TP-LINK®

User Guide

TL-MR3420
3G/4G Wireless N Router

REV: 4.0.0
1910011461

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 © 2015 TP-LINK TECHNOLOGIES CO., LTD. All rights reserved.

http://www.tp-link.com

FCC STATEMENT

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

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

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

1） This device may not cause harmful interference.

2） This device must accept any interference received, including interference that may cause undesired operation.

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

Note: The manufacturer is not responsible for any radio or TV interference caused by unauthorized modifications to this equipment. Such modifications could void the user's authority to operate the equipment.

FCC RF Radiation Exposure Statement:

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

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

CE Mark Warning

CE1588

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 (1999/519/EC) 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

This device is intended for home and office use in all EU countries (and other countries following the EU directive 1999/5/EC) without any limitation except for the countries mentioned below:

Country	Restriction	Reason/remark
Belarus	Not implemented	
Norway	Implemented	This subsection does not apply for the geographical area within a radius of 20 km from the centre of Ny-Ålesund on Svalbard
Italy	Implemented	The public use is subject to general authorisation by the respective service provider
Russian Federation	Limited implementation	**1. SRD with FHSS modulation** 1.1. Maximum 2.5 mW e.i.r.p. 1.2. Maximum 100 mW e.i.r.p. Permitted for use SRD for outdoor applications without restriction on installation height only for purposes of gathering telemetry information for automated monitoring and resources accounting systems. Permitted to use SRD for other purposes for outdoor applications only when the installation height is not exceeding 10 m above the ground surface. 1.3.Maximum 100 mW e.i.r.p. Indoor applications **2. SRD with DSSS and other than FHSS wideband**

		modulation 2.1. Maximum mean e.i.r.p. density is 2 mW/MHz. Maximum 100 mW e.i.r.p. 2.2. Maximum mean e.i.r.p. density is 20 mW/MHz. Maximum 100 mW e.i.r.p. It is permitted to use SRD for outdoor applications only for purposes of gathering telemetry information for automated monitoring and resources accounting systems or security systems. 2.3. Maximum mean e.i.r.p. density is 10 mW/MHz. Maximum 100 mW e.i.r.p. Indoor applications
Ukraine	Limited implementation	e.i.r.p. ≤100 mW with built-in antenna with amplification factor up to 6 dBi

ATTENTION: Due to EU law, the country settings must be identical to the country where the device is operating (important due to non-harmonised frequencies in the EU).

Canadian Compliance Statement

This device complies with Industry Canada license-exempt RSSs. 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.）

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 & BSMI Notice

注意！

依據 低功率電波輻射性電機管理辦法

第十二條 經型式認證合格之低功率射頻電機，非經許可，公司、商號或使用者均不得擅自變更頻率、加大功率或變更原設計之特性或功能。

第十四條 低功率射頻電機之使用不得影響飛航安全及干擾合法通行；經發現有干擾現象時，應立即停用，並改善至無干擾時方得繼續使用。前項合法通信，指依電信規定作業之無線電信。低功率射頻電機需忍受合法通信或工業、科學以及醫療用電波輻射性電機設備之干擾。

減少電磁波影響，請妥適使用。

[警語]

「電磁波曝露量 MPE 標準值 1mW/cm^2，送測產品實測值為 ( ) mW/cm^2」

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.

EAC

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.

This product can be used in the following countries:

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

Use only power supplies listed in the user instructions

Switching Power Supply (Manufacturer：TP-LINK Model: T120100-2C1 Input: 100-240V~50/60HZ 0.3A Output:12V1A)

For applicable power supplies see user instructions

DECLARATION OF CONFORMITY

For the following equipment:

Product Description: **3G/4G Wireless N Router**

Model No.: **TL-MR3420**

Trademark: **TP-LINK**

We declare under our own responsibility that the above products satisfy all the technical regulations applicable to the product within the scope of Council Directives:

Directives 1999/5/EC, Directives 2004/108/EC, Directives 2006/95/EC, Directives 1999/519/EC, Directives 2011/65/EU

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

EN 300 328 V1.8.1

EN 301 489-1 V1.8.1:2008 & EN 301 489-17 V2.2.1

EN 55022:2010

EN 55024:2010

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

EN 61000-3-3:2008

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

EN62311:2008

The product carries the CE Mark:

CE1588

Person is responsible for marking this declaration:

Yang Hongliang
Product Manager of International Business

Date of issue: September 25, 2015

TP-LINK TECHNOLOGIES CO., LTD.

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

CONTENTS

Package Contents **1**

Chapter 1. Introduction **2**

1.1 Overview of the Router 2

1.2 Conventions 2

1.3 Main Features 2

1.4 Panel Layout 3

1.4.1 The Front Panel 3

1.4.2 The Rear Panel 4

1.4.3 The Side Panel 4

Chapter 2. Connecting the Router **5**

2.1 System Requirements 5

2.2 Installation Environment Requirements 5

2.3 Connecting the Router 5

Chapter 3. Quick Installation Guide **7**

3.1 TCP/IP Configuration 7

3.2 Quick Installation Guide 7

Chapter 4. Basic **11**

4.1 Network Map 11

4.2 Internet 12

4.3 Wireless 17

Chapter 5. Configuring the Router **18**

5.1 Status 18

5.2 Network 19

5.2.1 Internet Access 19

5.2.2 3G/4G 20

5.2.3 WAN 22

5.2.4 MAC Clone 30

5.2.5 LAN 31

5.3 Wireless 2.4GHz 32

5.3.1 Wireless Settings 32

5.3.2 WPS 34

5.3.3 Wireless Security 36

5.3.4 Wireless MAC Filtering 39

5.3.5 Wireless Advanced 41

5.3.6 Wireless Statistics 42

5.4 DHCP 43
5.4.1 DHCP Settings 43
5.4.2 DHCP Clients List 44
5.4.3 Address Reservation 44
5.5 Forwarding 46
5.5.1 Virtual Servers 46
5.5.2 Port Triggering 48
5.5.3 DMZ 50
5.5.4 UPnP 50
5.6 Security 51
5.6.1 Basic Security 52
5.6.2 Advanced Security 53
5.6.3 Local Management 55
5.6.4 Remote Management 56
5.7 Parental Control 56
5.8 Access Control 59
5.8.1 Rule 59
5.8.2 Host 64
5.8.3 Target 66
5.8.4 Schedule 68
5.9 Advanced Routing 70
5.9.1 Static Routing List 70
5.9.2 System Routing Table 71
5.10 Bandwidth Control 72
5.10.1 Control Settings 72
5.10.2 Rules List 72
5.11 IP & MAC Binding 74
5.11.1 Binding Settings 74
5.11.2 ARP List 75
5.12 Dynamic DNS 76
5.12.1 Comexe DDNS 76
5.12.2 Dyn DDNS 77
5.12.3 No-ip DDNS 78
5.13 IPv6 Support 79
5.13.1 IPv6 Status 79
5.13.2 IPv6 Setup 80
5.14 System Tools 88

5.14.1 Time Settings 89
5.14.2 Diagnostic 90
5.14.3 Firmware Upgrade 92
5.14.4 Factory Defaults 93
5.14.5 Backup & Restore 93
5.14.6 Reboot 94
5.14.7 Password 95
5.14.8 System Log 95
5.14.9 Statistics 98
Appendix A: FAQ 100
Appendix B: Configuring the PC 105
Appendix C: Specifications 109
Appendix D: Glossary 110
Appendix E: Compatible 3G/4G USB Modem 112

Package Contents

The following items should be found in your package:

- TL-MR3420 3G/4G Wireless N Router
- DC Power Adapter for TL-MR3420 3G/4G Wireless N Router
- Ethernet Cable
- Quick Installation Guide
- Resource CD for TL-MR3420 3G/4G Wireless N Router, including:
  - This Guide
  - Other Helpful Information

☞ **Note:**

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

Chapter 1. Introduction

1.1 Overview of the Router

TP-LINK understands the need for sharing the 3G/4G connection locally that benefits our end users. We realize the convenience with our latest wireless N 3G/4G Routers ----- they give you the freedom to quickly set up a stable and high speed wireless network, up to 300Mbps, on-the-go and share a 3G/4G connection. By connecting a USB Card to the Router, a Wi-Fi hotspot is instantly established allowing users to share a Internet connection anywhere 3G/4G coverage is available. So whether you're on the train, camping, or at a construction site, you'll have a reliable wireless connection to accommodate your networking needs.

3G/4G and WAN Broadband

The TL-MR3420 3G/4G Wireless N Router provides 3G/4G and WAN (xDSL, static IP, or dynamic IP) two kinds of broadband connections to get on the Internet, you can via the Internet no matter at home or outside on business. Automatic 3G/4G and WAN failover feature just provide nonstop internet connection.

Incredibly High Speed

TP-LINK 3G/4G Router provides up to 300Mbps, faster than that of traditional 11g products, surpasses 11G performance enabling the use of high bandwidth-consuming applications such as HD Videos.

Wi-fi Protected Setup

With just pressing on the 'WPS' button, the Router automatically establishes a WPA2 secure connection for solid security in under a minute.

1.2 Conventions

The Router or TL-MR3420 mentioned in this guide stands for TL-MR3420 3G/4G Wireless N Router without any explanation.

1.3 Main Features

- One 10/100M Auto-Negotiation RJ45 WAN port, four 10/100M Auto-Negotiation RJ45 LAN ports, supporting Auto MDI/MDIX
- Compatible with LTE/HSPA+/HSUPA/HSDPA/UMTS/EVDO USB modem
- Automatic 3G/4G and WAN failover
- Wireless N speed up to 300Mbps
- 2T2R MIMO, CCA technologies deliver greater coverage and higher speed
- Wireless security encryption easily at a push of "WPS" button
- WDS wireless bridge provides seamless bridging to expand your wireless network
- Backward compatible with 802.11b and 802.11g devices

- Provides WPA/WPA2-Enterprise, WPA/WPA2-Personal authentication, TKIP/AES encryption security
- Supports 3G/4G/Dynamic IP/Static IP/PPPoE/L2TP/PPTP Internet access
- Supports Virtual Server, Special Application and DMZ host
- Supports UPnP, Dynamic DNS, Static Routing
- Provides Automatic-connection and Scheduled Connection on certain time to the Internet
- Built-in NAT and DHCP server supporting static IP address distributing
- Connects Internet on demand and disconnects from the Internet when idle for PPPoE
- Provides 64/128-bit WEP encryption security and wireless LAN ACL (Access Control List)
- Supports Flow Statistics
- Supports IPv6.
- Supports firmware upgrade and Web management

1.4 Panel Layout

1.4.1 The Front Panel

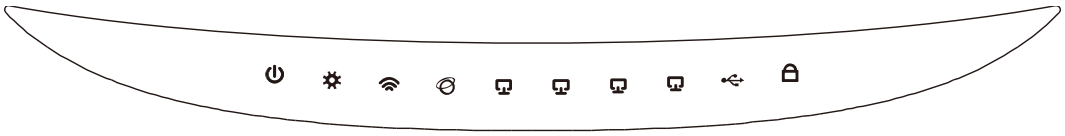


Figure 1-1 Front Panel sketch

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

Item	Status	Indication
(PWR)	On	Power is on.
	Off	Power is off.
(SYS)	On	The Router is initializing.
	Flashing	The Router is working properly.
	Off	The Router has a system error.
(WLAN)	Flashing	The Wireless function is enabled.
	Off	The Wireless function is disabled.
（WAN） （LAN1-4）	On	A device is linked to the corresponding port but there is no activity.
	Flashing	An active device is linked to the corresponding port.
	Off	No device is linked to the corresponding port.
（USB）	On	The USB 3G/4G modem is connected but no data being transferred.
	Flashing	Data is received or sent through the 3G/4G modem.
	Off	The USB 3G/4G modem is not connected.
（WPS）	Slow Flash	A wireless device is connecting to the network by WPS function. This process will last in the first 2 minutes.
	On	A wireless device has been successfully added to the network by WPS function.
	Quick Flash	A wireless device failed to be added to the network by WPS function.

Table 1-1 The LEDs description

☞ **Note:**

After a device is successfully added to the network by WPS function, the WPS LED will keep on for about 5 minutes and then turn off.

1.4.2 The Rear Panel

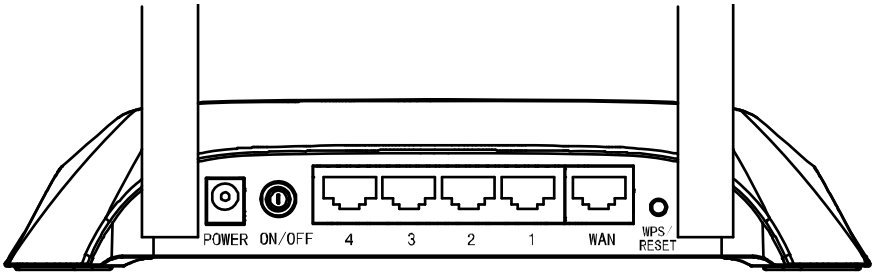


Figure 1-2 Rear Panel sketch

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

- **POWER:** The Power socket is where you will connect the power adapter. Please use the power adapter provided with this TL-MR3420 3G/4G Wireless N Router.
- **ON/OFF:** The switch is for you to turn on/off the Router, but only with the Router powered on.
- **4,3,2,1 (LAN):** These ports (4,3,2,1) connect the Router to the local PC(s)
- **WAN:** This WAN port is where you will connect the DSL/cable Modem, or Ethernet
- **WPS/RESET:**

  There are two ways to reset to the Router's factory defaults:

  1) Use the **Factory Defaults** function on "**System Tools** -> **Factory Defaults**" page in the Router's Web-based Utility.
  2) Use the Factory Default **Reset** button: With the Router powered on, use a pin to press and hold the **WPS/RESET** button (about 5 seconds) until the SYS LED becomes quick-flash from slow-flash. And then release the button and wait the Router to reboot to its factory default settings.
- **Wireless antenna:** To receive and transmit the wireless data.

1.4.3 The Side Panel

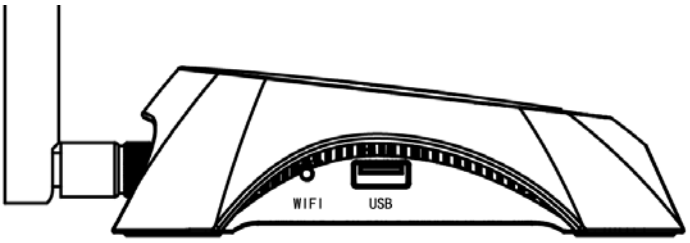


Figure 1-3 Side Panel sketch

The following parts are located on the side plate (View from left to right).

- **WIFI:** This switch is an easy and convenient operation for you to turn on or off the wireless network.
- **USB:** Connect to the USB Modem.

Chapter 2. Connecting the Router

2.1 System Requirements

- 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.)
- PCs with a working Ethernet Adapter and an Ethernet cable with RJ45 connectors
- TCP/IP protocol on each PC
- Web browser, such as Microsoft Internet Explorer 5.0 , Netscape Navigator 6.0 or above

2.2 Installation Environment Requirements

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

2.3 Connecting the Router

Before installing the Router, make sure your PC is connected to the Internet through the broadband service successfully. If there is any problem, please contact your ISP. After that, please install the Router according to the following steps. Don't forget to pull out the power plug and keep your hands dry.

1. Power off your Cable/DSL Modem, and the Router.
2. Locate an optimum location for the Router. The best place is usually at the center of your wireless network. The place must accord with the Installation Environment Requirements.
3. Adjust the direction of the antenna. Normally, upright is a good direction.
4. Connect the PC(s) or Switch/Hub in your LAN to the LAN Ports of the 3G/4G Router with Ethernet cable.
5. The 3G/4G Router supports both 3G/4G and WAN connection; so you can insert 3G/4G USB Modem to the USB port of the Router (as shown in Figure 2-1), or connect the DSL/Cable Modem to the WAN port of the Router (as shown in Figure 2-2). Please visit our website http://www.tp-link.com to get the latest USB modems compatibility, and we recommend you to check whether the modem in your hand has already been tested by us.
6. Connect the power adapter to the power socket on the Router, and the other end into an electrical outlet. The Router will start to work automatically.
7. Power on your Cable/DSL Modem.

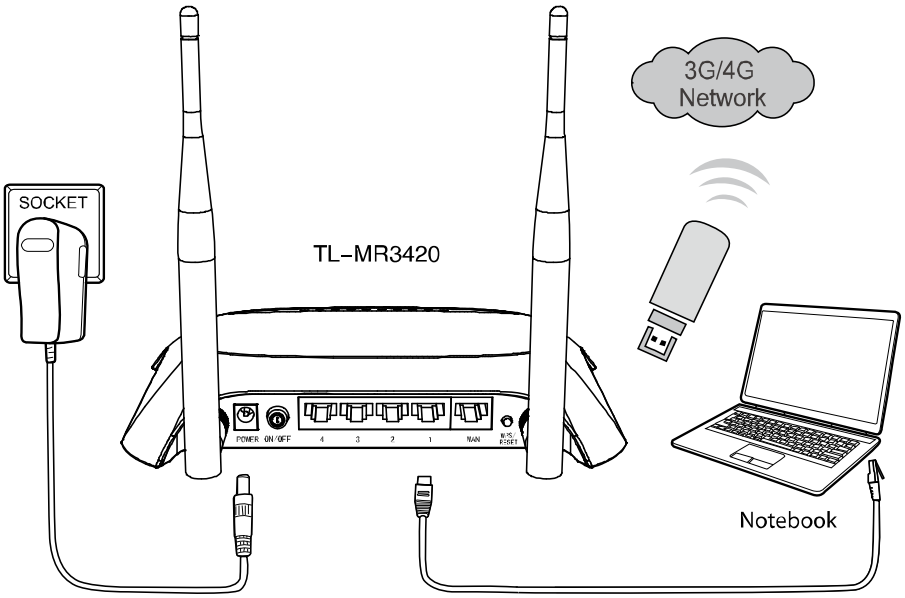


Figure 2-1 Hardware Installation – 3G/4G connection

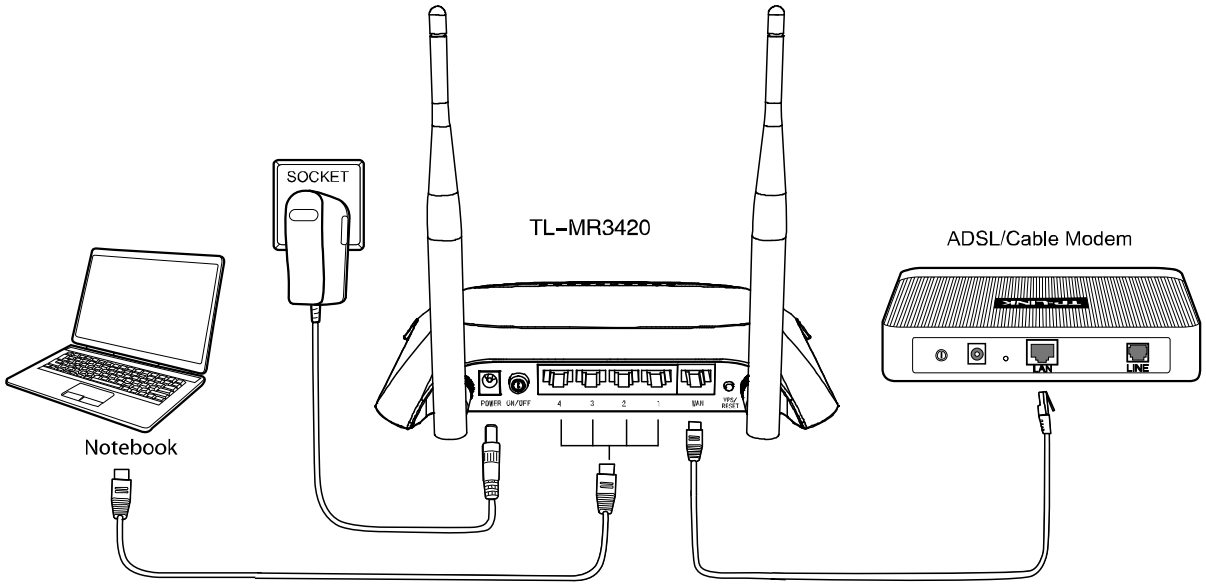


Figure 2-2 Hardware Installation – WAN connection

Chapter 3. Quick Installation Guide

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

3.1 TCP/IP Configuration

The default IP address of the 3G/4G Wireless N Router is 192.168.0.1. 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.

Connect the local PC to the LAN ports of the Router. And then you can configure the IP address for your PC in the following two ways.

- Configure the IP address manually

1) Set up the TCP/IP Protocol for your PC. If you need instructions as to how to do this, please refer to Appendix B: "Configuring the PC."
2) Configure the network parameters. The IP address is 192.168.0.xxx ("xxx" is any number from 2 to 254), Subnet Mask is 255.255.255.0, and Gateway is 192.168.0.1 (The Router's default IP address)

- Obtain an IP address automatically

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.

3.2 Quick Installation Guide

☞ **Note:**

If you are trying to connect to TL-MR3420 wirelessly, please refer to the label on the bottom of the Router for the **Wireless Password**.

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.

Figure 3-1 Login the Router

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

Figure 3-2 Login Windows

Note:

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

2. After successful login, the **Quick Setup** page will appear for you to select your **Region** and **Time zone**. After finishing the selection, click **Next**.

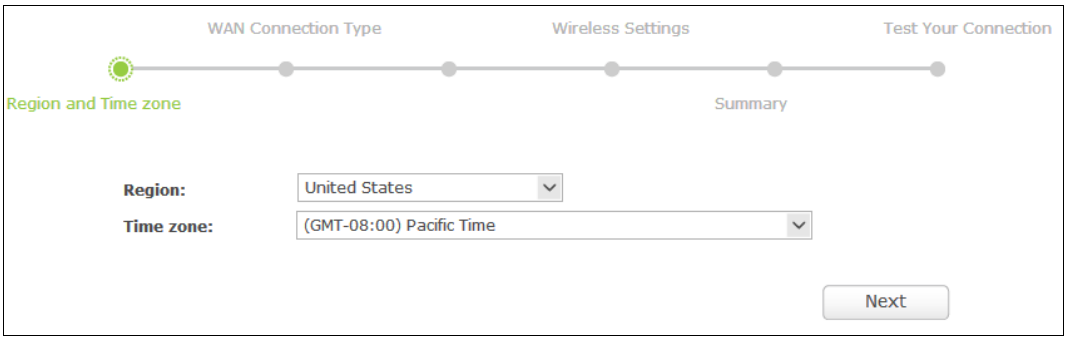
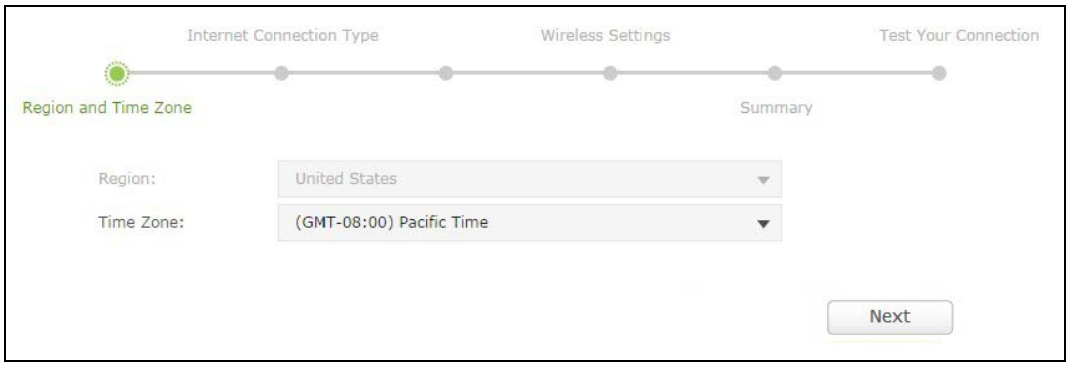


Figure 3-3 Quick Setup

Note:

Per FCC regulations, all Wi-Fi products marketed in the U.S. must be fixed to the U.S. region only.



3. Select a desired **Internet Access** mode and then click **Next**. The configuration for each mode is similar. As follows we will take **3G/4G Only** mode for example.

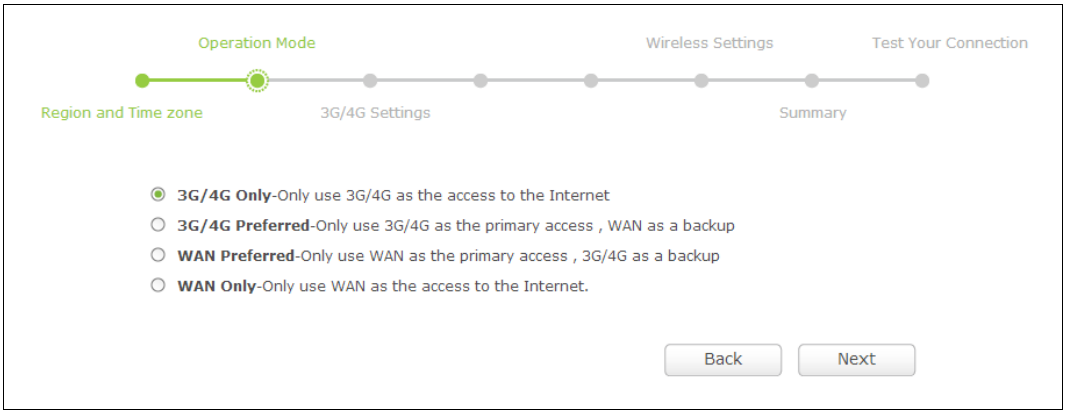


Figure 3-4 Choose Internet Access Mode

- **3G/4G Only**

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

- **3G/4G Preferred**

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

- **WAN Preferred**

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

- **WAN Only**

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

4. The next screen will appear as shown in Figure 3-5. You need to set the required parameters and then click **Next**.

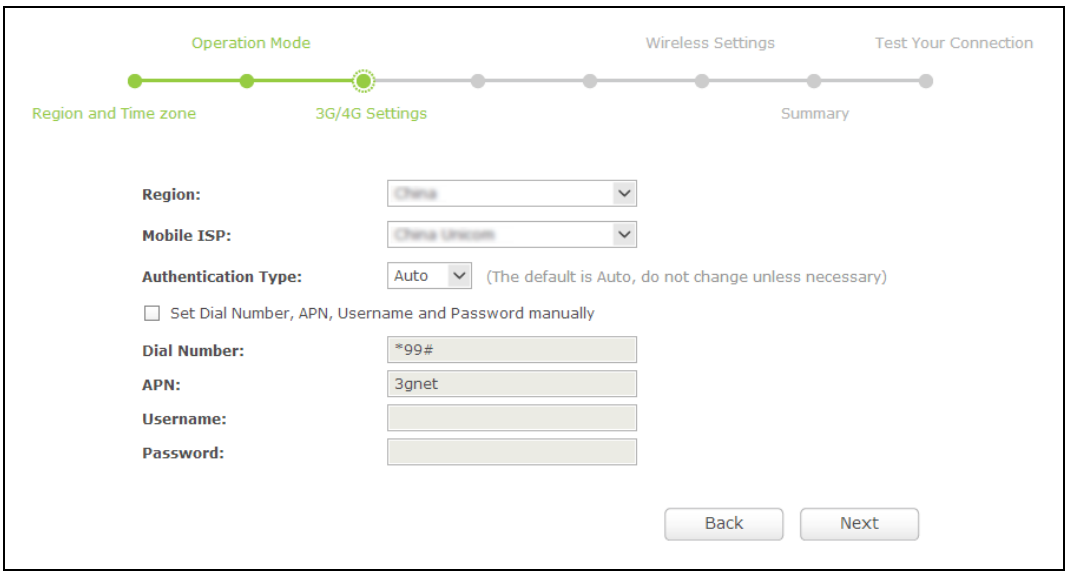


Figure 3-5

- **Region -** Select the location where you're enjoying the 3G/4G card.

- **Mobile ISP -** Select the ISP (Internet Service Provider) you apply to for 3G/4G service. The Router will show the default Dial Number and APN of that ISP. If your ISP is not listed in the **Mobile ISP**, check the box before **Set the Dial Number, APN, Username and Password manually** and fill the Dial Number and APN blanks below.
- **Authentication Type -** Some ISPs need a specific authentication type. Please confirm it with your ISP or keep it Auto.
- **Dial Number & APN -** Set these two parameters manually after **Set the Dial Number, APN, Username and Password manually** is checked.
- **Username/Password -** Enter the Username and Password provided by your ISP. These fields are optional but case-sensitive.

5. Configure the Wireless settings on the screen as shown in Figure 3-6, then click **Next**.

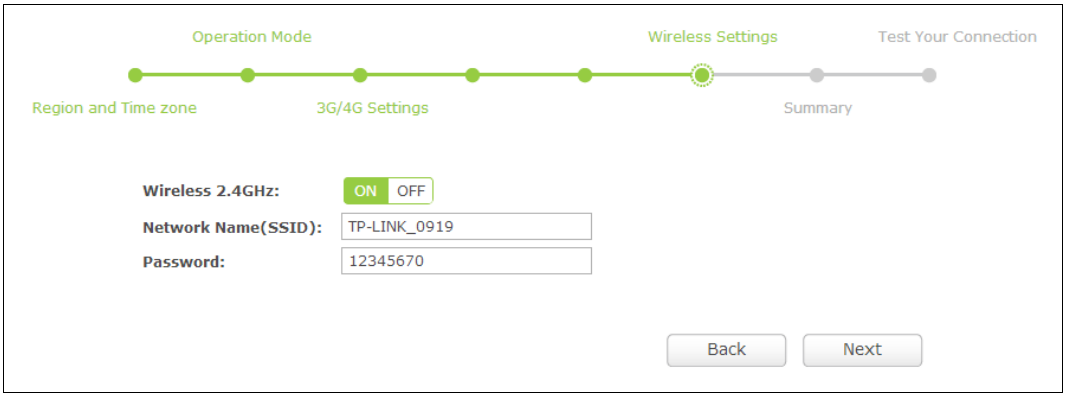


Figure 3-6 Quick Setup – Wireless

- **Wireless 2.4GHz -** Displays whether the wireless function is enabled or not.
- **Network Name (SSID) -** Also called the SSID (Service Set Identification). Enter a value of up to 32 characters. The same name must be assigned to all wireless devices in your network. This value is case-sensitive. For example, *TEST* is NOT the same as *test*.
- **Password -** Create a password for your wireless network.

6. Click **Finish** to complete the **Quick Setup**.

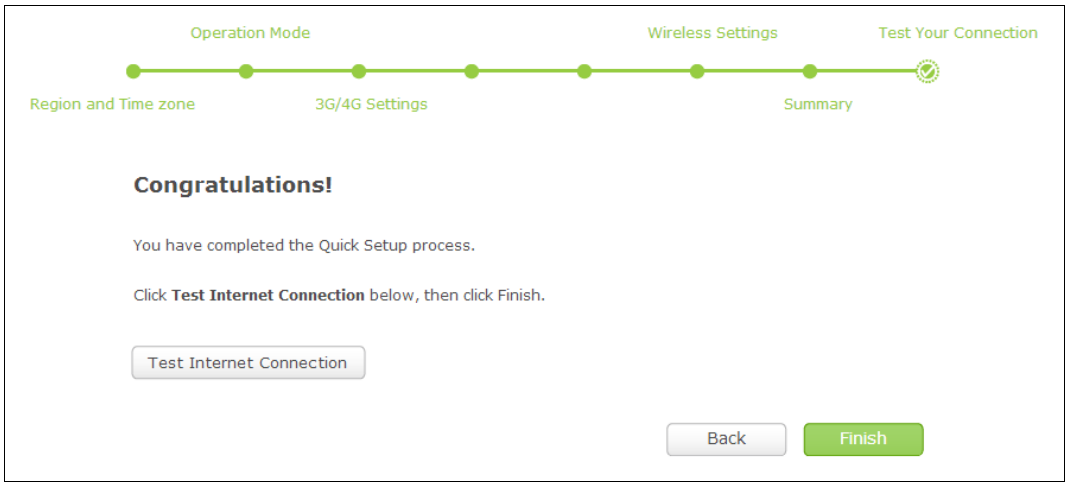


Figure 3-7 Quick Setup – Finish

After the rebooting, please check whether you can access the Internet or not in the 5.1 Status page.

Chapter 4. Basic

4.1 Network Map

Network Map provides a router-centered dashboard that lets you see the status of your Internet connection and network at a glance. You can click any of the six sections of the dashboard to view the detail information. All the information is read-only.

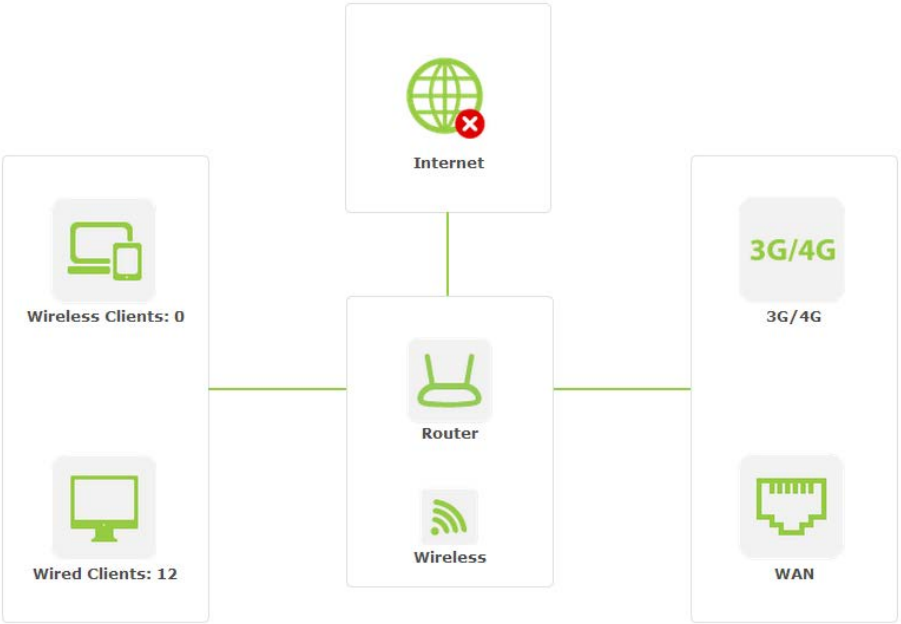


Figure 4-1 Network Map

- **Internet -** Click to view the ISP settings of your router.
- **Wireless Clients -** Click to view the wireless devices connected to your network.
- **Wired Clients -** Click to view the wired devices connected to your network.
- **Wireless -** Click to view or change the wireless settings for your router.
- **3G/4G –** Click to view or change the parameters apply to the 3G/4G USB modem of the Router.
- **USB Disk -** Click to view the information of the USB storage device connected to your network.

4.2 Internet

Choose menu "**Basic→Internet**", and you can view or change the basic ISP information for your router.

- **3G/4G**

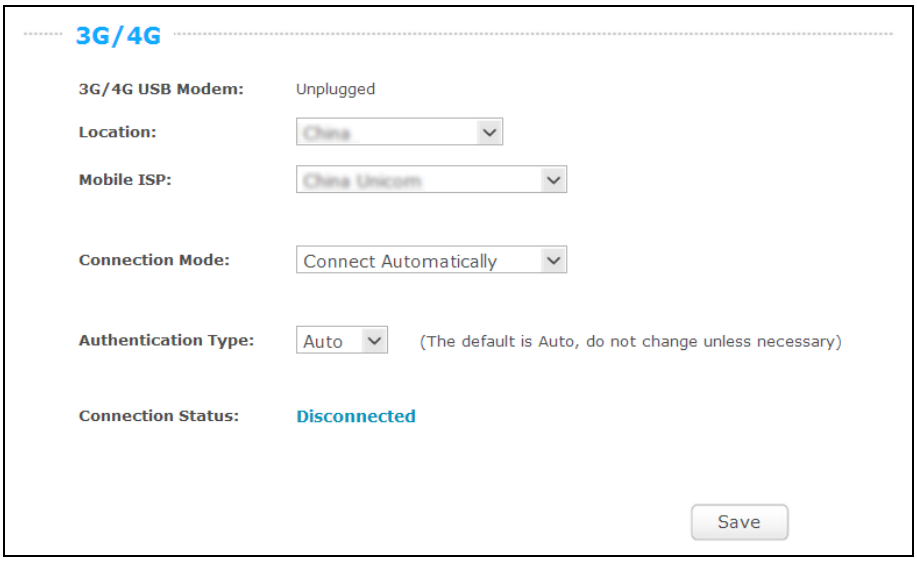


Figure 4-2 Internet

- **3G/4G USB Modem -** 3G/4G device status Plugged or Unplugged.
- **Location -** Please select the location where you're enjoying the 3G/4G card.
- **Mobile ISP -** Please select the ISP(Internet Service Provider) you apply to for 3G/4G service. The router will show the default Dial Number and APN of that ISP.
- **Connection Mode -** Please select the Connection Mode to accessing the Internet with 3G/4G.

  Connect on Demand - You can configure the Router to disconnect your Internet connection after a specified period of the Internet connectivity (**Max Idle Time**). If your Internet connection has been terminated due to inactivity, **Connect on Demand** enables the Router to automatically re-establish your connection as soon as you attempt to access the Internet again. If you wish to activate **Connect on Demand**, click the radio button. If you want your Internet connection to remain active at all times, enter **0** in the **Max Idle Time** field. Otherwise, enter the number of minutes you want to have elapsed before your Internet connection terminates.
  Note - Sometimes the connection cannot be disconnected although you specify a time to **Max Idle Time** because some applications visit the Internet continually in the background.

  Connect Automatically - Connect automatically after the Router is disconnected. To use this option, click the radio button.
  Connect Manually - You can configure the Router to make it connect or disconnect manually. After a specified period of inactivity (**Max Idle Time**), the Router will disconnect your Internet connection, and not be able to re-establish your connection

automatically as soon as you attempt to access the Internet again. To use this option, click the radio button. If you want your Internet connection to remain active at all times, enter **0** in the **Max Idle Time**field. Otherwise, enter the number in minutes that you wish to have the Internet connecting last unless a new link requested.

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

- **Authentication Type -** Some ISPs need a specifical authentication type, please confirm it with your ISP or keep it Auto. There are three choices:

  Auto : The router will have dynamic negotiation with the dialing server and the **Autnentication Type** need not to be specified. The default type is Auto.

  PAP : Password Authentication Protocol. This protocol allows the router to establish authentication with the peer using two handshakes. Select this option if the ISP requires this authentication type.

  CHAP : Challenge Handshake Authentication Protocol. This protocol allows the route to establish authentication with the peer using three handshakes and checking the peer identity periodically. Select this option if the ISP requires this authentication type.

- **Connection Status -** 3G/4G Connection status: Disconnected,Connected Or Connecting.

WAN

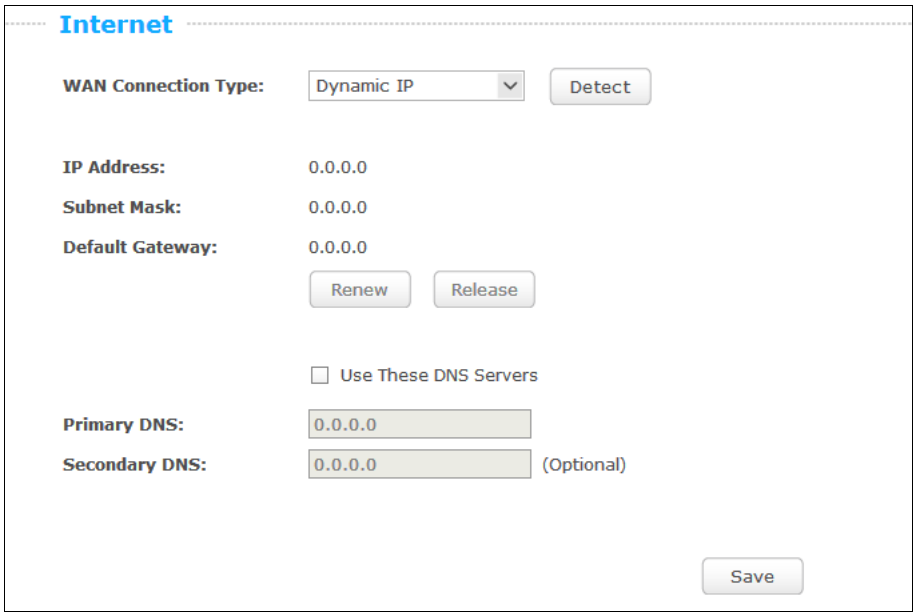


Figure 4-3 Dynamic IP

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 shown below.

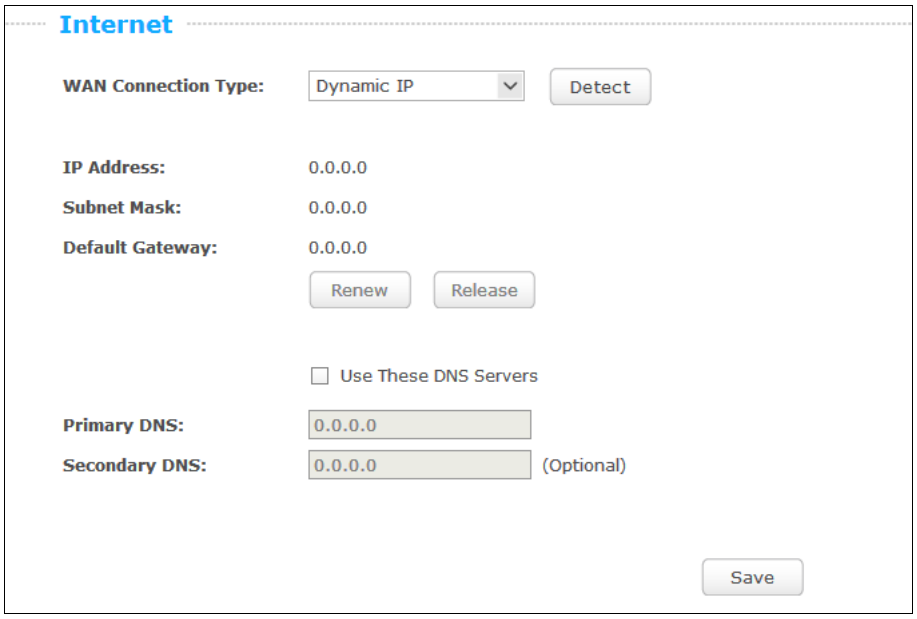


Figure 4-4 Dynamic IP

- **IP Address -** Assigned dynamically by your ISP.
- **Subnet Mask -** Assigned dynamically by your ISP.
- **Default Gateway -** Assigned dynamically by your ISP.

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

- **Primary/Secondary DNS -** 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.

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

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

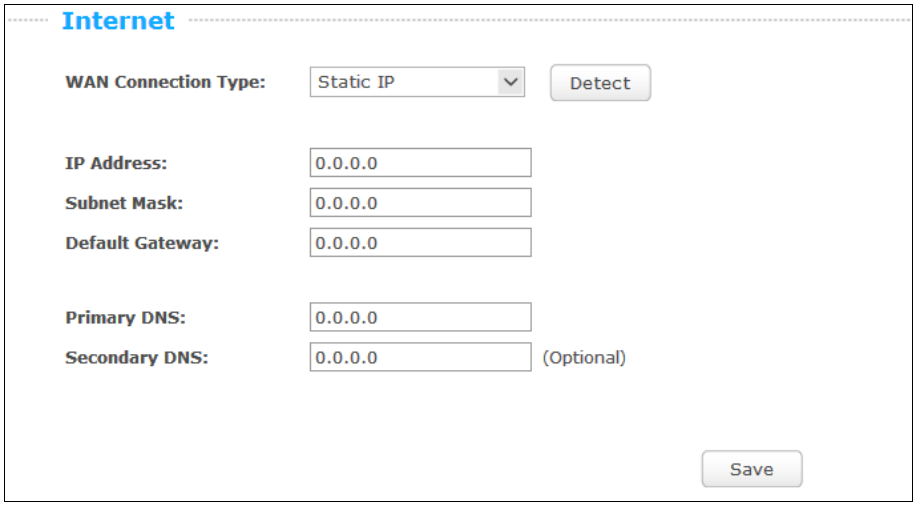


Figure 4-5 Static IP

- **IP Address -** Enter the IP address in dotted-decimal notation provided by your ISP.
- **Subnet Mask -** Enter the subnet Mask in dotted-decimal notation provided by your ISP, usually is 255.255.255.0.
- **Default Gateway -** Enter the gateway IP address in dotted-decimal notation provided by your ISP.
- **Primary/Secondary DNS -** 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. And you should enter the following parameters in the screen below.

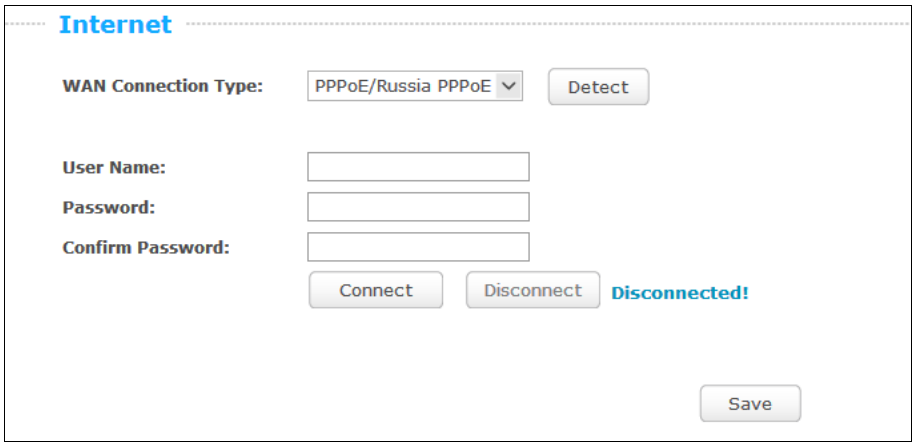


Figure 4-6 PPPoE

- **User Name/Password -** Enter the User Name and Password provided by your ISP. These fields are case-sensitive. Click the **Connect** button to connect immediately. Click the **Disconnect** button to disconnect immediately.

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

4. If your ISP provides L2TP connection, please select **L2TP/Russia L2TP** option. And you should enter the following parameters in the screen below.

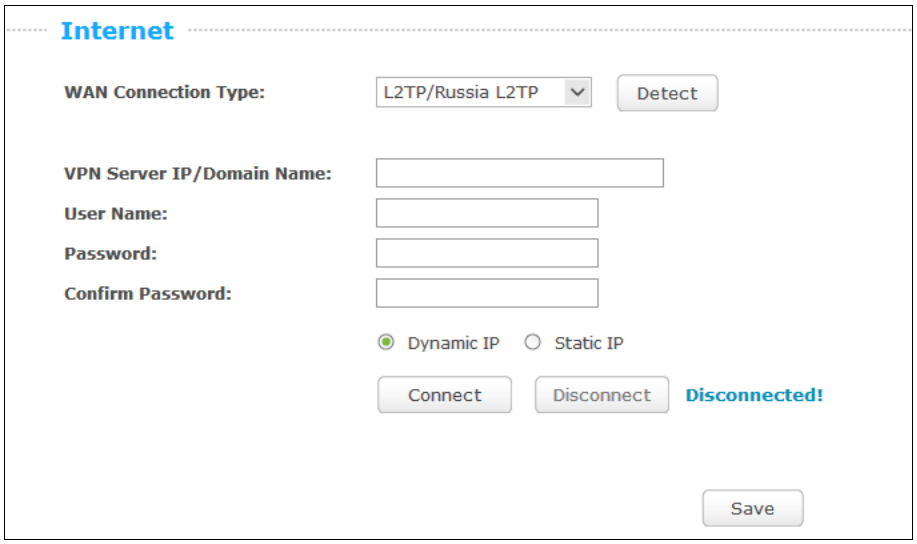


Figure 4-7 L2TP/Russia L2TP

- **VPN Server IP/Domain Name -** Enter the IP address or domain name of your VPN server.
- **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.

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 (Figure 5-10).

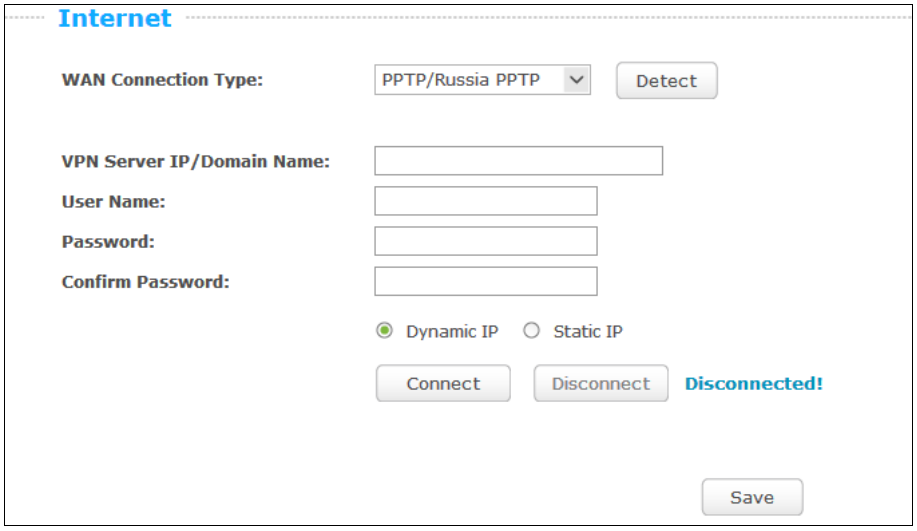


Figure 4-8 PPTP/Russia PPTP

- **VPN Server IP/Domain Name -** Enter the IP address or domain name of your VPN server.
- **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.

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

☞ **Note:**

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

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

The router cannot detect PPTP and L2TP connections with your ISP. If your ISP uses one of these protocols, then you must configure your connection manually.

4.3 Wireless

Choosing menu "**Basic→Wireless**", you can configure the basic settings for the wireless network

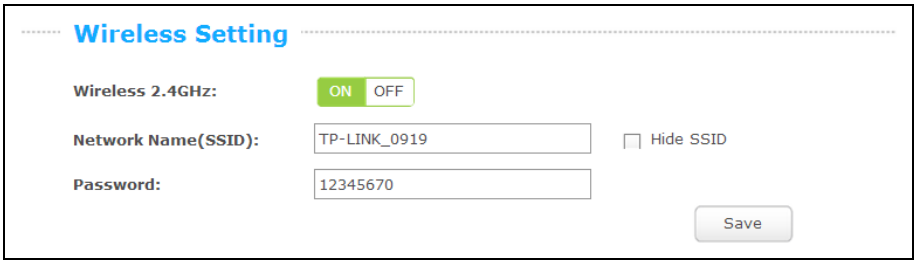


Figure 4-9 Wireless Setting

- **Wireless 2.4GHz -** Select **ON** to enable your wirelessnetwork, and select **OFF** to disable your wireless network.
- **Network Name (SSID) -** Create a name (up to 32 characters) for your wireless network. If the **Hide SSID** checkbox is selected, the SSID of your wireless network will be hidden from the Wi-Fi network.
- **Password -** Create a password for your wireless network. The password must have a minimum of 8 characters in length.

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

Chapter 5. Configuring the Router

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

5.1 Status

Choose menu "**Advanced→Status**", you can see the current status information about the router.

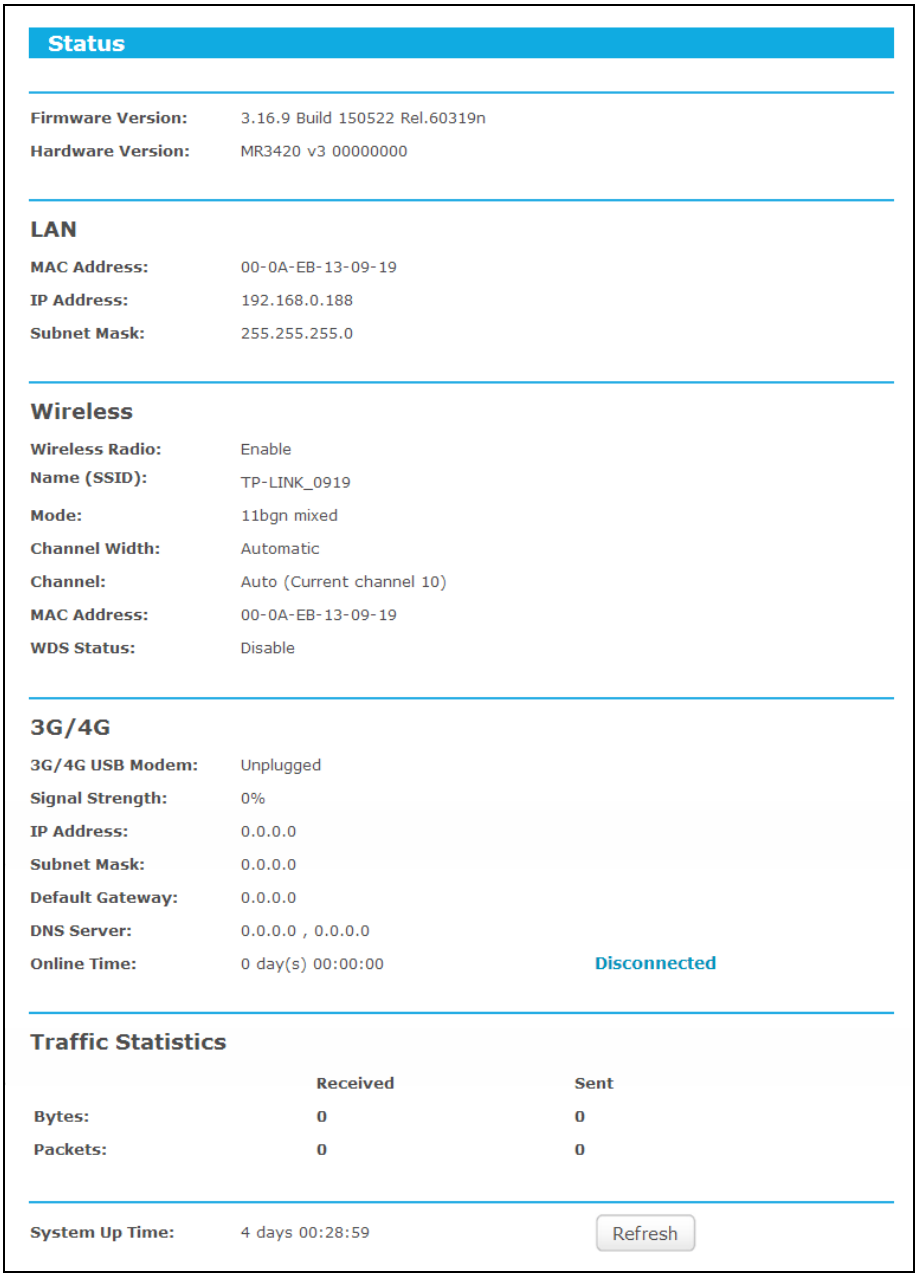


Figure 5-1 Status

5.2 Network

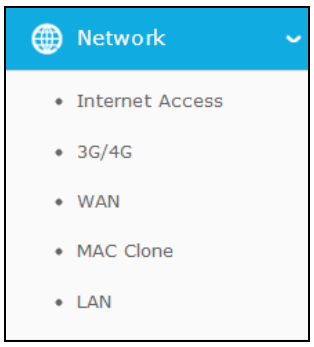


Figure 5-2 the Network menu

There are three submenus under the Network menu as shown in Figure 5-2: **Inernet Access**, **3G/4G**, **WAN**, **MAC Clone**, and **LAN**. Click any of them, and you will be able to configure the corresponding function.

5.2.1 Internet Access

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

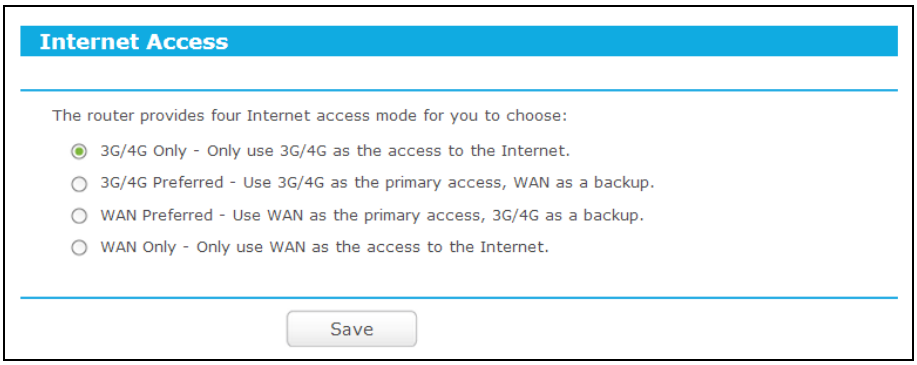


Figure 5-3 Status

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

- When the router succeeds to connect to the WAN network, the router would stop the 3G/4G connection and switch back to WAN access immediately.

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

Note:

1. If you are using the **3G/4G Preferred** or **WAN Preferred**, the router would connect, disconnect or switch the current access automatically. The Connect/Disconnect button (on 3G/4G, PPPoE, PPTP, L2TP) and some related parameters could not be set manually.
2. Only when the WAN connection is Dynamic IP, Static IP or PPPoE can the router support the switch between 3G/4G mode and WAN mode.

5.2.2 3G/4G

Choose menu "**Network→3G/4G**", you can configure parameters for 3G/4G function on the screen below. To use the 3G/4G function, you should first insert your USB modem on the USB port of the Router. There is already much 3G/4G USB modem information embedded in the Router. The USB modem parameters will be set automatically if the card is supported by the Router. If your USB modem inserted is supported by the Router, then "**Identify successfully**" will display in the 3G/4G USB Modem field as shown in Figure 5-1.

☞ **Note:**

3G/4G settings are unavailable when the Internet Access mode is set to **WAN Only** mode. Please change settings on 5.2.1 Internet Access if you want to use 3G/4G.

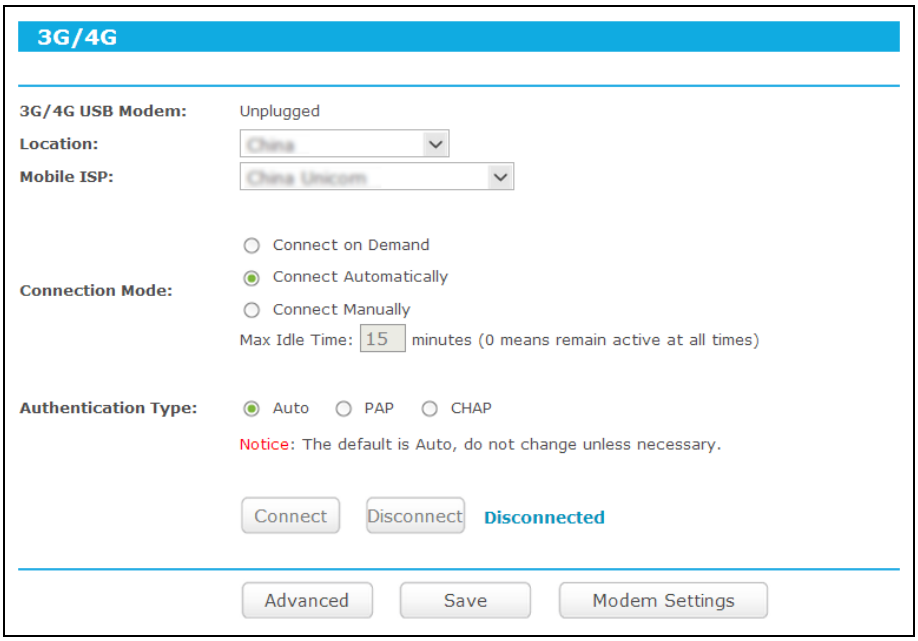


Figure 5-4 3G/4G

- **3G/4G USB Modem -** 3G/4G device status Plugged or Unplugged.
- **Location -** Please select the location where you're enjoying the 3G/4G card.
- **Mobile ISP -** Please select the ISP(Internet Service Provider) you apply to for 3G/4G service. The router will show the default Dial Number and APN of that ISP.
- **Connection Mode -** Please select the Connection Mode to accessing the Internet with 3G/4G.
  - **Connect on Demand -** You can configure the Router to disconnect your Internet connection after a specified period of the Internet connectivity (**Max Idle Time**). If your Internet connection has been terminated due to inactivity,**Connect on Demand** enables the Router to automatically re-establish your connection as soon as you attempt to access the Internet again. If you wish to activate **Connect on Demand**, click the radio button. If you want your Internet connection to remain active at all times, enter **0** in the **Max Idle Time** field. Otherwise, enter the number of minutes you want to have elapsed before your Internet connection terminates.
  - **Note** - Sometimes the connection cannot be disconnected although you specify a time to **Max Idle Time** because some applications visit the Internet continually in the background.
  - **Connect Automatically -** Connect automatically after the Router is disconnected. To use this option, click the radio button.
  - **Connect Manually -** You can configure the Router to make it connect or disconnect manually. After a specified period of inactivity (**Max Idle Time**), the Router will disconnect your Internet connection, and not be able to re-establish your connection automatically as soon as you attempt to access the Internet again. To use this option, click the radio button. If you want your Internet connection to remain active at all times, enter **0** in the **Max Idle Time**field. Otherwise, enter the number in minutes that you wish to have the Internet connecting last unless a new link requested.

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

➢ **Authentication Type -** Some ISPs need a specifical authentication type, please confirm it with your ISP or keep it Auto. There are three choices:

- **Auto -** The router will have dynamic negotiation with the dialing server and the **Autnentication Type** need not to be specified. The default type is Auto.
- **PAP -** Password Authentication Protocol. This protocol allows the router to establish authentication with the peer using two handshakes. Select this option if the ISP requires this authentication type.
- **CHAP -** Challenge Handshake Authentication Protocol. This protocol allows the route to establish authentication with the peer using three handshakes and checking the peer identity periodically. Select this option if the ISP requires this authentication type.

Click the **Connect** button to connect to Internet with 3G/4G.

Click the **Disconnect** button to disconnect to Internet with 3G/4G while connecting to Internet with 3G/4G.

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

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

Click the **Modem Settings** button if your 3G/4G USB Modem is not supported by the Router.

5.2.3 WAN

Choose menu "**Advanced→Network→WAN**", 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, shown in Figure 5-5.

Figure 5-5 WAN – Dynamic IP

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

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

Note:

If you find error when you go to a 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, Gateway and DNS setting, select **Static IP**. The Static IP settings page will appear, shown in Figure 5-6.

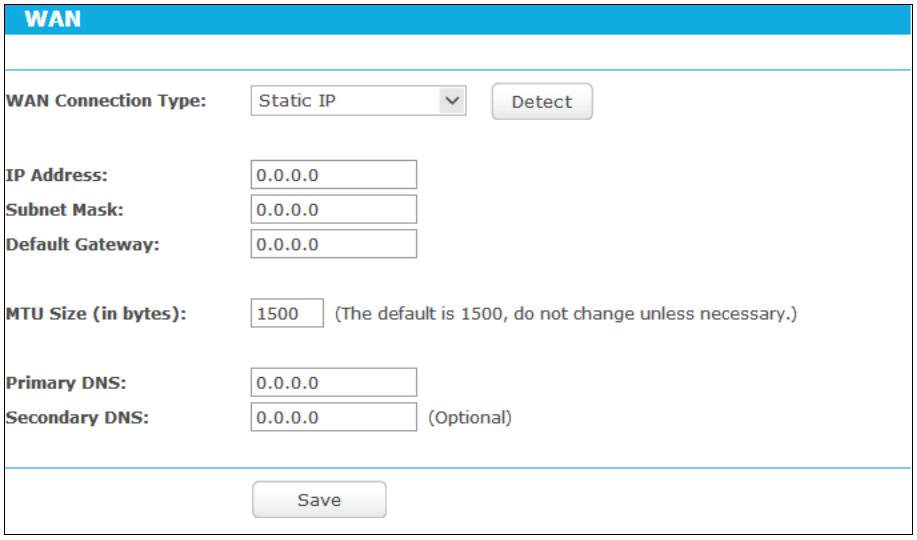


Figure 5-6 WAN - Static IP

- **IP Address -** Enter the IP address in dotted-decimal notation provided by your ISP.
- **Subnet Mask -** Enter the subnet Mask 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. And you should enter the following parameters (Figure 5-7).

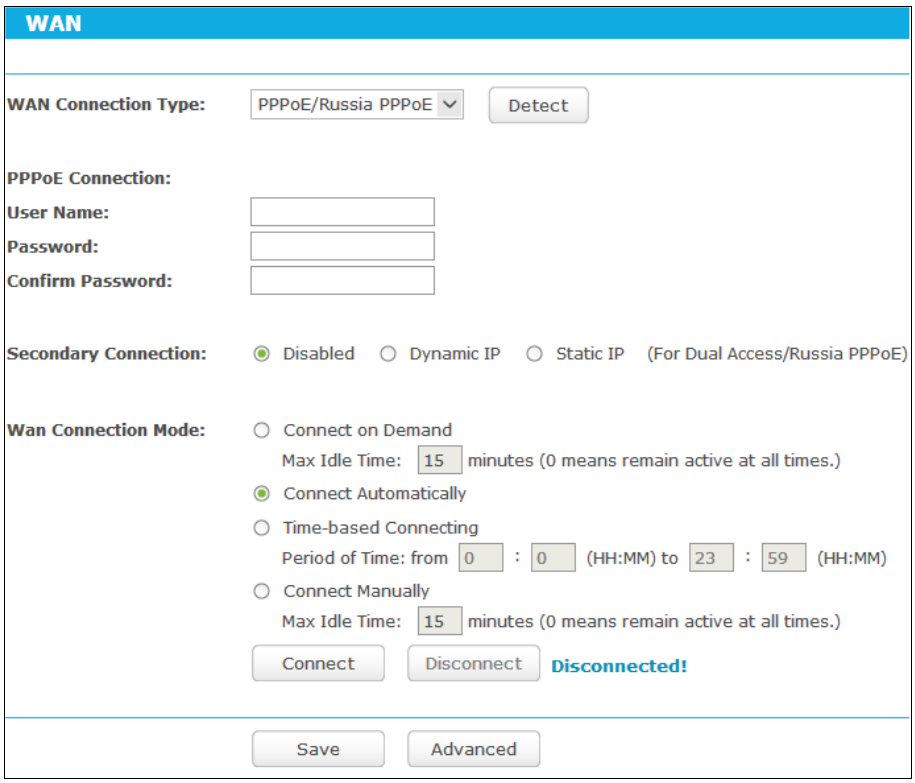


Figure 5-7 WAN - PPPoE

- **User Name/Password -** Enter the User Name and Password provided by your ISP. These fields are case-sensitive.
- **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 "**Advanced→System Tools→Time Settings**" 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 in Figure 5-8 will then appear.

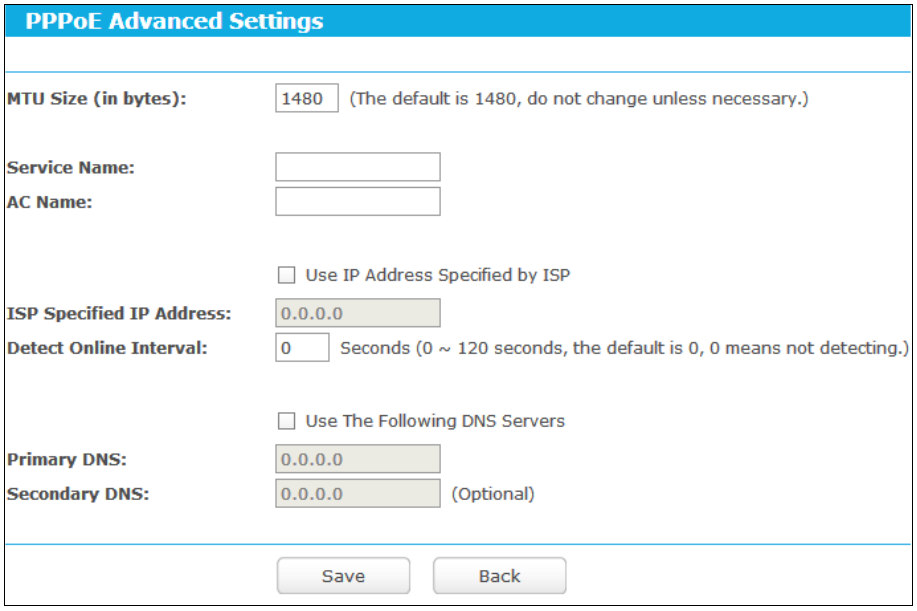


Figure 5-8 PPPoE Advanced Settings

- **MTU Size -** The default MTU size is "1480" bytes, which is usually fine. It is not recommended that you change the default **MTU Size** unless required by your ISP.
- **Service Name/AC Name -** The service name and AC (Access Concentrator) name 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. And you should enter the following parameters (Figure 5-9).

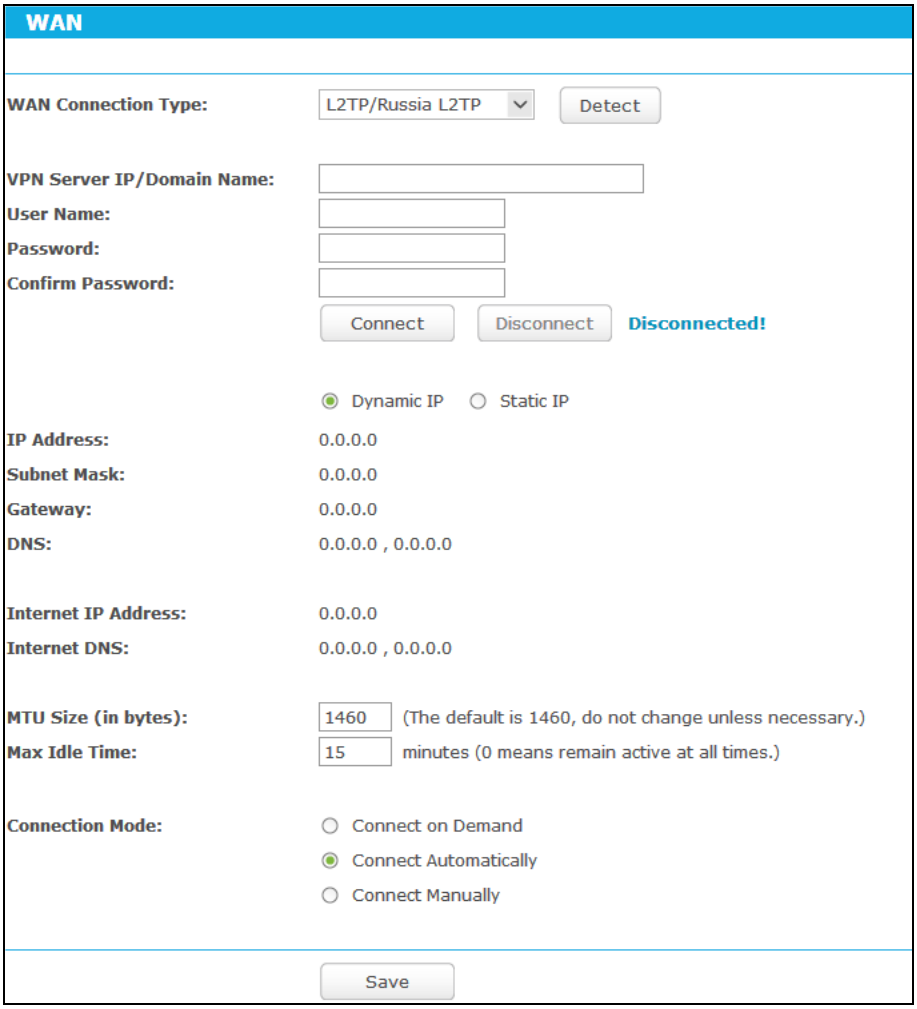


Figure 5-9 WAN - L2TP/Russia L2TP

- **VPN Server IP/Domain Name -** Enter the IP address or domain name of the VPN server provided by your ISP.
- **User Name/Password -** Enter the User Name and Password provided by your ISP. These fields are case-sensitive.
- **Dynamic IP/ Static IP -** Select **Static IP** if IP address, subnet mask, gateway and DNS server address have been provided by your ISP. Otherwise, please select **Dynamic IP**.
- **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 (Figure 5-10).

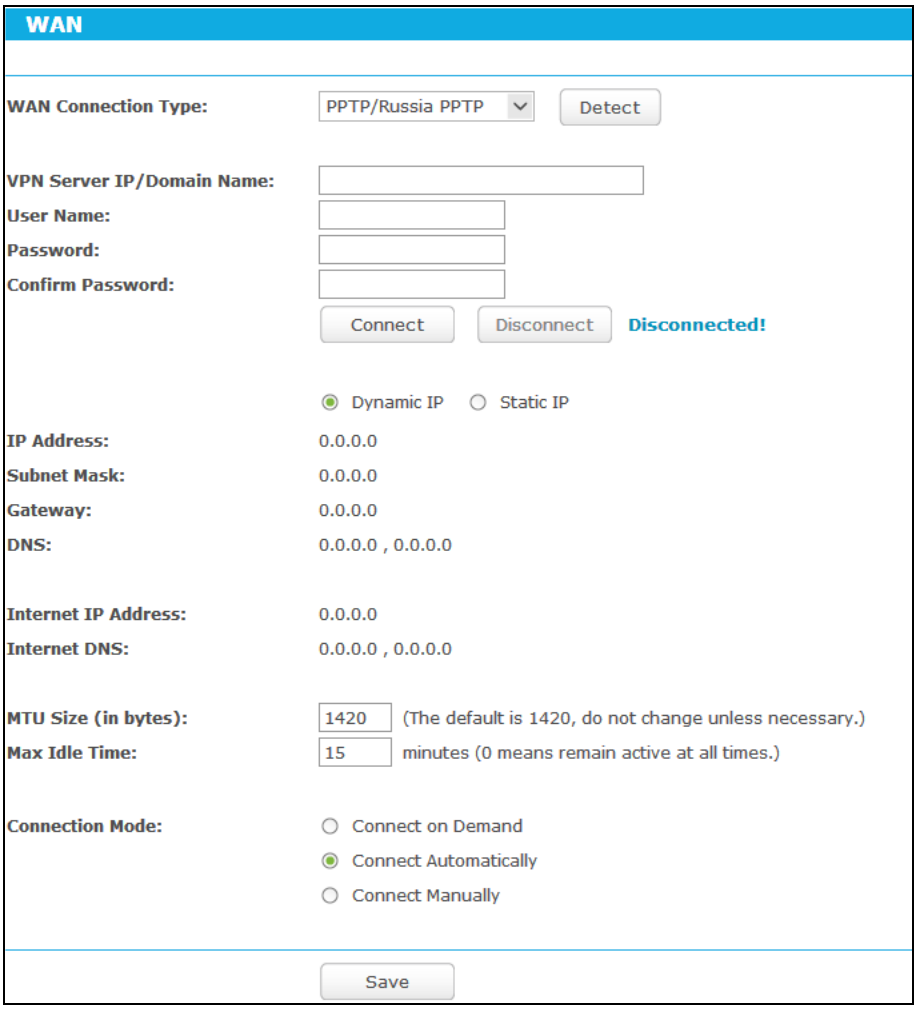


Figure 5-10 PPTP Settings

- **VPN Server IP/Domain Name -** Enter the IP address or domain name of the VPN server provided by your ISP.
- **User Name/Password -** Enter the User Name and Password provided by your ISP. These fields are case-sensitive.
- **Dynamic IP/ Static IP -** Select **Static IP** if IP address, subnet mask, gateway and DNS server address have been provided by your ISP. Otherwise, please select **Dynamic IP**.
- **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.

☞ **Note:**

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

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

The router cannot detect PPTP/L2TP connections with your ISP. If your ISP uses one of these protocols, then you must configure your connection manually.

5.2.4 MAC Clone

Choose menu "**Advanced→Network→MAC Clone**", you can configure the MAC address of the WAN on the screen below, Figure 5-11.

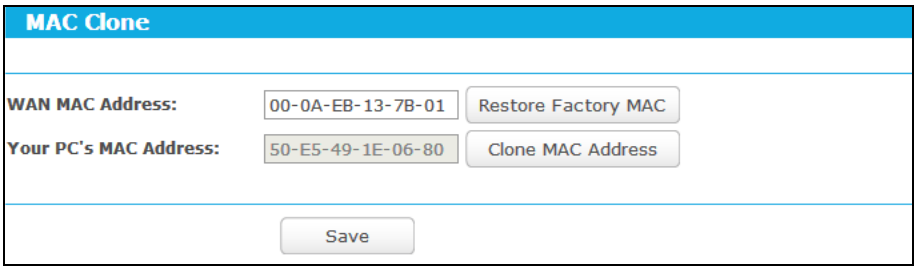


Figure 5-11 MAC Address Clone

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

- **WAN MAC Address -** This field displays the current MAC address of the Internet 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** button and this MAC address will fill in the **WAN MAC Address** field.

Click **Restore Factory MAC** to restore the MAC address of Internet port to the factory default value. Click the **Save** button to save your settings.

☞ **Note:**

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

5.2.5 LAN

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

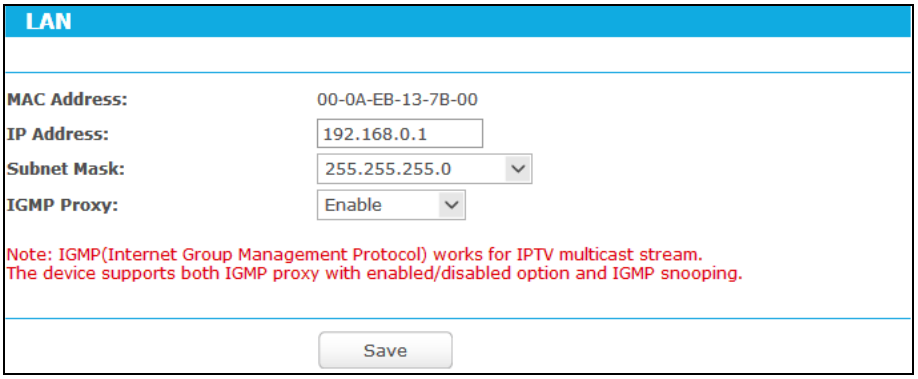


Figure 5-12 LAN

- **MAC Address -** The physical address of the router, as seen from the LAN. The value can't be changed.
- **IP Address -** Enter the IP address of your router or reset it in dotted-decimal notation (factory default: 192.168.0.1).
- **Subnet Mask -** An address code that determines the size of the network. Normally use 255.255.255.0 as the subnet mask.
- **IGMP Proxy -** If you want to watch TV through IGMP, please enable it.

☞ **Note:**

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

If the new LAN IP Address you set is not in the same subnet, the IP Address pool of the DHCP server will change accordingly at the same time, while the Virtual Server and DMZ Host will not take effect until they are re-configured.

5.3 Wireless 2.4GHz

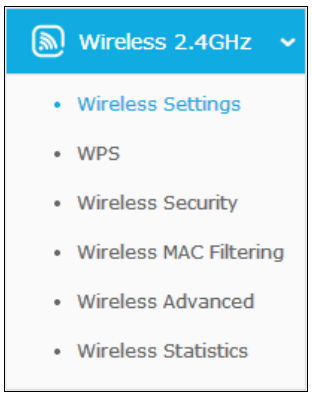


Figure 5-13 Wireless menu

There are six submenus under the Wireless menu, shown in Figure 5-13: **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 functions.

5.3.1 Wireless Settings

Choose menu "**Advanced→Wireless 2.4GHz→Wireless Settings**", you can configure the basic settings for the wireless network of 2.4GHz on this page.

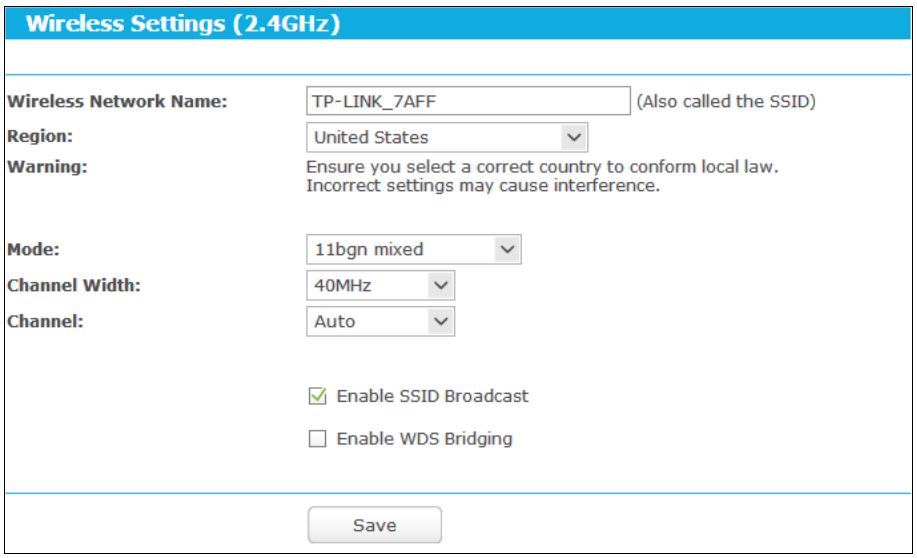


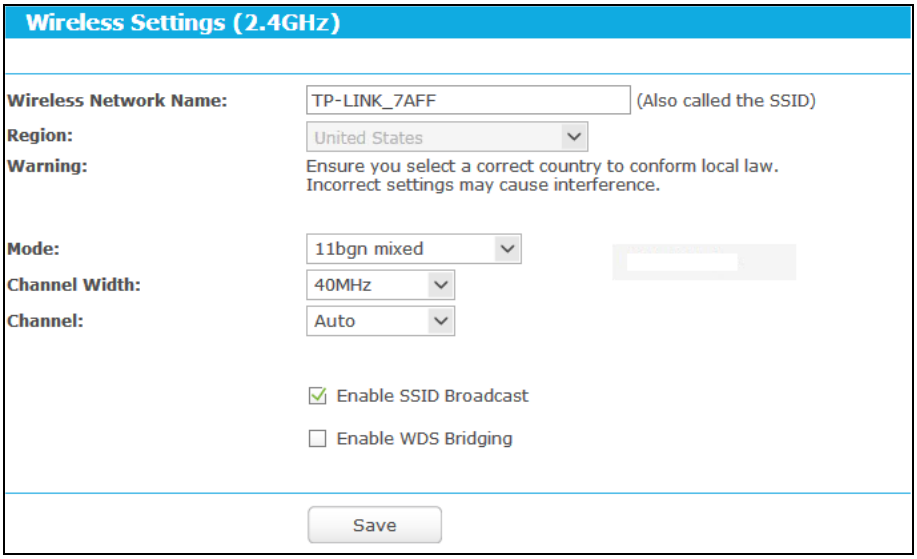
Figure 5-14 Wireless Settings (2.4GHz)

- **Wireless Network Name -** The wireless network name (SSID) that the router uses. You can create a new one with up to 32 characters. The default SSID is set to be TP-LINK_XXXX. This value is case-sensitive. For example, *TEST* is NOT the same as *test*.

- **Region -** The geographic region where the router is being used. This field specifies the region where the wireless function of the router can be used. It might be illegal to use the wireless features of the router in some parts of the world. If your country or region is not listed, please contact your local government agency for assistance.

Note:

Per FCC regulations, all Wi-Fi products marketed in the U.S. must be fixed to the U.S. region only.

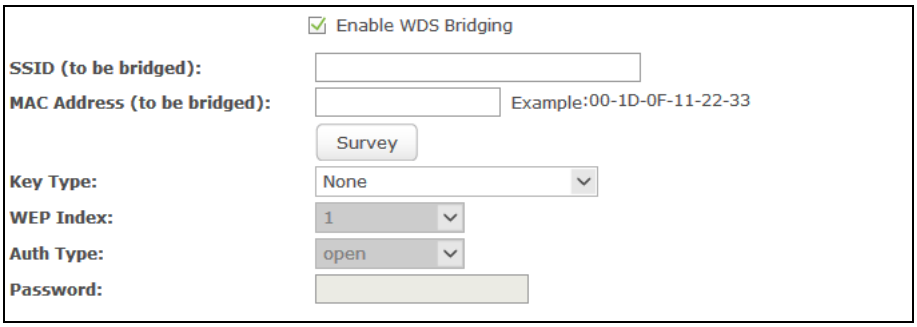


- **Mode -** Select the desired mode.
  - **11n only -** Select if you are using 802.11n wireless clients.
  - **11bg mixed -** Select if you are using both 802.11b and 802.11g wireless clients.
  - **11bgn mixed -** Select if you are using a mix of 802.11b, 11g, and 11n wireless clients. It is strongly recommended that you set the Mode to **802.11bgn mixed**, and all of 802.11b, 802.11g, and 802.11n wireless stations can connect to the router.
- **Channel Width -** Select the channel width from the drop-down list, including **Auto**, **20MHz**, **40MHz**. The default setting is **Auto**.

Note:

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

- **Channel -** This field determines which operating frequency will be used. The default channel is set to **Auto**, so the router will choose the best channel automatically. It is not necessary to change the wireless channel unless you notice interference problems with another nearby access point.
- **Enable SSID Broadcast -** When wireless clients survey the local area for wireless networks to associate with, they will detect the SSID broadcast by the router. If you select the **Enable SSID Broadcast** checkbox, the Wireless router will broadcast its name (SSID) on the air.
- **Enable WDS Bridging -** Check this box to enable WDS. With this function, the router can bridge two or more WLANs. If this checkbox is selected, you will have to set the following parameters as shown in Figure 5-15. Make sure the following settings are correct.



- Figure 5-15 WDS Settings

- **SSID (to be bridged)** - The SSID of the AP your router is going to connect to as a client. You can also use the Survey function to select the SSID to join.
- **MAC Address (to be bridged)** - The MAC address (BSSID) of the AP your router is going to connect to as a client. You can also use the Survey function to select the MAC address (BSSID) to join.
- **Survey** - Click this button, you can search the APs that run in all channels.
- **Key type** - This option should be chosen according to the AP's security configuration.
- **WEP Index** - This option should be chosen if the key type is WEP. It indicates the index of the WEP key.
- **Auth Type** - This option should be chosen if the key type is WEP. It indicates the authorization type of the Root AP.
- **Password** - If the AP your router is going to connect needs password, you need to fill the password in this blank.

5.3.2 WPS

Choose menu "**Advanced→Wireless 2.4GHz→WPS**", you can see the screen as shown in Figure 5-16. This section will guide you to add a new wireless device to an existing network quickly by WPS (Wi-Fi Protected Setup) function.

Figure 5-16 WPS

- **WPS Status -** Enable or disable the WPS function here.
- **Current PIN -** Displays the current value of the router's PIN. The default PIN of the router can be found in the label or User Guide.

- **Restore PIN -** Restore the PIN of the router to its default value.
- **Gen New PIN -** Click this button, and then you can get a new random value for the router's PIN. You can ensure the network security by generating a new PIN.
- **Add device -** You can add a new device to the existing network manually by clicking this button.

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

I. Use the Wi-Fi Protected Setup Button

Use this method if your client device has a WPS button.

Step 1: Press the **WPS/Reset** button on the back panel of the router.

Step 2: Press and hold the **WPS** button of the client device. The WPS LED flashes for two minutes during the Wi-Fi Protected Setup process.

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

II. Enter the client device's PIN on the router

Use this method if your client device does not have the WPS button, but has a Wi-Fi Protected Setup PIN number.

Step 4: Enable WPS. The default is enabled. Click the **Add device** button in Figure 5-16, then Figure 5-17 will appear.

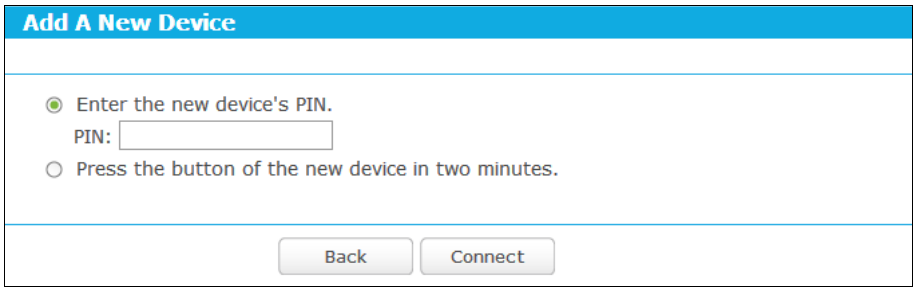


Figure 5-17 Add A New Device

Step 5: Enter the PIN number from the client device in the field on the WPS screen above. Then click **Connect** button.

Step 6: "**Connect successfully**" will appear on the screen of Figure 5-17, which means the client device has successfully connected to the router.

Note:

1) The WPS LED on the router will light blue for five minutes if the device has been successfully added to the network.
2) The WPS function cannot be configured if the wireless function of the router is disabled. Please make sure the wireless function is enabled before configuring the WPS.

5.3.3 Wireless Security

Choose menu "**Advanced→Wireless 2.4GHz→Wireless Security**", you can configure the security settings of your wireless network. There are five wireless security modes supported by the router: WPA-Personal, WPA2-Personal, WPA-Enterprise, WPA2-Enterprise, and WEP.

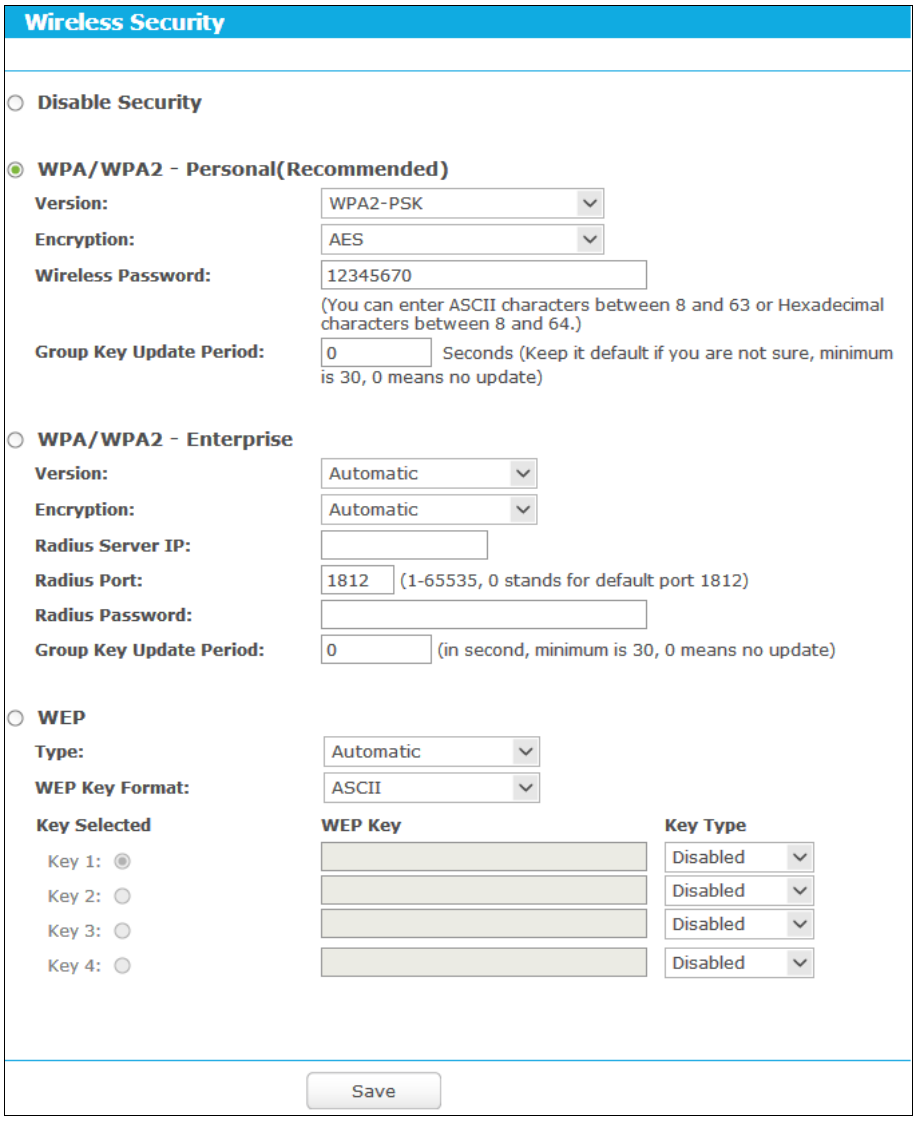


Figure 5-18 Wireless Security

- **Disable Security -** If you do not want to use wireless security, check this radio button. But it's strongly recommended to choose one of the following modes to enable security.
- **WPA/WPA2-Personal -** It's the WPA/WPA2 authentication type based on pre-shared passphrase. The router is configured by this security type by default.
  - **Version -** You can choose the version of the **WPA-PSK** or **WPA2-PSK** security on the drop-down list. The default setting is **WPA2-PSK**.
  - **Encryption -** You can select either **TKIP** or **AES** as Encryption. The default setting is **AES**.

Note:

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

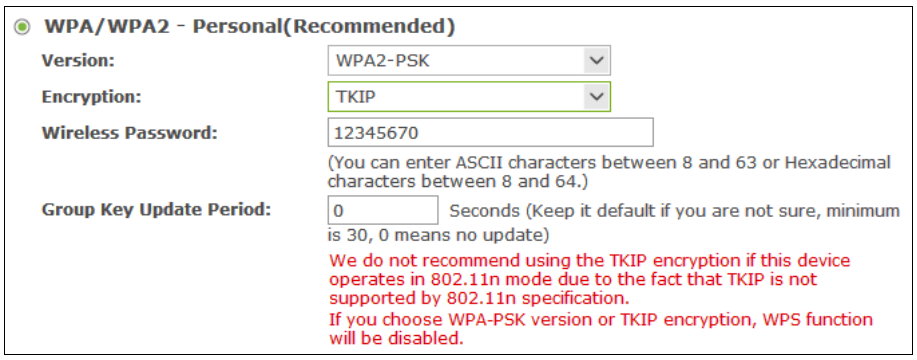


Figure 5-19 WPA/WPA2 – Personal

- **Wireless Password -** You can enter ASCII characters between 8 and 63 characters or 8 to 64 Hexadecimal characters. The default password is the same with the default PIN code, which is labeled on the router or can be found in Figure 5-16.
- **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.

➢ **WPA/WPA2- Enterprise -** It's based on Radius Server. If you choose WPA/WPA2 - Enterprise, WPS function will be disabled.

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

Note:

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

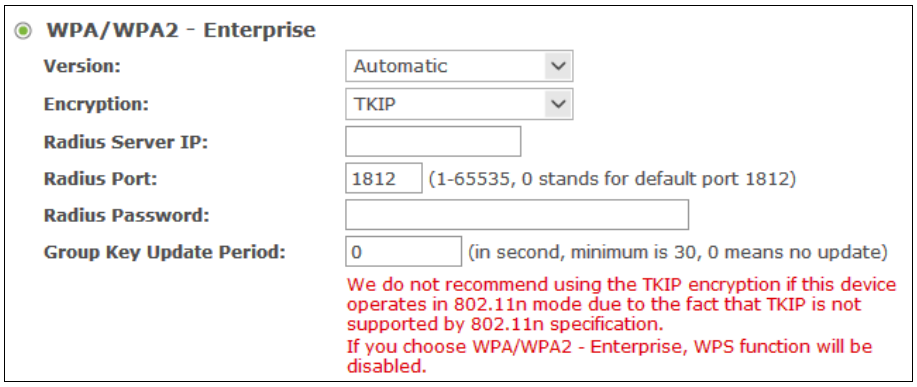


Figure 5-20 WPA/WPA2 - Enterprise

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

- **Radius Port -** Enter the port number of the Radius server.
- **Radius Password -** Enter the password for the Radius server.
- **Group Key Update Period -** Specify the group key update interval in seconds. The value should be 30 or above. Enter 0 to disable the update.

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

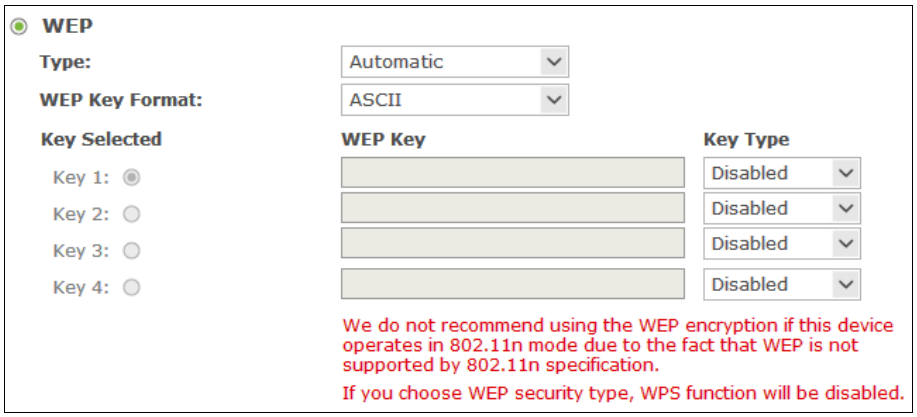


Figure 5-21 WEP

- **Type -** you can choose the type for the WEP security on the drop-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 -** 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) 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.

  ☞ **Note:**

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

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

5.3.4 Wireless MAC Filtering

Choose menu "**Advanced→Wireless 2.4GHz→Wireless MAC Filtering**", you can control the wireless access by configuring the **Wireless MAC Filtering** function, shown in Figure 5-22.

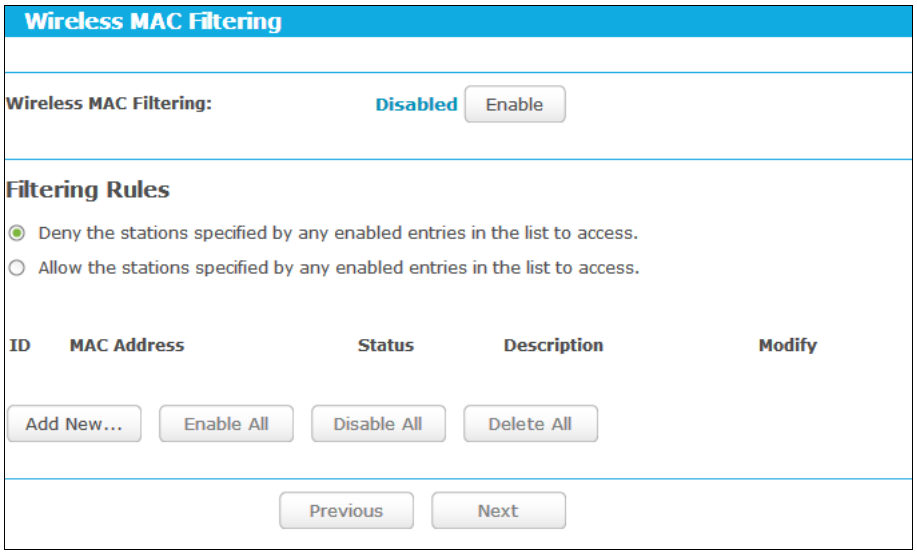


Figure 5-22 Wireless MAC Filtering

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

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

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

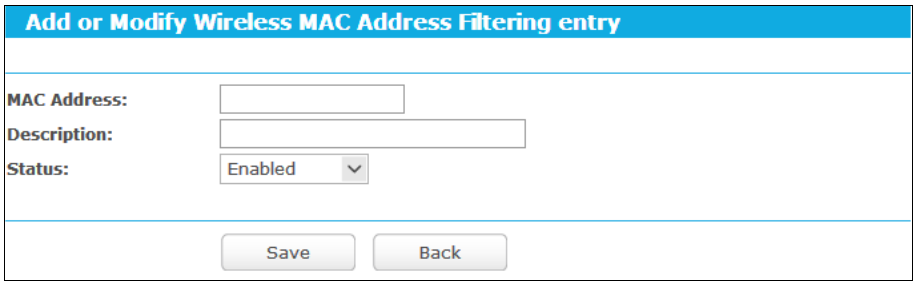


Figure 5-23 Add or Modify Wireless MAC Address Filtering entry

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

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

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

To modify or delete an existing entry:

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

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

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

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

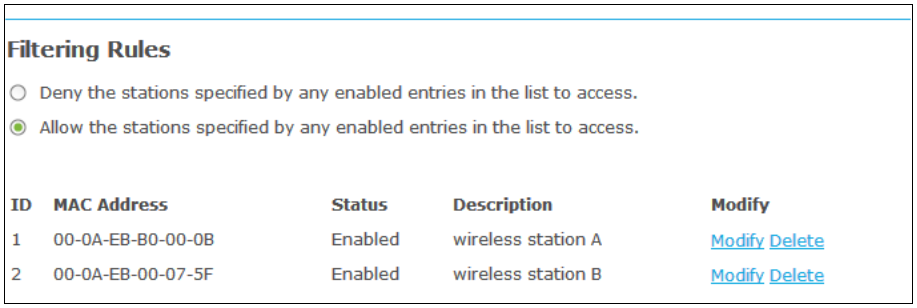
Click the **Next** button to go to the next page.

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

For example: If you desire that the wireless station A with MAC address 00-0A-EB-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** drop-down list.
   4) Click the **Save** button.

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



5.3.5 Wireless Advanced

Choose menu "**Advanced→Wireless 2.4GHz→Wireless Advanced**", you can configure the advanced settings of your wireless network.

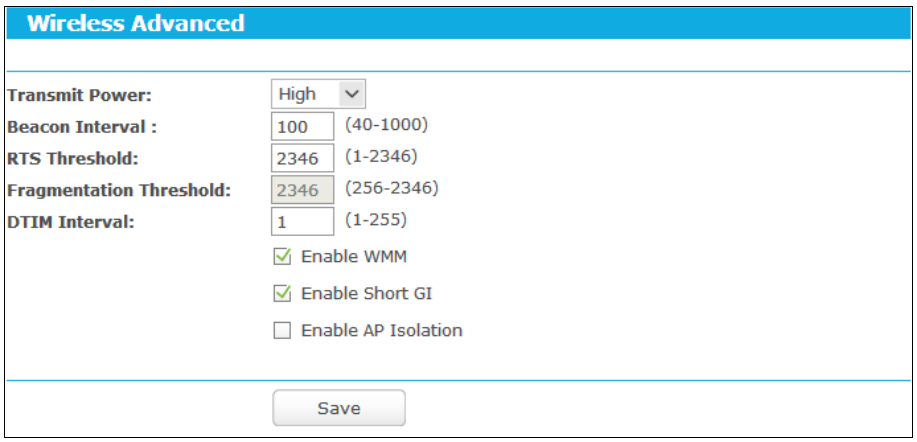


Figure 5-24 Wireless Advanced

- **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 40-1000 milliseconds for Beacon Interval here. The beacons are the packets sent by the router to synchronize a wireless network. Beacon Interval value determines the time interval of the beacons. The default value is 100.
- **RTS Threshold -** Here you can specify the RTS (Request to Send) Threshold. If the packet is larger than the specified RTS Threshold size, the router will send RTS frames to a particular receiving station and negotiate the sending of a data frame. The default value is 2346.
- **Fragmentation Threshold -** This value is the maximum size determining whether packets will be fragmented. Setting the Fragmentation Threshold too low may result in poor network performance 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.
- **Enable Short GI -** This function is recommended for it will increase the data capacity by reducing the guard interval time.

- **Enabled AP Isolation -** This function can isolate wireless stations on your network from each other. Wireless devices will be able to communicate with the router but not with each other. To use this function, check this box. AP Isolation is disabled by default.

☞ **Note:**

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

5.3.6 Wireless Statistics

Choose menu "**Advanced→Wireless 2.4GHz→Wireless Statistics**", you can see the MAC Address, Current Status, Received Packets and Sent Packets for each connected wireless station.

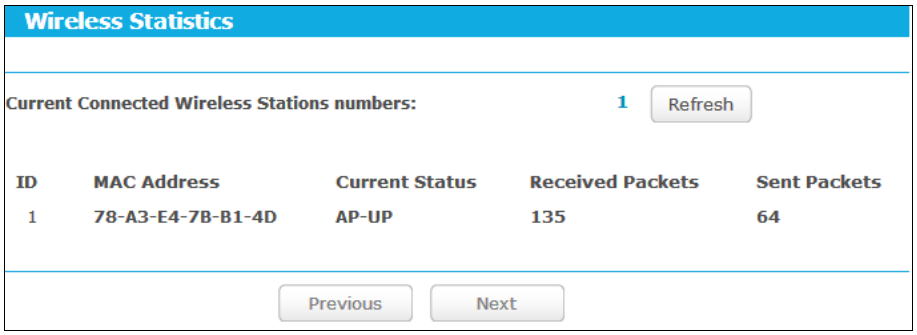


Figure 5-25 Wireless Statistics

- **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.

5.4 DHCP

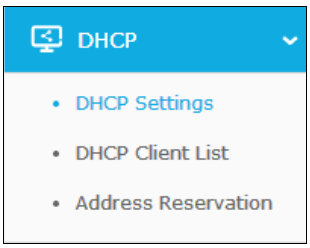


Figure 5-26 The DHCP menu

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

5.4.1 DHCP Settings

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

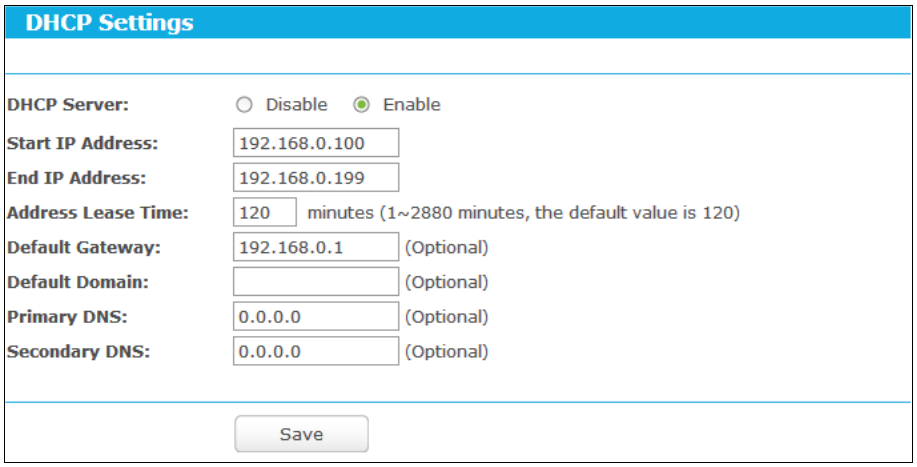


Figure 5-27 DHCP Settings

- **DHCP Server - Enable** or **Disable** the DHCP server. If you disable the Server, you must have another DHCP server within your network or else you must configure the computer manually.
- **Start IP Address -** Specify an IP address for the DHCP Server to start with when assigning IP addresses. 192.168.0.100 is the default start address.
- **End IP Address -** Specify an IP address for the DHCP Server to end with when assigning IP addresses. 192.168.0.199 is the default end address.
- **Address Lease Time -** The **Address Lease Time** is the amount of time a network user will be allowed connection to the router with their current dynamic IP Address. Enter the amount of time in minutes and the user will be "leased" this dynamic IP Address. After the

time is up, the user will be automatically assigned a new dynamic IP address. The range of the time is 1 ~ 2880 minutes. The default value is 120 minutes.

- **Default Gateway -** (Optional.) It is suggested to input the IP address of the Ethernet 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.
- **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".

5.4.2 DHCP Clients List

Choose menu "**Advanced→DHCP→DHCP Clients List**", you can view the information about the clients attached to the router in the screen as shown in Figure 5-28.

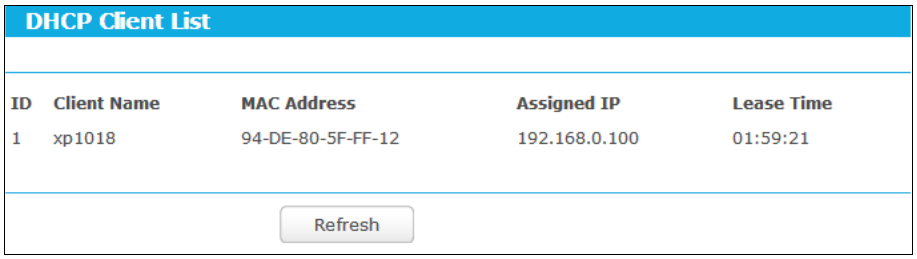


Figure 5-28 DHCP Clients List

- **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.

5.4.3 Address Reservation

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

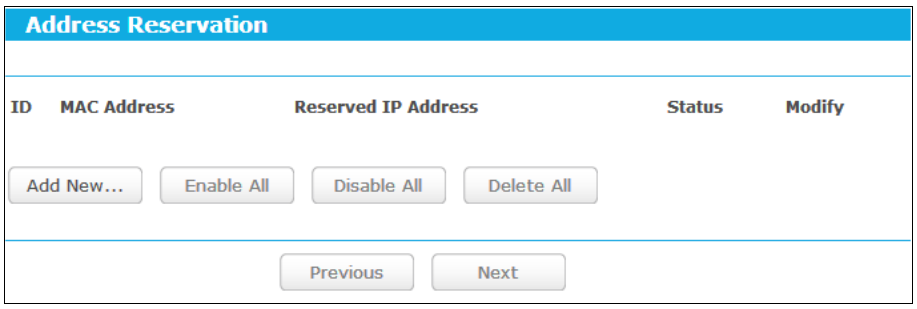


Figure 5-29 Address Reservation

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

To Reserve an IP address:

1. Click the **Add New…** button. Then Figure 5-30 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.

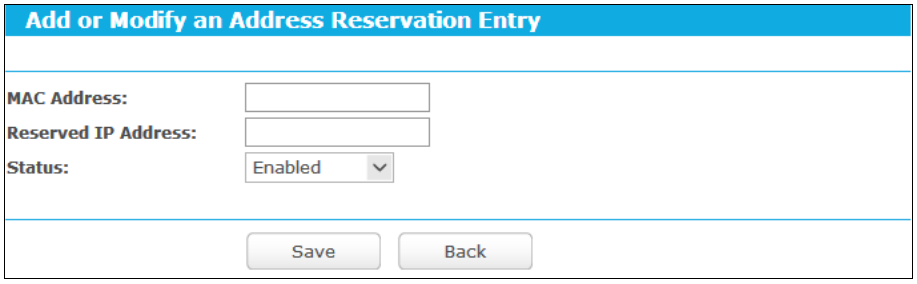


Figure 5-30 Add or Modify an Address Reservation Entry

To modify or delete an existing entry:

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

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

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

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

5.5 Forwarding

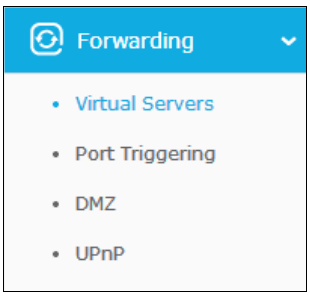


Figure 5-31 The Forwarding menu

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.

5.5.1 Virtual Servers

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

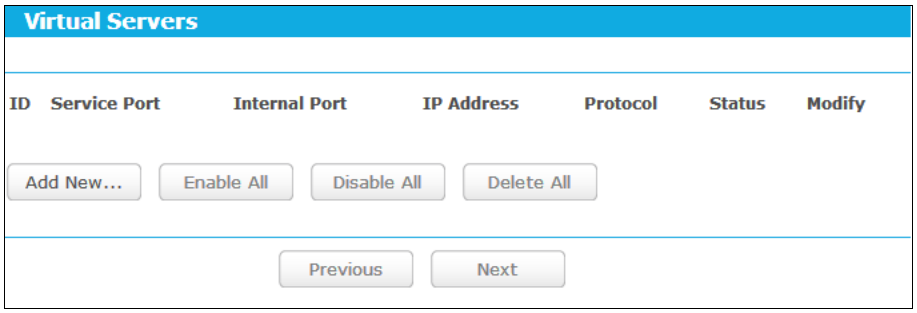


Figure 5-32 Virtual Servers

- **Service Port** - The numbers of External Service Ports. You can enter a service port or a range of service ports (the format is XXX – YYY; XXX is the Start port and YYY is the End port).
- **Internal Port** - The Internal Service Port number of the PC running the service application. You can leave it blank if the **Internal Port** is the same as the **Service Port**, or enter a specific port number when **Service Port** is a single one.
- **IP Address** - The IP address of the PC running the service application.
- **Protocol** - The protocol used for this application, either **TCP**, **UDP**, or **All** (all protocols supported by the router).
- **Status** - The status of this entry, "Enabled" means the virtual server entry is enabled.

- **Common Service Port** - Some common services already exist in the drop-down list.
- **Modify** - To modify or delete an existing entry.

To setup a virtual server entry:

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

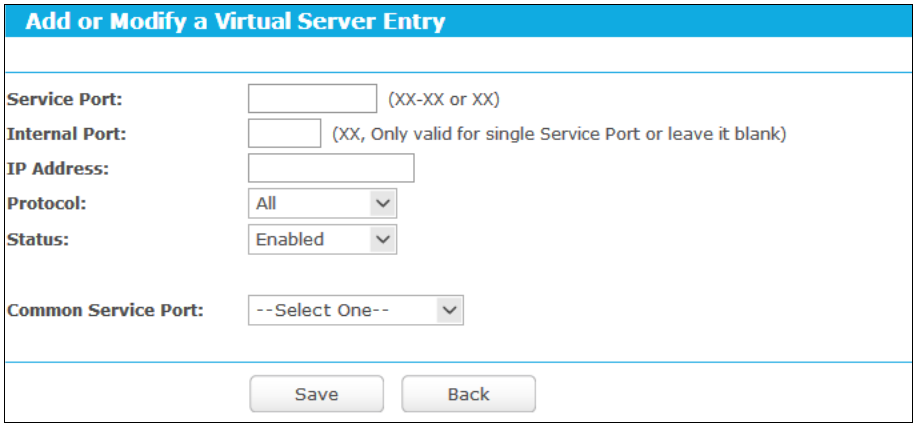


Figure 5-33 Add or Modify a Virtual Server Entry

Note:

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

To modify or delete an existing entry:

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

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

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

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

Note:

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

5.5.2 Port Triggering

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

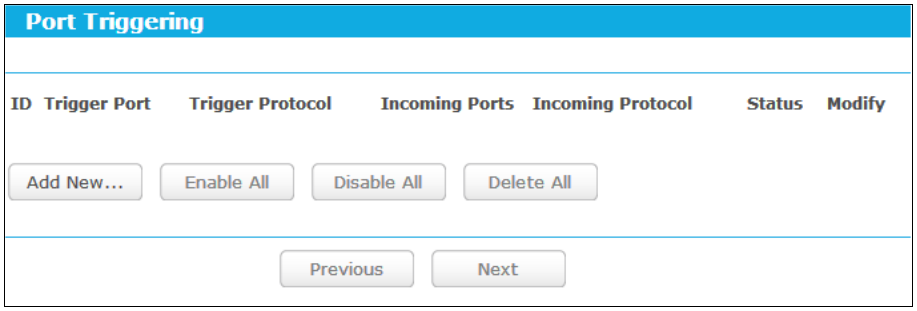


Figure 5-34 Port Triggering

To add a new rule, follow the steps below.

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

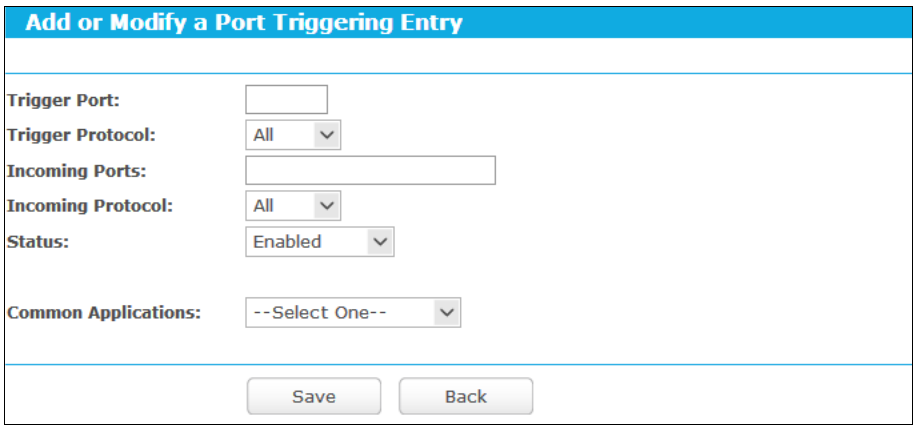


Figure 5-35 Add or Modify a Triggering Entry

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

To modify or delete an existing entry:

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

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

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

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

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

1. A local host makes an outgoing connection to an external host using a destination port number defined in the **Trigger Port** field.
2. The router records this connection, opens the incoming port or ports associated with this entry in the **Port Triggering** table, and associates them with the local host.

3. When necessary, the external host will be able to connect to the local host using one of the ports defined in the **Incoming Ports** field.

Note:

1. When the trigger connection is released, the corresponding opened ports will be closed.
2. Each rule can only be used by one host on the LAN at a time. The trigger connection of other hosts on the LAN will be refused.
3. **Incoming Ports** ranges cannot overlap each other.

5.5.3 DMZ

Choose menu "**Advanced→Forwarding→DMZ**", and then you can view and configure DMZ host in the screen shown in Figure 5-36. The DMZ host feature allows one local host to be exposed to the Internet for a special-purpose service such as Internet gaming or videoconferencing. The router forwards packets of all services to the DMZ host. Any PC whose port is being forwarded must have its DHCP client function disabled and should have a new static IP Address assigned to it because its IP Address may be changed when using the DHCP function.

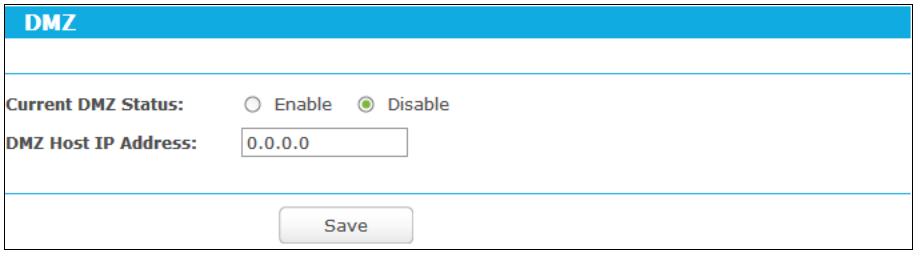


Figure 5-36 DMZ

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

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

5.5.4 UPnP

Choose menu "**Advanced→Forwarding→UPnP**", and then you can view the information about **UPnP** in the screen shown in Figure 5-37. The **Universal Plug and Play (UPnP)** feature allows the devices, such as Internet computers, to access the local host resources or devices as needed. UPnP devices can be automatically discovered by the UPnP service application on the LAN.

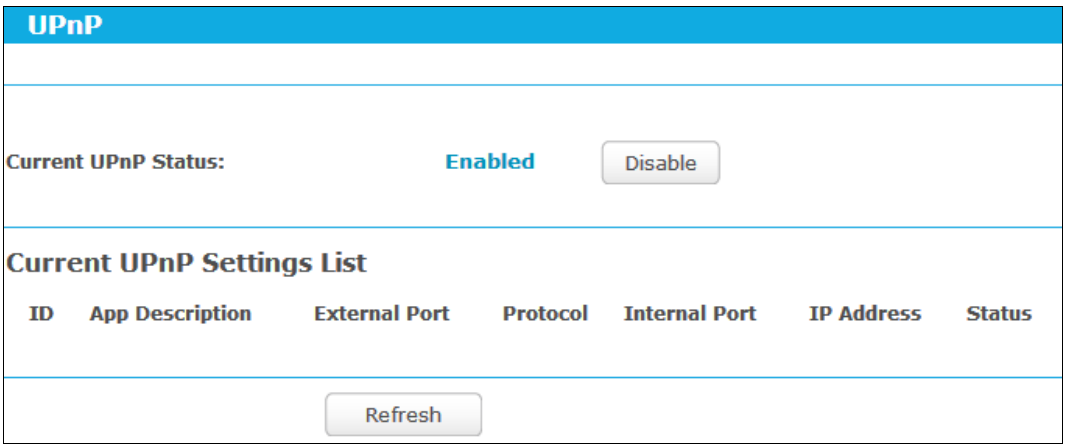


Figure 5-37 UPnP Setting

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

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

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

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

5.6 Security

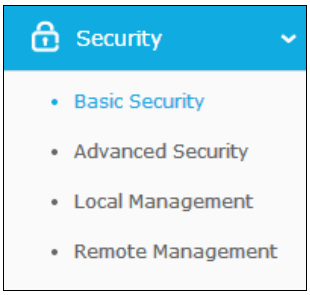


Figure 5-38 The Security menu

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 functions.

5.6.1 Basic Security

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

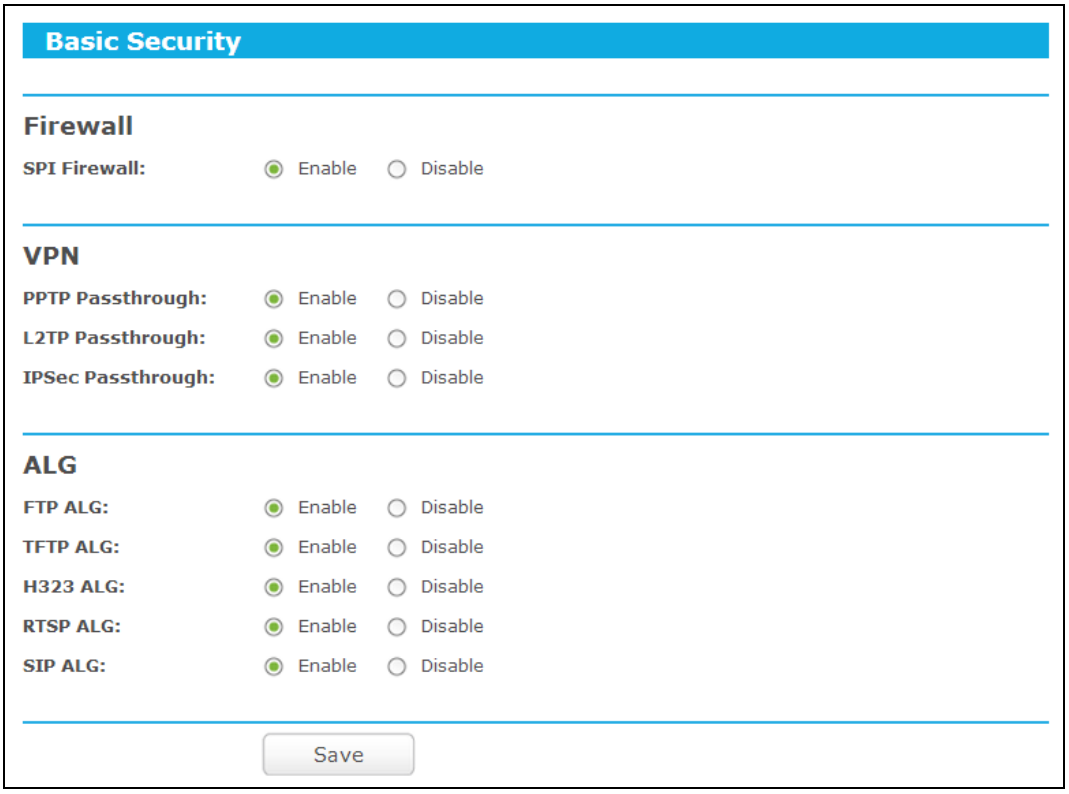


Figure 5-39 Basic Security

- **Firewall -** A firewall protects your network from the outside world. Here you can enable or disable the router's firewall.
  - **SPI Firewall** - SPI (Stateful Packet Inspection, also known as dynamic packet filtering) helps to prevent cyber attacks by tracking more state per session. It validates that the traffic passing through the session conforms to the protocol. SPI Firewall is enabled by factory default. If you want all the computers on the LAN exposed to the outside world, you can disable it.
- **VPN -** VPN Passthrough must be enabled if you want to allow VPN tunnels using VPN protocols to pass through the router.
  - **PPTP Passthrough** - Point-to-Point Tunneling Protocol (PPTP) allows the Point-to-Point Protocol (PPP) to be tunneled through an IP network. To allow PPTP tunnels to pass through the router, click **Enable**.
  - **L2TP Passthrough** - Layer Two Tunneling Protocol (L2TP) is the method used to enable Point-to-Point sessions via the Internet on the Layer Two level. To allow L2TP tunnels to pass through the router, click **Enable**.
  - **IPSec Passthrough** - Internet Protocol security (IPSec) is a suite of protocols for ensuring private, secure communications over Internet Protocol (IP) networks,

through the use of cryptographic security services. To allow IPSec tunnels to pass through the router, click **Enable**.

- **ALG -** It is recommended to enable Application Layer Gateway (ALG) because ALG allows customized Network Address Translation (NAT) traversal filters to be plugged into the gateway to support address and port translation for certain application layer "control/data" protocols such as FTP, TFTP, H323 etc.
  - **FTP ALG** - To allow FTP clients and servers to transfer data across NAT, click **Enable**.
  - **TFTP ALG** - To allow TFTP clients and servers to transfer data across NAT, click **Enable**.
  - **H323 ALG** - To allow Microsoft NetMeeting clients to communicate across NAT, click **Enable**.
  - **RTSP ALG** - To allow some media player clients to communicate with some streaming media servers across NAT, click **Enable**.
  - **SIP ALG** - To allow some multimedia clients to communicate across NAT, click Enable.

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

5.6.2 Advanced Security

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

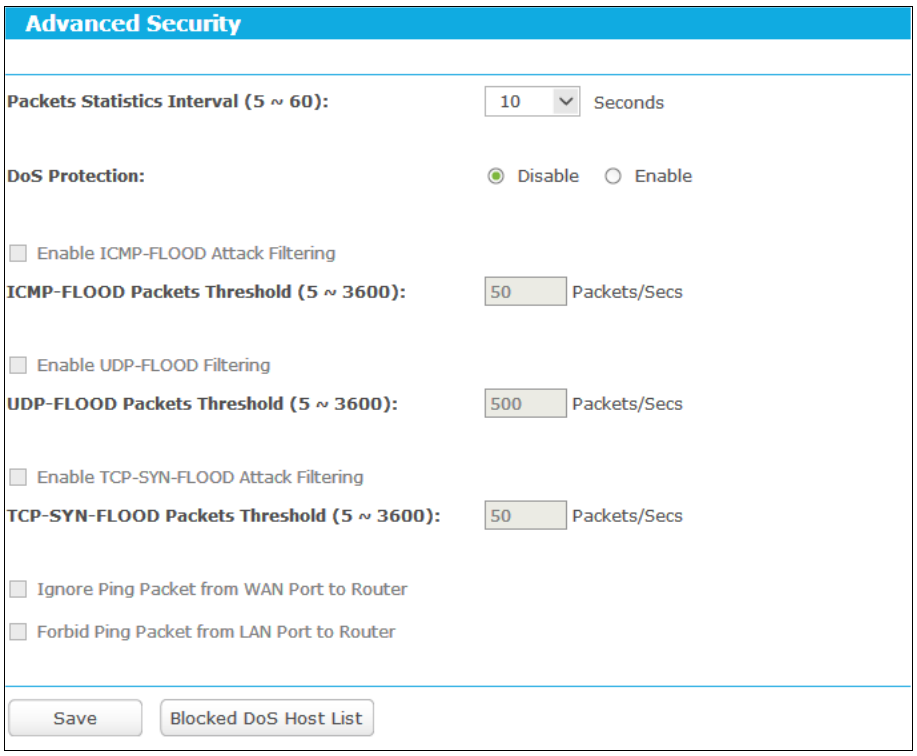


Figure 5-40 Advanced Security

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

☞ **Note:**

Dos Protection will take effect only when the **Traffic Statistics** in "**Advanced→System Tools→Statistics**" is enabled.

- **Enable ICMP-FLOOD Attack Filtering -** Enable or Disable the ICMP-FLOOD Attack Filtering.
- **ICMP-FLOOD Packets Threshold (5~3600) -** The default value is 50. Enter a value between 5 ~ 3600. When the current ICMP-FLOOD Packets number is beyond the set value, the router will startup the blocking function immediately.
- **Enable UDP-FLOOD Filtering -** Enable or Disable the UDP-FLOOD Filtering.
- **UDP-FLOOD Packets Threshold (5~3600) -** The default value is 500. Enter a value between 5 ~ 3600. When the current UPD-FLOOD Packets number is beyond the set value, the router will startup the blocking function immediately.
- **Enable TCP-SYN-FLOOD Attack Filtering -** Enable or Disable the TCP-SYN-FLOOD Attack Filtering.

- **TCP-SYN-FLOOD Packets Threshold (5~3600) -** The default value is 50. Enter a value between 5 ~ 3600. When the current TCP-SYN-FLOOD Packets numbers is beyond the set value, the router will startup the blocking function immediately.
- **Ignore Ping Packet From WAN Port -** Enable or Disable Ignore Ping Packet From WAN Port. The default setting is disabled. If enabled, the ping packet from the Internet cannot access the router.
- **Forbid Ping Packet From LAN Port -** Enable or Disable Forbid Ping Packet From LAN Port. The default setting is disabled. If enabled, the ping packet from LAN cannot access the router. This function can be used to defend against some viruses.

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

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

5.6.3 Local Management

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

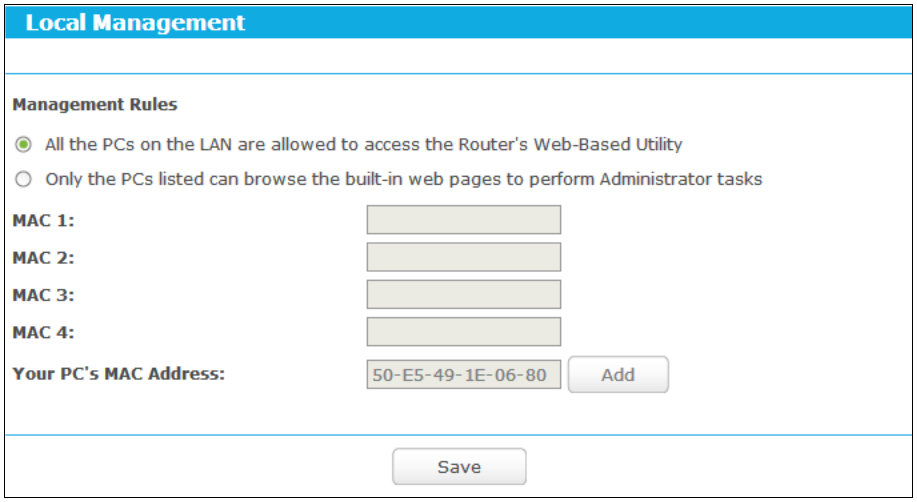


Figure 5-41 Local Management

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

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

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

☞ **Note:**

If your PC is blocked but you want to access the router again, use a pin to press and hold the **WPS/Reset** button (hole) on the back panel for about 5 seconds to reset the router's factory defaults on the router's Web-Based Utility.

5.6.4 Remote Management

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

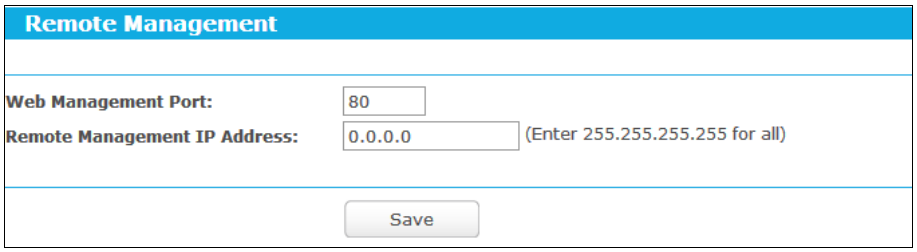


Figure 5-42 Remote Management

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

☞ **Note:**

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

5.7 Parental Control

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

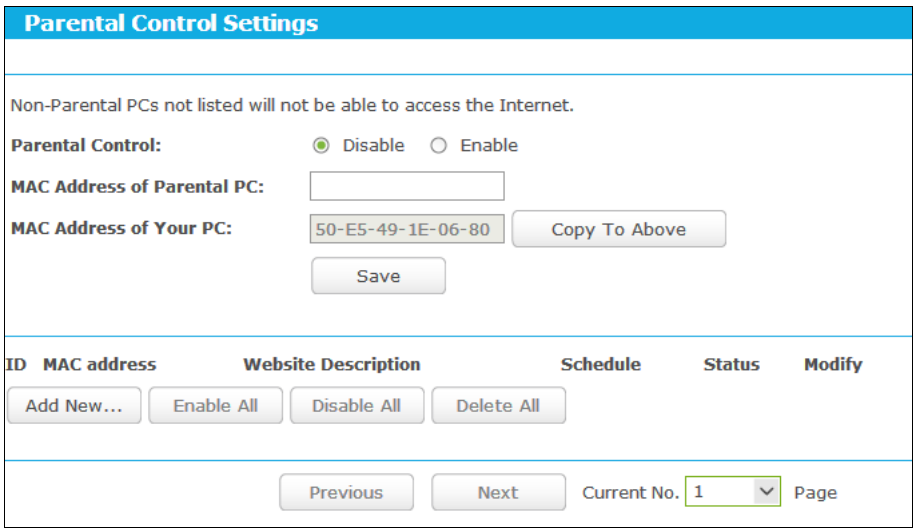


Figure 5-43 Parental Control Settings

- **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 "**Advanced→Access Control→Schedule**".
- **Status** - Check to enable the corresponding entry.
- **Modify -** Here you can edit or delete an existing entry.

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

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

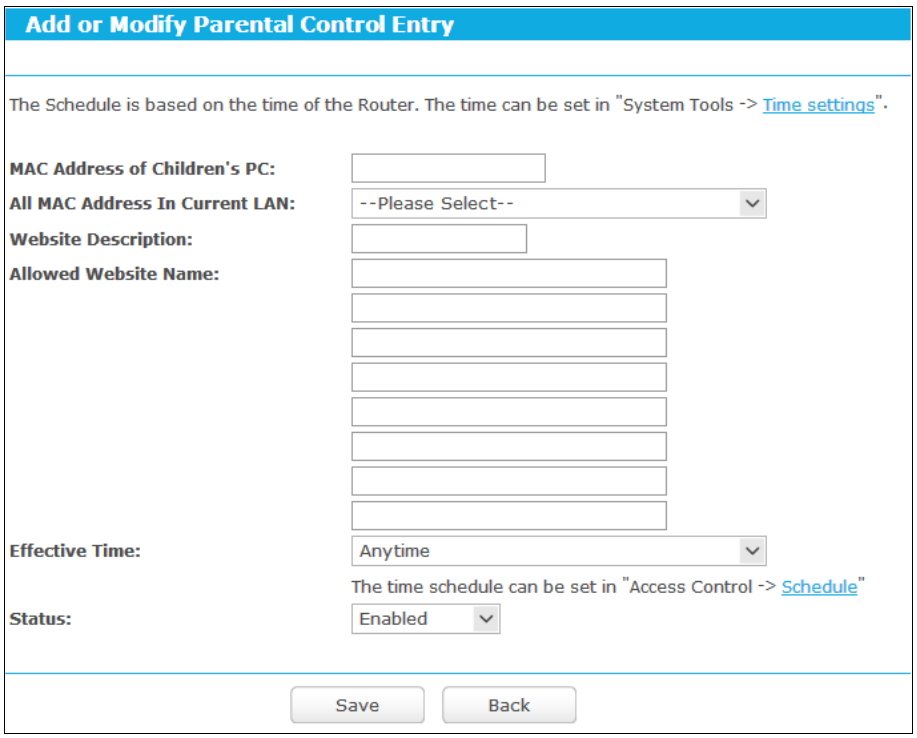


Figure 5-44 Add or Modify Parental Control Entry

2. Enter the MAC address of the PC (e.g. 00-11-22-33-44-AA) you'd like to control in the **MAC Address of Child PC** field, or you can choose the MAC address from the **All Address in Current LAN** drop-down list.
3. Give a description (e.g. Allow tp-link) for the website allowed to be accessed in the **Website Description** field.
4. Enter the allowed website name, e.g. www.tp-link.com.
5. Select the schedule (e.g. Schedule_1) you want from the Effective Time drop-down list. If there are not suitable schedules for you, please go to "Access Control->Schedule" page to create the schedule you need.
6. In the Status field, you can select **Enabled** or **Disabled** to enable or disable your entry.
7. Click the **Save** button.

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

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

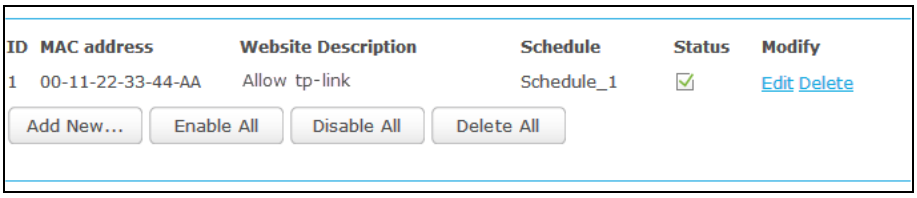
Click the **Delete All** button to delete all the entries in the table.

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

For example: If you desire that the child PC with MAC address 00-11-22-33-44-AA can access www.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 "**Advanced→Access Control→Schedule**" on the left to enter the Schedule Settings page. Click **Add New...** button to create a new schedule with Schedule Description is Schedule_1, Day is Sat and Time is all day-24 hours.
3. Click "**Parental Control**" menu on the left to go back to the Add or Modify Parental Control Entry page:
   1. Click **Add New...** button.
   2. Enter 00-11-22-33-44-AA in the **MAC Address of Child PC** field.
   3. Enter "Allow tp-link" in the **Website Description** field.
   4. Enter "www.tp-link.com" in the **Allowed Website Name** field.
   5. Select "Schedule_1" you create just now from the **Effective Time** drop-down list.
   6. In **Status** field, select Enable.
4. Click **Save** to complete the settings.

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



5.8 Access Control

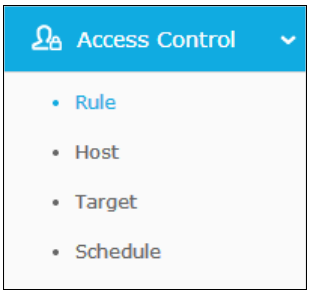


Figure 5-45 Access Control

There are four submenus under the Access Control menu as shown in Figure 5-45: **Rule**, **Host**, **Target** and **Schedule**. Click any of them, and you will be able to configure the corresponding function.

5.8.1 Rule

Choose menu "**Advanced→Access Control→Rule**", and then you can view and set Access Control rules in the screen as shown in Figure 5-46.

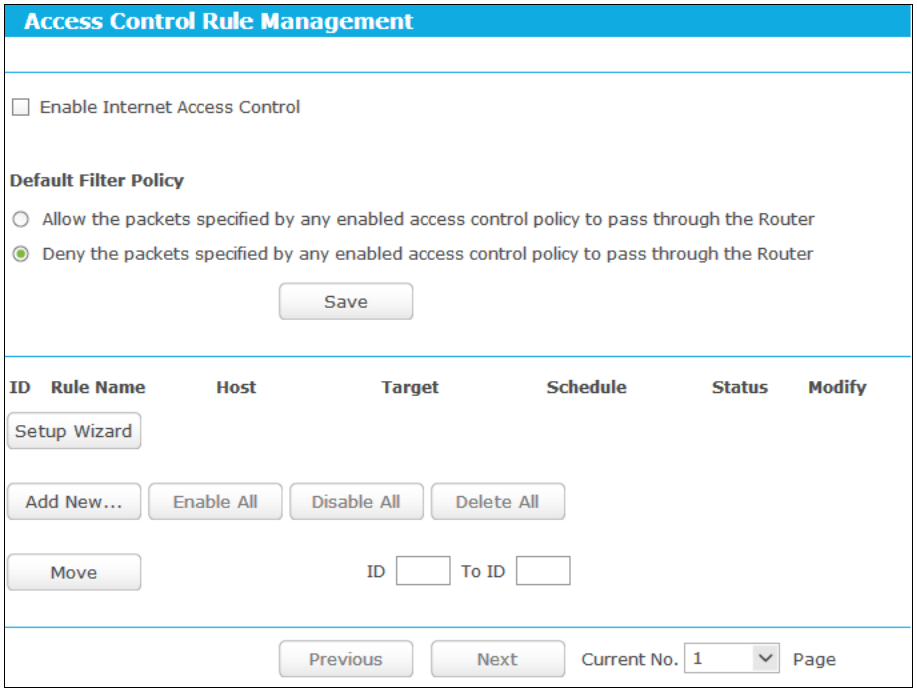


Figure 5-46 Access Control Rule Management

- **Enable Internet Access Control -** Select the checkbox to enable the Internet Access Control function, so the Default Filter Policy can take effect.
- **Rule Name -** Displays the name of the rule and this name is unique.
- **Host -** Displays the host selected in the corresponding rule.
- **Target -** Displays the target selected in the corresponding rule.
- **Schedule -** Displays the schedule selected in the corresponding rule.
- **Status -** Displays the status of the rule, enabled or not. Select the corresponding checkbox to enable the entry.
- **Modify -** Here you can edit or delete an existing rule.
- **Setup Wizard -** Click the **Setup Wizard** button to create a new rule entry.
- **Add New... -** Click the **Add New...** button to add a new rule entry.
- **Enable All -** Click the **Enable All** button to enable all the rules in the list.
- **Disable All -** Click the **Disable All** button to disable all the rules in the list.
- **Delete All -** Click the **Delete All** button to delete all the entries in the table.
- **Move -** You can change the entry's order as desired. Enter in the first box the ID number of the entry you want to move and in the second box another ID number, and then click the **Move** button to change the entries' order.

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

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

There are two methods to add a new rule.

Method One:

1. Click **Setup Wizard** button and the next screen will appear as shown in Figure 5-47.

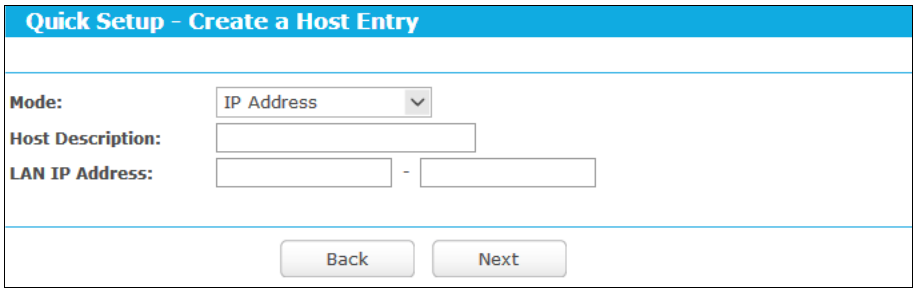


Figure 5-47 Quick Setup – Create a Host Entry

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

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

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

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

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

2. Click **Next** when finishing creating the host entry. The next screen will appear as shown in Figure 5-48.

Figure 5-48 Quick Setup – Create an Access Target Entry

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

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

- **IP Address** - Enter the IP address (or address range) of the target (targets) in dotted-decimal format (e.g. 192.168.0.33).
- **Target Port** - Specify the port or port range for the target. For some common service ports, you can make use of the Common Service Port item below.
- **Protocol** - Here are four options, All, TCP, UDP, and ICMP. Select one of them from the drop-down list for the target.
- **Common Service Port** - Lists some common service ports. Select one from the drop-down list and the corresponding port number will be filled in the Target Port field automatically. For example, if you select "FTP", "21" will be filled in the Target Port automatically.

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

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

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

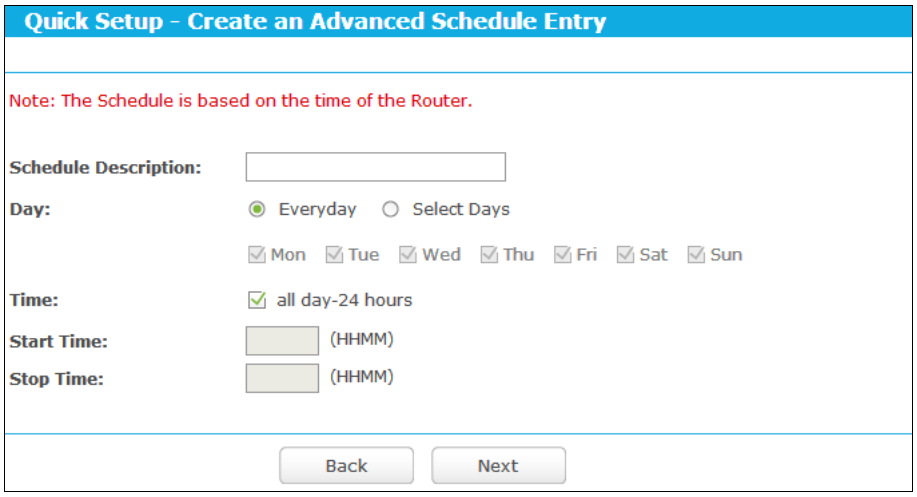


Figure 5-49 Quick Setup – Create an Advanced Schedule Entry

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

- **Stop Time** - Enter the stop time in HHMM format (HHMM are 4 numbers). For example 2000 is 20:00.

4. Click **Next** when finishing creating the advanced schedule entry. The next screen will appear as shown in Figure 5-50.

Figure 5-50 Quick Setup – Create an Internet Access Control Entry

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

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

Method Two:

1. Click the **Add New…** button and the next screen will pop up as shown in Figure 5-47.
2. Give a name (e.g. Rule_1) for the rule in the **Rule Name** field.
3. Select a host from the **Host** drop-down list or choose "**Click Here To Add New Host List**".
4. Select a target from the **Target** drop-sown list or choose "**Click Here To Add New Target List**".
5. Select a schedule from the **Schedule** drop-down list or choose "**Click Here To Add New Schedule**".
6. In the **Status** field, select **Enabled** or **Disabled** to enable or disable your entry.
7. Click the **Save** button.

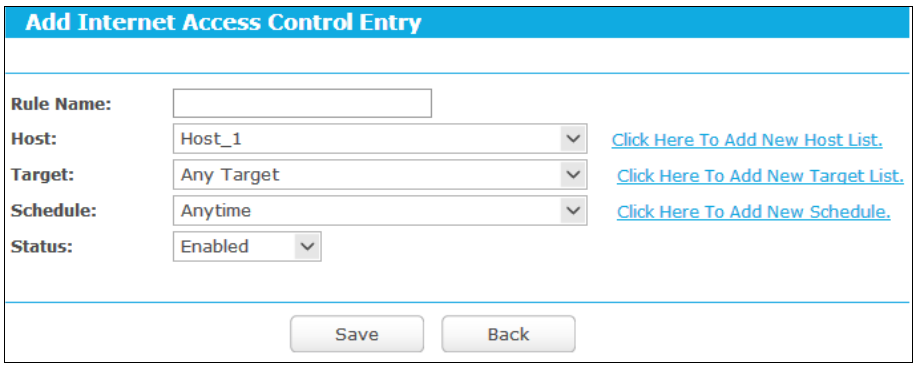
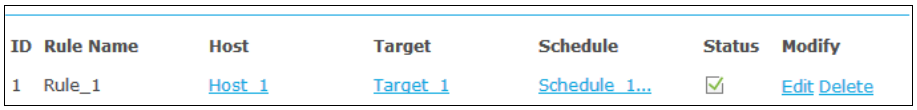


Figure 5-51 Add Internet Access Control Entry

For example: If you desire to allow the host with MAC address 00-11-22-33-44-AA to access www.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 the menu **Access Control** on the left. Select **Enable Internet Access Control** and choose "**Allow the packets specified by any enabled access control policy to pass through the router**".
2. Click **Setup Wizard** button.
3. Add a new host with the Host Description is Host_1 and MAC Address is 00-11-22-33-44-AA, and click **Next**.
4. Add a new target with the Target Description is Target_1 and Domain Name is www.tp-link.com, and click **Next**.
5. Add a new schedule with the Schedule Description is Schedule_1, Day is Sat and Sun, Start Time is 1800 and Stop Time is 2000, and click **Next**.
6. Add a new rule with the Rule Description is Rule_1, Host is Host_1, Target is Target_1, Schedule is Schedule_1, Status is Enabled, and click **Finish**.

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



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

5.8.2 Host

Choose menu "**Advanced→Access Control→Host**", and then you can view and set a Host list in the screen as shown in Figure 5-52. The host list is necessary for the Access Control Rule.

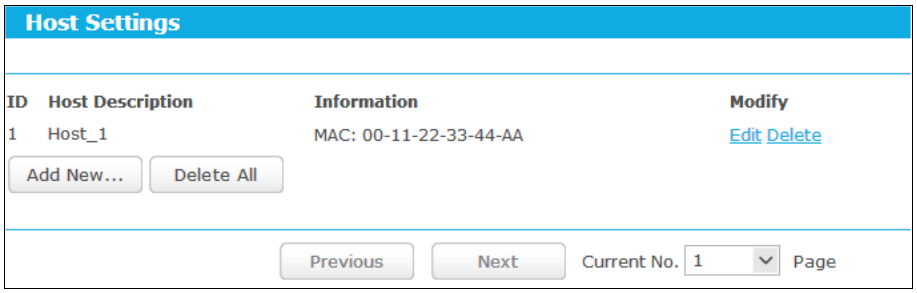


Figure 5-52 Host Settings

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

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

1. Click the **Add New…** button.
2. In the **Mode** field, select IP Address or MAC Address.
   - If you select IP Address, the screen is shown as Figure 5-53.
     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.

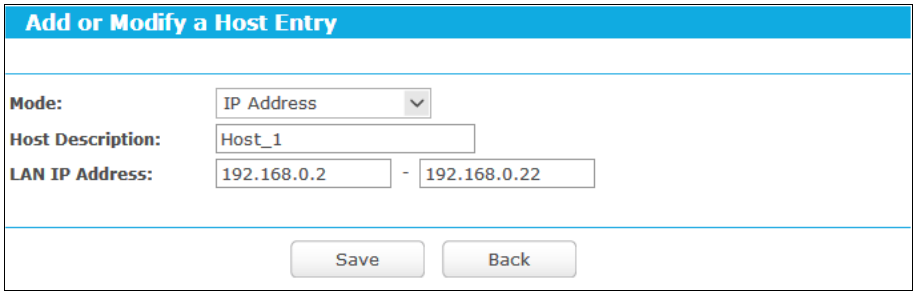


Figure 5-53 Add or Modify a Host Entry

   - If you select MAC Address, the screen is shown as Figure 5-54.
     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.

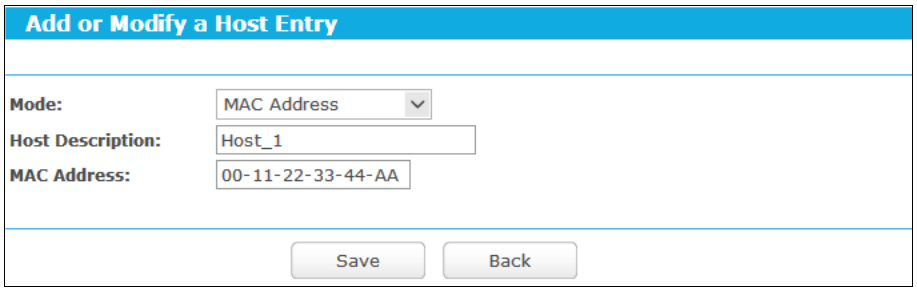


Figure 5-54 Add or Modify a Host Entry

3. Click the **Save** button to complete the settings.

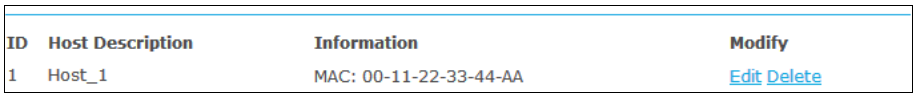
Click the **Delete All** button to delete all the entries in the table.

Click the **Next** button to go to the next page, or click the **Previous** button to 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 in Figure 5-52 to enter the Add or Modify a Host Entry page.
2. In **Mode** field, select MAC Address from the drop-down list.
3. In **Host Description** field, create a **unique** description for the host (e.g. Host_1).
4. In **MAC Address** field, enter 00-11-22-33-44-AA.
5. Click **Save** to complete the settings.

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



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

5.8.3 Target

Choose menu "**Advanced→Access Control→Target**", and then you can view and set a Target list in the screen as shown in Figure 5-55. The target list is necessary for the Access Control Rule.

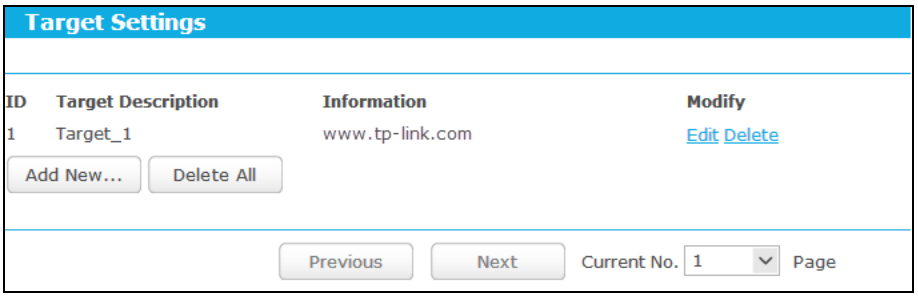


Figure 5-55 Target Settings

- **Target Description -** 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**.
3. If you select **IP Address**, the screen is shown as Figure 5-56.

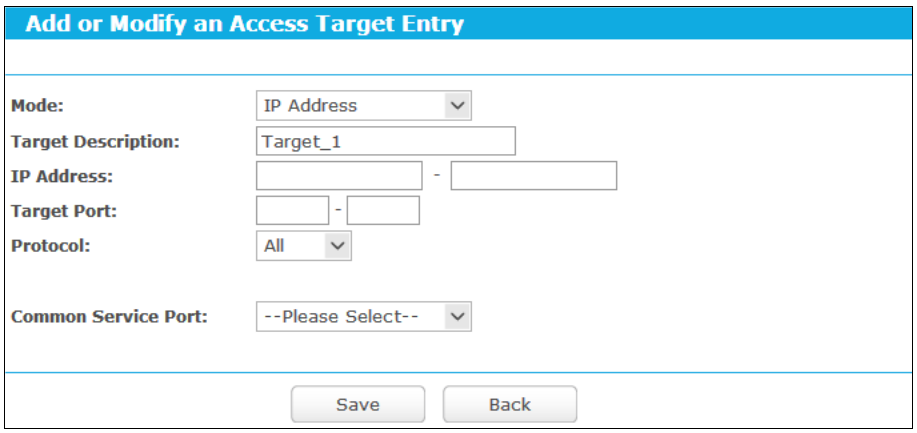


Figure 5-56 Add or Modify an Access Target Entry

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 from the drop-down list.

4. If you select **Domain Name**, the screen is shown as Figure 5-57.

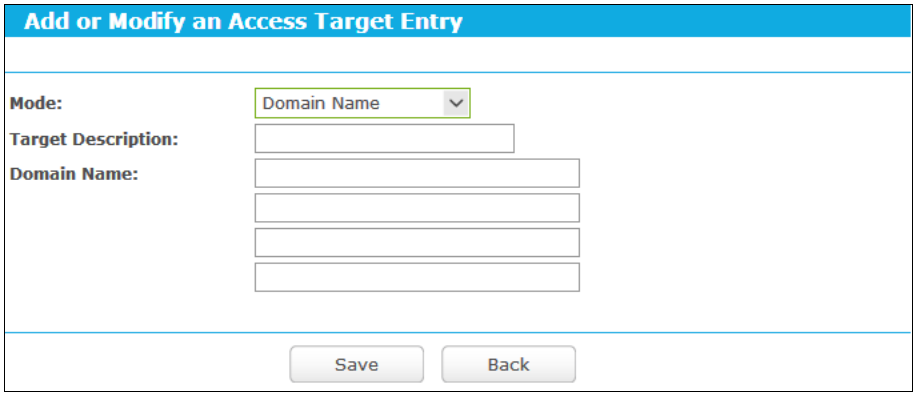


Figure 5-57 Add or Modify an Access Target Entry

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 (e.g. tp-link) in the blank. Any domain name with keywords in it (www.tp-link.com, www.tp-link.cn) will be blocked or allowed. You can enter 4 domain names.

5. 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 to 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 in Figure 5-55.
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.

ID	Target Description	Information	Modify
1	Target_1	www.tp-link.com	Edit Delete

5.8.4 Schedule

Choose menu "**Advanced→Access Control→Schedule**", and then you can view and set a schedule in the next screen as shown in Figure 5-58. The schedule is necessary for the Access Control Rule.

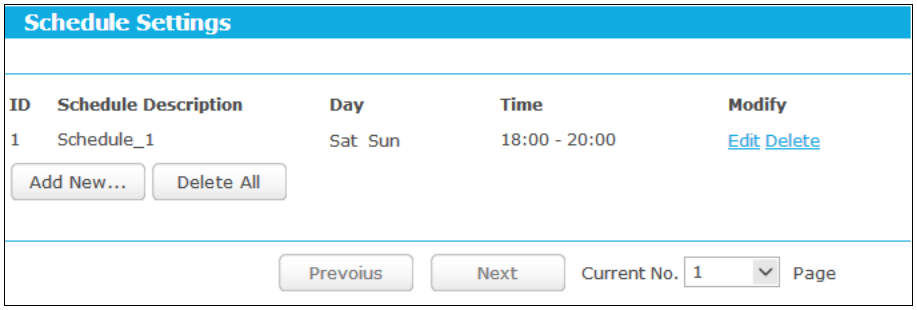


Figure 5-58 Schedule Settings

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

To add a new schedule, follow the steps below:

1. Click **Add New...** button shown in Figure 5-58 and the next screen will pop-up as shown in Figure 5-59.
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 to return to the previous page.

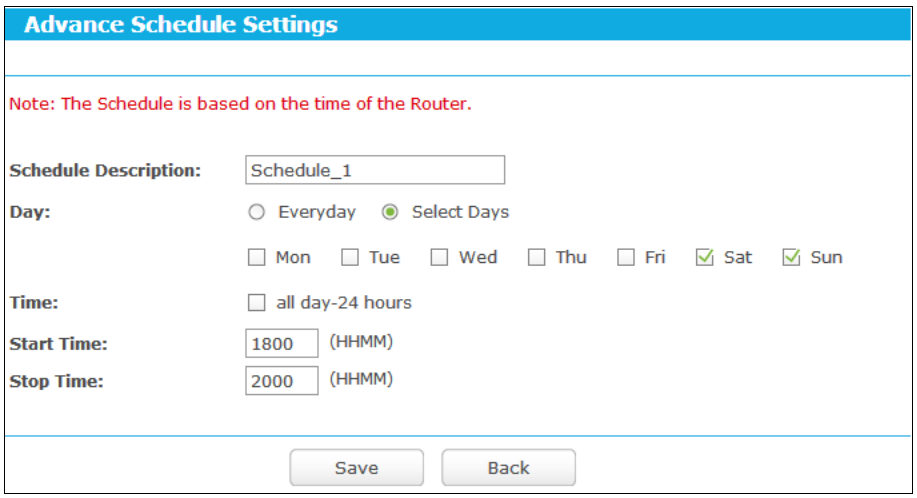


Figure 5-59 Advanced Schedule Settings

For example: If you desire to restrict the internet activities of host with MAC address 00-11-22-33-44-AA to access www.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 shown in Figure 5-58 to enter the Advanced Schedule Settings page.
2. In **Schedule Description** field, create a unique description for the schedule, e.g. Schedule_1.
3. In **Day** field, check the Select Days radio button and then select Sat and Sun.
4. In **Time** field, enter 1800 in Start Time field and 2000 in Stop Time field.
5. Click **Save** to complete the settings.

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

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

5.9 Advanced Routing

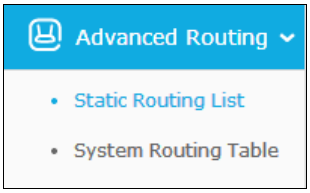


Figure 5-60 Advanced Routing

There are two submenus under the Advanced Routing menu as shown in Figure 5-60: **Static Routing List** and **System Routing Table**. Click any of them, and you will be able to configure the corresponding function.

5.9.1 Static Routing List

Choose menu "**Advanced→Advanced Routing→Static Routing List**", and then you can configure the static route in the next screen (shown in Figure 5-61). A static route is a pre-determined path that network information must travel to reach a specific host or network.

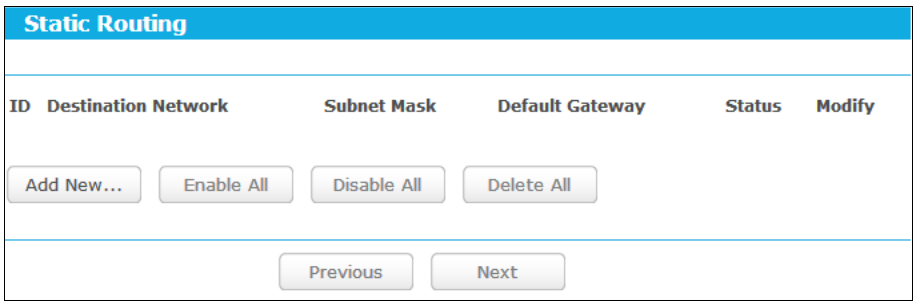


Figure 5-61 Static Routing

To add static routing entries:

1. Click **Add New…** shown in Figure 5-61, you will see the following screen.

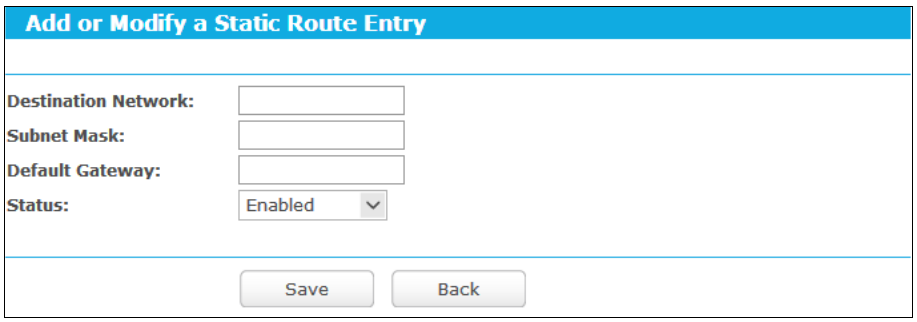


Figure 5-62 Add or Modify a Static Route Entry

2. Enter the following data:

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

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

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

Other configurations for the entries:

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

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

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

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

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

5.9.2 System Routing Table

Choose menu "**Advanced→Advanced Routing→System Routing Table**", and then you can view the System Routing Table in the next screen (shown in Figure 5-63). System routing table views all of the valid route entries in use. The Destination IP address, Subnet Mask, Gateway, and Interface will be displayed for each entry.

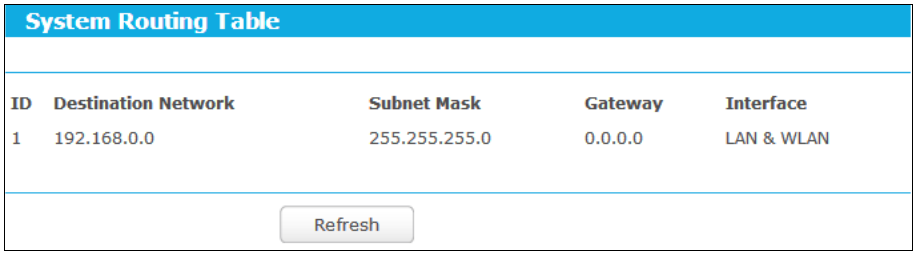


Figure 5-63 System Routing Table

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

5.10 Bandwidth Control

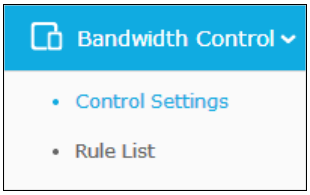


Figure 5-64 Bandwidth Control

There are two submenus under the Bandwidth Control menu as shown in Figure 5-64: **Control Settings** and **Rules List**. Click any of them, and you will be able to configure the corresponding function. The detailed explanations for each submenu are provided below.

Note:

Bandwidth Control will become invalid if NAT Boost is enabled. If you want to enable Bandwidth Control, please go to "**Advanced→NAT Boost**" to disable NAT Boost first.

5.10.1 Control Settings

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

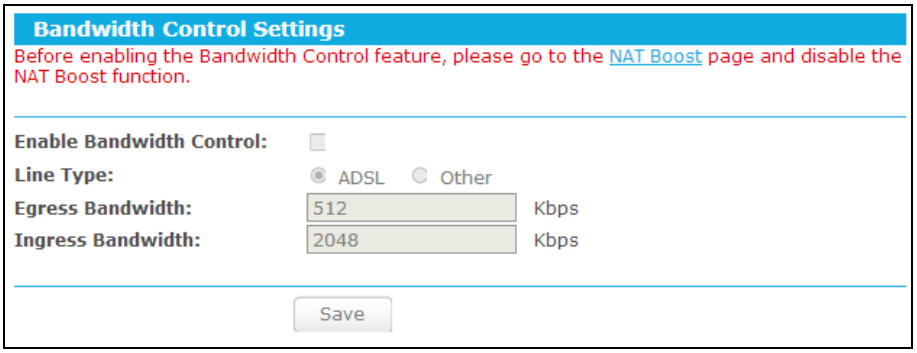


Figure 5-65 Bandwidth Control Settings

- **Enable Bandwidth Control -** Select this checkbox 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 Internet port.
- **Ingress Bandwidth -** The download speed through the Internet port.

5.10.2 Rules List

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

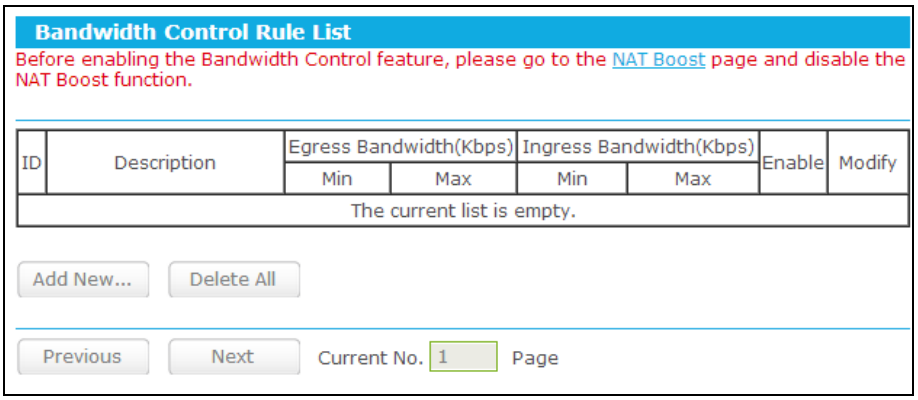


Figure 5-66 Bandwidth Control Rules List

- **Description -** This is the information about the rules such as address range.
- **Egress bandwidth -** This field displays the max and mix upload bandwidth through the Internet port, the default is 0.
- **Ingress bandwidth -** This field displays the max and mix download bandwidth through the Internet port, the default is 0.
- **Enable -** This displays the status of the rule.
- **Modify -** Click **Modify** to edit the rule. Click **Delete** to delete the rule.

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

1. Click **Add New…** shown in Figure 5-66, you will see a new screen shown in Figure 5-67.
2. Enter the information like the screen shown below.

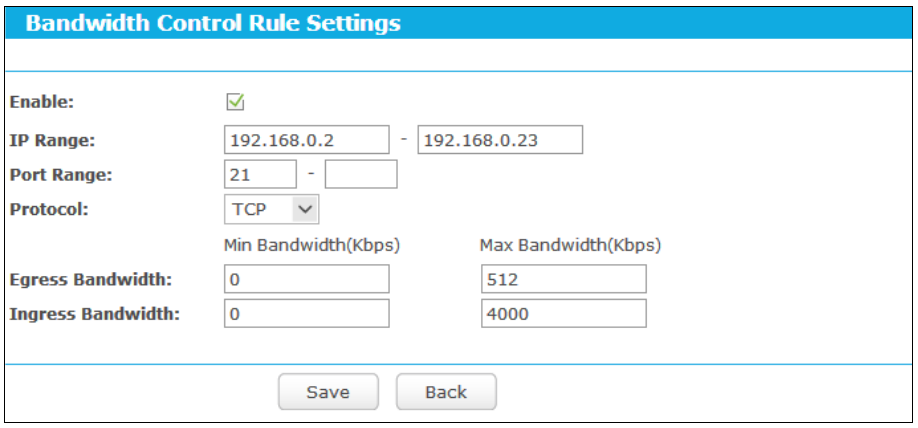


Figure 5-67 Bandwidth Control Rule Settings

3. Click the **Save** button.

5.11 IP & MAC Binding

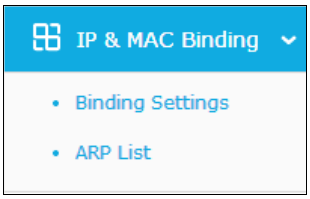


Figure 5-68 the IP & MAC Binding menu

There are two submenus under the IP &MAC Binding menu, shown in Figure 5-68: **Binding Settings** and **ARP List**. Click any of them, and you will be able to scan or configure the corresponding function. The detailed explanations for each submenu are provided below.

5.11.1 Binding Settings

Choose menu "**Advanced→Bandwidth Control→Binding Setting**", you can configure the IP & MAC binding rules in the screen as shown in Figure 5-69.

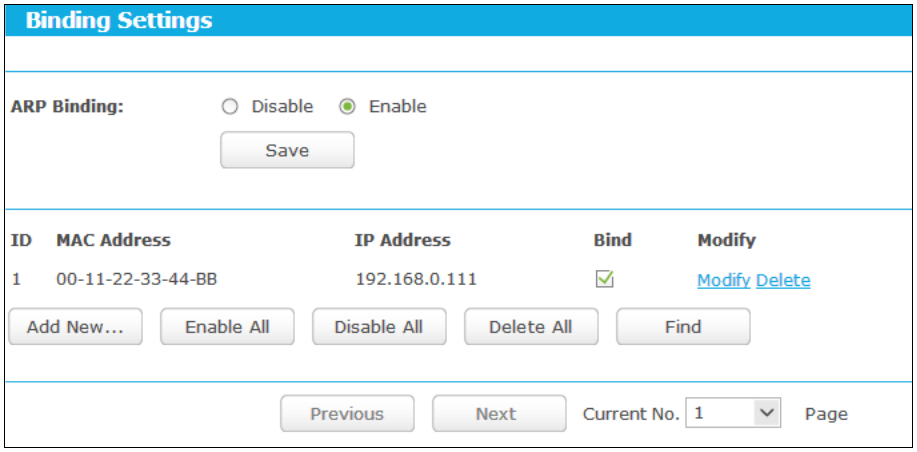


Figure 5-69 Binding Setting

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

When you want to add or modify an IP & MAC Binding entry, you can click the **Add New…** button or **Modify** button, and then you will go to the next page. This page is used for adding or modifying an IP & MAC Binding entry, shown in Figure 5-70.

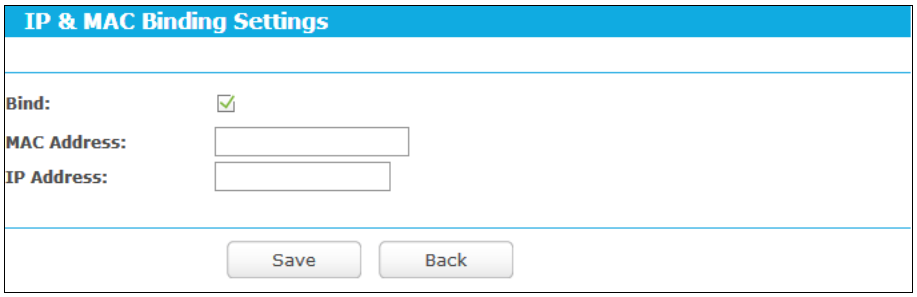


Figure 5-70 IP & MAC Binding Setting (Add & Modify)

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

1. Click the **Add New...** button as shown in Figure 5-69.
2. Enter the MAC Address and IP Address.
3. Select the Bind checkbox.
4. Click the **Save** button to save it.

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

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

To find an existing entry, follow the steps below.

1. Click the **Find** button in Figure 5-69.
2. Enter the MAC Address or IP Address.
3. Click the **Find** button in Figure 5-71.

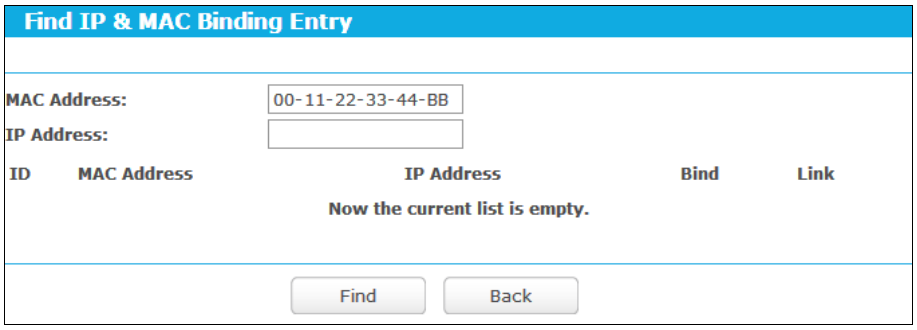


Figure 5-71 Find IP & MAC Binding Entry

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

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

5.11.2 ARP List

Choose menu "**Advanced→Bandwidth Control→ARP List**", you can see the ARP List, showing all the existing IP & MAC Binding entries as shown in Figure 5-72. To manage the computer, you could observe the computers in the LAN by checking the relationship of MAC address and IP address on the ARP list, and you could also configure the items on the ARP list.

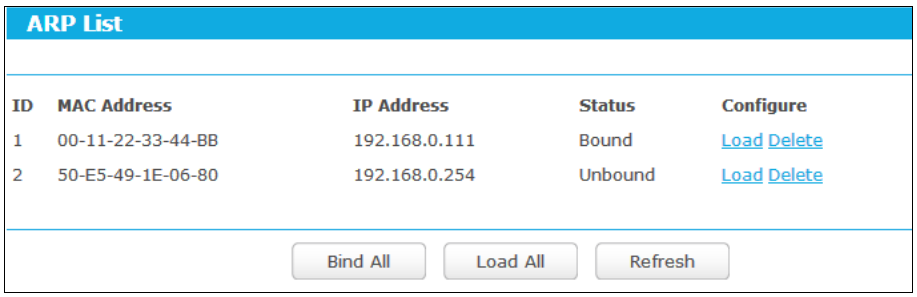


Figure 5-72 ARP List

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

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

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

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

Note:

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

5.12 Dynamic DNS

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

The router offers the **DDNS** (Dynamic Domain Name System) feature, which allows the hosting of a website, FTP server, or e-mail server with a fixed domain name (named by yourself) and a dynamic IP address, and then your friends can connect to your server by entering your domain name no matter what your IP address is. Before using this feature, you need to sign up for DDNS service providers such as www.comexe.cn, dyn.com/dns, or www.no-ip.com. The Dynamic DNS client service provider will give you a password or key.

5.12.1 Comexe DDNS

If the dynamic DNS **Service Provider** you select is www.comexe.cn, the page will appear as shown in Figure 5-73.

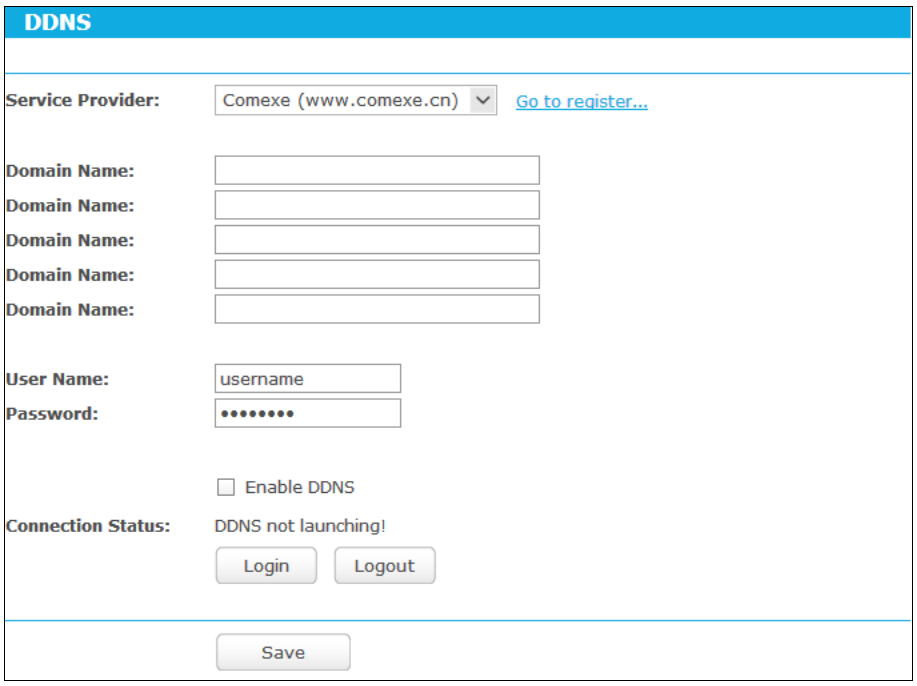


Figure 5-73 Comexe.cn DDNS Settings

To set up for DDNS, follow these instructions:

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

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

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

Note:

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

5.12.2 Dyn DDNS

If the dynamic DNS **Service Provider** you select is dyn.com/dns, the page will appear as shown in Figure 5-74.

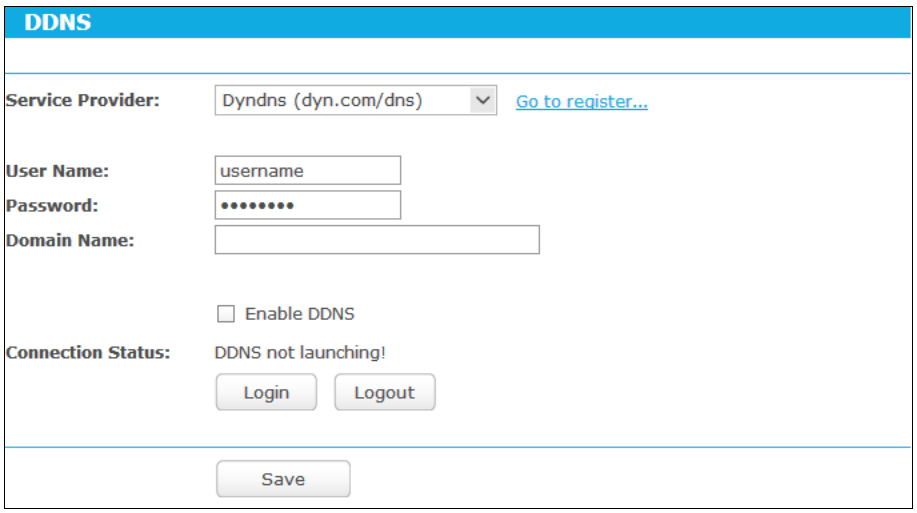


Figure 5-74 Dyndns.org DDNS Settings

To set up for DDNS, follow these instructions:

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

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

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

Note:

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

5.12.3 No-ip DDNS

If the dynamic DNS **Service Provider** you select is www.no-ip.com, the page will appear as shown in Figure 5-75.

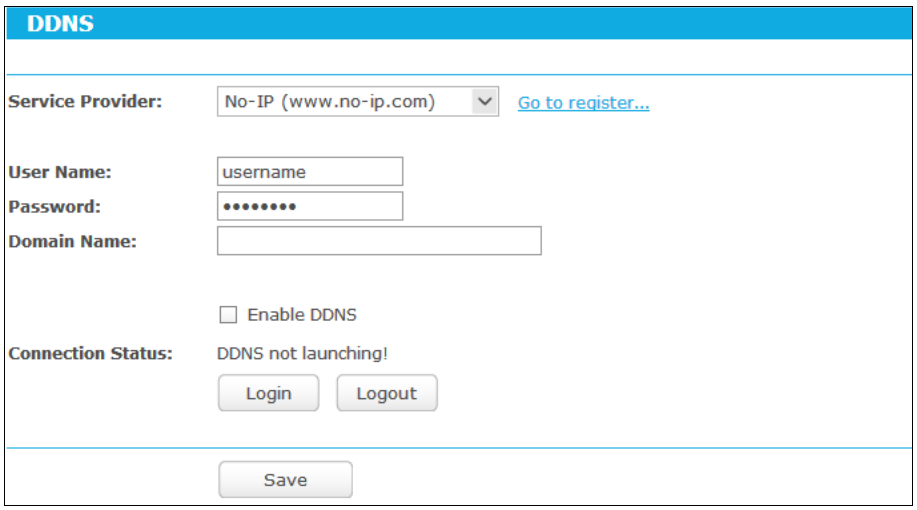


Figure 5-75 No-ip.com DDNS Settings

To set up for DDNS, follow these instructions:

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

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

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

Note:

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

5.13 IPv6 Support

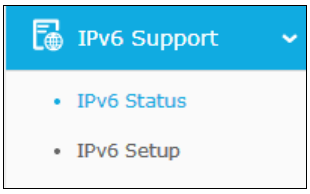


Figure 5-76 IPv6 Support

There are two submenus under the IPv6 Support menu (shown in Figure 5-76): **IPv6 Status** and **IPv6 Setup**. Click either of them, and you will be able to scan or configure the corresponding function. The detailed explanations for each submenu are provided below.

5.13.1 IPv6 Status

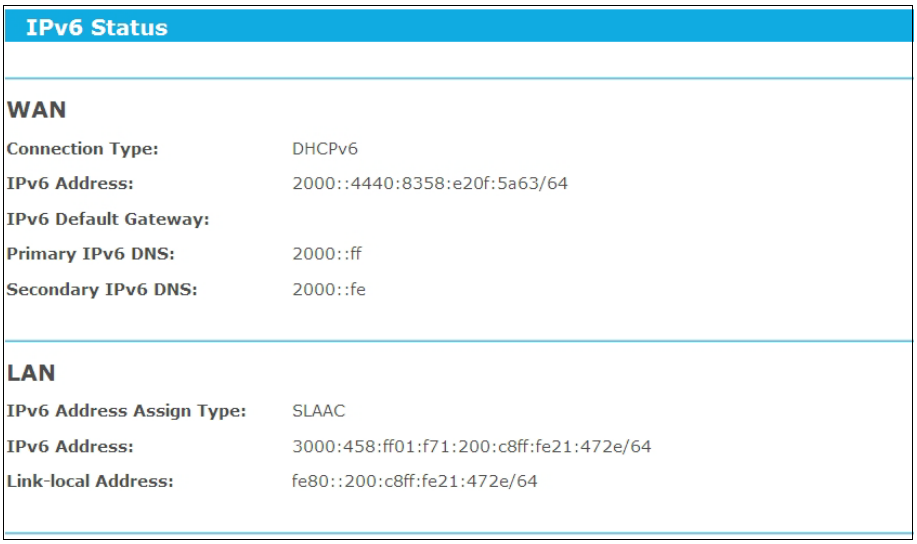


Figure 5-77 IPv6 Status

The **IPv6 Status** page displays the router's current IPv6 status and configuration. All information is read-only.

➢ **WAN**

- **Connection Type -** The IPv6 connection way for WAN
- **IPv6 Address -** The WAN IPv6 address
- **IPv6 Default Gateway -** The router's default gateway
- **Primary IPv6 DNS -** The primary IPv6 DNS address
- **Secondary IPv6 DNS -** The secondary IPv6 DNS address

➢ **LAN**

- **IPv6 Address Assign Type** - There are two types of assignation for IPv6 address: SLAAC (Stateless address auto-configuration) and DHCPv6 (Dynamic Host Configuration Protocol for IPv6) Server.

  1) SLAAC

  - **IPv6 Address Prefix** -The Prefix of IPv6 Address

  2) DHCPv6 Server

  - **Release Time** - the length of time a network user will be allowed to keep connecting to the router with the current DHCPv6 Address. Enter the amount of time (in seconds) that the DHCPv6 address will be leased. The time range is 1~691200 seconds. The default value is 86400 seconds.
  - **IPv6 Address** - Displays the LAN IPv6 Address.

5.13.2 IPv6 Setup

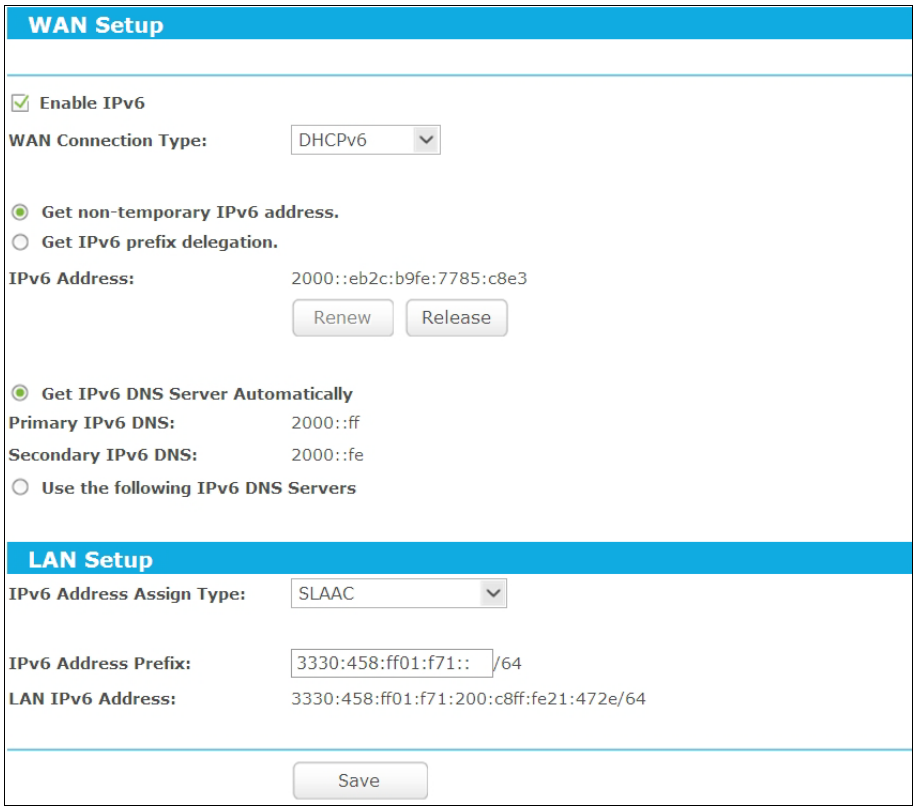


Figure 5-78 Enable/Disable IPv6

➢ **Enable IPv6** - Tick the checkbox to enable the IPv6 function. It's enabled by default.

➢ **WAN Connection Type** - Choose the correct WAN connection type based on your ISP network topology.

- **DHCPv6** - Connections which use dynamic IPv6 address assignment.
- **Static IPv6** - Connections which use static IPv6 address assignment.
- **PPPoEv6** - Connections which use PPPoEV6 that requires a user name and password.
- **Tunnel 6to4** - Connections which use 6to4 address assignment.

Different types of WAN connection require you to do different settings. Below are the detailed explanations for the respective type.

1) DHCPv6

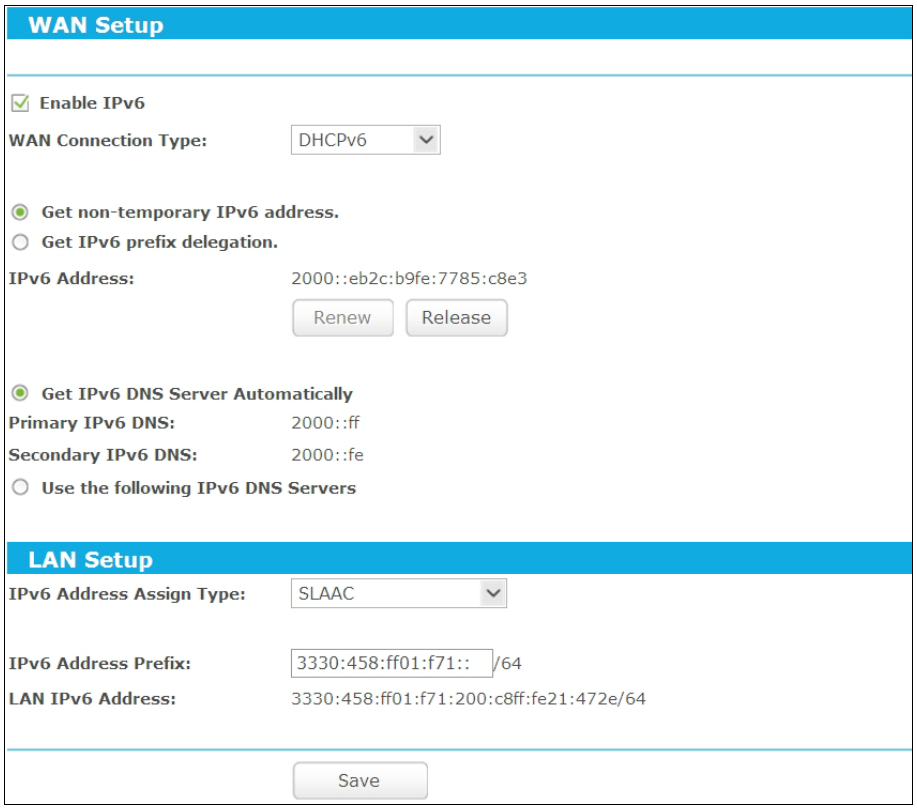


Figure 5-79 DHCPv6 - SLAAC

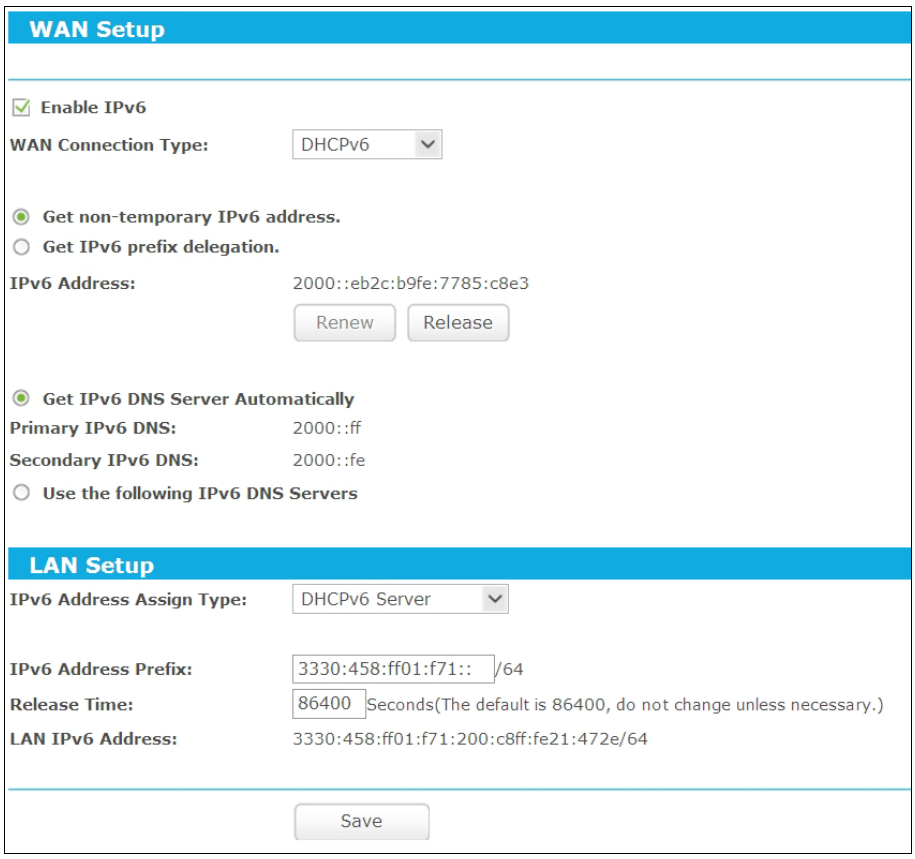


Figure 5-80 DHCPv6 – DHCPv6 Server

- **Get non-temporary IPv6 address** - Get a non-temporary IPv6 address from the ISP.
- **Get IPv6 prefix delegation** - Get a temporary IPv6 address and IPv6 prefix from the ISP, the temporary IPv6 address is set to the WAN port, and the LAN port advertise IPv6 address by RADVD or DHCPs.
- **IPv6 Address** - The IPv6 address assigned by your ISP dynamically.

Click the **Renew** button to renew the IPv6 parameters from your ISP.

Click the **Release** button to release the IPv6 parameters from your ISP.

If your ISP gives you one or two DNS IPv6 addresses, select **Use the following IPv6 DNS Servers** and enter the **Primary IPv6 DNS** and **Secondary IPv6 DNS** into the correct fields. Otherwise, the DNS servers will be assigned from ISP dynamically.

- **Primary IPv6 DNS** - Enter the DNS IPv6 address in dotted-decimal notation provided by your ISP.
- **Secondary IPv6 DNS** - Enter another DNS IPv6 address in dotted-decimal notation provided by your ISP.

Note:

If you get Address not found error when you access a Web site, it is likely that your DNS servers are set up improperly. You should contact your ISP to get DNS server addresses.

- **IPv6 Address Assign Type** - There are two types of assignation for IPv6 address: SLAAC (Stateless address auto-configuration) and DHCPv6 (Dynamic Host Configuration Protocol for IPv6) Server.

  SLAAC

  - **IPv6 Address Prefix** -The Prefix of IPv6 Address.

  DHCPv6 Server

  - **IPv6 Address Prefix** -The Prefix of IPv6 Address.
  - **Release Time** - the length of time a network user will be allowed to keep connecting to the router with the current DHCPv6 Address. Enter the amount of time (in seconds) that the DHCPv6 address will be leased. The time range is 1~691200 seconds. The default value is 86400 seconds.

- **LAN IPv6 Address** - Displays the LAN IPv6 Address.

2) Static IPv6

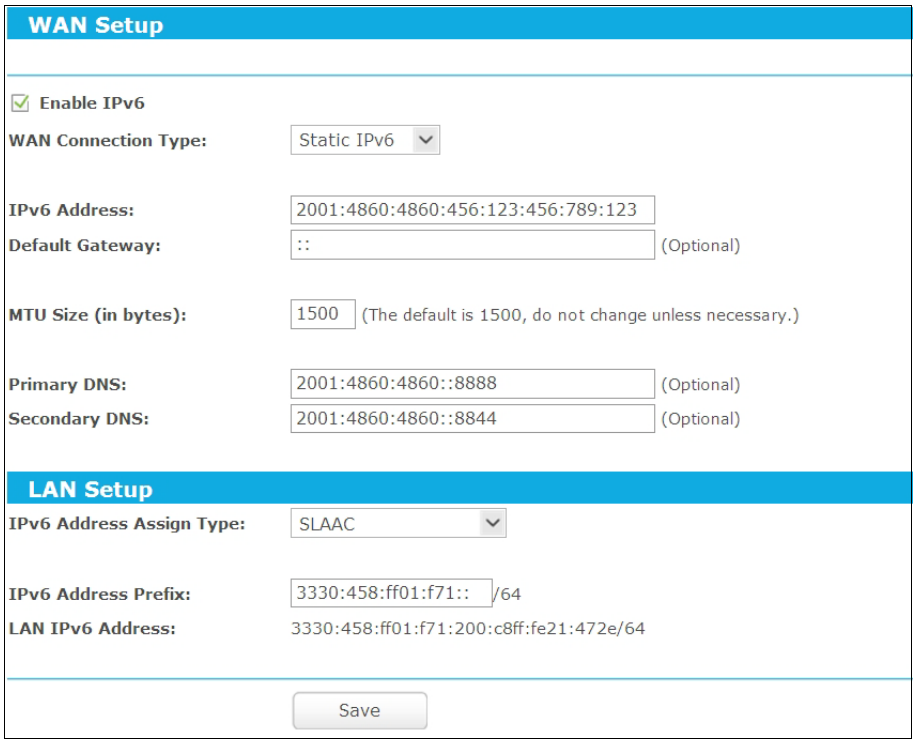


Figure 5-81 Static IPv6 - SLAAC

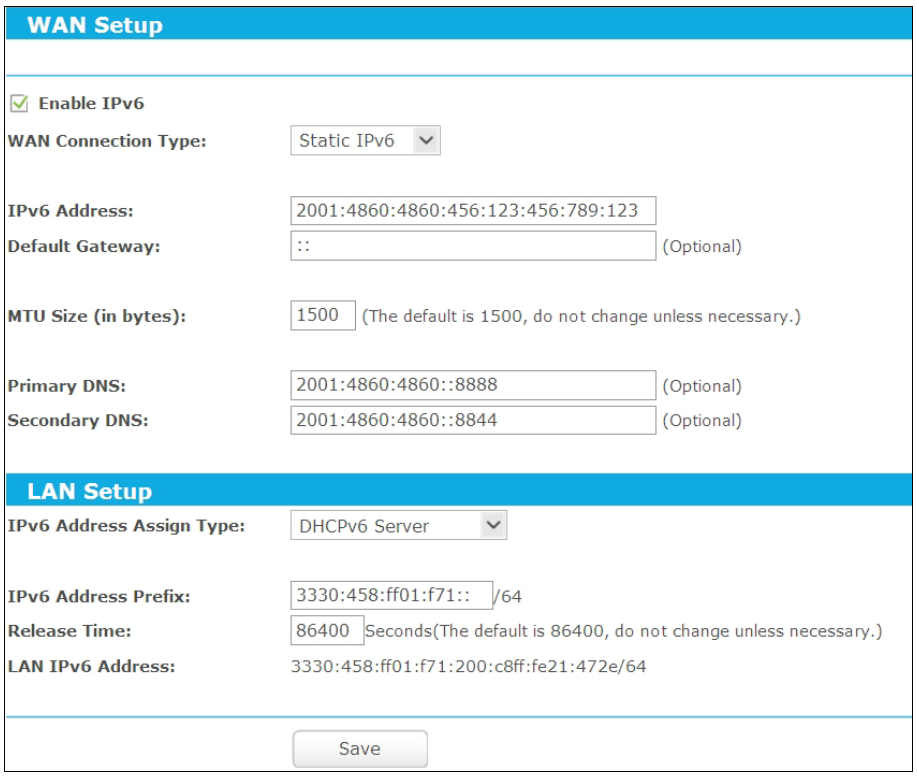


Figure 5-82 Static IPv6 – DHCPv6 Server

- **IPv6 Address** - Enter the IPv6 address in dotted-decimal notation provided by your ISP.
- **Default Gateway** - Enter the default gateway in dotted-decimal notation provided by your ISP.
- **MTU Size** - The normal MTU (Maximum Transmission Unit) value for most Ethernet networks is 1500 Bytes. For some ISPs, you may need to modify the MTU. But this is rarely required, and should not be done unless you are sure it is necessary for your ISP connection.
- **Primary DNS** - Enter the DNS IPv6 address in dotted-decimal notation provided by your ISP.
- **Secondary DNS** - Enter another DNS IPv6 address in dotted-decimal notation provided by your ISP.
- **IPv6 Address Assign Type** - There are two types of assignation for IPv6 address: SLAAC (Stateless address auto-configuration) and DHCPv6 (Dynamic Host Configuration Protocol for IPv6) Server.

SLAAC

- **IPv6 Address Prefix** -The Prefix of IPv6 Address

DHCPv6 Server

- **IPv6 Address Prefix** -The Prefix of IPv6 Address
- **Release Time** - the length of time a network user will be allowed to keep connecting to the router with the current DHCPv6 Address. Enter the amount of time (in seconds)

that the DHCPv6 address will be leased. The time range is 1~691200 seconds. The default value is 86400 seconds.

➢ **LAN IPv6 Address** - Displays the LAN IPv6 Address.

3) PPPoEv6

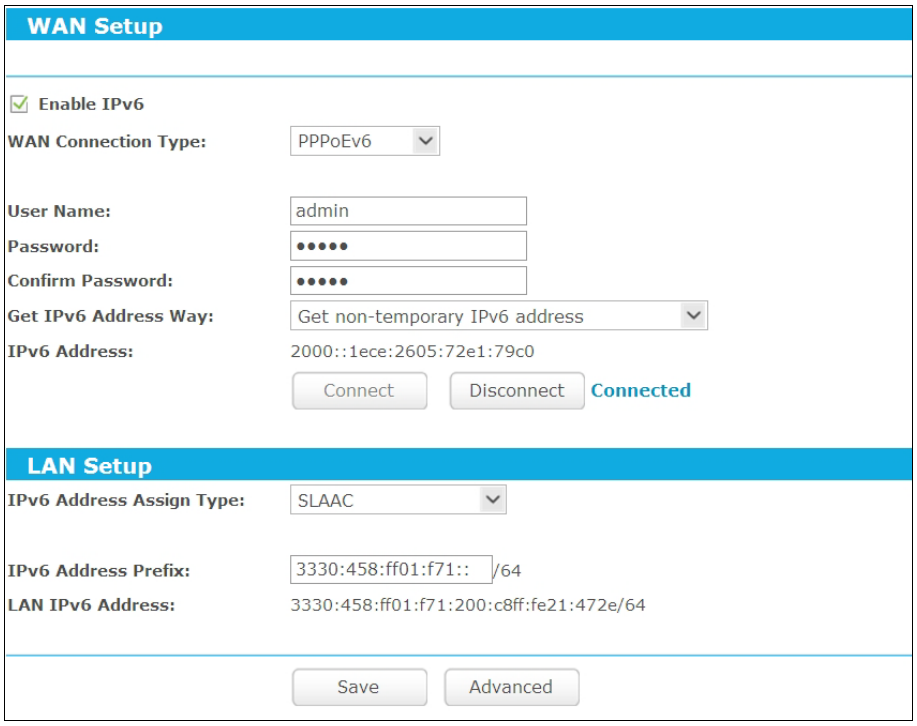


Figure 5-83 PPPoEv6 - SLAAC

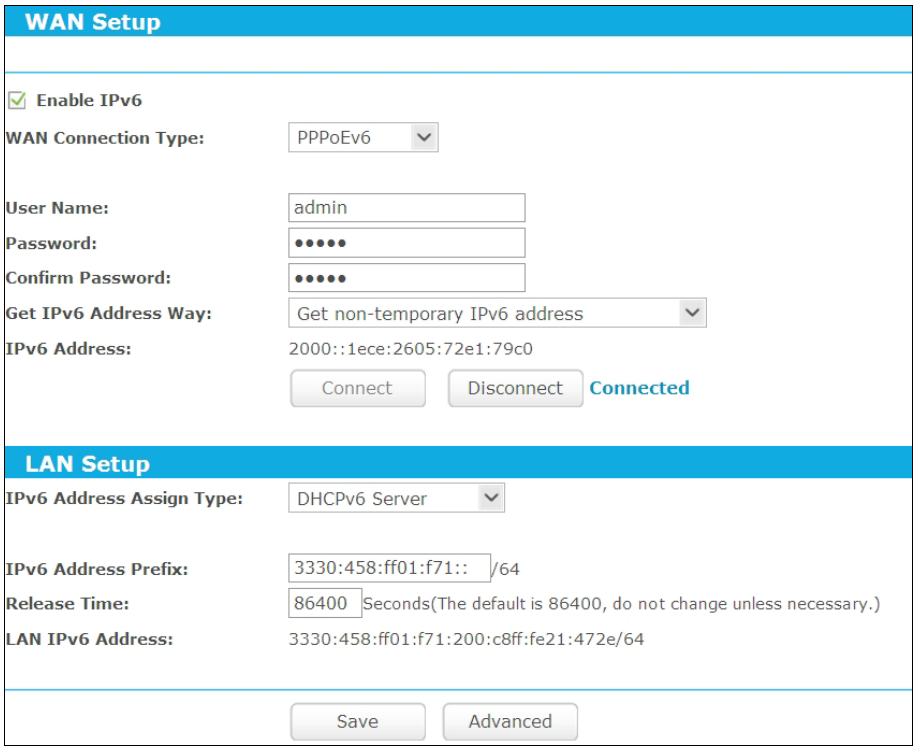


Figure 5-84 PPPoEv6 – DHCPv6 Server

- **User Name/Password** - Enter the User Name and Password provided by your ISP. These fields are case-sensitive.
- **Get IPv6 Address Way**
  - **Get non-temporary IPv6 address** - Get a non-temporary IPv6 address by DHCPv6 from the ISP.
  - **Get IPv6 prefix delegation** - Get a prefix delegation IPv6 address by DHCPv6 from the ISP, and the clients in LAN create IPv6 address with the delegation.
  - **Use IP address specified by ISP** - Input a static IPv6 address from the ISP

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

- **IPv6 Address Assign Type** - There are two types of assignation for IPv6 address: SLAAC (Stateless address auto-configuration) and DHCPv6 (Dynamic Host Configuration Protocol for IPv6) Server.

  SLAAC

  - **IPv6 Address Prefix** -The Prefix of IPv6 Address

  DHCPv6 Server

  - **IPv6 Address Prefix** -The Prefix of IPv6 Address
  - **Release Time** - the length of time a network user will be allowed to keep connecting to the router with the current DHCPv6 Address. Enter the amount of time (in seconds) that the DHCPv6 address will be leased. The time range is 1~691200 seconds. The default value is 86400 seconds.
- **LAN IPv6 Address** - Displays the LAN IPv6 Address.

4) Tunnel 6to4

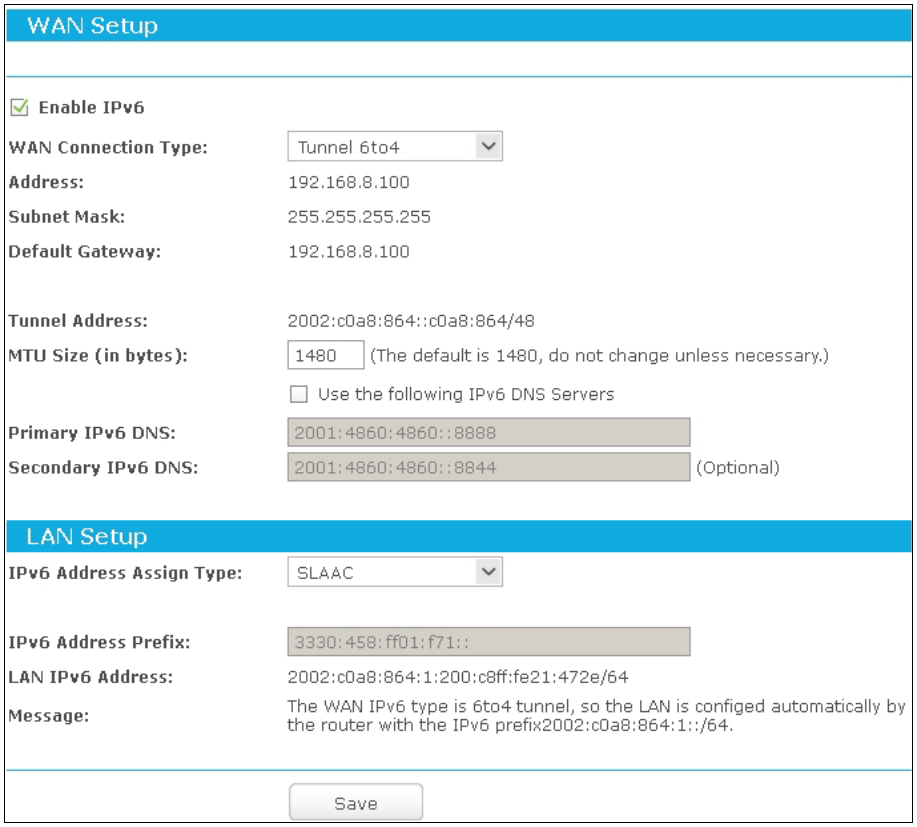


Figure 5-85 Tunnel 6to4 - SLAAC

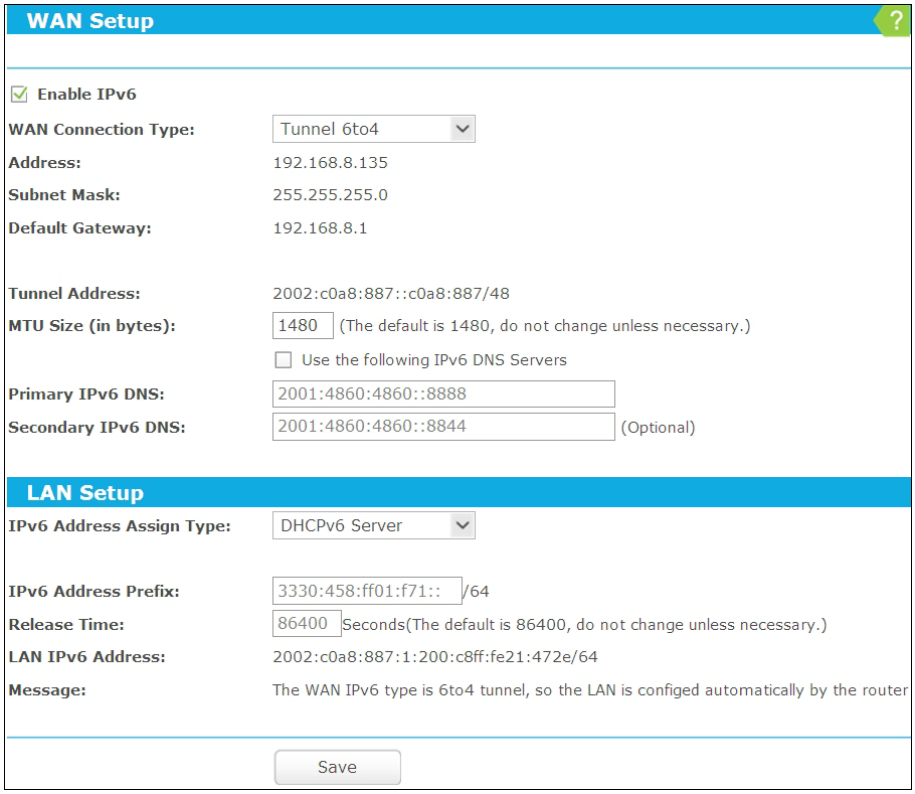


Figure 5-86 Tunnel 6to4 – DHCPv6 Server

- **Address/Subnet Mask/Default Gateway** - the IPv4 address/ subnet mask/ default gateway assigned, in dotted-decimal notation.

- **MTU Size** - The normal MTU (Maximum Transmission Unit) value for most Ethernet networks is 1480 Bytes. For some ISPs, you may need to modify the MTU. But this is rarely required, and should not be done unless you are sure it is necessary for your ISP connection.

If your ISP gives you one or two DNS IPv6 addresses, select **Use the following IPv6 DNS Servers** and enter the **Primary IPv6 DNS** and **Secondary IPv6 DNS** into the correct fields. Otherwise, the DNS servers will be assigned from ISP dynamically.

- **Primary IPv6 DNS** - Enter the DNS IPv6 address in dotted-decimal notation provided by your ISP.
- **Secondary IPv6 DNS** - Enter another DNS IPv6 address in dotted-decimal notation provided by your ISP.
- **IPv6 Address Assign Type** - There are two types of assignation for IPv6 address: SLAAC (Stateless address auto-configuration) and DHCPv6 (Dynamic Host Configuration Protocol for IPv6) Server.

  SLAAC

  - **IPv6 Address Prefix** -The Prefix of IPv6 Address

  DHCPv6 Server

  - **IPv6 Address Prefix** -The Prefix of IPv6 Address
  - **Release Time** - the length of time a network user will be allowed to keep connecting to the router with the current DHCPv6 Address. Enter the amount of time (in seconds) that the DHCPv6 address will be leased. The time range is 1~691200 seconds. The default value is 86400 seconds.
- **IPv6 Address** - Displays the LAN IPv6 Address.

5.14 System Tools

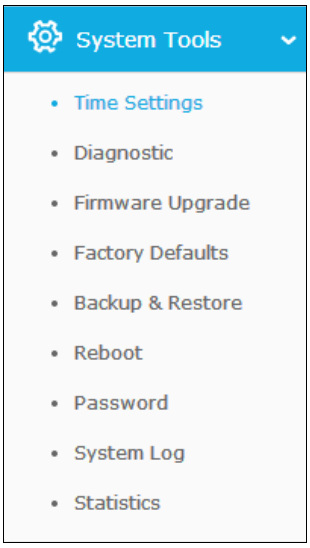


Figure 5-87 The System Tools menu

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

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

5.14.1 Time Settings

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

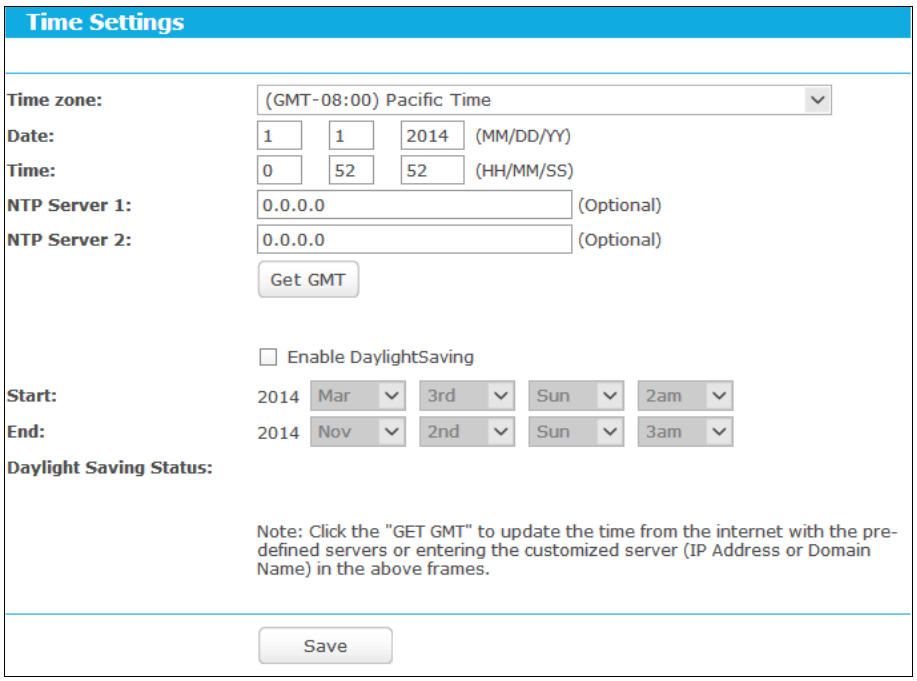


Figure 5-88 Time settings

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

To set time manually:

1. Select your local time zone.

2. Enter the **Date** in Month/Day/Year format.
3. Enter the **Time** in Hour/Minute/Second format.
4. Click **Save**.

To set time automatically:

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

To set Daylight Saving:

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

Figure 5-89 Time settings

Note:

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

5.14.2 Diagnostic

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

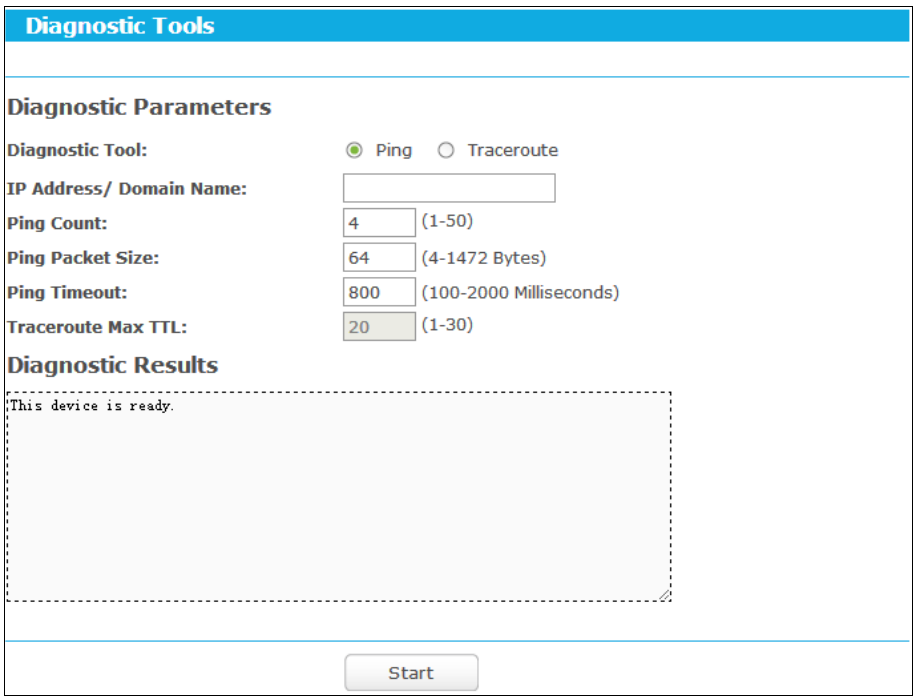


Figure 5-90 Diagnostic Tools

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

Note:

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

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

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

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

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

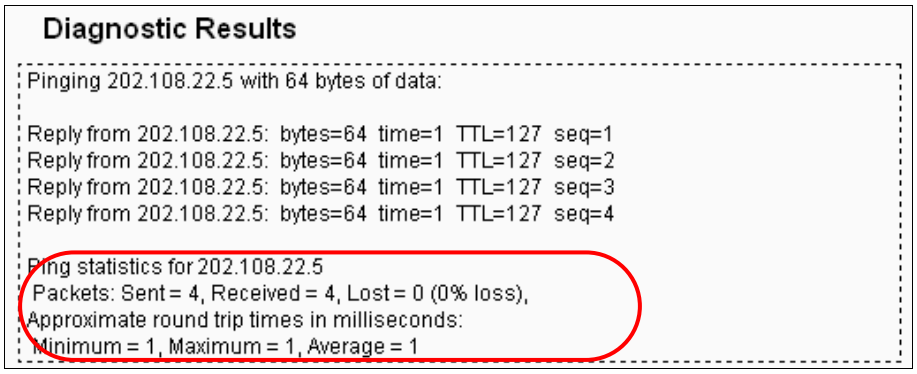


Figure 5-91 Diagnostic Results

Note:

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

5.14.3 Firmware Upgrade

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

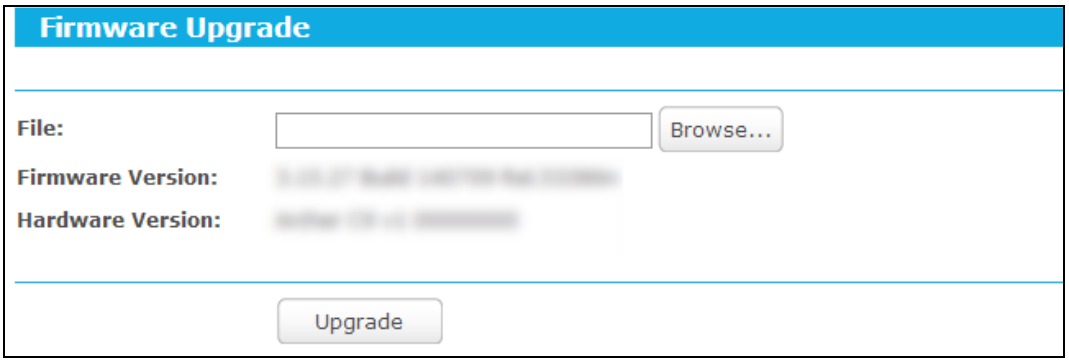


Figure 5-92 Firmware Upgrade

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

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

1. Download a most recent firmware upgrade file from our website (www.tp-link.com).
2. Enter or select the path name where you save the downloaded file on the computer into the **File** blank.
3. Click the **Upgrade** button.
4. The router will reboot while the upgrading has been finished.

Note:

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

5.14.4 Factory Defaults

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

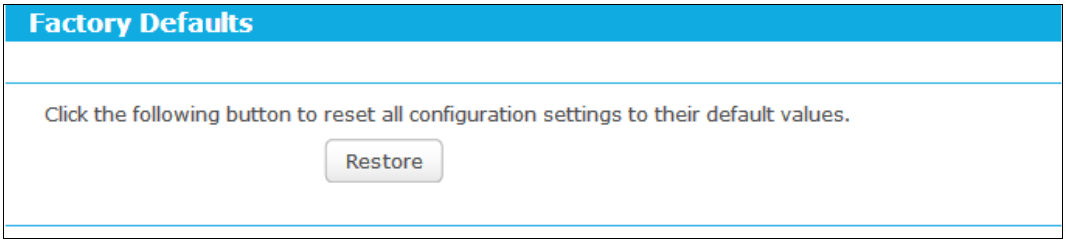


Figure 5-93 Restore Factory Default

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

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

Note:

All changed settings will be lost when defaults are restored.

5.14.5 Backup & Restore

Choose menu "**Advanced→System Tools→Backup & Restore**", and then you can save the current configuration of the router as a backup file and restore the configuration via a backup file as shown in Figure 5-94.

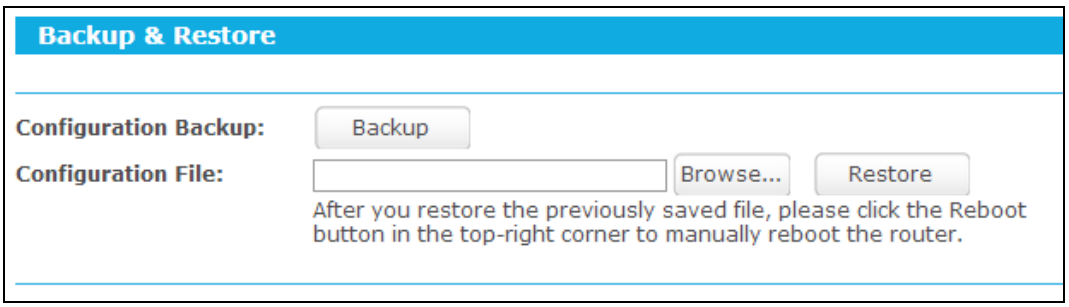


Figure 5-94 Backup & Restore Configuration

- Click the **Backup** button to save all configuration settings as a backup file in your local computer.
- To upgrade the router's configuration, follow these instructions.
  - Click the **Browse** button to find the configuration file which you want to restore.
  - Click the **Restore** button to update the configuration with the file whose path is the one you have input or selected in the blank.

Note:

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

5.14.6 Reboot

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

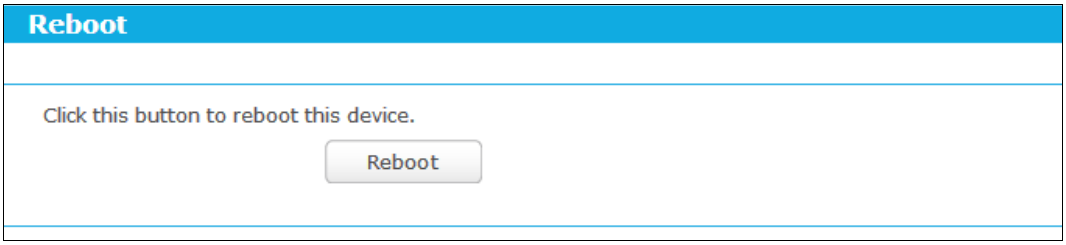


Figure 5-95 Reboot the router

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

- Change the LAN IP Address (system will reboot automatically).
- Change the DHCP Settings.
- Change the Wireless configurations.
- Change the Web Management Port.
- Upgrade the firmware of the router (system will reboot automatically).
- Restore the router's settings to factory defaults (system will reboot automatically).
- Update the configuration with the file (system will reboot automatically.

5.14.7 Password

Choose menu "**Advanced→System Tools→Password**", and then you can change the factory default user name and password of the router in the next screen as shown in Figure 5-96.

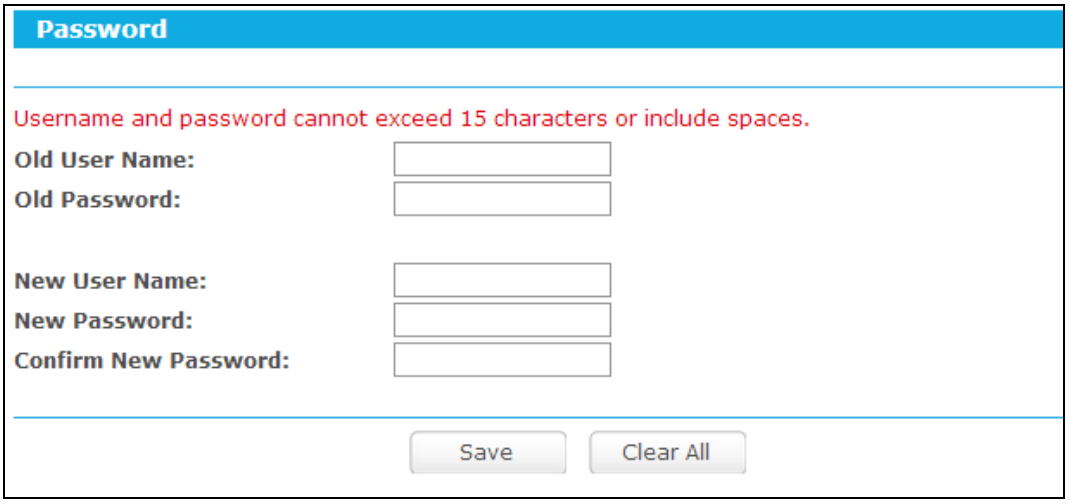


Figure 5-96 Password

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

Note:

The new user name and password must not exceed 15 characters in length and not include any spaces. Enter the new Password twice to confirm it.

Click the **Save** button when finished.

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

5.14.8 System Log

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

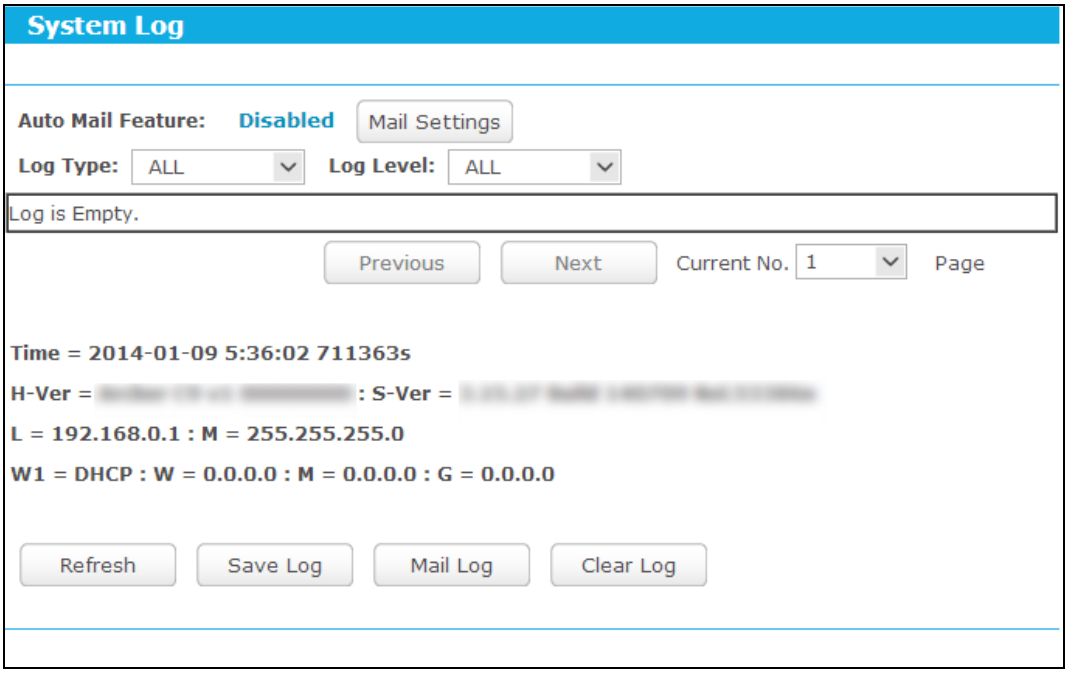


Figure 5-97 System Log

- **Auto Mail Feature -** Indicates whether auto mail feature is enabled or not.
- **Mail Settings -** Set the receiving and sending mailbox address, server address, validation information as well as the timetable for Auto Mail Feature, as shown in Figure 5-98.

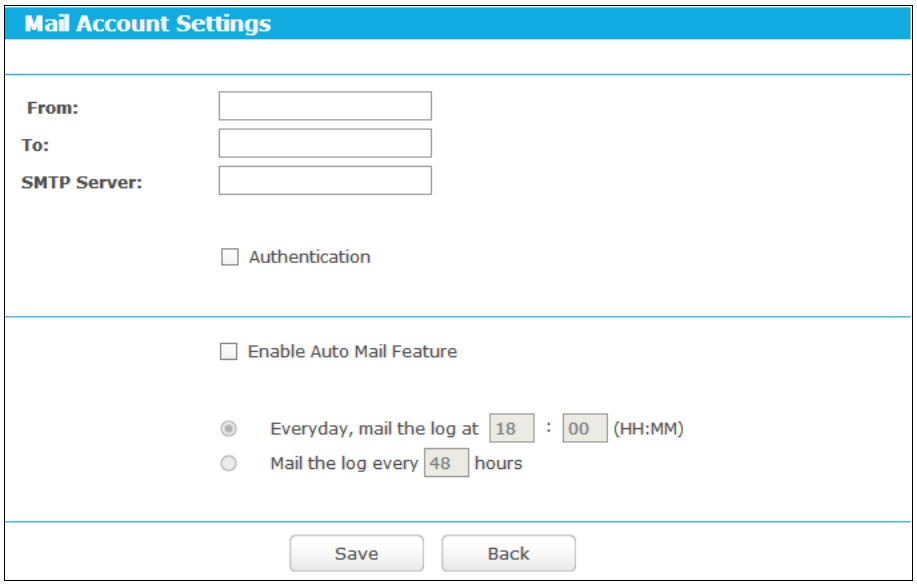


Figure 5-98 Mail Account Settings

- **From -** Your mail box address. The router would connect it to send logs.
- **To -** Recipient's address. The destination mailbox where the logs would be received.
- **SMTP Server -** Your smtp server. It corresponds with the mailbox filled in the **From** field. You can log on the relevant website for help if you are not clear with the address.
- **Authentication -** Most SMTP Server requires Authentication. It is required by most mailboxes that need User Name and Password to log in.

☞ **Note:**

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

- **User Name -** Your mail account name filled in the From field. The part behind @ is included.
- **Password -** Your mail account password.
- **Confirm The Password -** Enter the password again to confirm.
- **Enable Auto Mail Feature -** Select it to mail logs automatically. You could mail the current logs either at a specified time every day or by intervals, but only one could be the current effective rule. Enter the desired time or intervals in the corresponding field as shown in Figure 5-98.

Click **Save** to keep your settings.

Click **Back** to return to the previous page.

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

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

5.14.9 Statistics

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

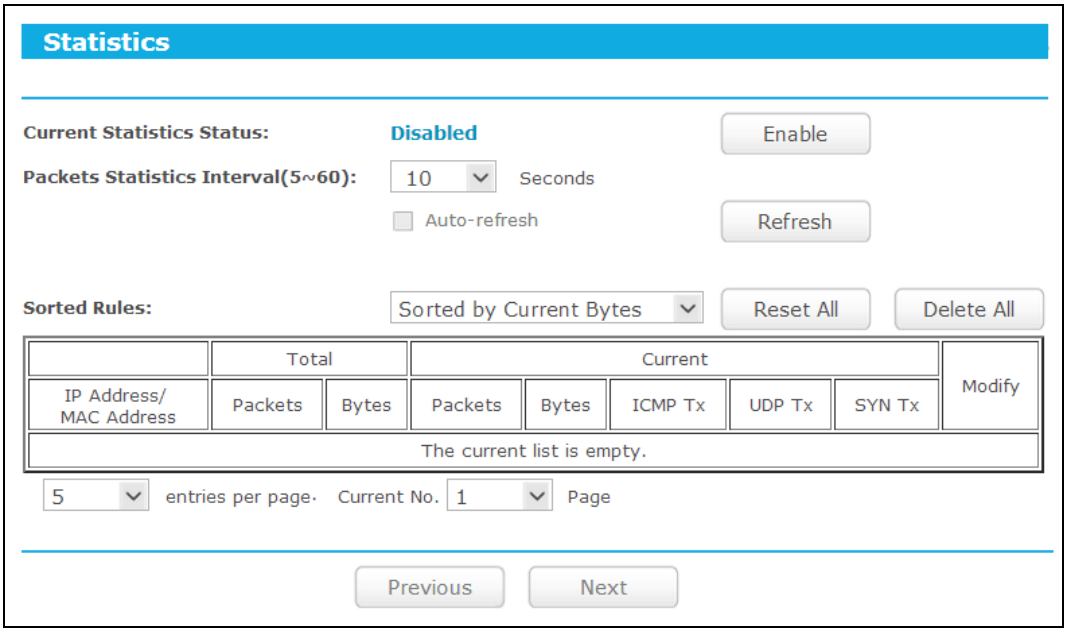


Figure 5-99 Statistics

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

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

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

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

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

Statistics Table:

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

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

Appendix A: FAQ

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

1) First, configure the ADSL Modem configured in RFC1483 bridge model.

2) Connect the Ethernet cable from your ADSL Modem to the Internet port on the router. The telephone cord plugs into the Line port of the ADSL Modem.

3) Login to the router, click the “Network” menu on the left of your browser, and click "WAN" submenu. On the WAN page, select “PPPoE/Russia PPPoE” for WAN Connection Type. Type user name in the “User Name” field and password in the “Password” field, type password in the “Confirm Password” field again, finish by clicking “Connect”.

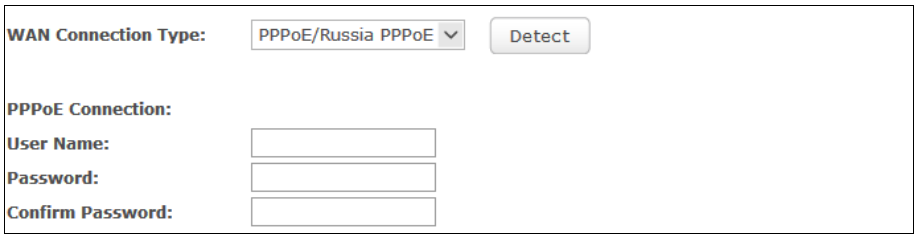


Figure A-1 PPPoE Connection Type

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

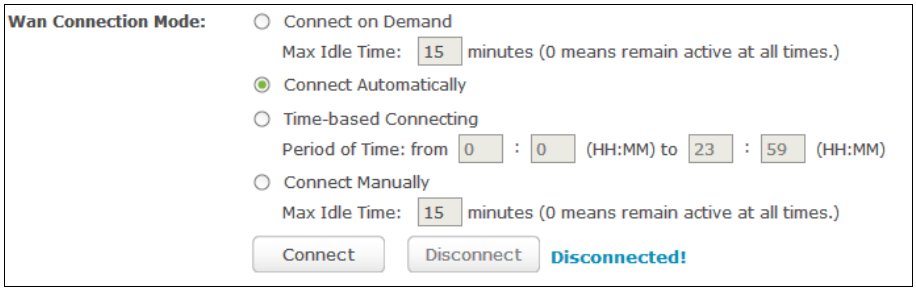


Figure A-2 PPPoE Connection Mode

Note:

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

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

1) Login to the router, click the “Network” menu on the left of your browser, and click "WAN" submenu. On the WAN page, select “Dynamic IP” for "WAN Connection Type", finish by clicking “Save”.

2) Some ISPs require that you register the MAC Address of your adapter, which is connected to your cable/DSL Modem during installation. If your ISP requires MAC register, login to the router and click the "Network" menu link on the left of your browser, and then click "MAC Clone" submenu link. On the "MAC Clone" page, if your PC’s MAC address is proper MAC address, click the "Clone MAC Address" button and your PC’s MAC address will fill in the "WAN MAC Address" field. Or else, type the MAC Address into the "WAN MAC Address" field. The format for the MAC Address is XX-XX-XX-XX-XX-XX. Then click the "Save" button. It will take effect after rebooting.

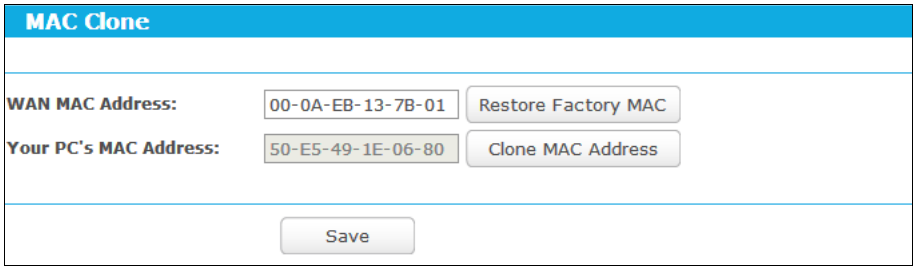


Figure A-3 MAC Clone

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

1) If you start Netmeeting as a host, you don’t need to do anything with the router.

2) If you start as a response, you need to configure Virtual Server or DMZ Host and make sure the H323 ALG is enabled.

3) How to configure Virtual Server: Log in to the router, click the “**Forwarding**” menu on the left of your browser, and click "**Virtual Servers**" submenu. On the "**Virtual Servers**" page, click **Add New…**. Then on the “**Add or Modify a Virtual Server Entry**” page, enter “1720” for the “Service Port” blank, and your IP address for the “IP Address” blank, taking 192.168.0.169 for an example, remember to **Enable** and **Save**.

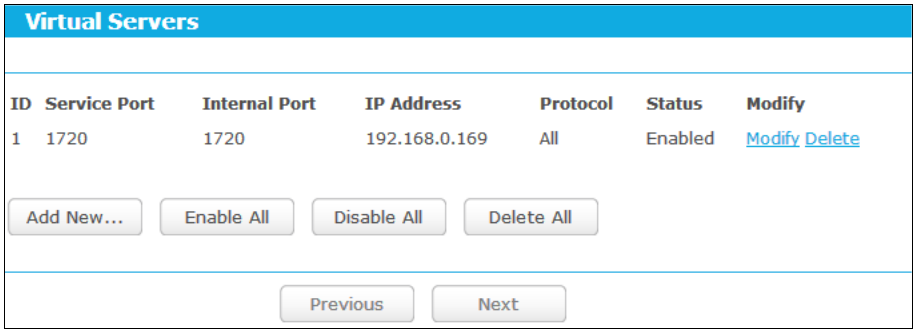


Figure A-4 Virtual Servers

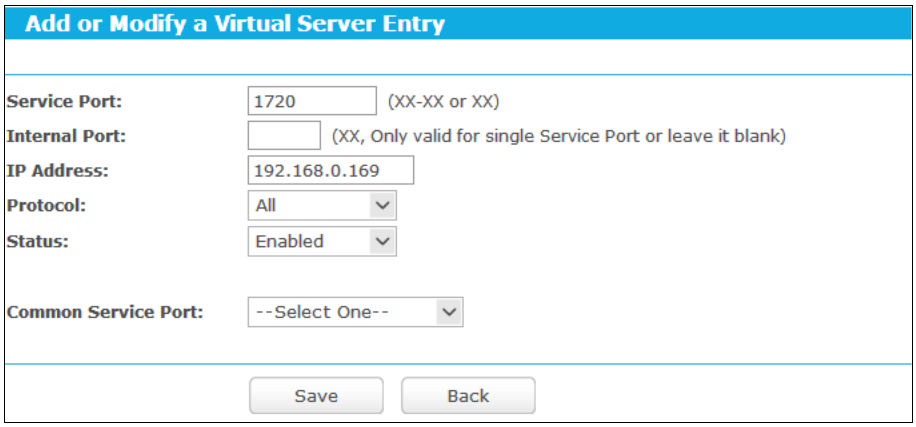


Figure A-5 Add or Modify a Virtual server Entry

Note:

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

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

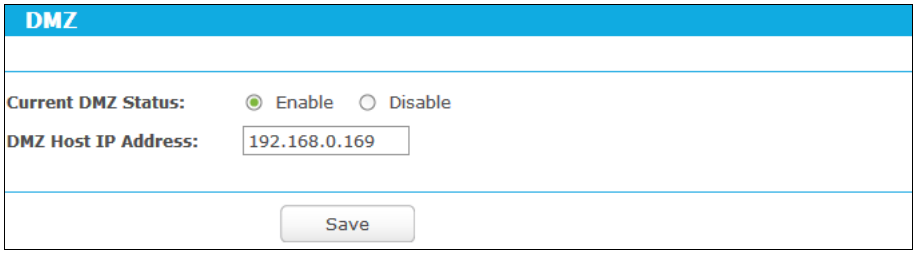


Figure A-6 DMZ

5) How to enable H323 ALG: Log in to the router, click the “**Security**” menu on the left of your browser, and click “**Basic Security**” submenu. On the “**Basic Security**” page, check the **Enable** radio button next to **H323 ALG**. Remember to click the **Save** button.

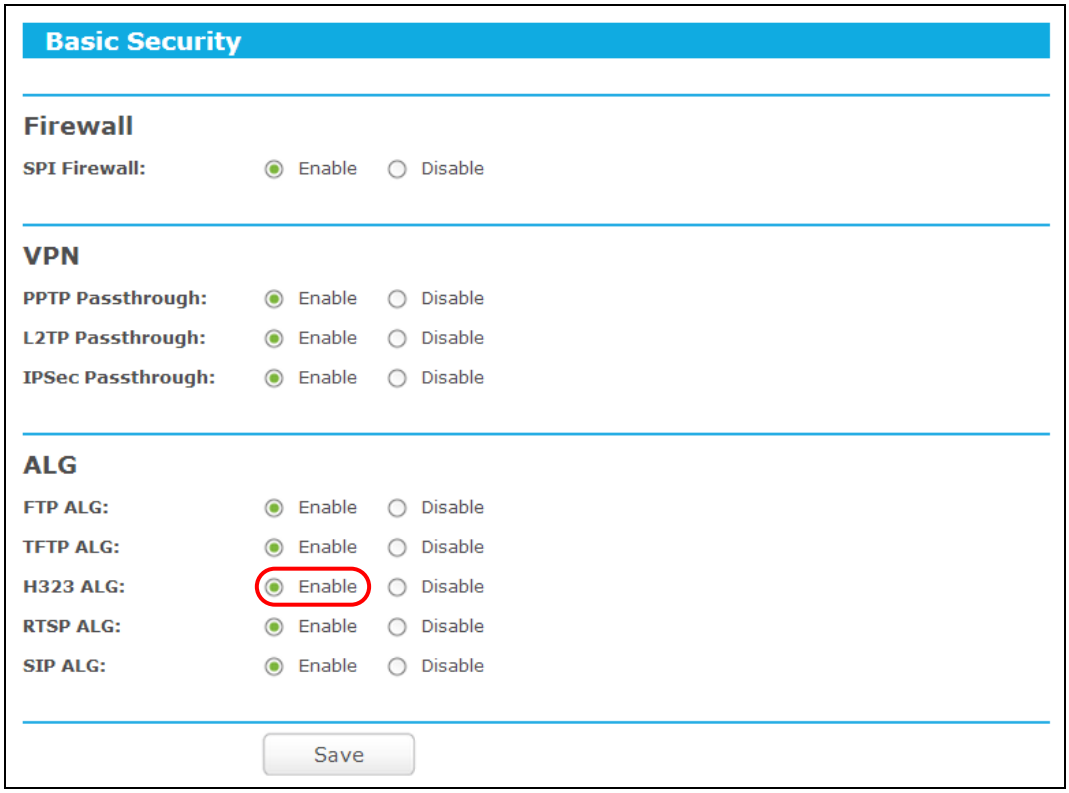


Figure A-7 Basic Security

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

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

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

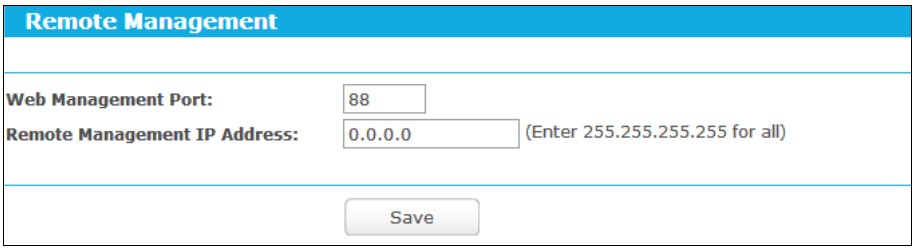


Figure A-8 Remote Management

Note:

If the above configuration takes effect, you can visit and configure the router by typing http://192.168.0.1:88 (the router's LAN IP address: Web Management Port) in the address field of the Web browser. If the LAN IP of the modem connected with your router is 192.168.0.x, the default LAN IP of the router will automatically switch from 192.168.0.1 to 192.168.1.1 to avoid IP conflict; in this case, please try http://192.168.1.1:88.

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

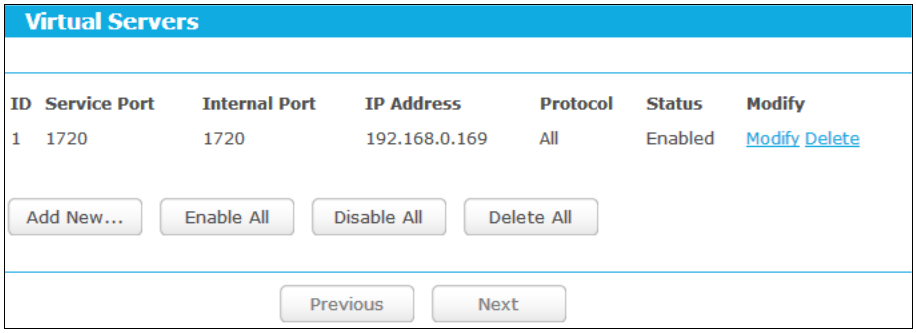


Figure A-9 Virtual Servers

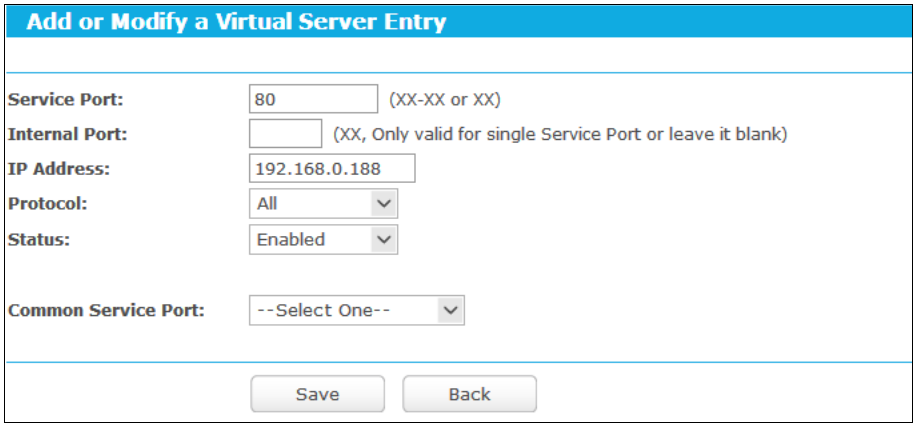


Figure A-10 Add or Modify a Virtual server Entry

5. The wireless stations cannot connect to the router.

1) Make sure the "**Wireless router Radio**" is enabled.

2) Make sure that the wireless stations' SSID accord with the router's SSID.

3) Make sure the wireless stations have right KEY for encryption when the router is encrypted.

4) If the wireless connection is ready, but you can’t access the router, check the IP Address of your wireless stations.

Appendix B: Configuring the PC

In this section, we'll introduce how to install and configure the TCP/IP correctly in Windows 7. First make sure your Ethernet Adapter is working, refer to the adapter's manual if needed.

1. Install TCP/IP component

1) On the Windows taskbar, click the **Start** button, and then click **Control Panel**.

2) Click the **Network and Internet**, and click the **Network and Sharing Center**, then click **Change adapter settings**.

3) Right click the icon that showed below, select **Properties** on the prompt page.

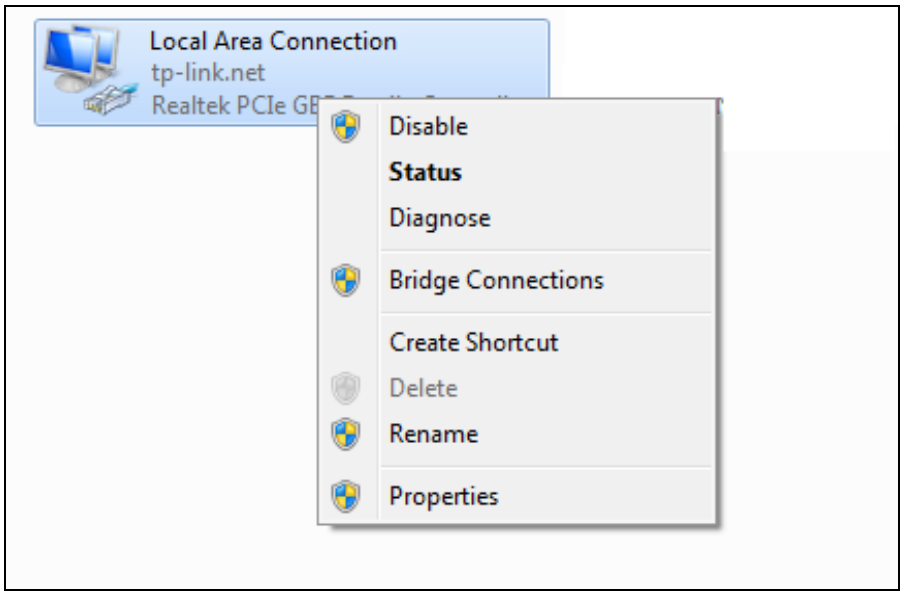


Figure B-1

4) In the prompt page that showed below, double click on the **Internet Protocol Version 4 (TCP/IPv4)**.

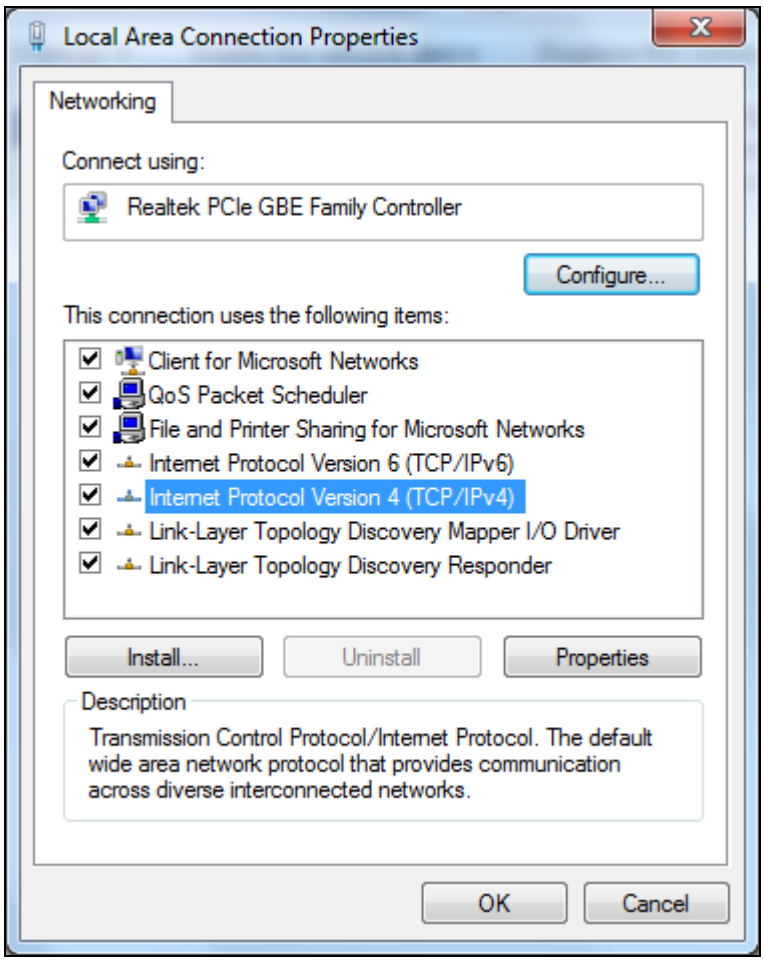


Figure B-2

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

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

➢ **Setting IP address automatically**

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

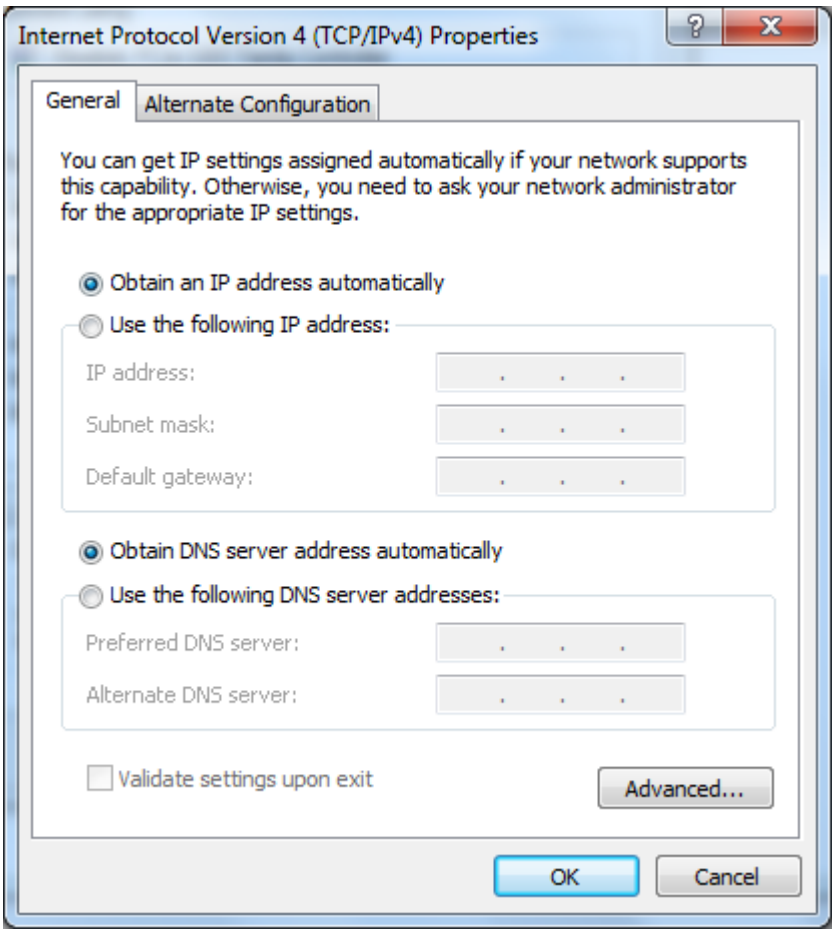


Figure B-3

➢ **Setting IP address manually**

1 Select **Use the following IP address** radio button. And the following items available

2 If the router's LAN IP address is 192.168.0.1, specify the IP address as 192.168.0.x (x is from 2 to 254), and **Subnet mask** is 255.255.255.0.

3 Type the router's LAN IP address (the default IP is 192.168.0.1) into the **Default gateway** field.

4 Select **Use the following DNS server addresses** radio button. In the **Preferred DNS Server** field you can type the DNS server IP address, which has been provided by your ISP

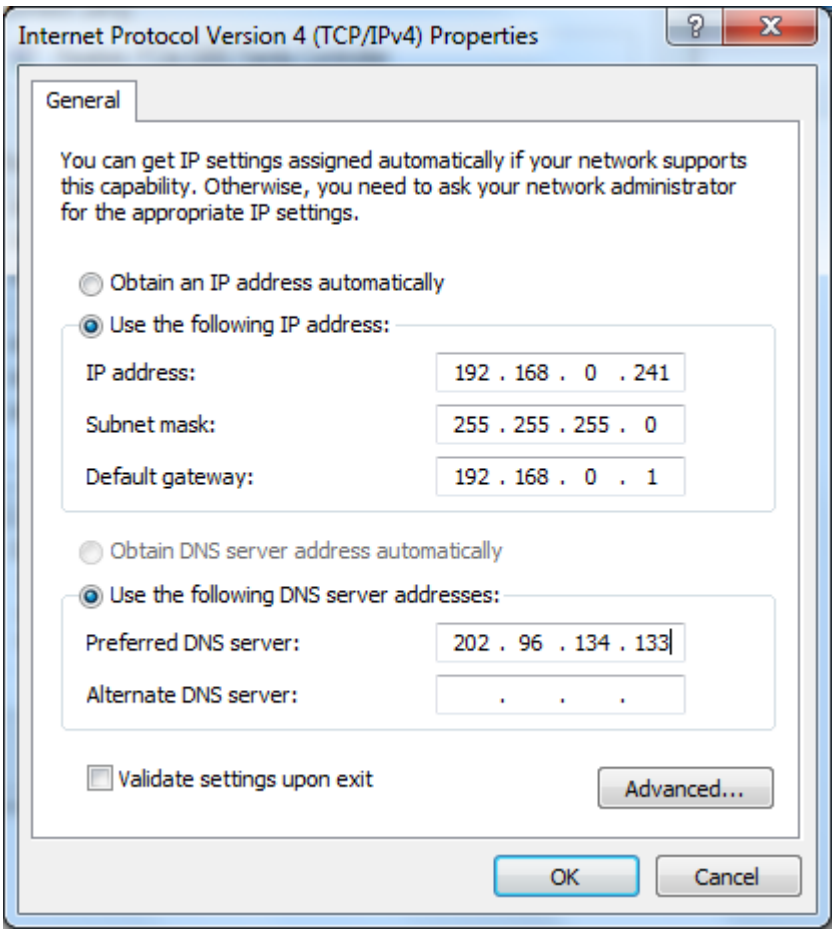

Internet Protocol Version 4 (TCP/IPv4) Properties
General
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.
Obtain an IP address automatically
Use the following IP address:
IP address: 192 . 168 . 0 . 241
Subnet mask: 255 . 255 . 255 . 0
Default gateway: 192 . 168 . 0 . 1
Obtain DNS server address automatically
Use the following DNS server addresses:
Preferred DNS server: 202 . 96 . 134 . 133
Alternate DNS server:
Validate settings upon exit
Advanced...
OK
Cancel

Figure B-4

Appendix C: Specifications

General	
Standards	IEEE 802.11n, IEEE 802.11b, IEEE 802.11g, IEEE 802.3, IEEE 802.3u, IEEE 802.1x, IEEE 802.11e, IEEE 802.11i, IEEE 802.3x
Protocols	TCP/IP, PPPoE, DHCP, ICMP, NAT, SNTP
Ports	One RJ45 WAN port, Four RJ45 LAN ports, One USB 2.0 WAN port (for 3G/4G network connection)
LEDs	(PWR), (SYS), (WLAN), (WAN）, (LAN1-4), (USB), (WPS)
Safety & Emissions	FCC, CE
Wireless	
Frequency Band	2.4~2.4835GHz
Radio Data Rate	11n：up to 300Mbps (Automatic) 11g：54/48/36/24/18/12/9/6M (Automatic) 11b：11/5.5/2/1M (Automatic)
Frequency Expansion	DSSS (Direct Sequence Spread Spectrum)
Modulation	DBPSK, DQPSK, CCK, OFDM, 16-QAM, 64-QAM
Security	WEP, WPA/WPA2-Enterprise, WPA/WPA2-Personal
Sensitivity @PER	130M: -68dBm@10% PER 108M: -68dBm@10% PER; 54M: -68dBm@10% PER 11M: -85dBm@8% PER; 6M: -88dBm@10% PER 1M: -90dBm@8% PER
Antenna Gain	5dBi
Environmental and Physical	
Temperature.	Operating : 0℃~40℃ (32℉~104℉) Storage: -40℃~70℃(-40℉~158℉)
Humidity	Operating: 10% ~ 90% RH, Non-condensing Storage: 5% ~ 90% RH, Non-condensing

Appendix D: Glossary

- **802.11n -** 802.11n builds upon previous 802.11 standards by adding MIMO (multiple-input multiple-output). MIMO uses multiple transmitter and receiver antennas to allow for increased data throughput via spatial multiplexing and increased range by exploiting the spatial diversity, perhaps through coding schemes like Alamouti coding. The Enhanced Wireless Consortium (EWC) [3] was formed to help accelerate the IEEE 802.11n development process and promote a technology specification for interoperability of next-generation wireless local area networking (WLAN) products.
- **802.11b -** The 802.11b standard specifies a wireless networking at 11 Mbps using direct-sequence spread-spectrum (DSSS) technology and operating in the unlicensed radio spectrum at 2.4GHz, and WEP encryption for security. 802.11b networks are also referred to as Wi-Fi networks.
- **802.11g -** specification for wireless networking at 54 Mbps using direct-sequence spread-spectrum (DSSS) technology, using OFDM modulation and operating in the unlicensed radio spectrum at 2.4GHz, and backward compatibility with IEEE 802.11b devices, and WEP encryption for security.
- **DDNS** (**D**ynamic **D**omain **N**ame **S**ystem) **-** The capability of assigning a fixed host and domain name to a dynamic Internet IP Address.
- **DHCP** (**D**ynamic **H**ost **C**onfiguration **P**rotocol) **-** A protocol that automatically configure the TCP/IP parameters for the all the PC(s) that are connected to a DHCP server.
- **DMZ** (**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

shared key algorithm, as described in the IEEE 802.11 standard.

- **Wi-Fi -** A trade name for the 802.11b wireless networking standard, given by the Wireless Ethernet Compatibility Alliance (WECA, see http://www.wi-fi.net), an industry standards group promoting interoperability among 802.11b devices.
- **WLAN** (**W**ireless **L**ocal **A**rea **N**etwork) **-** A group of computers and associated devices communicate with each other wirelessly, which network serving users are limited in a local area.

Appendix E: Compatible 3G/4G USB Modem

The UMTS/HSPA/EVDO USB modems we've tested in the field are listed below. You can find the latest compatibility list in our website: http://www.tp-link.com.

Compatible 3G/4G USB Modem (Tested in the field)

HUAWEI	E398(4G), E392(4G), EC1261-2, E173, E1752, E180, E176G, E1820, E1556, E160, E153, E1750, E1762, E1552, EC122, E1550, E177, E220, E3715, E3765, E367u-2, E352, E353, E368
ZTE	MF820D(4G), AC2726i, AC2746, MF112, MF637, MF626, MF683, MF591, MF668, MF631, K3770-Z, MF180, K3565Z, MF110
NOVATEL	USB 551L(4G)
LG	VL600(4G)
SIERRA WIRELESS	Aircard 313U(4G)
PANTECH	UML290(4G)
ONDA	MDC835UP, MT833UP, MW833UP, MSA110UP
ALCATEL	X220S, X225S, X310E, X215S