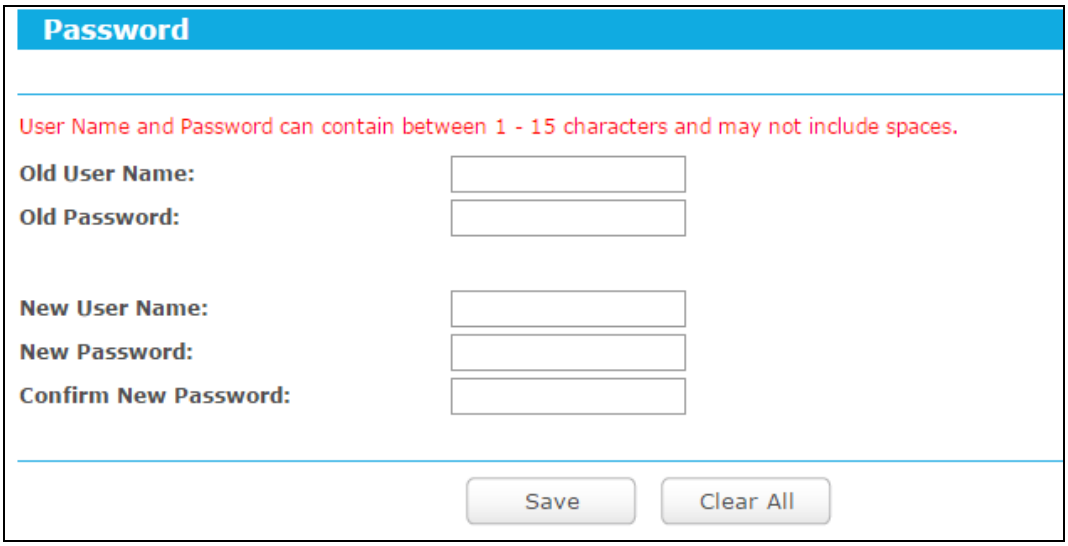
Some settings of the Router will take effect only after rebooting, which include:

- 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).

5.7.7 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 below.



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:

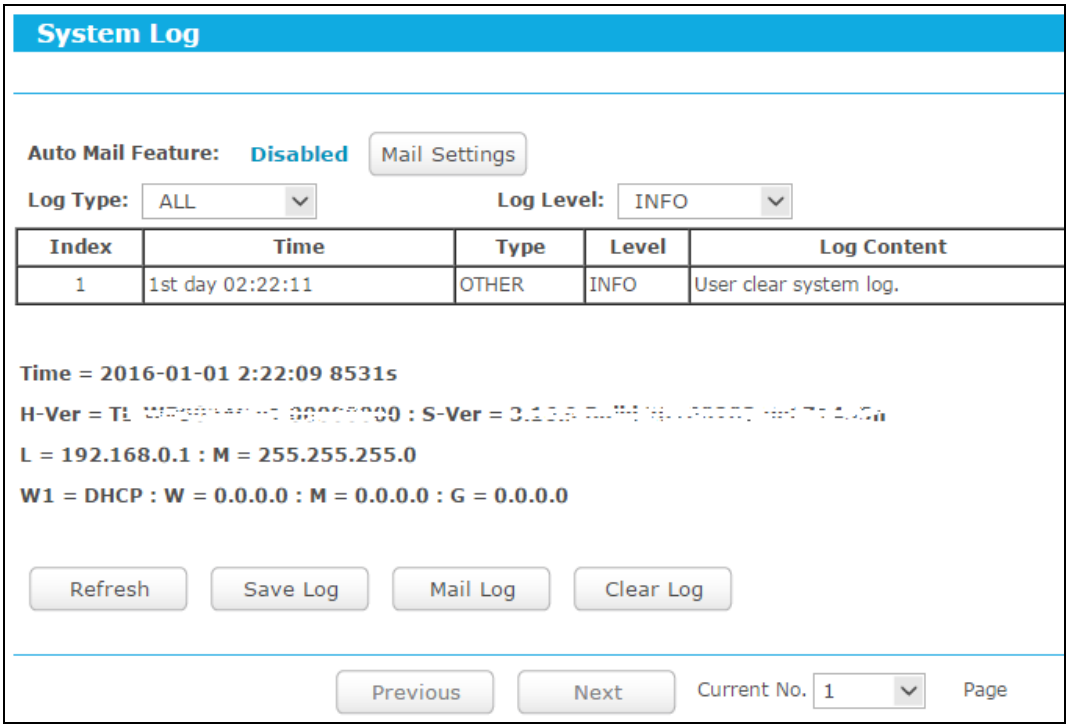
The new user name and password must not exceed 14 characters in length and not include any spaces. Enter the new Password twice to confirm.

Click the **Save** button when finished.

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

5.7.8 System Log

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



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

5.8 Logout

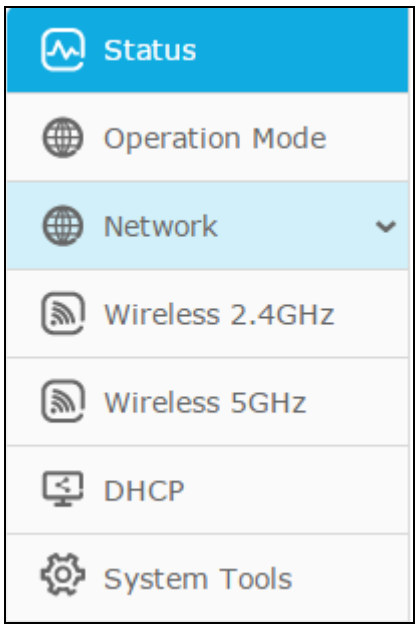
Click the **Logout** tab at the bottom of the main menu, and then the web-page will be logged out and return to the login window.

Chapter 6. Configuration for Range Extender Mode

This chapter will show each Web page's key functions and the configuration way for Range Extender Mode of TL-WR902AC.

6.1 Login

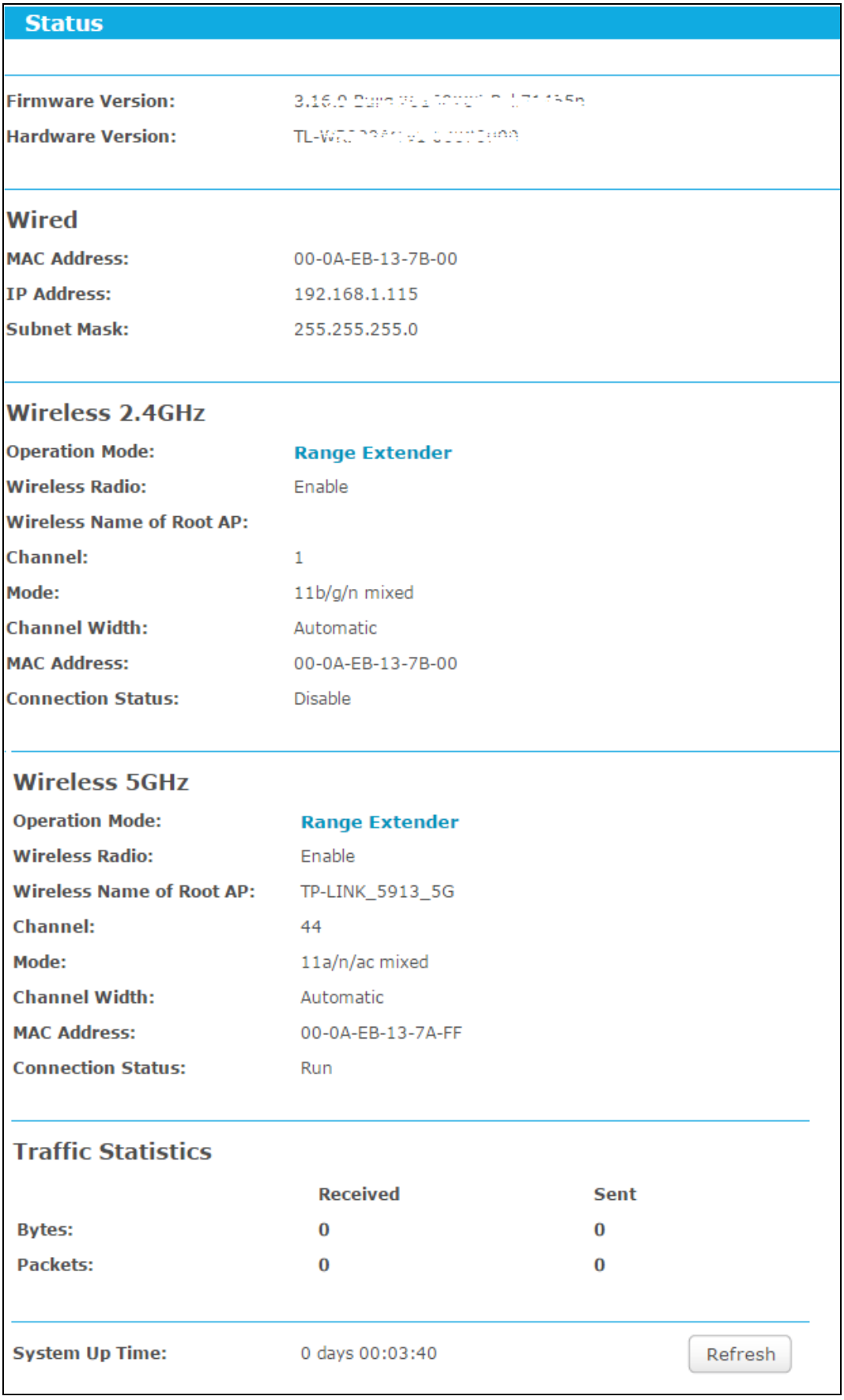
After your successful login, you can configure and manage the device. There are main menus on the left of the web-based utility. Submenus will be available after you click one of the main menus. On the right, there are the corresponding explanations and instructions.



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

6.2 Status

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



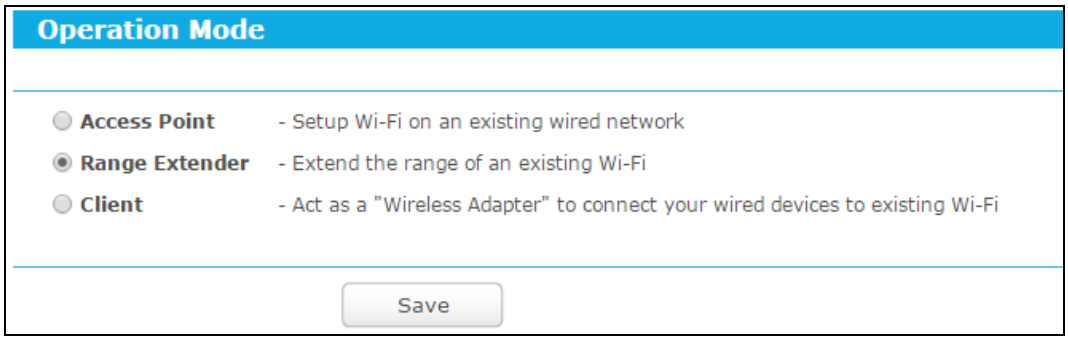
- **Firmware Version -** The version information of the Router's firmware.

- **Hardware Version -** The version information of the Router's hardware.
- **Wired -** This field displays the current settings or information for the LAN, you can configure them in the **Network > LAN** page.
  - **MAC address -** The physical address of the Router, as seen from the LAN.
  - **IP address -** The LAN IP address of the Router.
  - **Subnet Mask -** The subnet mask associated with LAN IP address.
- **Wireless -** This field displays basic information or status for wireless function, you can configure them in the **Wireless > Wireless Settings** page.
  - **Operation Mode -** The current wireless working mode in use.
  - **Wireless Name of Root AP -** The SSID of Root AP.
  - **Channel -** The current wireless channel in use.
  - **Mode -** The current wireless mode which the Router works on.
  - **Channel Width -** The current wireless channel width in use.
  - **MAC Address -** The physical address of the Router, as seen from the WLAN.
- **Traffic Statistics -** The Router's traffic statistics.
  - **Received (Bytes) -** Traffic that counted in bytes has been received out from the WAN port.
  - **Received (Packets) -** Traffic that counted in packets has been received out from the WAN port.
  - **Sent (Bytes) -** Traffic that counted in bytes has been sent out from the WAN port.
  - **Sent (Packets) -** Traffic that counted in packets has been sent out from the WAN port.
- **System Up Time -** The length of the time since the Router was last powered on or reset.

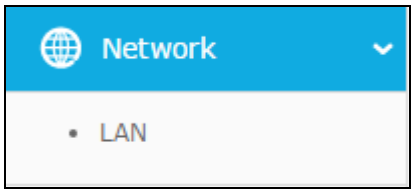
Click the **Refresh** button to get the latest status and settings of the Router.

6.3 Operation Mode

The Router supports five operation mode types: **Wireless Router**, **Access Point, Range Extender, Client** and **Hotspot**. Please select one you need and click **Save**.



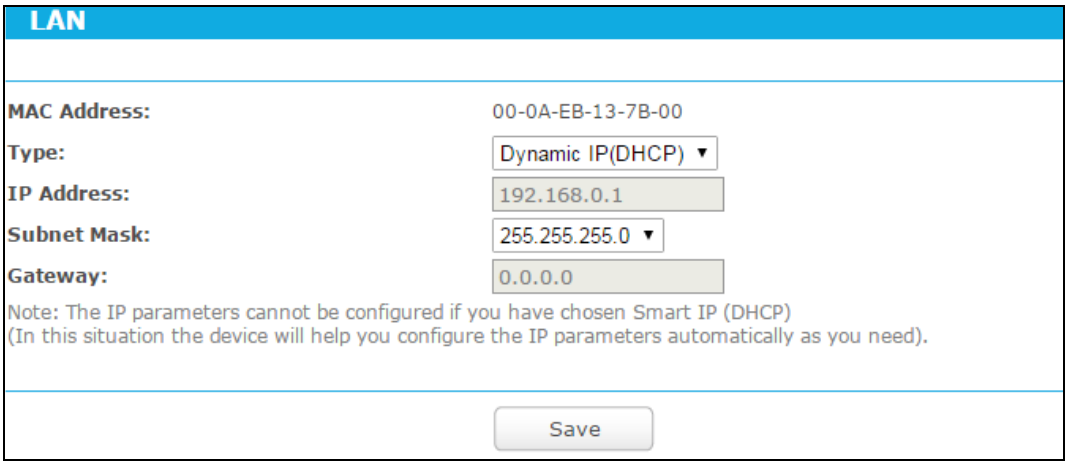
6.4 Network



There is only one submenu under the Network menu: **LAN**.

6.4.1 LAN

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

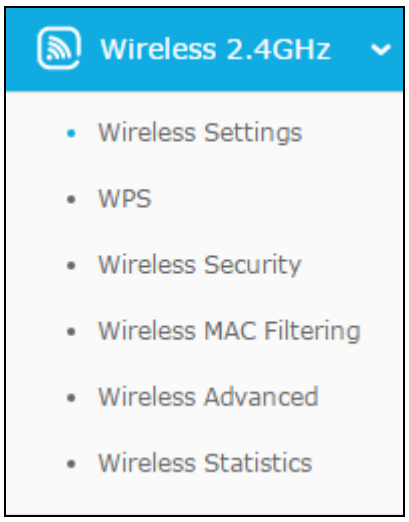


- **MAC Address -** The physical address of the LAN ports, as seen from the LAN. The value can't be changed.
- **Type** - Choosing Smart IP (DHCP) to get IP address from DHCP server, or choosing static IP to config IP address manually.
- **IP Address** - Enter the IP address of your system in dotted-decimal notation (factory default - 192.168.0.254).
- **Subnet Mask** - An address code that determines the size of the network. Normally 255.255.255.0 is used as the subnet mask.

Note:

1. If you change the IP Address of LAN, you must use the new IP Address to login to the Router.
2. If the new LAN IP Address you set is not in the same subnet with the previous one, the IP Address pool in the DHCP server will be configured automatically，while the Virtual Server and DMZ Host will not take effect until they are re-configured.

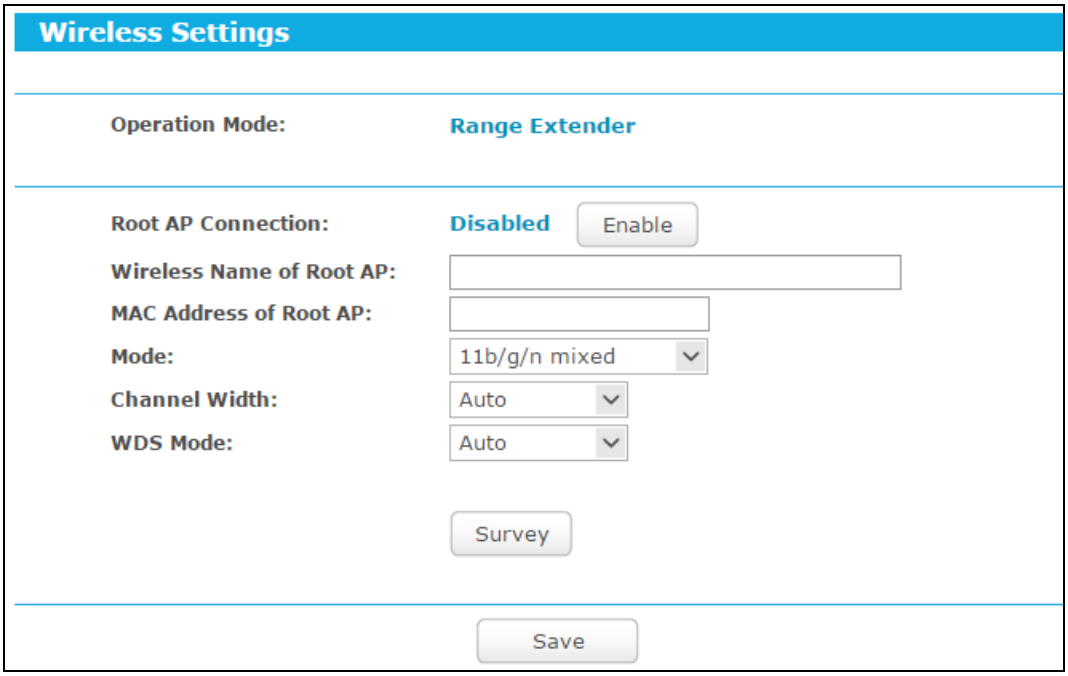
6.5 Wireless 2.4GHz/5GHz



There are six submenus under the Wireless menu: **Wireless Settings**, **Wireless Security**, **MAC Filtering**, **Wireless Advanced** and **Wireless Statistics**. Click it, and you will be able to configure the corresponding function.

6.5.1 Wireless Settings

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



- **Wireless Name of Root AP -** The SSID of AP that you want to access.
- **MAC Address of Root AP -** The MAC address of AP that you want to access.
- **Mode -** Select the desired mode. The default setting is 11bgn mixed.
  - **11n only -** Select if you are using only 802.11n wireless clients.

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

It is strongly recommended that you set the Mode to 11bgn mixed, and all of 802.11b/g/n 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 automatically adjust the channel width for your clients.
- **WDS Mode –**
- **Survey -** Click this button, you can search the AP which runs in the environment.
- **WDS Mode -**

Click **Survey** button on the Wireless page, and then AP List page will appear as shown below. Find the SSID of the network you want to extend, and click **Connect** in the corresponding row.

AP List

AP Count: 60

ID	BSSID	SSID	Signal	Channel	Security	Choose
1	F8-1A-67-6F-8F-01	TP-LINK_8F01	39dB	6	WPA2-PSK	Connect
2	80-F6-2E-00-F6-22	CMCC-FREE	35dB	11	None	Connect
3	1C-60-DE-24-14-3E	MERCURY_123	33dB	1	WPA-PSK/WPA2-PSK	Connect
4	80-F6-2E-00-F6-20	CMCC-WEB	33dB	11	None	Connect
5	00-0A-EB-13-09-19	TP-LINK_0919	32dB	4	WPA2-PSK	Connect
6	40-16-9F-02-00-59	TP-LINK_0059	30dB	7	WPA2-PSK	Connect
7	40-16-9F-BF-58-11	TP-LINK_5811	29dB	3	WPA2-PSK	Connect
8	00-0A-EB-13-7A-FF	TP-LINK_7AFF	27dB	13	None	Connect
9	40-16-9F-BF-59-13	TP-LINK_5913	27dB	13	WPA2-PSK	Connect

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

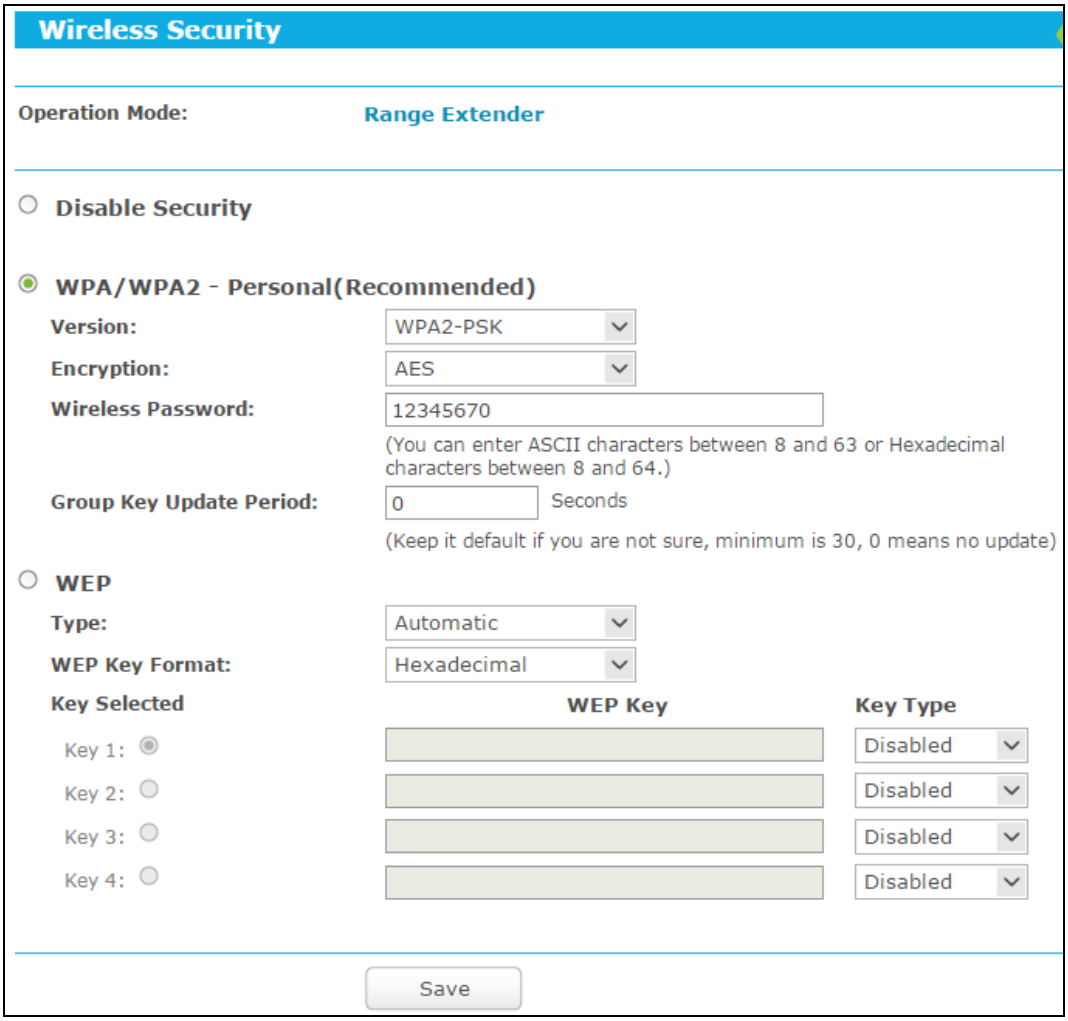
Note:

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.
   - 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.

6.5.2 Wireless Security

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

There are three wireless security modes supported by the Router: WPA/WPA2-Personal, WPA/WPA2-Enterprise and WEP (Wired Equivalent Privacy).

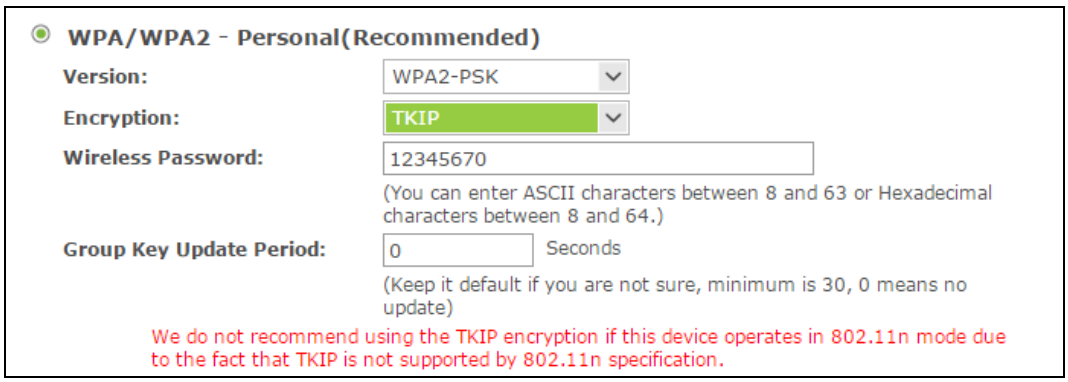


- **Disable Security -** The wireless security function can be enabled or disabled. If disabled, the wireless stations will be able to connect the Router without encryption. But it's strongly recommended to choose one of the following modes to enable security.
- **WPA-PSK/WPA2-Personal -** It's the WPA/WPA2 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** radio button and choose TKIP encryption, you will find a notice in red as shown below.



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

- **Version** - you can choose the version of the WPA security from 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 **Automatic**, **TKIP** or **AES.**
- **Radius Server IP -** Enter the IP address of the Radius server.
- **Radius Port -** Enter the port that Radius server 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.

- **Type -** you can choose the type for the WEP security on the pull-down list. The default setting is **Automatic**, which can select **Shared Key** or **Open System** authentication type automatically based on the wireless station's capability and request.
- **WEP Key Format - Hexadecimal** and **ASCII** formats are provided here. **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 (Password) -** 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.

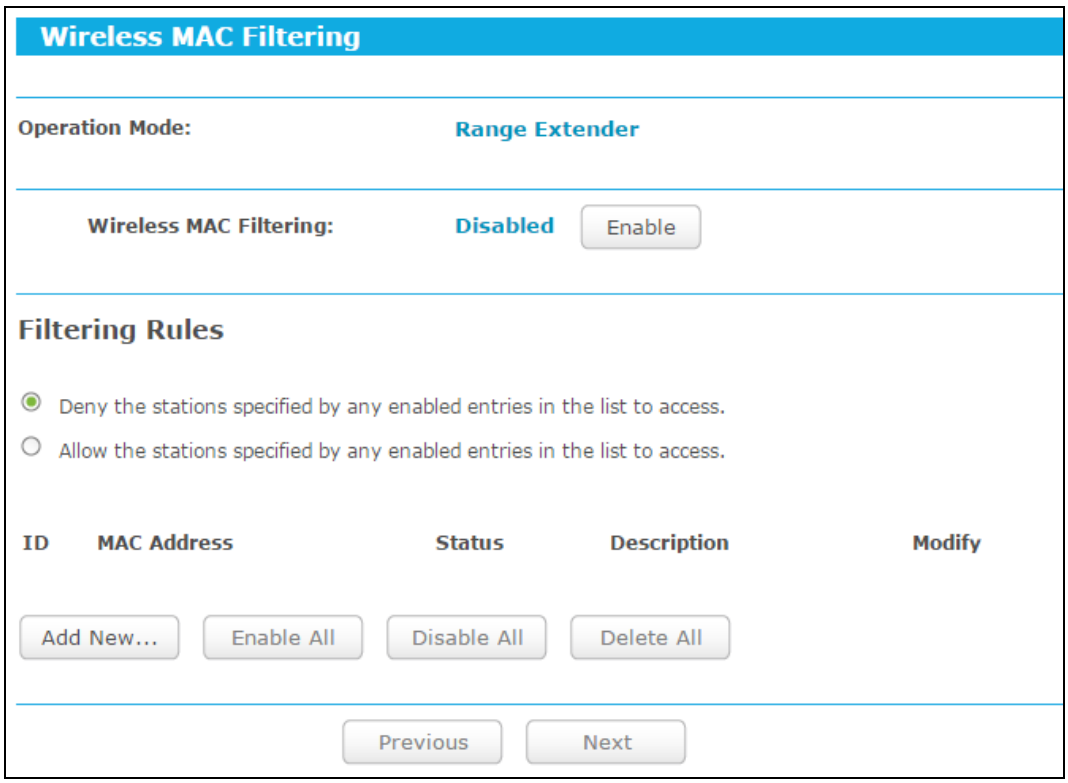
  152-bit - You can enter 32 hexadecimal digits (any combination of 0-9, a-f, A-F, zero key is not promoted) or 16 ASCII characters.

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.

6.5.3 Wireless MAC Filtering

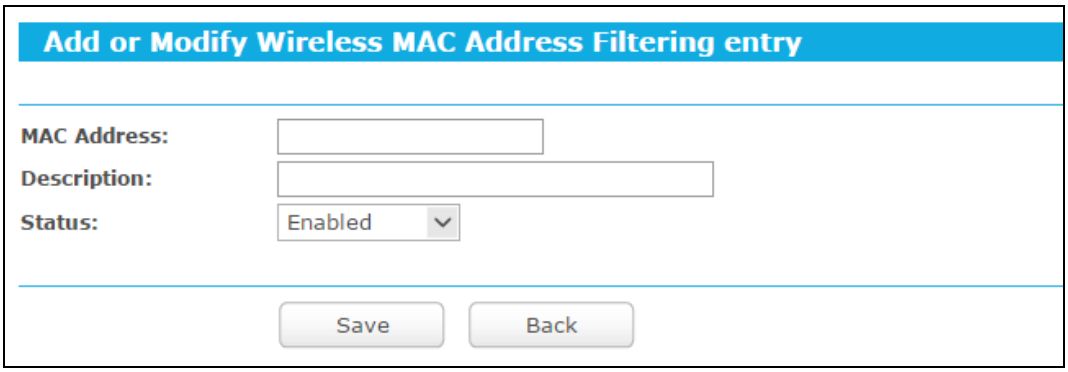
Choose menu "**Wireless → Wireless MAC Filtering**", and then you can control the wireless access by configuring the **Wireless MAC Filtering** function.



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 access.
- **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:



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

1. Enter the appropriate MAC Address into the **MAC Address** field. The format of the MAC Address is XX-XX-XX-XX-XX-XX (X is any hexadecimal digit). For example: 00-0A-EB-B0-00-0B.
2. Give a simple description for 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 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.

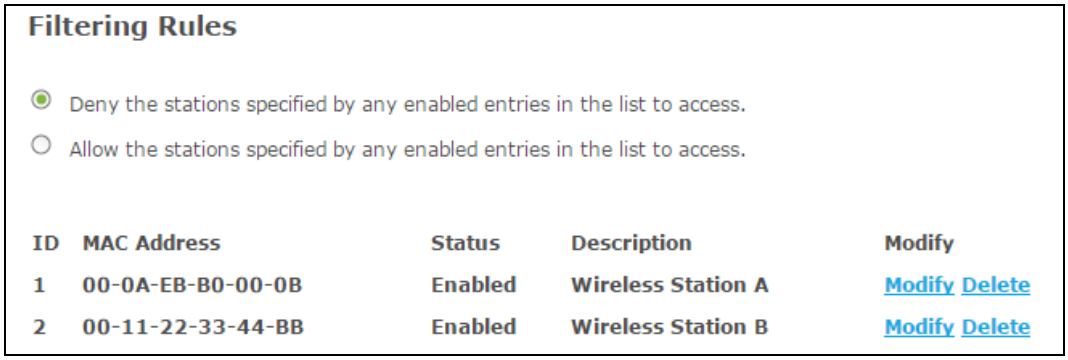
For example: If you desire that the wireless station A with MAC address 00-0A-EB-B0-00-0B and the wireless station B with MAC address 00-0A-EB-00-07-5F are able to access the Router, but all the other wireless stations cannot access the Router, you can configure the **Wireless MAC Address Filtering** list by following these steps:

1. Click the **Enable** button to enable this function.
2. Select the radio button “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.

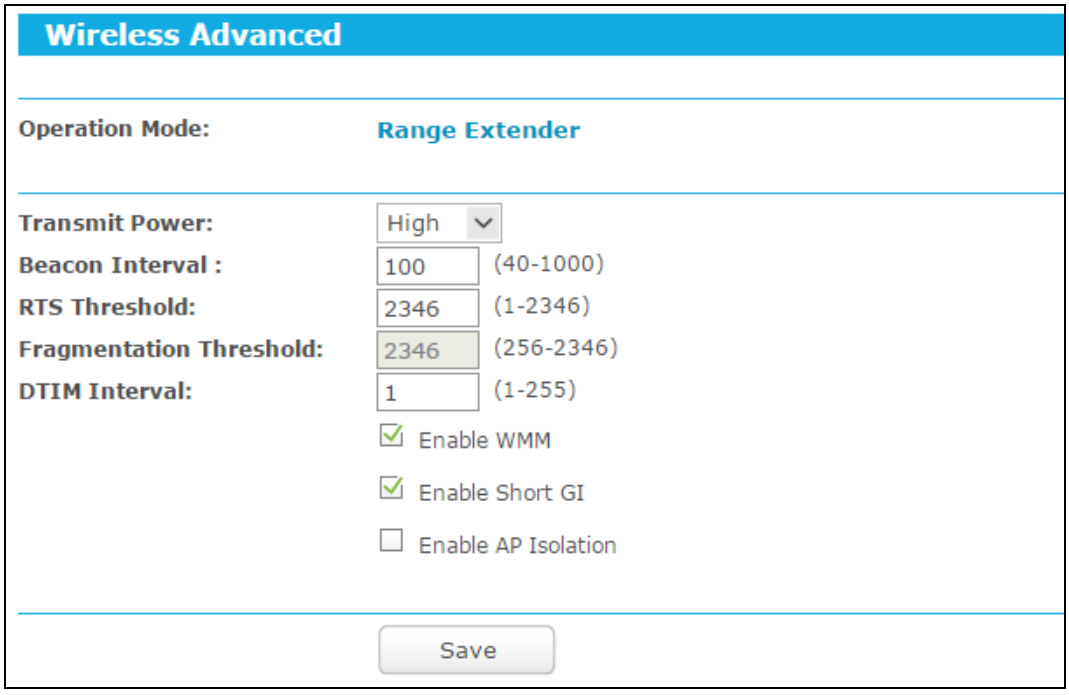
- Enter the MAC address 00-0A-EB-B0-00-0B/00-0A-EB-00-07-5F in the **MAC Address** field.
- Enter wireless station A/B in the **Description** field.
- Select **Enabled** in the **Status** pull-down list.
- Click the **Save** button.
- Click the **Back** button.

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



6.5.4 Wireless Advanced

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



➢ **Transmit Power -** Here you can specify the transmit power of Router. You can select High, Middle or Low which you would like. High is the default setting and is recommended.

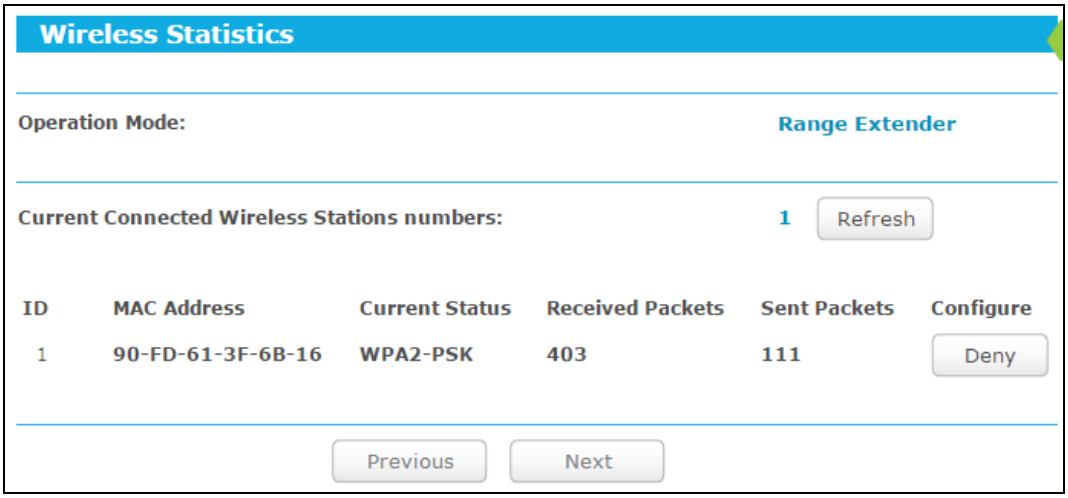
- **Beacon Interval -** Enter a value between 20-1000 milliseconds for Beacon Interval here. The beacons are the packets sent by the Router to synchronize a wireless network. Beacon Interval value determines the time interval of the beacons. The default value is 100.
- **RTS Threshold -** Here you can 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 because of 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.
- **Enable AP Isolation -** This function isolate all connected wireless stations so that wireless stations cannot access each other through WLAN. This function will be disabled if WDS/Bridge is enabled.

☞ **Note:**

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

6.5.5 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.



- **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.
- **Configure -** The button is used for loading the item to the **Wireless MAC Filtering** list.

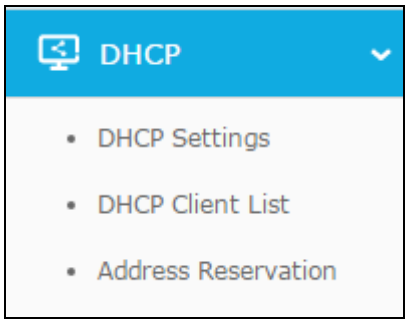
You cannot change any of the values on this page. To update this page and to show the current connected wireless stations, click on the **Refresh** button.

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.

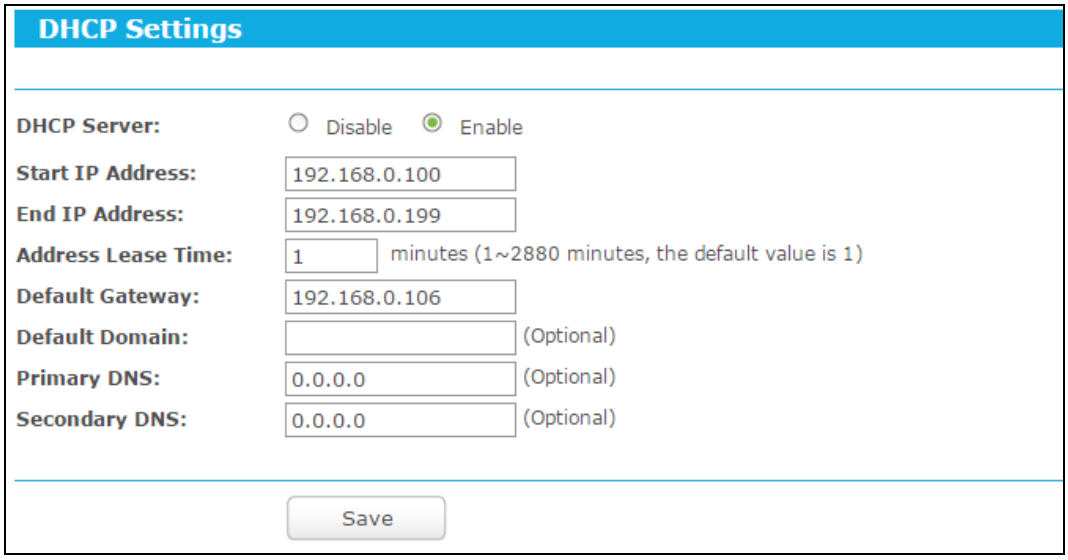
6.6 DHCP



There are three submenus under the DHCP menu: **DHCP Settings**, **DHCP Client List** and **Address Reservation.** Click any of them, and you will be able to configure the corresponding function.

6.6.1 DHCP Settings

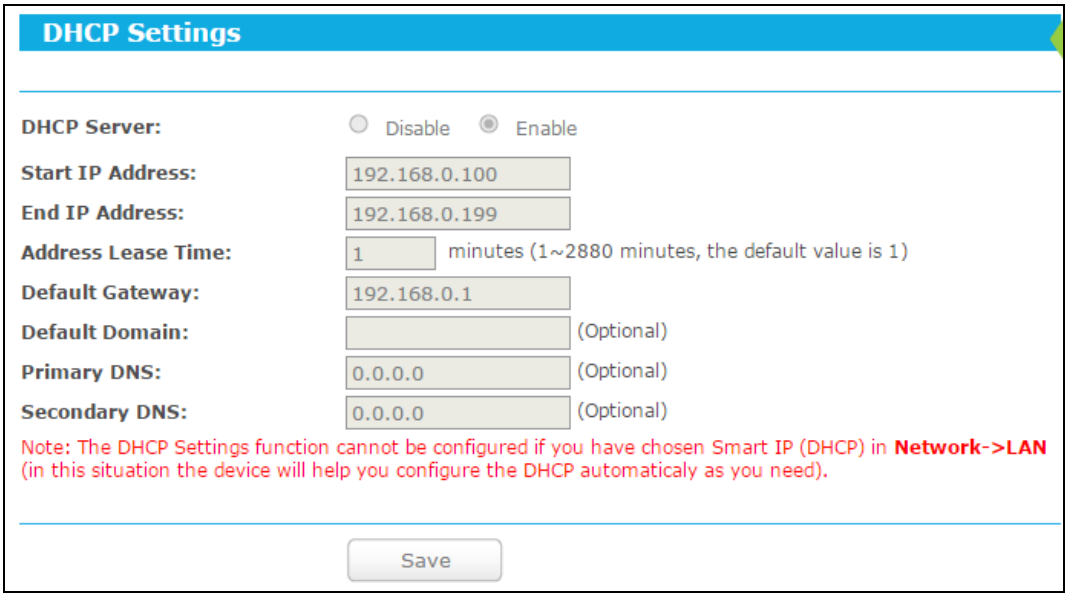
Choose menu "**DHCP → DHCP Settings**", and then you can configure the DHCP Server on the page as shown below. The Router is set up by default as a DHCP (Dynamic Host Configuration Protocol) server, which provides the TCP/IP configuration for all the PC(s) that are connected to the Router in the LAN.



- **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) **-** It is suggested to input the IP address of the LAN port of the Router. The 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.

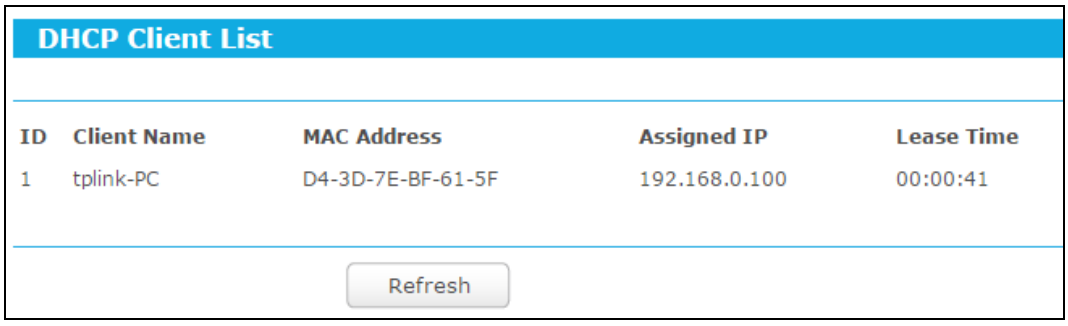
Note:

1. To use the DHCP server function of the Router, you must configure all computers on the LAN as "Obtain an IP Address automatically".
2. When you choose the Smart IP (DHCP) mode in Network → LAN, the DHCP Server function will be disabled. You will see the page as below.



6.6.2 DHCP Client List

Choose menu "**DHCP → DHCP Client List**", and then you can view the information about the clients attached to the Router in the screen as shown below.

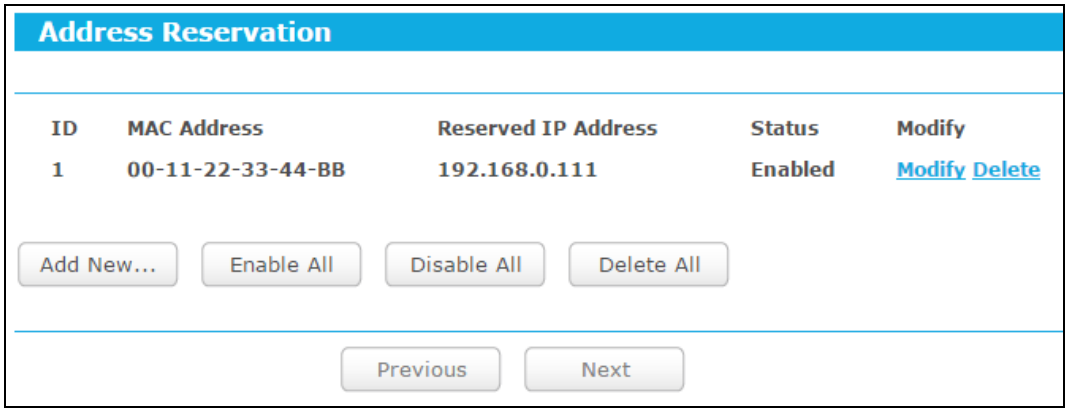


- **Client Name -** The name of the DHCP client.
- **MAC Address -** The MAC address of the DHCP client.
- **Assigned IP -** The IP address that the Router has allocated to the DHCP client.
- **Lease Time -** The time of the DHCP client leased. After the dynamic IP address has expired, a new dynamic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

6.6.3 Address Reservation

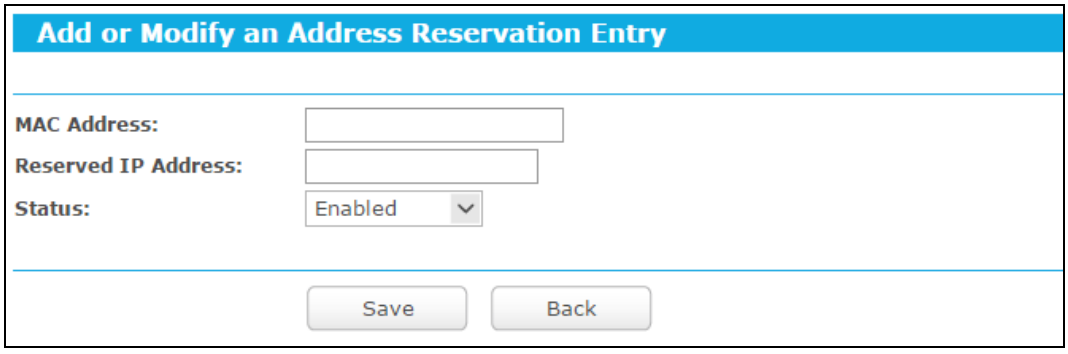
Choose menu "**DHCP → Address Reservation**", and then you can view and add a reserved address for clients via the next screen. When you specify a reserved IP address for a PC on the LAN, that PC will always receive the same IP address each time when it accesses the DHCP server. Reserved IP addresses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



- **MAC Address -** The MAC address of the PC for which you want to reserve an IP address.
- **Reserved IP Address -** The IP address reserved for the PC by the Router.
- **Status -** The status of this entry either **Enabled** or **Disabled**.
- **Modify -** To modify or delete an existing entry.

To Reserve an IP address:

1. Click the **Add New…** button.
2. Enter the MAC address (in XX-XX-XX-XX-XX-XX format) and IP address (in dotted-decimal notation) of the computer for which you want to reserve an IP address.
3. Click the **Save** button.



To modify or delete an existing entry:

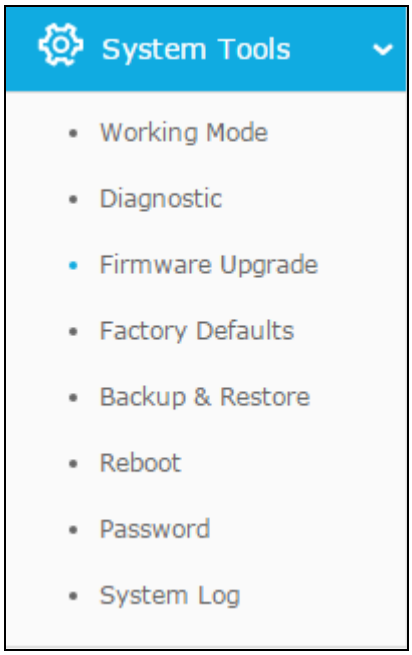
1. Click the **Modify** in the entry you want to modify. If you want to delete the entry, click the **Delete**.
2. Modify the information.
3. Click the **Save** button.

Click the **Enable/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.

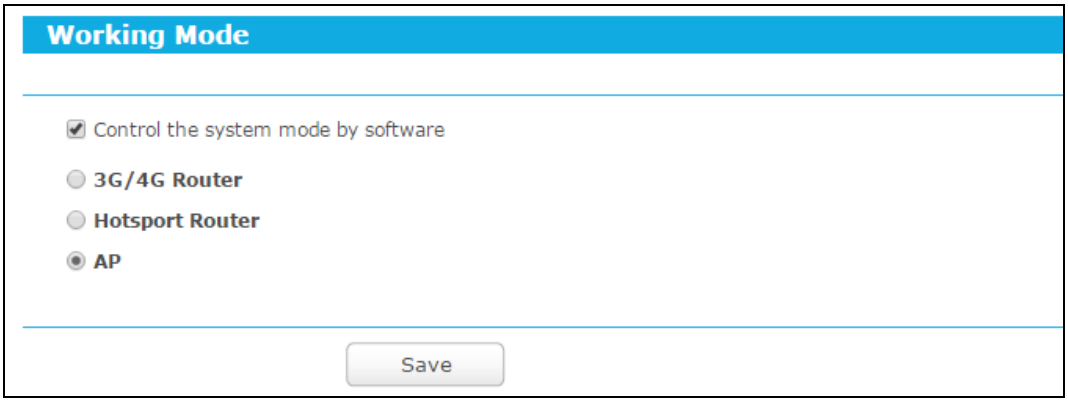
6.7 System Tools



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

6.7.1 Working Mode

Choose menu "**System Tools** → **Working Mode**", check **Control the system mode by software** and then you can see the following screen.



➢ **3G/4G Router -** This mode stands for Wireless Router Mode. It functions as a standard

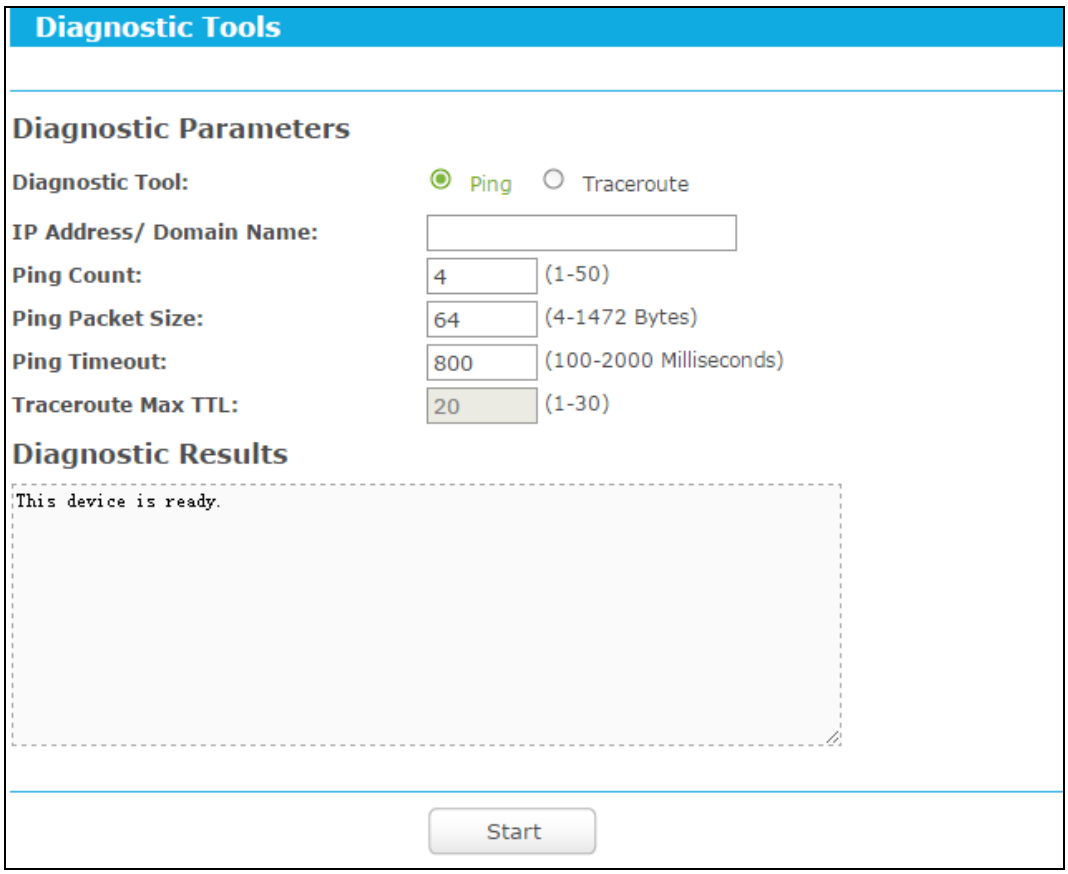
wireless router and you can also plug in a 3G/4G USB modem if you need.

- **Hotspot Router -** It functions as a hotspot router.
- **AP –** This mode stands for Access Point Mode, Repeater Mode and Client Mode. When selected, you have to go to the **Quick Setup** to specify the mode you need.

  Note: If **Control the system mode by software** is checked, the operation mode switch of the router will be disabled.

6.7.2 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.



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

Note:

You can use ping/traceroute to test both numeric IP address or domain name. If pinging/tracerouting the IP address is successful, but pinging/tracerouting the domain name is not,

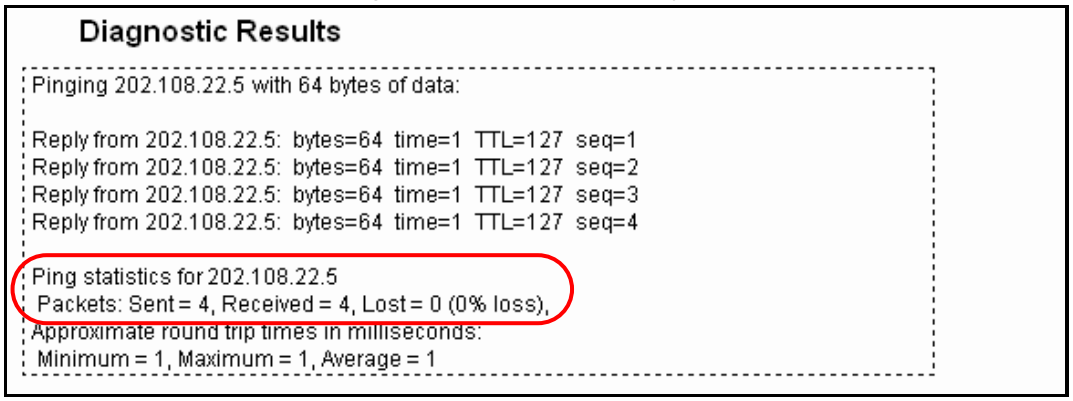
you might have a name resolution problem. In this case, ensure that the domain name you are specifying can be resolved by using Domain Name System (DNS) queries.

- **IP Address/Domain Name -** Type the destination IP address (e.g. 202.108.22.5) or Domain name (e.g. http://www.tp-link.com).
- **Pings Count -** The number of Ping packets for a Ping connection. The default is 4.
- **Ping Packet Size -** The size of Ping packet. The default is 64.
- **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. The default is 800.
- **Traceroute Max TTL -** The max number of hops for a Traceroute connection. 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.

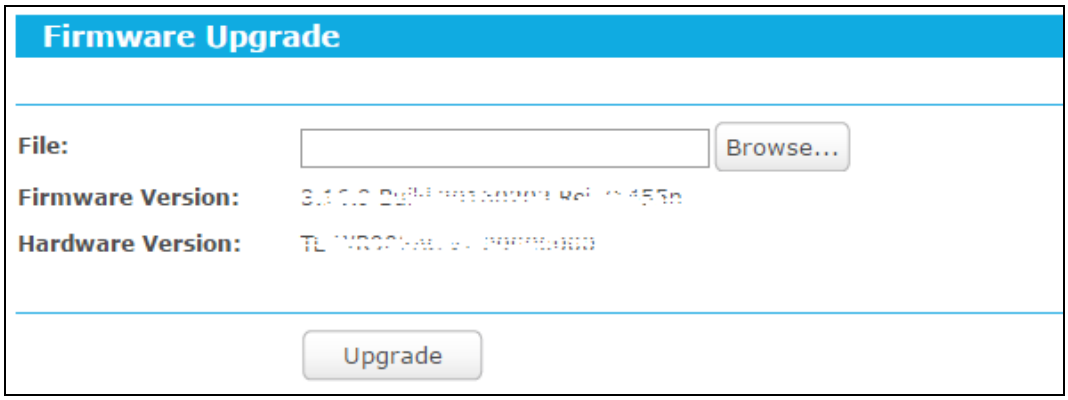


Note:

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.

6.7.3 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.



- **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:

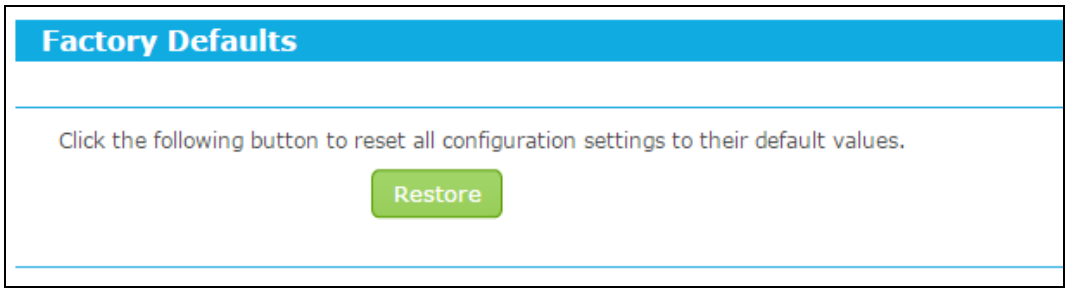
1. Download a more recent firmware upgrade file from the TP-LINK website (http://www.tp-link.com).
2. Type the path and file name of the update file into the **File** field, or click the **Browse** button to locate the update file.
3. Click the **Upgrade** button.

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.

6.7.4 Factory Defaults

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



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

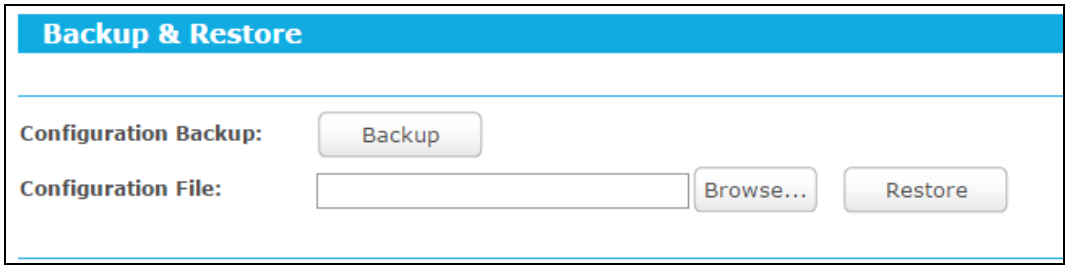
- The default User Name: admin
- The default Password: admin
- The default access: tplinkwifi.net

Note:

All changed settings will be lost when defaults are restored.

6.7.5 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 below.



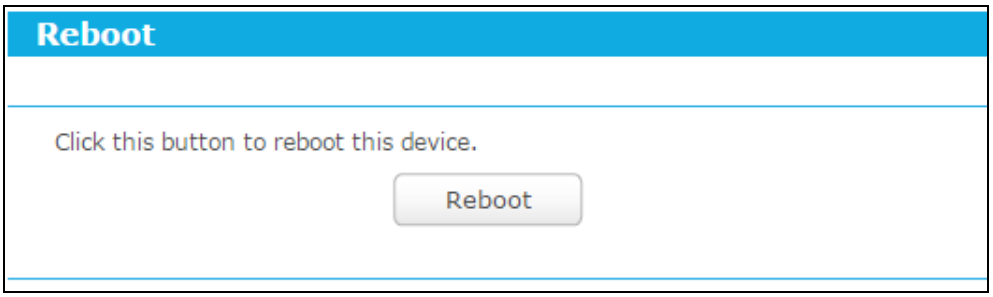
- Click the **Backup** button to save all configuration settings as a backup file in your local computer.
- To upgrade the Router's configuration, follow these instructions.
  - Click the **Browse…** button to locate the update file for the Router, or enter the exact path to the Setting file in the text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

6.7.6 Reboot

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



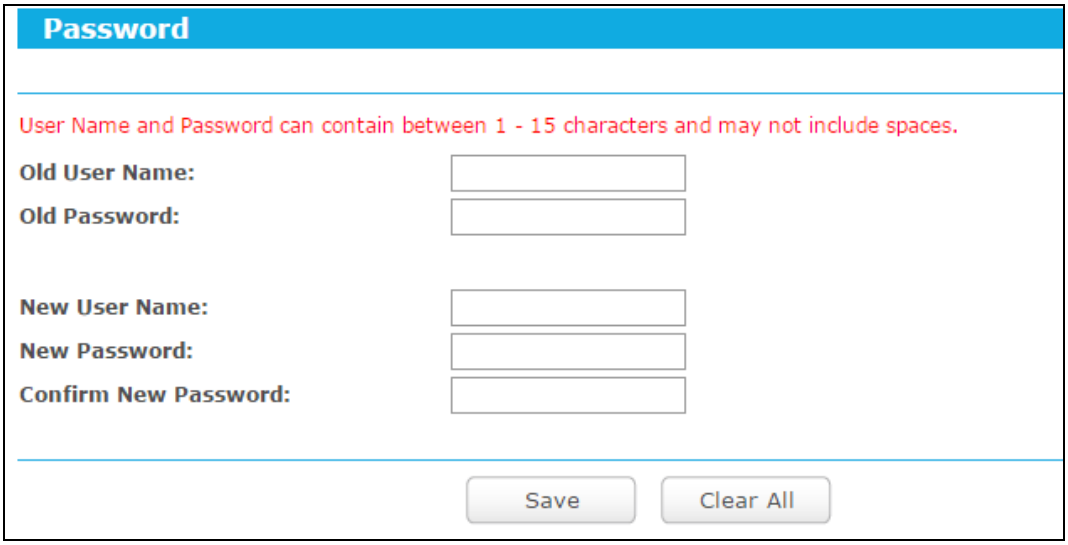
Some settings of the Router will take effect only after rebooting, including:

- Change the LAN IP Address (system will reboot automatically).
- Change the DHCP Settings.
- Change the Wireless configurations.

- Change the Web Management Port.
- Upgrade the firmware of the 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.

6.7.7 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 below.



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:**

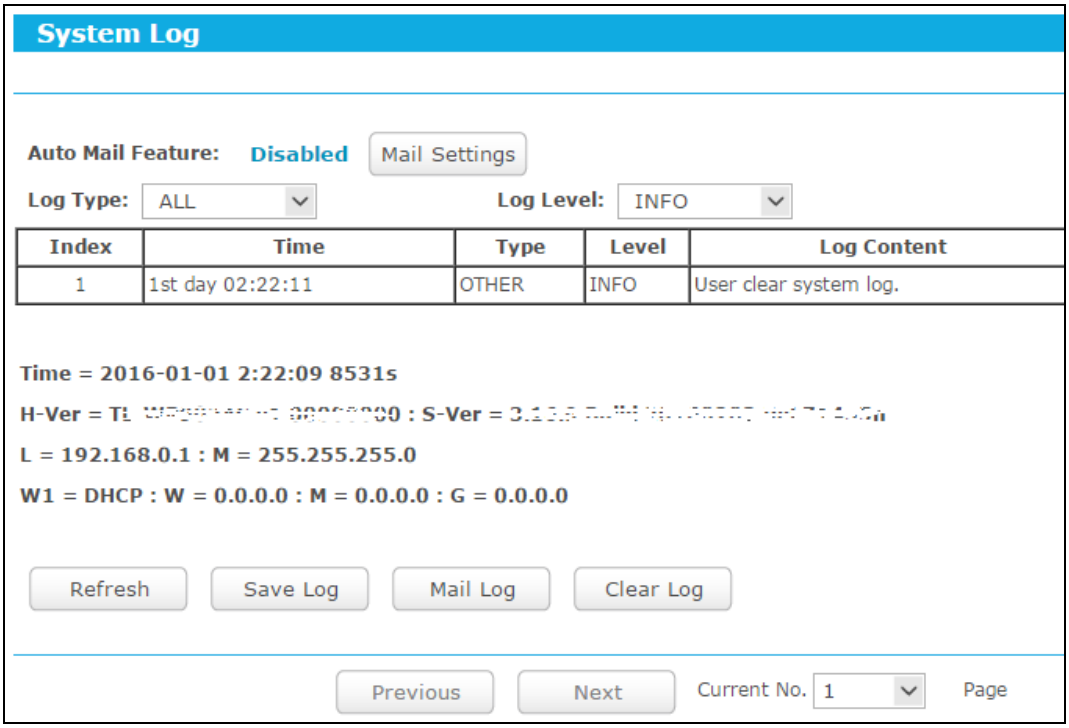
The new user name and password must not exceed 14 characters in length and not include any spaces. Enter the new Password twice to confirm.

Click the **Save** button when finished.

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

6.7.8 System Log

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



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

6.8 Logout

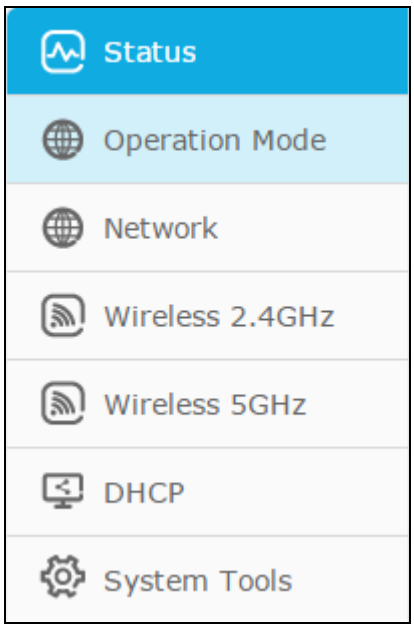
Click the **Logout** tab at the bottom of the main menu, and then the web-page will be logged out and return to the login window.

Chapter 7. Configuration for Client Mode

This chapter will show each Web page's key functions and the configuration way for Client Mode of TL-WR902AC.

7.1 Login

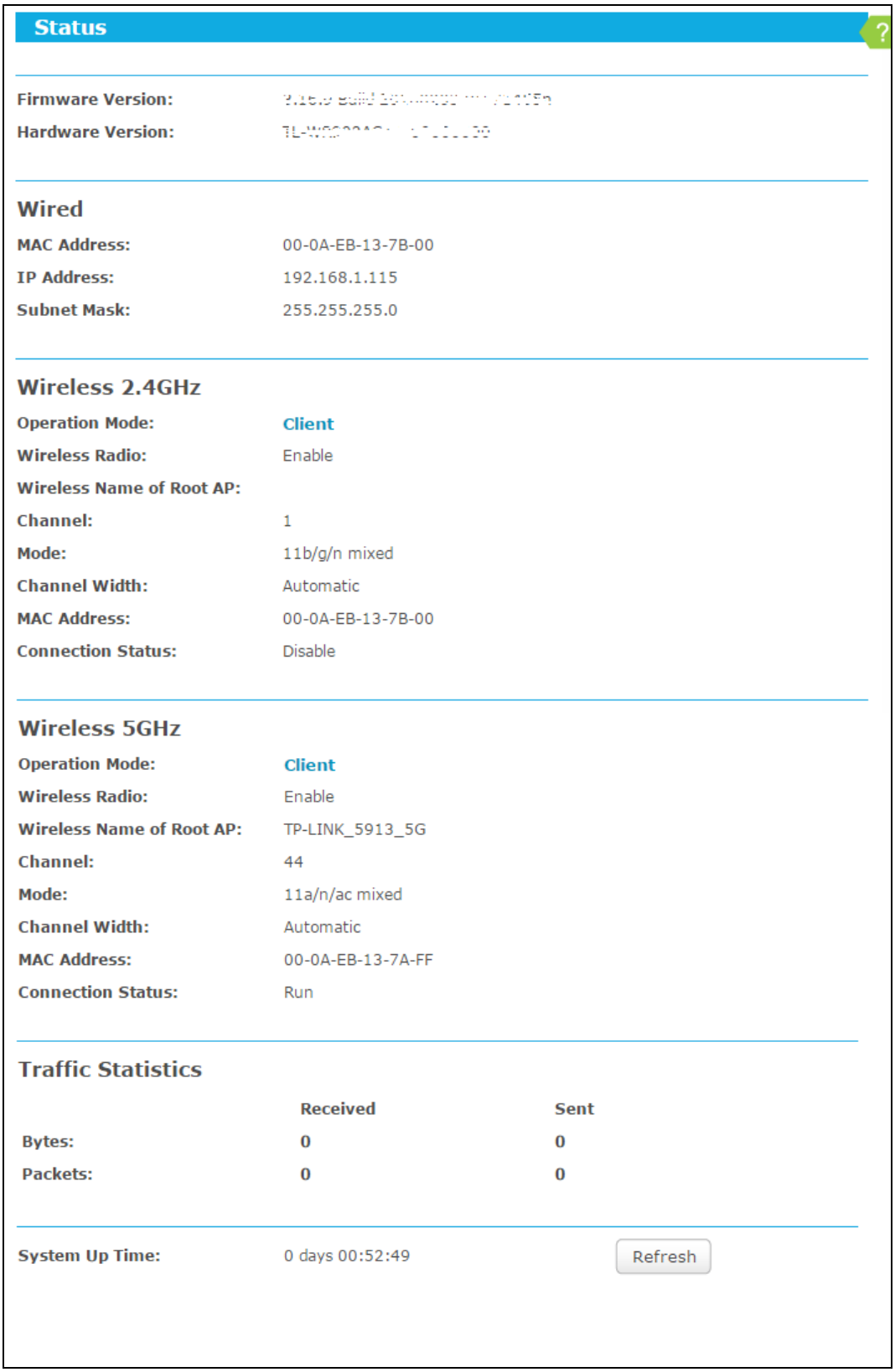
After your successful login, you can configure and manage the device. There are main menus on the left of the web-based utility. Submenus will be available after you click one of the main menus. On the right, there are the corresponding explanations and instructions.



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

7.2 Status

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



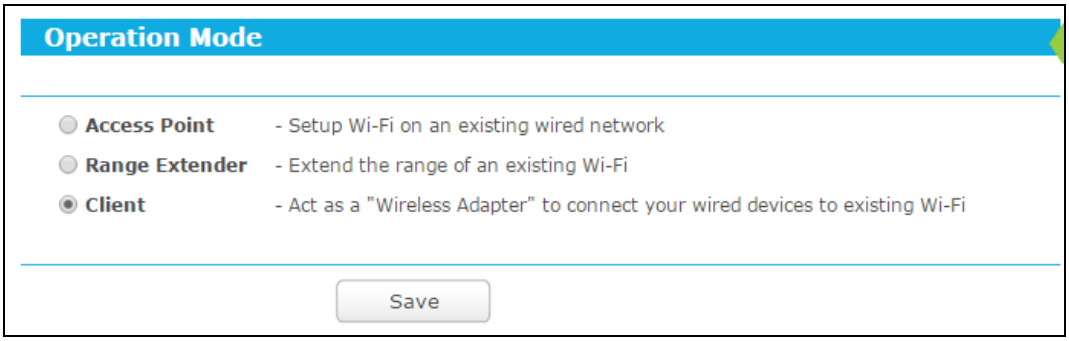
- **Firmware Version -** The version information of the Router's firmware.
- **Hardware Version -** The version information of the Router's hardware.

- **Wired -** This field displays the current settings or information for the LAN, you can configure them in the **Network > LAN** page.
  - **MAC address -** The physical address of the Router, as seen from the LAN.
  - **IP address -** The LAN IP address of the Router.
  - **Subnet Mask -** The subnet mask associated with LAN IP address.
- **Wireless -** This field displays basic information or status for wireless function, you can configure them in the **Wireless > Wireless Settings** page.
  - **Operation Mode -** The current wireless working mode in use.
  - **Wireless Name of Root AP -** The SSID of Root AP.
  - **Channel -** The current wireless channel in use.
  - **Mode -** The current wireless mode which the Router works on.
  - **Channel Width -** The current wireless channel width in use.
  - **MAC Address -** The physical address of the Router, as seen from the WLAN.
- **Traffic Statistics -** The Router's traffic statistics.
  - **Received (Bytes) -** Traffic that counted in bytes has been received out from the WAN port.
  - **Received (Packets) -** Traffic that counted in packets has been received out from the WAN port.
  - **Sent (Bytes) -** Traffic that counted in bytes has been sent out from the WAN port.
  - **Sent (Packets) -** Traffic that counted in packets has been sent out from the WAN port.
- **System Up Time -** The length of the time since the Router was last powered on or reset.

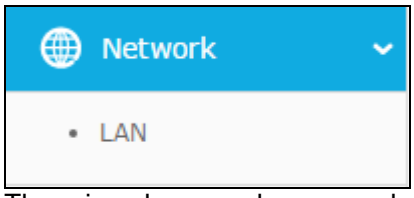
Click the **Refresh** button to get the latest status and settings of the Router.

7.3 Operation Mode

The Router supports five operation mode types: **Wireless Router**, **Access Point, Range Extender, Client** and **Hotspot**. Please select one you need and click **Save**.



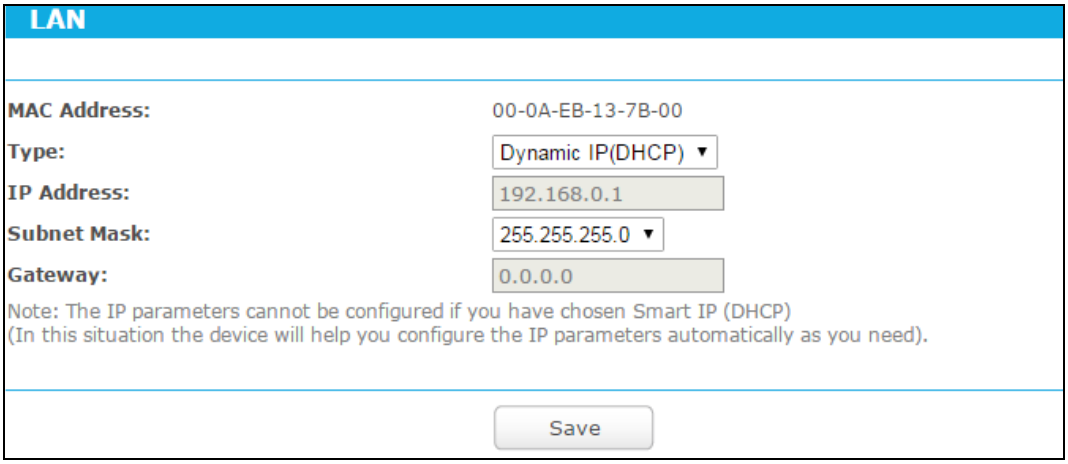
7.4 Network



There is only one submenu under the Network menu: **LAN**.

7.4.1 LAN

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



- **MAC Address -** The physical address of the LAN ports, as seen from the LAN. The value can't be changed.
- **Type** - Choosing Smart IP (DHCP) to get IP address from DHCP server, or choosing static IP to set IP address manually.
- **IP Address** - Enter the IP address of your system in dotted-decimal notation (factory default - 192.168.0.254).
- **Subnet Mask** - An address code that determines the size of the network. Normally 255.255.255.0 is used as the subnet mask.

☞ **Note:**

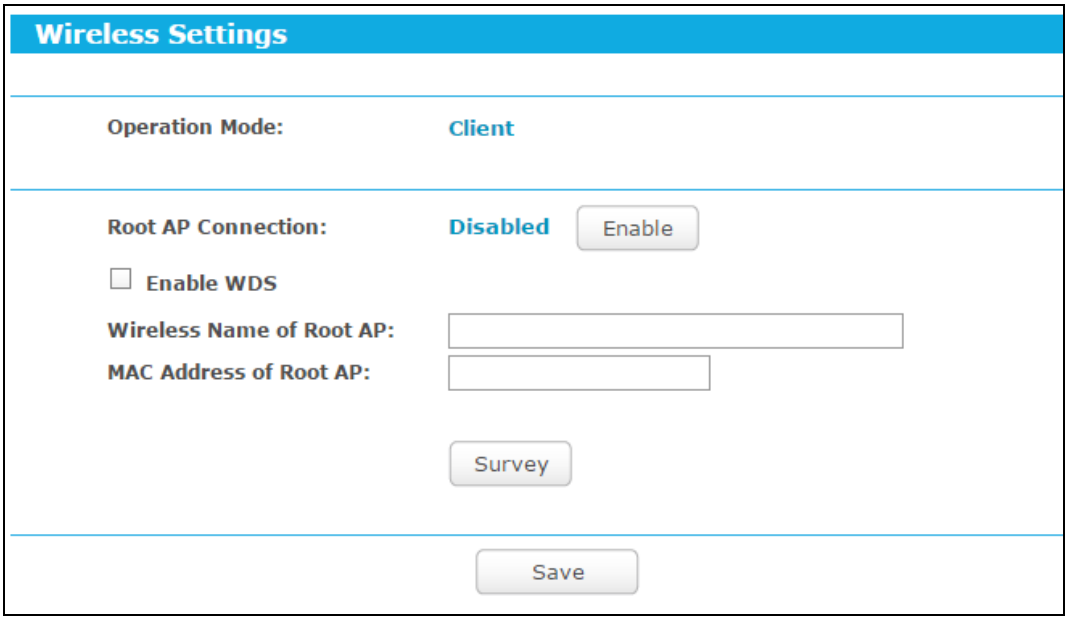
1. If you change the IP Address of LAN, you must use the new IP Address to login to the Router.
2. If the new LAN IP Address you set is not in the same subnet with the previous one, the IP Address pool in the DHCP server will be configured automatically，while the Virtual Server and DMZ Host will not take effect until they are re-configured.
3. When you choose the **Smart IP (DHCP)** mode, the DHCP Server function will be disabled.

7.5 Wireless 2.4GHz/5GHz

There are four submenus under the Wireless menu: **Wireless Settings**, **Wireless Security**, **Wireless Advanced**, and **Wireless Statistics**. Click any of them, and you will be able to configure the corresponding function.

7.5.1 Wireless Settings

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



- **Enable WDS** - The AP client can connect to AP with WDS enabled or disabled. If WDS is enabled, all traffic from wired networks will be forwarded in the format of WDS frames consisting of four address fields. If WDS is disabled, three address frames are used. If your AP supports WDS well, please enable this option.
- **Wireless Name of Root AP** - Enter the SSID of AP that you want to access.
- **MAC Address of Root AP** - Enter the MAC address of AP that you want to access.
- **Survey** - Click this button, you can search the APs.

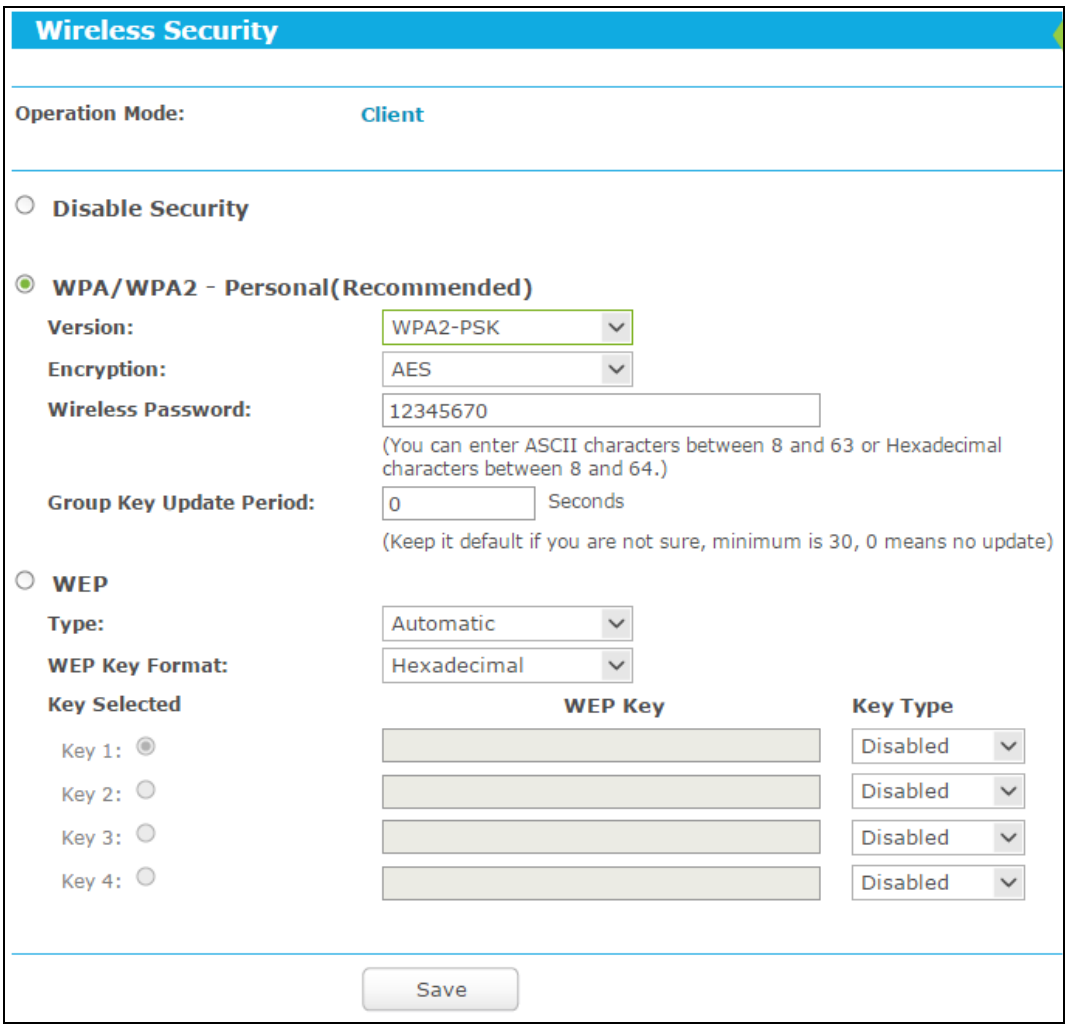
Note:

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.
   - 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.

7.5.2 Wireless Security

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

There are three wireless security modes supported by the Router: WPA/WPA2-Personal, WPA/WPA2-Enterprise and WEP (Wired Equivalent Privacy).



- **Disable Security -** The wireless security function can be enabled or disabled. If disabled, the wireless stations will be able to connect the Router without encryption. But it's strongly recommended to choose one of the following modes to enable security.

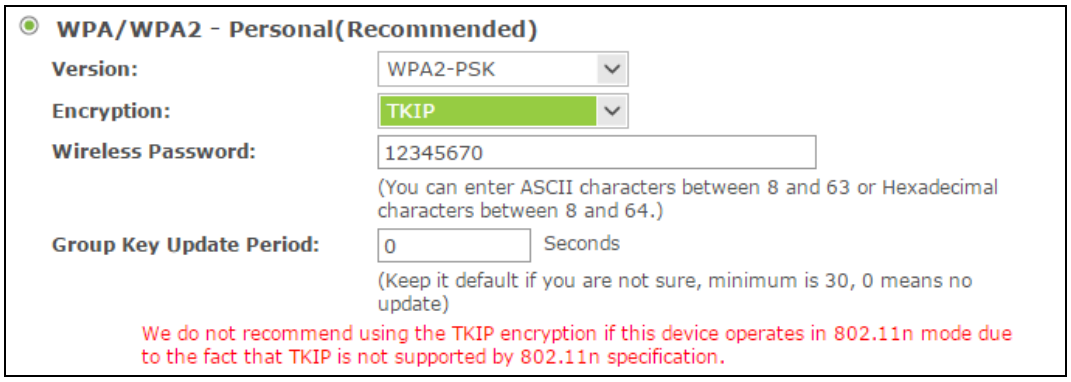
- **WPA-PSK/WPA2-Personal -** It's the WPA/WPA2 authentication type based on pre-shared passphrase.

  - **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** radio button and choose TKIP encryption, you will find a notice in red as shown below.



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

  - **Version -** you can choose the version of the WPA security from 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 **Automatic**, **TKIP** or **AES.**

  - **Radius Server IP -** Enter the IP address of the Radius server.

  - **Radius Port -** Enter the port that Radius server 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.

- **Type -** you can choose the type for the WEP security on the pull-down list. The default setting is **Automatic**, which can select **Shared Key** or **Open System** authentication type automatically based on the wireless station's capability and request.
- **WEP Key Format - Hexadecimal** and **ASCII** formats are provided here. **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 (Password) -** 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.

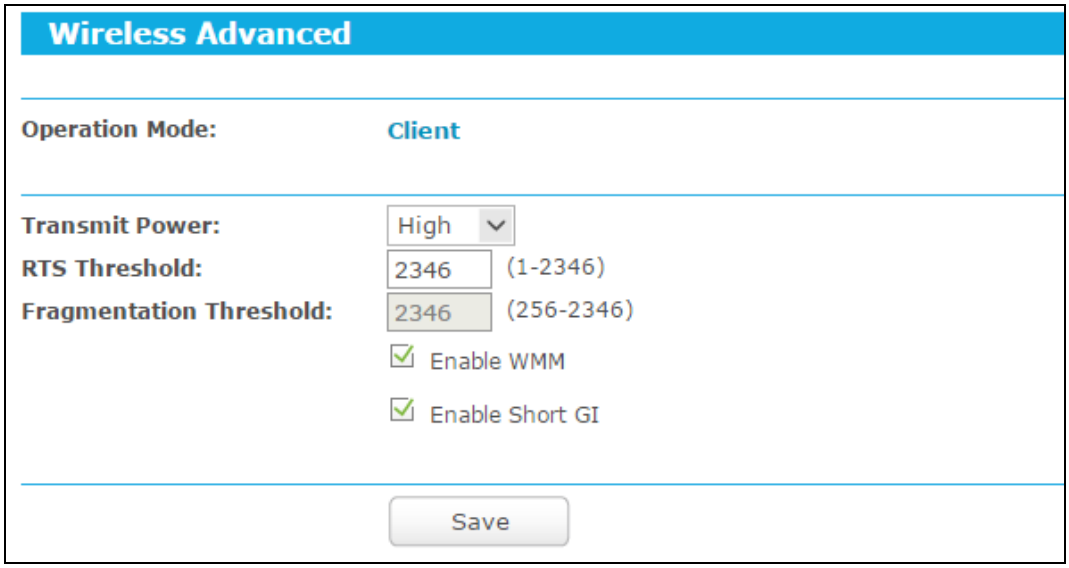
  152-bit - You can enter 32 hexadecimal digits (any combination of 0-9, a-f, A-F, zero key is not promoted) or 16 ASCII characters.

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.

7.5.3 Wireless Advanced

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



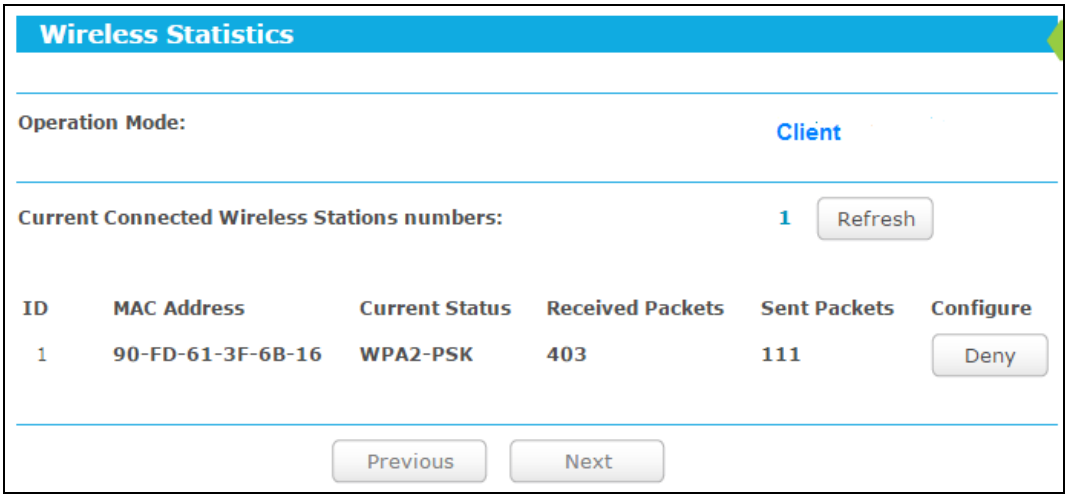
- **Transmit Power -** Here you can specify the transmit power of Router. You can select High, Middle or Low which you would like. High is the default setting and is recommended.
- **RTS Threshold -** Here you can specify the RTS (Request to Send) Threshold. If the packet is larger than the specified 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 because of excessive packets. 2346 is the default setting and is recommended.
- **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.

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.

7.5.4 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.



- **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.

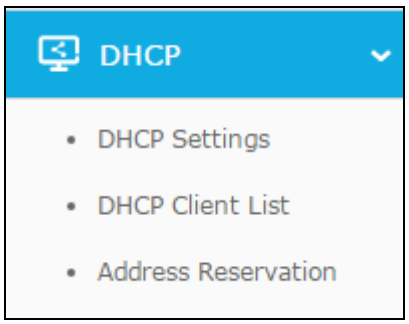
You cannot change any of the values on this page. To update this page and to show the current connected wireless stations, click on the **Refresh** button.

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.

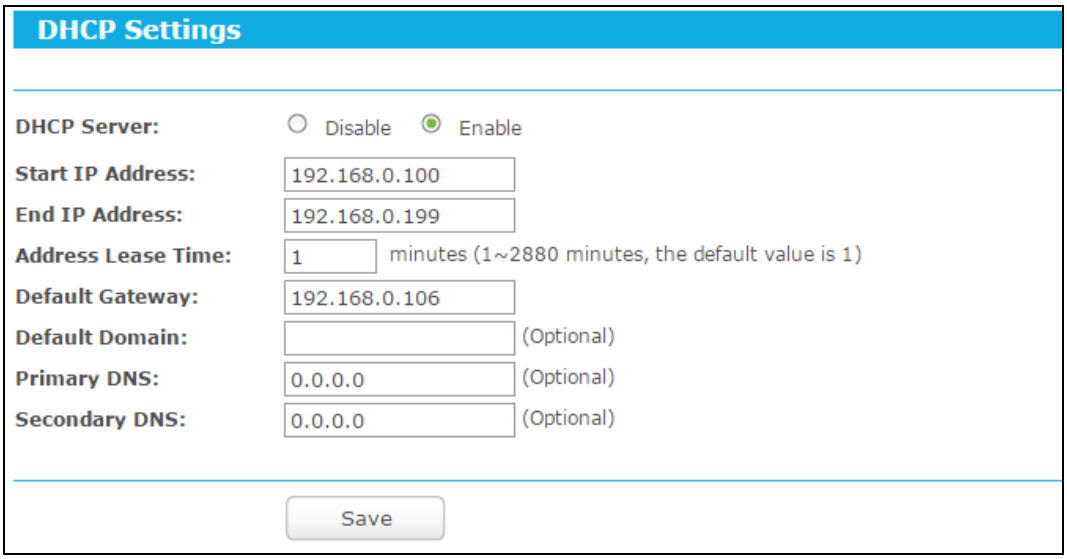
7.6 DHCP



There are three submenus under the DHCP menu, **DHCP Settings**, **DHCP Client List** and **Address Reservation.** Click any of them, and you will be able to configure the corresponding function.

7.6.1 DHCP Settings

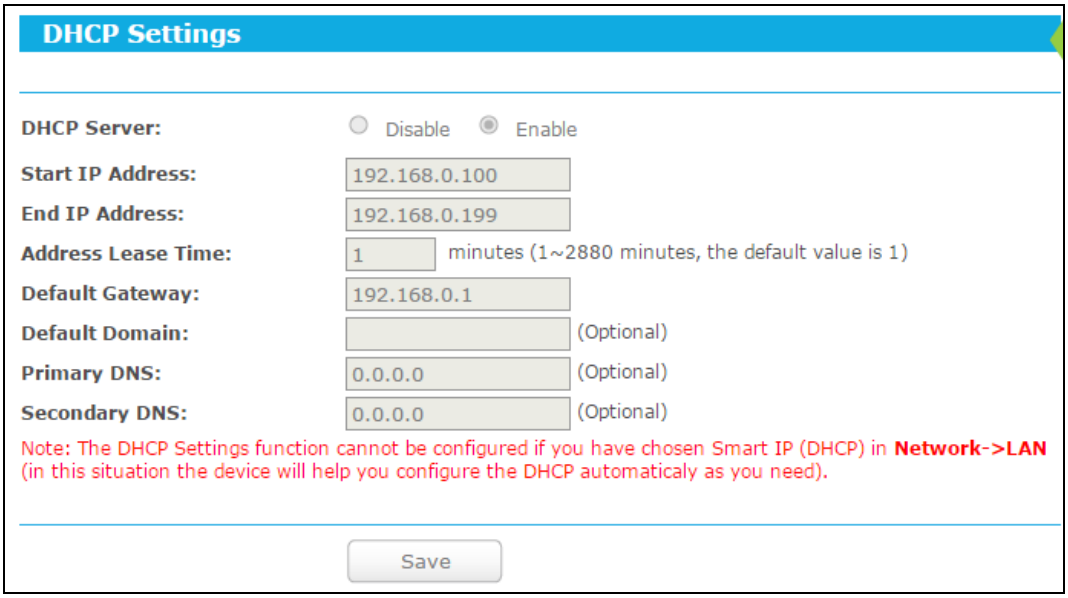
Choose menu "**DHCP → DHCP Settings**", and then you can configure the DHCP Server on the page as shown below. The Router is set up by default as a DHCP (Dynamic Host Configuration Protocol) server, which provides the TCP/IP configuration for all the PC(s) that are connected to the Router in the LAN.



- **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) **-** It is suggested to input the IP address of the LAN port of the Router. The 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.

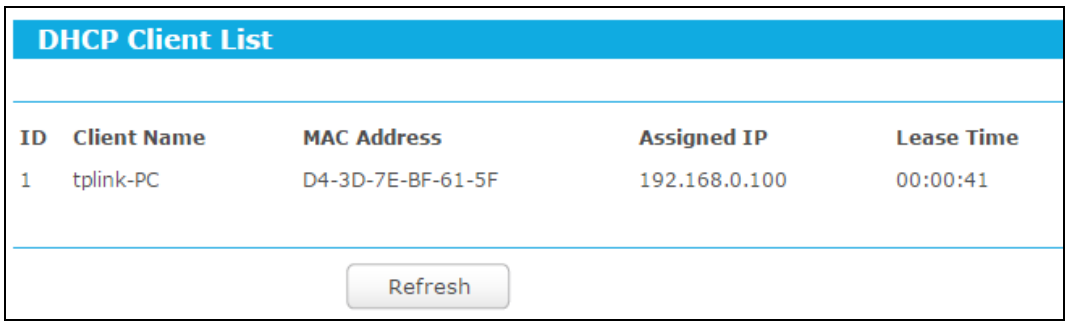
Note:

1. To use the DHCP server function of the Router, you must configure all computers on the LAN as "Obtain an IP Address automatically". This function will take effect until this device reboots.
2. When you choose the **Smart IP (DHCP)** mode in **Network → LAN**, the DHCP Server function will be disabled. You will see the page as below.



7.6.2 DHCP Client List

Choose menu "**DHCP → DHCP Client List**", and then you can view the information about the clients attached to the Router in the screen as shown below.

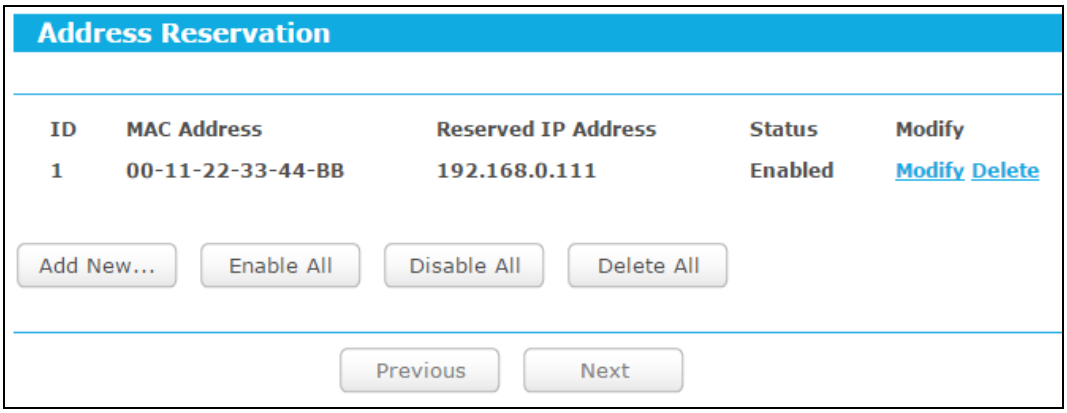


- **Client Name -** The name of the DHCP client.
- **MAC Address -** The MAC address of the DHCP client.
- **Assigned IP -** The IP address that the Router has allocated to the DHCP client.
- **Lease Time -** The time of the DHCP client leased. After the dynamic IP address has expired, a new dynamic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

7.6.3 Address Reservation

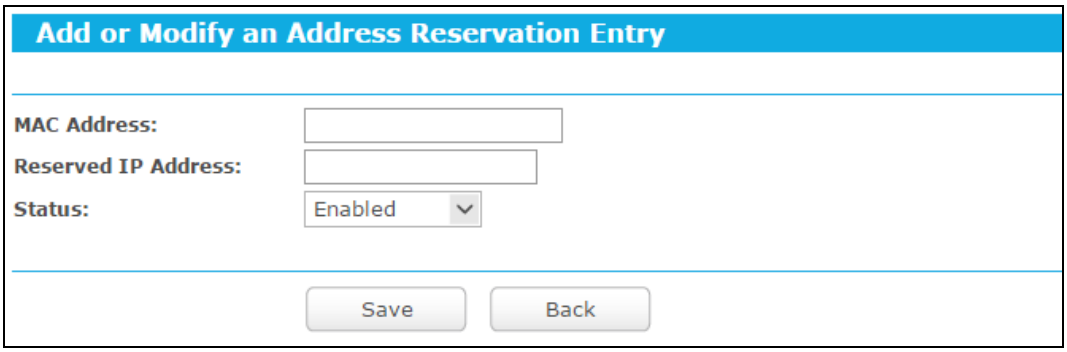
Choose menu "**DHCP → Address Reservation**", and then you can view and add a reserved address for clients via the next screen. When you specify a reserved IP address for a PC on the LAN, that PC will always receive the same IP address each time when it accesses the DHCP server. Reserved IP addresses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



- **MAC Address -** The MAC address of the PC for which you want to reserve an IP address.
- **Reserved IP Address -** The IP address reserved for the PC by the Router.
- **Status -** The status of this entry either **Enabled** or **Disabled**.
- **Modify -** To modify or delete an existing entry.

To Reserve an IP address:

1. Click the **Add New…** button.
2. Enter the MAC address (in XX-XX-XX-XX-XX-XX format.) and IP address (in dotted-decimal notation) of the computer for which you want to reserve an IP address.
3. Click the **Save** button.



To modify or delete an existing entry:

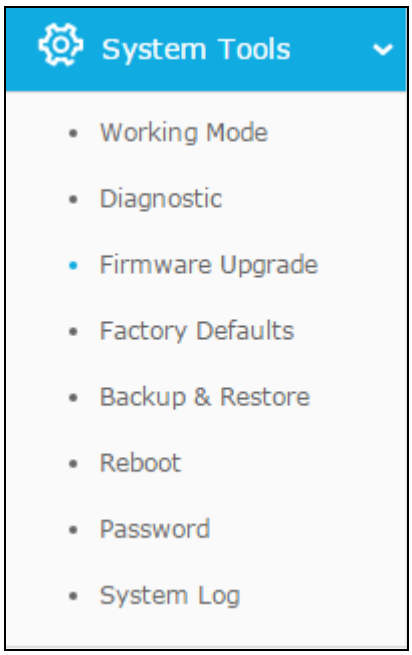
1. Click the **Modify** in the entry you want to modify. If you want to delete the entry, click the **Delete**.
2. Modify the information.
3. Click the **Save** button.

Click the **Enable/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.

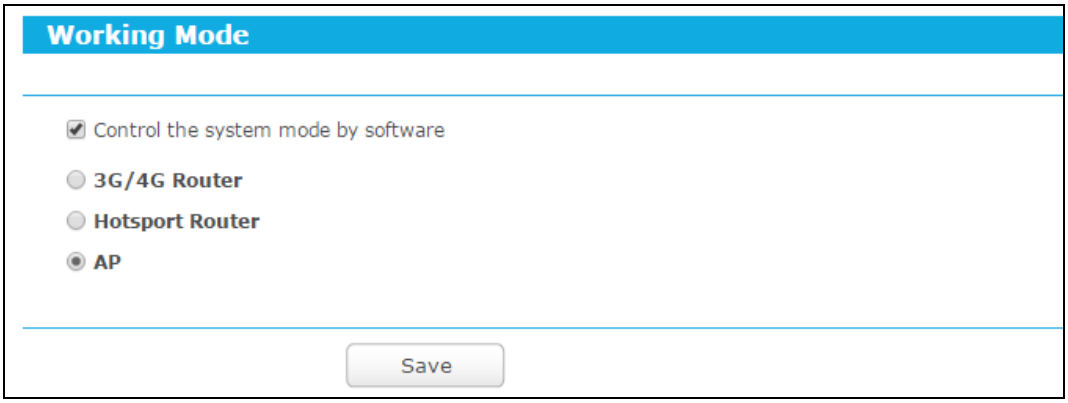
7.7 System Tools



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

7.7.1 Working Mode

Choose menu "**System Tools** → **Working Mode**", check **Control the system mode by software** and then you can see the following screen.



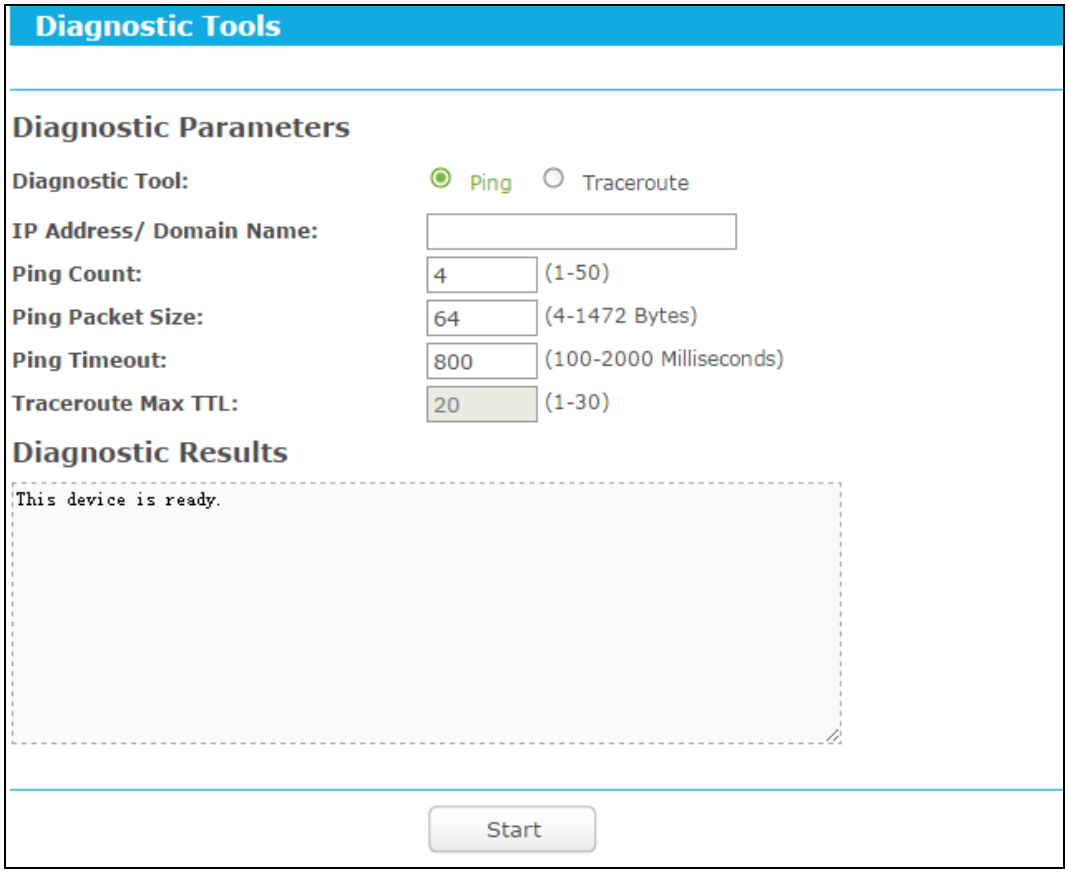
- **3G/4G Router -** This mode stands for Wireless Router Mode. It functions as a standard wireless router and you can also plug in a 3G/4G USB modem if you need.
- **Hotspot Router -** It functions as a hotspot router.
- **AP –** This mode stands for Access Point Mode, Repeater Mode and Client Mode. When

selected, you have to go to the **Quick Setup** to specify the mode you need.

Note: If **Control the system mode by software** is checked, the operation mode switch of the router will be disabled.

7.7.2 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.



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

Note:

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

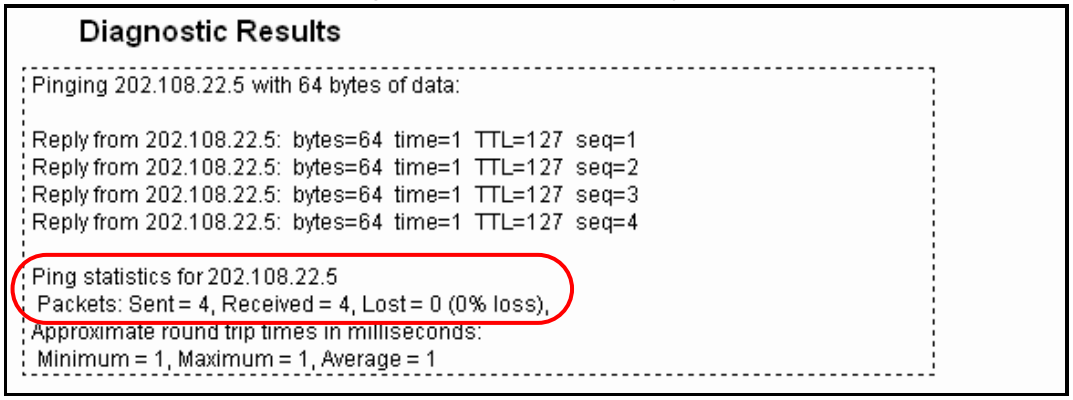
- **IP Address/Domain Name -** Type the destination IP address (e.g. 202.108.22.5) or Domain name (e.g. http://www.tp-link.com).
- **Pings Count -** The number of Ping packets for a Ping connection. The default is 4.

- **Ping Packet Size -** The size of Ping packet. The default is 64.
- **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. The default is 800.
- **Traceroute Max TTL -** The max number of hops for a Traceroute connection. 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.

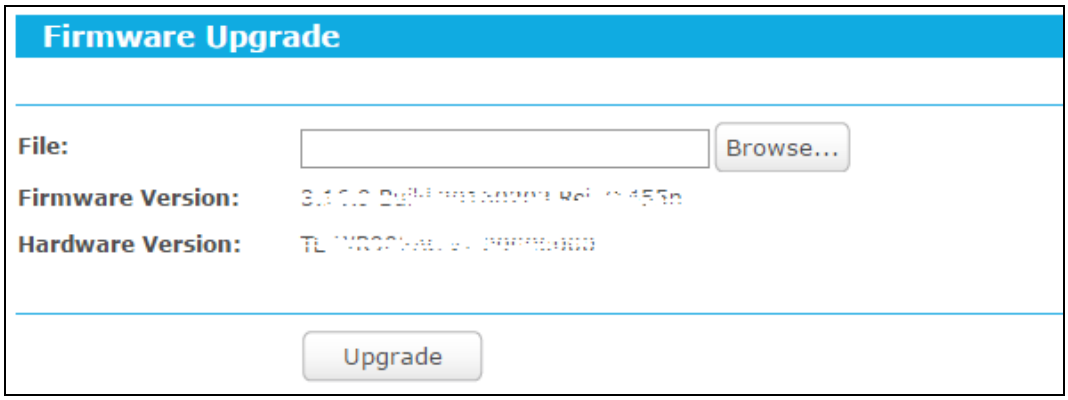


Note:

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.

7.7.3 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.



- **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:

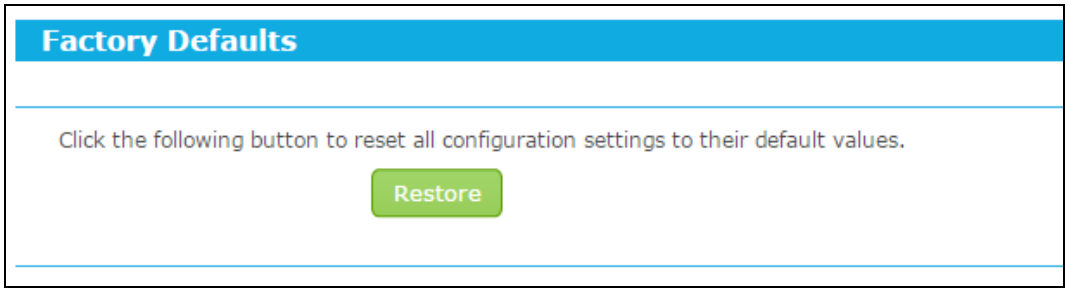
1. Download a more recent firmware upgrade file from the TP-LINK website (http://www.tp-link.com).
2. Type the path and file name of the update file into the **File** field, or click the **Browse** button to locate the update file.
3. Click the **Upgrade** button.

☞ **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.

7.7.4 Factory Defaults

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



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

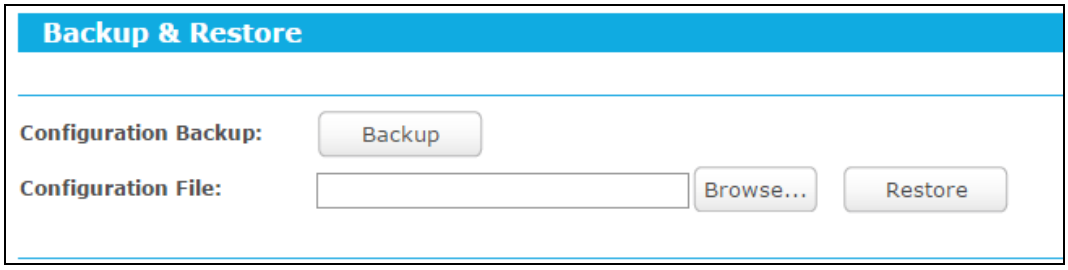
- The default User Name: admin
- The default Password: admin
- The default access: tplinkwifi.net

☞ **Note:**

All changed settings will be lost when defaults are restored.

7.7.5 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 below.



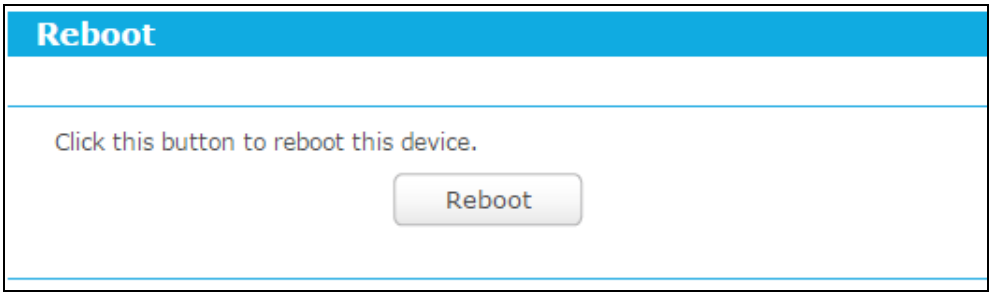
- Click the **Backup** button to save all configuration settings as a backup file in your local computer.
- To upgrade the Router's configuration, follow these instructions.
  - Click the **Browse…** button to locate the update file for the Router, or enter the exact path to the Setting file in the text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

7.7.6 Reboot

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



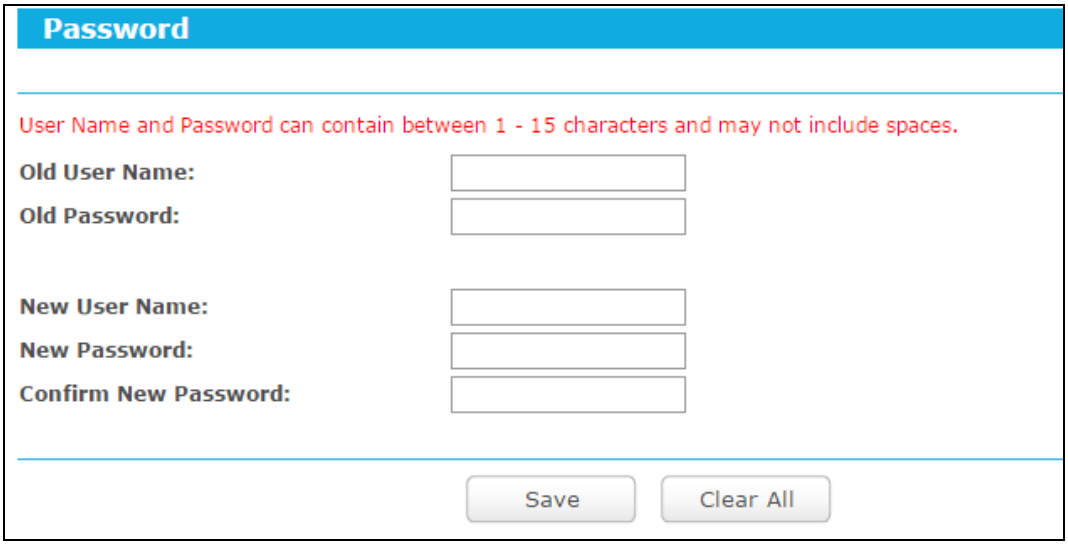
Some settings of the Router will take effect only after rebooting, which include:

- 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.

7.7.7 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 below.



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:

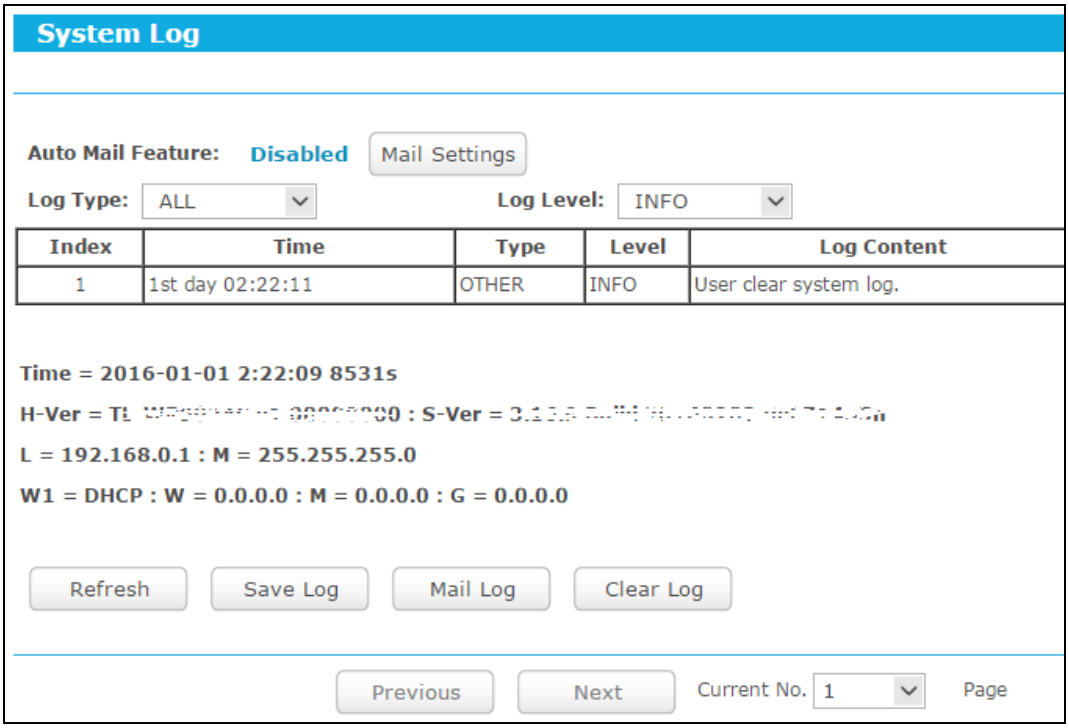
The new user name and password must not exceed 14 characters in length and not include any spaces. Enter the new Password twice to confirm.

Click the **Save** button when finished.

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

7.7.8 System Log

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



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

7.8 Logout

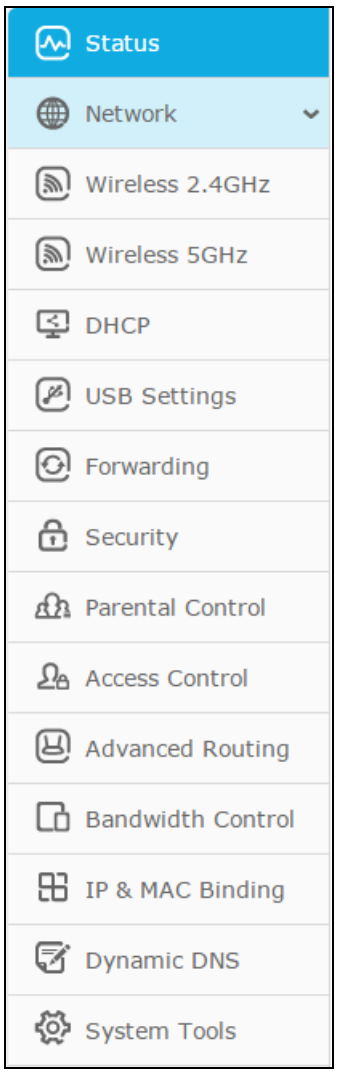
Click the **Logout** tab at the bottom of the main menu, and then the web-page will be logged out and return to the login window.

Chapter 8. Configuration for Hotspot Mode

This chapter will show each Web page's key functions and the configuration way for Hotspot Router Mode of TL-WR902AC.

8.1 Login

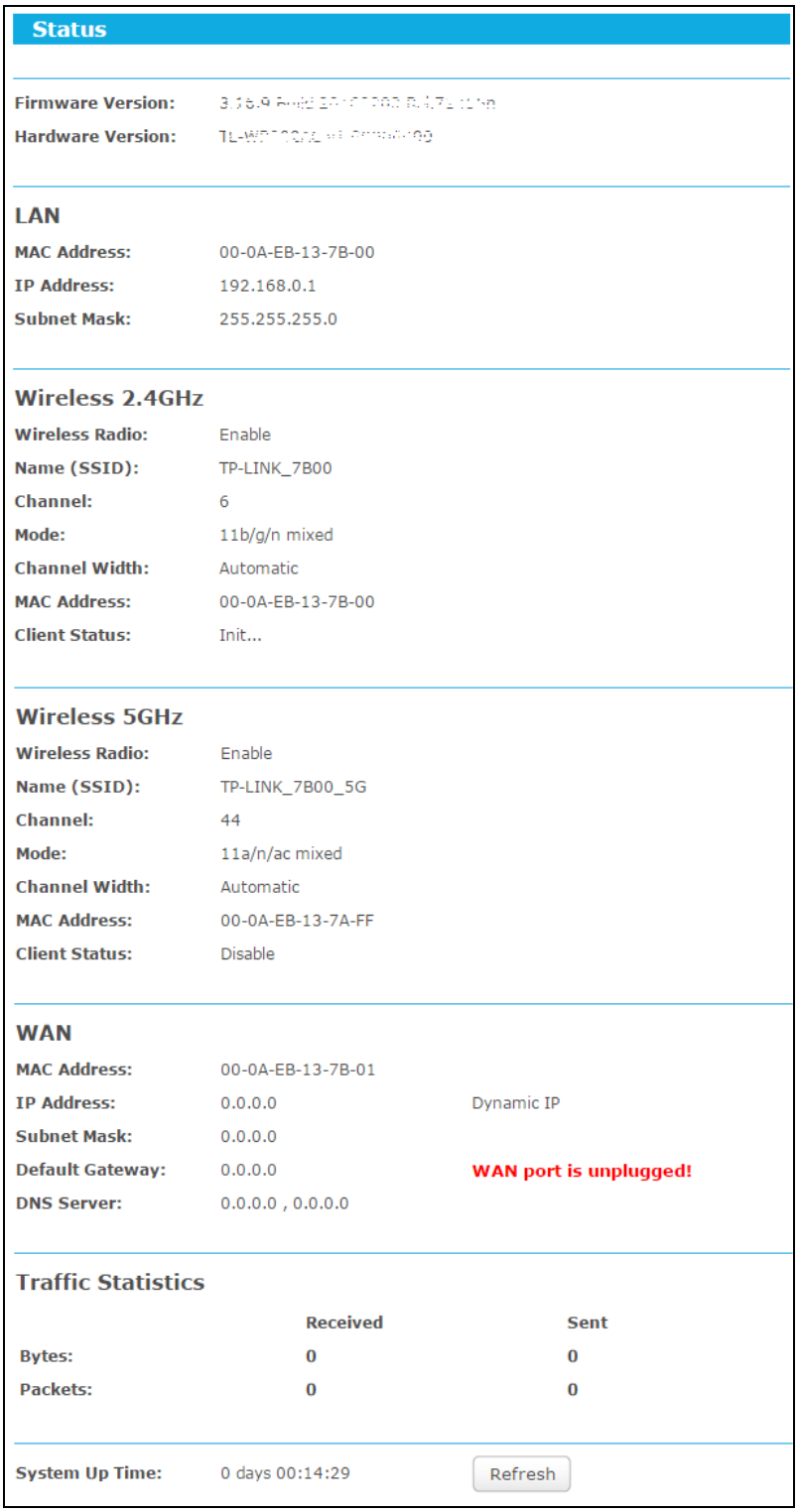
After your successful login, you can configure and manage the device. There are main menus on the left of the web-based utility. Submenus will be available after you click one of the main menus. On the right, there are the corresponding explanations and instructions.



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

8.2 Status

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



- **Firmware Version -** The version information of the Router's firmware.

- **Hardware Version -** The version information of the Router's hardware.
- **LAN -** This field displays the current settings or information for the LAN, you can configure them in the **Network > LAN** page.
  - **MAC Address -** The physical address of the Router, as seen from the LAN.
  - **IP Address -** The LAN IP address of the Router.
  - **Subnet Mask -** The subnet mask associated with LAN IP address.
- **Wireless -** This field displays basic information or status for wireless function, you can configure them in the **Wireless > Wireless Settings** page.
  - **Operation Mode -** The current wireless working mode in use.
  - **Wireless Radio -** Indicates whether the wireless radio feature of the AP is enabled or disabled.
  - **Name (SSID) -** The SSID of the router.
  - **Channel -** The current wireless channel in use.
  - **Mode -** The current wireless mode which the Router works on.
  - **Channel Width -** The current wireless channel width in use.
  - **MAC Address -** The physical address of the Router, as seen from the WLAN.
  - **Client Status -** The status of Client.
- **WAN -** This field displays the current settings or information for the WAN, you can configure them in the **Network > WAN** page.
  - **MAC Address -** The physical address of the WAN port, as seen from the Internet.
  - **IP Address -** The current WAN (Internet) IP Address. This field will be blank or 0.0.0.0 if the IP Address is assigned dynamically and there is no connection to the Internet.
  - **Subnet Mask -** The subnet mask associated with the WAN IP Address.
  - **Default Gateway -** The Gateway currently used by the Router is shown here. When you use **Dynamic IP** as the connection Internet type, the **Renew** button will be displayed here. Click the **Renew** Button to obtain new IP parameters dynamically from the ISP. And if you have got an IP address, **Release** button will be displayed here. Click the **Release** button to release the IP address the Router has obtained from the ISP.
  - **DNS Server** - The DNS (Domain Name System) server IP addresses currently used by the Router.
  - **Online Time** - The time that you online. When you use **PPPoE** as WAN connection type, the online time is displayed here. Click the **Connect** or **Disconnect** button to connect to or disconnect from Internet.

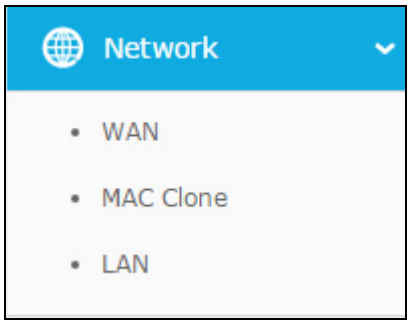
- **Secondary Connection -** Besides PPPoE, if you use an extra connection type to connect to a local area network provided by ISP, then parameters of this secondary connection will be shown in this area.
  - **IP Address -** The current WAN (Internet) IP Address. This field will be blank or 0.0.0.0 if the IP Address is assigned dynamically and there is no connection to the Internet.
  - **Subnet Mask -** The subnet mask associated with the WAN IP Address.

Click the **Release** to delete the network parameters, and click the **Renew** button to obtaining network parameters.

- **Traffic Statistics -** The Router's traffic statistics.
  - **Received (Bytes) -** Traffic that counted in bytes has been received out from the WAN port.
  - **Received (Packets) -** Traffic that counted in packets has been received out from the WAN port.
  - **Sent (Bytes) -** Traffic that counted in bytes has been sent out from the WAN port.
  - **Sent (Packets) -** Traffic that counted in packets has been sent out from the WAN port.
- **System Up Time -** The length of the time since the Router was last powered on or reset.

Click the **Refresh** button to get the latest status and settings of the Router.

8.3 Network

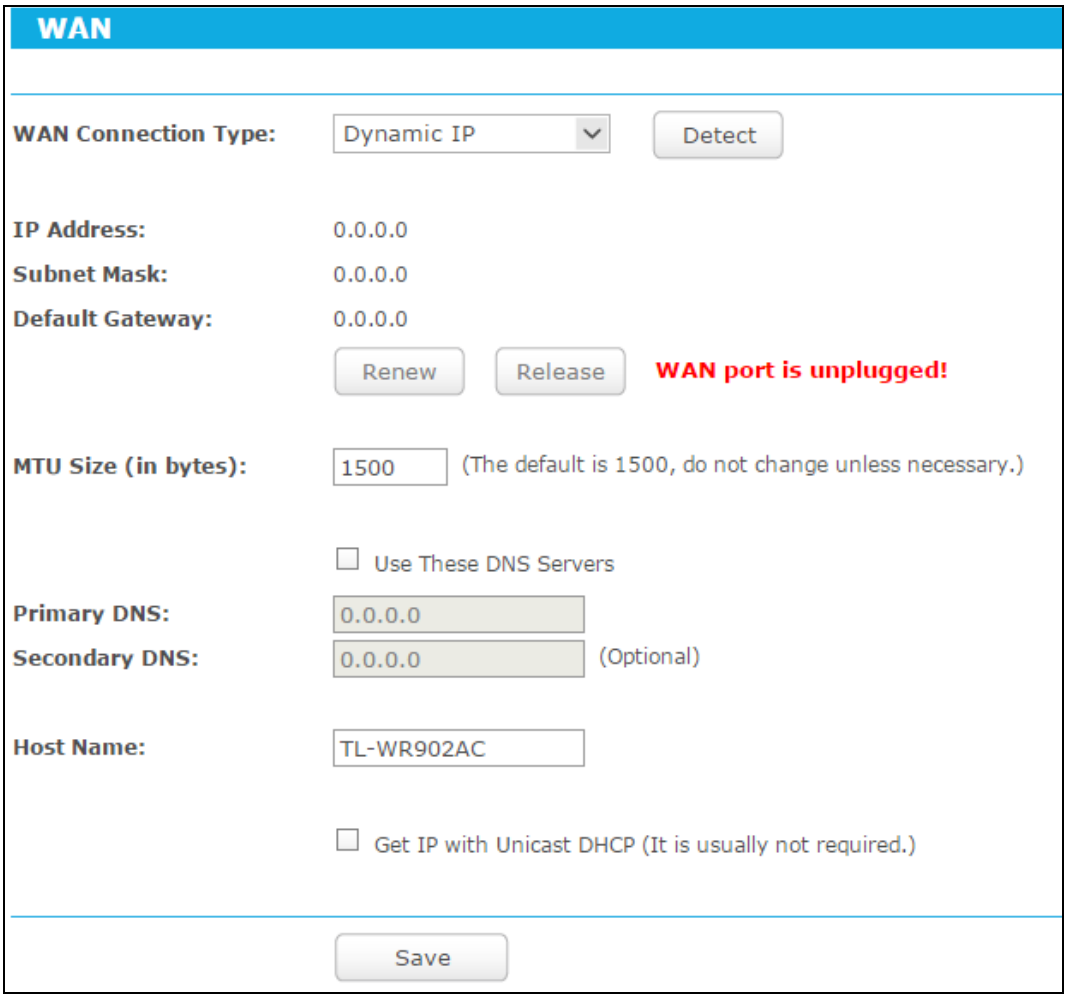


There are three submenus under the Network menu: **WAN**, **MAC Clone** and **LAN**. Click any of them, and you will be able to configure the corresponding function.

8.3.1 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 below:



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.

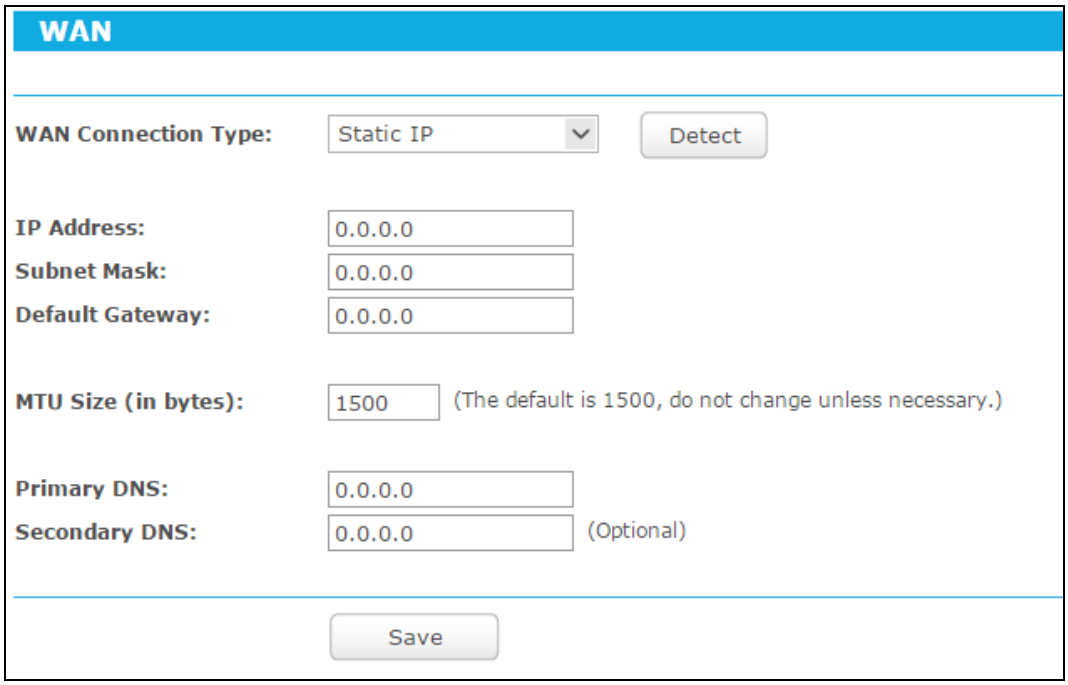
Note:

If you find error when you go to a website 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.

- **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.)

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

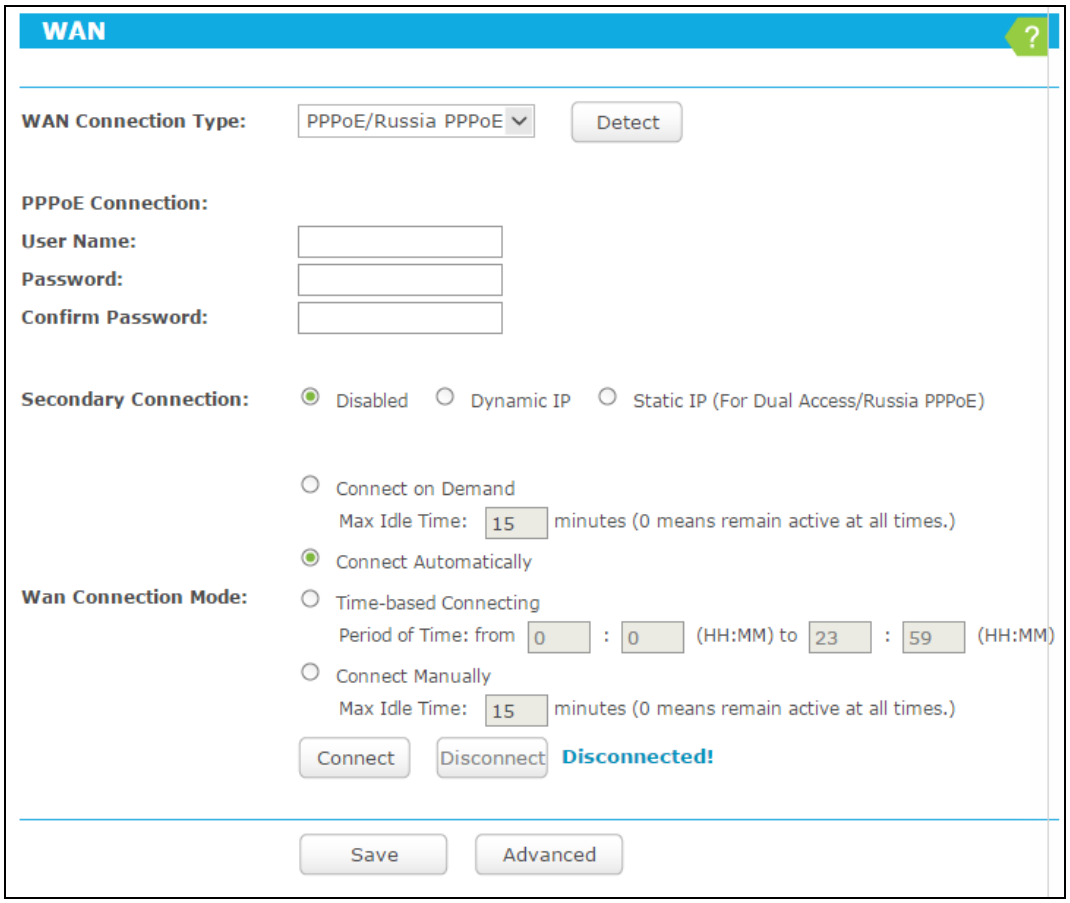
2. If your ISP provides a static or fixed **IP Address**, **Subnet Mask**, **Default Gateway** and **DNS** setting, select **Static IP**. The Static IP settings page will appear as shown below.



- **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 -** 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.

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

3. If your ISP provides a PPPoE connection, select **PPPoE/Russia PPPoE** option. Then you should enter the following parameters:



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

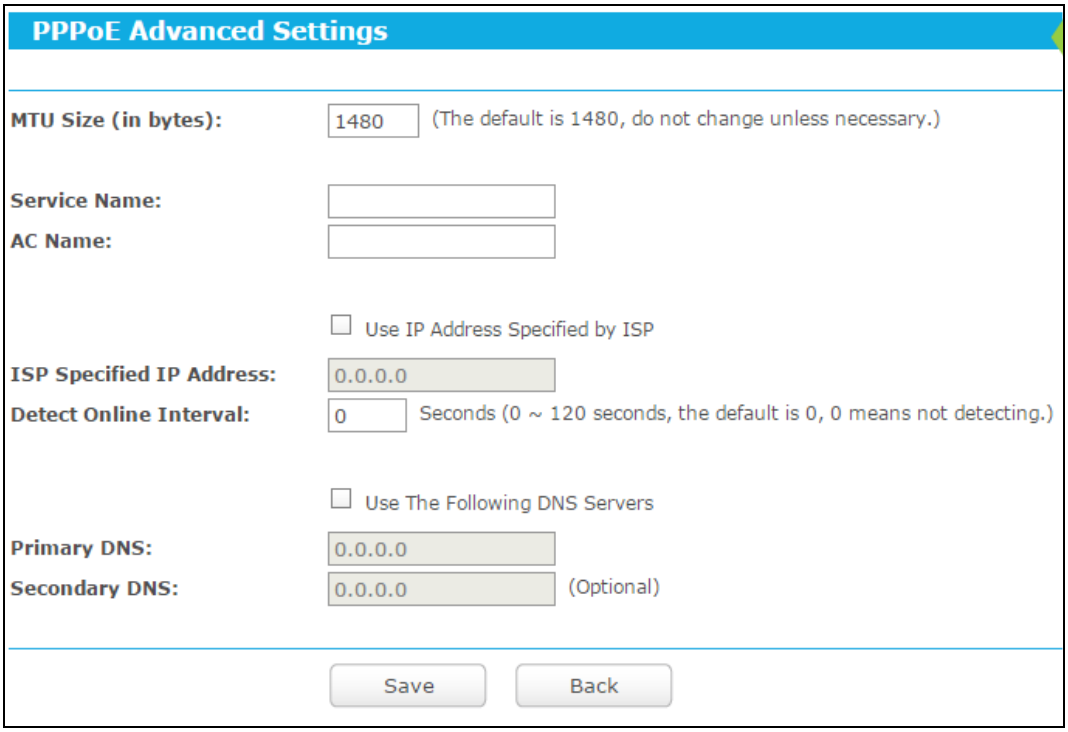
  Only when you have configured the system time on "**System Tools** → **Time**" page, will the **Time-based Connecting** function can take effect.

- **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.

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.

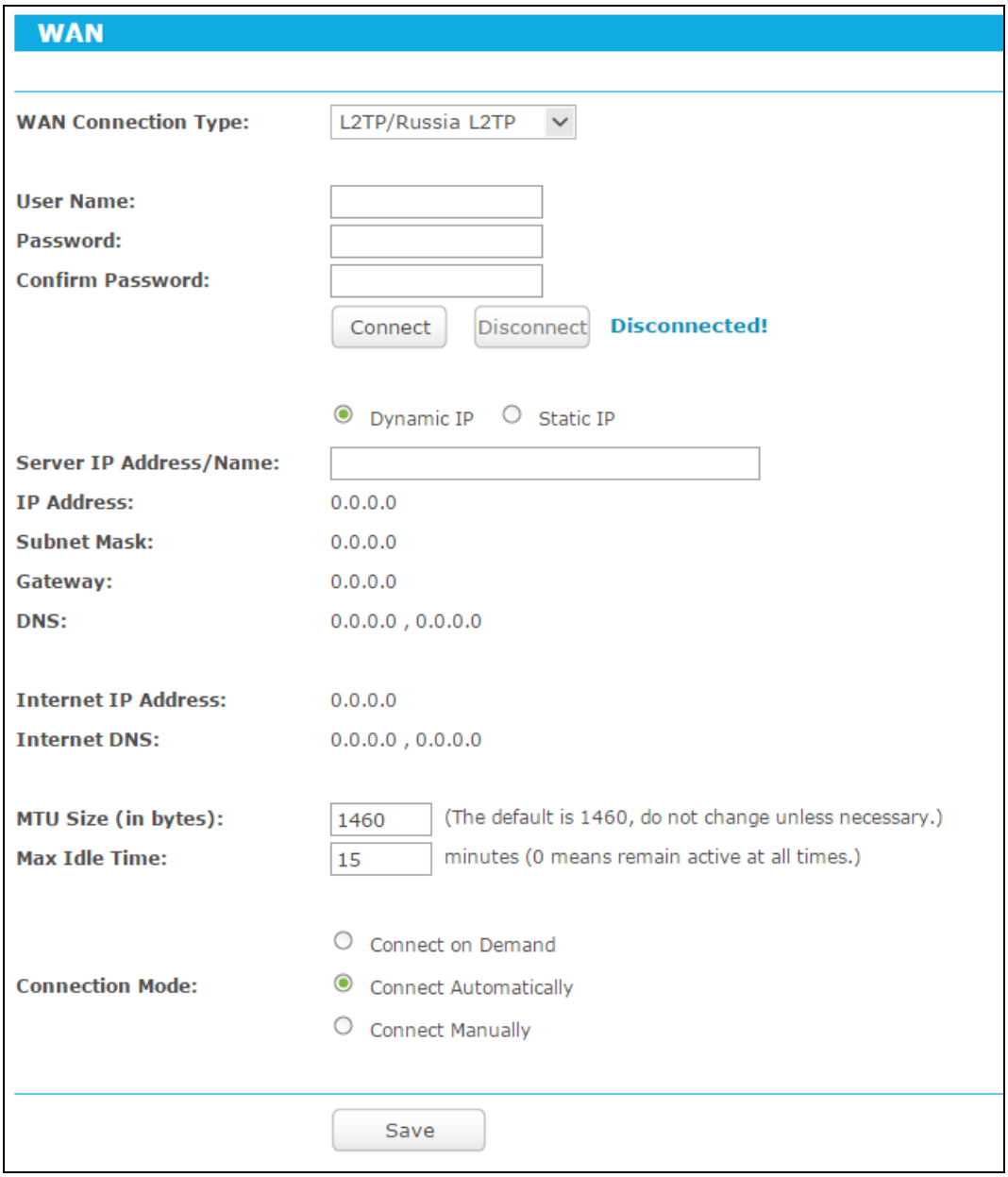
If you want to do some advanced configurations, please click the **Advanced** button, and the page shown below will then appear:



- **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 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.
- **Primary DNS/Secondary DNS -** 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 L2TP connection, please select **L2TP/Russia L2TP** option. Then you should enter the following parameters:



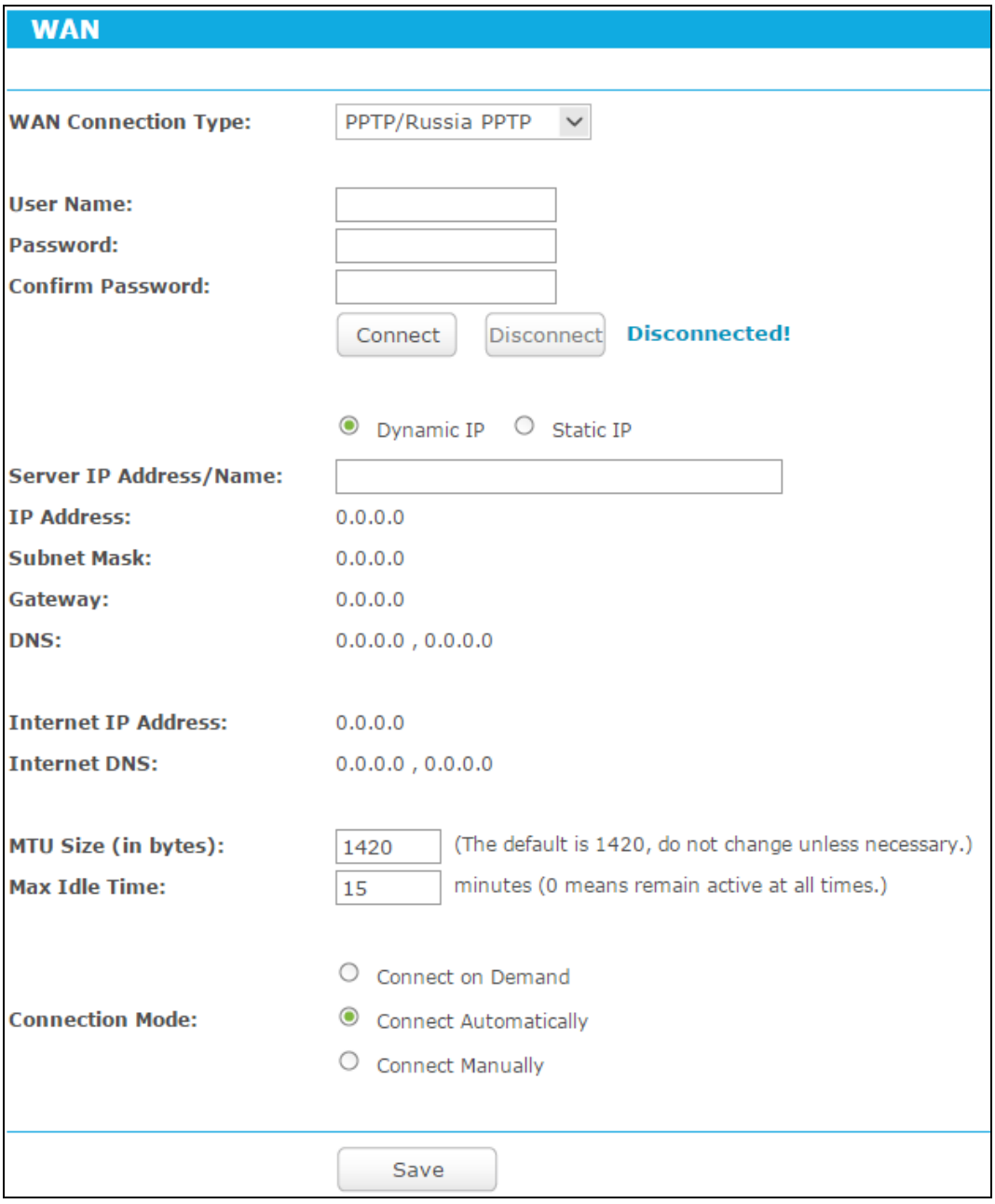
- **User Name/Password -** Enter the User Name and Password provided by your ISP. These fields are case-sensitive.
- **Dynamic IP/ Static IP -** Choose either as you are given by your ISP. Click the **Connect** button to connect immediately. Click the **Disconnect** button to disconnect immediately.
- **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**, check the radio button. If you want your Internet connection to remain active at all times, enter 0 in the **Max Idle Time** field. Otherwise, enter the number of minutes you want to have elapsed before your Internet connection terminates.

- **Connect Automatically -** Connect automatically after the Router is disconnected. To use this option, check 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, check the radio button. If you want your Internet connection to remain active at all times, enter "0" in the **Max Idle Time** field. Otherwise, enter the number of minutes 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**, because some applications are visiting the Internet continually in the background.

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

5. If your ISP provides PPTP connection, please select **PPTP/Russia PPTP** option. And you should enter the following parameters:



- **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**, check the radio button. If you want your Internet connection to remain active at all times, enter “0” in the **Max Idle Time** field. Otherwise, enter the number of minutes you want to have elapsed before your Internet connection terminates.

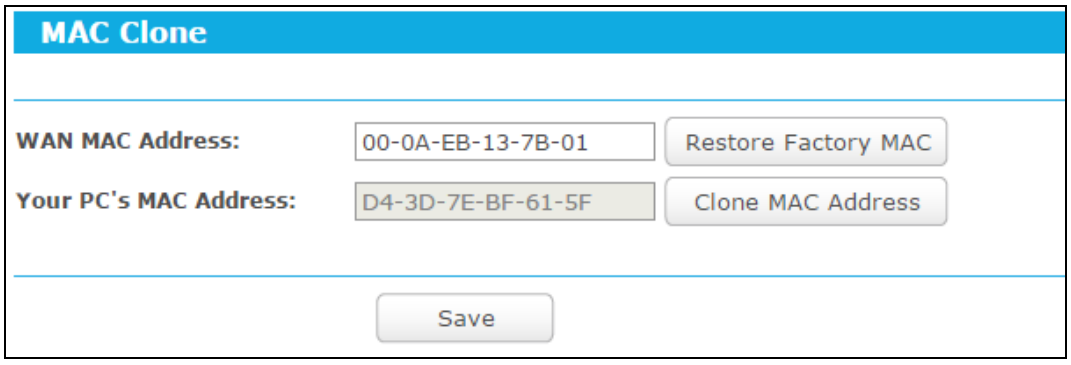
- **Connect Automatically -** Connect automatically after the Router is disconnected. To use this option, check the radio button.
- **Connect Manually -** You can configure the Router to make it connect or disconnect manually. After a specified period of inactivity (**Max Idle Time**), the Router will 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** because some applications are visiting the Internet continually in the background.

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

8.3.2 MAC Clone

Choose menu “**Network → MAC Clone**”, and then you can configure the WAN MAC address on the screen below:



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.

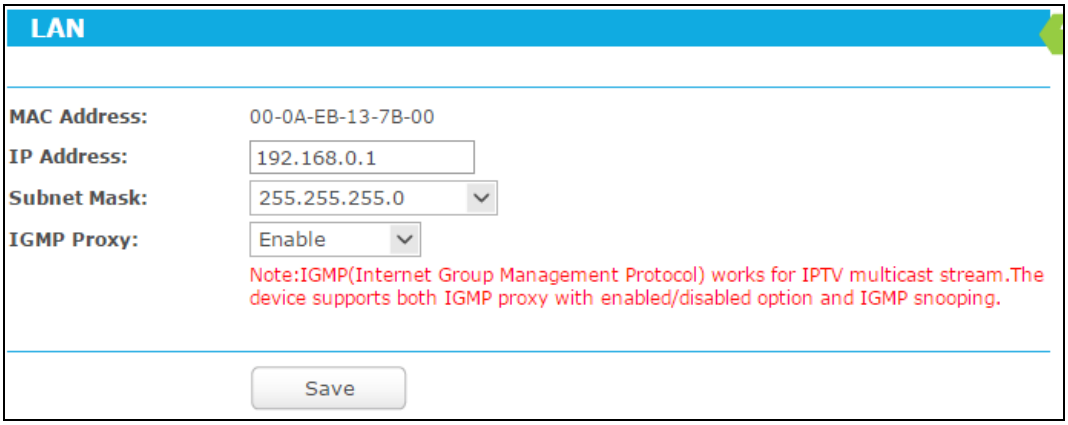
Click **Save**.

Note:

1. Only the PC on your LAN can use the **MAC Address Clone** function.
2. If you change WAN MAC Address when the WAN connection is PPPoE, it will not take effect until the connection is re-established.

8.3.3 LAN

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

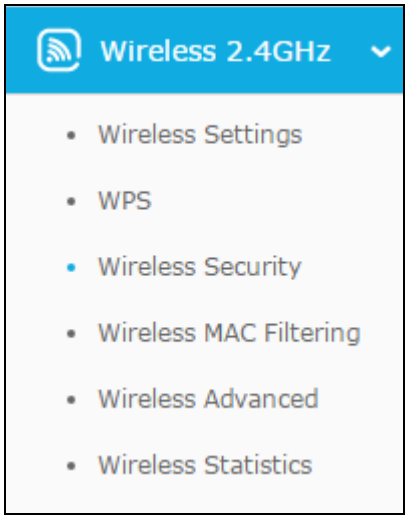


- **MAC Address -** The physical address of the LAN ports, as seen from the LAN. The value can't be changed.
- **IP Address -** Enter the IP address of your Router in dotted-decimal notation (factory default: 192.168.0.1).
- **Subnet Mask -** An address code that determines the size of the network. Normally use 255.255.255.0 as the subnet mask.
- **IGMP Proxy** - The Internet Group Management Protocol (IGMP) feature allows your devices in LAN can watch TV.

Note:

1. If you change the IP Address of LAN, you must use the new IP Address to login to the Router.
2. If the new LAN IP Address you set is not in the same subnet with the previous one, the IP Address pool in the DHCP server will be configured automatically, while the Virtual Server and DMZ Host will not take effect until they are re-configured.

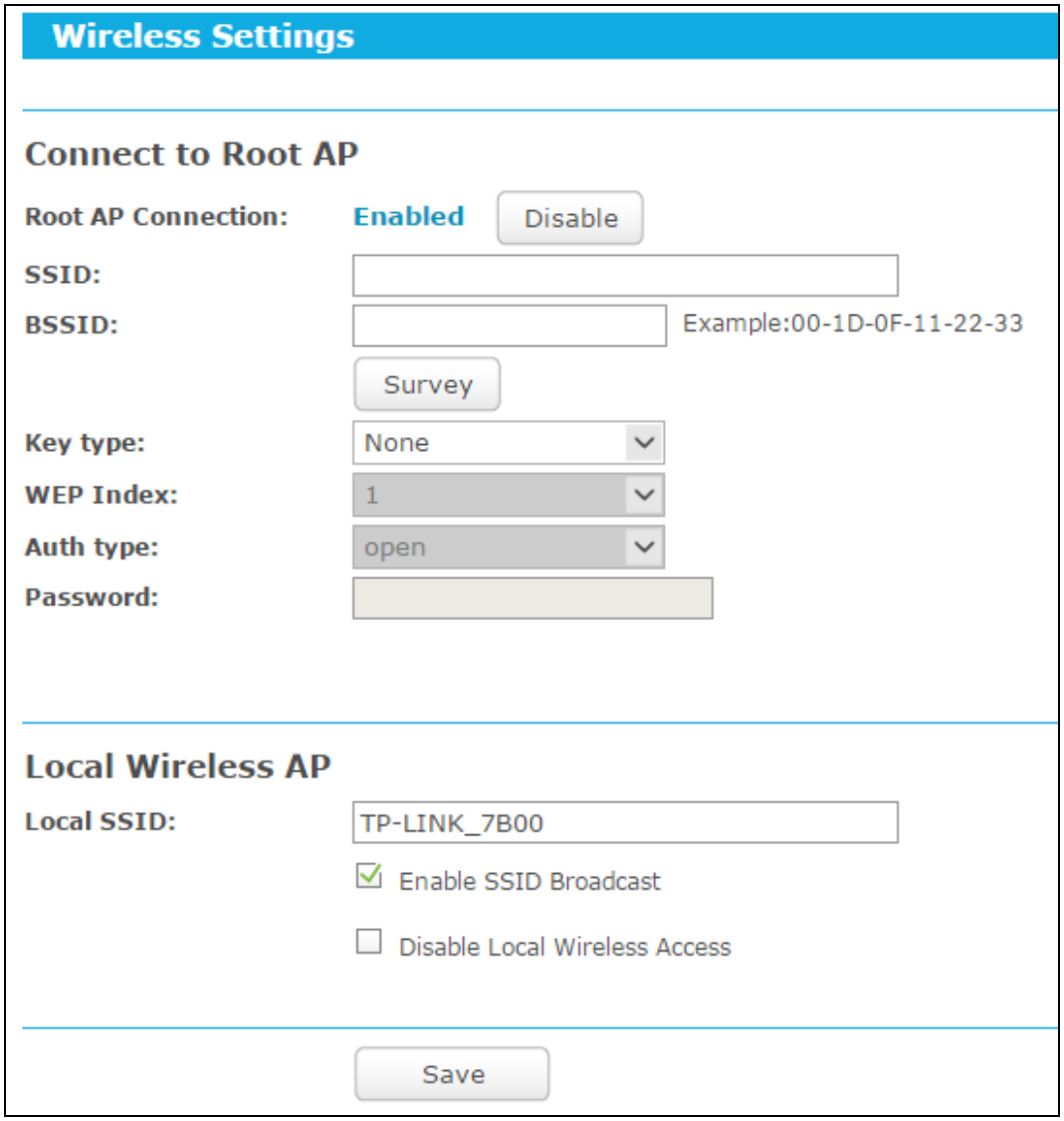
8.4 Wireless 2.4GHz/5GHz



There are six submenus under the Wireless menu: **Wireless Settings**, **WPS**, **Wireless Security**, **Wireless MAC Filtering**, **Wireless Advanced** and **Wireless Statistics**. Click any of them, and you will be able to configure the corresponding function.

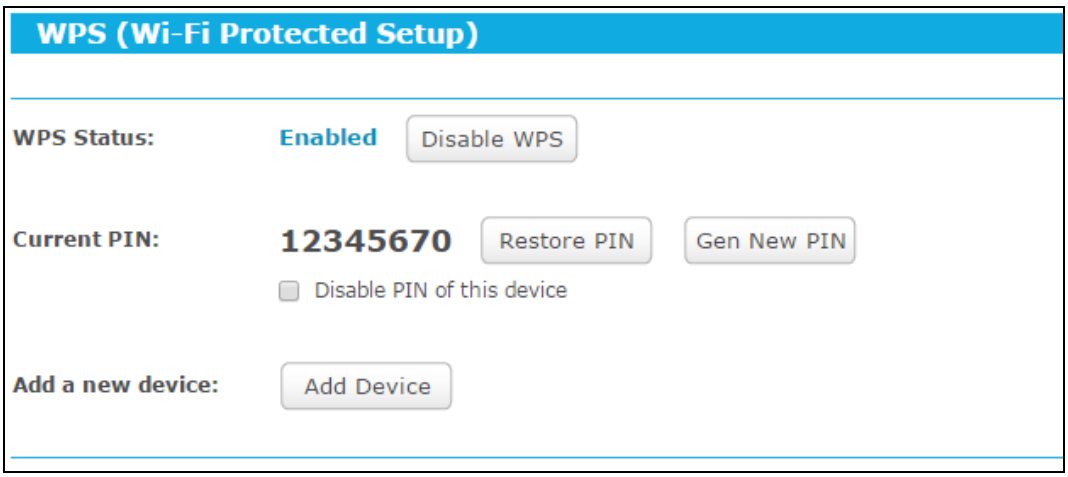
8.4.1 Wireless Settings

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



8.4.2 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. Select menu "**WPS**", you will see the next screen shown below.



- **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.
- **Disable PIN of this Device -** WPS external registrar of entering the device's PIN can be disabled or enabled manually. If the device receives multiple failed attempts to authenticate an external Registrar, this function will be disabled automatically.
- **Add Device -** You can add 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.

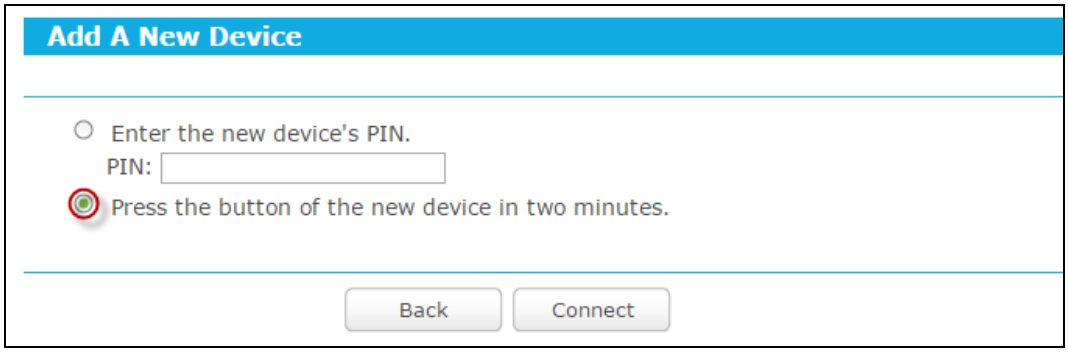
For the configuration of the new device, here takes the Wireless Adapter of our company for example.

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: Keep the WPS Status as **Enabled** and click the **Add Device** button, then the following screen will appear.



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

Step 3: For the configuration of the wireless adapter, please choose "**Push the button on my access point or wireless router**" in the configuration utility of the WPS as below, and click **Connect**.

The WPS Configuration Screen of Wireless Adapter

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

The WPS Configuration Screen of Wireless Adapter

Method Two: Enter the PIN into my AP

Step 1: For the configuration of the wireless adapter, please choose "**Enter the PIN of this device into my access point or wireless router**" in the configuration utility of the WPS as below, and click **Connect**.

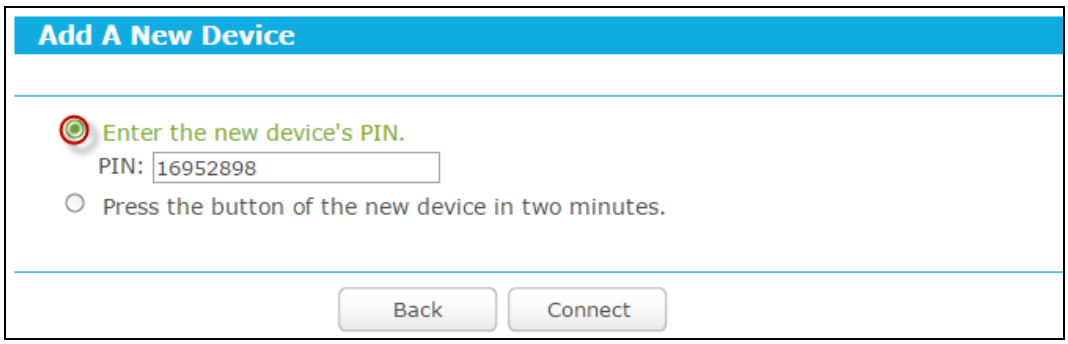
The WPS Configuration Screen of Wireless Adapter

Note:

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

Step 2: Keep the WPS Status as **Enabled** and click the **Add Device** button.

Step 3: Choose "**Enter the new device's PIN**" and enter the PIN code （take 16952898 for example） of the wireless adapter in the field after **PIN** as shown in the figure below. Then click **Connect**.



Method Three: Enter the PIN from my AP.

Step 1: Get the Current PIN code of the AP (each AP has its unique PIN code. Here takes the PIN code 12345670 of this AP for example).

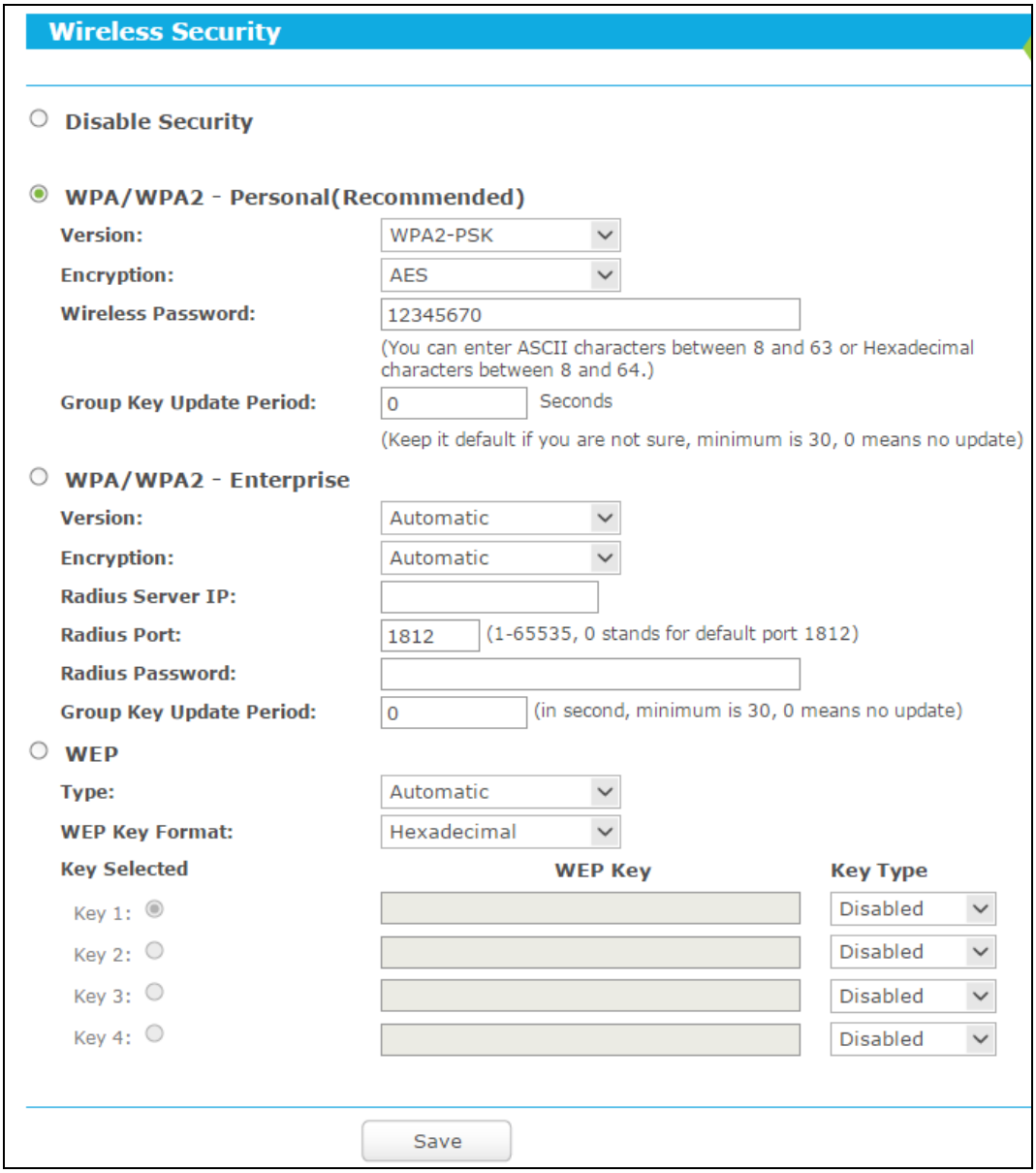
Step 2: For the configuration of the wireless adapter, please choose "**Enter the PIN of my access point or wireless router**" in the configuration utility of the WPS as below, and enter the PIN code of the AP into the field after "**Access Point PIN**". Then click **Connect**.

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.

8.4.3 Wireless Security



- **Disable Security -** The wireless security function can be enabled or disabled. If disabled, the wireless stations will be able to connect the Router without encryption. But it's strongly recommended to choose one of the following modes to enable security.

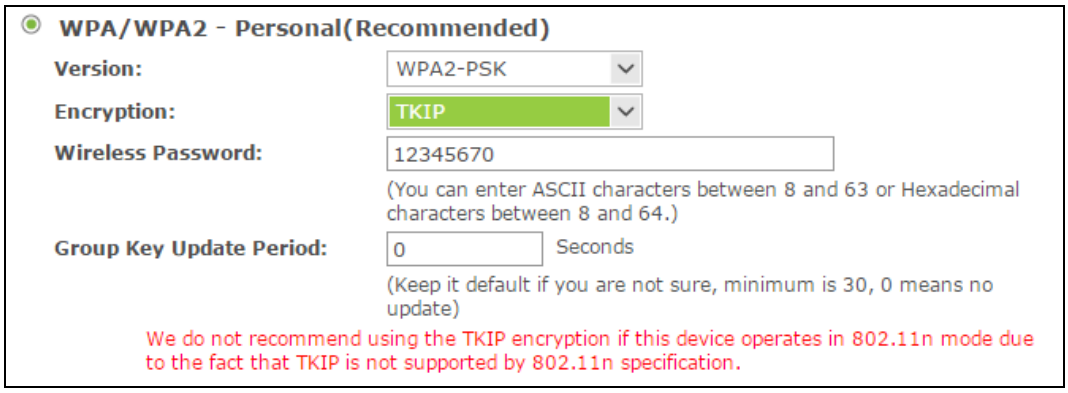
- **WPA-PSK/WPA2-Personal -** It's the WPA/WPA2 authentication type based on pre-shared passphrase.

  - **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** radio button and choose TKIP encryption, you will find a notice in red as shown below.



- **WPA /WPA2-Enterprise -** It's based on Radius Server.
  - **Version -** you can choose the version of the WPA security from 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 **Automatic**, **TKIP** or **AES**.
  - **Radius Server IP -** Enter the IP address of the Radius server.
  - **Radius Port -** Enter the port that Radius server 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.
  - **Type -** you can choose the type for the WEP security on the pull-down list. The default setting is **Automatic**, which can select **Shared Key** or **Open System** authentication type automatically based on the wireless station's capability and request.
  - **WEP Key Format - Hexadecimal** and **ASCII** formats are provided here. **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 (Password) -** 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.

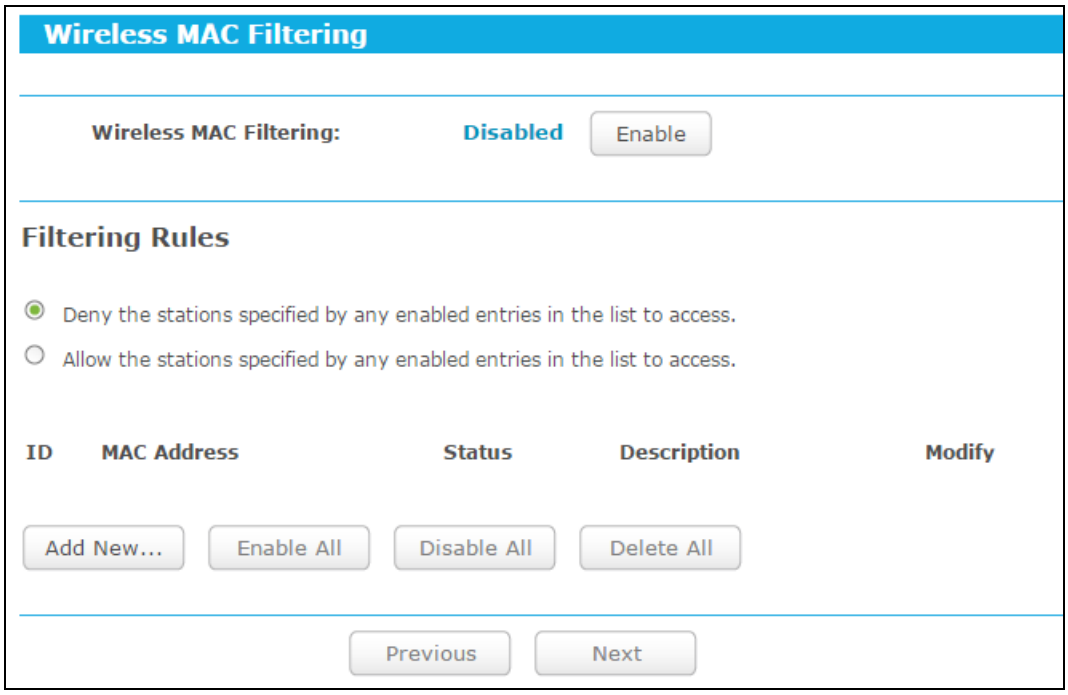
Note:

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

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

8.4.4 Wireless MAC Filtering

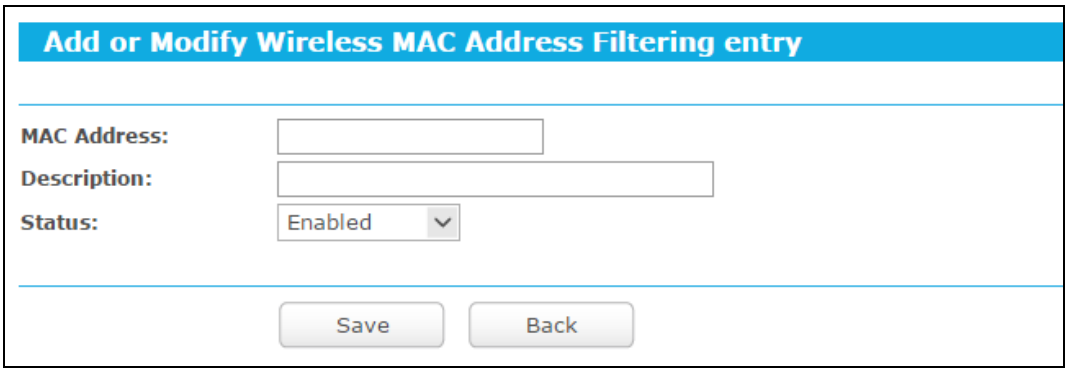
Choose menu "**Wireless → Wireless MAC Filtering**", and then you can control the wireless access by configuring the **Wireless MAC Filtering** function as shown below.



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 access.
- **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:



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

1. Enter the appropriate MAC Address into the **MAC Address** field. The format of the MAC Address is XX-XX-XX-XX-XX-XX (X is any hexadecimal digit). For example: 00-0A-EB-B0-00-0B.
2. Give a simple description for 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 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.

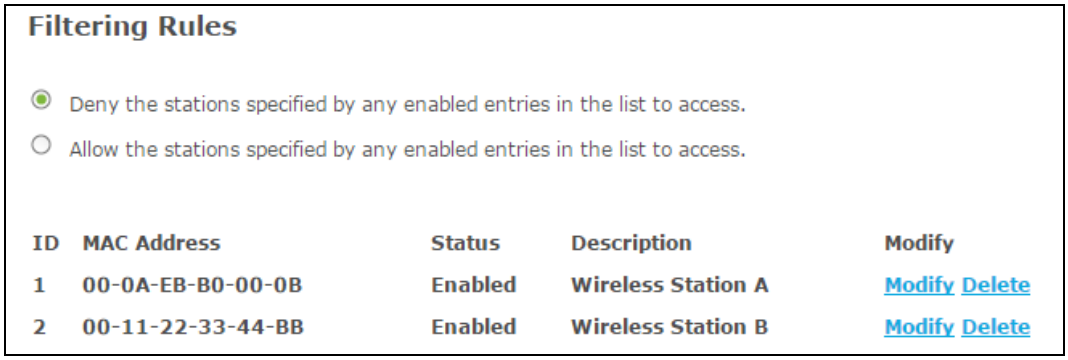
For example: If you desire that the wireless station A with MAC address 00-0A-EB-B0-00-0B and the wireless station B with MAC address 00-0A-EB-00-07-5F are able to access the Router, but all the other wireless stations cannot access the Router, you can configure the **Wireless MAC Address Filtering** list by following these steps:

1. Click the **Enable** button to enable this function.
2. Select the radio button “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.

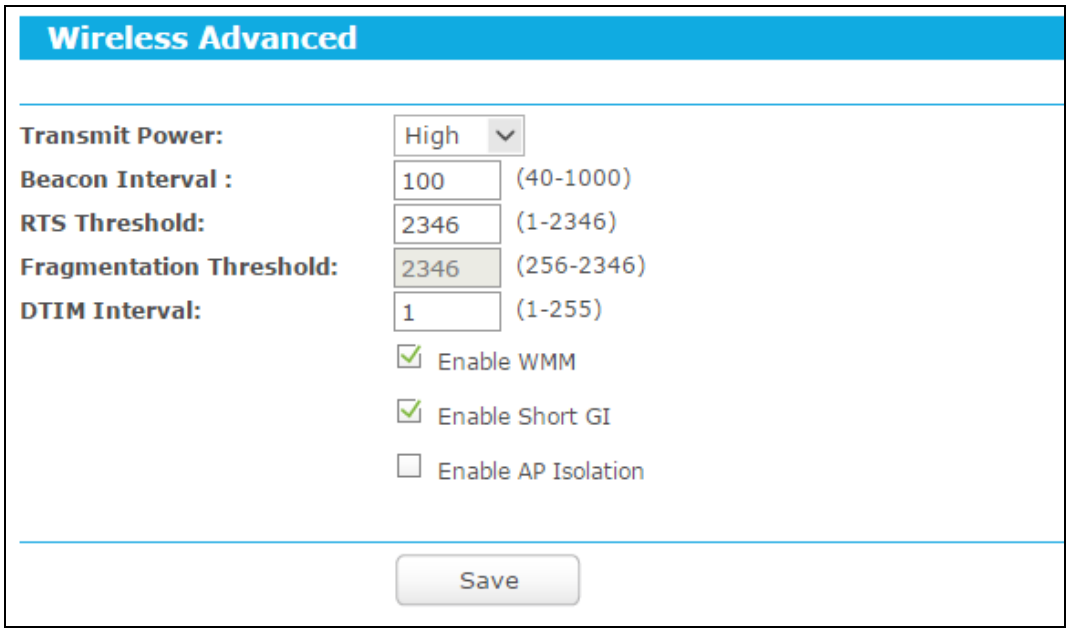
   1) Enter the MAC address 00-0A-EB-B0-00-0B/00-0A-EB-00-07-5F in the **MAC Address** field.
   2) Enter wireless station A/B in the **Description** field.
   3) Select **Enabled** in the **Status** pull-down list.
   4) Click the **Save** button.
   5) Click the **Back** button.

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



8.4.5 Wireless Advanced

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



- **Transmit Power -** Here you can specify the transmit power of Router. You can select High, Middle or Low which you would like. High is the default setting and is recommended.
- **Beacon Interval -** Enter a value between 20-1000 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.

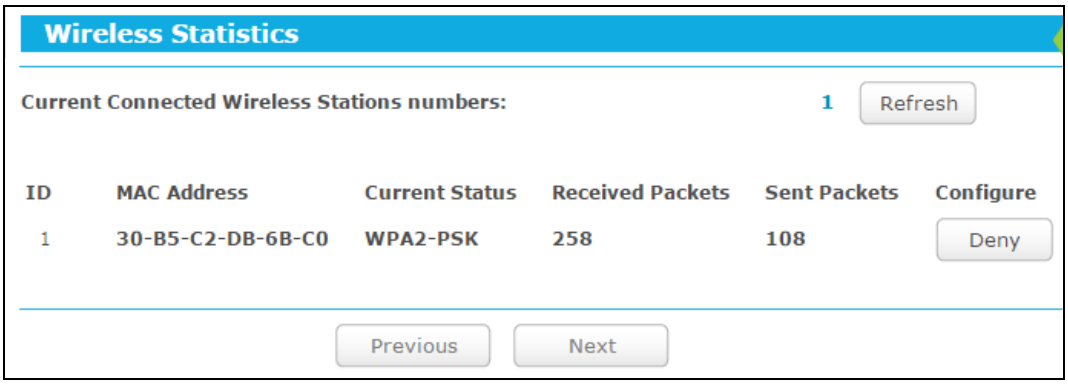
- **RTS Threshold -** Here you can specify the RTS (Request to Send) Threshold. If the packet is larger than the specified RTS Threshold size, the Router will send RTS frames to a particular receiving station and negotiate the sending of a data frame. The default value is 2346.
- **Fragmentation Threshold -** This value is the maximum size determining whether packets will be fragmented. Setting the Fragmentation Threshold too low may result in poor network performance because of 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.
- **Enable AP Isolation -** This function isolate all connected wireless stations so that wireless stations cannot access each other through WLAN. This function will be disabled if WDS/Bridge is enabled.

Note:

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

8.4.6 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.



- **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.
- **Configure -** The button is used for loading the item to the **Wireless MAC Filtering** list.
  - **Allow -** If the **Wireless MAC Filtering** function enable, allow the station to access.
  - **Deny -** If the **Wireless MAC Filtering** function enable, deny the station to access.

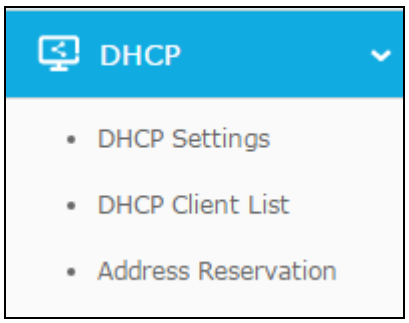
You cannot change any of the values on this page. To update this page and to show the current connected wireless stations, click on the **Refresh** button.

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.

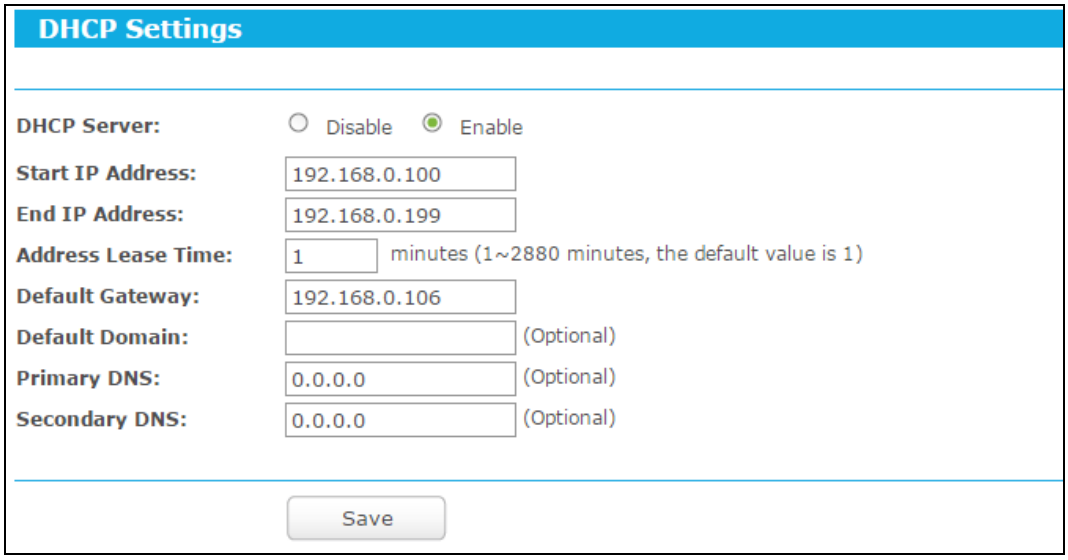
8.5 DHCP



There are three submenus under the DHCP menu: **DHCP Settings**, **DHCP Client List** and **Address Reservation**. Click any of them, and you will be able to configure the corresponding function.

8.5.1 DHCP Settings

Choose menu "**DHCP → DHCP Settings**", and then you can configure the DHCP Server on the page as shown below. 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 in the LAN.



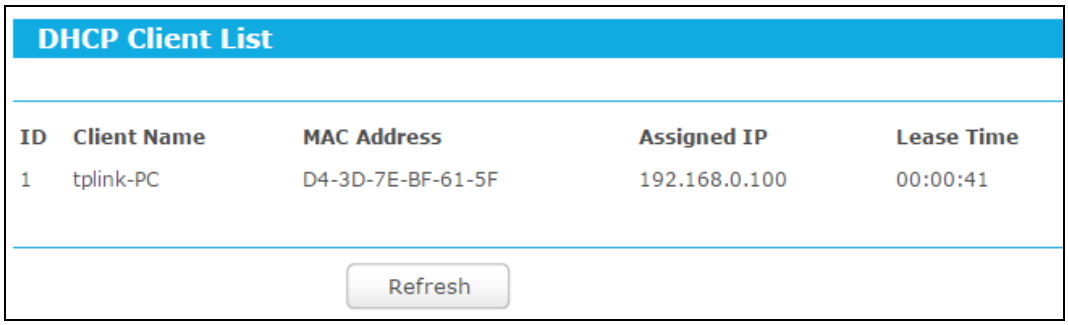
- **DHCP Server - Enable** or **Disable** the DHCP server. If you disable the Server, you must have another DHCP server within your network or else you must configure the computer manually.
- **Start IP Address -** Specify an IP address for the DHCP Server to start with when assigning IP addresses. 192.168.0.100 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) **-** It is suggested to input the IP address of the LAN port of the Router. The default value is 192.168.0.1.
- **Default Domain** (Optional) **-** Input the domain name of your network.
- **Primary DNS -** (Optional) Input the DNS IP address provided by your ISP or consult your ISP. 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".

8.5.2 DHCP Client List

Choose menu "**DHCP → DHCP Client List**", and then you can view the information about the clients attached to the Router in the screen as shown below.

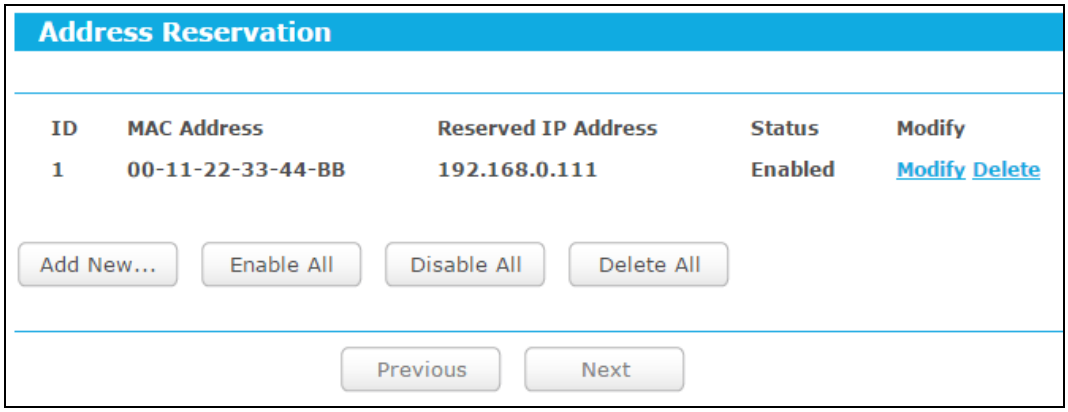


- **Client Name -** The name of the DHCP client
- **MAC Address -** The MAC address of the DHCP client
- **Assigned IP -** The IP address that the Router has allocated to the DHCP client
- **Lease Time -** The time of the DHCP client leased. After the dynamic IP address has expired, a new dynamic IP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

8.5.3 Address Reservation

Choose menu "**DHCP → Address Reservation**", and then you can view and add a reserved address for clients via the next screen. 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.

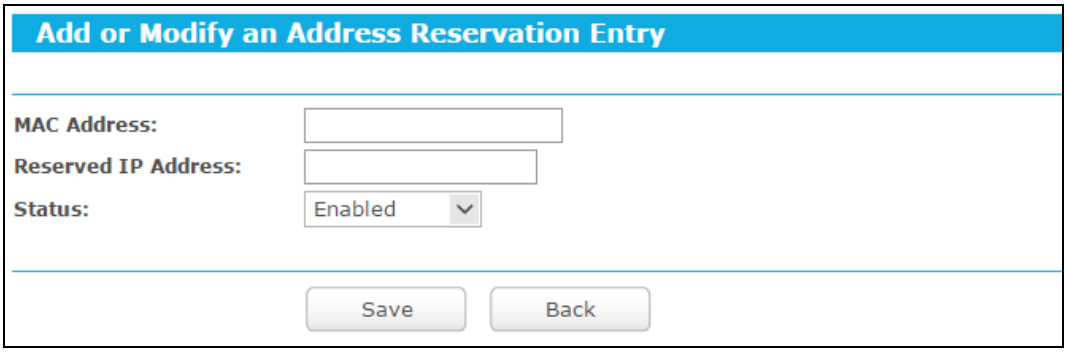


- **MAC Address -** The MAC address of the PC for which you want to reserve an IP address.

- **Reserved IP Address -** The IP address reserved for the PC by the Router.
- **Status -** The status of this entry, either **Enabled** or **Disabled**.
- **Modify -** To modify or delete an existing entry.

To Reserve an IP address:

1. Click the **Add New…** button. Then will pop-up.
2. Enter the MAC address (in XX-XX-XX-XX-XX-XX format.) and IP address (in dotted-decimal notation) of the computer for which you want to reserve an IP address.
3. Click **Save**.



To modify or delete an existing entry:

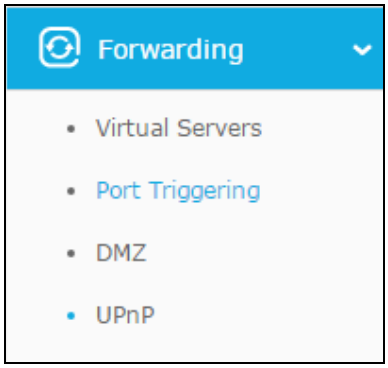
1. Click the **Modify** in the entry you want to modify. If you want to delete the entry, click the **Delete**.
2. Modify the information.
3. Click the **Save** button.

   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.

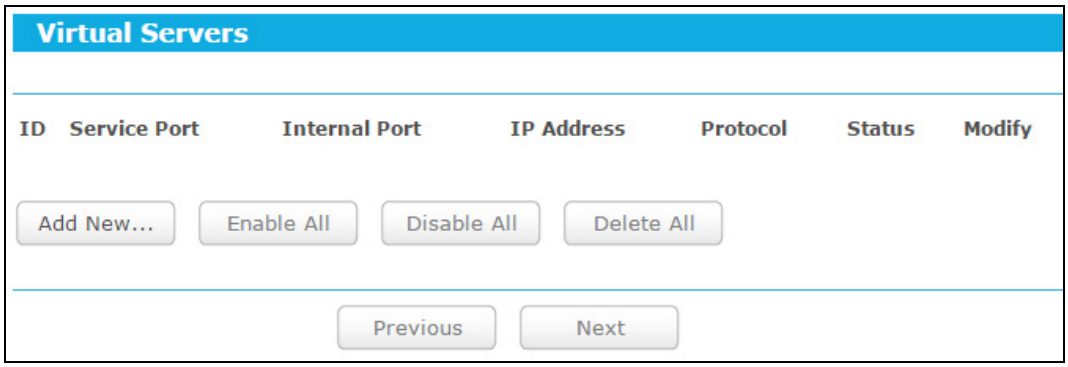
8.6 Forwarding



There are four submenus under the Forwarding menu: **Virtual Servers**, **Port Triggering**, **DMZ** and **UPnP**. Click any of them, and you will be able to configure the corresponding function.

8.6.1 Virtual Servers

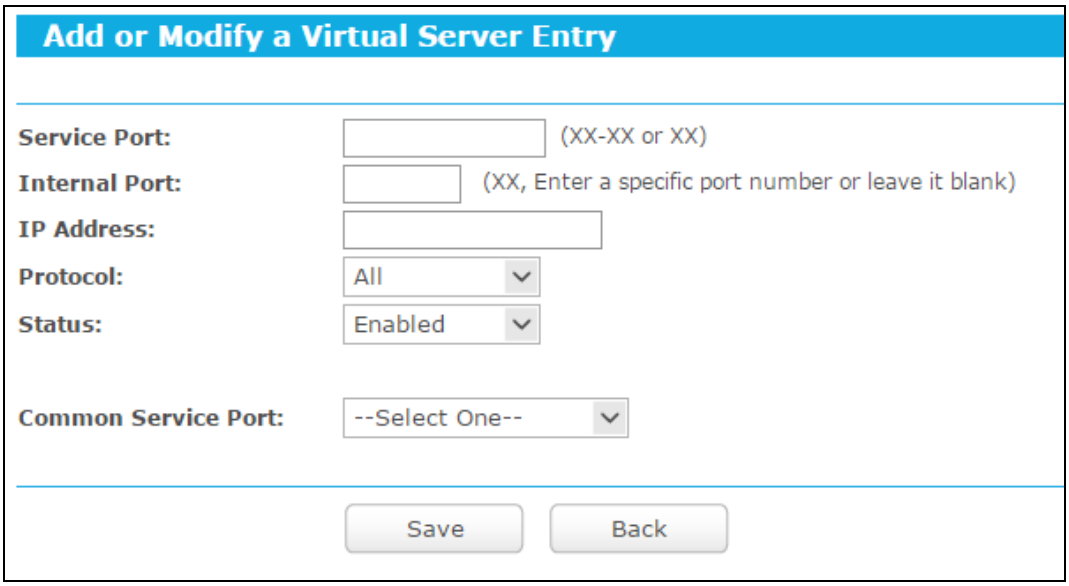
Choose menu "**Forwarding → Virtual Servers**", and then you can view and add virtual servers in the screen as shown below. Virtual servers can be used for setting up public services on your LAN, such as DNS, Email and FTP. A virtual server is defined as a service port, and all requests from the Internet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



- **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**.
- **Modify -** To modify or delete an existing entry.

To setup a virtual server entry:

1. Click the **Add New…** button, the next screen will pop-up.
2. Select the service port 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 service port number 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**, **UDP**, or **All**.
5. Select the **Enable** to enable the virtual server.
6. Click **Save**.



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.

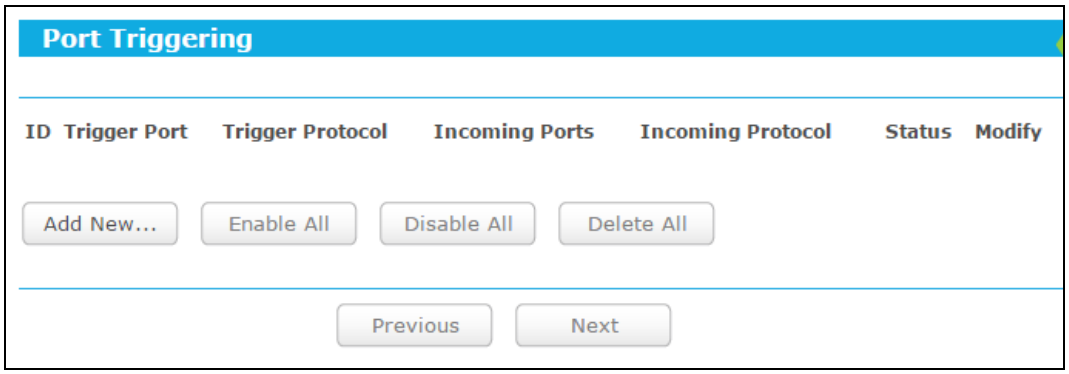
Click the **Next** button to go to the next page and click the **Previous** button to return the previous page.

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.

8.6.2 Port Triggering

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



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

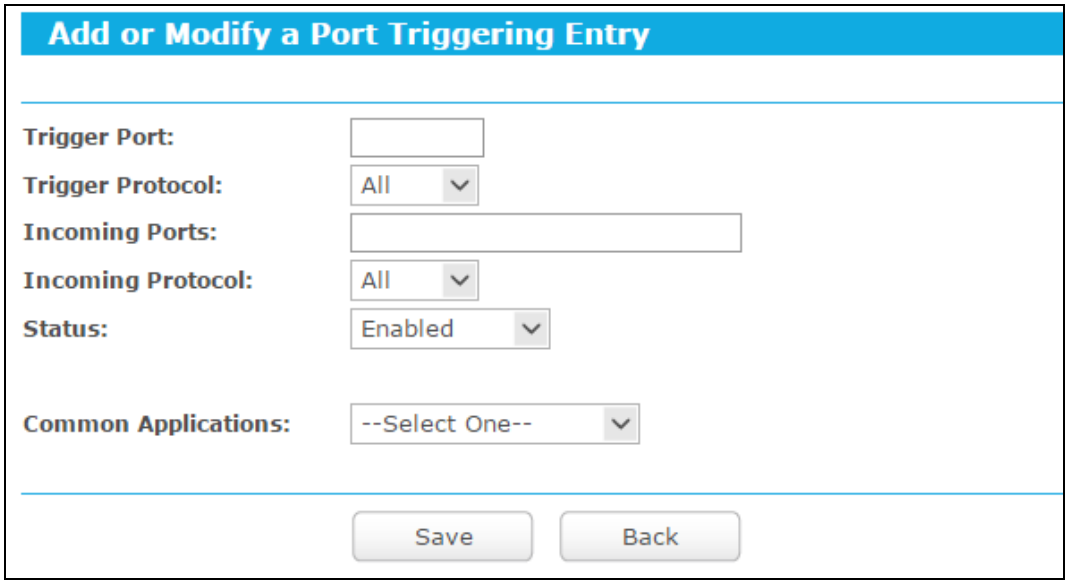
1. A local host makes an outgoing connection using a destination port number defined in the Trigger Port field.
2. The Router records this connection, opens the incoming port or ports associated with this entry in the Port Triggering table, and associates them with the local host.
3. When necessary， 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 Ports -** 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 sections). 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**.
- **Modify -** To modify or delete an existing entry.

To add a new rule, follow the steps below:

1. Click the **Add New…** button, the next screen will pop-up.
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.



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.

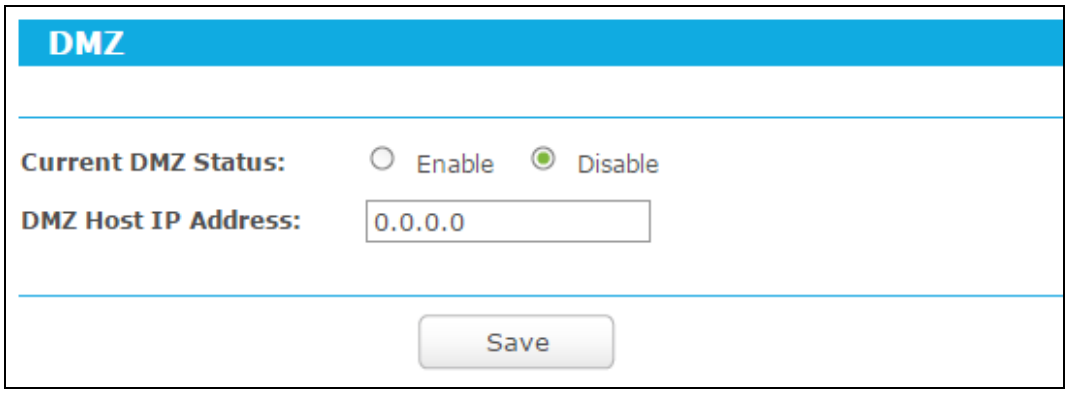
Click the **Delete All** button to delete all entries.

Note:

1. When the trigger connection is released, the corresponding opening ports will be closed.
2. Each rule is 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.

8.6.3 DMZ

Choose menu "**Forwarding → DMZ**", and then you can view and configure DMZ host in the screen as shown below. 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.



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

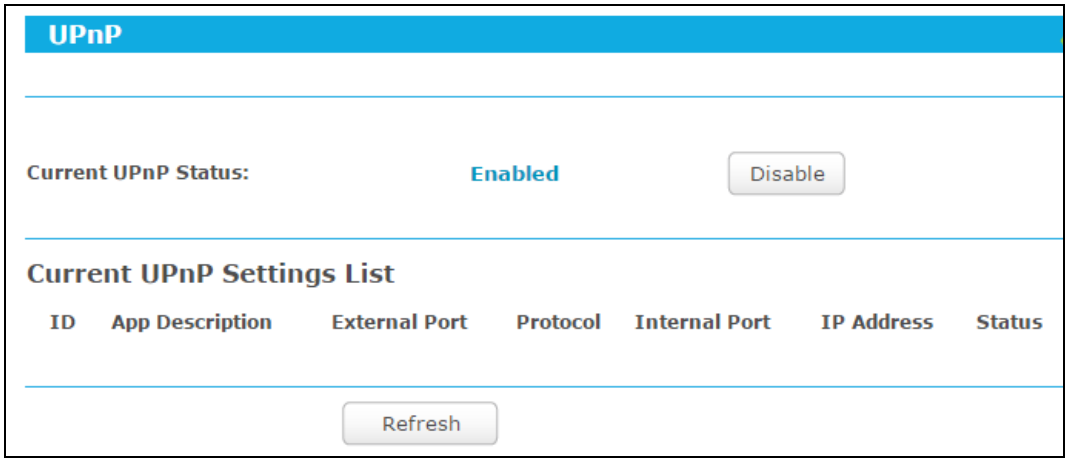
1. Check the **Enable** radio button.
2. Enter the IP Address of a local host in the **DMZ Host IP Address** field.
3. Click the **Save** button.

Note:

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

8.6.4 UPnP

Choose menu "**Forwarding** → **UPnP**", and then you can view the information about **UPnP** (Universal Plug and Play) in the screen as shown below. 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.

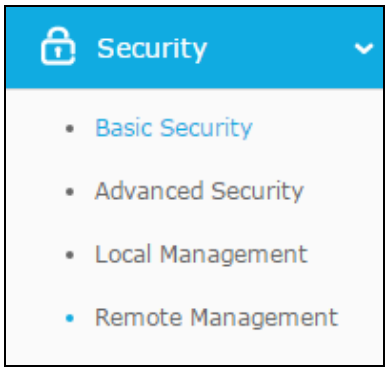


- **Current UPnP Status -** UPnP can be enabled or disabled by clicking the **Enable** or **Disable** button.
- **Current UPnP Settings List -** This table displays the current UPnP information.
  - **App Description -** The description provided by the application in the UPnP request.
  - **External Port -** The external port the Router opens for the application.
  - **Protocol -** The type of protocol the Router opens for the application.
  - **Internal Port -** The Internal port the Router opens for local host.

- **IP Address -** The IP address of the UPnP device that is currently accessing the Router.
- **Status -** The status of the port is displayed here. “Enabled” means that the port is still active. Otherwise, the port is inactive.

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

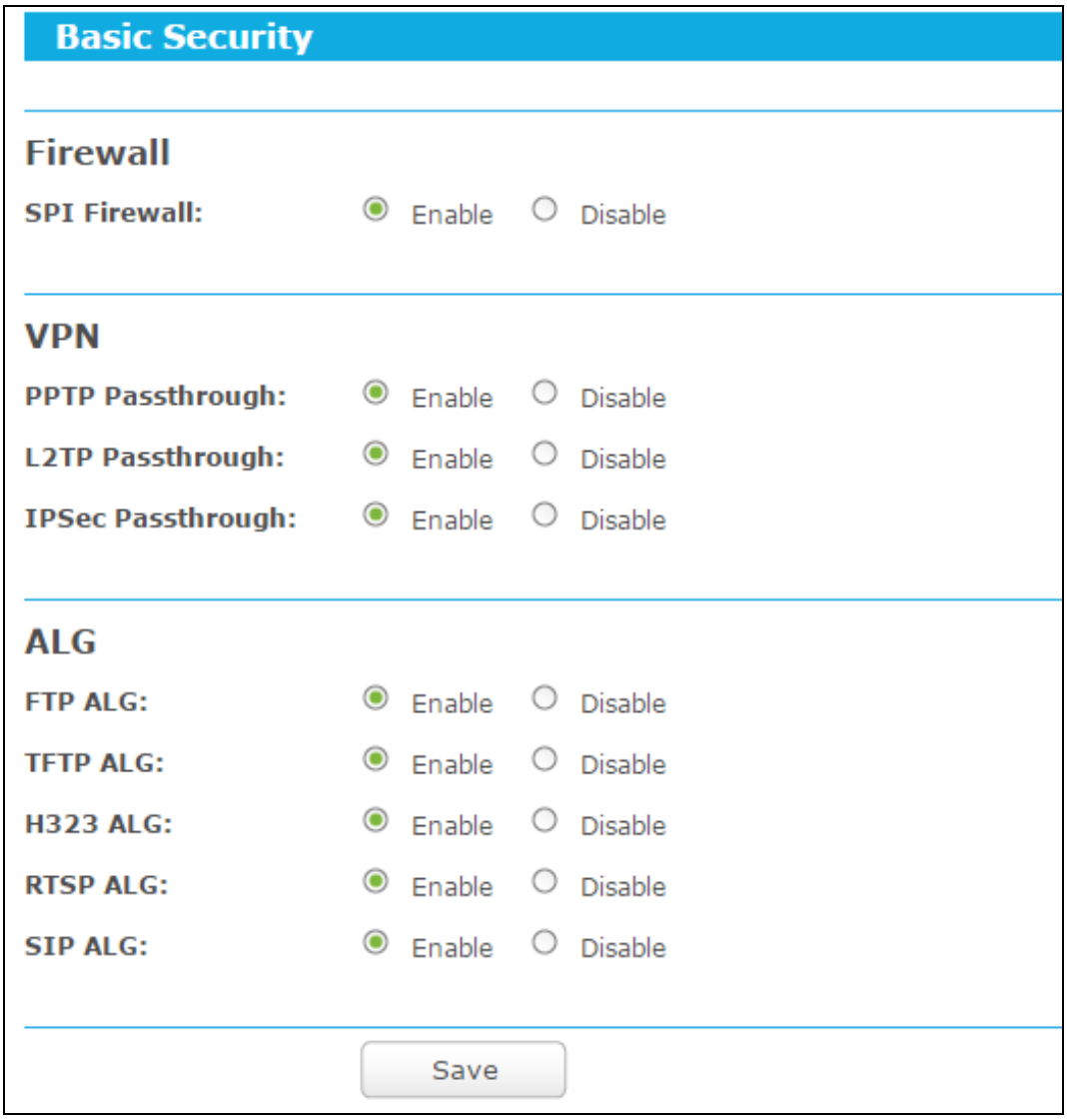
8.7 Security



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

8.7.1 Basic Security

Choose menu “**Security → Basic Security**”, you can configure the basic security in the screen as shown below.



- **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, **Enabled**.
  - **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, **Enabled**.

- **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, **Enabled**.

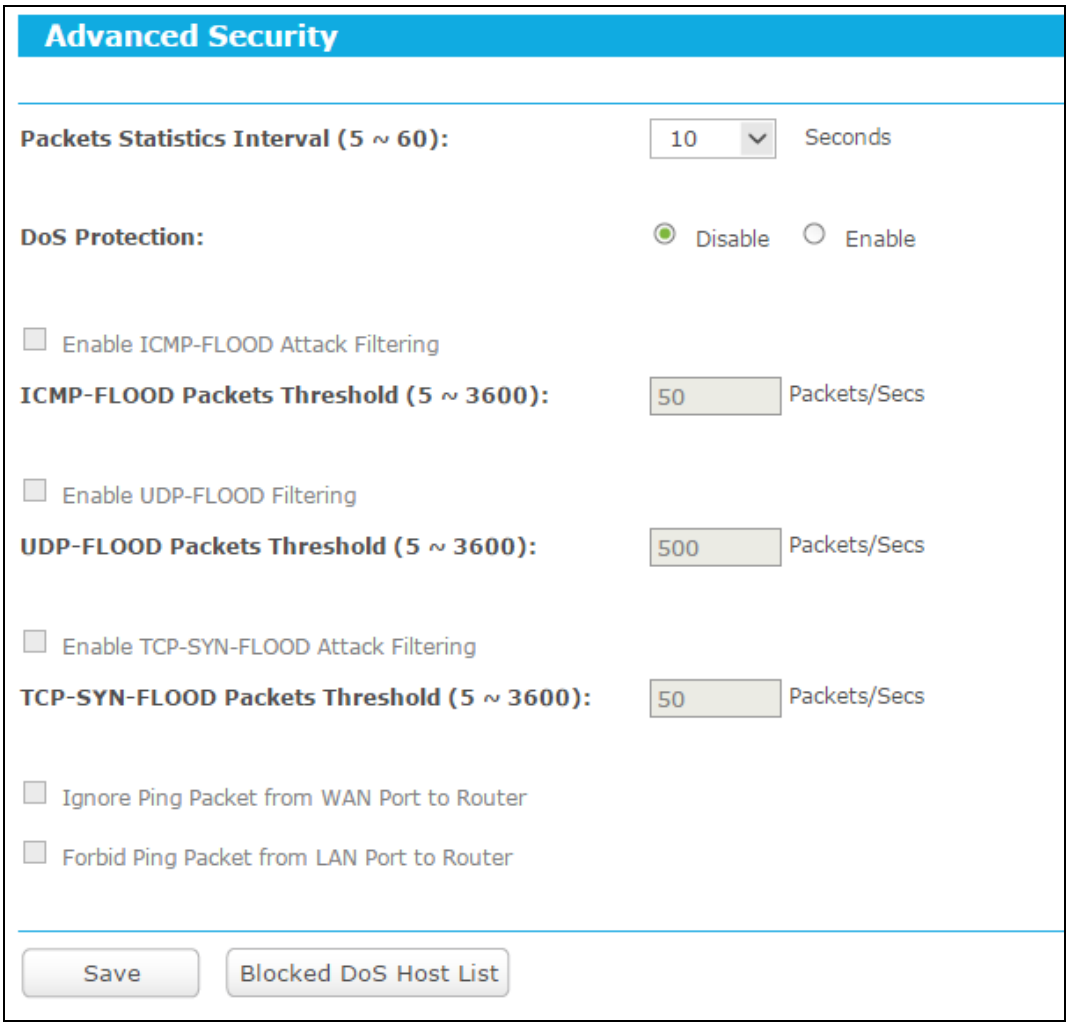
➢ **ALG -** It is recommended to enable Application Layer Gateway (ALG) because ALG allows customized Network Address Translation (NAT) traversal filters to be plugged into the gateway to support address and port translation for certain application layer "control/data" protocols such as FTP, TFTP, H323 etc.

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

Click **Save**.

8.7.2 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 belows.



- **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.

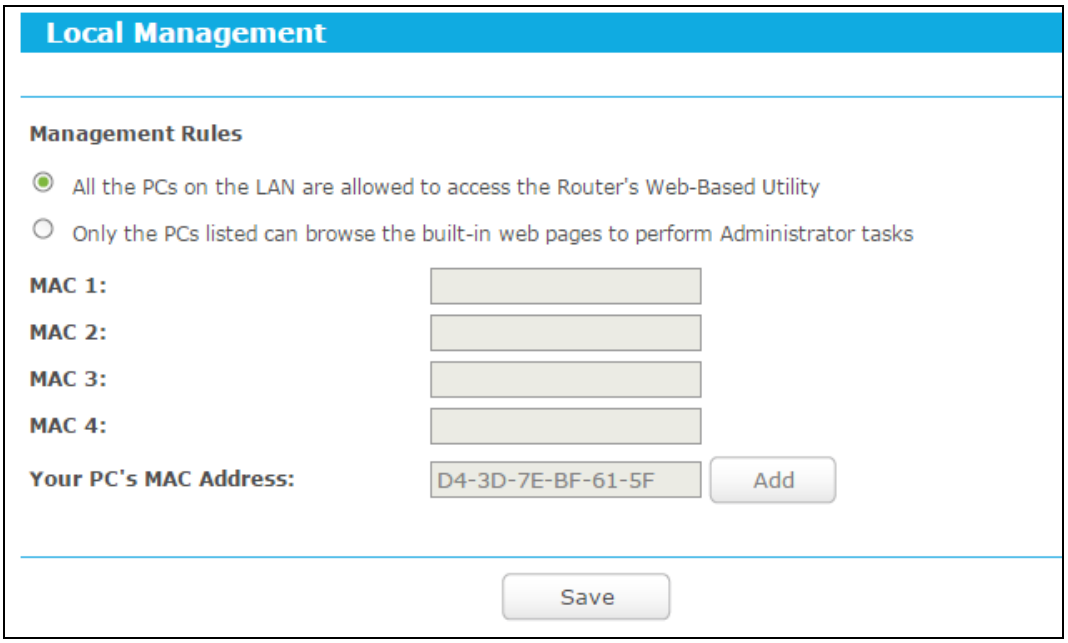
- **Enable UDP-FLOOD Filtering -** Enable or Disable the UDP-FLOOD Filtering.
- **UDP-FLOOD Packets Threshold (5~3600) -** The default value is 500. Enter a value between 5 ~ 3600. When the current UPD-FLOOD Packets number is beyond the set value, the Router will startup the blocking function immediately.
- **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.

8.7.3 Local Management

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



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.

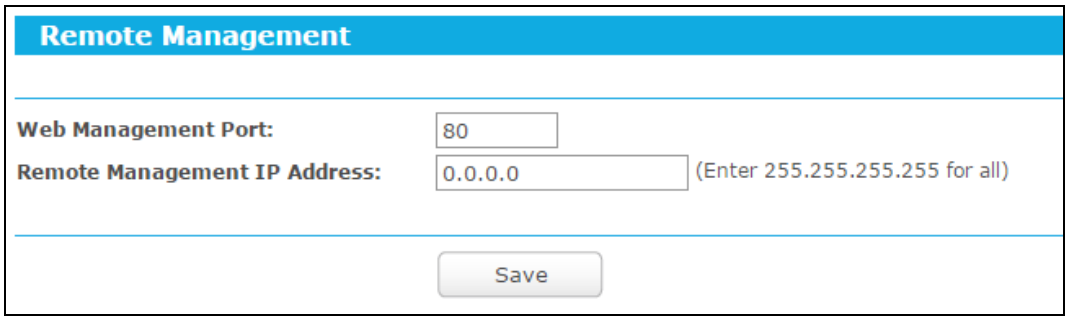
Click **Save**.

☞ **Note:**

If your PC is blocked but you want to access the Router again, press and hold the WPS button for more than 5 seconds to reset the Router to factory defaults.

8.7.4 Remote Management

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



- **Web Management Port -** Web browser access normally uses the standard HTTP service port 80. This router's default remote management Web port number is 80. For greater security, you can change the remote management Web interface to a custom port by entering that number in this box provided. Choose a number between 1024 and 65535, but do not use the number of any common service port.
- **Remote Management IP Address -** This is the current address you will use when accessing your router from the Internet. The default IP Address is 0.0.0.0. It means this function is disabled. To enable this function, change the default IP Address to another IP Address as desired.

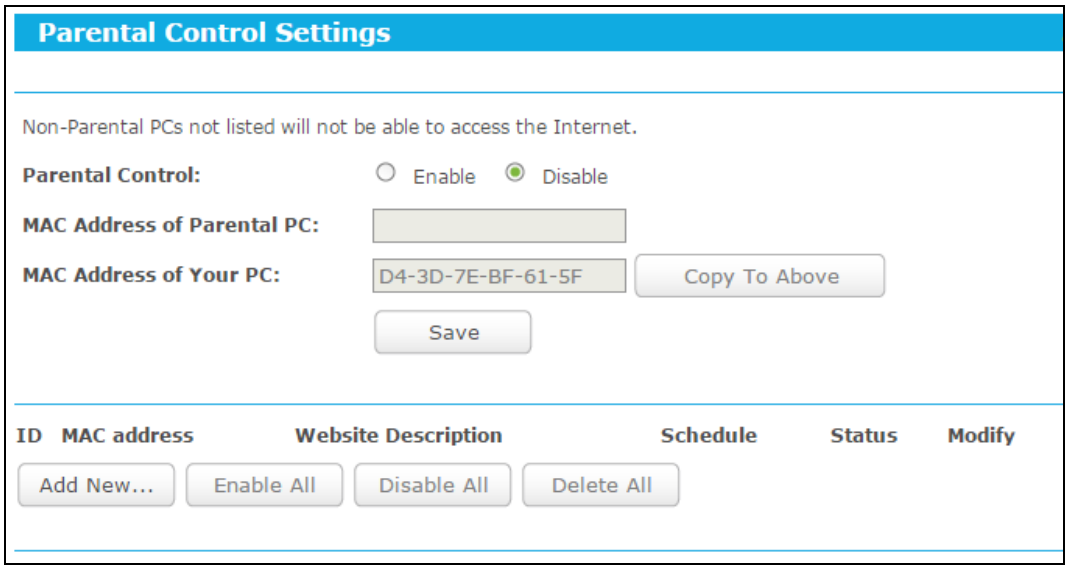
To access the router, you will type your router's WAN IP Address into your browser's Address (in IE) or Location (in Navigator) box, followed by a colon and the custom port number. For example, if your Router's WAN address is 202.96.12.8 and you use port number 8080, enter in your browser: http://202.96.12.8:8080.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

☞ **Note:**

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

8.8 Parental Control

Choose menu "**Parental Control**", and you can configure the parental control in the screen. 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.



- **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 Restriction→ 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.
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 TP-LINK) 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. tp-link) in the Allowed Domain Name field. Any domain name with keywords in it (e.g. www.tp-link.com) 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.

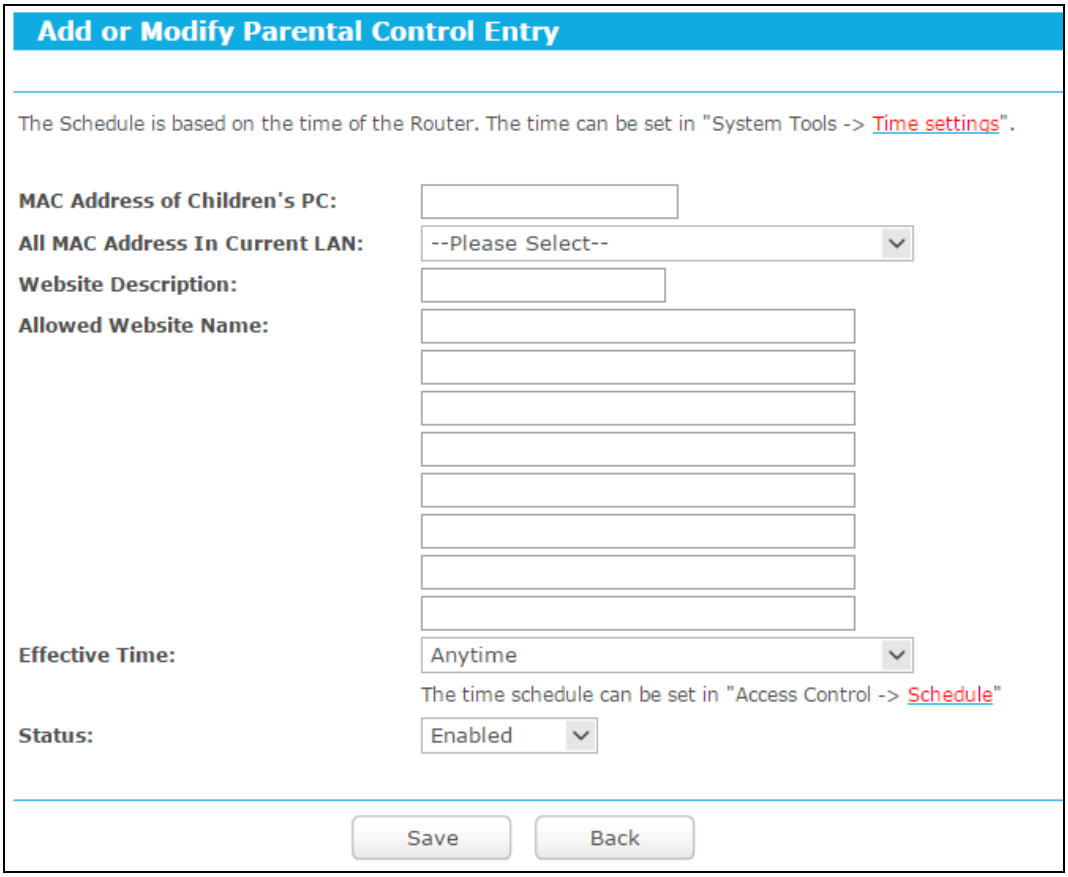
7. Click the **Save** button.

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.



For example: If you desire that the child PC with MAC address 00-11-22-33-44-AA can access www.tp-link.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.

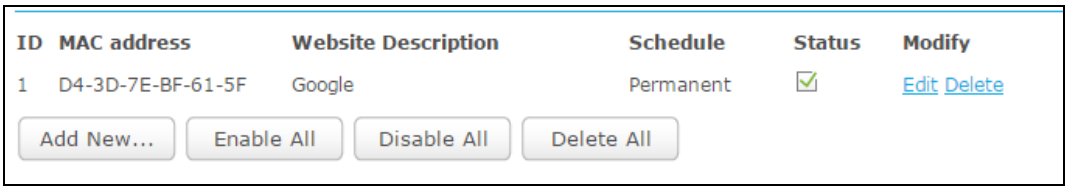
2. Click "**Access Restriction** → **Schedule**" on the left to enter the Schedule Settings page. Click **Add New...** button to create a new schedule with Schedule Description is Schedule_1, Day is Sat and Time is all day-24 hours.

3. Click "**Parental Control**" menu on the left to go back to the Add or Modify Parental Control Entry page:

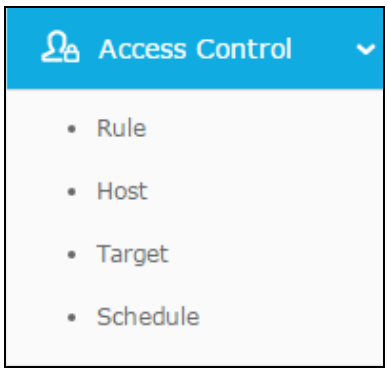
- Click **Add New...** button.
- Enter 00-11-22-33-44-AA in the **MAC Address of Child PC** field.
- Enter “Allow TP-LINK” in the **Website Description** field.
- Enter “www.tp-link.com” in the **Allowed Domain Name** field.
- Select “Schedule_1” you create just now from the **Effective Time** drop-down 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



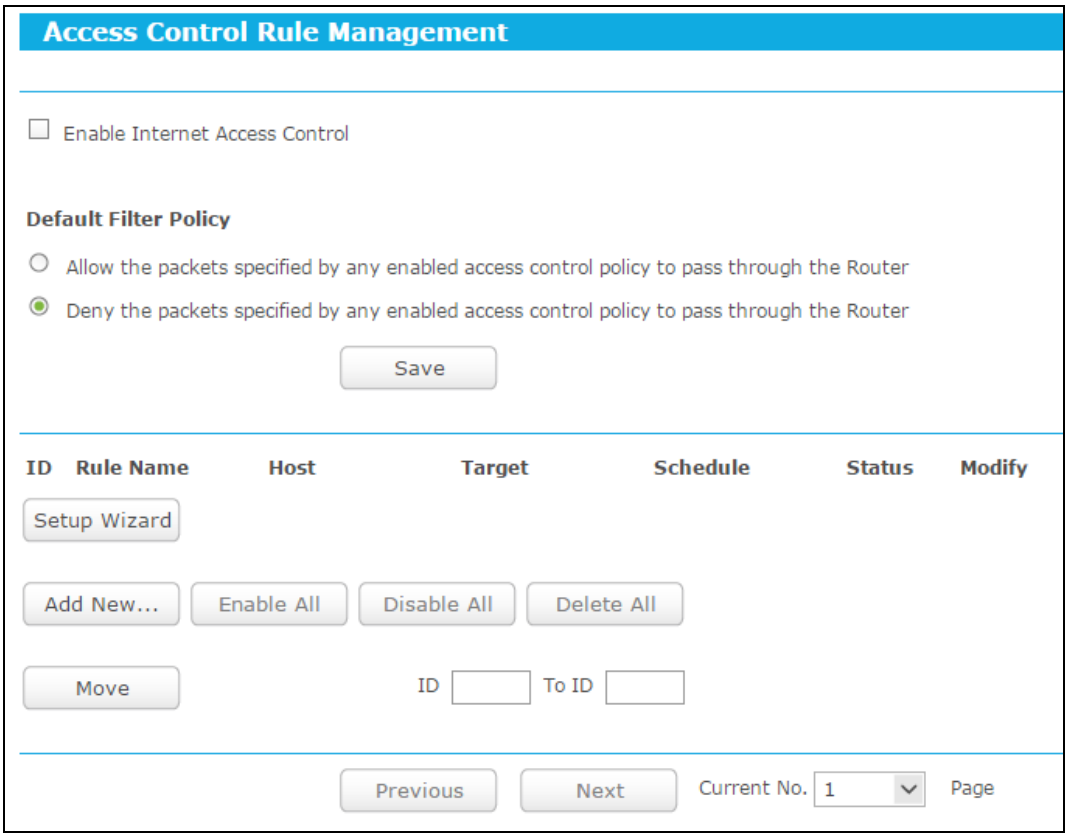
8.9 Access Control



There are four submenus under the Access Restriction menu: **Rule**, **Host**, **Target** and **Schedule**. Click any of them, and you will be able to configure the corresponding function.

8.9.1 Rule

Choose menu “**Access Control→ Rule**”, you can view and set Access Restriction rules in the screen as shown below.



- **Enable Internet Access Restriction -** Select the check box to enable the Internet Access Restriction 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.
- **Action -** Here displays the action the Router takes to deal with the packets. It could be **Allow** or **Deny**. **Allow** means that the Router permits the packets to go through the Router. **Deny** means that the Router rejects the packets to go through the Router.
- **Status -** This field displays the status of the rule. **Enabled** means the rule will take effect, **Disabled** means the rule will not take effect.
- **Modify -** Here you can edit or delete an existing rule.

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

1. Click the **Add New…** button and the next screen will pop-up.
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 **Action** field, select **Deny** or **Allow**.
7. In the **Status** field, select **Enabled** or **Disabled** to enable or disable your entry.
8. Click the **Save** button.

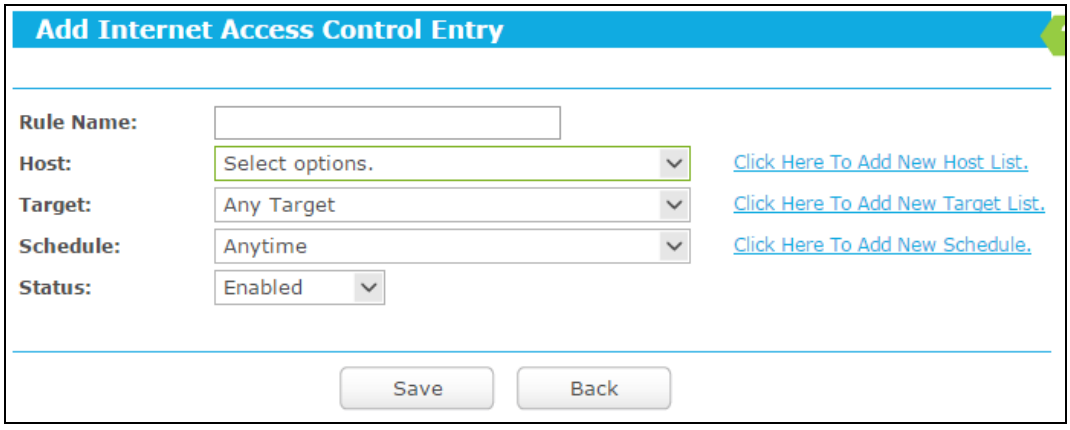
   Click the **Enable All** button to enable all the rules in the list.

   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.

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

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



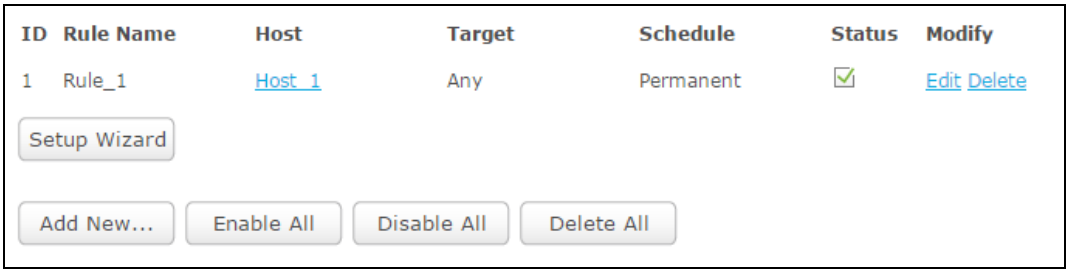
For example: If you desire to allow the host with MAC address 00-11-22-33-44-AA to access **www.tp-link.com** only from **18:00** to **20:00** on **Saturday and Sunday**, and forbid other hosts in the LAN to access the Internet, you should follow the settings below:

1. Click "**Access Restriction → Host**" in the left to enter the Host Settings page. Add a new entry with the Host Description is Host_1 and MAC Address is 00-11-22-33-44-AA.
2. Click "**Access Restriction → Target**" in the left to enter the Target Settings page. Add a new entry with the Target Description is Target_1 and Domain Name is www.tp-link.com.
3. Click "**Access Restriction → Schedule**" in the left to enter the Schedule Settings 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.
4. Click "**Access Restriction → Rule**" in the left to return to the Access Restriction Rule Management page. Select "**Enable Internet Access Restriction**" and choose "Deny the packets not specified by any access Restriction policy to pass through the Router".

5. Click **Add New...** button to add a new rule as follows:

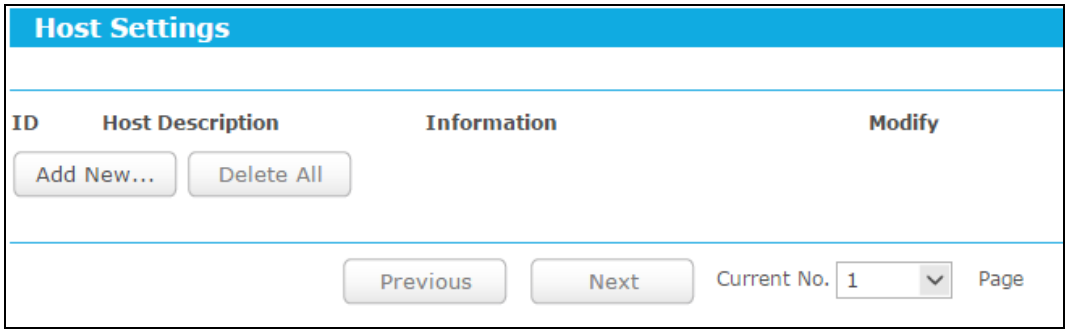
- In **Rule Name** field, create a name for the rule. Note that this name should be unique, for example Rule_1.
- In **Host** field, select Host_1.
- In **Target** field, select Target_1.
- In **Schedule** field, select Schedule_1.
- In **Action** field, select Allow.
- In **Status** field, select Enabled.
- Click **Save** to complete the settings.

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



8.9.2 Host

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



- **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:
     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:

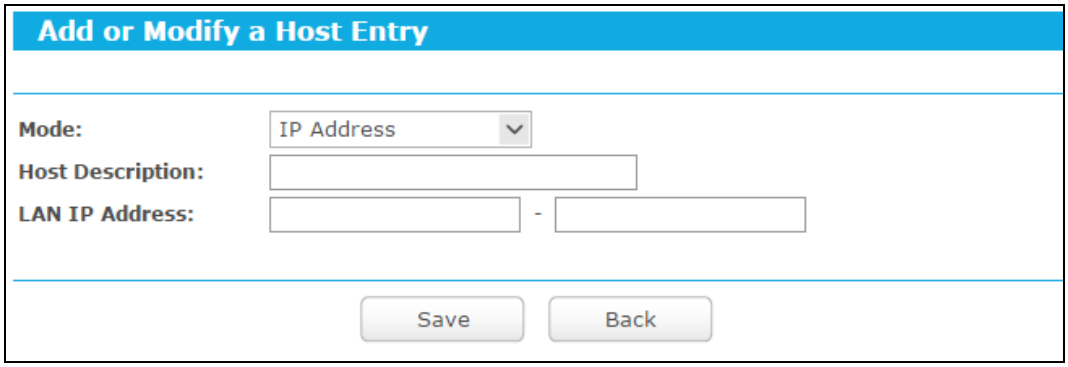
1) In **Host Description** field, create a unique description for the host (e.g. Host_1).

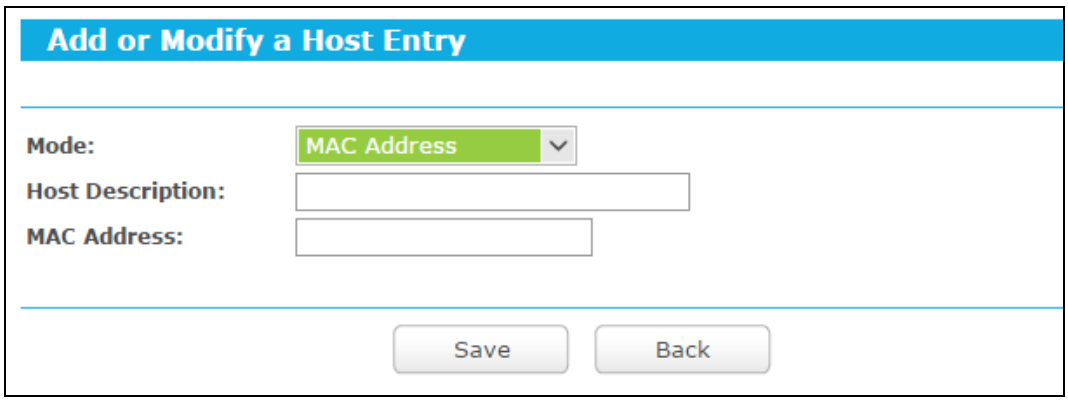
2) In **MAC Address** field, enter the MAC address.

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.

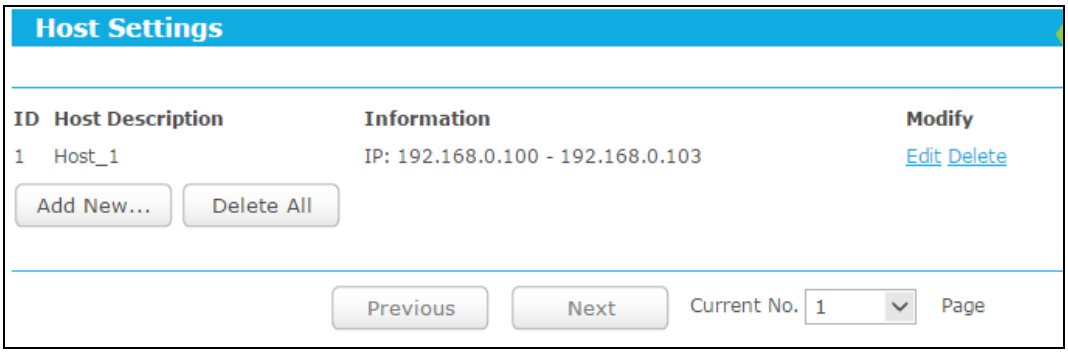




For example: If you desire to restrict the internet activities of host with MAC address 00-11-22-33-44-AA, you should first follow the settings below:

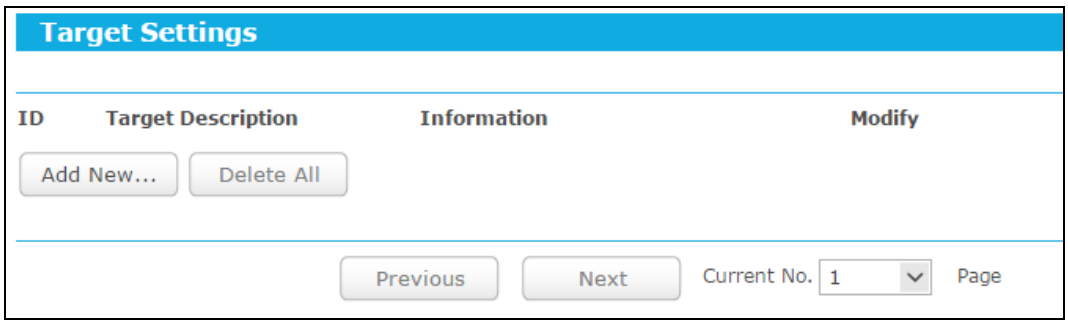
1. Click **Add New...** button to enter the Add or Modify a Host Entry page.
2. In **Mode** field, select MAC Address from the drop-down list.
3. In **Host Description** field, create a **unique** description for the host (e.g. Host_1).
4. In **MAC Address** field, enter 00-11-22-33-44-AA.
5. Click **Save** to complete the settings.

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



8.9.3 Target

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



- **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.

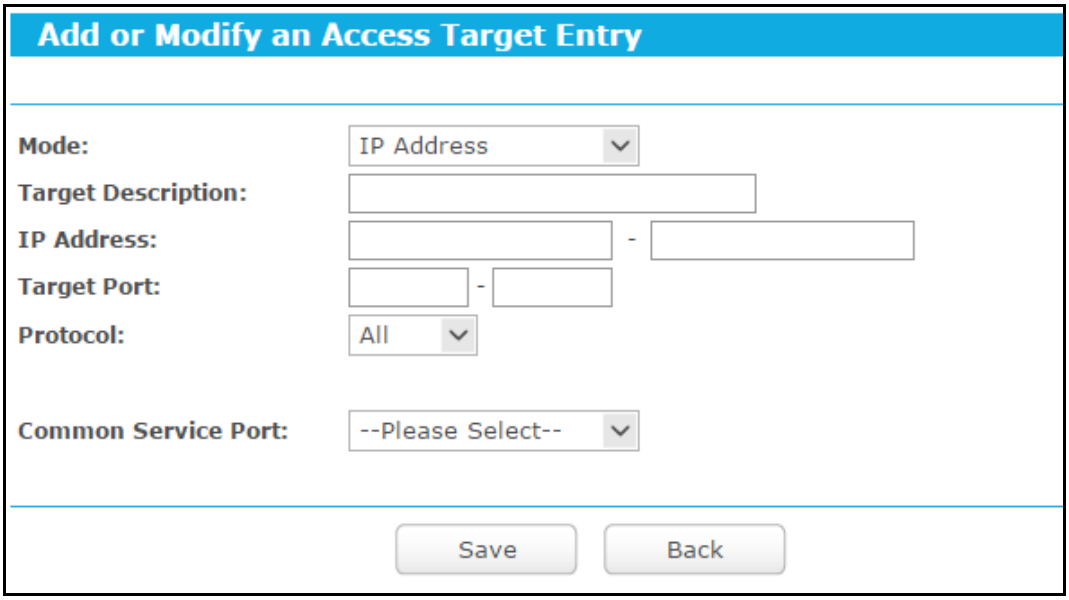
1. Click the **Add New…** button.
2. In **Mode** field, select IP Address or Domain Name.
   - If you select **IP Address**:
     1) In **Target Description** field, create a unique description for the target (e.g. Target_1).
     2) In **IP Address** field, enter the IP address of the target.
     3) 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**:
     1) In **Target Description** field, create a unique description for the target (e.g. Target_1).

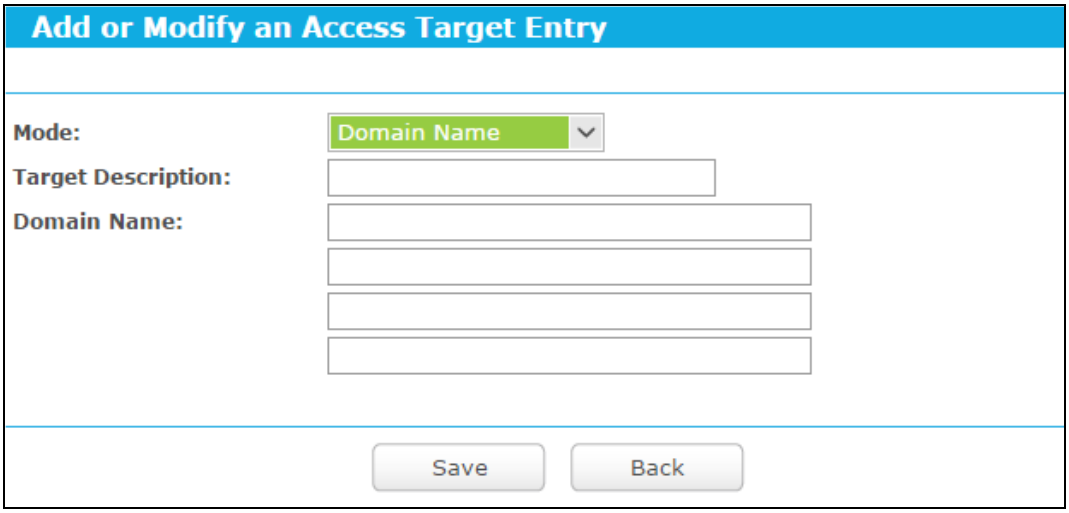
2) In **Domain Name** field, enter the domain name, either the full name or the keywords (for example TP-LINK) in the blank. Any domain name with keywords in it (e.g.www.tp-link.com) will be blocked or allowed. You can enter 4 domain names.

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.



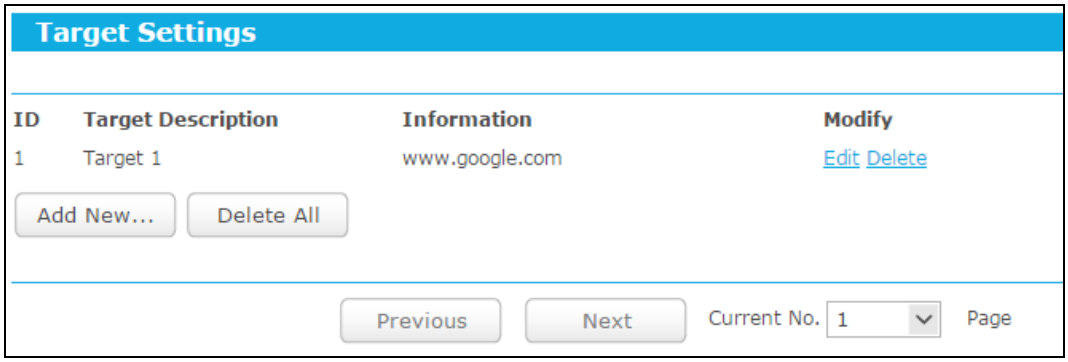


For example: If you desire to restrict the internet activities of host with MAC address 00-11-22-33-44-AA in the LAN to access **www.tp-link.com** only, you should first follow the settings below:

1. Click **Add New…** button 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.tp-link.com.

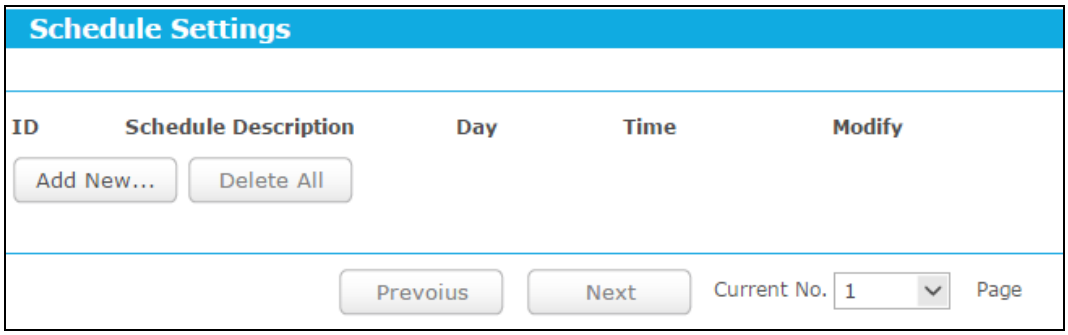
5. Click **Save** to complete the settings.

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



8.9.4 Schedule

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



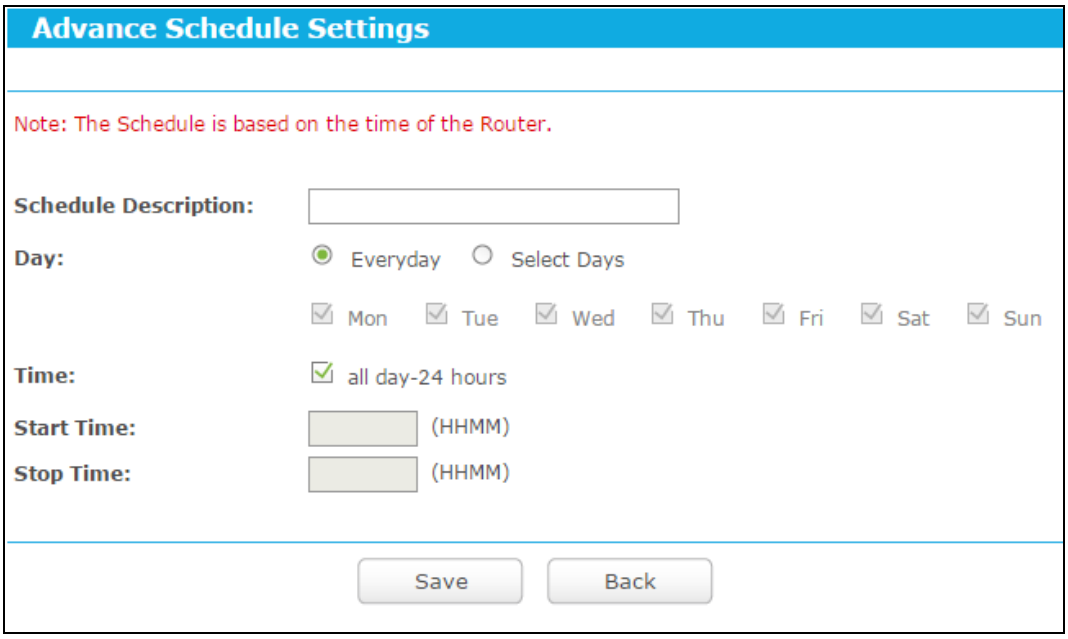
- **Schedule Description -** Here displays the description of the schedule and this description is unique.
- **Day -** Here displays the day(s) in a week.
- **Time -** Here displays the time period in a day.
- **Modify -** Here you can edit or delete an existing schedule.

To add a new schedule, follow the steps below.

1. Click **Add New...** button and the next screen will pop-up.
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.

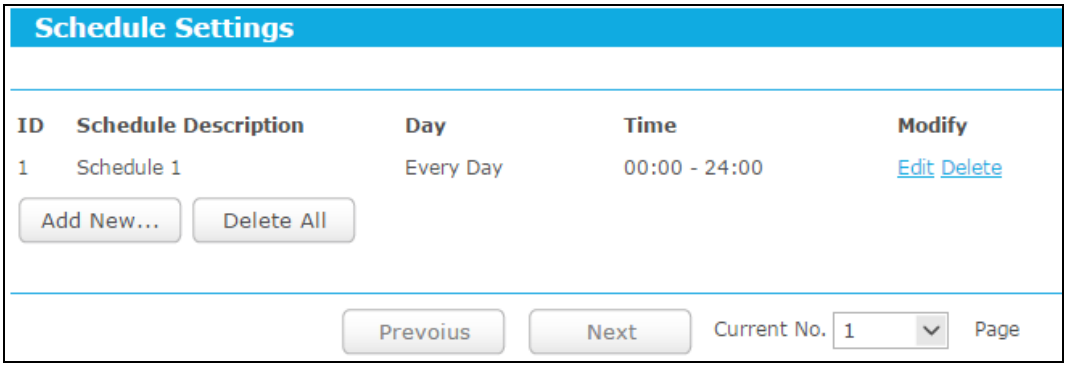
Click the **Next** button to go to the next page, or click the **Previous** button return to the previous page.



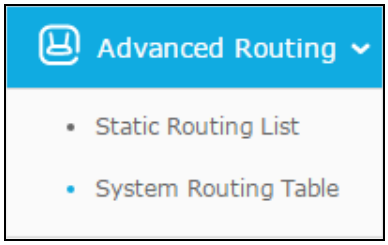
For example: If you desire to restrict the internet activities of host with MAC address 00-11-22-33-44-AA to access www.tp-link.com only from **18:00 to 20:00** on **Saturday** and **Sunday**, you should first follow the settings below:

1. Click **Add New...** button to enter the 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.



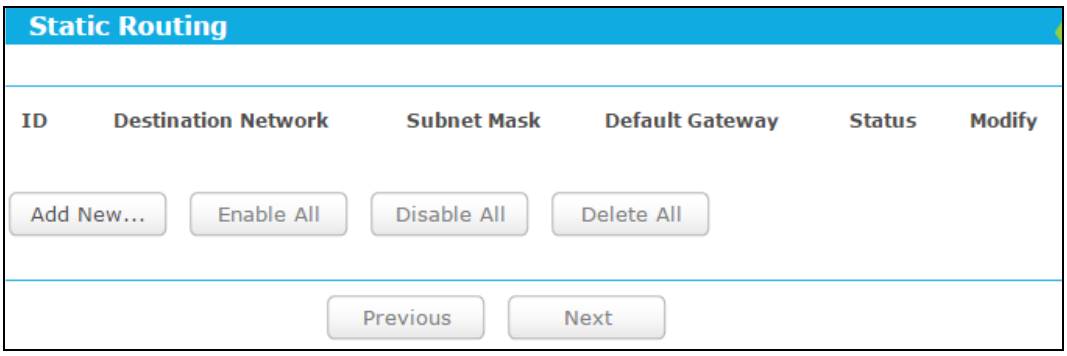
8.10 Advanced Routing



There are two submenus under the Network menu: **Static Routing List** and **System Routing Table**. Click any of them, and you will be able to configure the corresponding function.

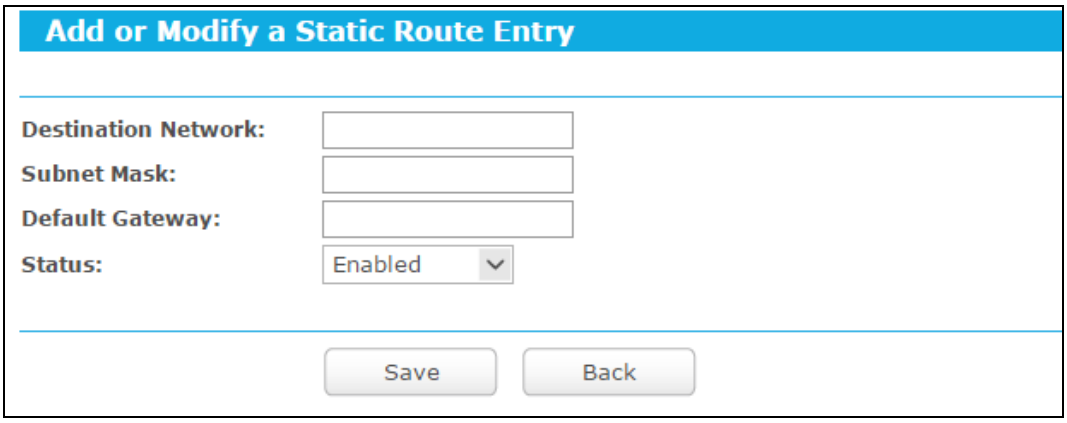
8.10.1 Static Routing List

Choose menu **"Static Routing"**, and you can configure the static route in the next screen. A static route is a pre-determined path that network information must travel to reach a specific host or network.



To add static routing entries, follow the steps below.

1. Click **Add New…**, and you will see the following screen.



2. Enter the following data.

- **Destination Network -** The **Destination IP Address** is the address of the network or host that you want to assign to a static route.
- **Subnet Mask -** The **Subnet Mask** determines which portion of an IP Address is the network portion, and which portion is the host portion.

- **Default Gateway -** This is the IP Address of the gateway device that allows for contact between the Router and the network or host.

3. Select **Enabled** or **Disabled** for this entry on the **Status** drop-down list.
4. Click the **Save** button to make the entry take effect.

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

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

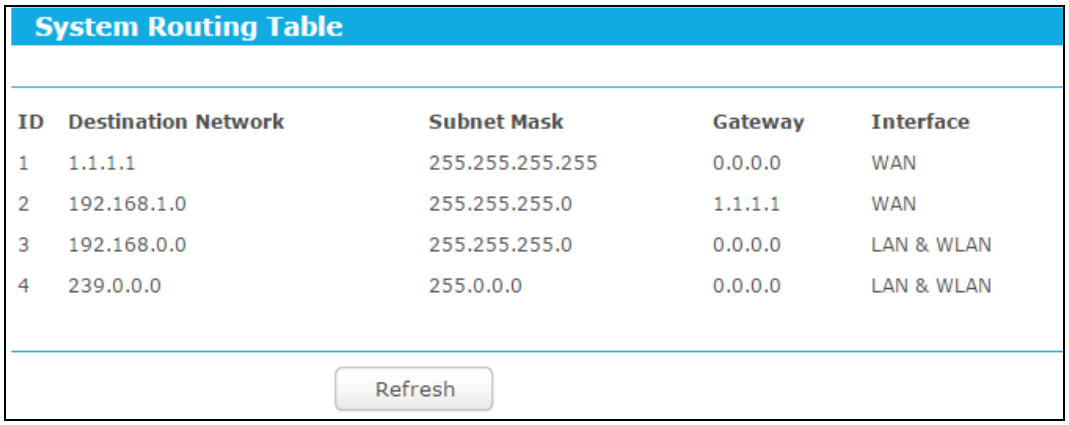
   Click the **Disable All** button to disable all the entries.

   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.

8.10.2 System Routing Table

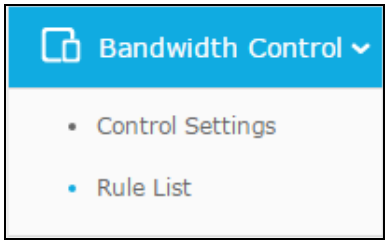
Choose menu **"Advanced Routing → System Routing Table"**, and you can views all of the valid route entries in use. The Destination IP address, Subnet Mask, Gateway, and Interface will be displayed for each entry.



- **Destination Network -** The Destination IP Address 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)**.

Click the **Refresh** button to refresh the data displayed.

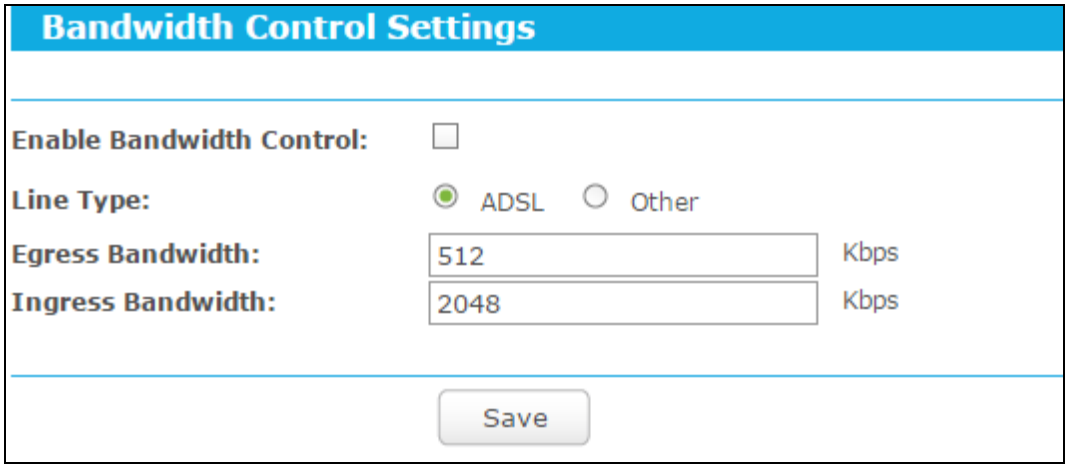
8.11 Bandwidth Control



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

8.11.1 Control Settings

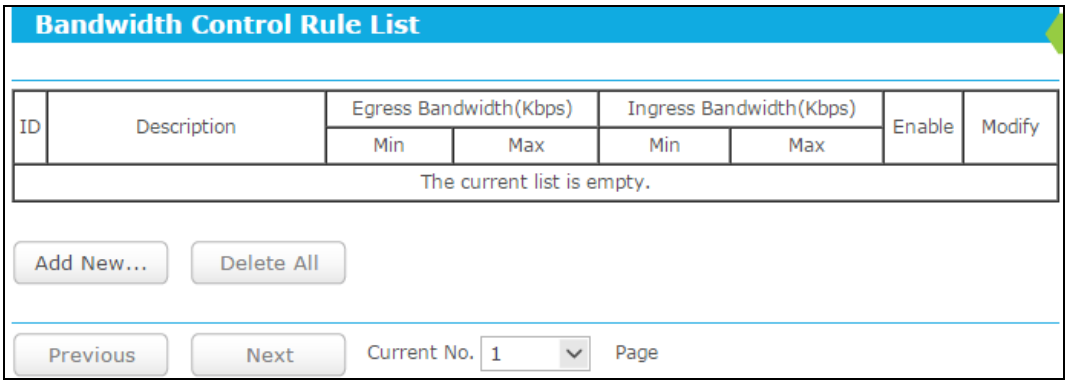
Choose menu "**Bandwidth Control → Control Settings**", you can configure the Egress Bandwidth and Ingress Bandwidth in the next screen. Their values you configure should be less than 100000Kbps. For optimal control of the bandwidth, please select the right Line Type and ask your ISP for the total bandwidth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



- **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.

8.11.2 Rule List

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

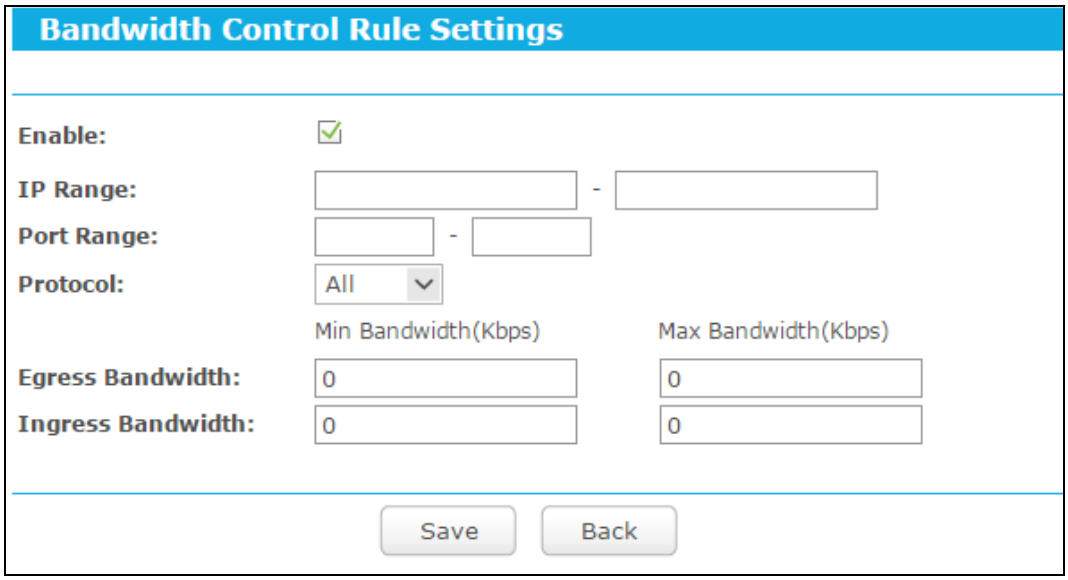


- **Description -** This is the information about the rules such as address range.
- **Egress Bandwidth -** This field displays the max and mix upload bandwidth through the WAN port, the default is 0.
- **Ingress Bandwidth -** This field displays the max and mix download bandwidth through the WAN port, 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.

Step 1: Click **Add New…**, and you will see a new screen.

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

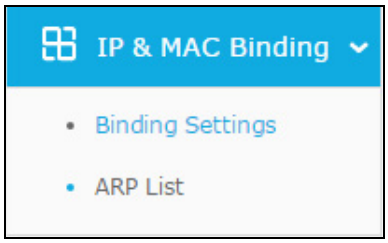


- **Enable** - Enable or disable the rule.
- **IP Range** - Interior PC address range. If both are blank (or 0.0.0.0), the domain is no effective.
- **Port Range** - The port range which the Interior PC access the outside PC. If all are blank (or 0), the domain is no effective.

- **Protocol** - Transport layer protocol, here there are All, TCP, UDP.
- **Egress Bandwidth** - The max and the min upload speed which through the WAN port, default number is 0.
- **Ingress Bandwidth** - The max and the min download speed through the WAN port, default number is 0.

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

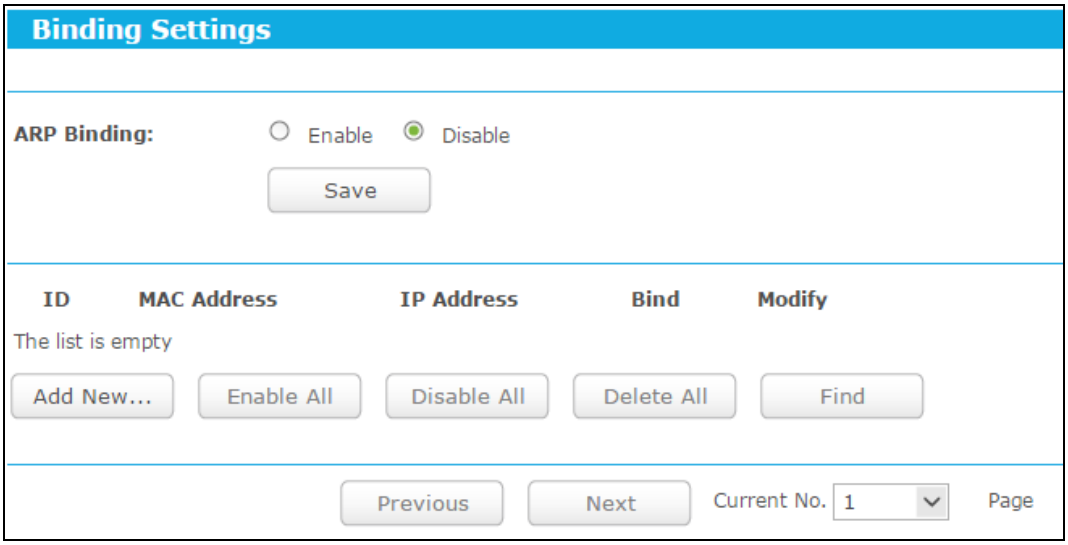
8.12 IP & MAC Binding



There are two submenus under the IP & MAC Binding menu: **Binding Setting** 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.

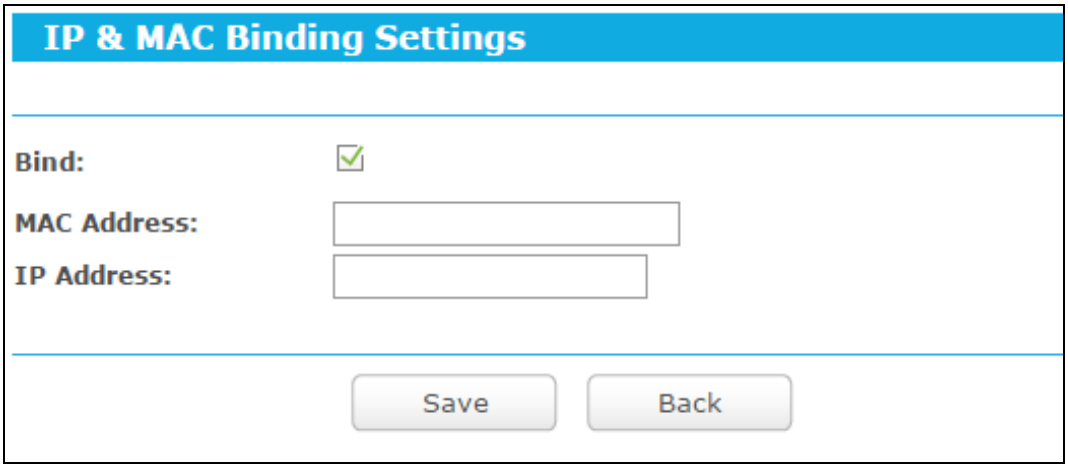
8.12.1 Binding Setting

This page displays the IP & MAC Binding Setting table; you can operate it in accord with your desire.



- **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 -** Whether or not enable the ARP binding.
- **Modify -** Edit or delete item.

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.



To add IP & MAC Binding entries:

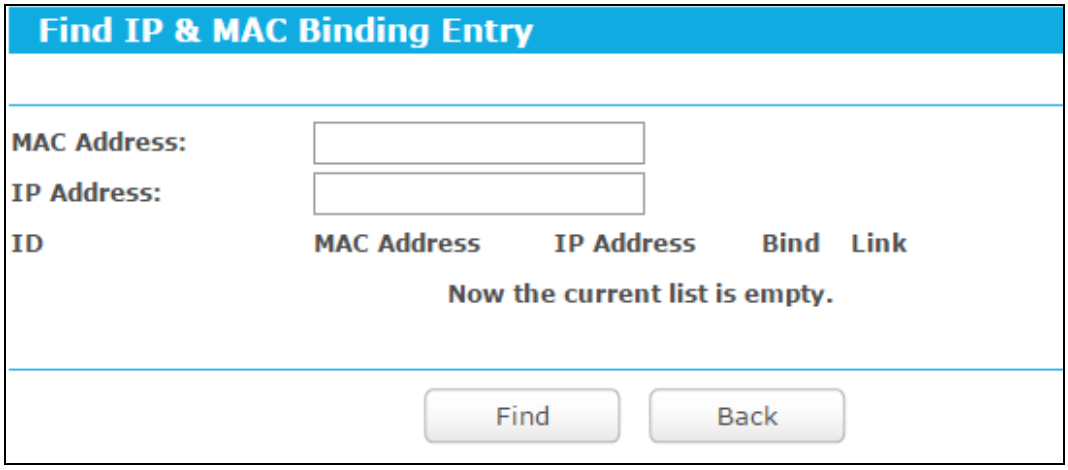
1. Click the **Add New…** button.
2. Enter the MAC Address and IP Address.
3. Select the Bind checkbox.
4. Click the **Save** button to save it.

To modify or delete an existing entry:

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

To find an existing entry:

1. Click the **Find** button.
2. Enter the MAC Address or IP Address.
3. Enter the **Find** button in the next page as shown below.

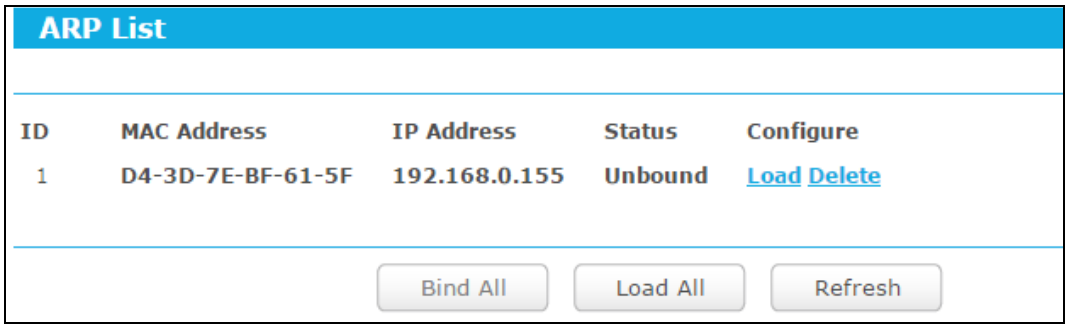


Click the **Enable All** button to make all entries enabled.

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

8.12.2 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.



- **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 -** Enabled or Disabled of the MAC address and IP address binding.
- **Configure -** Load or delete item.
- **Load -** Load the item to the IP & MAC Binding list.
- **Delete -** Delete the item.

1. Click the **Bind All** button to bind all the current items, available after enable.
2. Click the **Load All** button to load all items to the IP & MAC Binding list.
3. Click the **Refresh** button to refresh all items.

Note:

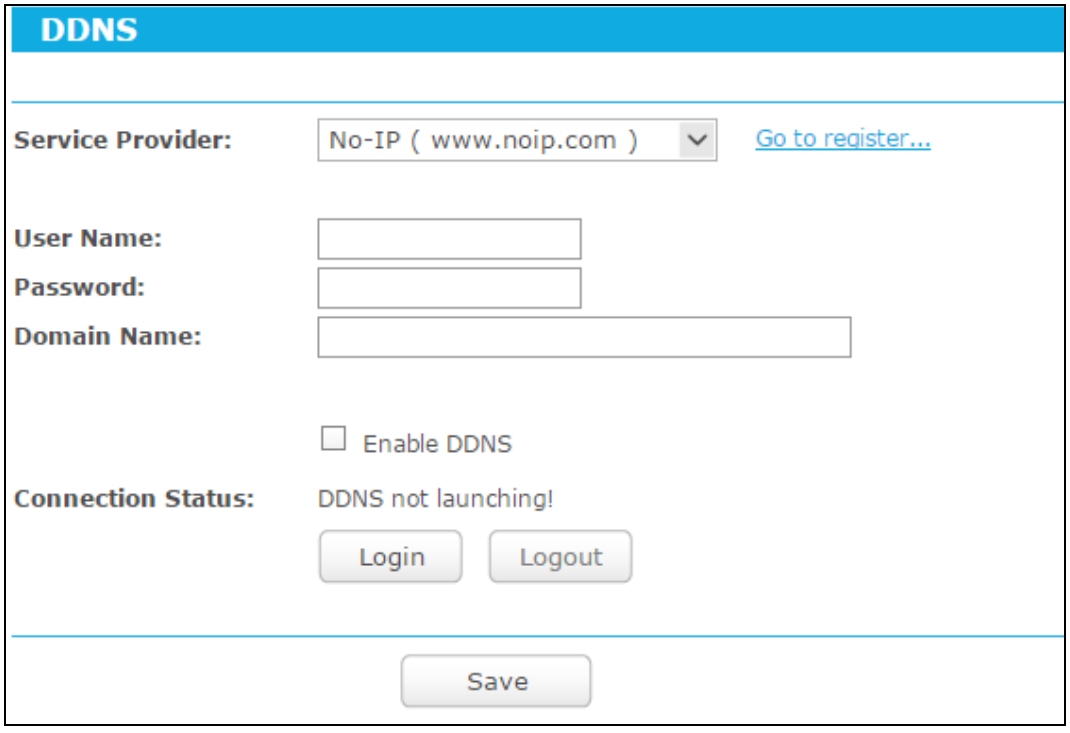
An item could not be loaded to the IP & MAC Binding list if the IP address of the item has been loaded before. Error warning will prompt as well. Likewise, "Load All" only loads the items without interference to the IP & MAC Binding list.

8.13 Dynamic DNS

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.noip.com, www.comexe.cn, or www.dyn.com. The Dynamic DNS client service provider will give you a password or key.

8.13.1 No-IP DDNS

If the dynamic DNS **Service Provider** you select is www.noip.com, the page will appear as shown below.



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.

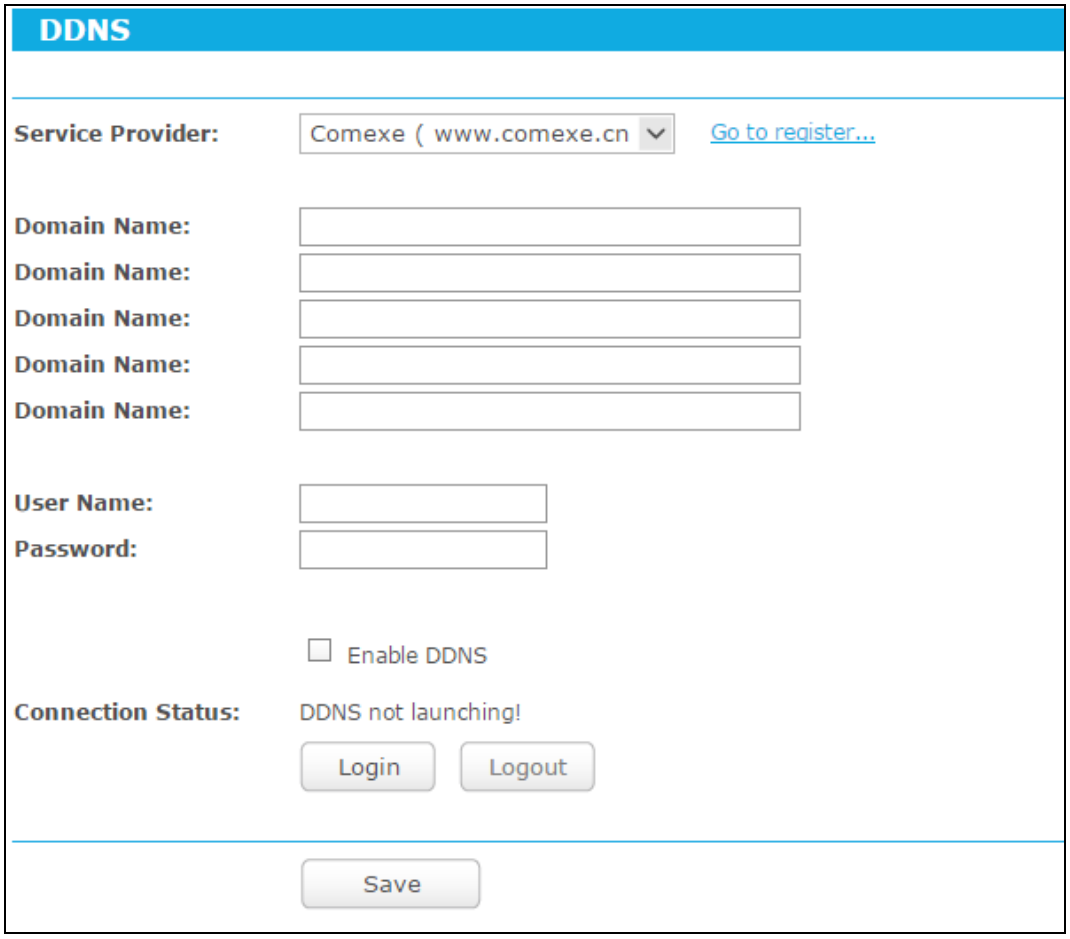
Click **Logout** to log out the DDNS service.

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.

8.13.2 Comexe.cn DDNS

If the dynamic DNS **Service Provider** you select is www.comexe.cn, the page will appear as shown below.



To set up for DDNS, follow these instructions:

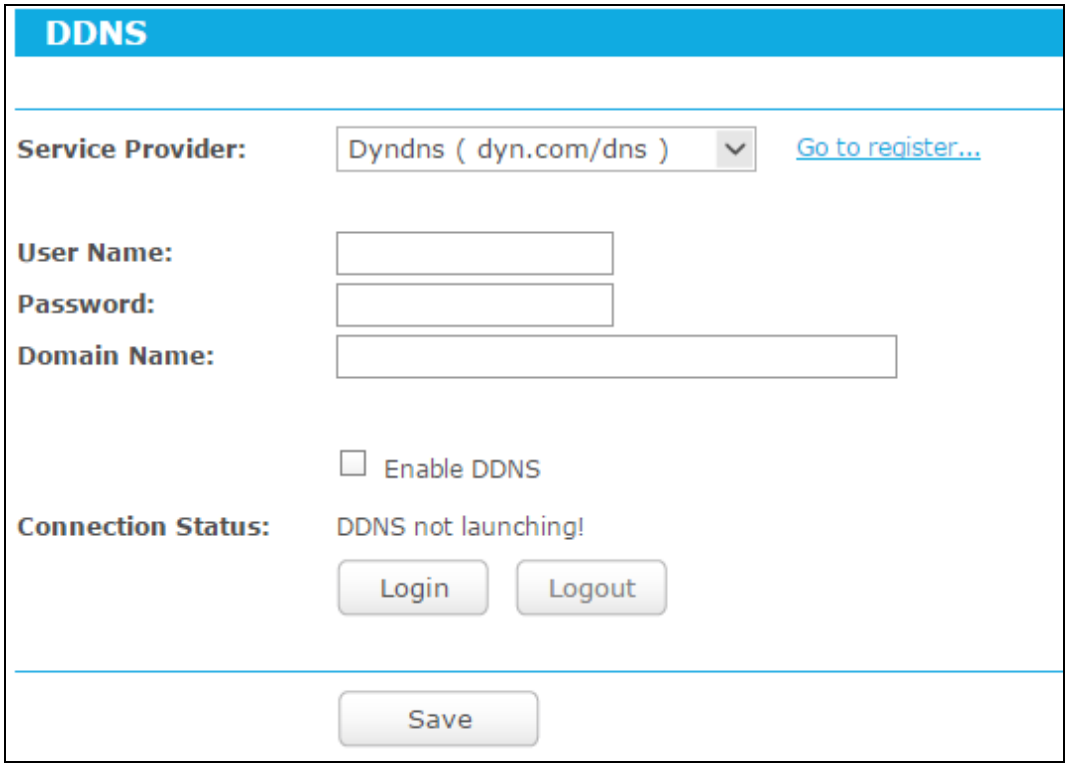
1. Type the **Domain Name** received from your dynamic DNS service provider.
2. Type the **User Name** for your DDNS account.
3. Type the **Password** for your DDNS account.
4. Click the **Login** button to log in to the DDNS service.

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

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

8.13.3 Dyndns DDNS

If the dynamic DNS **Service Provider** you select is www.dyndns.com, the page will appear as shown below.



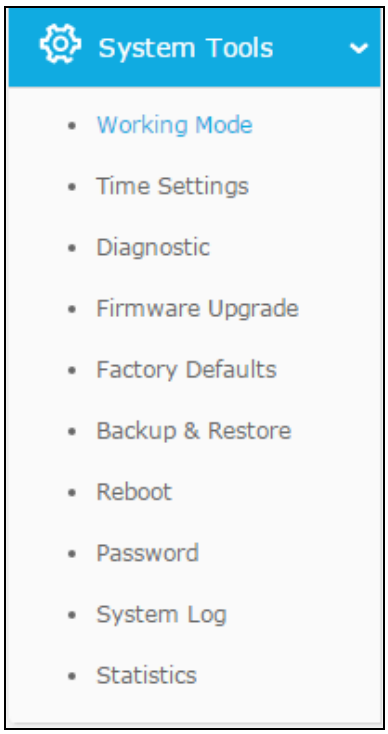
To set up for DDNS, follow these instructions:

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.

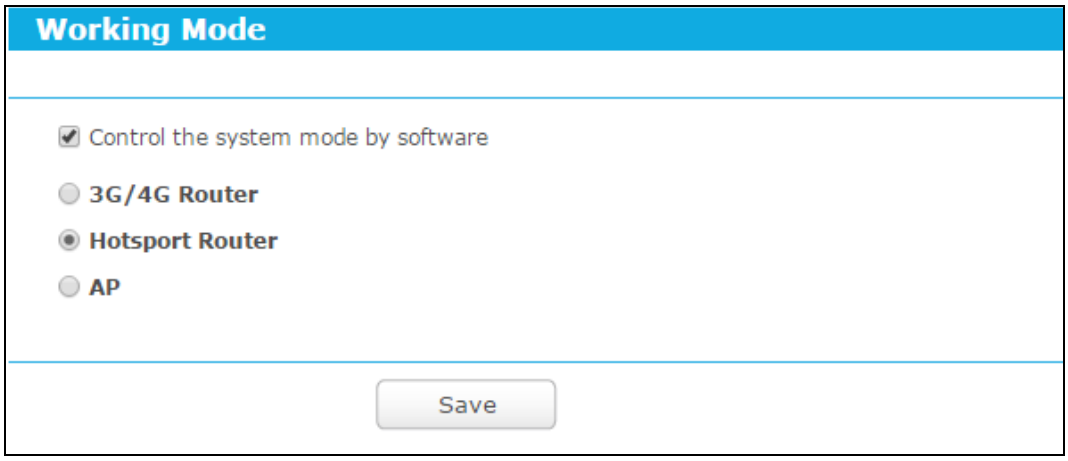
8.14 System Tools



There are nine submenus under the System Tools menu: **Time Settings**, **Diagnostic**, **Firmware Upgrade**, **Factory Defaults**, **Backup and 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.

8.14.1 Working Mode

Choose menu "**System Tools → Working Mode**", check **Control the system mode by software** and then you can see the following screen.



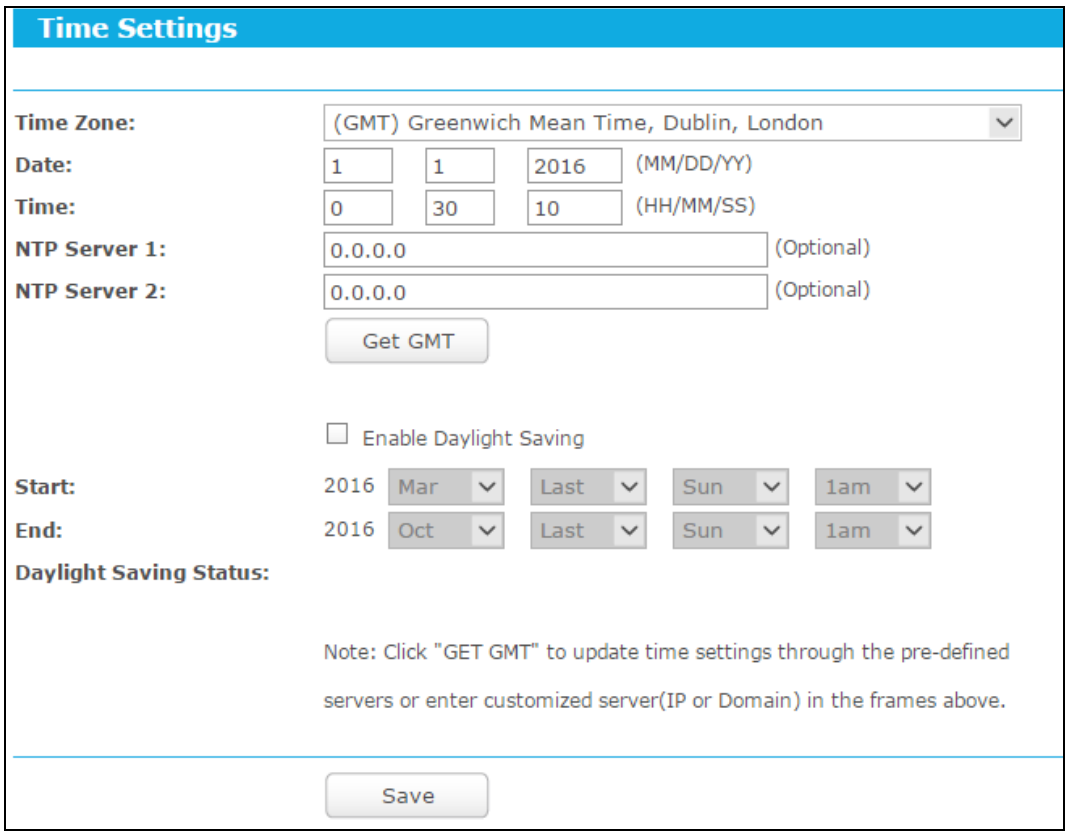
- **3G/4G Router -** This mode stands for Wireless Router Mode. It functions as a standard wireless router and you can also plug in a 3G/4G USB modem if you need.

- **Hotspot Router -** It functions as a hotspot router.
- **AP -** This mode stands for Access Point Mode, Repeater Mode and Client Mode. When selected, you have to go to the **Quick Setup** to specify the mode you need.

  Note: If **Control the system mode by software** is checked, the operation mode switch of the router will be disabled.

8.14.2 Time Settings

You can set time manually or get GMT from the Internet for the router on this page:



- **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.

To set time manually, follow the steps below:

1. Select your local time zone.
2. Enter the **Date** in Month/Day/Year format.
3. Enter the **Time** in Hour/Minute/Second format.
4. Click **Save**.

For automatic time synchronization:

1. Enter the address of the **NTP Server 1 or NTP Server 2**.
2. Click the **Get GMT** button to get GMT time from Internet if you have connected to Internet.

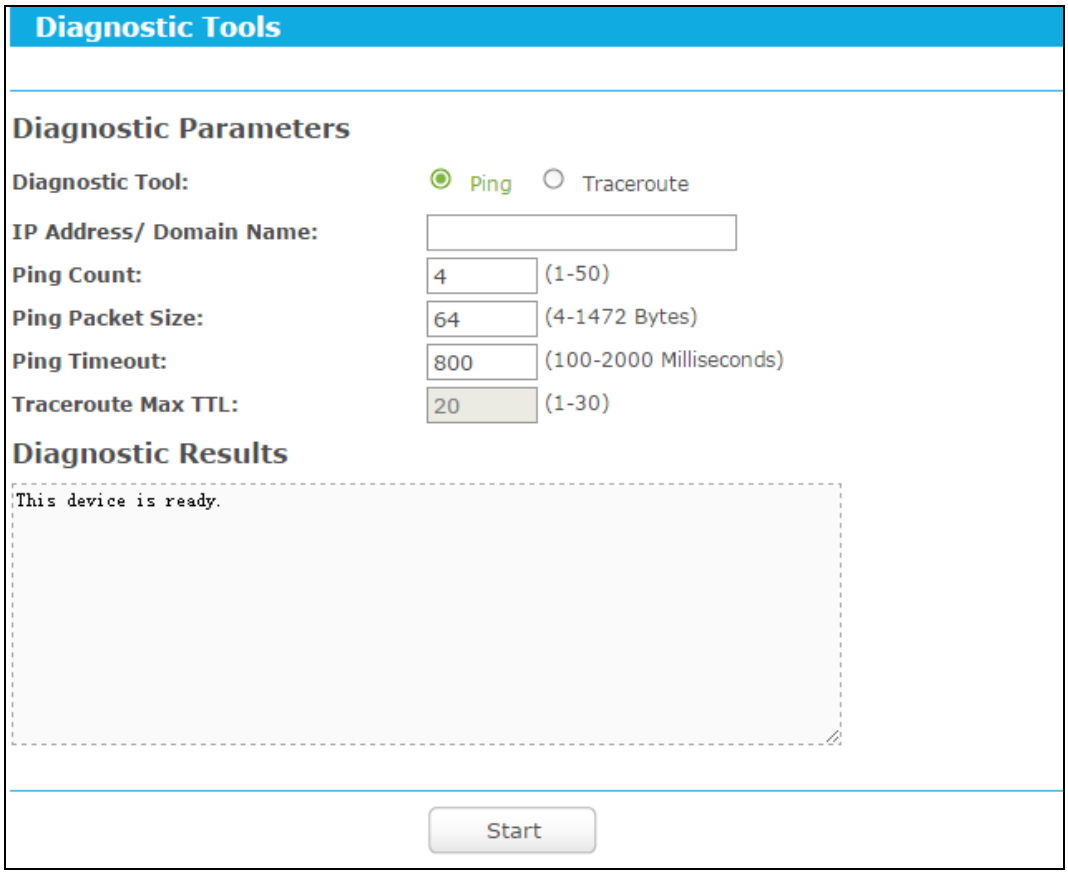
Note:

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

- The time will be lost if the router is turned off.
- The router will obtain GMT automatically from Internet if it has already connected to Internet.

8.14.3 Diagnostic

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



- **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

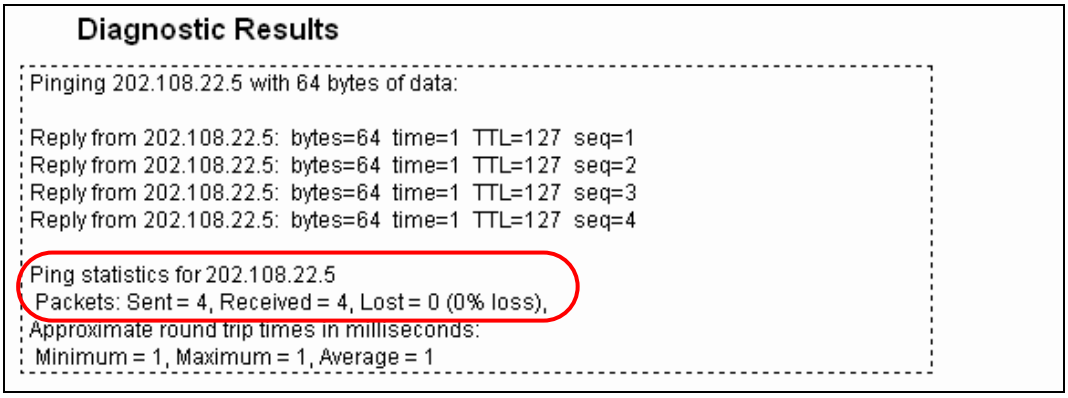
specifying can be resolved by using Domain Name System (DNS) queries.

- **IP Address/Domain Name -** Type the destination IP address (such as 202.108.22.5) or Domain name (such as www.baidu.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.

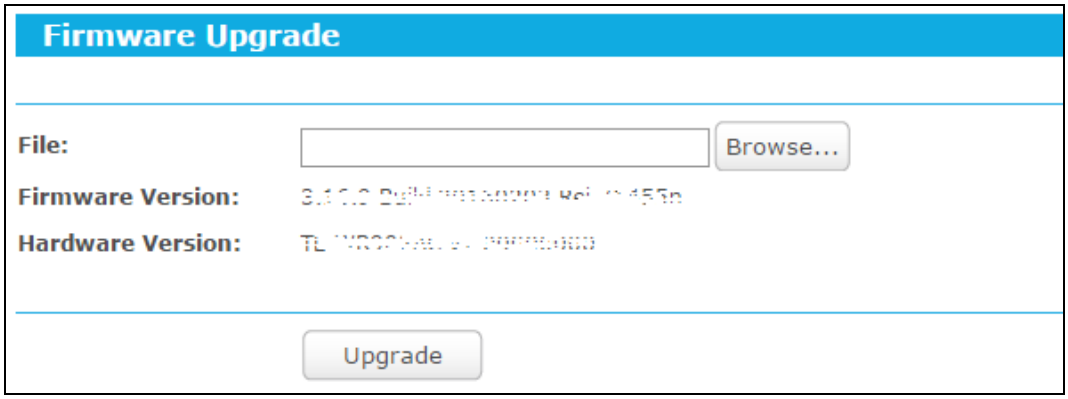


Note:

Only one user can use this tool at one time. "Ping Count", "Ping Packet Size" and "Ping Timeout" are Ping Parameters. "Traceroute Max TTL" is Traceroute Parameter.

8.14.4 Firmware Upgrade

The page allows you to upgrade the latest version firmware to keep your router up-to-date.



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

Note:

1. When you upgrade the router's firmware, you will lose current configuration settings, so make sure you backup the router's settings before you upgrade its firmware.
2. Make sure that your computer is connected to the Internet through the cable when you upgrade the firmware. To upgrade through wireless connection is not allowed.
3. Set your IP address as static IP before upgrading.

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

1. Download the latest firmware upgrade file from our website http://www.tp-link.com.
2. Enter or select the path name where you save the downloaded file on the computer into the **File** blank.
3. Click the **Upgrade** button.

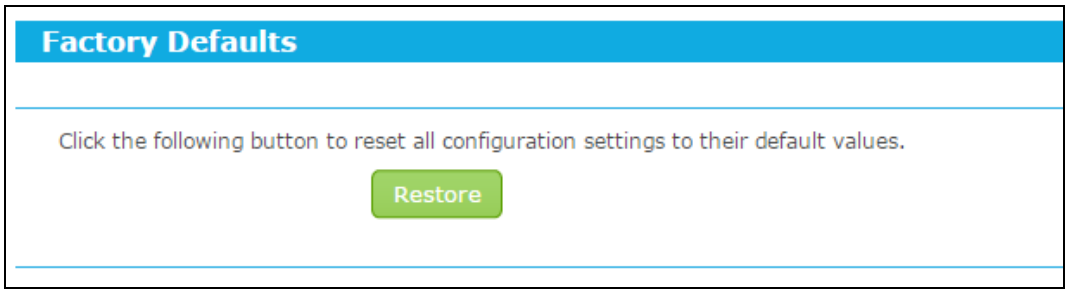
- **Firmware Version -** Displays the current firmware version.
- **Hardware Version -** Displays the current hardware version. The hardware version of the upgrade file must accord with the current hardware version.

Note:

The firmware version must correspond to the hardware. The upgrade process takes a few minutes and the Router will restart automatically when the upgrade is completed. It is important to keep power on during the entire process. Loss of power during the upgrade could damage the Router.

8.14.5 Factory Defaults

This page allows you to restore the factory default settings for the router.



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

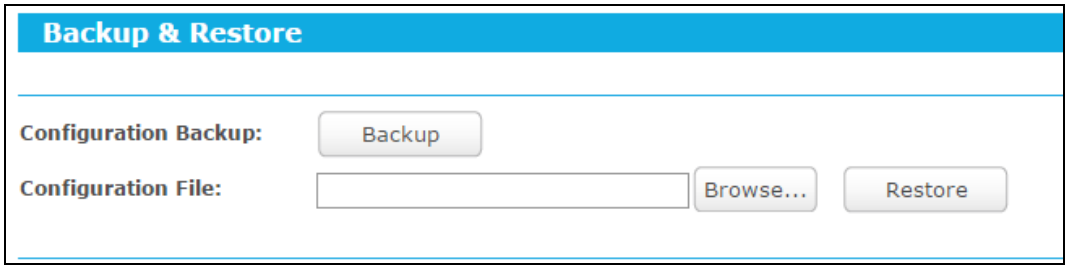
- The default User Name: admin
- The default Password: admin
- The default access: tplinkwifi.net

Note:

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

8.14.6 Backup & Restore

This page allows you to save current configuration of router as backup or restore the configuration file you saved before.



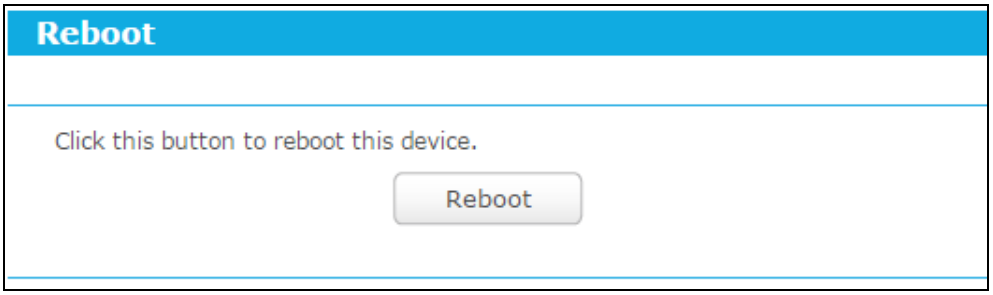
- Click the **Backup** button to save all configuration settings as a backup file in your local computer.
- To restore the router's configuration, follow these instructions:
  - Click the **Browse** button to select the backup file which you want to restore.
  - Click the **Restore** button.

Note:

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

8.14.7 Reboot

This page allows you to reboot the router.



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

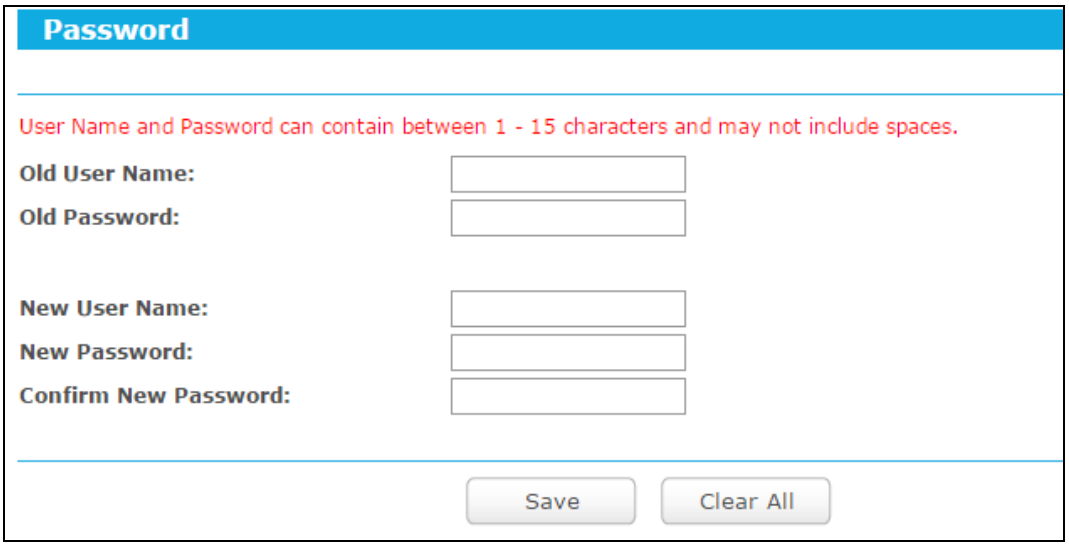
Some settings of the router will take effect only after rebooting, which include:

- Change LAN IP Address. (System will reboot automatically)
- MAC Clone (system will reboot automatically)
- DHCP service function.

- Static address assignment of DHCP server.
- Web Service Port of the router.
- Upgrade the firmware of the router (system will reboot automatically).
- Restore the router's settings to factory default (system will reboot automatically).

8.14.8 Password

This page allows you to change the factory default user name and password of the router.



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

Note:

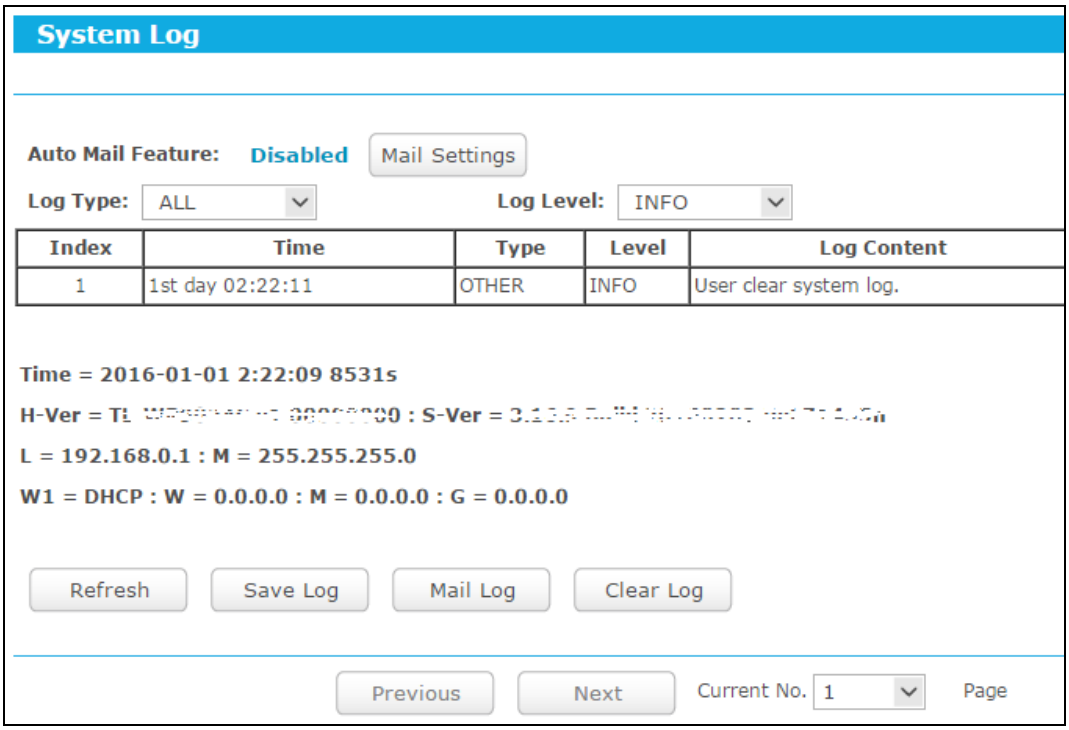
The new user name and password must not exceed 14 characters in length and must not include any spaces. Enter the new Password twice to confirm it.

Click the **Save** button when finished.

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

8.14.9 System Log

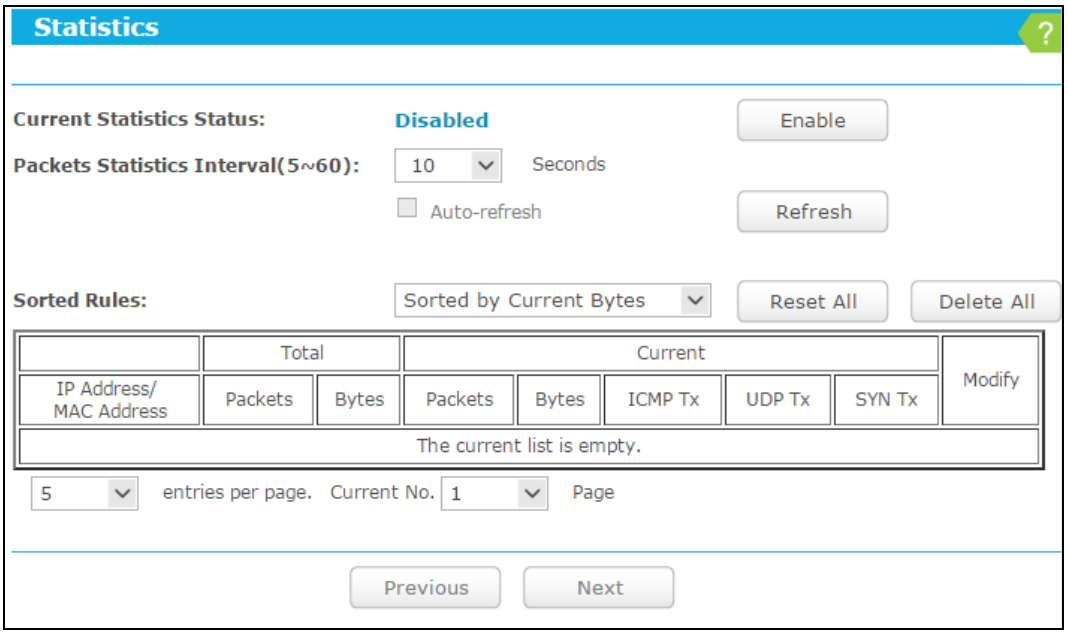
This page allows you to query the logs of the router.



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

8.14.10 Statistics

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



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

Statistics Table:

IP Address		The IP Address displayed with statistics
Total	**Packets**	The total amount of packets received and transmitted by the router.
	Bytes	The total amount of bytes received and transmitted by the router.
Current	**Packets**	The total amount of packets received and transmitted in the last **Packets Statistic interval** seconds.
	Bytes	The total amount of bytes received and transmitted in the last **Packets Statistic interval** seconds.
	ICMP Tx	The total amount of the ICMP packets transmitted to WAN in the last **Packets Statistic interval** seconds.
	UDP Tx	The total amount of the UDP packets transmitted to WAN in the last **Packets Statistic interval** seconds.
	TCP SYN Tx	The total amount of the TCP SYN packets transmitted to WAN in the last **Packets Statistic interval** seconds.

Click the **Save** button to save the **Packets Statistic interval** value.

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

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

8.15 Logout

Click the **Logout** tab at the bottom of the main menu, and then the web-page will be logged out and return to the login window.

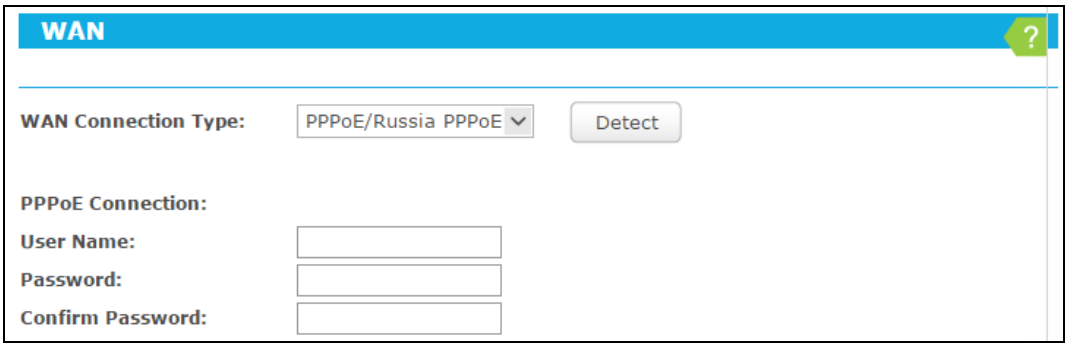
Appendix A: FAQ

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

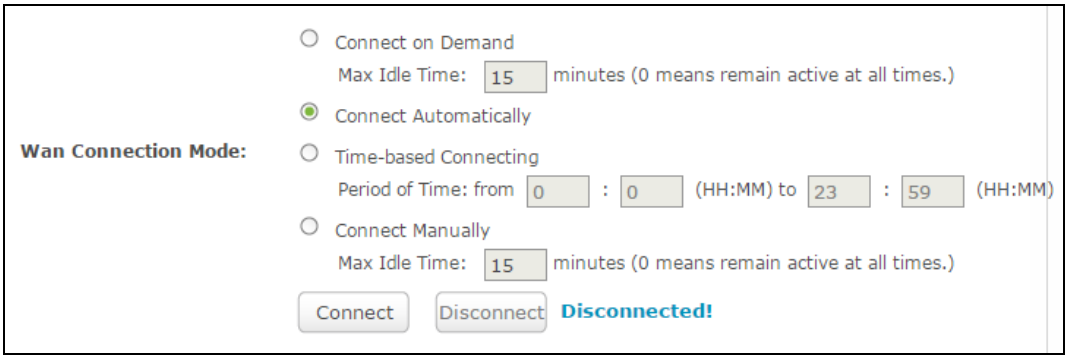
1) First, configure the ADSL Modem configured in RFC1483 bridge model.

2) Connect the Ethernet cable from your ADSL Modem to the WAN port on the Router. The telephone cord plugs into the Line port of the ADSL Modem.

3) Log in 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 and the "**Confirm Password**" field, and finish it by clicking **Connect**.



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.



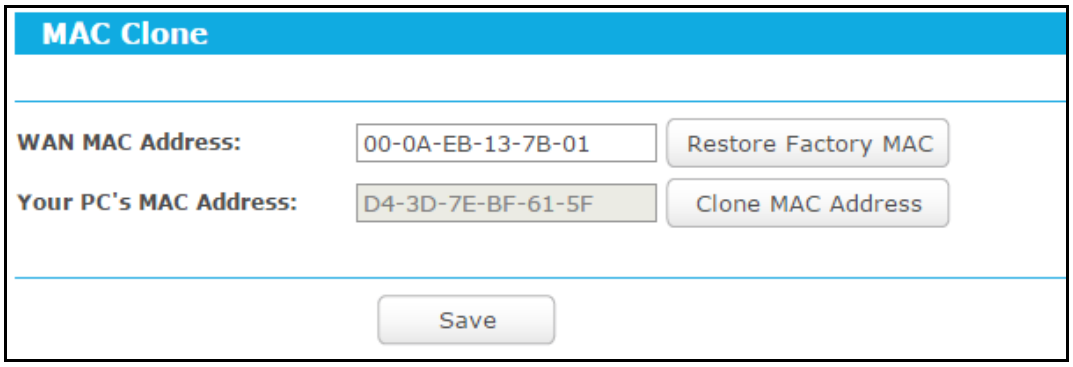
Note:

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

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

1) Log in 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, log in 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.

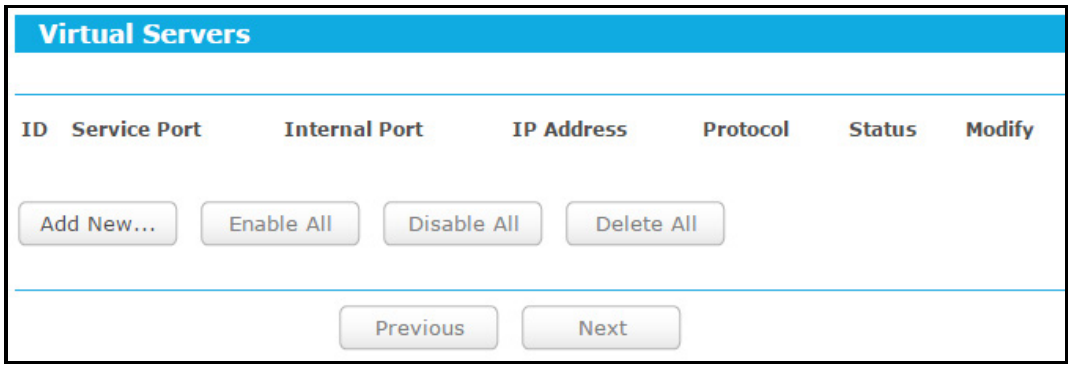


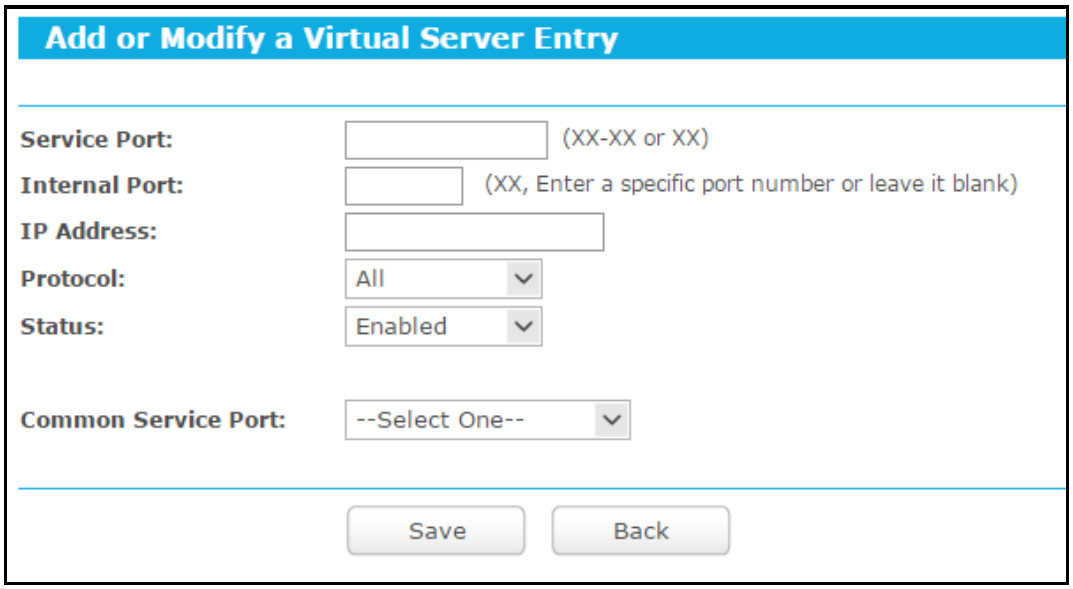
3. I want to use NetMeeting, what do I need to do?

1) If you start NetMeeting as a sponsor, you don’t need to do anything with the Router.

2) If you start as a response, you need to configure Virtual Server or DMZ Host 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**.

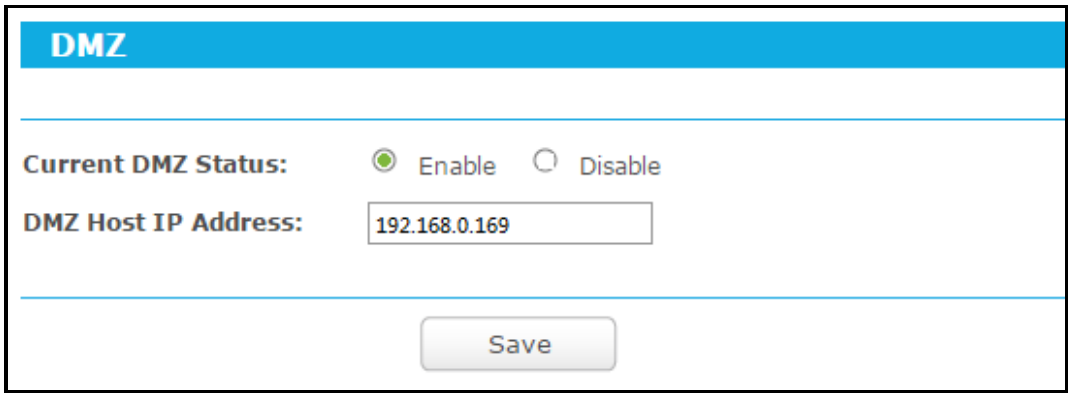




Note:

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

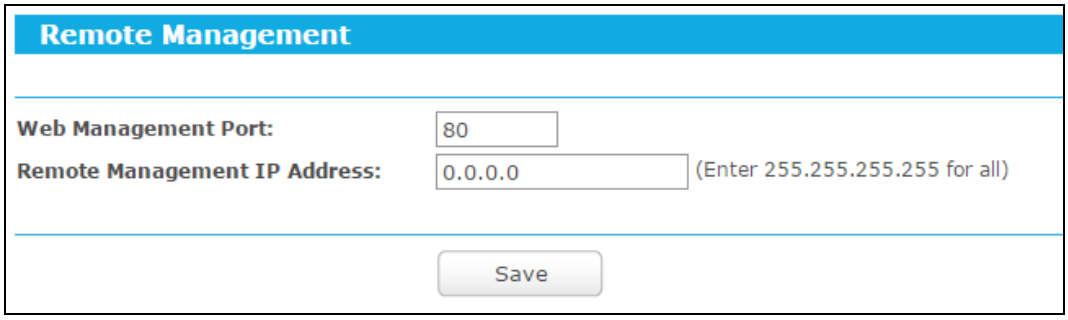
4) How to enable DMZ Host: Log in to the Router, click the “**Forwarding**” menu on the left of your browser, and click "**DMZ**" submenu. On the "DMZ" page, click **Enable** radio button and type your IP address into the “DMZ Host IP Address” field, using 192.168.0.169 as an example, remember to click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



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.

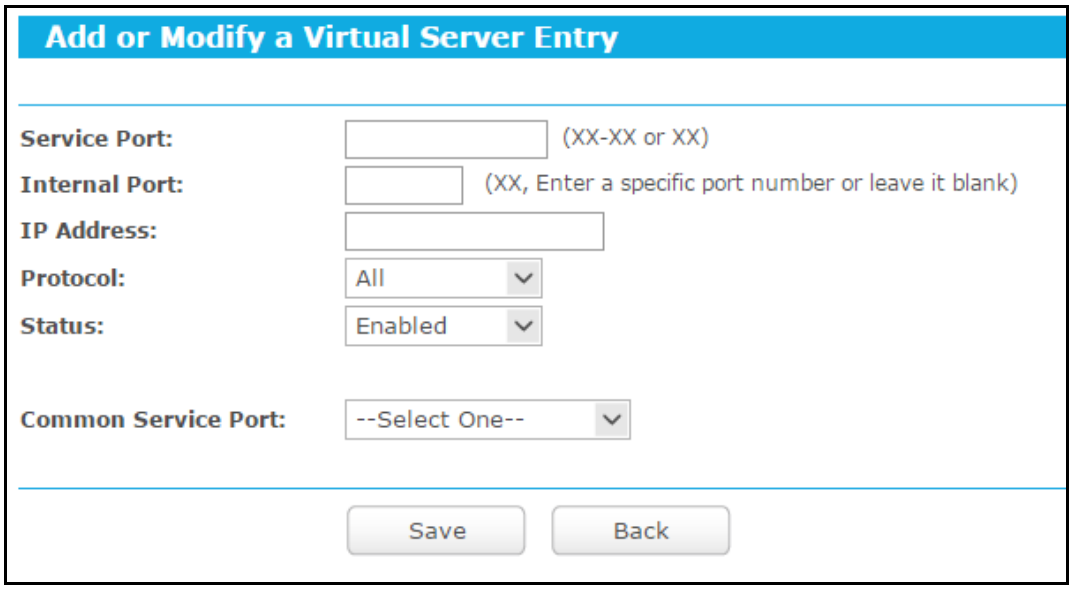
2) To change the WEB management port number: Log in to the Router, click the “**Security**” menu on the left of your browser, and click "**Remote Management**" submenu. On the "**Remote Management**" page, type a port number except 80, such as 88, into the "Web Management Port" field. Click **Save**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



Note:

If the above configuration takes effect, configure to the Router by typing 192.168.0.188 (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 “88” into the blank next to the “**Service Port**”, and your IP address next to the “**IP Address**”, assuming 192.168.0.88 for an example, remember to **Enable** and **Save**.



5. The wireless stations cannot connect to the Router.

1) Make sure the "**Enable Wireless Router Radio**" is checked.

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 PC

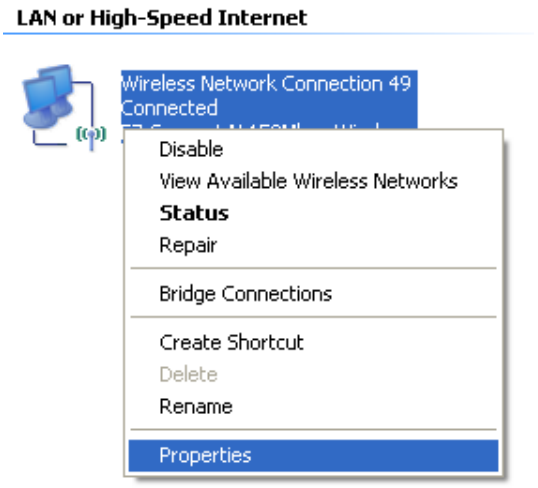
In this section, we'll introduce how to install and configure the TCP/IP correctly in Windows XP. First make sure your Ethernet Adapter is working, refer to the adapter's manual if necessary.

1. Configure TCP/IP component

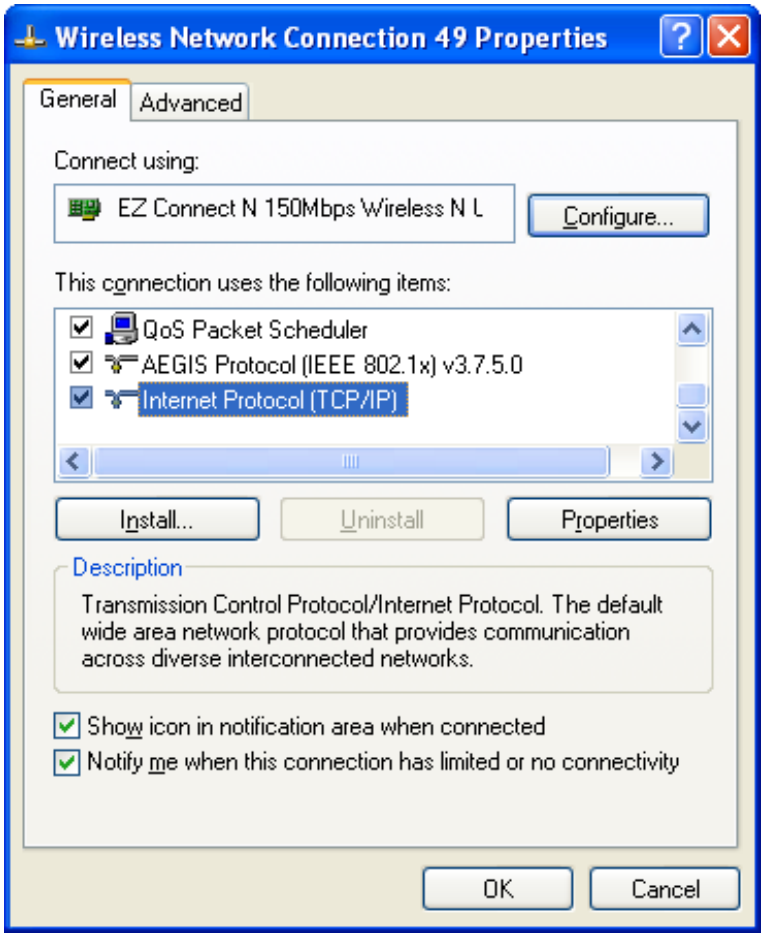
1) On the Windows taskbar, click the **Start** button, and then click **Control Panel**.

2) Click the **Network and Internet Connections** icon, and then click on the **Network Connections** tab in the appearing window.

3) Right click the icon that showed below, select Properties on the prompt page.

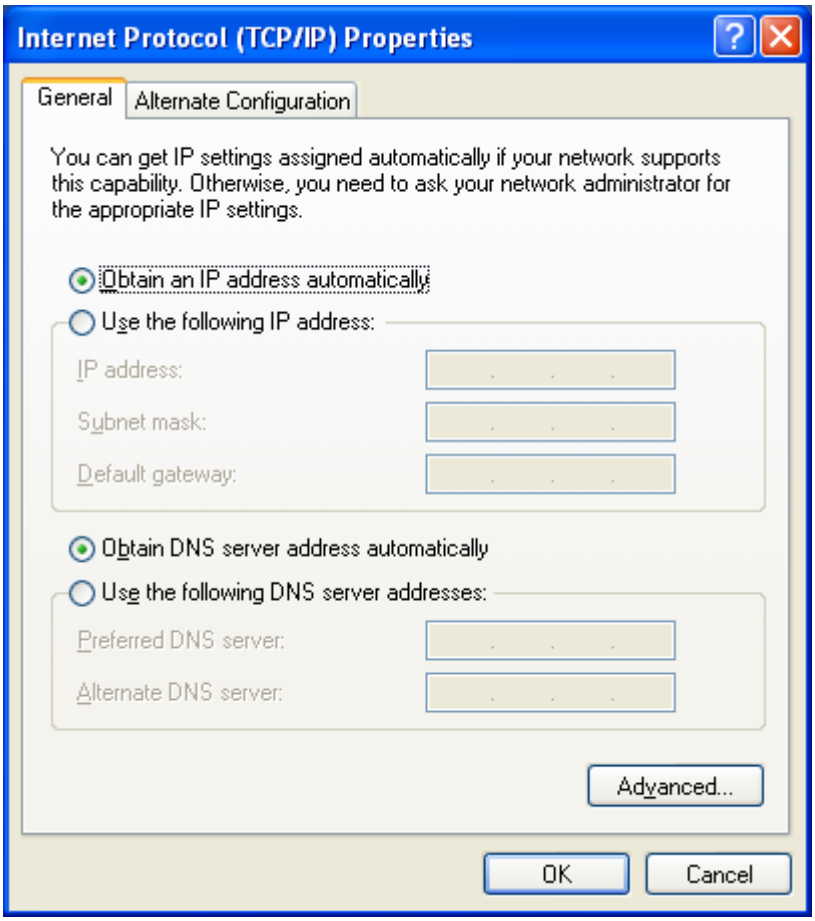


4) In the prompt page that showed below, double click on the **Internet Protocol (TCP/IP)**.



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

6) Select Obtain an IP address automatically, Choose Obtain DNS server automatically, as shown in the figure below:



Note:

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

7) Click **OK** to keep your settings.

Appendix C: Specifications

General	
Standards	5GHz：IEEE 802.11ac/n/a 2.4GHz：EEE 802.11b/g/n
Protocols	TCP/IP, PPPoE, DHCP, ICMP, NAT, SNTP
Port	One 10/100Mbps LAN/WAN 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)
LED	Power, Internet, Wireless, USB, WPS
Dimensions (L×W×H)	74mm×67mm×22mm
Safety & Emissions	FCC, CE
Wireless	
Frequency Band	2.4GHz, 5GHz（CE：5150~5250MHz；FCC：5150~5250MHz，5745~5825MHz）
Radio Data Rate	2.4G: up to 300Mbps（Automatic） 5G: up to 433Mbps （Automatic）
Frequency Expansion	DSSS(Direct Sequence Spread Spectrum)
Modulation	DBPSK, DQPSK, CCK, 16-QAM, 64-QAM, BPSK, QPSK
Security	64/128/152-bit WEP, WPA/WPA2, WPA2-PSK/WPA-PSK
Sensitivity @PER	2.4G： 135M: -70dBm@10% PER 65M: -72dBm@10% PER 54M: -75dBm@10% PER 6M: -89dBm@10% PER 5G： 135M: -68dBm@10% PER 65M: -71dBm@10% PER 54M: -75dBm@10% PER 6M: -91dBm@10% PER
Mode	Wireless Router Mode, Access Point Mode, Range Extender Mode, Client Mode, Hotspot Mode
Environmental and Physical	
Temperature	Operating : 0℃~40℃ (32℉~104℉)

	Storage:	-25℃~70℃(-13℉~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** (**Dem**ilitarized **Z**one) **-** A Demilitarized Zone allows one local host to be exposed to the Internet for a special-purpose service such as Internet gaming or videoconferencing.
- **DNS** (**D**omain **N**ame **S**ystem) **–** An Internet Service that translates the names of websites into IP addresses.
- **Domain Name -** A descriptive name for an address or group of addresses on the Internet.
- **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.