AC750 Wireless Dual Band Gigabit Router

RNX-AC750RT

User Manual

REV1.0.0

1910020730

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."

The frequency band of 5150MHz – 5250MHz is required indoor users only.

CE Mark Warning

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

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
Bulgaria	None	General authorization required for outdoor use and public service
France	Outdoor use limited to 10 mW e.i.r.p. within the band 2454-2483.5 MHz	Military Radiolocation use. Refarming of the 2.4 GHz band has been ongoing in recent years to allow current relaxed regulation. Full implementation planned 2012
Italy	None	If used outside of own premises, general authorization is required
Luxembourg	None	General authorization required for network and service supply(not for spectrum)
Norway	Implemented	This subsection does not apply for the geographical area within a radius of 20 km from the centre of Ny-Ålesund
Russian Federation	None	Only for indoor applications

Note: Please don’t use the product outdoors in France.

CONTENTS

Package Contents **1**

Chapter 1. Introduction **2**

1.1 Overview of the Router 2

1.2 Conventions 3

1.3 Main Features 3

1.4 Panel Layout 4

1.4.1 The Front Panel 4

1.4.2 The Rear Panel 5

Chapter 2. Connecting the router **7**

2.1 System Requirements 7

2.2 Installation Environment Requirements 7

2.3 Connecting the Router 7

Chapter 3. Quick Installation Guide **9**

3.1 TCP/IP Configuration 9

3.2 Quick Installation Guide 10

Chapter 4. Configuring the router **22**

4.1 Login 22

4.2 Status 22

4.3 Quick Setup 24

4.4 Network 24

4.4.1 WAN 24

4.4.2 LAN 35

4.4.3 MAC Clone 35

4.5 Dual Band Selection 36

4.6 Wireless 2.4GHz 37

4.6.1 Basic Settings 37

4.6.2 WPS 40

4.6.3 Wireless Security 42

4.6.4 Wireless MAC Filtering 46

4.6.5 Wireless Advanced 48

4.6.6 Wireless Statistics 49

4.7 Wireless 5GHz 50

4.7.1 Basic Settings 50
4.7.2 WPS 53
4.7.3 Wireless Security 55
4.7.4 Wireless MAC Filtering 59
4.7.5 Wireless Advanced 61
4.7.6 Wireless Statistics 62
4.8 Guest Network 63
4.9 DHCP 65
4.9.1 DHCP Settings 65
4.9.2 DHCP Clients List 67
4.9.3 Address Reservation 67
4.10 USB Settings 68
4.10.1 USB Mass Storage 69
4.10.2 User Accounts 69
4.10.3 Storage Sharing 71
4.10.4 FTP Server 73
4.10.5 Media Server 74
4.11 NAT 76
4.12 Forwarding 77
4.12.1 Virtual Server 77
4.12.2 Port Triggering 79
4.12.3 DMZ 81
4.12.4 UPnP 82
4.13 Security 83
4.13.1 Basic Security 83
4.13.2 Advanced Security 85
4.13.3 Local Management 86
4.13.4 Remote Management 87
4.14 Parent Control 88
4.15 Access Control 92
4.15.1 Rule 92
4.15.2 Host 94
4.15.3 Target 96
4.15.4 Schedule 99
4.16 Advanced Routing 100
4.16.1 Static Route List 101

4.16.2 System Routing Table 102
4.17 Bandwidth Control 103
4.18 IP & MAC Binding 104
4.18.1 Binding Settings 104
4.18.2 ARP List 106
4.19 Dynamic DNS 106
4.19.1 No-ip.com DDNS 107
4.19.2 Comexe.cn DDNS 107
4.19.3 Dyndns.com DDNS 108
4.20 IPv6 109
4.20.1 IPv6 Status 110
4.20.2 IPv6 WAN 111
4.20.3 IPv6 LAN 115
4.21 System Tools 116
4.21.1 Time Settings 116
4.21.2 Diagnostic 118
4.21.3 Firmware Upgrade 120
4.21.4 Factory Defaults 120
4.21.5 Backup & Restore 121
4.21.6 Reboot 122
4.21.7 Password 122
4.21.8 System Log 123
4.21.9 Statistics 123
4.22 Logout 126
Appendix A: FAQ 127
Appendix B: Configuring the PC 131
Appendix C: Specifications 133
Appendix D: Glossary 134

Package Contents

The following items should be found in your package:

- RNX-AC750RT AC750 Wireless Dual Band Gigabit Router
- DC Power Adapter for RNX-AC750RT AC750 Wireless Dual Band Gigabit Router
- Quick Installation Guide
- Resource CD for RNX-AC750RT AC750 Wireless Dual Band Gigabit Router, including:
  - This Guide
  - Other Helpful Information

☞ **Note:**

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

Chapter 1. Introduction

1.1 Overview of the Router

The RNX-AC750RT AC750 Wireless Dual Band Gigabit Router integrates 4-port Switch, Firewall, NAT-router and Wireless AP. The AC750 Wireless Dual Band Gigabit Router delivers exceptional range and speed, which can fully meet the need of Small Office/Home Office (SOHO) networks and the users demanding higher networking performance. Your wireless connections are radio band selectable to avoid interference in your area, and the four built-in Gigabit ports supply high-speed connection to your wired devices.

Incredible Speed

The RNX-AC750RT AC750 Wireless Dual Band Gigabit Router provides up to 750Mbps wireless connection with other wireless clients. The incredible speed makes it ideal for handling multiple data streams at the same time, which ensures your network stable and smooth. The performance of this 802.11ac wireless router will give you the unexpected networking experience at speed much faster than 802.11n. It is also compatible with all IEEE 802.11n, IEEE 802.11a, IEEE 802.11b and IEEE 802.11g products.

Multiple Security Protections

With multiple protection measures, including SSID broadcast control and wireless LAN 64/128-bit WEP encryption, Wi-Fi Protected Access (WPA2- PSK, WPA- PSK), as well as advanced Firewall protections, the RNX-AC750RT AC750 Wireless Dual Band Gigabit Router provides complete data privacy.

Flexible Access Control

The RNX-AC750RT AC750 Wireless Dual Band Gigabit Router provides flexible access control, so that parents or network administrators can establish restricted access policies for children or staff. It also supports Virtual Server and DMZ host for Port Triggering, and then the network administrators can manage and monitor the network in real time with the remote management function.

Simple Installation

Since the router is compatible with virtually all the major operating systems, it is very easy to manage. Quick Setup Wizard is supported and detailed instructions are provided step by step in this user guide. Before installing the router, please look through this guide to know all the router's functions.

1.2 Conventions

The router or RNX-AC750RT mentioned in this guide stands for RNX-AC750RT AC750 Wireless Dual Band Gigabit Router without any explanation.

1.3 Main Features

- Complies with IEEE 802.11ac.
- One 10/100/1000M Auto-Negotiation RJ45 WAN port, four 10/100/1000M Auto-Negotiation RJ45 LAN ports, supporting Auto MDI/MDIX.
- Provides USB ports supporting storage/FTP/Media.
- Provides WPA/WPA2, WPA-PSK/WPA2-PSK authentication, TKIP/AES encryption security.
- Shares data and Internet access for users, supporting Dynamic IP/ Static IP/ PPPoE/ PPTP/ L2TP/ BigPond Internet access.
- Supports simultaneous 2.4GHz and 5GHz connections for 750Mbps of total available bandwidth.
- 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.
- Supports Parent Control and Access Control.
- 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 LEDs on the front panel

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

Name	Status	Indication
(Power)	Off	Power is off.
	On	Power is on.
(Wireless)	Off	The wireless function is disabled.
	On	The wireless function is enabled. The router is working on 2.4GHz or 5GHz or both radio band.
(Ethernet)	Off	No device is connected to the LAN ports.
	On	At least one device has connected to the LAN ports.
(Internet)	Off	The Internet connection is not available.
	On	The network is available with a successful Internet connection.
(USB)	Off	No storage device is plugged into the USB port.
	Flashing	A plugged-in storage device is being recognized.
	On	The storage device has been successfully recognized.
(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:**

1. 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.
2. The router is set to work concurrently in 2.4GHz and 5GHz by default. If you desire to choose the working frequency, please go to 4.5 Dual Band Selection.

1.4.2 The Rear Panel

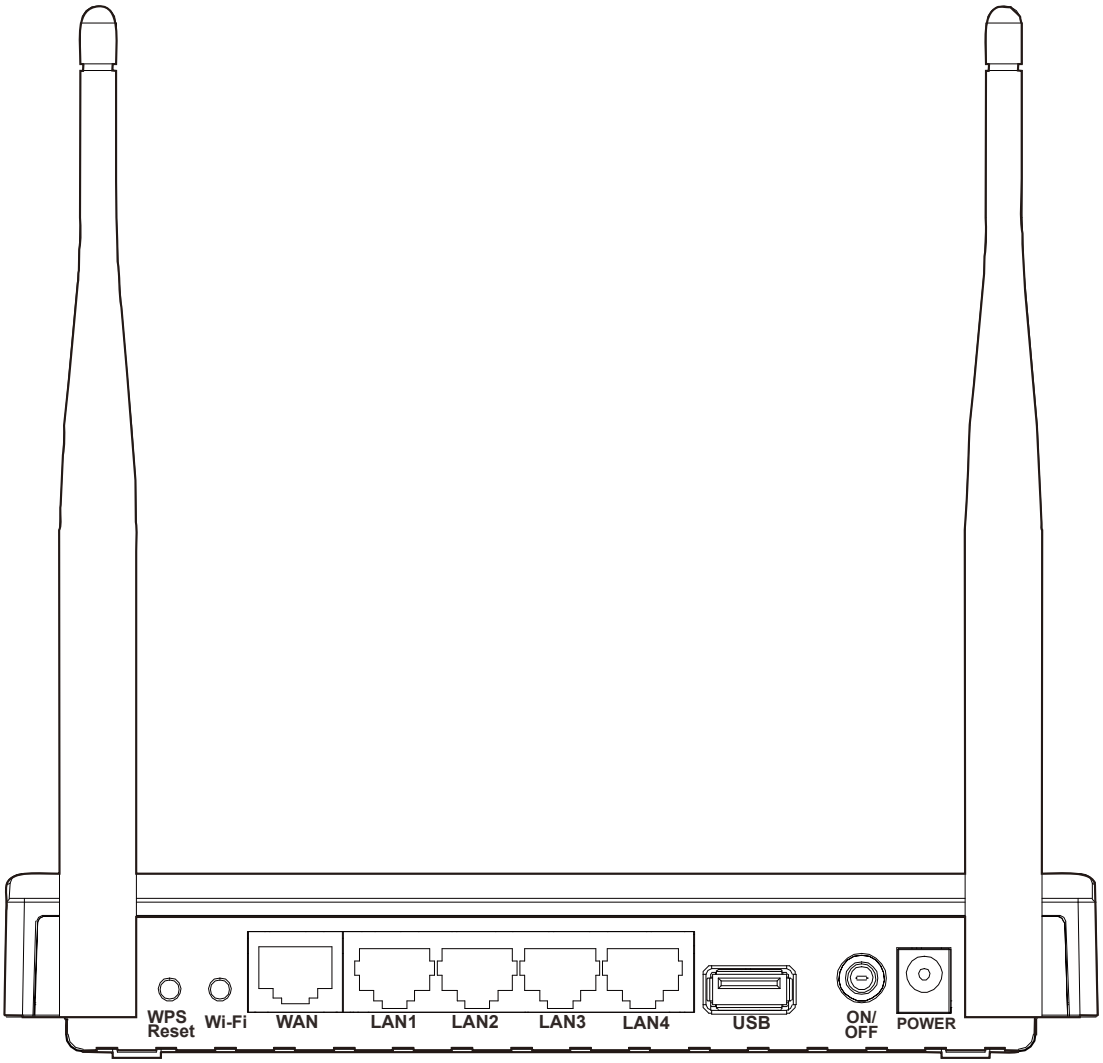


Figure 1-2 Rear Panel sketch

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

- **WPS/Reset:**

  Pressing this button for less than 5 seconds enables the WPS function. If your client devices, such as wireless adapters, support Wi-Fi Protected Setup, then you can press this button to quickly establish a connection between the router and client devices and automatically configure wireless security for your wireless network.

  Pressing this button for more than 5 seconds enables the Reset function. With the router powered on, press and hold the **WPS/Reset** button (approximately 8 seconds) until all LEDs are lit. And then release the button and wait for the router to reboot to its factory default settings.

- **Wi-Fi:** The button for turning on/off the wireless function.
- **WAN:** This port is where you will connect the DSL/cable Modem, or Ethernet.

- **LAN (1, 2, 3, 4):** These ports (1, 2, 3, 4) connect the router to the local PC(s).
- **USB:** The USB port connects to a USB storage device.
- **ON/OFF:** The switch for the power.
- **POWER:** The Power socket is where you will connect the power adapter. Please use the power adapter provided with this RNX-AC750RT AC750 Wireless Dual Band Gigabit Router.
- **Wireless antenna:** To receive and transmit the wireless data.

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, Mozilla Firefox or Apple Safari

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 modem (if the modem has a backup battery, please remove it too.), and disconnect your existing router if you have one.
2. Connect the **WAN** port on your router to the modem's LAN port with an Ethernet cable.
3. Connect your computer to one of the **LAN** ports labeled 1~4 on the router with an Ethernet cable.
4. Power on the modem and wait for 2 minutes.
5. Then plug the provided power adapter into the **POWER** jack and the other end to a standard electrical wall socket. Press the **ON/OFF** button to power on the router. (Before you power on

the router, please make sure your computer is NOT connected to any other wireless network.)

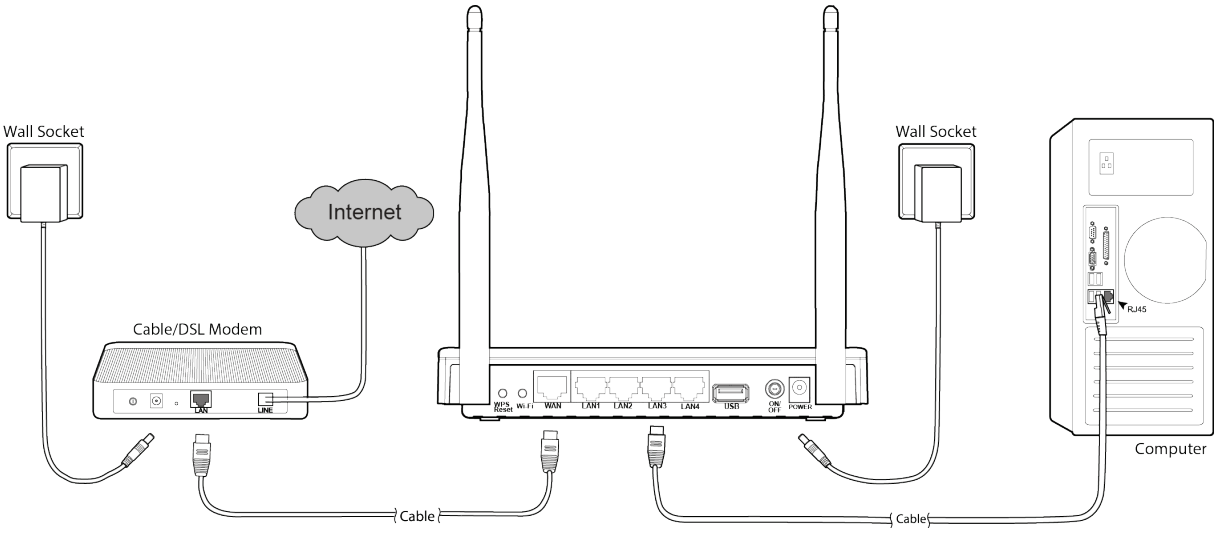


Figure 2-1 Hardware Installation

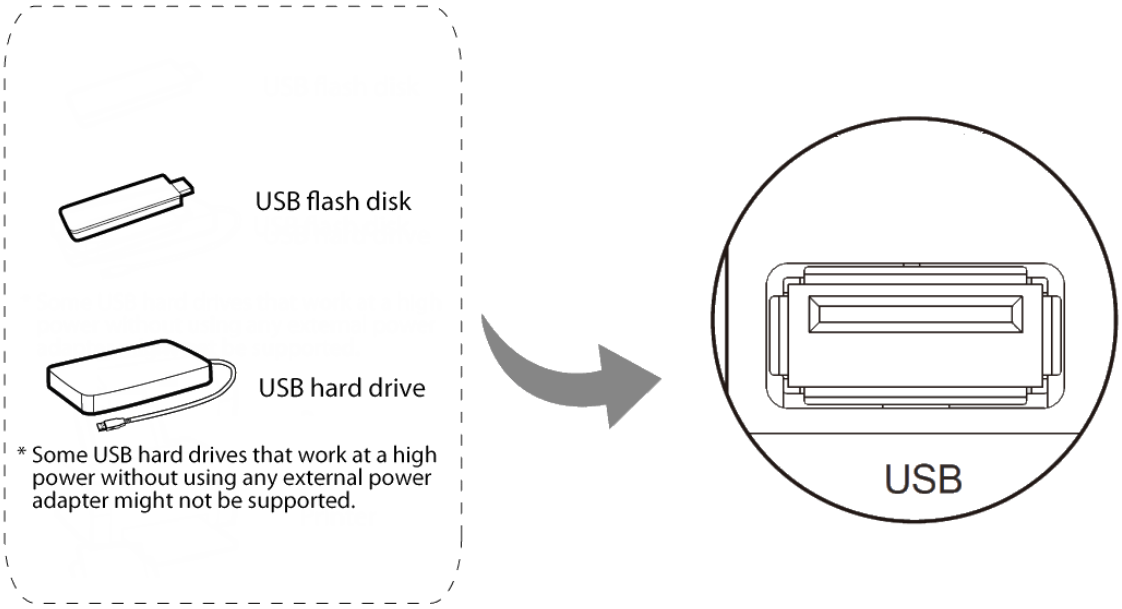


Figure 2-2 USB Installation

Note:

If you want to use the router to share files, plug the USB storage device to the USB port.

Chapter 3. Quick Installation Guide

This chapter will show you how to configure the basic functions of your AC750 Wireless Dual Band Gigabit Router using **Quick Setup Wizard** within minutes.

3.1 TCP/IP Configuration

The default IP address of the router is **192.168.1.1** 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 by the following method: 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. Then the built-in DHCP server will assign IP address for the PC.

Now, you can run the Ping command in the **command prompt** to verify the network connection between your PC and the router. The following example is in Windows XP OS.

Open a command prompt, and type *ping 192.168.1.1*, and then press **Enter**.

- If the result displayed is similar to the Figure 3-1, it means the connection between your PC and the router has been established well.

```
Pinging 192.168.1.1 with 32 bytes of data:

Reply from 192.168.1.1: bytes=32 time<1ms TTL=64
Reply from 192.168.1.1: bytes=32 time<1ms TTL=64
Reply from 192.168.1.1: bytes=32 time<1ms TTL=64
Reply from 192.168.1.1: bytes=32 time<1ms TTL=64

Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

Figure 3-1 Success result of Ping command

- If the result displayed is similar to Figure 3-2, it means the connection between your PC and the router failed.

```
Pinging 192.168.1.1 with 32 bytes of data:

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

Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

Figure 3-2 Failure result of Ping command

Please check the connection following these steps:

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

☞ **Note:**

The Ethernet LED on the router and LEDs on your PC's adapter should be lit.

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

☞ **Note:**

If the router's IP address is 192.168.1.1, your PC's IP address must be within the range of 192.168.1.2 ~ 192.168.1.254.

3. Is the default LAN IP of the router correct?

☞ **Note:**

If the LAN IP of the modem connected with your router is 192.168.1.x, the default LAN IP of the router will automatically switch from 192.168.1.1 to 192.168.0.1 to avoid IP conflict.

3.2 Quick Installation Guide

With a Web-based utility, it is easy to configure and manage the AC750 Wireless Dual Band Gigabit Router. The Web-based utility can be used on any Windows, Macintosh or UNIX OS with a Web browser, such as Microsoft Internet Explorer, Mozilla Firefox or Apple Safari.

1. To access the configuration utility, open a web-browser and type in the default IP address http:/192.168.1.1 in the address field.

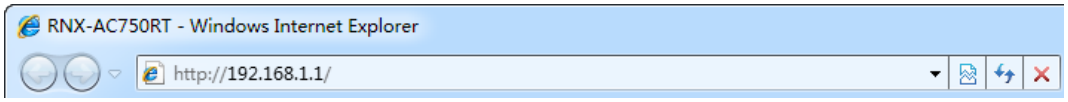


Figure 3-3 Log in the router

After a moment, a login window will appear, similar to Figure 3-4. Enter **admin** for the User Name and Password, both in lower case letters. Then click the **Login** button or press the **Enter** key.

Figure 3-4 Login Windows

☞ **Note:**

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

2. After successful login, the **Quick Setup** page will appear for you to quickly configure your router.

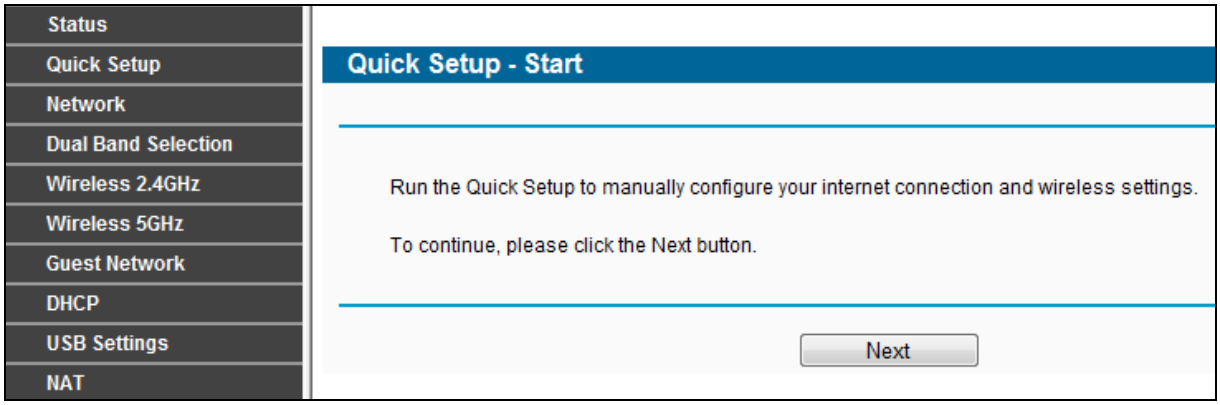


Figure 3-5 Quick Setup

3. Click **Next**, and then **WAN Connection Type** page will appear, shown in Figure 3-6.

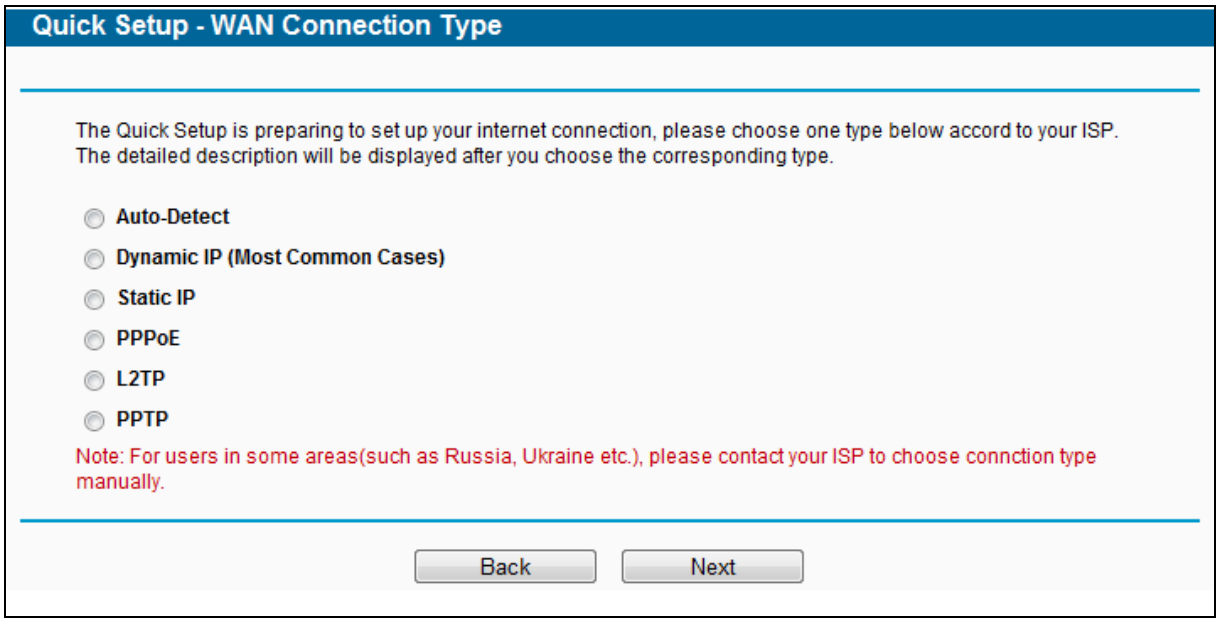


Figure 3-6 WAN Connection Type

The router provides **Auto-Detect** function and supports five types of WAN connection: **Dynamic IP**, **Static IP**, **PPPoE**, **L2TP**, and **PPTP**. It's recommended that you make use of the **Auto-Detect** function. If you are sure of what kind of connection type your ISP provides, you can select the very type and click **Next** to go on configuring.

4. If you select **Auto-Detect**, the router will automatically detect the connection type your ISP provides. Make sure the cable is securely plugged into the WAN port before detection. The appropriate configuration page will be displayed when an active Internet service is successfully detected by the router.

   ☞ **Note:**

   If Auto-Detect fails, you can select the connection type your ISP provides in Figure 3-6, and follow the configuring procedures below to continue.

   1) If the connection type detected is **Dynamic IP**, there will appear the MAC Clone page (as shown in Figure 3-7). In most cases, there is no need to clone the MAC address. You can select "**No, I do NOT need to clone MAC address**" and then click **Next**. If it is necessary in your case, please select "**Yes, I need to clone MAC address**" and then click **Next**.

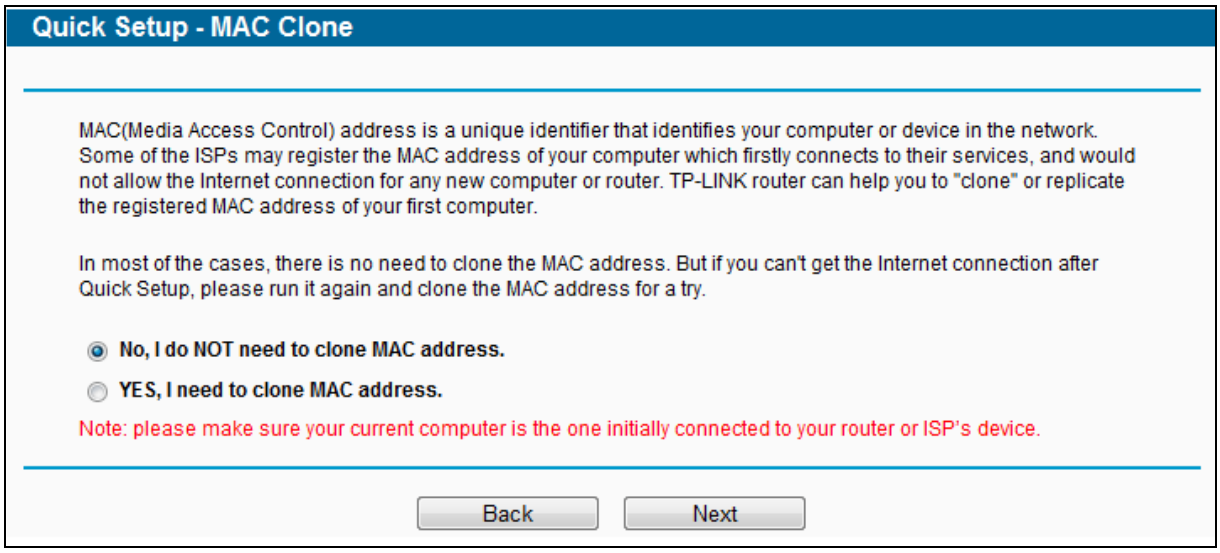


Figure 3-7 Quick Setup – MAC Clone

2) If the connection type detected is **Static IP**, the next screen will appear as shown in Figure 3-8. Configure the following parameters and then click **Next** to continue.

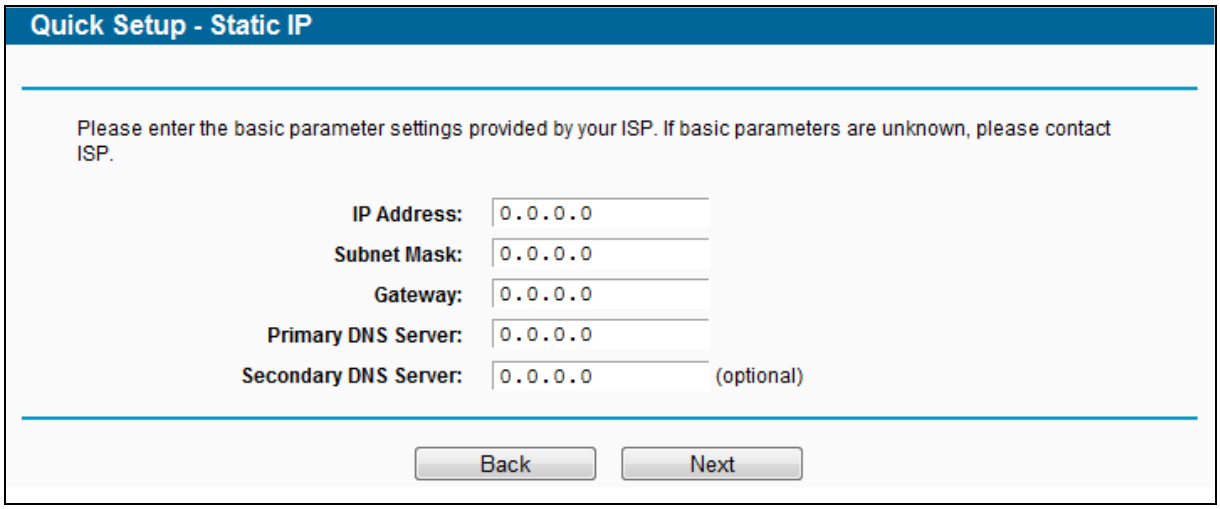


Figure 3-8 Quick Setup - Static IP

- **IP Address -** This is the WAN IP address as seen by external users on the Internet (including your ISP). Your ISP will provide you with the IP address you need to enter here. Enter the IP address into the field.
- **Subnet Mask -** The Subnet Mask is used for the WAN IP address. Your IPS will provide you with the subnet mask which is usually 255.255.255.0.
- **Gateway -** Your ISP will provide you with the Gateway address which is the ISP server's address. Enter the gateway IP address into the box if required.
- **DNS Server -** （Optional）Enter the DNS Server IP address into the box if required.

- **Secondary DNS Server-**（Optional） If your ISP provides another DNS server, enter it into this field.

3) If the connection type detected is **PPPoE**, the next screen will appear as shown in Figure 3-9. Configure the following parameters and then click **Next** to continue.

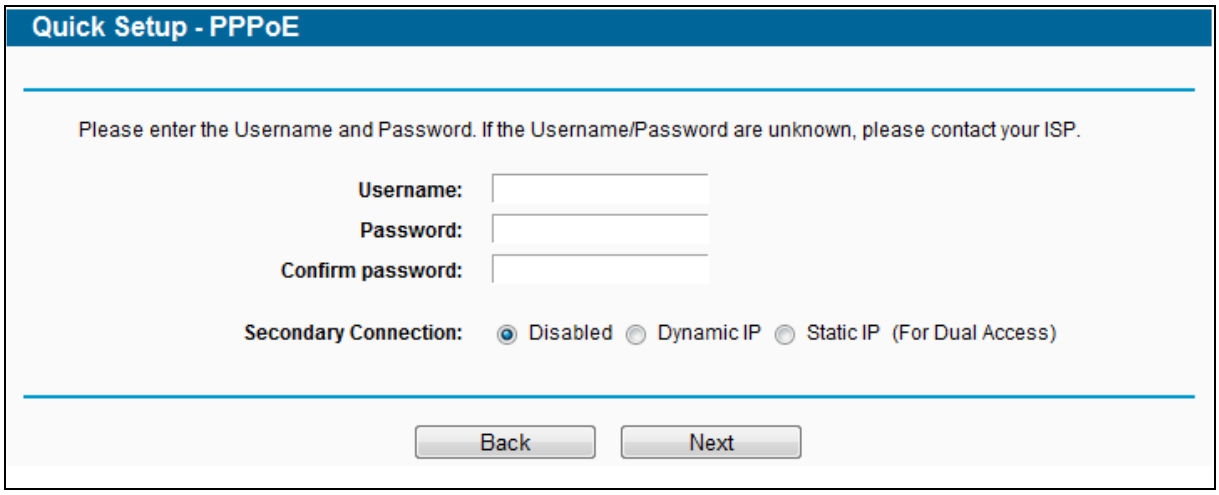


Figure 3-9 Quick Setup – PPPoE

- **User Name/Password -** Enter the **User Name** and **Password** provided by your ISP. These fields are case-sensitive. If you have difficulty with this process, please contact your ISP.
- **Confirm Password -** Enter the password again to make sure that the password is correct.

4) If your connection type is **L2TP**, select L2TP in Figure 3-6 and the next screen will appear as shown in Figure 3-10.Configure the following parameters and then click **Next** to continue.

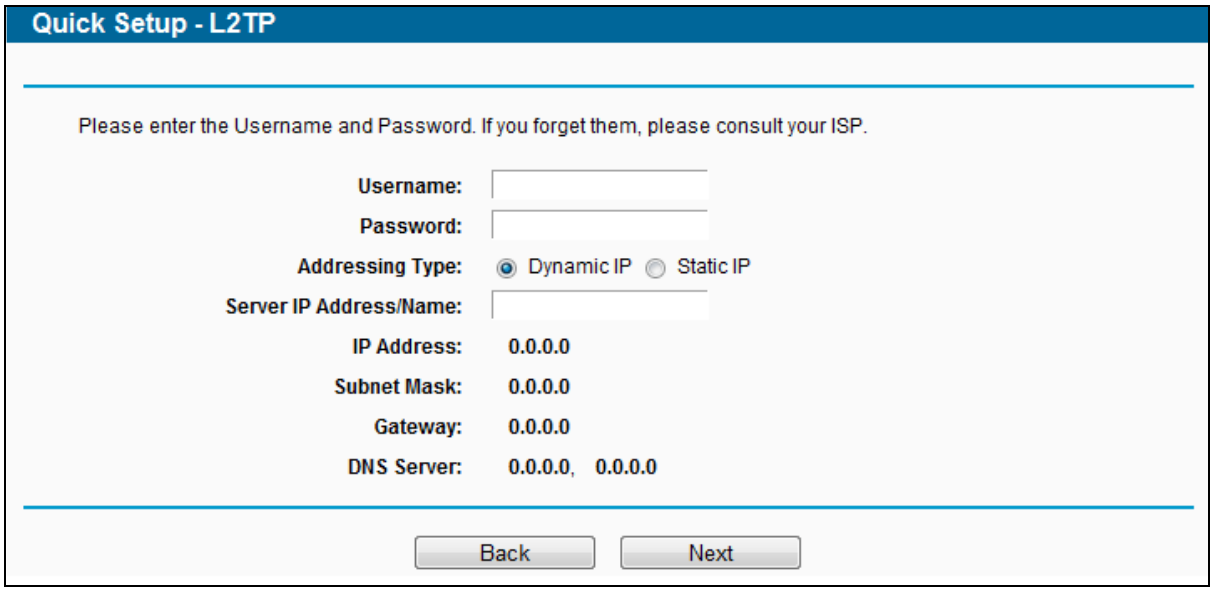
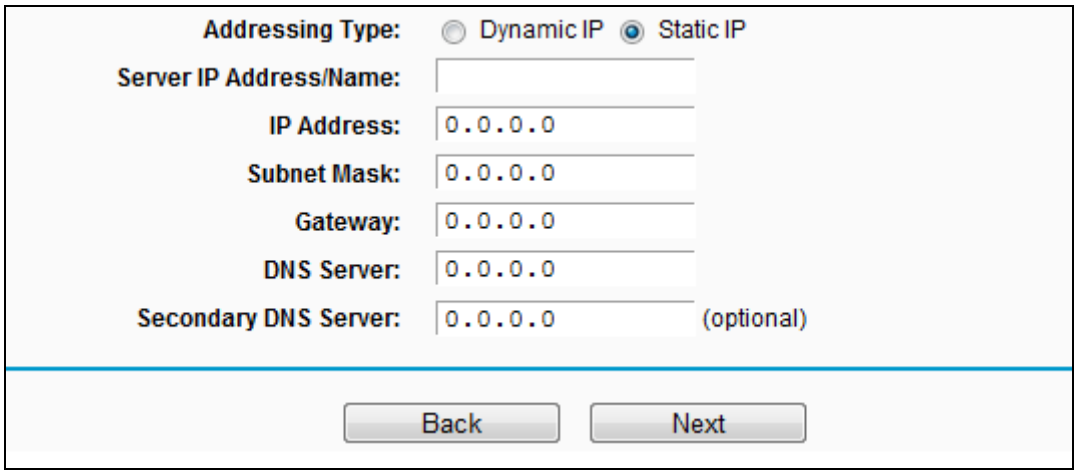


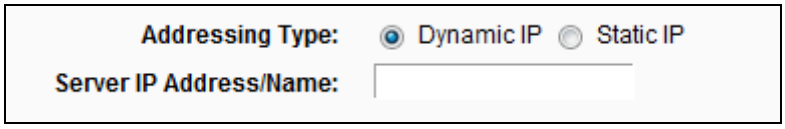
Figure 3-10 Quick Setup – L2TP

- **Username/Password -** Enter the **Username** and **Password** provided by your ISP. These fields are case-sensitive. If you have difficulty with this process, please contact your ISP.

Select **Static IP** if the IP Address/ Subnet Mask/ Gateway and DNS server address have been provided by your ISP. Then please enter server IP address or domain name provided by your ISP, and also enter the corresponding parameters.



Select **Dynamic IP** if none of the above parameters are provided. Then you just need to enter server IP address or domain name provided by your ISP.



5) If your connection type is **PPTP**, select PPTP in Figure 3-6 and the next screen will appear as shown in Figure 3-11. Configure the following parameters and then click **Next** to continue.

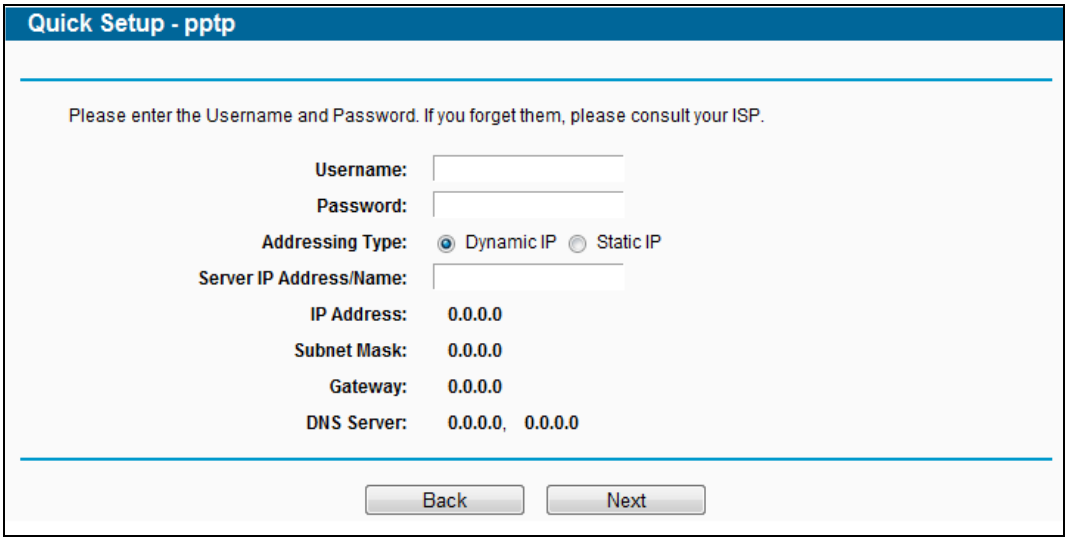
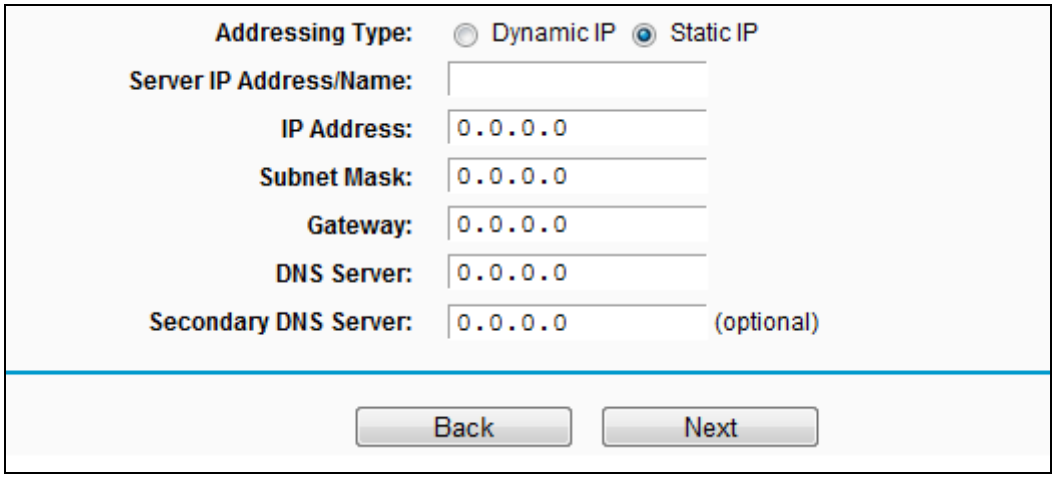


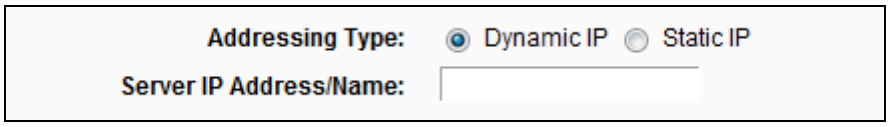
Figure 3-11 Quick Setup – PPTP

- **Username/Password -** Enter the **Username** and **Password** provided by your ISP. These fields are case-sensitive. If you have difficulty with this process, please contact your ISP.

Select **Static IP** if the IP Address/ Subnet Mask/ Gateway and DNS server address have been provided by your ISP. Then please enter server IP address or domain name provided by your ISP, and also enter the corresponding parameters.



Select **Dynamic IP** if none of the above parameters are provided. Then you just need to enter server IP address or domain name provided by your ISP.



5. After finishing the WAN Connection Type selection, the **Dual Band Selection** page will appear as shown in Figure 3-12. Here we take “2.4GHz and 5GHz” for example. Click **Next** to continue.

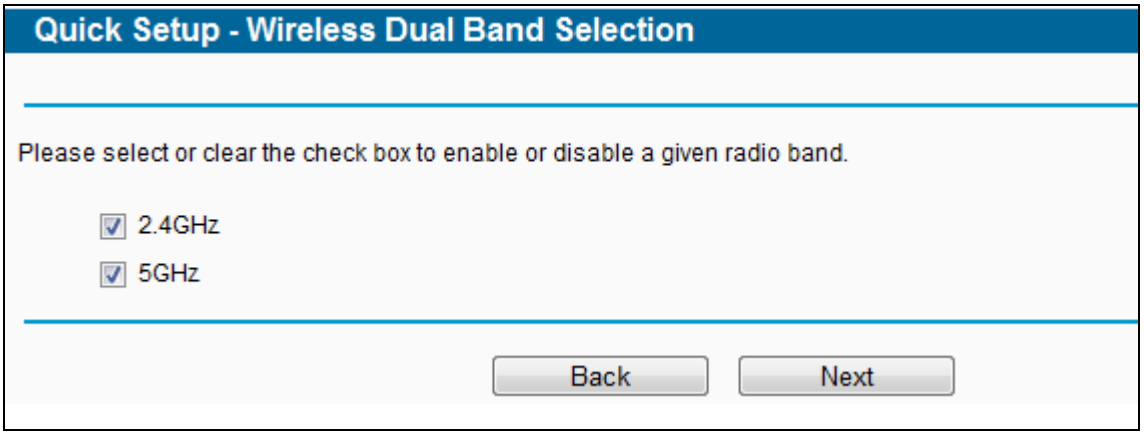


Figure 3-12 Quick Setup – Dual Band Selection

- **2.4GHz** - You can use the 2.4GHz band to connect to many classic wireless devices like gaming consoles, laptops, DVRs, etc.

- **5GHz** - This band is less crowded and is used for time-sensitive music, video streaming or gaming. Using this band can avoid interference with 2.4GHz networks or noisy devices like cordless phones and microwave ovens.

6. Configure the basic parameters for 2.4GHz wireless network in the following screen as shown in Figure 3-13, and then click **Next**.

Figure 3-13 Quick Setup – Wireless 2.4GHz

- **Wireless Network Name -** 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. The default SSID is set to be Rosewill_2.4GHz_XXXXXX. This value is case-sensitive. For example, *TEST* is NOT the same as *test*.

- **Region -** Select your region from the drop-down list. This field specifies the region where the wireless function of the router can be used. It may be illegal to use the wireless function of the router in a region other than one of those specified in this field. If your country or region is not listed, please contact your local government agency for assistance.

  ☞ **Note:**

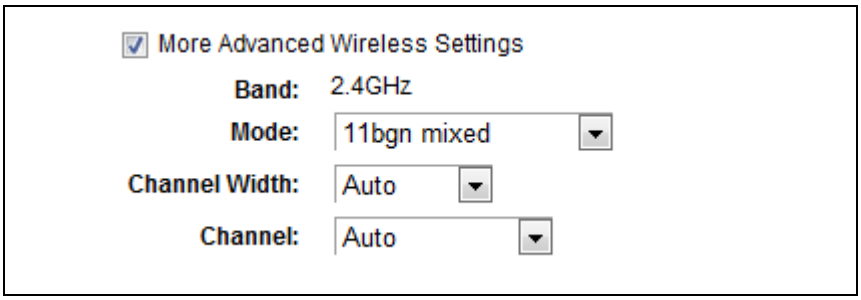
  Limited by local law regulations, version for North America does not have region selection option.

- **Security**

  - **Enable Security (WPA-PSK/WPA2-PSK) –** It's selected by default, with the default PSK password the same as the default PIN code.

- **Disable Wireless Security -** The wireless security function can be enabled or disabled. If disabled, the wireless stations will be able to connect the router without encryption.

The above settings are only for basic wireless parameters. For advanced settings, please check "**More Advanced Wireless Settings**", and then you can set the following parameters.



- **Band -** This field displayed the operating frequency being configured.
- **Mode -** This field determines the wireless mode which the router works on.
  - **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.
- **Channel Width -** Select any channel width from the drop-down list. The default setting is "Auto", which can adjust the channel width for your clients automatically.
- **Channel -** This field determines which operating frequency will be used. It is not necessary to change the wireless channel unless you notice interference problems with another nearby access point. If you select "Auto", then the AP will select the best channel automatically.

7. Configure the basic parameters for 5GHz wireless network in the following screen as shown in Figure 3-14, and then click **Next**.

Figure 3-14 Quick Setup – Wireless 5GHz

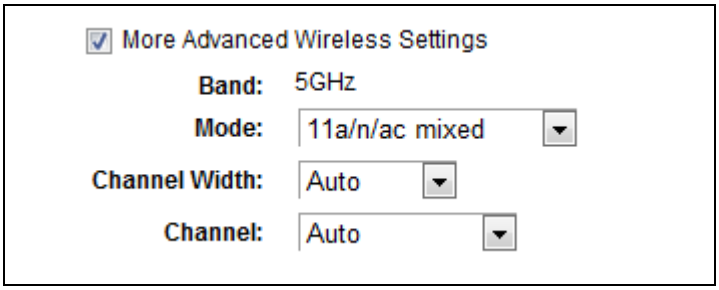
- **Wireless Network Name -** Also called the SSID (Service Set Identification). Enter a value of up to 32 characters. The same name must be assigned to all wireless devices in your network. The default SSID is set to be Rosewill_5GHz_XXXXXX. This value is case-sensitive. For example, *TEST* is NOT the same as *test*.
- **Region -** Select your region from the drop-down list. This field specifies the region where the wireless function of the router can be used. It may be illegal to use the wireless function of the router in a region other than one of those specified in this field. If your country or region is not listed, please contact your local government agency for assistance.

☞ **Note:**

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

- **Security**
  - **Enable Security (WPA-PSK/WPA2-PSK) –** It's selected by default, with the default PSK password the same as the default PIN code.
  - **Disable Security -** The wireless security function can be enabled or disabled. If disabled, the wireless stations will be able to connect the router without encryption.

The above settings are only for basic wireless parameters. For advanced settings, please check "**More Advanced Wireless Settings**", and then you can set the following parameters.



- **Band -** This field displayed the operating frequency being configured.
- **Mode -** This field determines the wireless mode which the router works on.
  - **11an mixed -** Select if you are using both 802.11a and 802.11n wireless clients.
  - **11a/n/ac mixed** – Select if you are using 802.11a, 802.11n and 802.11ac wireless clients.
- **Channel Width -** Select any channel width from the drop-down list. The default setting is “Auto”, which can adjust the channel width for your clients automatically.
- **Channel -** This field determines which operating frequency will be used. It is not necessary to change the wireless channel unless you notice interference problems with another nearby access point. If you select “Auto”, then the AP will select the best channel automatically.

8. Confirm the parameters and click the **Save** button to make the settings take effect.

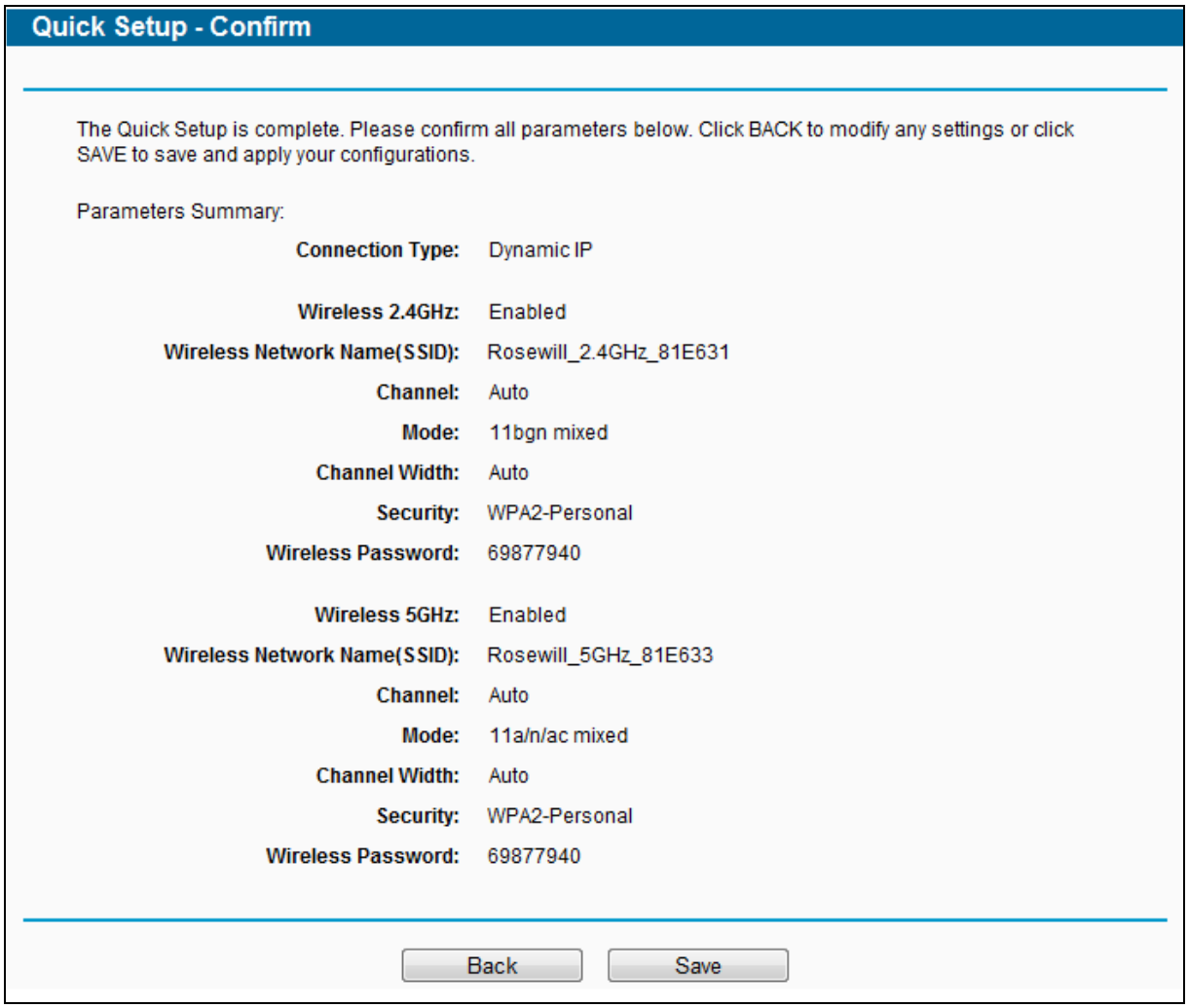


Figure 3-15 Quick Setup - Confirm

9. Click the **Finish** button to complete the **Quick Setup**.

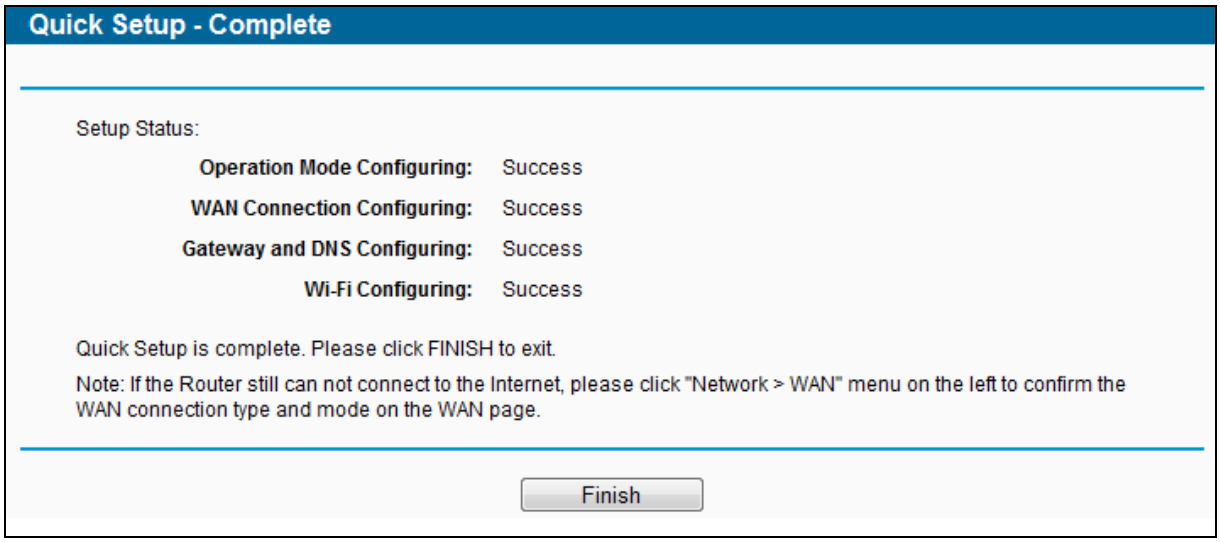


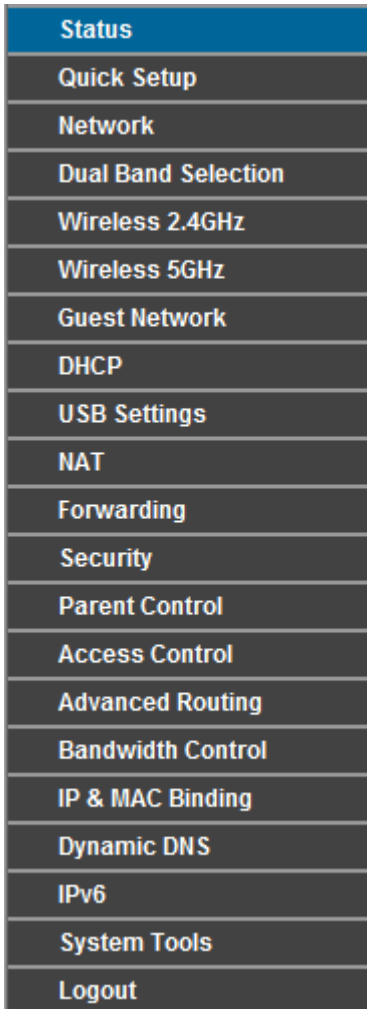
Figure 3-16 Quick Setup - Finish

Chapter 4. Configuring the router

This chapter will show each key function of the Web page and its configuration method.

4.1 Login

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



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

4.2 Status

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

Status

Firmware Version:	0.9.1 0.9 v0032.0 Build 140908 Rel.73720n
Hardware Version:	RNX-AC750RT v1 00000000

LAN

MAC Address:	E8:DE:27:81:E6:31
IP Address:	192.168.1.1
Subnet Mask:	255.255.255.0

Wireless 2.4GHz

Wireless Radio:	Enabled
Name(SSID):	Rosewill_2.4GHz_81E631
Mode:	11bgn mixed
Channel:	Auto(Channel 11)
Channel Width:	Auto
MAC Address:	E8:DE:27:81:E6:31
WDS Status:	Disabled

Wireless 5GHz

Wireless Radio:	Enabled
Name(SSID):	Rosewill_5GHz_81E633
Mode:	11a/n/ac mixed
Channel:	Auto(Channel 40)
Channel Width:	Auto
MAC Address:	E8:DE:27:81:E6:33
WDS Status:	Disabled

WAN

MAC Address:	E8:DE:27:81:E6:32
IP Address:	0.0.0.0(Dynamic IP)
Subnet Mask:	0.0.0.0
Default Gateway:	0.0.0.0
DNS Server:	0.0.0.0 0.0.0.0

System Up Time: 0 day(s) 00:54:44 [Refresh]

Figure 4-1 Status

4.3 Quick Setup

Please refer to 3.2 Quick Installation Guide.

4.4 Network

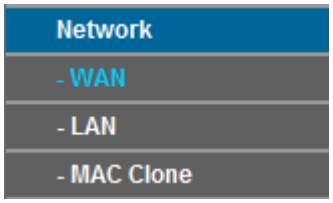


Figure 4-2 the Network menu

There are three submenus under the Network menu (shown in Figure 4-2): **WAN**, **LAN** and **MAC Clone**. Click any of them, and you will be able to configure the corresponding function.

4.4.1 WAN

Choose menu "**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 as follows (Figure 4-3):

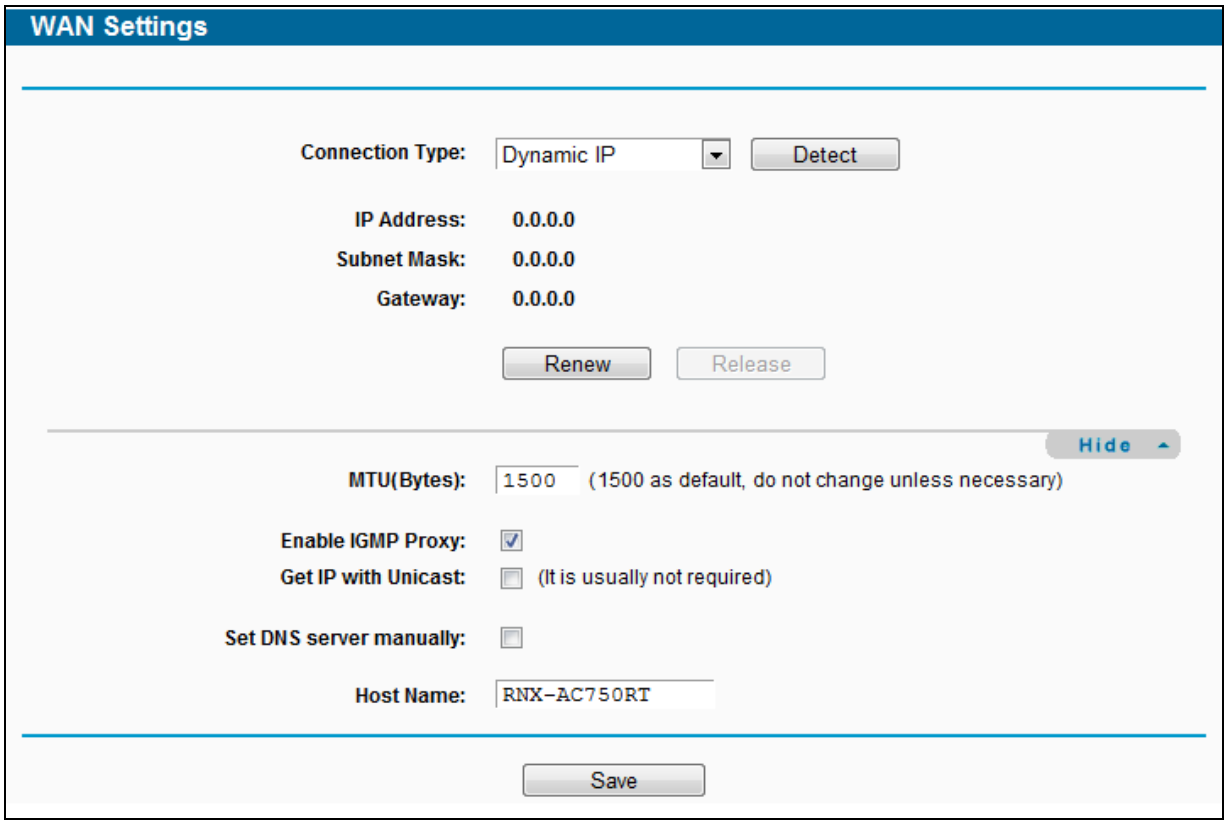


Figure 4-3 WAN – Dynamic IP

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.

If you want to do some advanced configurations, please click the **Advanced** button.

- **MTU(Bytes) -** 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.
- **Enable IGMP Proxy -** IGMP (Internet Group Management Protocol) is used to manage multicasting on TCP/IP networks. Some ISPs use IGMP to perform remote configuration for client devices, such as the modem router. The default value is enabled, and if you are not sure, please contact your ISP or just leave it.
- **Get IP with Unicast -** 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.)
- **Set DNS server manually -** If your ISP gives you one or two DNS addresses, select **Set DNS server manually** and enter the primary and secondary addresses into the correct fields. Otherwise, the DNS servers will be assigned automatically 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.

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 4-4.

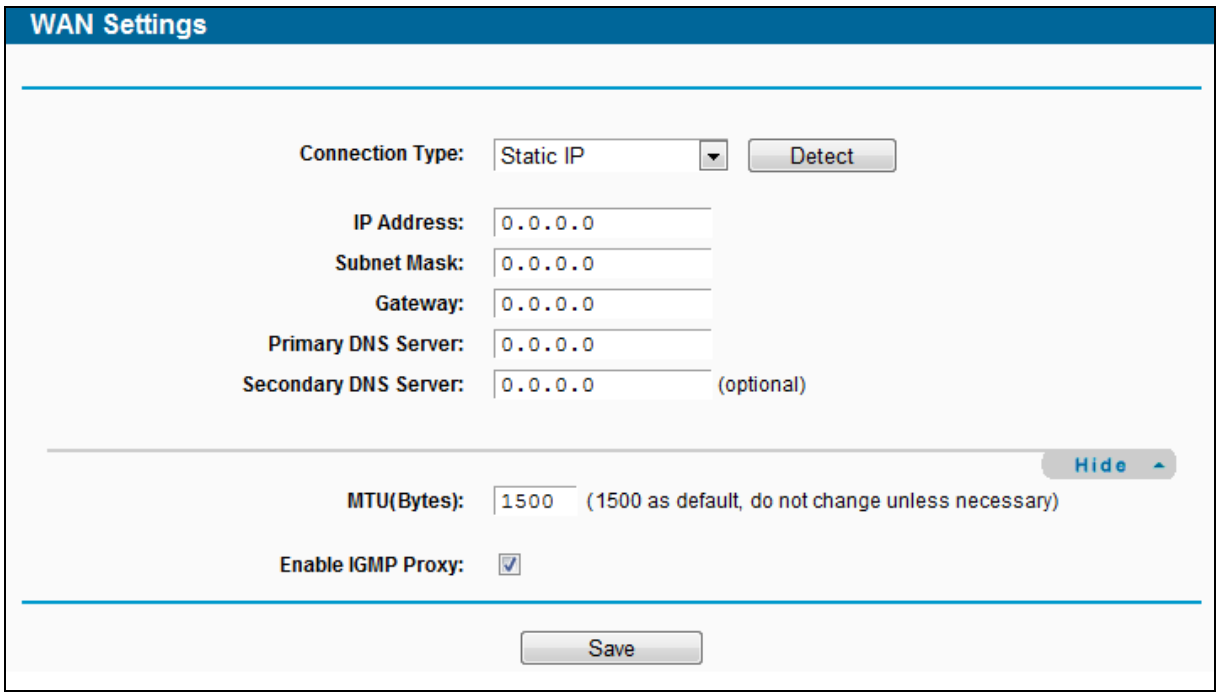


Figure 4-4 WAN - Static IP

- **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.
- **Gateway -** (Optional) Enter the gateway IP address in dotted-decimal notation provided by your ISP.
- **Primary DNS Server/Secondary DNS Server-** (Optional) Enter one or two DNS addresses in dotted-decimal notation provided by your ISP.
- **MTU (Bytes)-** 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.
- **Enable IGMP Proxy -** IGMP (Internet Group Management Protocol) is used to manage multicasting on TCP/IP networks. Some ISPs use IGMP to perform remote configuration for client devices, such as the modem router. The default value is enabled, and if you are not sure, please contact your ISP or just leave it.

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

3. If your ISP provides a PPPoE connection, select **PPPoE** option. And you should enter the following parameters (Figure 4-5):

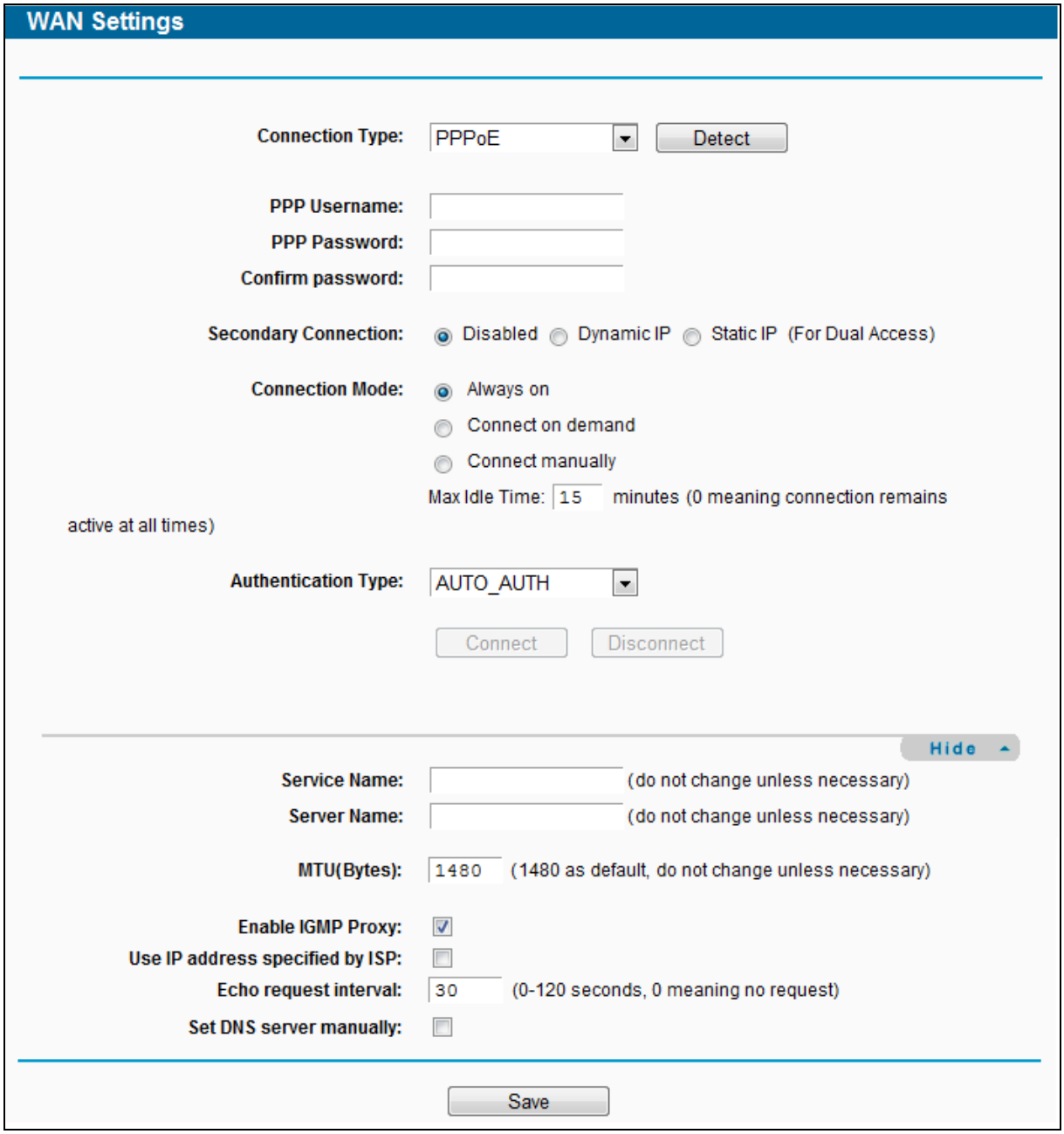


Figure 4-5 WAN - PPPoE

- **PPP Username/PPP 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.

➢ **Connection Mode-**choose the Internet connection mode.

- **Always on -** In this mode, the Internet connection will be active all the time.
- **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 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.

➢ **Service Name/Server Name -** The service name and server name should not be configured unless you are sure it is necessary for your ISP. In most cases, leaving these fields blank will work.

➢ **MTU(Bytes) -** 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.

➢ **Enable IGMP Proxy -** IGMP (Internet Group Management Protocol) is used to manage multicasting on TCP/IP networks. Some ISPs use IGMP to perform remote configuration for client devices, such as the modem router. The default value is enabled, and if you are not sure, please contact your ISP or just leave it.

➢ **Use IP address specified by ISP: -** 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.

➢ **Echo request interval -** The router will detect Access Concentrator online at every interval. The default value is "0". You can input the value between "0" and "120". The value "0" means no detect.

- **DNS/Secondary DNS -** If your ISP does not automatically assign DNS addresses to the router during login, please click "**Set DNS server manually**" check box and enter the IP address of your ISP's primary DNS server. If a secondary DNS server address is available, enter it as well.

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

4. If your ISP provides BigPond Cable (or Heart Beat Signal) connection, please select **BigPond Cable**. And you should enter the following parameters (Figure 4-6):

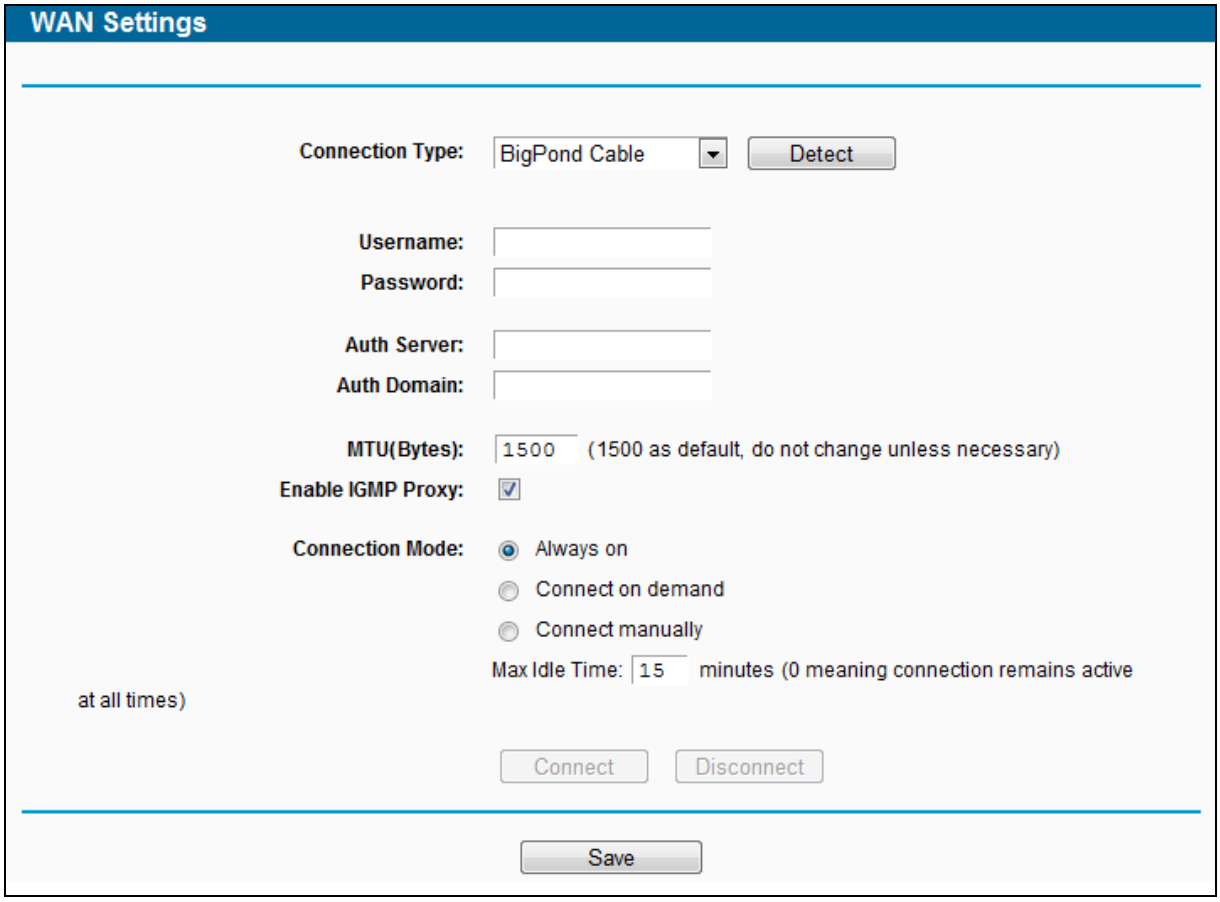


Figure 4-6 WAN - BigPond Cable

- **Username/Password -** Enter the User Name and Password provided by your ISP. These fields are case-sensitive.
- **Auth Server -** Enter the authenticating server IP address or host name.
- **Auth Domain -** Type in the domain suffix server name based on your location.

  e.g.

  NSW / ACT - **nsw.bigpond.net.au**
  VIC / TAS / WA / SA / NT - **vic.bigpond.net.au**
  QLD - **qld.bigpond.net.au**

- **MTU(Bytes)-** The normal **MTU** (Maximum Transmission Unit) value for most Ethernet networks is 1500 Bytes. It is not recommended that you change the default **MTU** value unless required by your ISP.
- **Enable IGMP Proxy -** IGMP (Internet Group Management Protocol) is used to manage multicasting on TCP/IP networks. Some ISPs use IGMP to perform remote configuration for client devices, such as the modem router. The default value is enabled, and if you are not sure, please contact your ISP or just leave it.
- **Connection Mode-**choose the Internet connection mode.
  - **Always on -** In this mode, the Internet connection will be active all the time.
  - **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. Enter the number of minutes you want to have elapsed before your Internet access disconnects.
  - **Connect Manually -** You can click the **Connect/Disconnect** button to connect/disconnect immediately. This mode also supports the **Max Idle Time** function as **Connect on Demand** mode. The Internet connection can be disconnected automatically after a specified inactivity period and re-established when you attempt to access the Internet again.

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

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

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

5. If your ISP provides L2TP connection, please select **L2TP** option. And you should enter the following parameters (Figure 4-7):

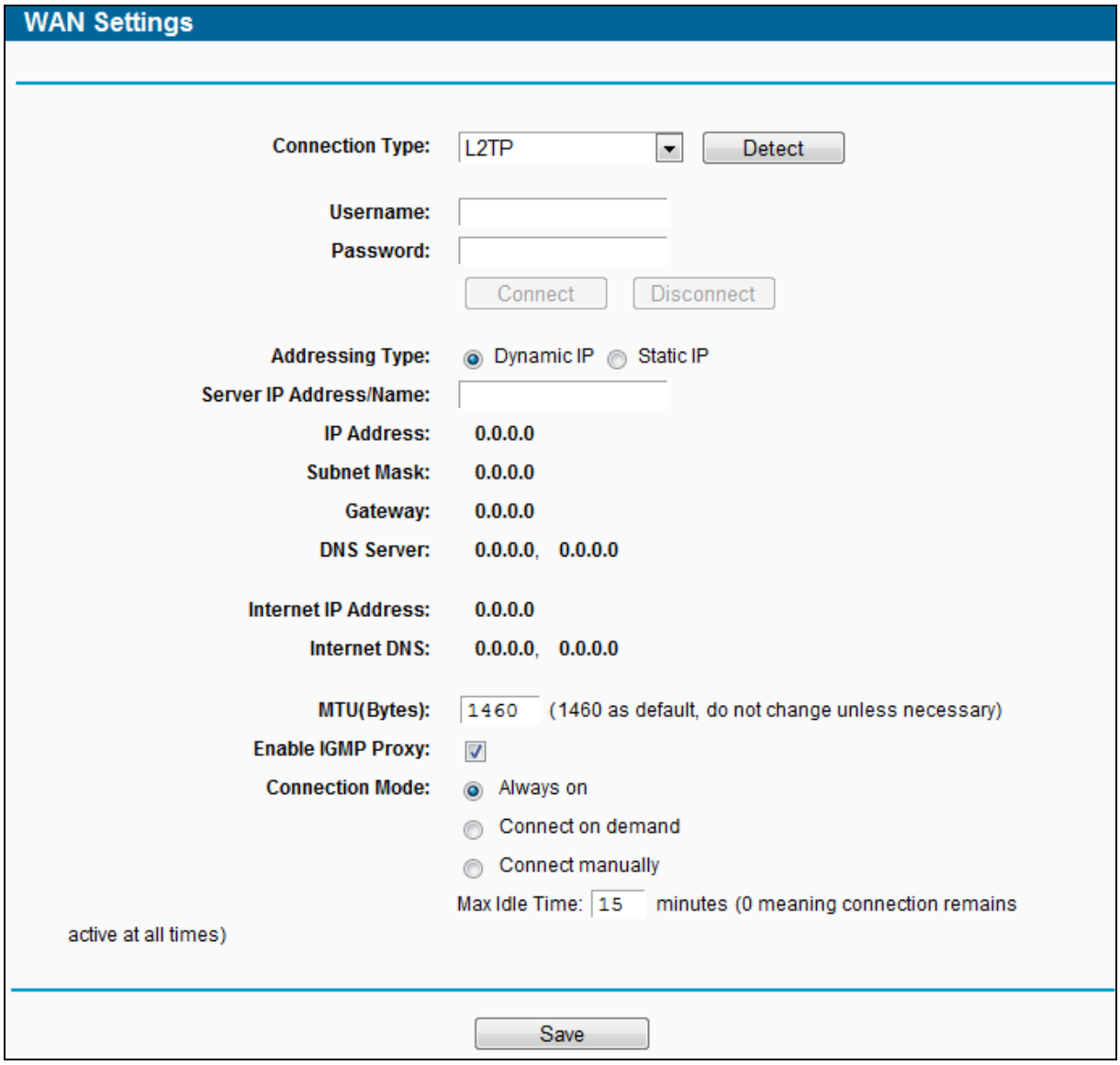


Figure 4-7 WAN - L2TP

- **Username/Password -** Enter the User Name and Password provided by your ISP. These fields are case-sensitive.
- **Addressing Type -** Choose the addressing type given by your ISP, either Dynamic IP or Static IP. Click the **Connect** button to connect immediately. Click the **Disconnect** button to disconnect immediately.
- **MTU(Bytes) -** The default MTU size is "1460" bytes, which is usually fine. It is not recommended that you change the default **MTU Size** unless required by your ISP.
- **Enable IGMP Proxy -** IGMP (Internet Group Management Protocol) is used to manage multicasting on TCP/IP networks. Some ISPs use IGMP to perform remote configuration for client devices, such as the modem router. The default value is enabled, and if you are not sure, please contact your ISP or just leave it.
- **Connection Mode-**choose the Internet connection mode.

- **Always on -** In this mode, the Internet connection will be active all the time.
- **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 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.

6. If your ISP provides PPTP connection, please select **PPTP** option. And you should enter the following parameters (Figure 4-8):

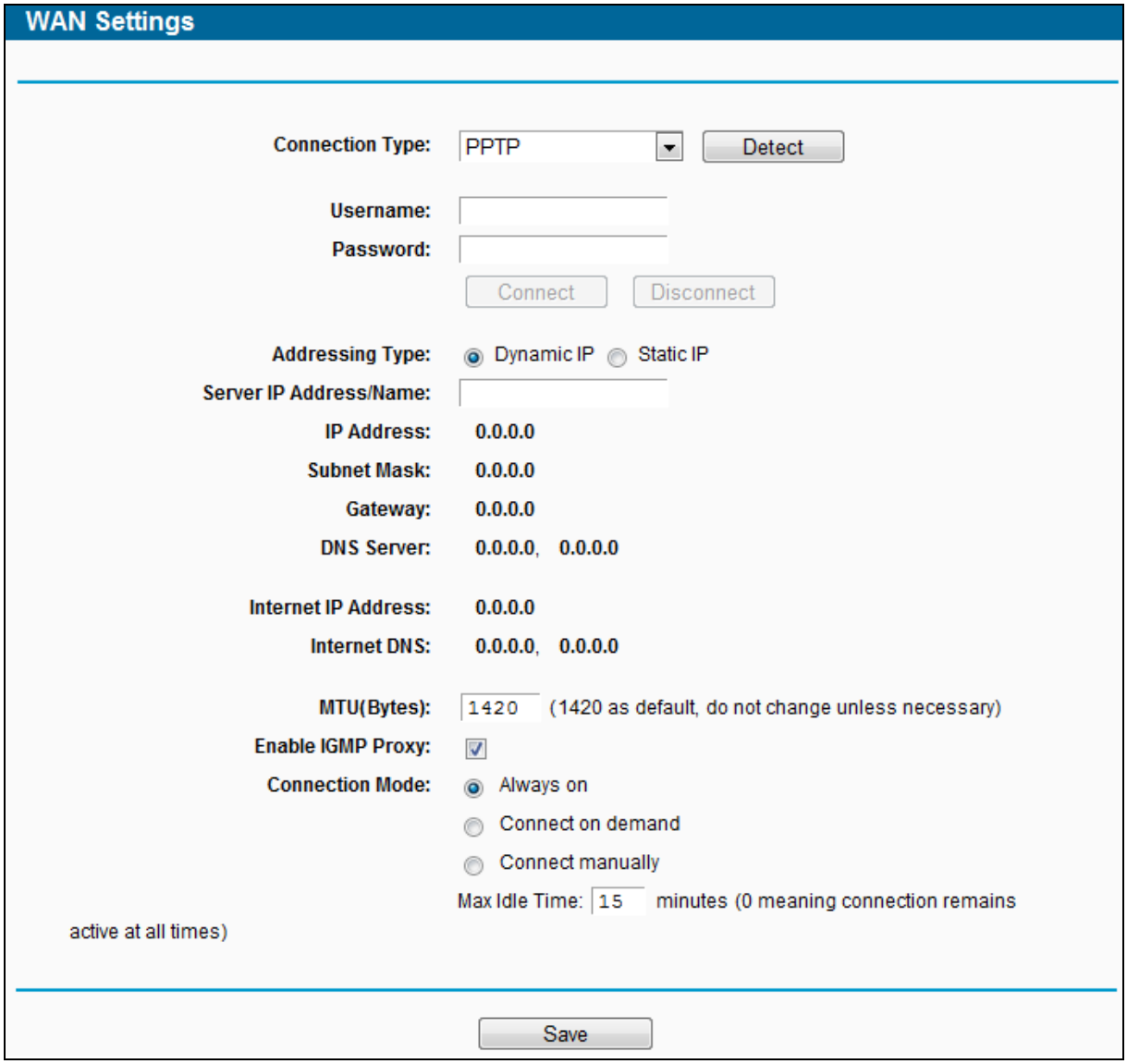


Figure 4-8 PPTP Settings

- **Username/Password -** Enter the User Name and Password provided by your ISP. These fields are case-sensitive.
- **Dynamic IP/ Static IP -** Choose the addressing type given by your ISP, either Dynamic IP or Static IP, 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.
- **MTU(Bytes)** The default MTU size is "1420" bytes, which is usually fine. It is not recommended that you change the default **MTU Size** unless required by your ISP.

- **Enable IGMP Proxy -** IGMP (Internet Group Management Protocol) is used to manage multicasting on TCP/IP networks. Some ISPs use IGMP to perform remote configuration for client devices, such as the modem router. The default value is enabled, and if you are not sure, please contact your ISP or just leave it.
- **Connection Mode-**choose the Internet connection mode.
  - **Always on -** In this mode, the Internet connection will be active all the time.
  - **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 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/Big Pond connections with your ISP. If your ISP uses one of these protocols, then you must configure your connection manually.

4.4.2 LAN

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

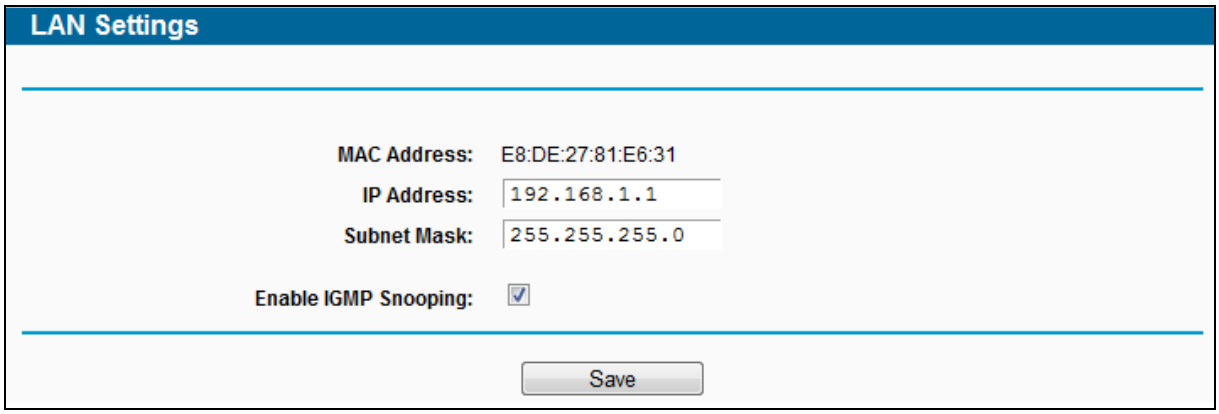


Figure 4-9 LAN Settings

- **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: 192.168.1.1).
- **Subnet Mask -** An address code that determines the size of the network. Normally use 255.255.255.0 as the subnet mask.

☞ **Note:**

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

4.4.3 MAC Clone

Choose menu "**Network → MAC Clone**", you can configure the MAC address of the WAN on the screen below, Figure 4-10:

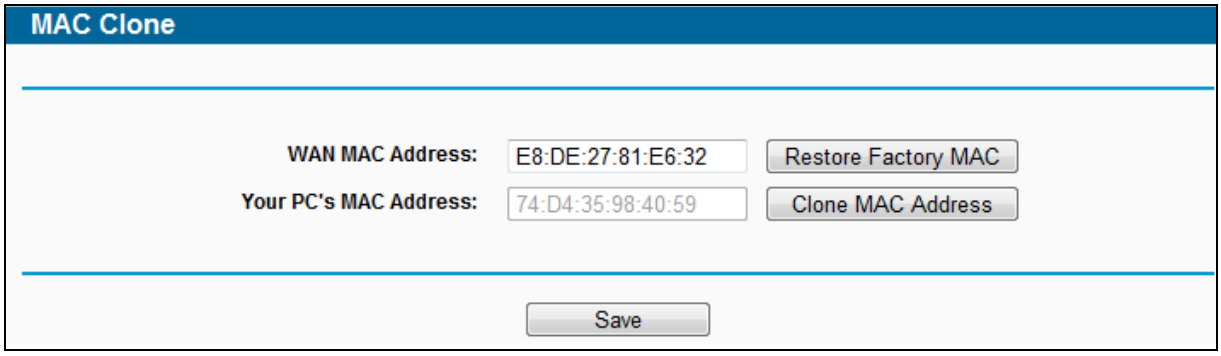


Figure 4-10 MAC Clone

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

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

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

☞ **Note:**

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

4.5 Dual Band Selection

Choose menu "**Dual Band Selection**", and you can choose the working frequency for your router. It is recommended that your computers and devices running video and voice applications use the 5GHz band, while your guest access and computers that are only browsing the web use the 2.4GHz band.

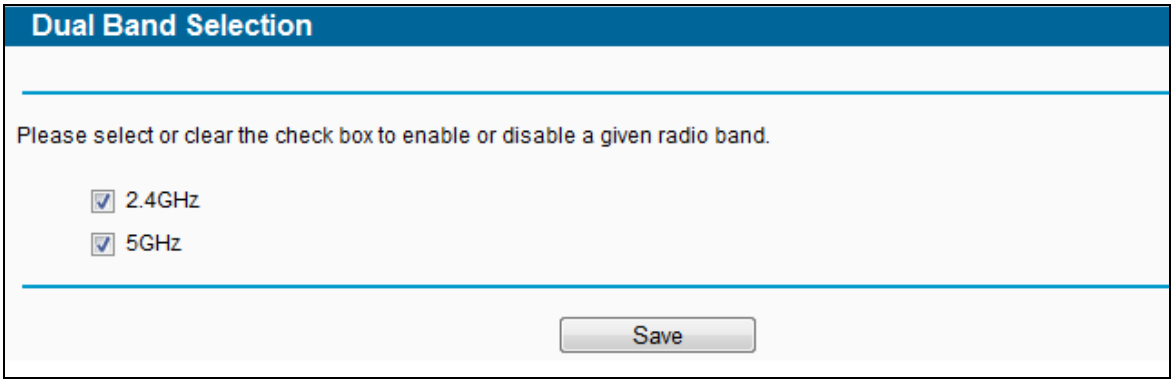


Figure 4-11 Dual Band Selection

- **2.4GHz (802.11b/g/n) -** Click the box, and then the router will only work in 2.4GHz frequency. You can use the 2.4GHz band to connect to many classic wireless devices like gaming consoles, laptops, DVRs, etc.
- **5GHz (802.11a/n/ac) -** Click the box, and then the router will only work in 5GHz frequency. This band is less crowded and is used for time-sensitive music, video streaming or gaming. Using this band can avoid interference with 2.4GHz networks or noisy devices like cordless phones and microwave ovens.

4.6 Wireless 2.4GHz

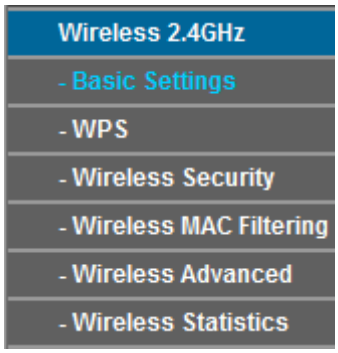


Figure 4-12 Wireless menu

There are six submenus under the Wireless menu (shown in Figure 4-12): **Basic 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.

4.6.1 Basic Settings

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

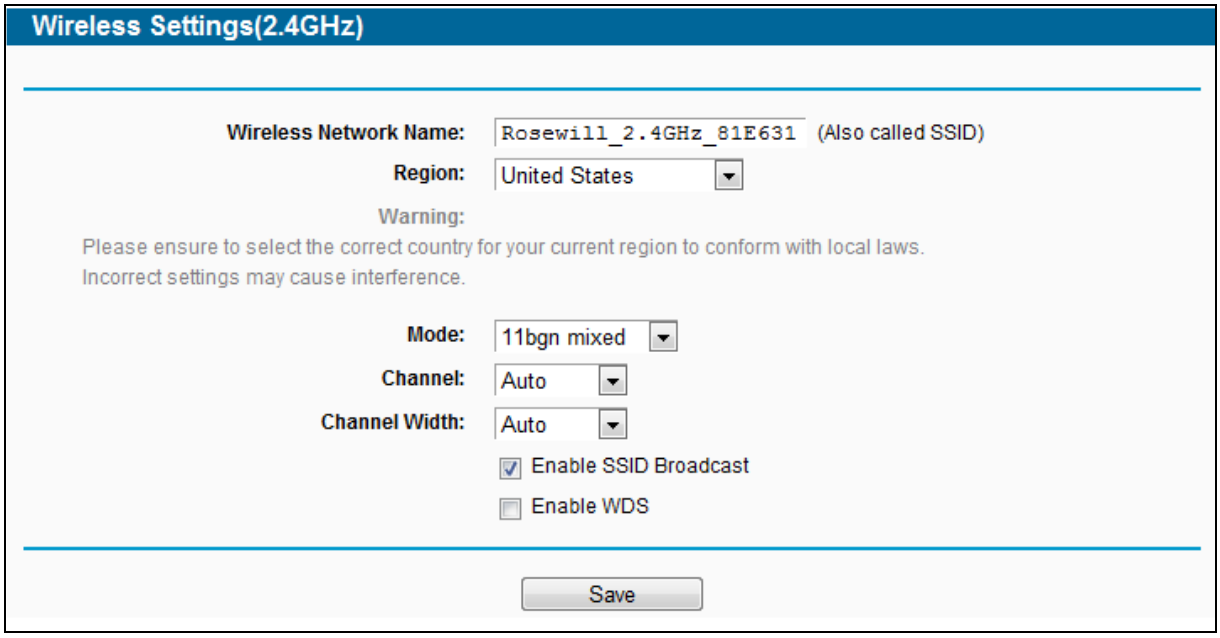
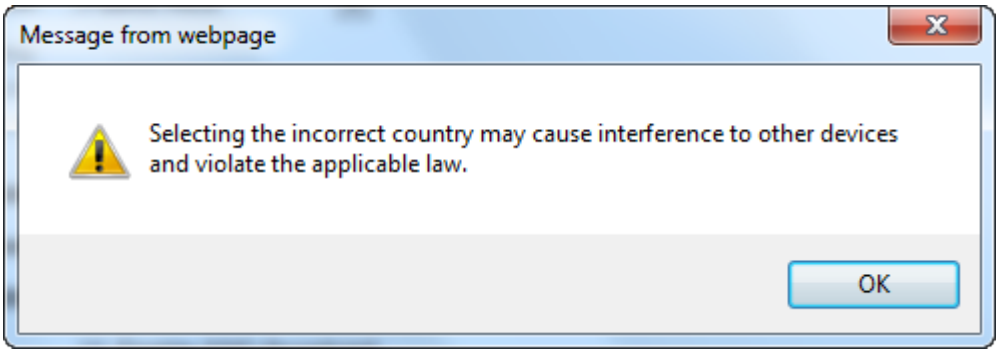


Figure 4-13 Wireless Settings – 2.4GHz

- **Wireless Network Name -** 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. Considering your wireless network security, the default SSID is set to be Rosewill_2.4GHz_XXXXXX. This value is case-sensitive. For example, *TEST* is NOT the same as *test*.

- **Region -** Select your region from the drop-down list. This field specifies the region where the wireless function of the router can be used. It may be illegal to use the wireless function of the router in a region other than one of those specified in this field. If your country or region is not listed, please contact your local government agency for assistance.

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



Note Dialog

☞ **Note:**

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

- **Mode -** Select the desired mode.
  - **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 -** This field determines which operating frequency will be used. The default channel is set to **Auto**, so the AP 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.
- **Channel Width -** Select the channel width from the drop-down list. The default setting is automatic, which can adjust the channel width for your clients automatically.

☞ **Note:**

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

- **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 -** 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 4-14. Make sure the following settings are correct.

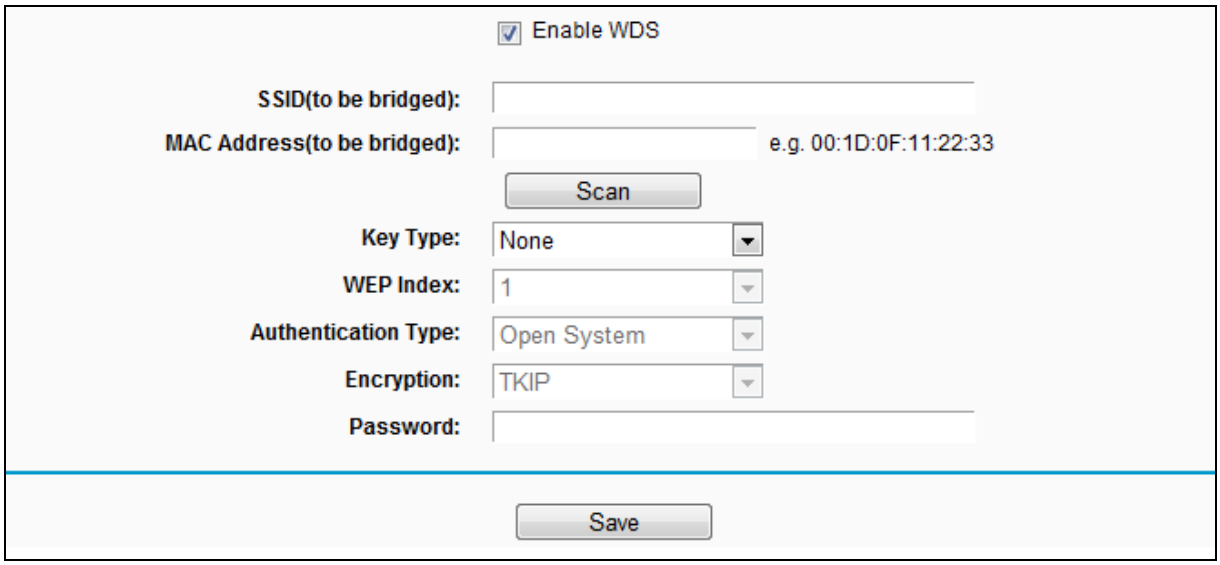


Figure 4-14 WDS Setting

- **SSID (to be bridged)** - The SSID of the AP your router is going to connect to as a client. You can also use the search function to select the SSID to join.
- **MAC Address (to be bridged)** - The BSSID of the AP your router is going to connect to as a client. You can also use the search function to select the BSSID to join.
- **Scan** - Click this button, you can search the AP which runs in the current channel.
- **Key type** - This option should be chosen according to the AP's security configuration. It is recommended that the security type is the same as your AP's security type
- **WEP Index** - This option should be chosen if the key type is WEP(ASCII) or WEP(HEX). It indicates the index of the WEP key.
- **Authentication Type** - This option should be chosen if the key type is WEP(ASCII) or WEP(HEX). It indicates the authorization type of the Root AP.
- **Encryption** - When **WPA** is set as the Authentication Type, you can select either TKIP or AES as Encryption.
- **Password** - If the AP your router is going to connect needs password, you need to fill the password in this blank.

4.6.2 WPS

Choose menu "**Wireless 2.4GHz →WPS**", you can the screen as shown in Figure 4-15. This section will guide you to add a new wireless device to an existing network quickly by WPS (Wi-Fi Protected Setup) function.

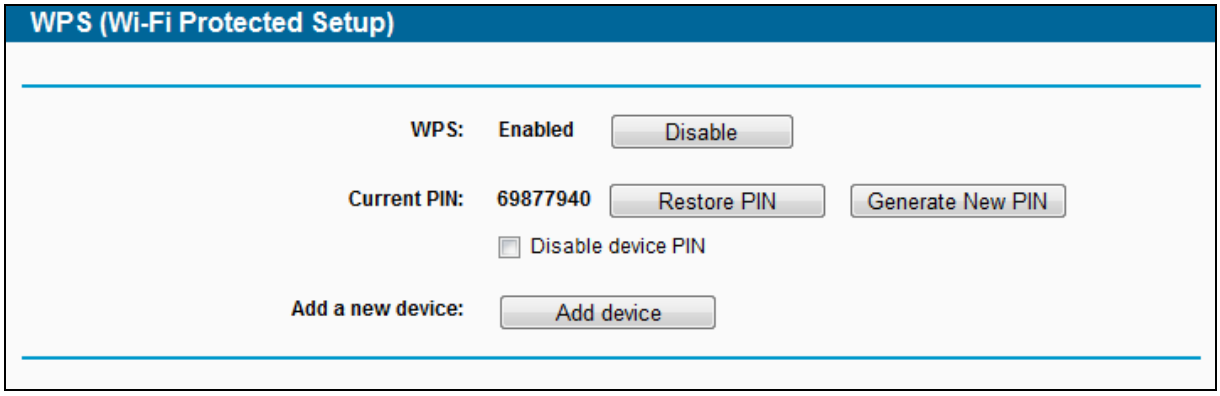


Figure 4-15 WPS

- **WPS -** Enable or disable the WPS function here.
- **Current PIN -** The current value of the router's PIN is displayed here. The default PIN of the router can be found in the label or User Guide.
- **Restore PIN -** Restore the PIN of the router to its default.

- **Generate 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.
- **Disable device PIN -** If this box is checked, and then wireless clients will not be able to connect to the wireless network with PIN code.
- **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 router using either Push Button Configuration (PBC) method or PIN method.

Note:

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

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, as shown in Figure 4-16. You can also keep the default WPS status as **Enabled** and click the **Add device** button in Figure 4-15. Then choose "**Press the button of the new device in two minutes**" and click **Connect**, shown in Figure 4-17.

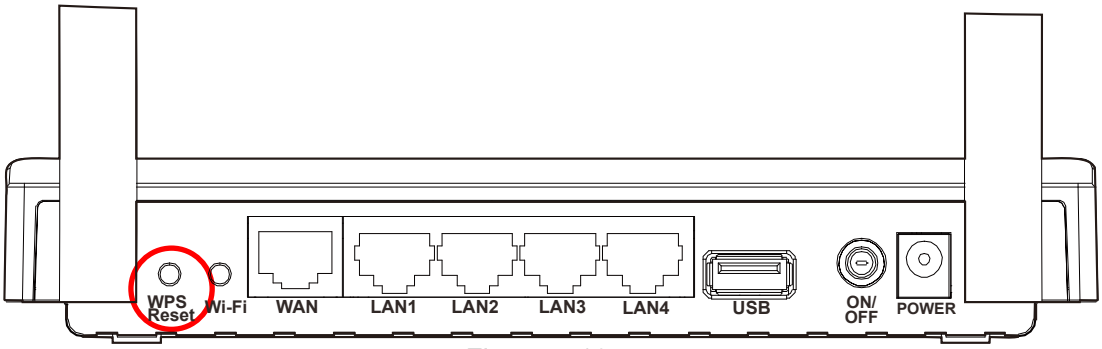


Figure 4-16

Figure 4-17 Add A New Device

Step 2: Press and hold the **WPS** button of the client device.

Step 3: The Wi-Fi Protected Setup LED flashes for two minutes during the Wi-Fi Protected Setup process.

Step 4: 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 1: Keep the default WPS status as **Enabled** and click the **Add device** button in Figure 4-15, then Figure 4-18 will appear.

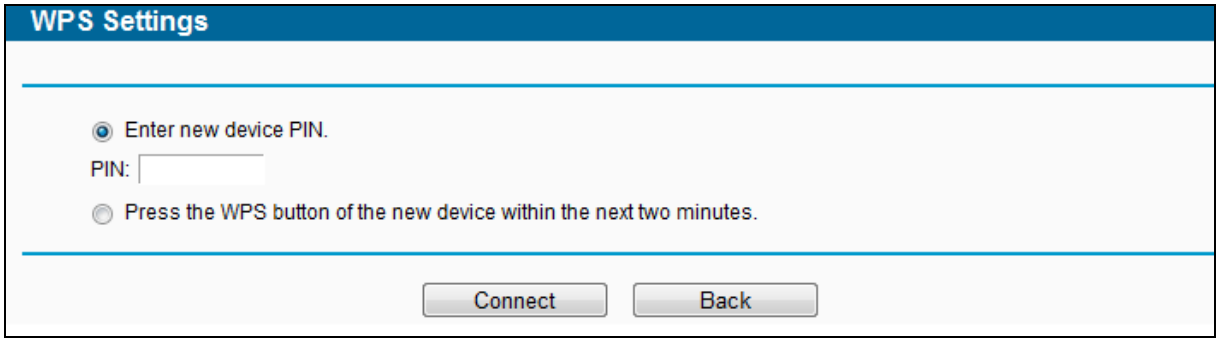


Figure 4-18 Add A New Device

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

Step 3: "**Connect successfully**" will appear on the screen of Figure 4-18, which means the client device has successfully connected to the router.

III. Enter the router's PIN on your client device

Use this method if your client device asks for the router's PIN number.

Step 1: On the client device, enter the PIN number listed on the router's Wi-Fi Protected Setup screen, shown in Figure 4-15 (It is also labeled on the bottom of the router).

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

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

☞ **Note:**

1) The WPS LED on the router will light green for five minutes if the device has been successfully added to the network.

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

4.6.3 Wireless Security

Choose menu "**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.

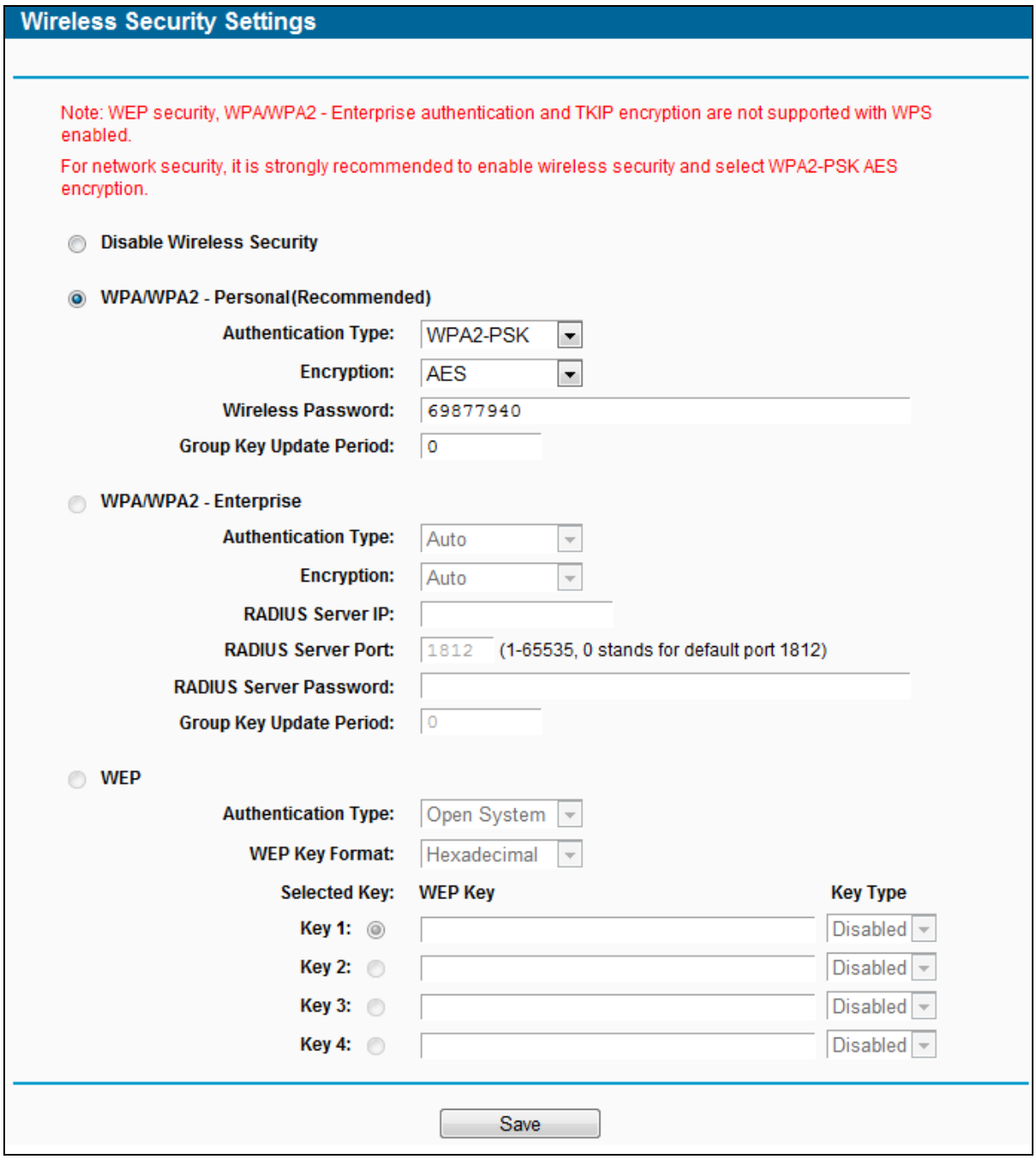


Figure 4-19 Wireless Security

- **Disable Wireless 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.
  - **Authentication Type -** you can choose the version of the WPA-PSK security on the drop-down list. The default setting is **Auto**, which can select **WPA-PSK** (Pre-shared key of WPA) or **WPA2-PSK** (Pre-shared key of WPA) automatically based on the wireless station's capability and request.

- **Encryption** - When **WPA-PSK** or **WPA** is set as the Authentication Type, you can select either **Automatic**, or **TKIP** or **AES** as Encryption.

☞ **Note:**

If you check the **WPA/WPA2-Personal** radio button and choose **TKIP** encryption, you will find a notice in red as shown in Figure 4-20.

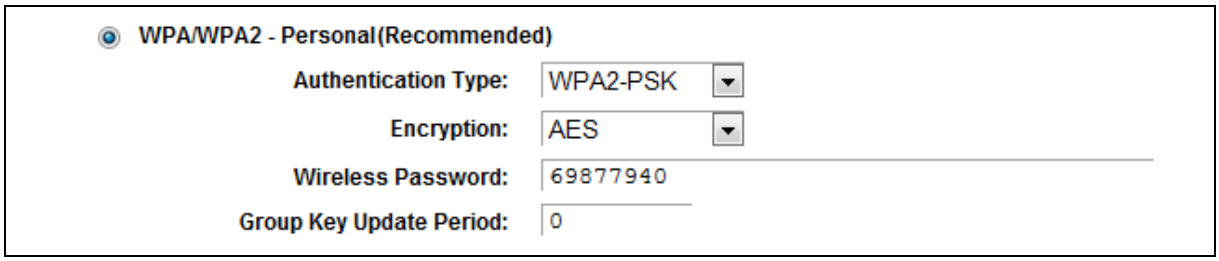


Figure 4-20 WPA/WPA2 – Personal

- **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 bottom of the router or can be found in Figure 4-15.
- **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.

- **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 4-21.

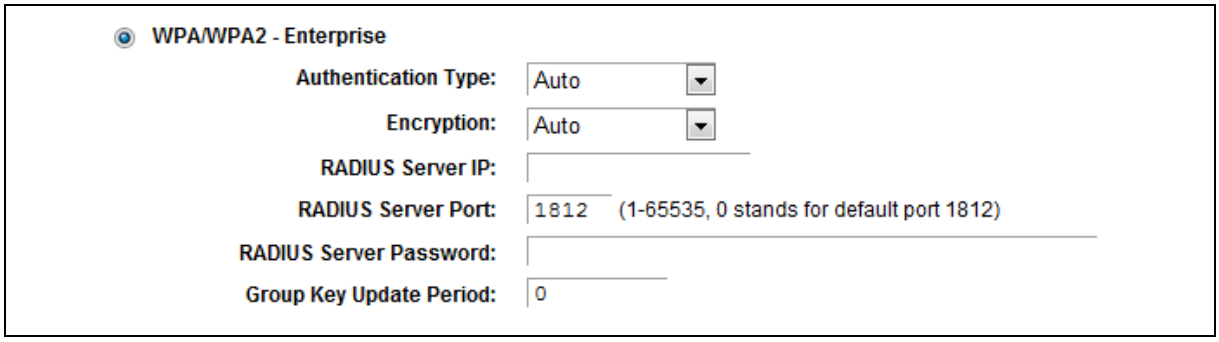


Figure 4-21 WPA/WPA2 - Enterprise

- **Radius Server IP -** Enter the IP address of the Radius server.
- **Radius Server Port -** Enter the port number of the Radius server.

- **Radius Server 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 show in Figure 4-22.

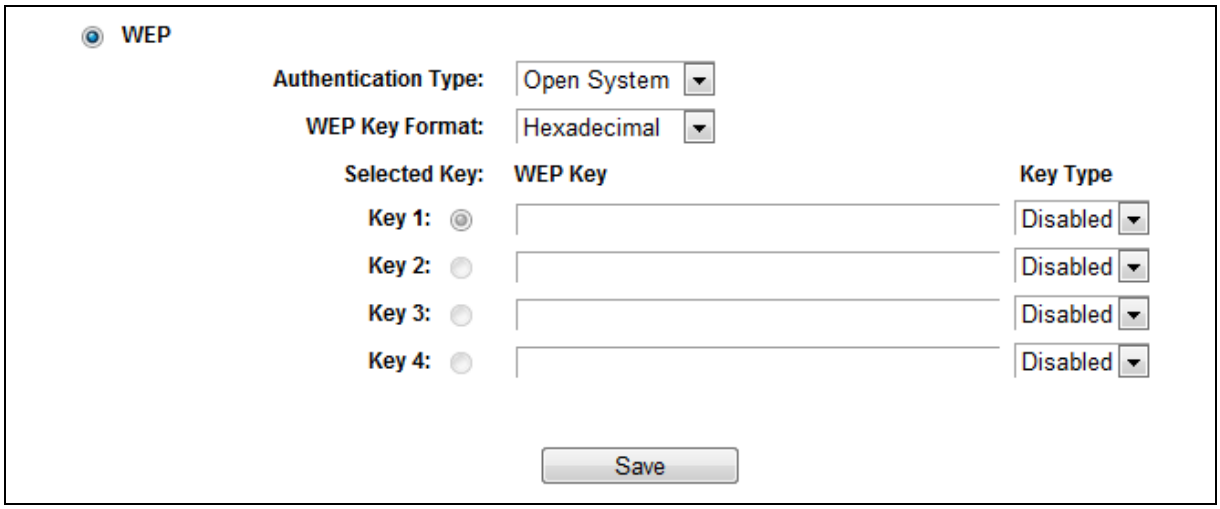


Figure 4-22 WEP

- **Authentication Type -** you can choose the type for the WEP security on the drop-down list. The default setting is **Auto**, 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, or 152-bit.) for encryption. "Disabled" means this WEP key entry is invalid.

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

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

  ☞ **Note:**

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

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

4.6.4 Wireless MAC Filtering

Choose menu "**Wireless 2.4GHz → Wireless MAC Filtering**", you can control the wireless access by configuring the **Wireless MAC Filtering** function, shown in Figure 4-23.

Figure 4-23 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**.
- **Host -** The host network for the filtering rules.
- **Description -** A simple description of the wireless station.

To Add a Wireless MAC Address filtering entry, click the **Add New** button. The "**Add or Modify Wireless MAC Address Filtering entry**" page will appear, shown in Figure 4-24:

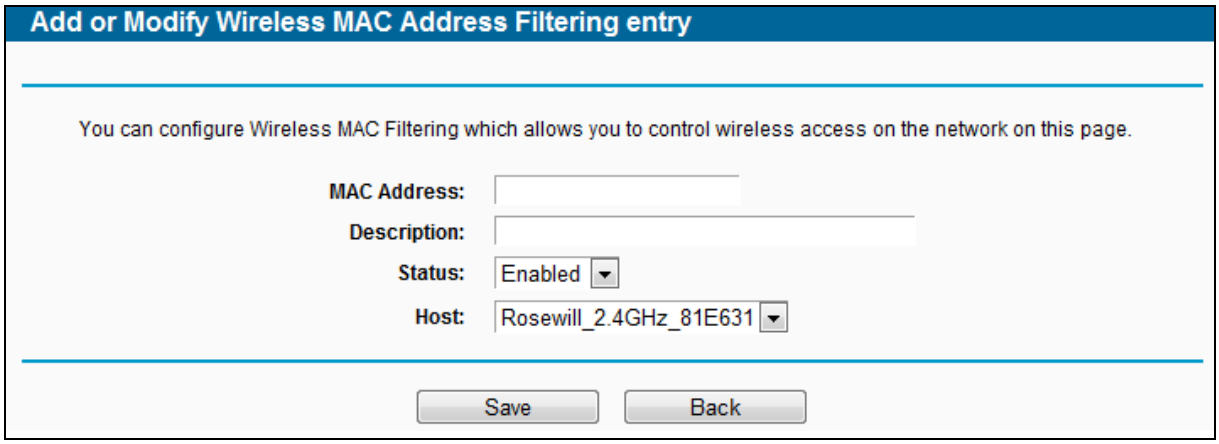


Figure 4-24 Add or Modify Wireless MAC Address Filtering entry

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 edit or delete an existing entry:

1. Click the **Edit** 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 Selected** button to make selected entries enabled

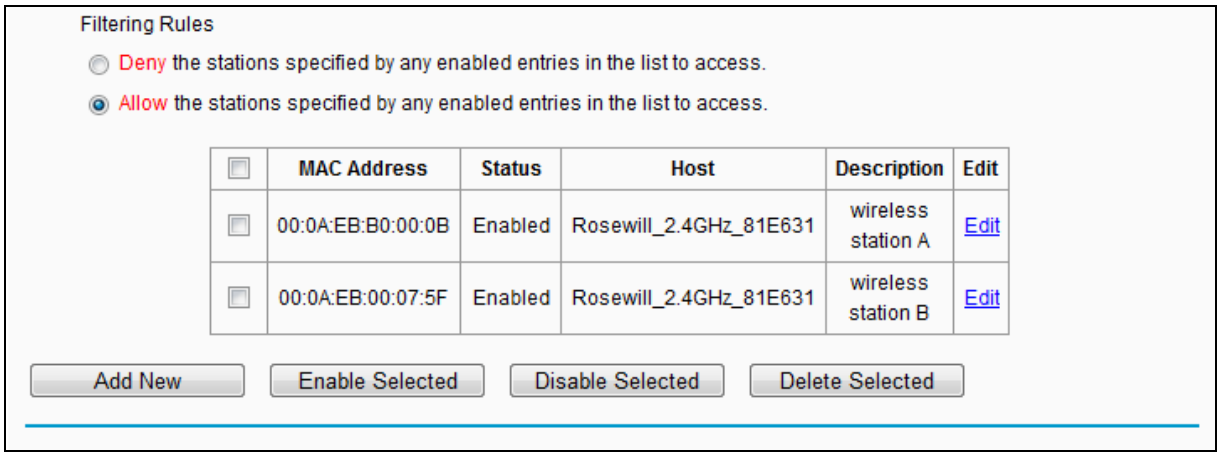
Click the **Disable Selected** button to make selected entries disabled.

Click the **Delete Selected** button to delete selected l entries.

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 entries 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:



4.6.5 Wireless Advanced

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

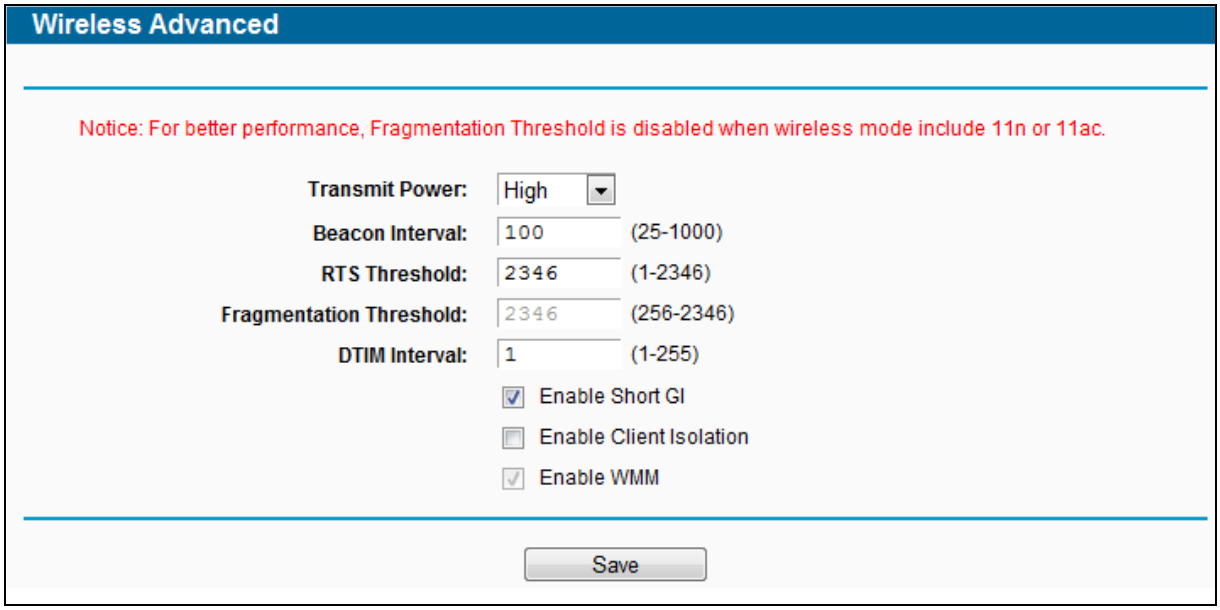


Figure 4-25 Wireless Advanced

- **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 20-1000 milliseconds for Beacon Interval here. The beacons are the packets sent by the router to synchronize a wireless network. Beacon Interval value determines the time interval of the beacons. The default value is 100.
- **RTS Threshold -** Here you can specify the RTS (Request to Send) Threshold. If the packet is larger than the specified RTS Threshold size, the router will send RTS frames to a particular receiving station and negotiate the sending of a data frame. The default value is 2346.

- **Fragmentation Threshold -** This value is the maximum size determining whether packets will be fragmented. Setting the Fragmentation Threshold too low may result in poor network performance because of excessive packets. 2346 is the default setting and is recommended.
- **DTIM Interval -** This value determines the interval of the Delivery Traffic Indication Message (DTIM). A DTIM field is a countdown field informing clients of the next window for listening to broadcast and multicast messages. When the router has buffered broadcast or multicast messages for associated clients, it sends the next DTIM with a DTIM Interval value. You can specify the value between 1-15 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.

4.6.6 Wireless Statistics

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

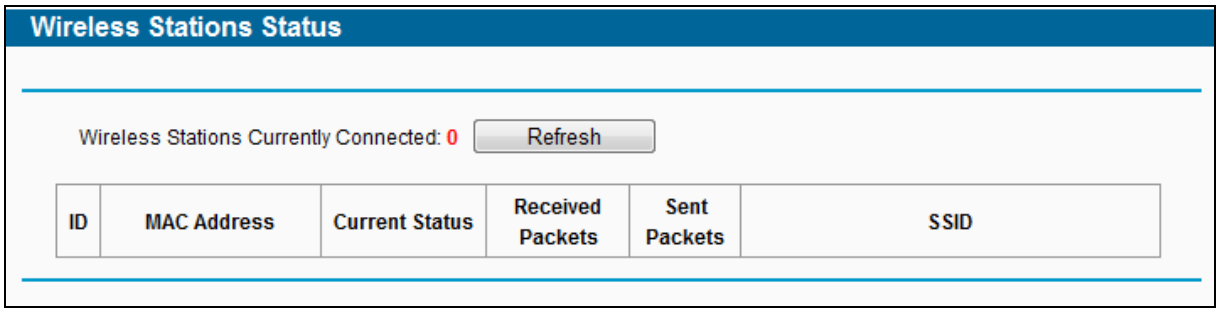


Figure 4-26 Wireless Statistics

- **MAC Address -** The connected wireless station's MAC address
- **Current Status -** The running status of the connected wireless stations.
- **Received Packets -** Packets received by the station

➢ **Sent Packets -** Packets sent by the station

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

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

☞ **Note:**

This page will be refreshed automatically every 5 seconds.

4.7 Wireless 5GHz

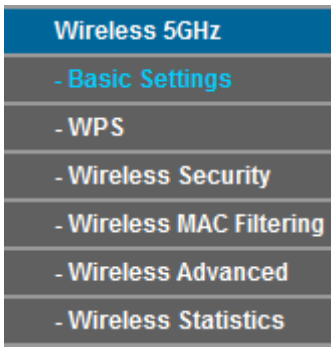


Figure 4-27 Wireless menu

There are six submenus under the Wireless menu (shown in Figure 4-12): **Basic 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.

4.7.1 Basic Settings

Choose menu "**Wireless 5GHz → Basic Settings**", you can configure the basic settings for the wireless network of 5GHz on this page.

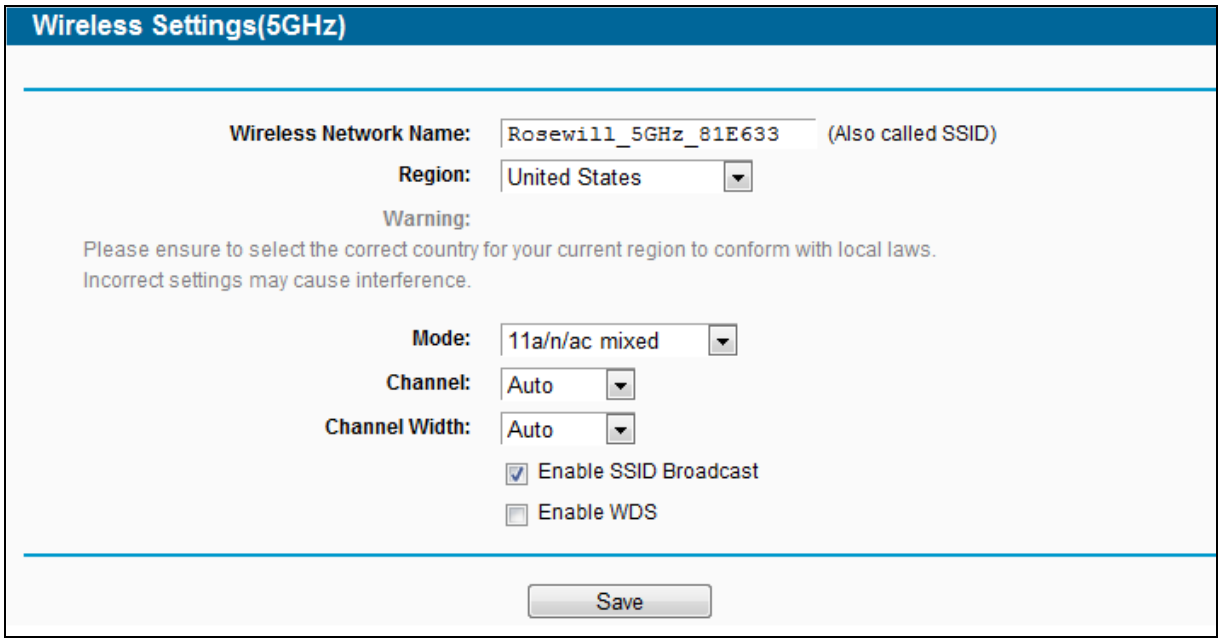
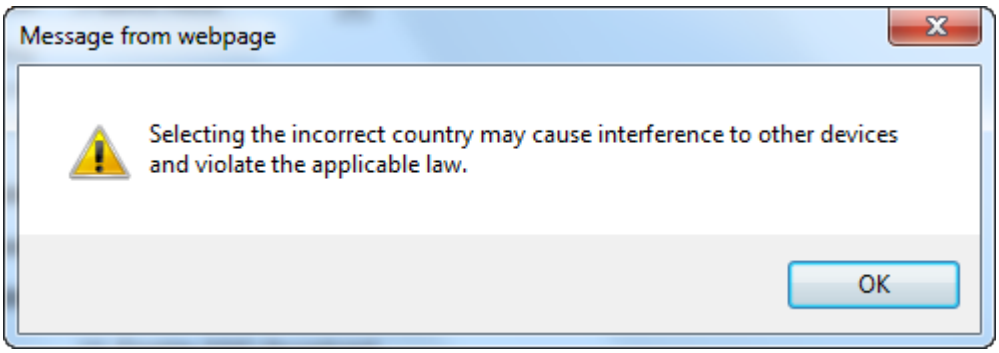


Figure 4-28 Wireless Settings – 5GHz

- **Wireless Network Name -** 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. Considering your wireless network security, the default SSID is set to be Rosewill_5GHz_XXXXXX. This value is case-sensitive. For example, *TEST* is NOT the same as *test*.

- **Region -** Select your region from the drop-down list. This field specifies the region where the wireless function of the router can be used. It may be illegal to use the wireless function of the router in a region other than one of those specified in this field. If your country or region is not listed, please contact your local government agency for assistance.

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



Note Dialog

☞ **Note:**

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

- **Mode -** Select the desired mode.
  - **11an mixed -** Select if you are using both 802.11a and 802.11n wireless clients. If you set the Mode **11an mixed**, all of 802.11a and 802.11n wireless stations can connect to the router.
  - **11a/n/ac mixed -** Select if you are using a mix of 802.11a, 802.11n and 802.11ac wireless clients. It is strongly recommended you set the Mode **11a/n/ac mixed**, all of 802.11a, 802.11n and 802.11ac wireless stations can connect to the router.
- **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 4-29. Make sure the following settings are correct.

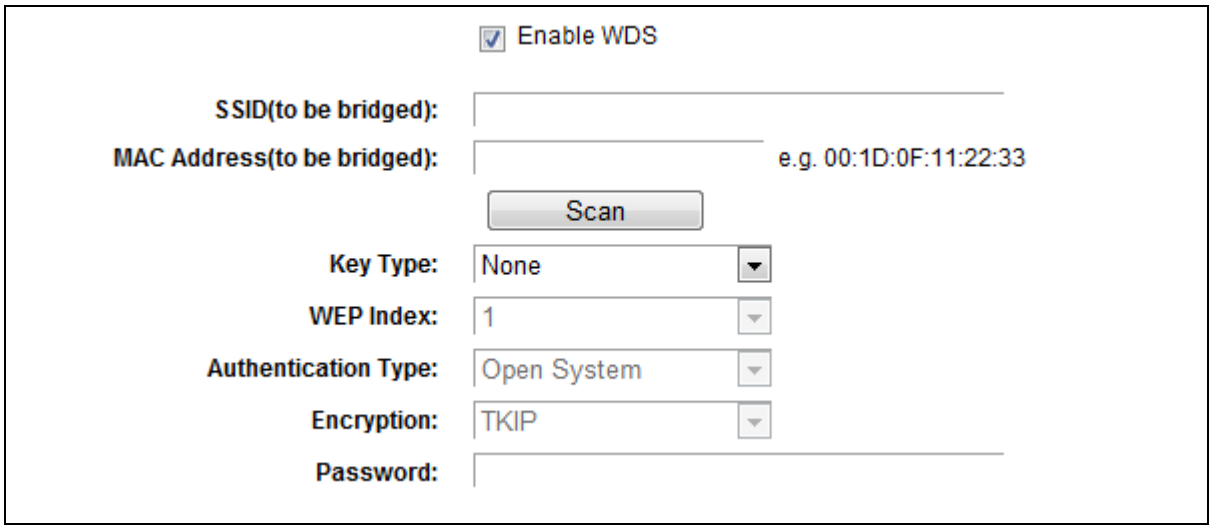


Figure 4-29

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

- **MAC Address (to be bridged)** - The BSSID of the AP your router is going to connect to as a client. You can also use the search function to select the BSSID to join.
- **Scan** - Click this button, you can search the AP which runs in the current channel.
- **Key type** - This option should be chosen according to the AP's security configuration. It is recommended that the security type is the same as your AP's security type
- **WEP Index** - This option should be chosen if the key type is WEP(ASCII) or WEP(HEX).It indicates the index of the WEP key.
- **Authentication Type** - This option should be chosen if the key type is WEP(ASCII) or WEP(HEX).It indicates the authorization type of the Root AP.
- **Encryption** - When **WPA** is set as the Authentication Type, you can select either TKIP or AES as Encryption.
- **Password** - If the AP your router is going to connect needs password, you need to fill the password in this blank.

4.7.2 WPS

Choose menu "**Wireless 5GHz →WPS**", you can the screen as shown in Figure 4-30. This section will guide you to add a new wireless device to an existing network quickly by WPS (Wi-Fi Protected Setup) function.

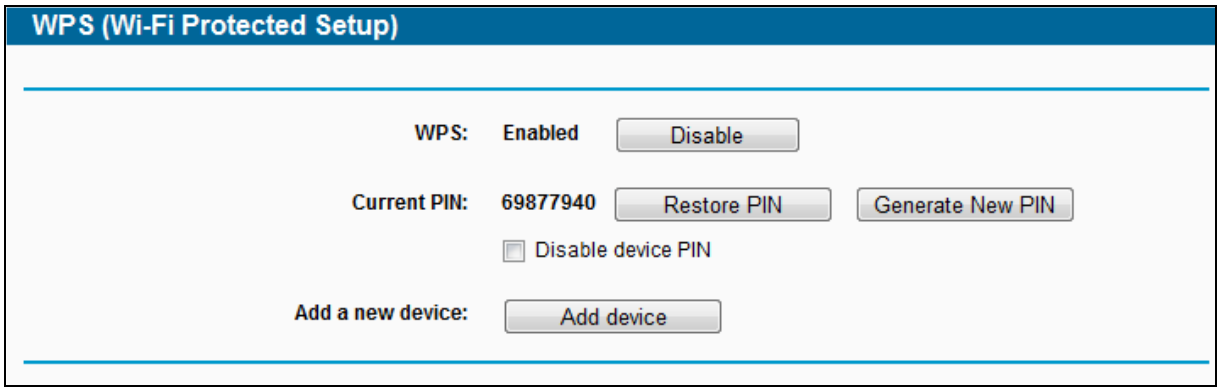


Figure 4-30 WPS

- **WPS -** Enable or disable the WPS function here.
- **Current PIN -** The current value of the router's PIN is displayed here. The default PIN of the router can be found in the label or User Guide.
- **Restore PIN -** Restore the PIN of the router to its default.
- **Generate 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 router using either Push Button Configuration (PBC) method or PIN method.

Note:

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

I. Use the Wi-Fi Protected Setup Button

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

Step 1: Press the **WPS/Reset** button on the back panel of the router, as shown in Figure 4-31. You can also keep the default WPS status as **Enabled** and click the **Add device** button in Figure 4-30. Then choose "**Press the button of the new device in two minutes**" and click **Connect**, shown in Figure 4-32.

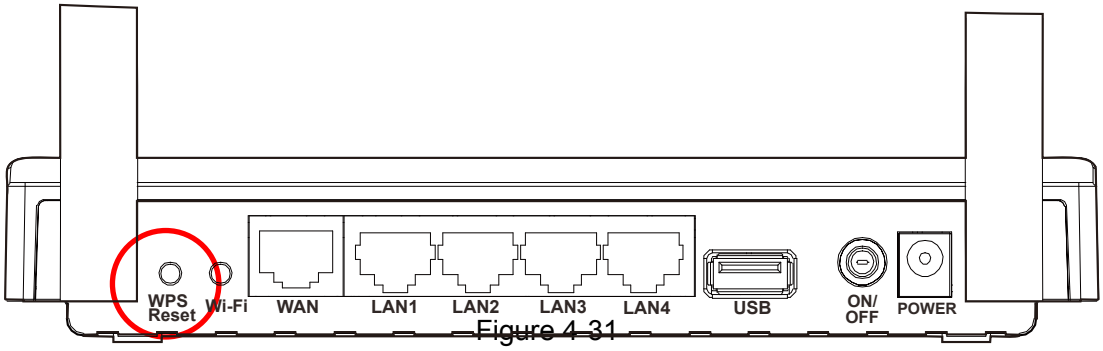


Figure 4-31

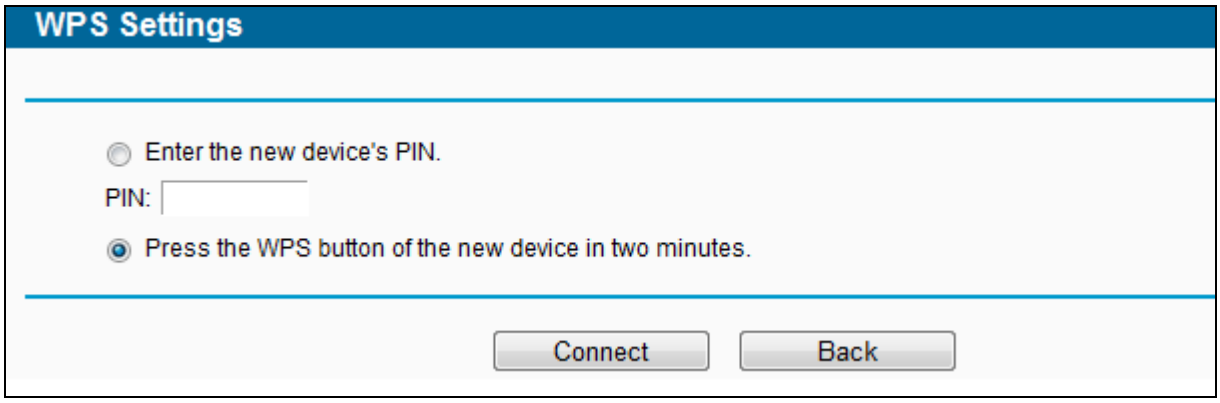


Figure 4-32 Add A New Device

Step 2: Press and hold the WPS button of the client device directly.

Step 3: The Wi-Fi Protected Setup LED flashes for two minutes during the Wi-Fi Protected Setup process.

Step 4: 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 1: Keep the default WPS status as **Enabled** and click the **Add device** button in Figure 4-30, then Figure 4-33 will appear.

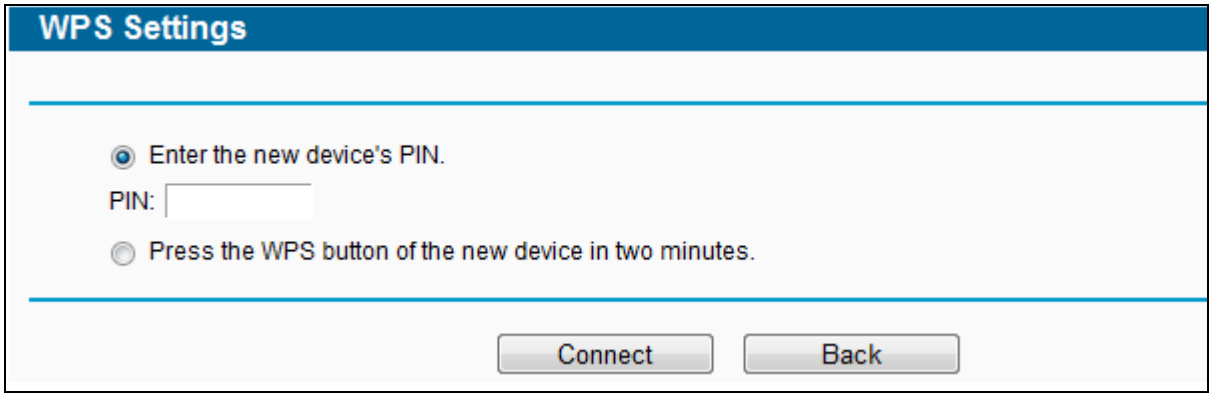


Figure 4-33 Add A New Device

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

Step 3: "**Connect successfully**" will appear on the screen of Figure 4-33, which means the client device has successfully connected to the router.

III. Enter the router's PIN on your client device

Use this method if your client device asks for the router's PIN number.

Step 1: On the client device, enter the PIN number listed on the router's Wi-Fi Protected Setup screen, shown in Figure 4-30 (It is also labeled on the bottom of the router).

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

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

☞ **Note:**

1) The WPS LED on the router will light green for five minutes if the device has been successfully added to the network.

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

4.7.3 Wireless Security

Choose menu "**Wireless 5GHz → 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.

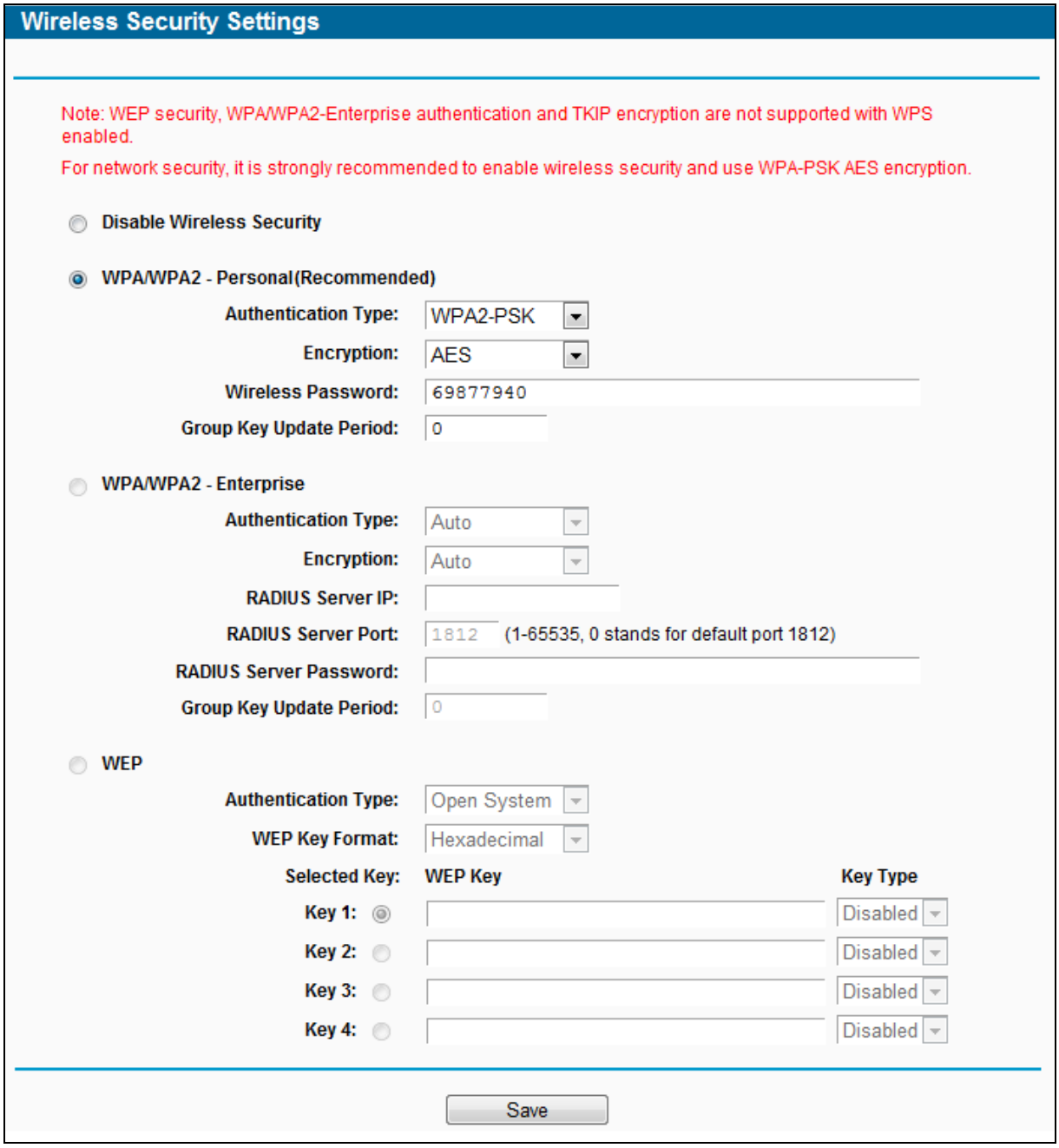


Figure 4-34 Wireless Security

- **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.
  - **Authentication Type-** you can choose the version of the WPA-PSK security on the drop-down list. The default setting is **Automatic**, which can select **WPA-PSK**

(Pre-shared key of WPA) or **WPA2-PSK** (Pre-shared key of WPA) automatically based on the wireless station's capability and request.

- **Encryption -** When **WPA-PSK** or **WPA** is set as the Authentication Type, you can select either **Automatic**, or **TKIP** or **AES** as Encryption.

☞ **Note:**

If you check the **WPA/WPA2-Personal** radio button and choose **TKIP** encryption, you will find a notice in red as shown in Figure 4-35.

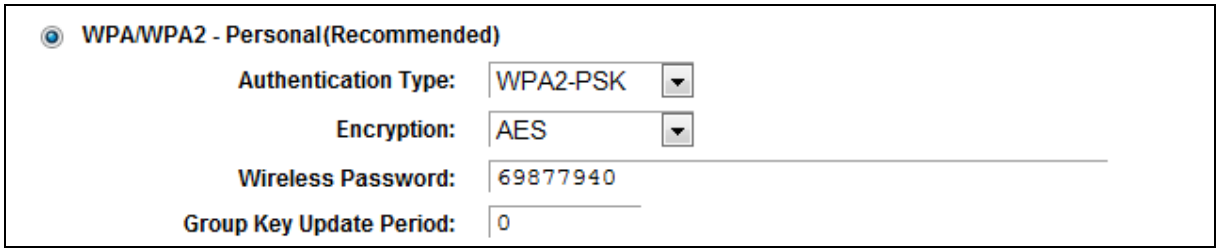


Figure 4-35 WPA/WPA2 – Personal

- **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 bottom of the router or can be found in Figure 4-30.
- **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.

- **Authentication Type -** 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 4-36.

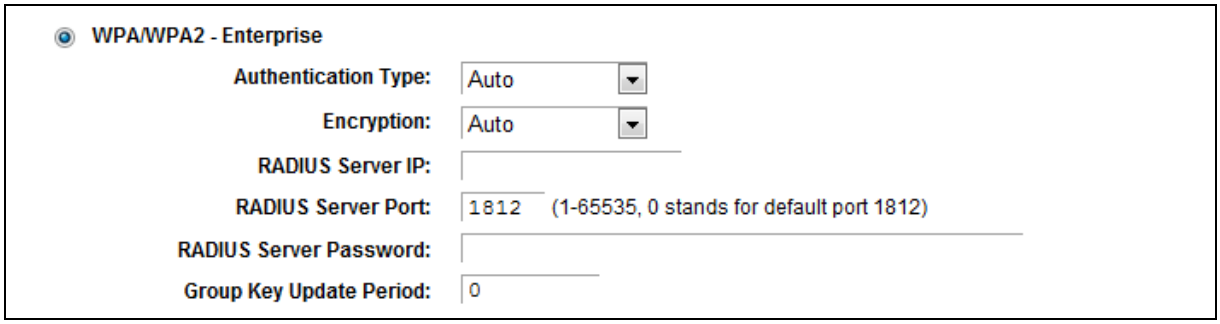


Figure 4-36 WPA/WPA2 - Enterprise

- **Radius Server IP -** Enter the IP address of the Radius server.
- **Radius Server Port -** Enter the port number of the Radius server.
- **Radius Server 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 show in Figure 4-37.

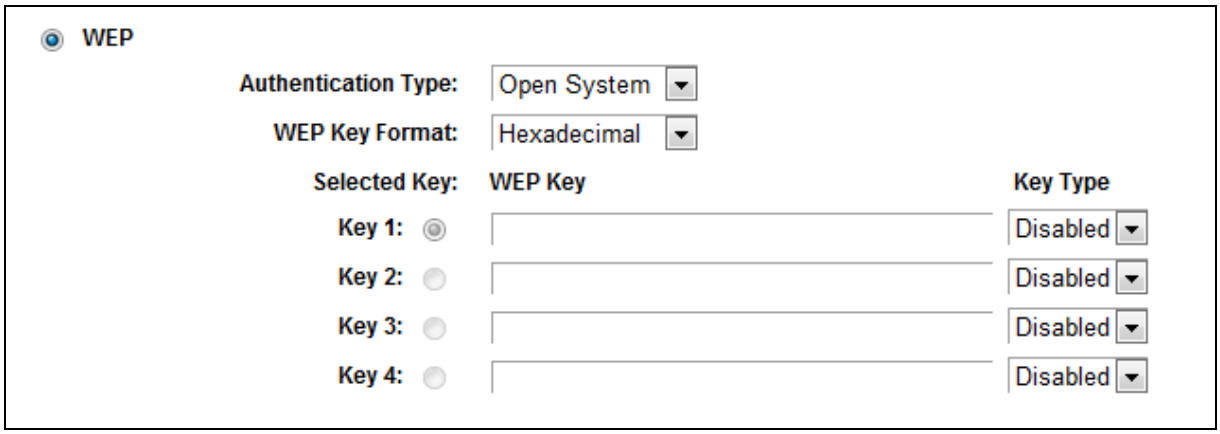


Figure 4-37 WEP

- **Authentication 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, or 152-bit.) for encryption. "Disabled" means this WEP key entry is invalid.

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

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

☞ **Note:**

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

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

4.7.4 Wireless MAC Filtering

Choose menu "**Wireless → MAC Filtering**", you can control the wireless access by configuring the **Wireless MAC Filtering** function, shown in Figure 4-23.

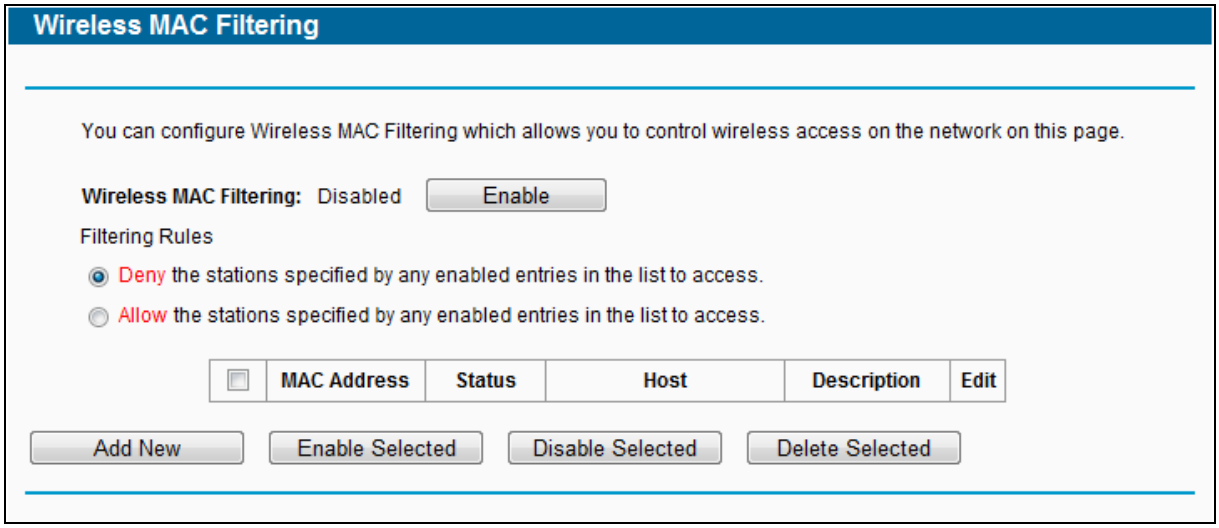


Figure 4-38 Wireless MAC Filtering

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**.
- **Host-** The host network for the filetring rules.
- **Description -** A simple description of the wireless station.

To Add a Wireless MAC Address filtering entry, click the **Add New** button. The "**Add or Modify Wireless MAC Address Filtering entry**" page will appear, shown in Figure 4-24:

Figure 4-39 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. Select the Host for the entry.
5. 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 Selected** button to make the selected entries enabled

Click the **Disable Selected** button to make the selected entries disabled.

Click the **Delete Selected** button to delete the selected entries.

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

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

Filtering Rules

Deny the stations specified by any enabled entries in the list to access.

Allow the stations specified by any enabled entries in the list to access.

	MAC Address	Status	Host	Description	Edit
	00:0A:EB:B0:00:0B	Enabled	Rosewill_5GHz_81E633	Wireless station A	Edit
	00:0A:EB:00:07:5F	Enabled	Rosewill_5GHz_81E633	wireless station B	Edit

4.7.5 Wireless Advanced

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

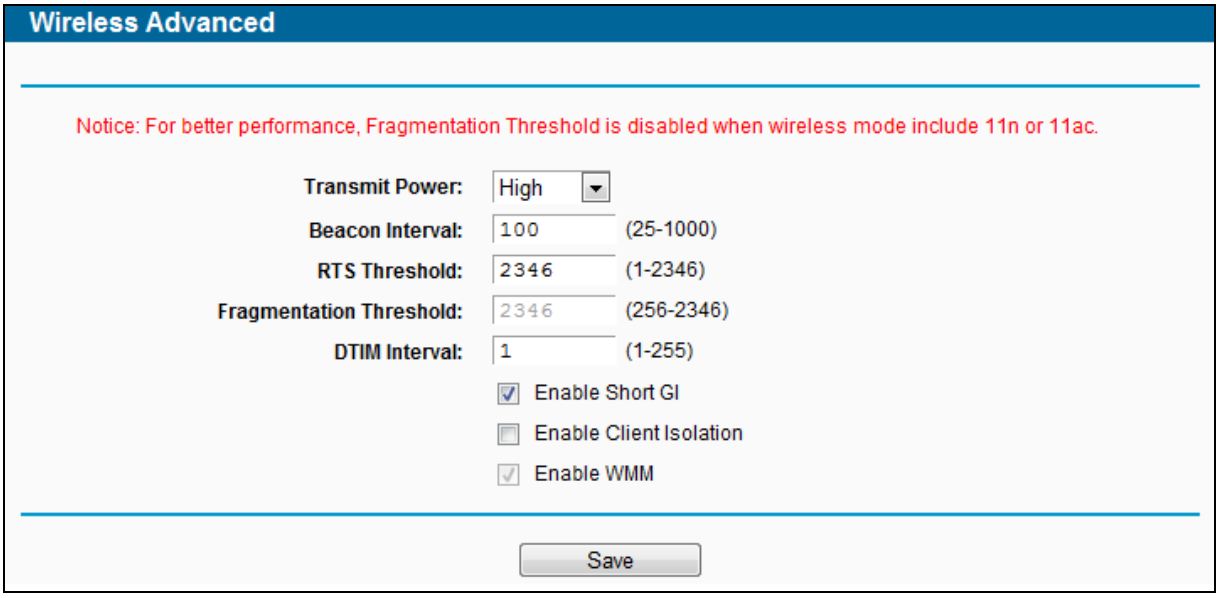


Figure 4-40 Wireless Advanced

- **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 20-1000 milliseconds for Beacon Interval here. The beacons are the packets sent by the router to synchronize a wireless network. Beacon Interval value determines the time interval of the beacons. The default value is 100.
- **RTS Threshold -** Here you can specify the RTS (Request to Send) Threshold. If the packet is larger than the specified RTS Threshold size, the router will send RTS frames to a particular receiving station and negotiate the sending of a data frame. The default value is 2346.
- **Fragmentation Threshold -** This value is the maximum size determining whether packets will be fragmented. Setting the Fragmentation Threshold too low may result in poor network performance because of excessive packets. 2346 is the default setting and is recommended.
- **DTIM Interval -** This value determines the interval of the Delivery Traffic Indication Message (DTIM). A DTIM field is a countdown field informing clients of the next window for listening to broadcast and multicast messages. When the router has buffered broadcast or multicast messages for associated clients, it sends the next DTIM with a DTIM Interval value. You can specify the value between 1-15 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.

4.7.6 Wireless Statistics

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

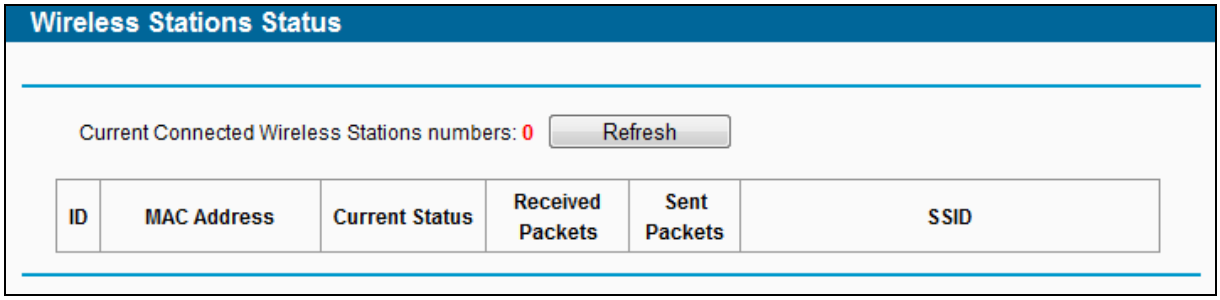


Figure 4-41 Wireless Statistics

- **MAC Address -** The connected wireless station's MAC address.
- **Current Status -** The connected wireless station's running status,
- **Received Packets -** Packets received by the station.
- **Sent Packets -** Packets sent by the station.

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

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

☞ **Note:**

This page will be refreshed automatically every 5 seconds.

4.8 Guest Network

Choose "**Guest Network**", and you can configure the Guest Network Wireless Settings on the page as shown in Figure 4-42.

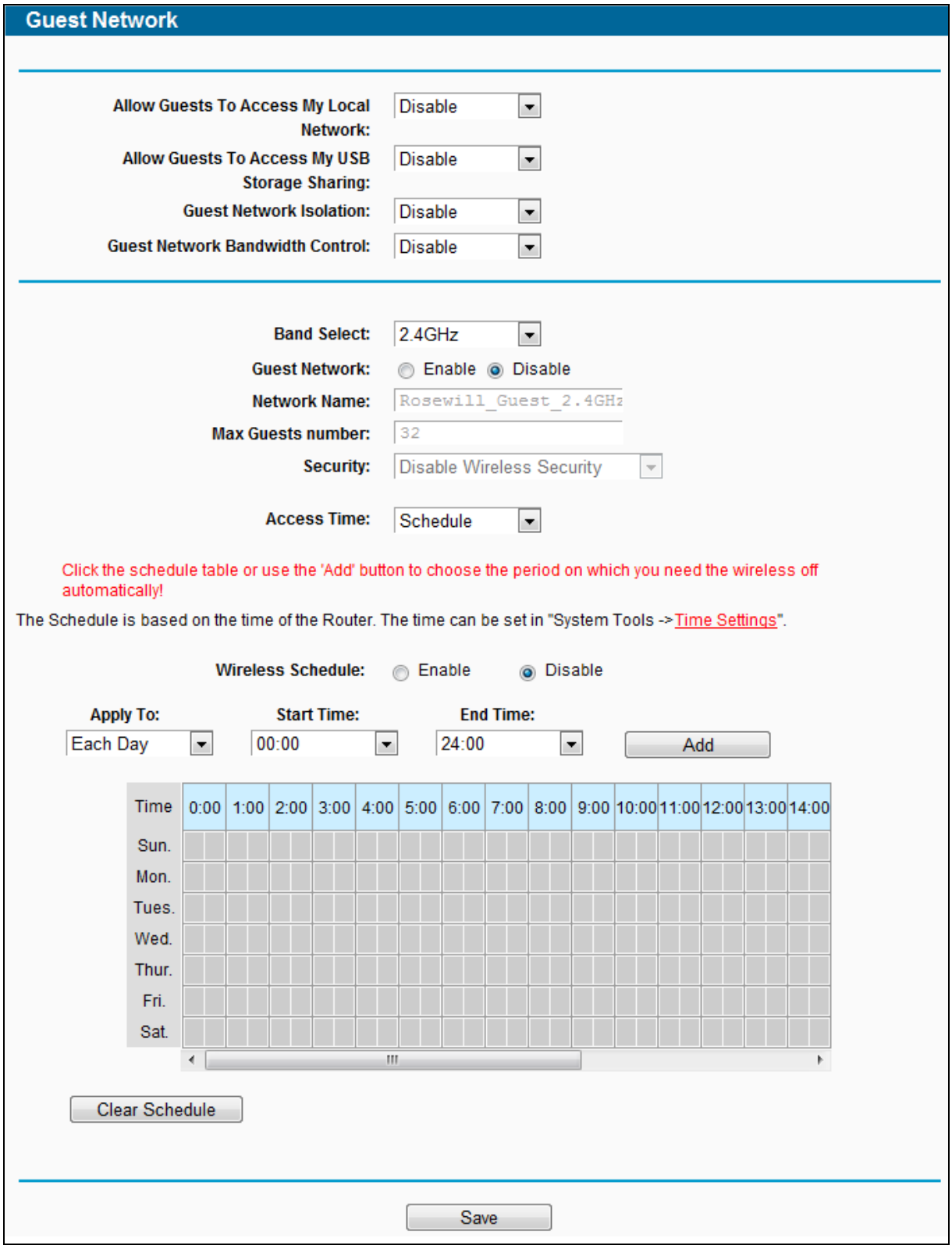


Figure 4-42 Guest Network Wireless Settings

- **Allow Guest To Access My Local Network** - If enabled, guests can communicate with hosts.
- **Allow Guest To Access My USB Storage Sharing** - If enabled, guests can access to USB

storage sharing servers.

- **Guest Network Isolation** -. If enabled, guests are isolated from each other.
- **Guest Network Bandwidth Control** - If enabled, the Guest Network Bandwidth Control rules will take effect.
- **Band Select/Guest Network** – Select the wireless network band (2.4G/5G) and enabled or disable its Guest Network function.
- **Network Name** - Enter a value of up to 32 characters. The same Name (SSID) must be assigned to all wireless devices in your Guest Network.
- **Max Guest number –** The maximum of guests at the same time,
- **Security** - You can configure the security of Guest Network here.
- **Access Time** - During this time the wireless stations could accessing the AP.

☞ **Note:**

The range of bandwidth for Guest Network is calculated according to the setting of Bandwidth Control on the page "Bandwidth Control->Control Settings".

4.9 DHCP

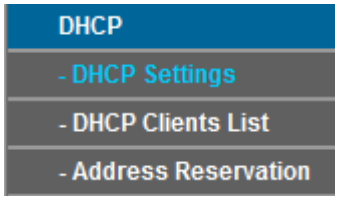


Figure 4-43 The DHCP menu

There are three submenus under the DHCP menu (shown in Figure 4-43): **DHCP Settings**, **DHCP Clients List** and **Address Reservation**. Click any of them, and you will be able to configure the corresponding functions.

4.9.1 DHCP Settings

Choose menu "**DHCP → DHCP Settings**", you can configure the DHCP Server on the page as shown in Figure 4-44.The router is set up by default as a DHCP (Dynamic Host Configuration Protocol) server, which provides the TCP/IP configuration for all the PC(s) that are connected to the router on the LAN.

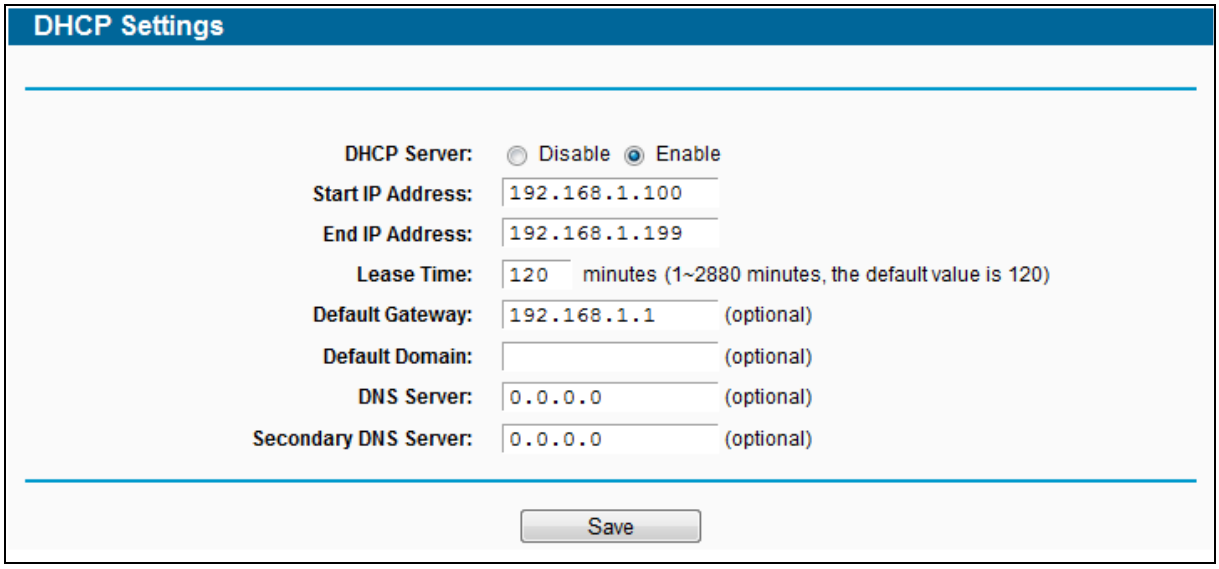


Figure 4-44 DHCP Settings

- **DHCP Server - Enable** or **Disable** the DHCP server. If you disable the Server, you must have another DHCP server within your network, otherwise you must configure the computer manually.
- **Start IP Address -** Specify an IP address for the DHCP Server to start with when assigning IP addresses. 192.168.1.100 is the default start address.
- **End IP Address -** Specify an IP address for the DHCP Server to end with when assigning IP addresses. 192.168.1.199 is the default end address.
- **Lease Time –** The **Lease Time** is the amount of time a network user will be allowed connection to the router with their current dynamic IP Address. Enter the amount of time in minutes and the user will be "leased" this dynamic IP Address. After the time is up, the user will be automatically assigned a new dynamic IP address. The range of the time is 1 ~ 2880 minutes. The default value is 120 minutes.
- **Default Gateway -** (Optional.) It is suggested to input the IP address of the LAN port of the router. The default value is 192.168.1.1.
- **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".

4.9.2 DHCP Clients List

Choose menu "**DHCP → DHCP Clients List**", you can view the information about the clients attached to the router in the screen as shown in Figure 4-45.

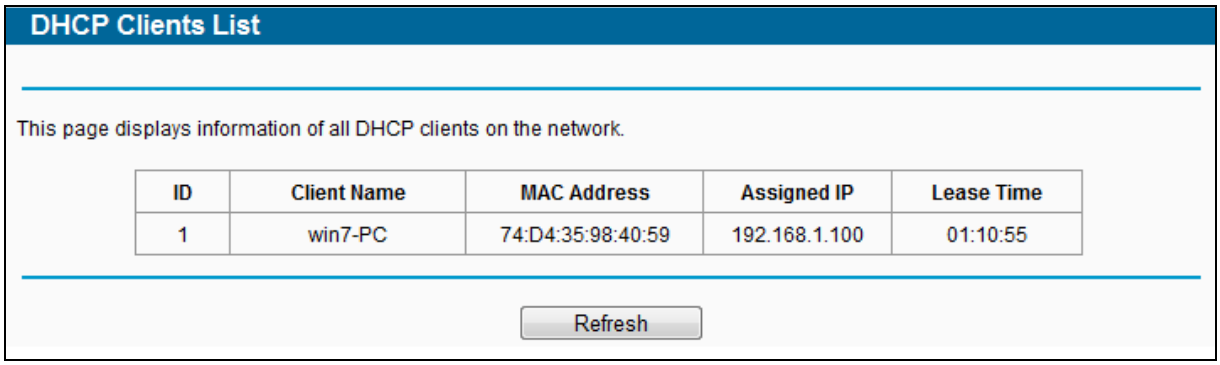


Figure 4-45 DHCP Clients List

- **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.

4.9.3 Address Reservation

Choose menu "**DHCP → Address Reservation**", you can view and add a reserved address for clients via the next screen (shown in Figure 4-46). When you specify a reserved IP address for a PC on the LAN, that PC will always receive the same IP address each time when it accesses the DHCP server. Reserved IP addresses should be assigned to the servers that require permanent IP settings.

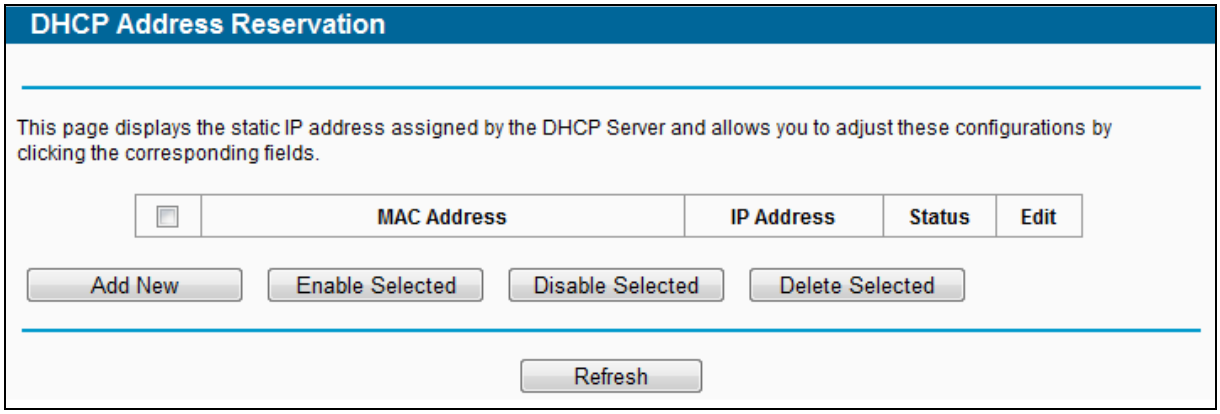


Figure 4-46 Address Reservation

- **MAC Address -** The MAC address of the PC for which you want to reserve an IP address.
- **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 4-47 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.

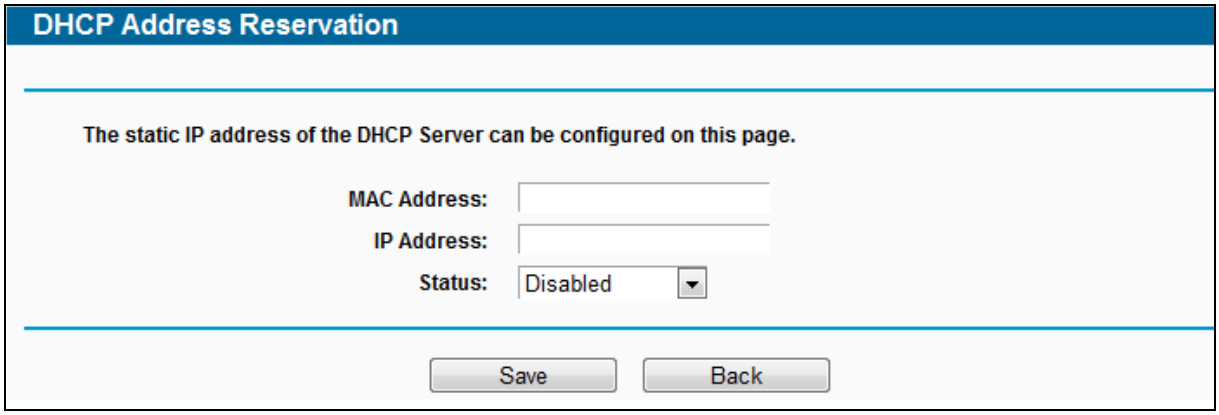


Figure 4-47 Add or Modify an Address Reservation Entry

To modify or delete an existing entry:

1. Click the **Edit** 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 Selected** button to make selected entries enabled/disabled

Click the **Delete Selected** button to delete selected entries.

4.10 USB Settings

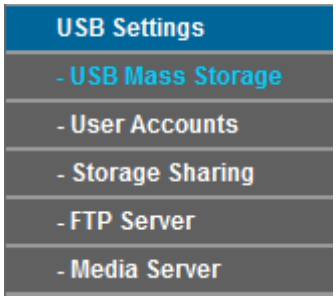


Figure 4-48 The USB Settings menu

There are six submenus under the USB Settings menu (shown in Figure 4-48): **USB Mass Storage**, **User Accounts**, **Storage Sharing**, **FTP Server** and **Media Server**. Click any of them, and you will be able to configure the corresponding functions.

4.10.1 USB Mass Storage

The **USB Mass Storage** page provides the basic information about the USB mass storage device. Click the **Refresh** button to update this page.

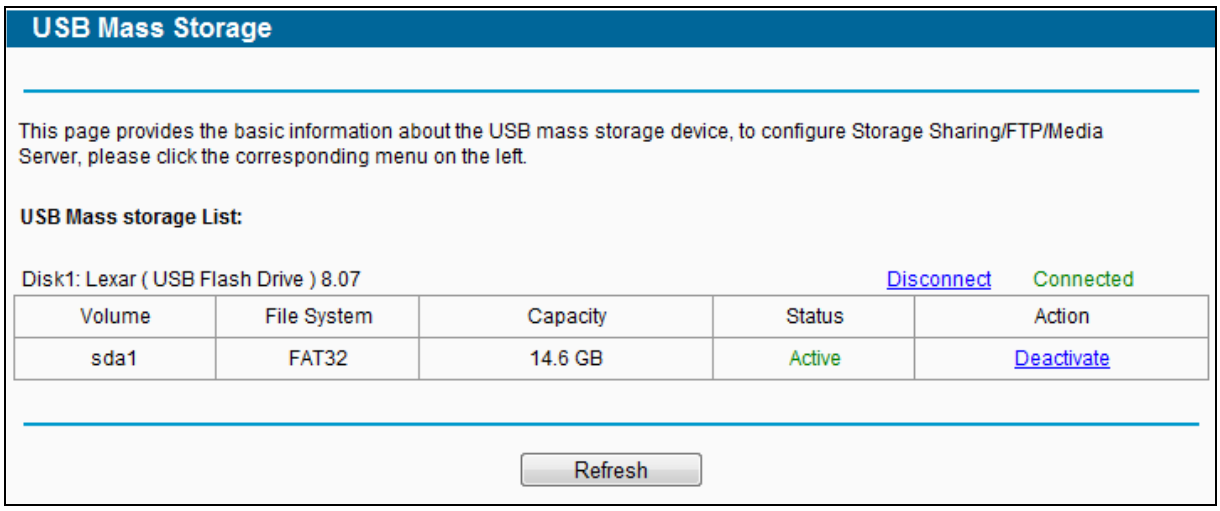


Figure 4-49 User Account Management

4.10.2 User Accounts

You can specify the user name and password for Storage Sharing and FTP Server users on this page. Storage Sharing users can use Internet Explorer to access files on the USB drive. FTP Server users can log into the FTP Server via FTP Client.

The default user account is **admin**. It has read/write access to Storage Sharing and can access FTP Server.

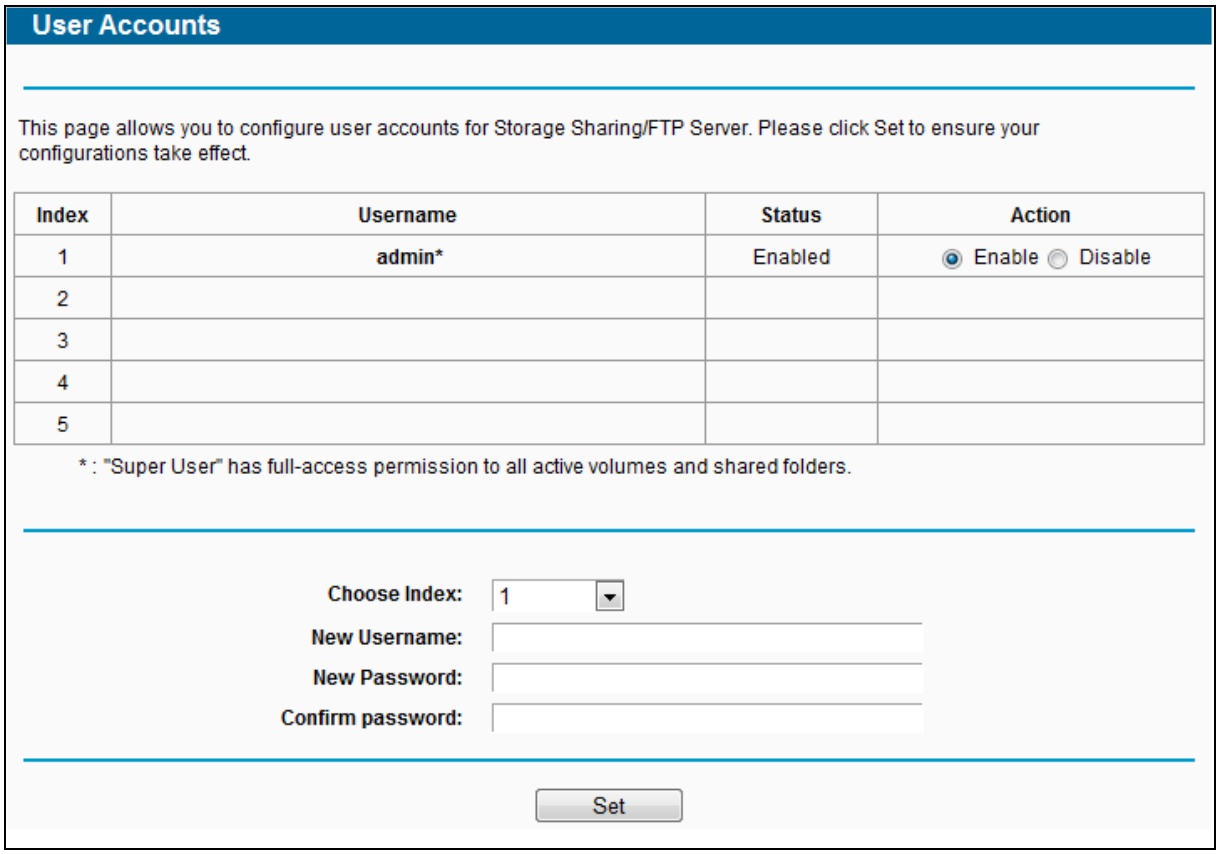


Figure 4-50 User Account Management

Only Administrator can use a Web browser to transfer the files from a PC to the Writable shared volume on the USB drive.

To add a new user account, please follow the steps below:

1. Choose the **Index** from the drop-down list.
2. Self-define a **User Name**.
3. Enter the password in the **Password** field.
4. Re-enter the password in the **Confirm Password** field.
5. Click **Set** to make your settings take effect.

- **New Username -** Type the user name that you want to give access to the USB drive. The user name must be composed of alphanumeric symbols not exceeding 15 characters in length.
- **New Password -** Enter the password in the Password field. The password must be composed of alphanumeric symbols not exceeding 15 characters in length. For security purposes, the password for each user account is not displayed.
- **Confirm Password -** Re-enter the password here.

Note:

1. Please restart the service for the new settings to take effect.
2. If you cannot use the new user name and password to access the shares, press **Windows logo + R** to open the Run dialog box and type **net use \\192.168.1.1 /delete /yes** and press Enter. (192.168.1.1 is your router's LAN IP address. If the LAN IP of the modem connected with your router is 192.168.1.x, the default LAN IP of the router will automatically switch from 192.168.1.1 to 192.168.0.1 to avoid IP conflict; in this case, please try **net use \\192.168.0.1 /delete / yes**.)

4.10.3 Storage Sharing

Choose menu "**USB Settings→Storage Sharing**", you can configure a USB disk drive attached to the router and view volume and share such properties as share name, directory, user access, and status on this page as shown below.

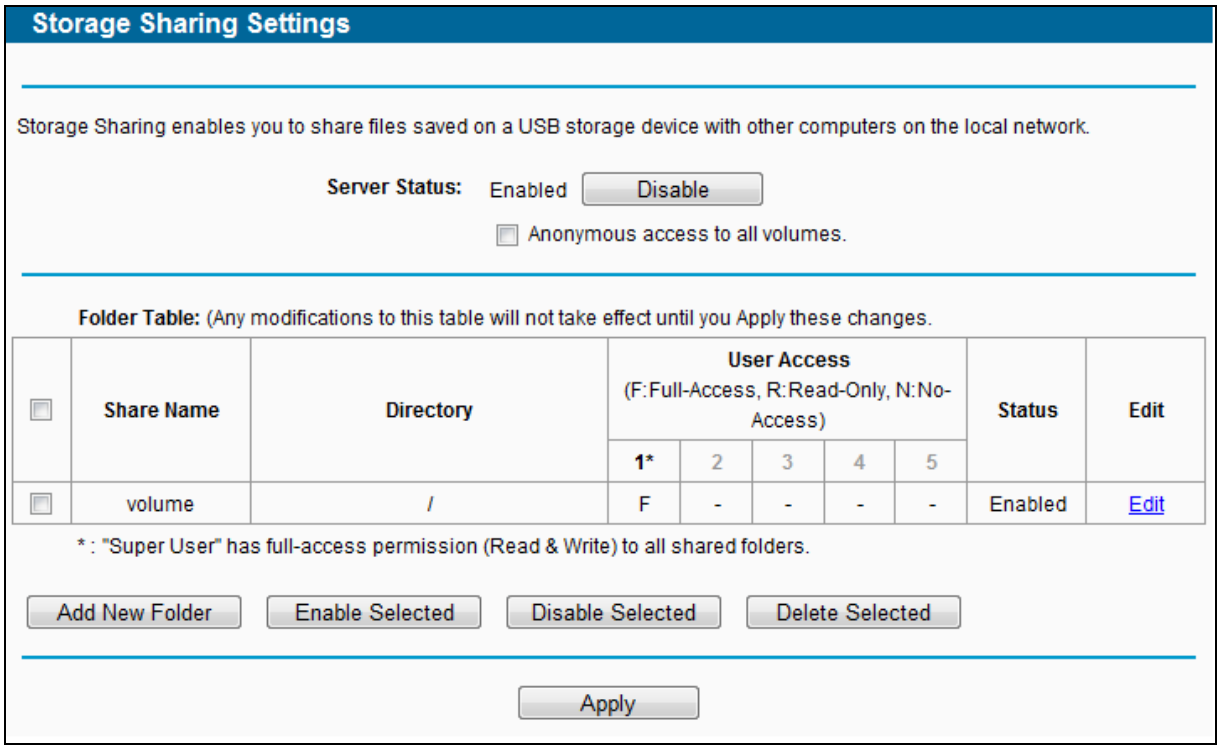


Figure 4-51 Storage Sharing

- **Server Status -** Indicates the Storage Sharing server's current status. You can click the **Enable** button to start the Storage Sharing service and click the **Disable** button to stop it.
- **Anonymous access to all volumes –** Check this box to allow users to access to all volumes without username or password
- **Shared Name -** The volume name of the USB drive the users have access to.
- **Directory -** The directory of the shared folder.

- **User Access –** Indicates user access of the shared folder. F stands for fully access, R stands for read-only and N stands for no-access.
- **Status -** Indicates the shared or non-shared status of the volume.
- **Edit –** Click **Edit** to edit the entry.

To add a new folder, follow the instructions below.

1. Click **Add New Folder** in Figure 4-51.

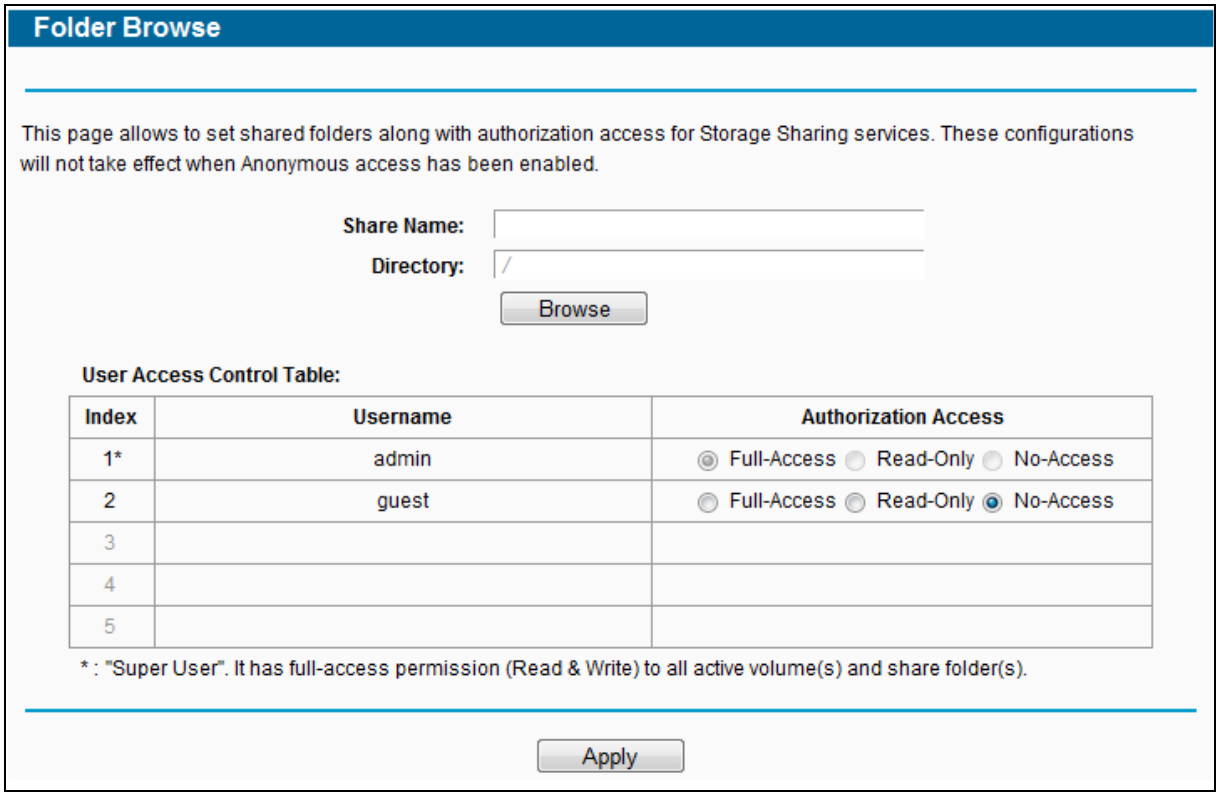


Figure 4-52 Add or Modify Share Folder

2. Enter display name of the share folder in **Shared Name** filed.
3. Click the **Browse** button to select the folder which you want to share.
4. Click the **Apply** button to save the settings.

☞ **Note:**

1. The max share folders number is 10. If you want to share a new folder when the number has reached 10, you can delete an existing share folder and then add a new one.
2. If you want to change the FTP settings, you need to restart FTP Server to make the changes take effect.

Click the **Enable Selected** button to make the selected entries enabled

Click the **Disable Selected** button to make the selected entries disabled.

Click the **Delete Selected** button to delete the selected entries.

Click the **Apply** button to make the settings take effect.

4.10.4 FTP Server

Choose menu "**USB Settings→FTP Server**", you can create an FTP server that can be accessed from the Internet or your local network.

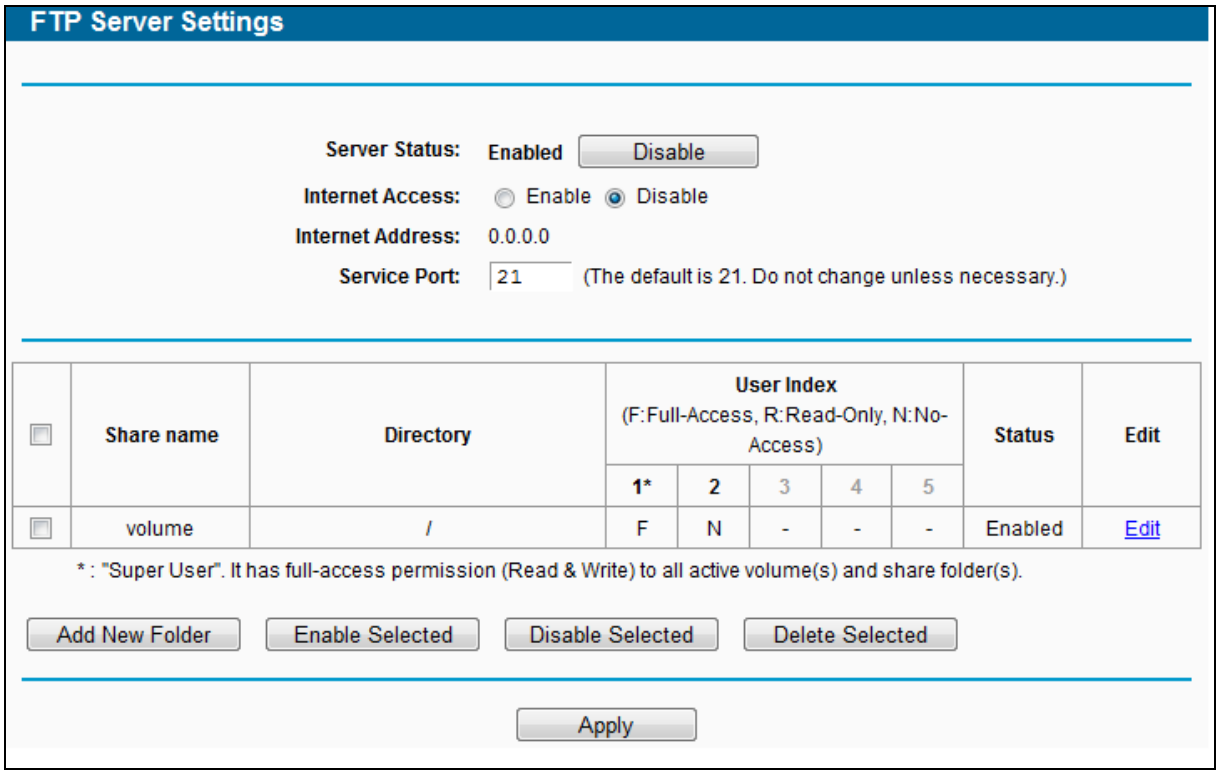


Figure 4-53 FTP Server Configuration

- **Server Status -** Indicates the FTP Server's current status.
- **Internet Access -** Select enable to allow access of the FTP server from the Internet. Otherwise, select disable to only allow local network access.
- **Internet Address** - The WAN IP address of this router,
- **Service Port -** Enter the FTP Port number to use. The default is 21.

To set up your FTP Server, please follow the instructions below:

1. Plug an external USB hard disk drive or USB flash drive into this router.
2. Click the **Enable/Disable** radio box to enable/disable Internet access to FTP from WAN port.
3. Specify a port for the FTP server to use (The default port number is 21).
4. The **Internet Address** displays the WAN IP address of this router, so that other users can access FTP via this address.

5. If WAN type is PPPoE/PPTP/L2TP, two connections will be available. Therefore, users can access FTP server via two connections. Users in a private LAN can access ftp server via **Public Address** while Internet users can access ftp server via **Internet Address**.

6. Click the **Apply** button to start the ftp server.

To add a new folder, follow the instructions below.

1. Click **Add New Folder** in Figure 4-53.

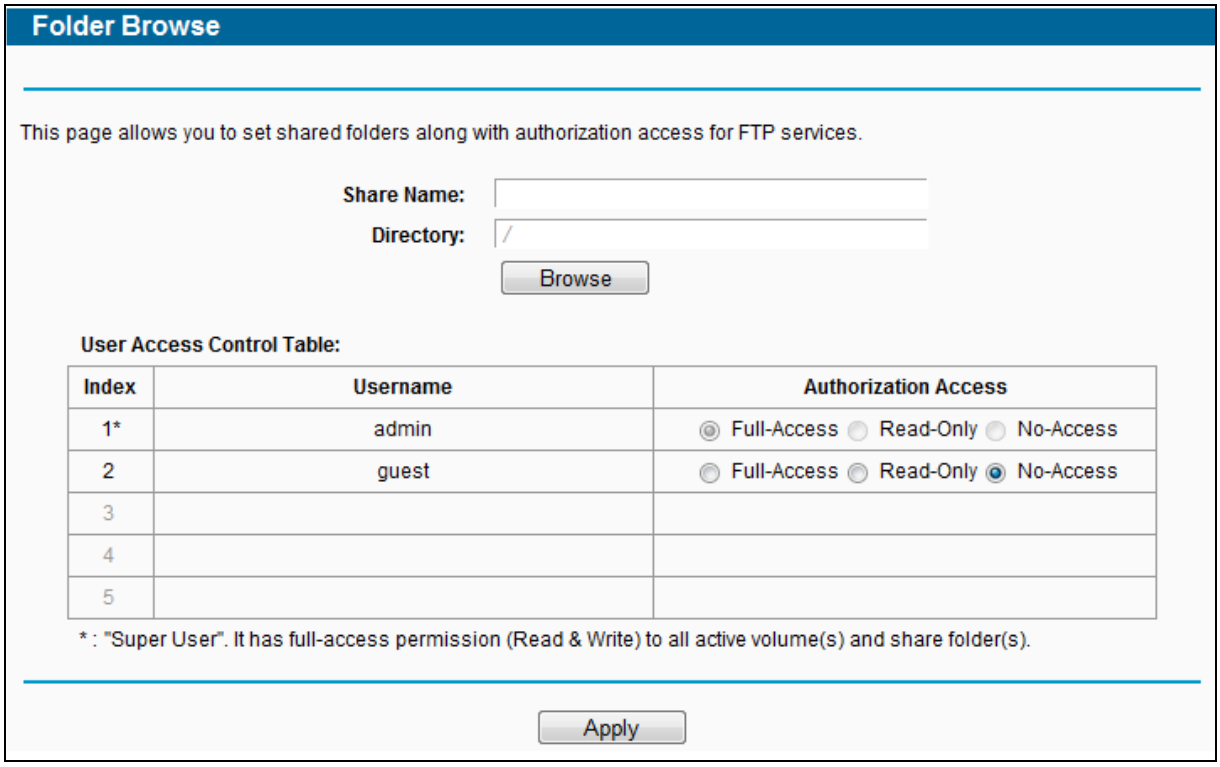


Figure 4-54 Add or Modify Share Folder

2. Enter display name of the share folder in **Shared Name** filed.

3. Click the **Browse** button to select the folder which you want to share.

4. Click the **Apply** button to save the settings.

☞ **Note:**

1. The max share folders number is 10. If you want to share a new folder when the number has reached 10, you can delete an existing share folder and then add a new one.
2. If you want to change the FTP settings, you need to restart FTP Server to make the changes take effect.

4.10.5 Media Server

Choose menu "**USB Settings→Media Server**", you can create media server that allows you to share stored content with other computers and devices on your home network and on the Internet.

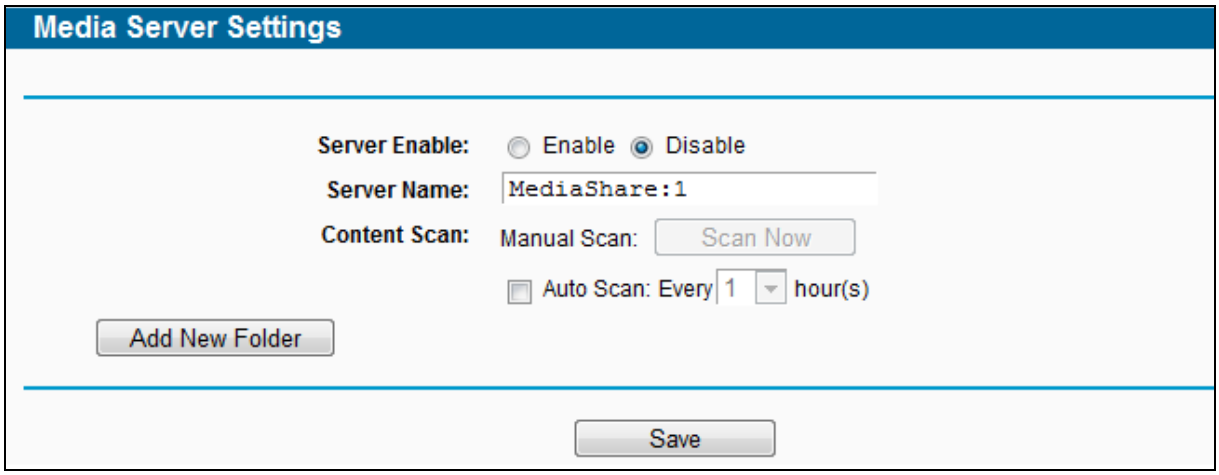


Figure 4-55 Media Server Setting

- **Server Enable** - Indicates the Media Server's current status, started or stopped. You can click the **Enable** button to enable the Media Server and click the **Disable** button to disable it.
- **Server Name -** The name of this Media Server.
- **Share Name** - The display name of this folder.
- **Folder Name** - The real full path of the specified folder.
- **Delete** - You can delete the share folder by click **Delete**.

To set up your media server, please follow the instructions below:

1. Plug an external USB hard disk drive or USB flash drive into this router, and then click the **Enable** button to start the media server. The screen will appear as shown in Figure 4-56.

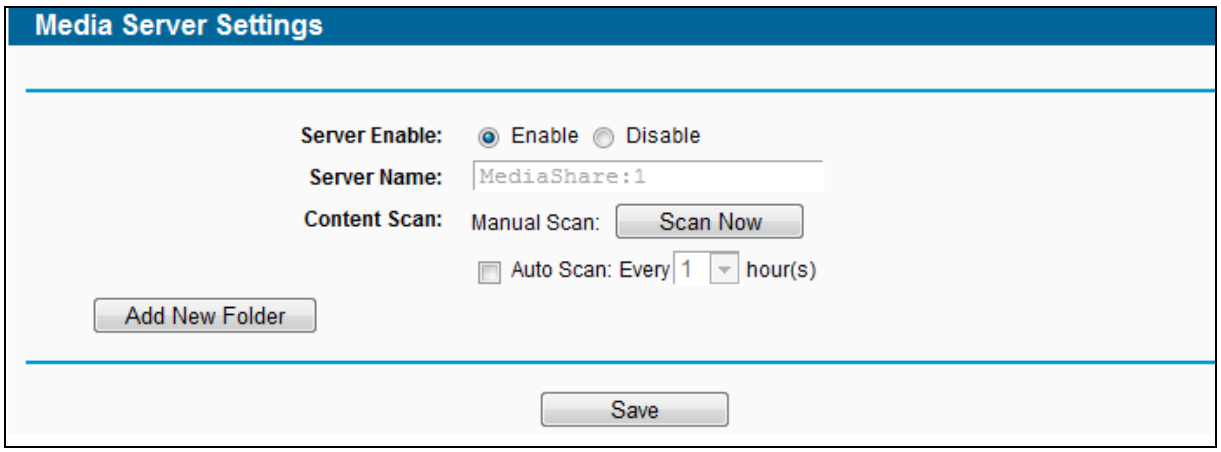


Figure 4-56 Media Server Setting

2. Click the **Add New Folder** button to specify a folder as the search path of media server. The screen will then appear as shown in Figure 4-57.

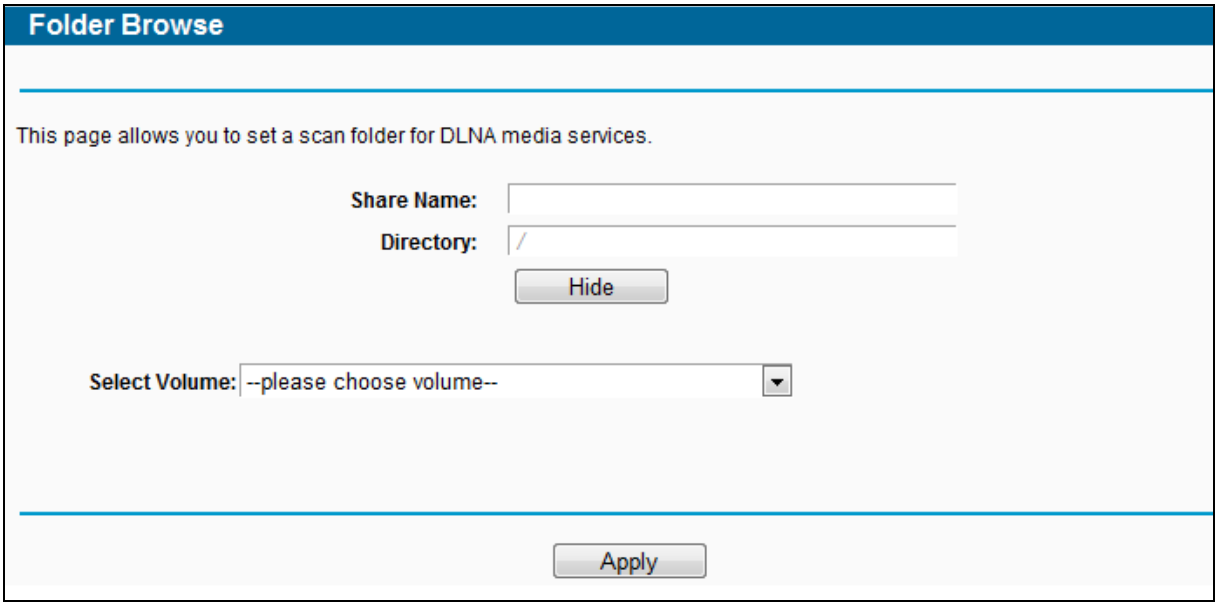


Figure 4-57 Add New Folder

- **Share Name** - You can enter a display name for the share folder.
- **Directory** - Displays the location of this folder.
- **Browse** – Click the button to select the folder to share.
- **Apply** - Click the button to save your settings.

3. Click the **Scan Now** button to scan all the share folders immediately. You can also select the **Auto-scan**, at the same time, select an auto scan interval time by drop-down list. In this case, the media server will auto scan the share folders.

☞ **Note:**

The max share folders number is 6. If you want share a new folder when the number has been reached to be 6, you can delete a share folder and then add a new one.

4.11 NAT

Choose "**NAT**", and you can enable or disable the NAT and Hardware NAT Control feature. The NAT Rules and Hardware NAT will work properly only when the NAT Control feature is enabled.

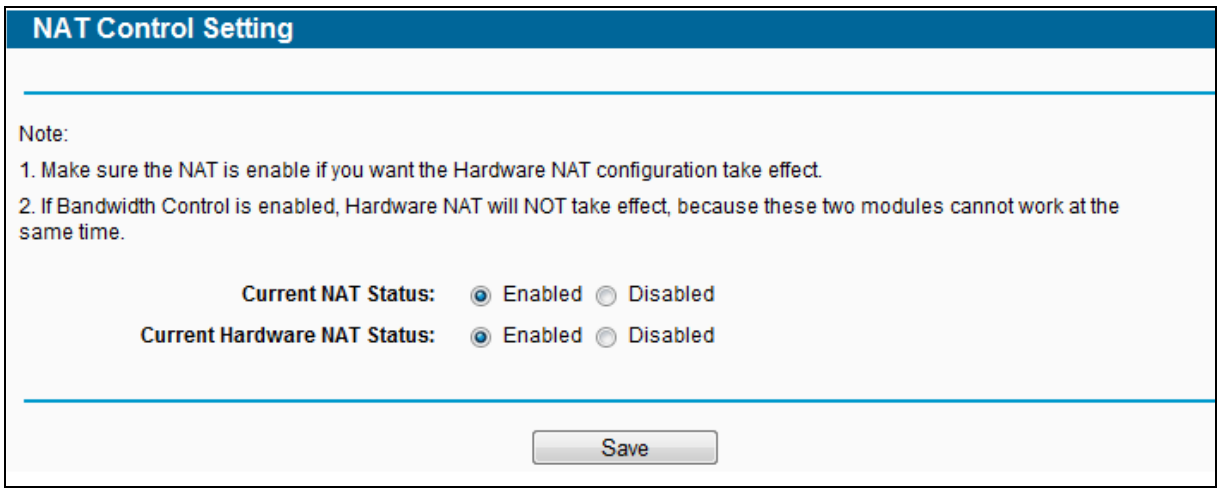


Figure 4-58 The Forwarding menu

- **Enable NAT Control** - If enabled, the NAT function and the Forwarding configuration will take effect.
- **Disable NAT Control** - If disabled, neither NAT function nor Forwarding configuration will take effect.
- **Enable Hardware NAT Control** - If enabled, the Hardware NAT feature will take effect.
- **Disable Hardware NAT Control** - If disabled, neither Hardware NAT feature will take effect.

4.12 Forwarding

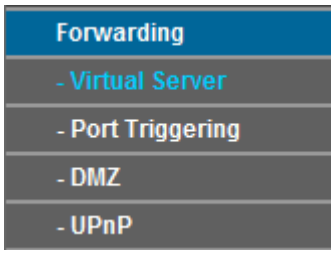


Figure 4-59 The Forwarding menu

There are four submenus under the Forwarding menu (shown in Figure 4-59): **Virtual Servers**, **Port Triggering**, **DMZ** and **UPnP**. Click any of them, and you will be able to configure the corresponding function.

4.12.1 Virtual Server

Choose menu "**Forwarding→Virtual Server**", and then you can view and add virtual servers on this page (shown in Figure 4-60). 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.

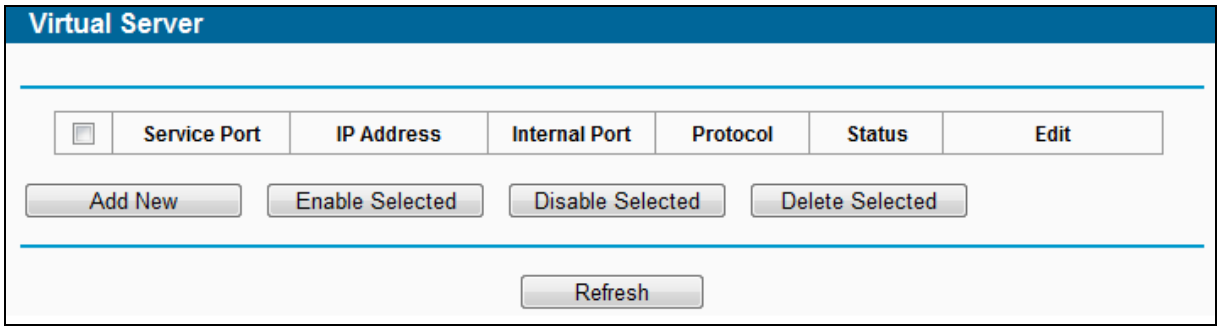


Figure 4-60 Virtual Servers

- **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).
- **IP Address** - The IP address of the PC running the service application.
- **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.
- **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.
- **Edit** - To edit or delete an existing entry.

To setup a virtual server entry:

1. Click the **Add New** button. (pop-up Figure 4-61)
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.

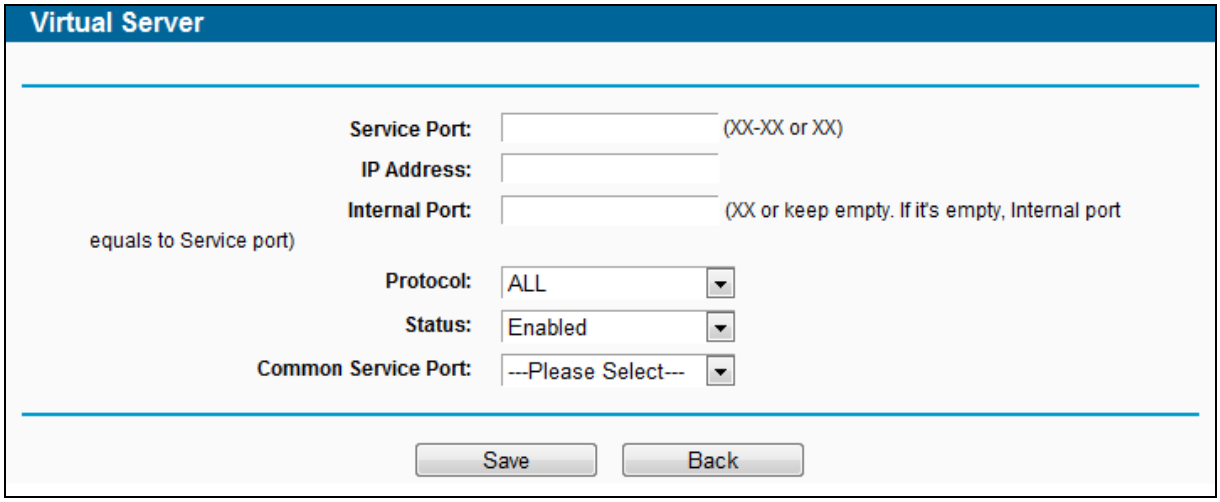


Figure 4-61 Add or Modify a Virtual Server Entry

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 **Edit** or **Delete** as desired on the **Edit** column.

Click the **Enable/ Disable Selected** button to make selected entries enabled/ disabled.

Click the **Delete Selected** button to delete selected entries.

Note:

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

4.12.2 Port Triggering

Choose menu "**Forwarding→Port Triggering**", you can view and add port triggering entry on this page (shown in Figure 4-62). Some applications require multiple connections, like Internet games, video conferencing, Internet telephoning and so on. Port Triggering is useful for those applications that cannot work with a pure NAT router.

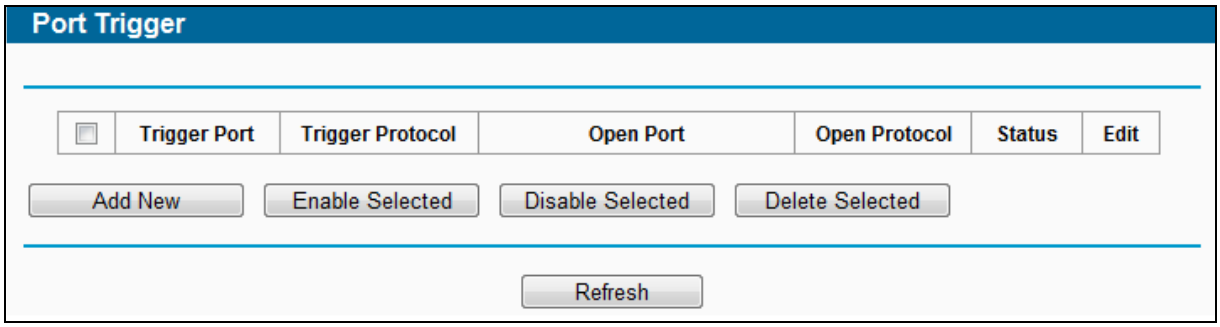


Figure 4-62 Port Triggering

- **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).
- **Open Port** - The port or port range used by the remote system when it responds to the outgoing request. A response using one of these ports will be forwarded to the PC which triggered this rule. You can input at most 5 groups of ports (or port sections). Every group of ports must be separated with ",", for example, 2000-2038, 2046, 2050-2051, 2085, 3010-3030.
- **Open Protocol** - The protocol used for **Open 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.
- **Edit** - To modify or delete an existing entry.
- **Common Applications** - Some popular applications already listed in the drop-down list of **Incoming Protocol**.

To add a new rule, follow the steps below.

1. Click the **Add New** button, the next screen will pop-up as shown in Figure 4-63.
2. Select a common application from the **Common Applications** drop-down list, then the **Trigger Port** field and the **Open Port** field will be automatically filled. If the **Common Applications** do not have the application you need, enter the **Trigger Port** and the **Open Port** 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 **Open 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.

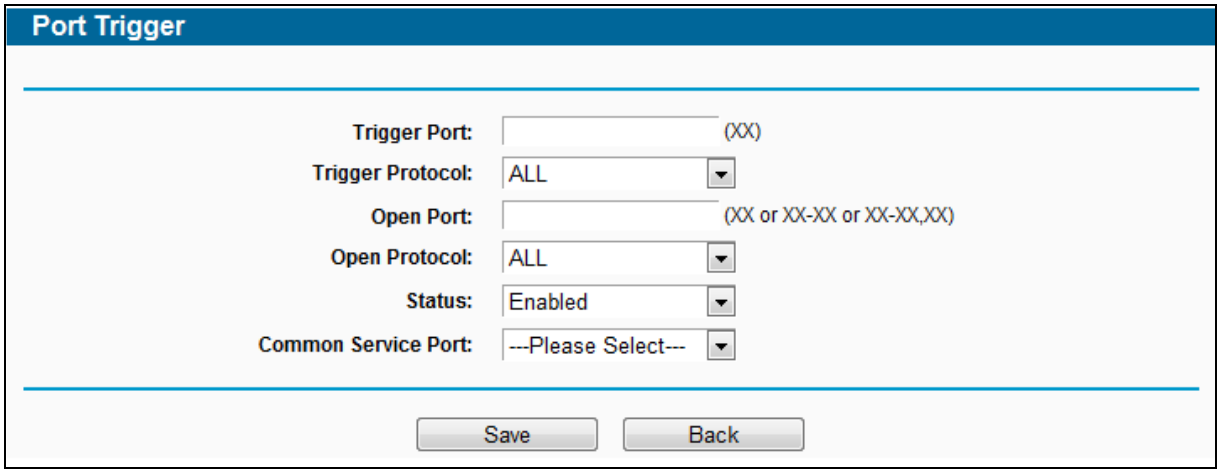


Figure 4-63 Add or Modify a Triggering Entry

To modify or delete an existing entry:

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

Click the **Enable Selected** button to make selected entries enabled.

Click the **Disable Selected** button to make selected entries disabled.

Click the **Delete Selected** button to delete selected 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 **Open 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. Open Ports ranges cannot overlap each other.

4.12.3 DMZ

Choose menu "**Forwarding→DMZ**", and then you can view and configure DMZ host in the screen (shown in Figure 4-64).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.

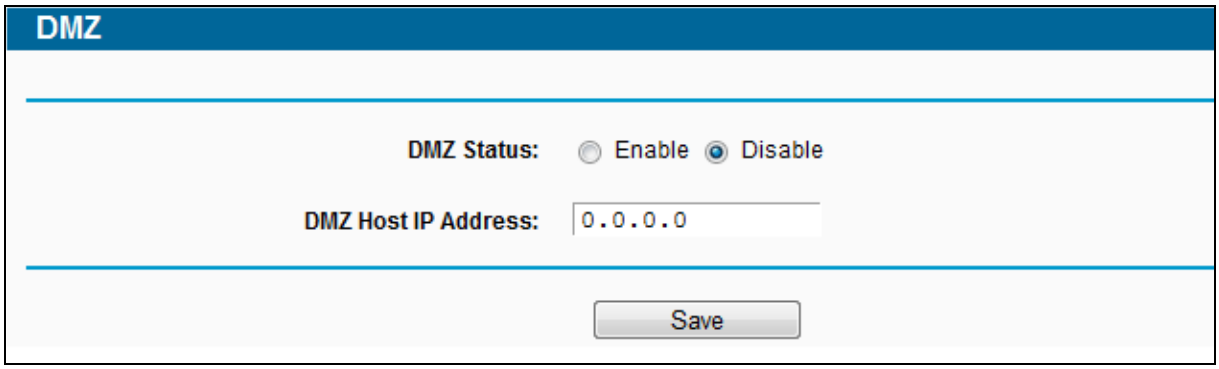


Figure 4-64 DMZ

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

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

4.12.4 UPnP

Choose menu "**Forwarding→UPnP**", and then you can view the information about **UPnP** in the screen (shown in Figure 4-65). The **Universal Plug and Play (UPnP)** feature allows the devices, such as Internet computers, to access the local host resources or devices as needed. UPnP devices can be automatically discovered by the UPnP service application on the LAN.

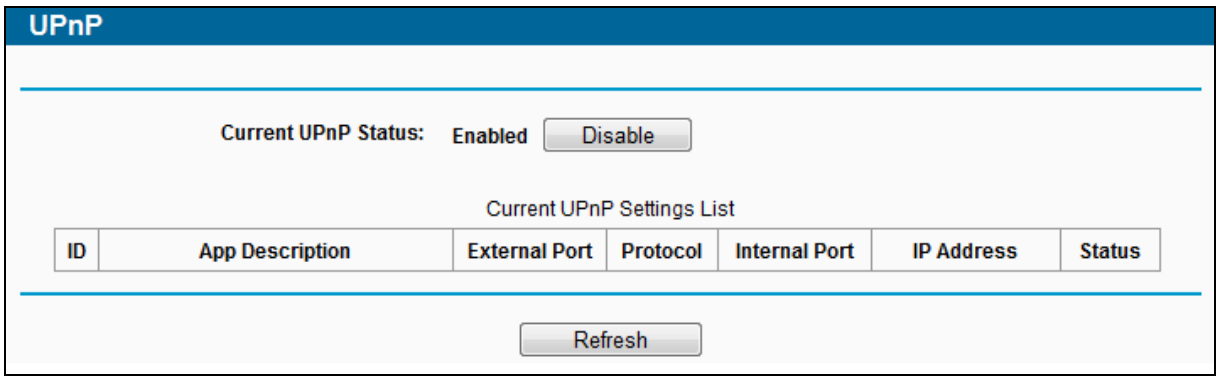


Figure 4-65 UPnP Setting

- **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.

4.13 Security

Figure 4-66 The Security menu

There are four submenus under the Security menu: **Basic Security**, **Advanced Security**, **Local Management** and **Remote Management**. (as shown in Figure 4-66). Click any of them, and you will be able to configure the corresponding functions.

4.13.1 Basic Security

Choose menu "**Security → Basic Security**", and then you can configure the basic security in the screen as shown in Figure 4-67.

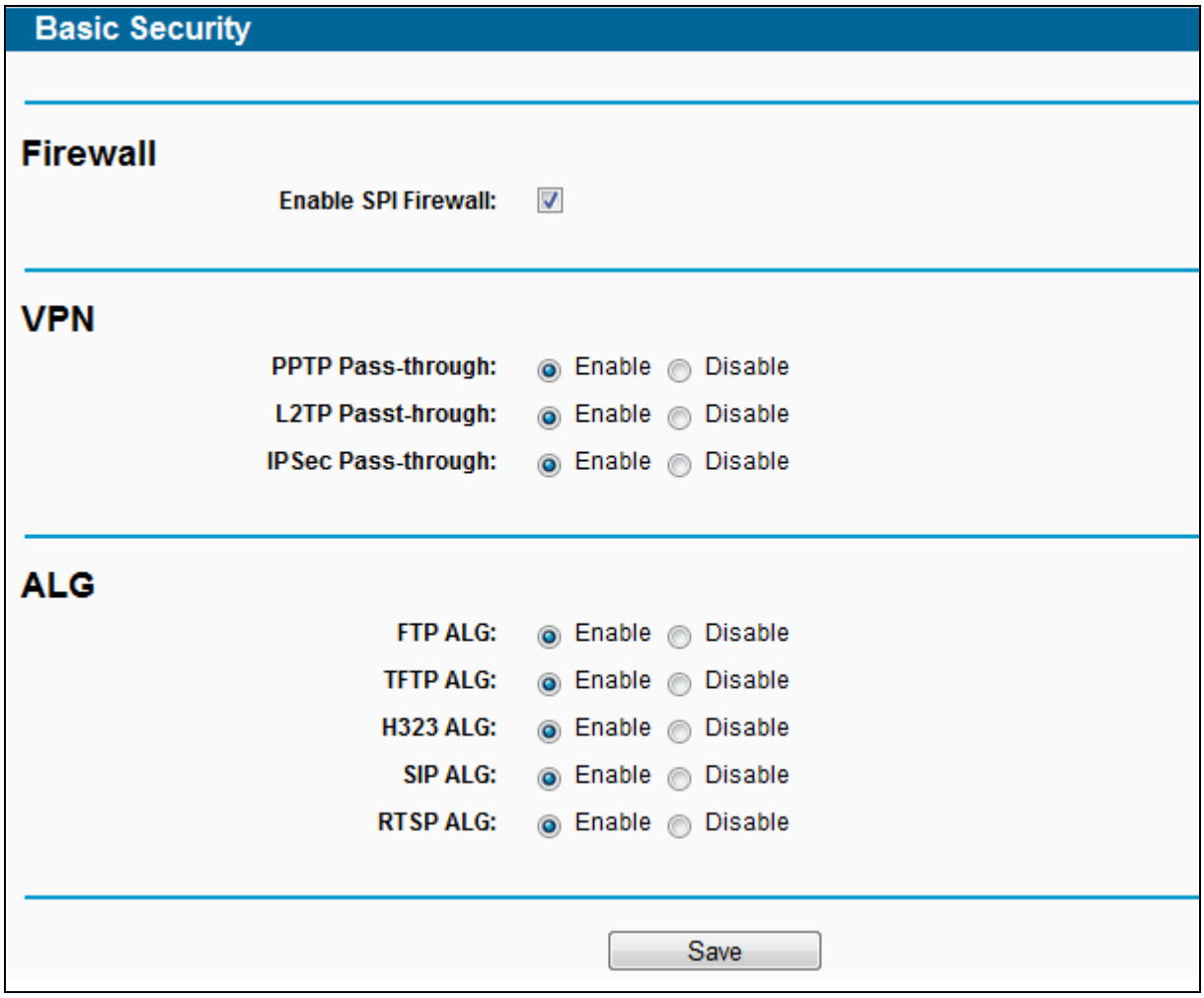


Figure 4-67 Basic Security

- **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**.
- **SIP ALG -** To allow SIP clients and servers to communicate across NAT, click **Enable.**
- **RTSP ALG** - To allow some media player clients to communicate with some streaming media servers across NAT, click **Enable**.

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

4.13.2 Advanced Security

Choose menu "**Security → Advanced Security**", and then you can protect the router from being attacked by TCP-SYN Flood, UDP Flood and ICMP-Flood in the screen as shown in Figure 4-68.

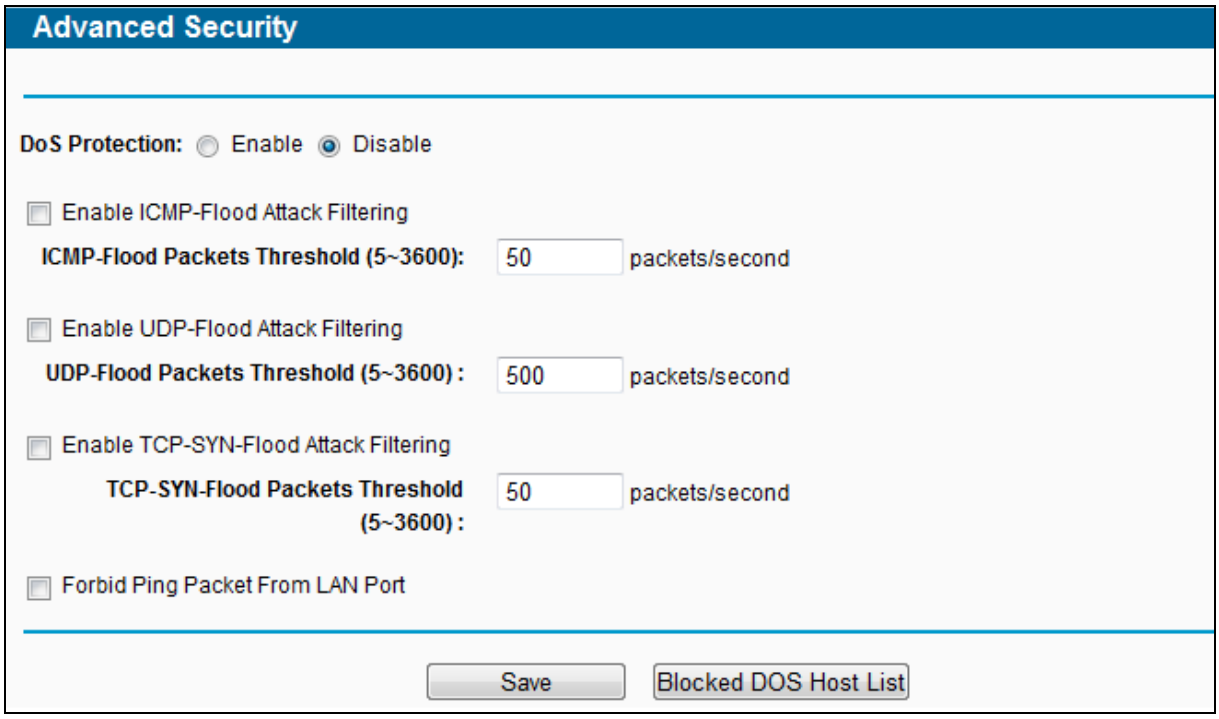


Figure 4-68 Advanced Security

- **DoS Protection -** Denial of Service protection. Check the Enable or Disable button to enable or disable the DoS protection function. Only when it is enabled, will the flood filters be enabled.

  ☞ **Note:**

  Dos Protection will take effect only when the **Traffic Statistics** in "**System Tool → 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.
- **Forbid Ping Packet From LAN Port -** Enable or Disable Forbid Ping Packet From LAN Port. The default setting is disabled. If enabled, the ping packet from LAN cannot access the router. This function can be used to defend against some viruses.

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

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

4.13.3 Local Management

Choose menu "**Security → Local Management**", and then you can configure the management rule in the screen as shown in Figure 4-69. The management feature allows you to deny computers in LAN from accessing the router.

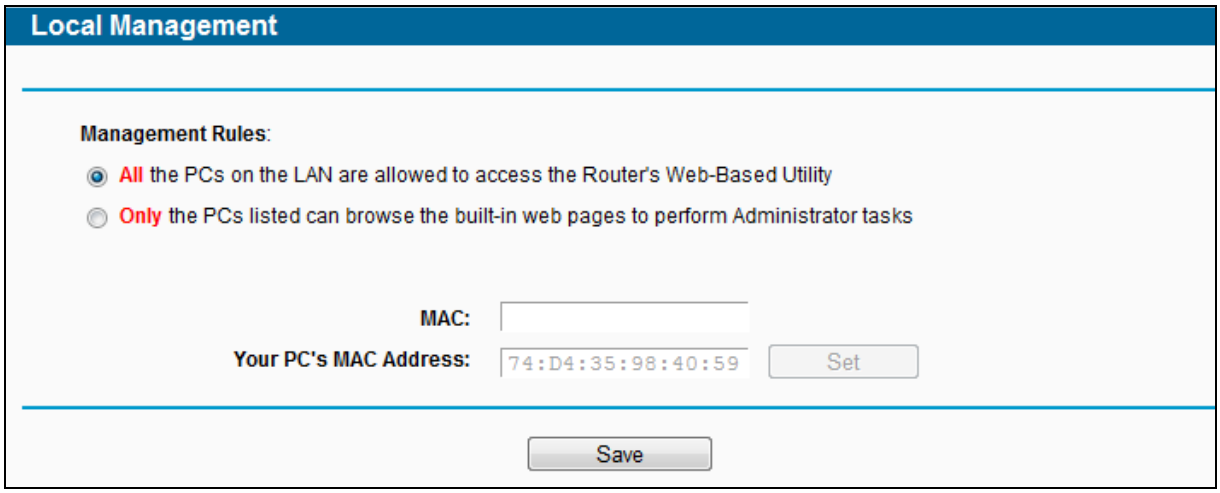


Figure 4-69 Local Management

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.

4.13.4 Remote Management

Choose menu "**Security → Remote Management**", and then you can configure the Remote Management function in the screen as shown in Figure 4-70. This feature allows you to manage your router from a remote location via the Internet.

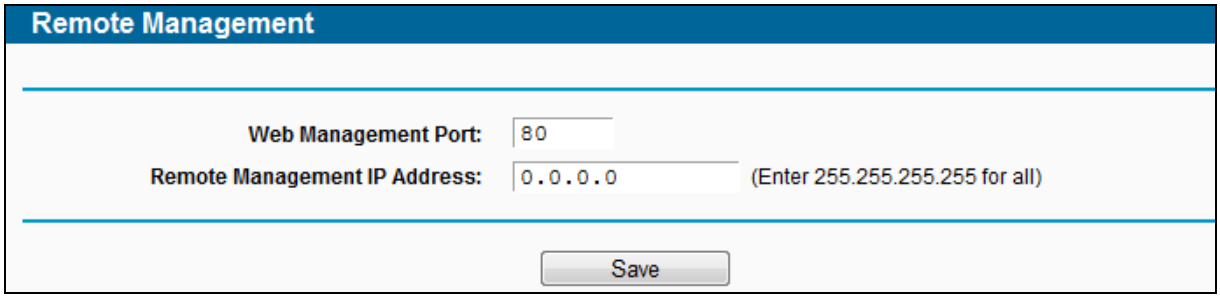


Figure 4-70 Remote Management

- **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 1024 and 65535 but do not use the number of any common service port.
- **Remote Management IP Address -** This is the current address you will use when accessing your router from the Internet. This function is disabled when the IP address is set to the default value of 0.0.0.0. To enable this function change 0.0.0.0 to a valid IP address. If set to 255.255.255.255, then all the hosts can access the router from internet.

☞ **Note:**

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

4.14 Parent Control

Choose menu "**Parent Control**", and then you can configure the parent control in the screen as shown in Figure 4-71. The Parent Control function can be used to control the Internet activities of the child, limit the child to access certain websites and restrict the time of surfing.

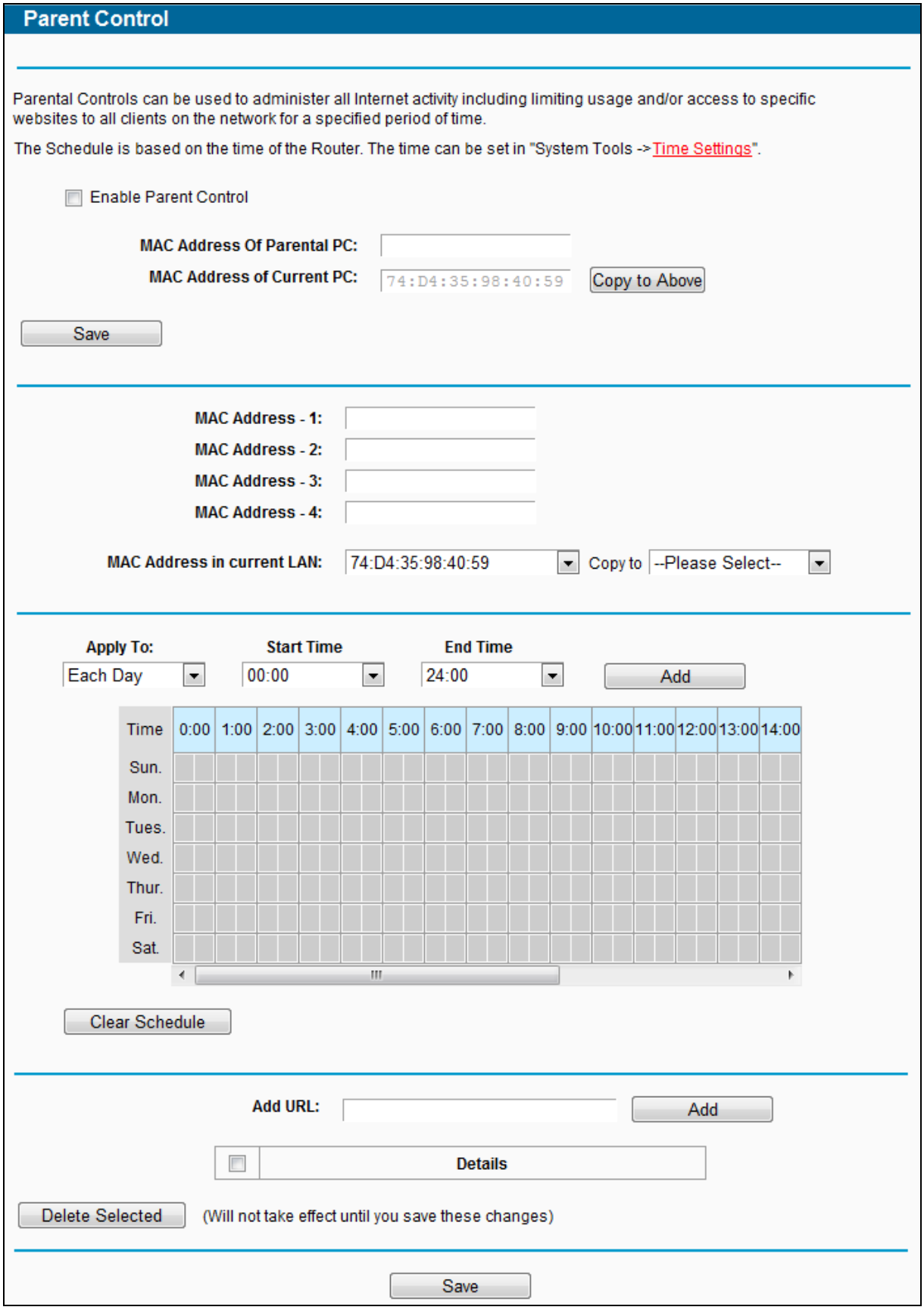


Figure 4-71 Parent Control Settings

➢ **Parent Control -** Check **Enable** if you want this function to take effect.

- **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 Current 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.

Click the **Save** button to make your settings take effect.

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

1. Check the **Enable Parent Control** box.
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 1-4** field, or you can choose the MAC address from the **MAC Address in current LAN** drop-down list.
3. Enter the allowed domain name of the website, either the full name or the keywords (e.g. google) in the **Add URL** field. Any domain name with keywords in it (www.google.com, www.google.com.hk) will be allowed. Click the **Add** button.
4. Set the time period allowed for the PC controlled to access the Internet. For detailed information, please go to "**Access Control → Schedule**".
5. Click the **Save** button.

Click the **Delete Selected** button to delete the selected entries in the table.

For example: If you desire that the child PC with MAC address 00:11:22:33:44:AA can access www.google.com on Saturday only while the parent PC with MAC address 00:11:22:33:44:BB is without any restriction, you should follow the settings below.

1. Click "**Parent Control**" menu on the left to enter the Parent 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 "**Parent Control**" menu on the left to go back to the Add or Modify Parent Control Entry page:
   1) Enter 00:11:22:33:44:AA in the **MAC Address 1** field.
   2) Create a new schedule with Day is Sat and Time is all day-24 hours. Click **Add**.
   3) Enter "www.google.com" in the **Add URL** field. Click **Add**.
3. Click **Save** to complete the settings.

   Then you will see the page as shown in Figure 4-72.

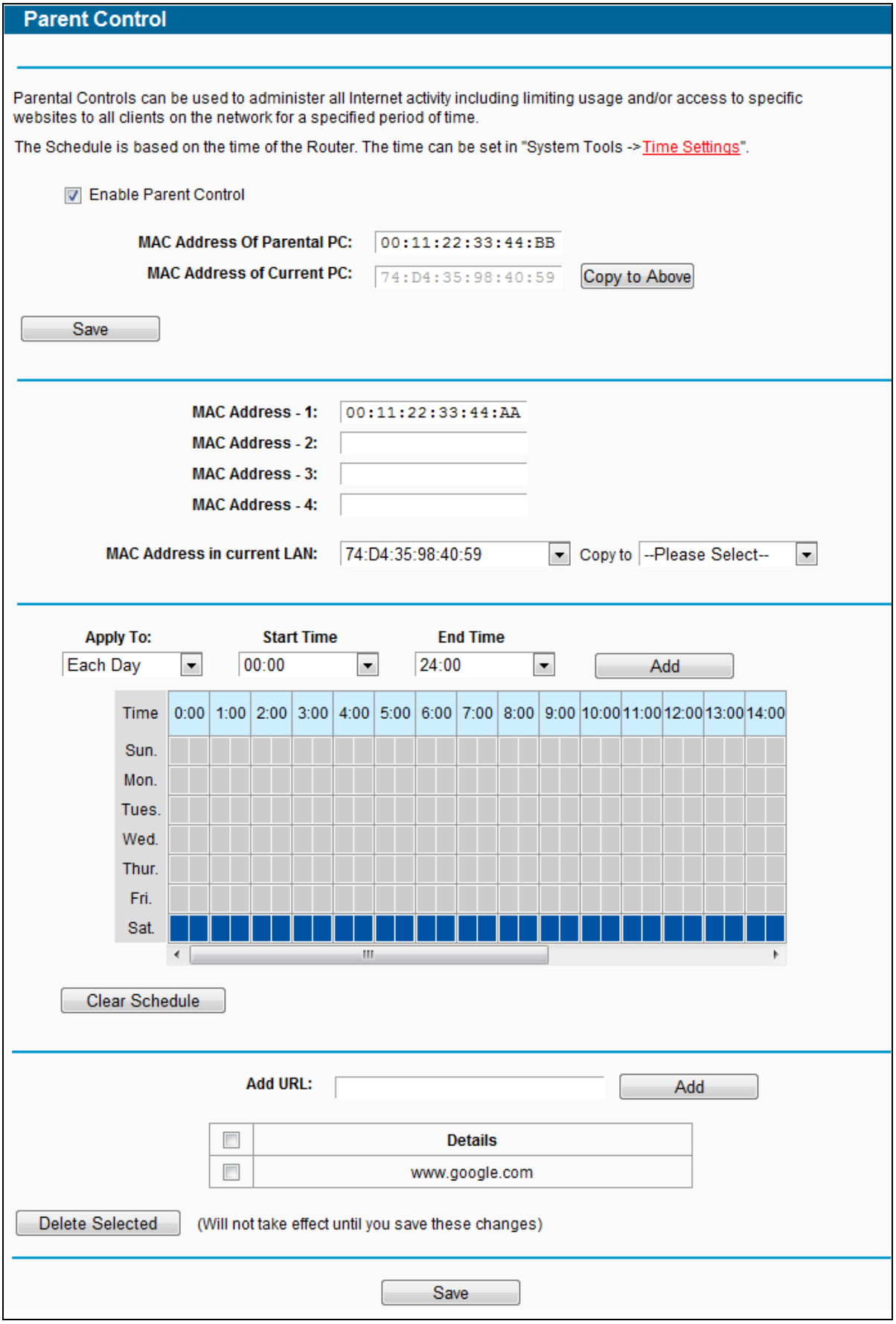


Figure 4-72 Parent Control Settings

4.15 Access Control

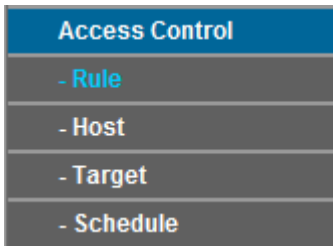


Figure 4-73 Access Control

There are four submenus under the Access Control menu: **Rule**, **Host**, **Target** and **Schedule** (as shown in Figure 4-73). Click any of them, and you will be able to configure the corresponding function.

4.15.1 Rule

Choose menu "**Access Control → Rule**", and then you can view and set Access Control rules in the screen as shown in Figure 4-74.

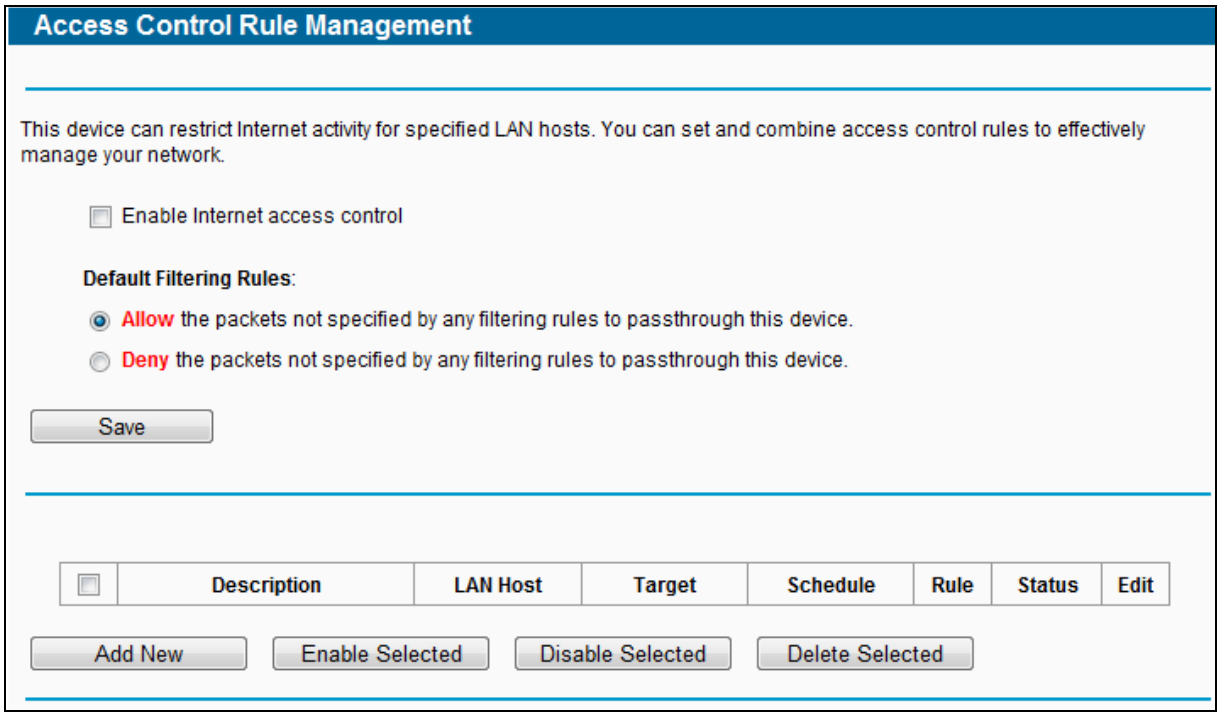


Figure 4-74 Access Control Rule Management

- **Enable Internet Access Control -** Select the check box to enable the Internet Access Control function, so the Default Filter Policy can take effect.
- **Description -** Here displays the name of the rule and this name is unique.
- **LAN Host -** Here displays the host selected in the corresponding rule.
- **Target -** Here displays the target selected in the corresponding rule.

- **Schedule -** Here displays the schedule selected in the corresponding rule.
- **Enable -** Here displays the status of the rule, enabled or not. Check this option to enable a specific entry.
- **Edit -** Here you can edit or delete an existing rule.
- **Add New -** Click the **Add New** button to add a new rule entry.
- **Enable Selected -** Click the **Enable Selected** button to enable selected rules in the list.
- **Disable Selected -** Click the **Disable Selected** button to disable selected rules in the list.
- **Delete Selected -** Click the **Delete Selected** button to delete selected entries in the table.

How to add a new rule:

1. Click the **Add New** button and the next screen will pop up as shown in Figure 4-75.
2. Give a name (e.g. Rule_1) for the rule in the **Description** field.
3. Select a host from the **LAN Host** drop-down list or click "**Add LAN Host**".
4. Select a target from the **Target** drop-sown list or click "**Add Target**".
5. Select a schedule from the **Schedule** drop-down list or click "**Add Schedule**".
6. In the **Status** field, select **Enabled** or **Disabled** to enable or disable your entry.
7. In the **Direction** field, select **IN** or **OUT**.
8. Select a schedule from the **Protocol** drop-down list.
9. Click the **Save** button.

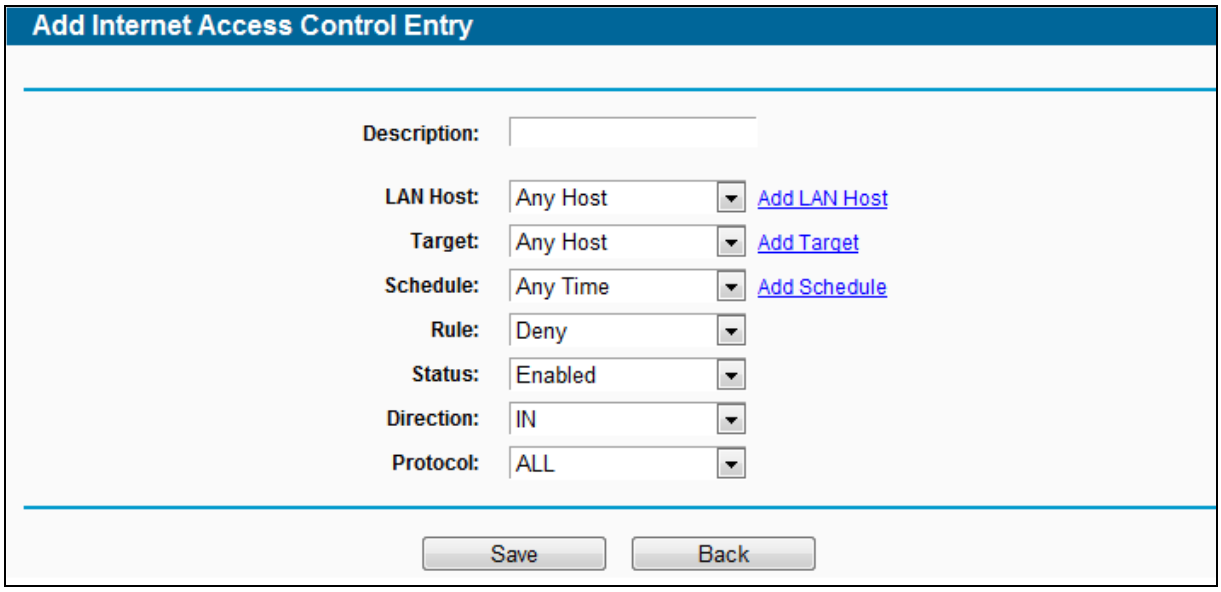
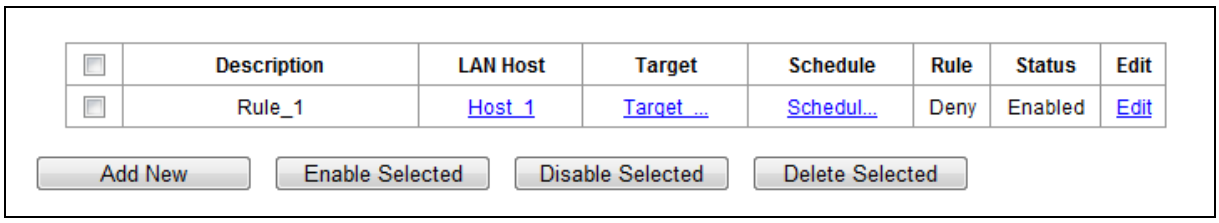


Figure 4-75 Add Internet Access Control Entry

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

1. Click the submenu **Rule of Access Control** in the left to return to the Rule List page. Select **Enable Internet Access Control** and choose "**Allow the packets specified by any enabled access control policy to pass through the router**".
2. We recommend that you click **Add New** button to finish all the following settings.
3. Click the submenu **Host of Access Control** in the left to enter the Host List page. Add a new entry with the Host Description is Host_1 and MAC Address is 00:11:22:33:44:AA.
4. Click the submenu **Target of Access Control** in the left to enter the Target List page. Add a new entry with the Target Description is Target_1 and Domain Name is www.google.com.
5. Click the submenu **Schedule of Access Control** in the left to enter the Schedule List page. Add a new entry with the Schedule Description is Schedule_1, Day is Sat and Sun, Start Time is 1800 and Stop Time is 2000.
6. Click the submenu **Rule of Access Control** in the left, Click **Add New** button to add a new rule as follows:
   1) In Rule Name field, create a name for the rule. Note that this name should be unique, for example Rule_1.
   2) In Host field, select Host_1.
   3) In Target field, select Target_1.
   4) In Schedule field, select Schedule_1.
   5) In Status field, select **Enabled**.
   6) Click **Save** to complete the settings.

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



	Description	LAN Host	Target	Schedule	Rule	Status	Edit
	Rule_1	Host_1	Target ...	Schedul...	Deny	Enabled	Edit

Add New | Enable Selected | Disable Selected | Delete Selected

4.15.2 Host

Choose menu "**Access Control → Host**", and then you can view and set a Host list in the screen as shown in Figure 4-76. The host list is necessary for the Access Control Rule.

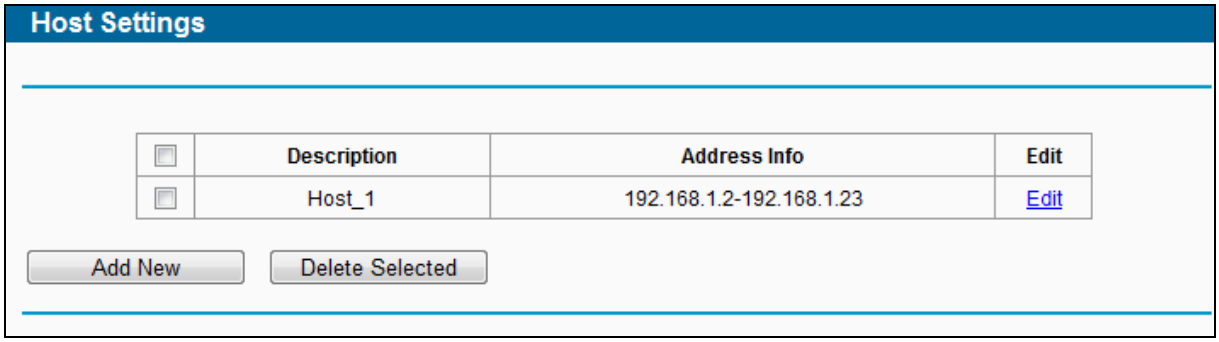


Figure 4-76 Host Settings

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

Click the **Delete Selected** button to delete the selected entries in the table.

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.
   1) If you select IP Address, the screen shown is Figure 4-77.
      - In **Description** field, create a unique description for the host (e.g. Host_1).
      - In **IP Address** field, enter the IP address.
   2) If you select MAC Address, the screen shown is Figure 4-78.
      - In **Description** field, create a unique description for the host (e.g. Host_1).
      - In **MAC Address** field, enter the MAC address.
3. Click the **Save** button to complete the settings.

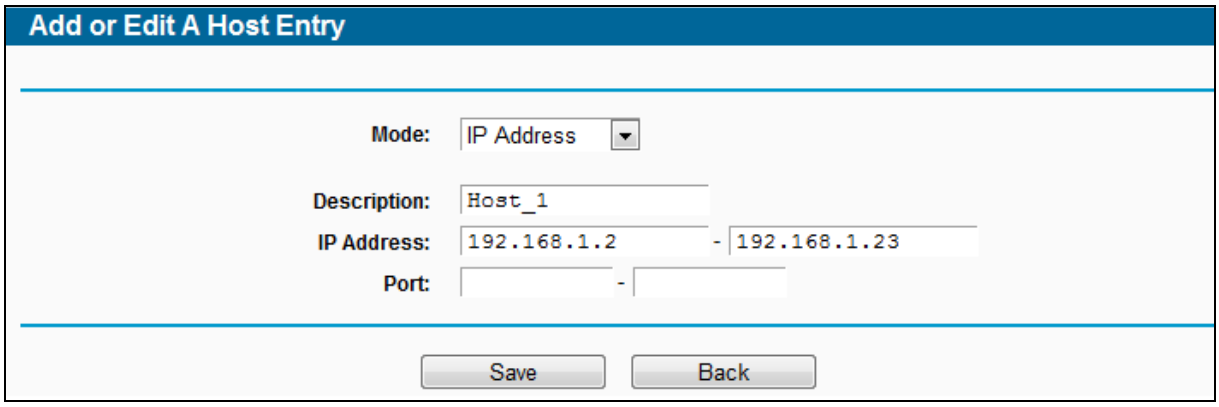


Figure 4-77 Add or Modify a Host Entry

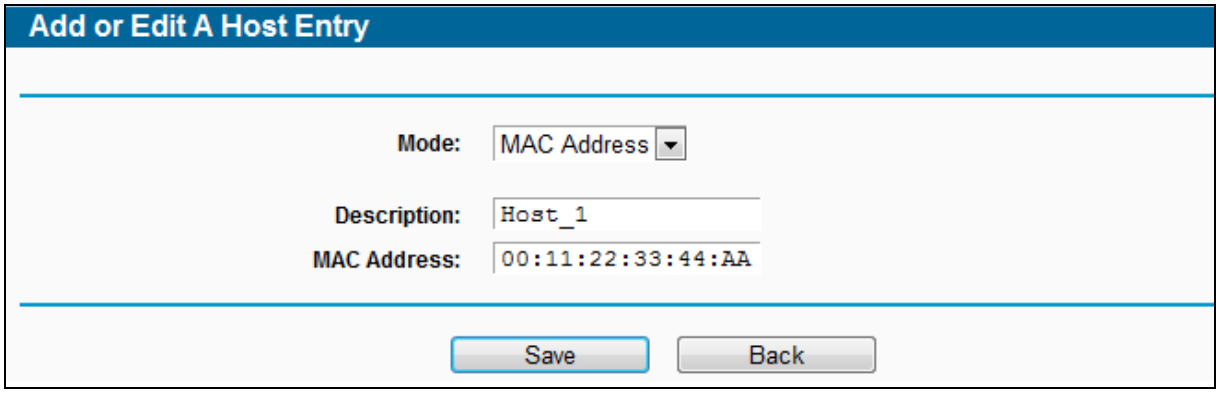


Figure 4-78 Add or Modify a Host Entry

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

1. Click **Add New** button in Figure 4-76 to enter the Add or Modify a Host Entry page.
2. In **Mode** field, select MAC Address from the drop-down list.
3. In **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.

	Description	Address Info	Edit
	Host_1	00:11:22:33:44:AA	Edit

4.15.3 Target

Choose menu "**Access Control → Target**", and then you can view and set a Target list in the screen as shown in Figure 4-79. The target list is necessary for the Access Control Rule.

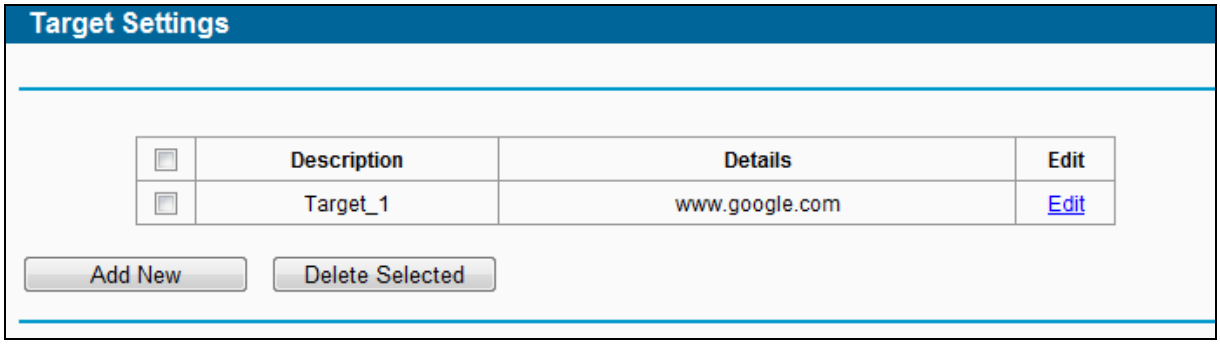


Figure 4-79 Target Settings

- **Description -** Here displays the description about the target and this description is unique.
- **Details -** The target can be IP address, port, or domain name.

➢ **Edit-** 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**, **MAC Address** or **URL Address**.

1） If you select **IP Address**, the screen shown is Figure 4-80.

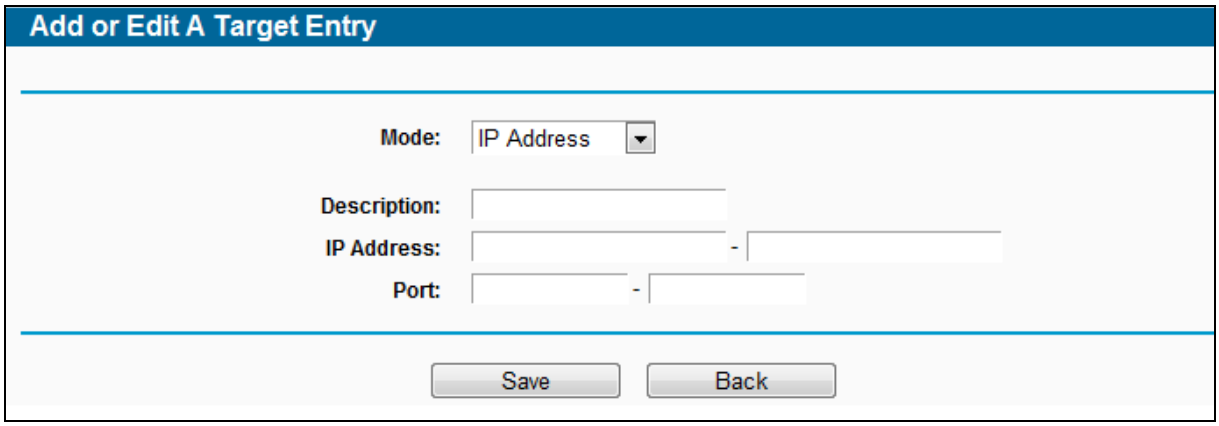


Figure 4-80 Add or Modify an Access Target Entry

I) In **Description** field, create a unique description for the target (e.g. Target_1).

II) In **IP Address** field, enter the IP address of the target.

III) Specify the **Target Port** manually.

2） If you select **MAC Address**, the screen shown is Figure 4-80.

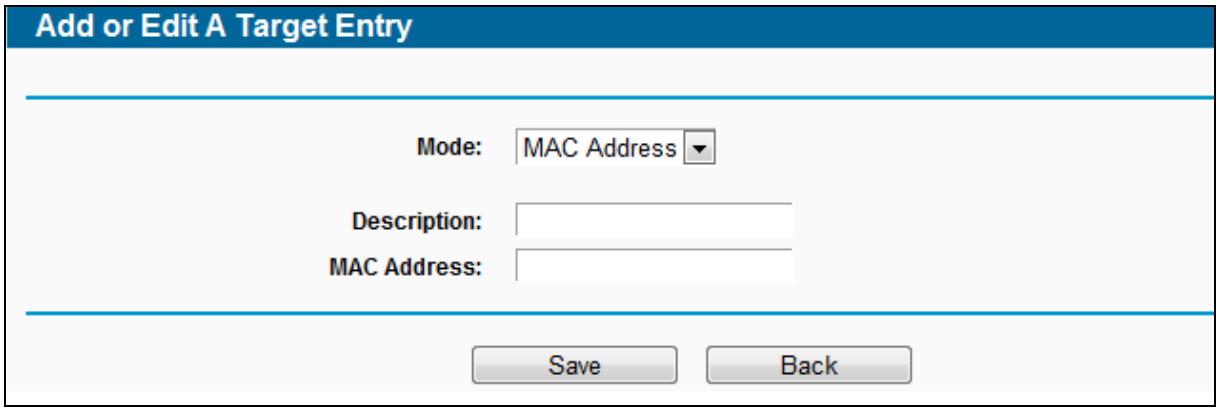


Figure 4-81 Add or Modify an Access Target Entry

I) In **Description** field, create a unique description for the target (e.g. Target_1).

II) In **IP Address** field, enter the IP address of the target.

III) Specify the **Target Port** manually.

3） If you select **URL Address**, the screen shown is Figure 4-82.

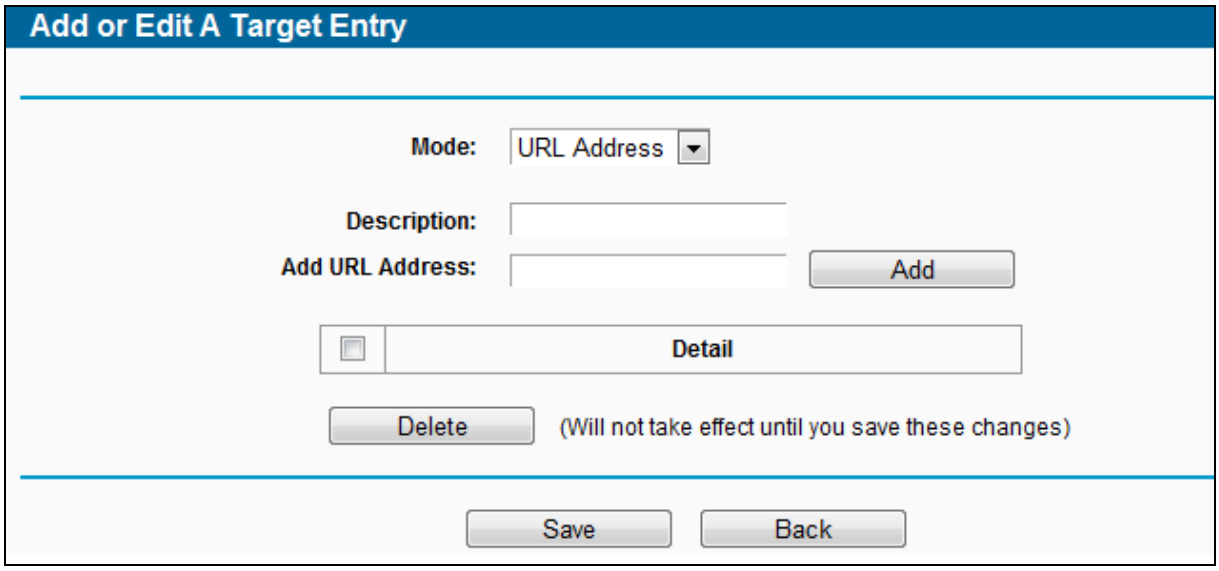


Figure 4-82 Add or Modify an Access Target Entry

I) In **Description** field, create a unique description for the target (e.g. Target_1).

II) In **Add URL Address** field, enter the domain name, either the full name or the keywords (for example, google) in the blank. Any domain name with keywords in it (www.google.com, www.google.cn) will be blocked or allowed. Click **Add** to save the address,

3. Click the **Save** button.

Click the **Delete Selected** button to delete the selected entries in the table.

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

1. Click **Add New** button in Figure 4-79 to enter the Add or Modify an Access Target Entry page.
2. In **Mode** field, select **URL Address** from the drop-down list.
3. In **Description** field, create a unique description for the target (e.g. Target_1).
4. In **Add URL Address** field, enter www.google.com. And then click **Add** to save the entry.
5. Click **Save** to complete the settings.

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

	Description	Details	Edit
	Target_1	www.google.com	Edit

4.15.4 Schedule

Choose menu "**Access Control → Schedule**", and then you can view and set a Schedule list in the next screen as shown in Figure 4-83. The Schedule list is necessary for the Access Control Rule.

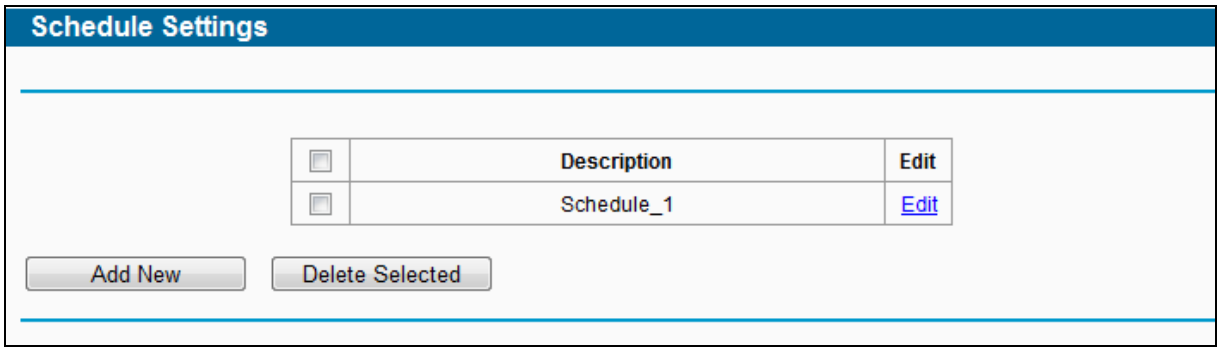


Figure 4-83 Schedule Settings

- **Description** - Here displays the description of the schedule and this description is unique.
- **Edit** - Here you can edit or delete an existing schedule.

To add a new schedule, follow the steps below:

1. Click **Add New** button shown in Figure 4-83 and the next screen will pop-up as shown in Figure 4-84.
2. In **Description** field, create a unique description for the schedule (e.g. Schedule_1).
3. Select the **Day** or days from the drop-down list. And then select the **Start Time** and **Stop Time** from the drop-down list. Click **Add** to save the entry.
4. Click **Save** to complete the settings.

Click the **Delete Selected** button to delete selected entries in the table.

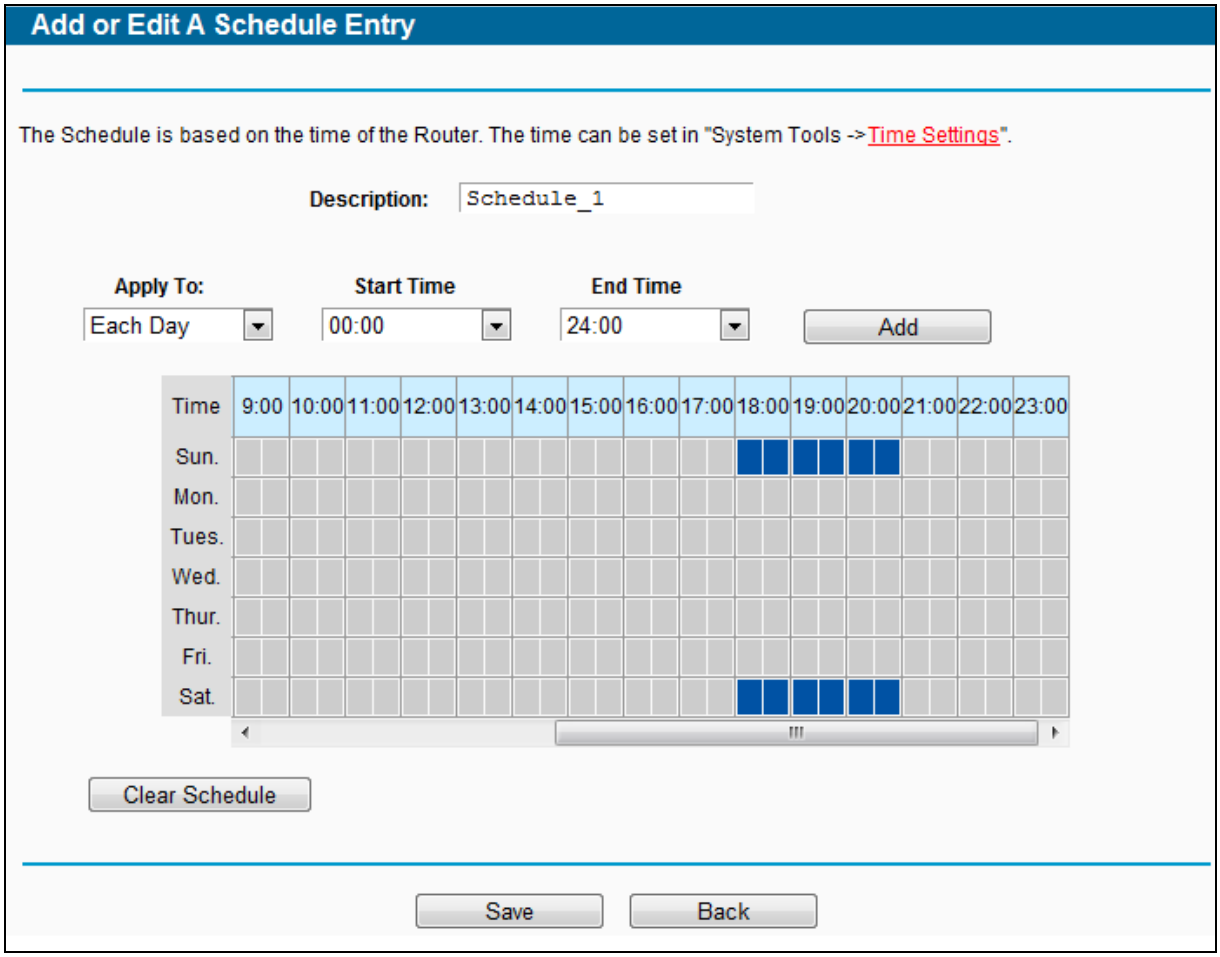


Figure 4-84 Advanced Schedule Settings

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

1. Click **Add New** button shown in Figure 4-83 to enter the Advanced Schedule Settings page.
2. In **Description** field, create a unique description for the schedule (e.g. Schedule_1).
3. In **Day** list, select **Each Week** from the drop-down list and click **Sat** and **Sun**.
4. In **Time** list, select 18:00 for Start Time field and 20:00 for Stop Time. And then click the **Add** button.
5. Click **Save** to complete the settings.

4.16 Advanced Routing

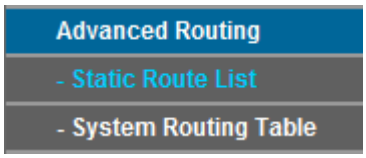


Figure 4-85 Advanced Routing

There are two submenus under the Advanced Routing menu as shown in Figure 4-85: **Static Route List** and **System Routing Table**. Click any of them, and you will be able to configure the corresponding function.

4.16.1 Static Route List

Choose menu "**Advanced Routing → Static Route List**", and then you can configure the static route in the next screen (shown in Figure 4-86). A static route is a pre-determined path that network information must travel to reach a specific host or network.

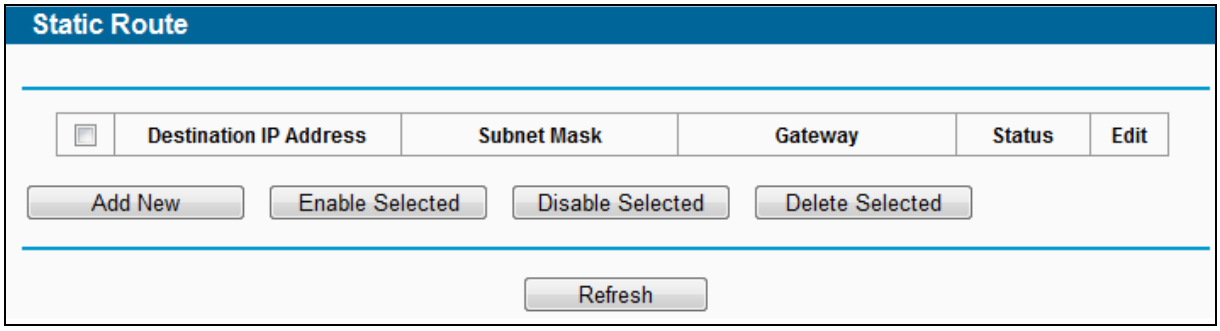


Figure 4-86 Static Route

To add static route entries:

1. Click **Add New** shown in Figure 4-86, you will see the following screen.

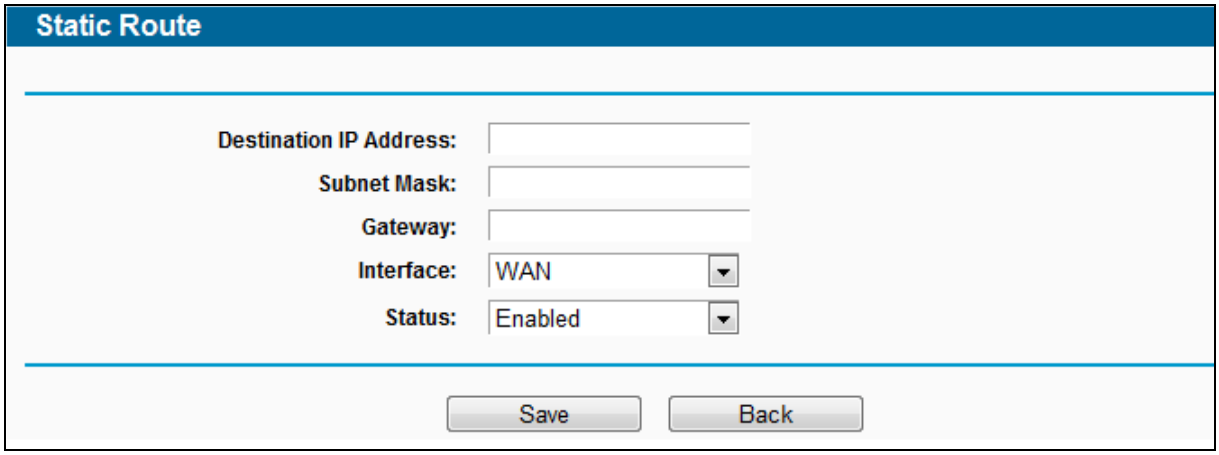


Figure 4-87 Add or Modify a Static Route Entry

2. Enter the following data:

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

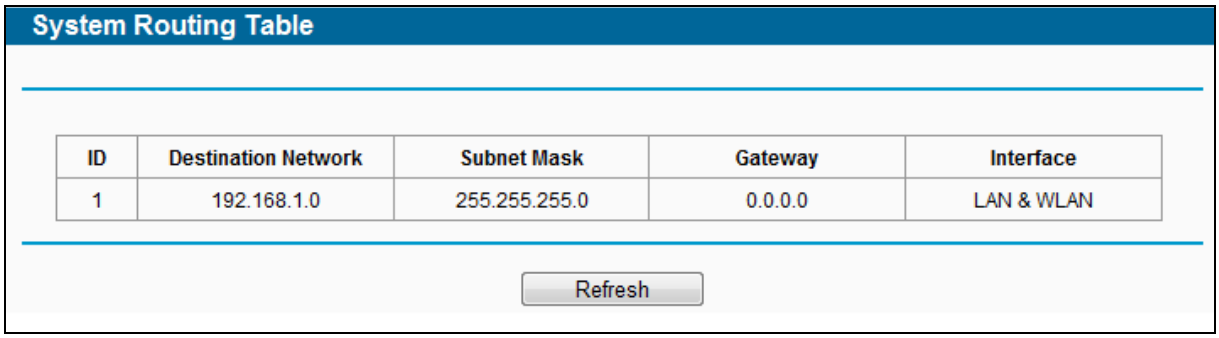
Click the **Enable Selected** button to enable the selected entries.

Click the **Disable Selected** button to disable the selected entries.

Click the **Delete Selected** button to delete the selected entries.

4.16.2 System Routing Table

Choose menu "**Advanced Routing → System Routing Table**", and then you can view the System Routing Table in the next screen (shown in Figure 4-88). 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.



ID	Destination Network	Subnet Mask	Gateway	Interface
1	192.168.1.0	255.255.255.0	0.0.0.0	LAN & WLAN

Figure 4-88 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).

4.17 Bandwidth Control

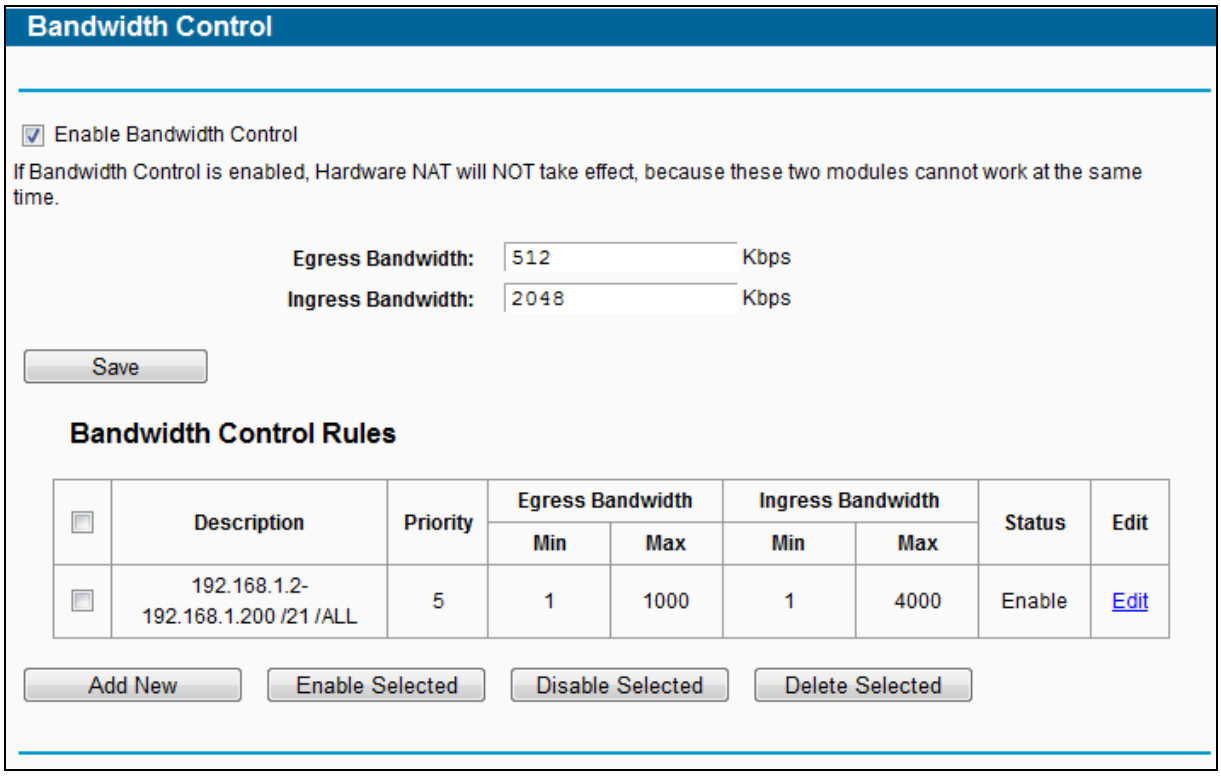


Figure 4-89 Bandwidth Control

Choose menu "**Bandwidth Control**", and then you can configure the bandwidth control in the screen as shown in Figure 4-89 Bandwidth Control.

You can configure the Egress Bandwidth and Ingress Bandwidth in this page. Their values you configure should be less than 100000Kbps. You can also view and configure the Bandwidth Control rules in this page.

- **Enable Bandwidth Control -** Check this box so that the Bandwidth Control settings can take effect.
- **Egress Bandwidth** - The upload speed through the WAN port.
- **Ingress Bandwidth -** The download speed through the WAN port.

Click **Save** to make the settings take effect.

- **Description -** This is the information about the rules such as address range.
- **Priority -** The priority of the rule, ranging from 1 to 8. 1 stands for the highest priority
- **Egress bandwidth -** This field displays the max and mix upload bandwidth through the WAN port, the default is 0.
- **Ingress bandwidth -** This field displays the max and mix download bandwidth through the WAN port, the default is 0.

- **Status -** This displays the status of the rule.
- **Edit -** Click **Edit** 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 4-89, you will see a new screen shown in Figure 4-90.
2. Enter the information like the screen shown below.

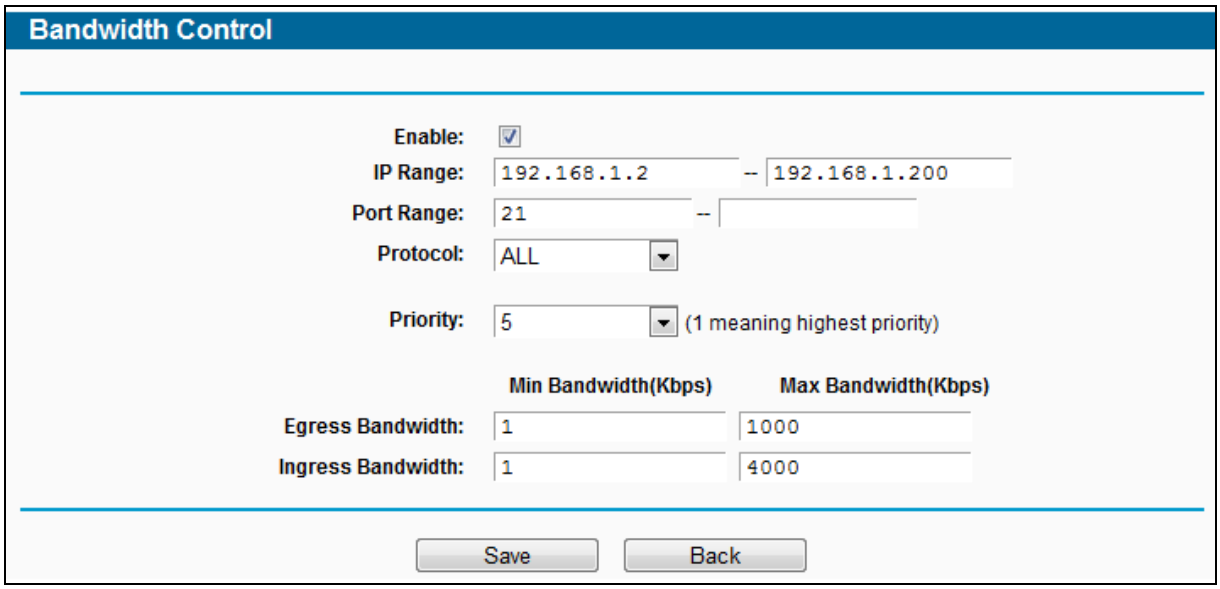


Figure 4-90 Bandwidth Control Rule Settings

3. Click the **Save** button.

4.18 IP & MAC Binding

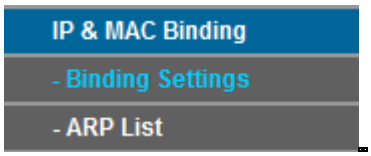


Figure 4-91 the IP & MAC Binding menu

There are two submenus under the IP &MAC Binding menu (shown in Figure 4-91): **Binding Settings** and **ARP List**. Click any of them, and you will be able to scan or configure the corresponding function. The detailed explanations for each submenu are provided below.

4.18.1 Binding Settings

This page displays the **IP & MAC Binding Setting** table; you can operate it in accord with your desire (shown in Figure 4-92).

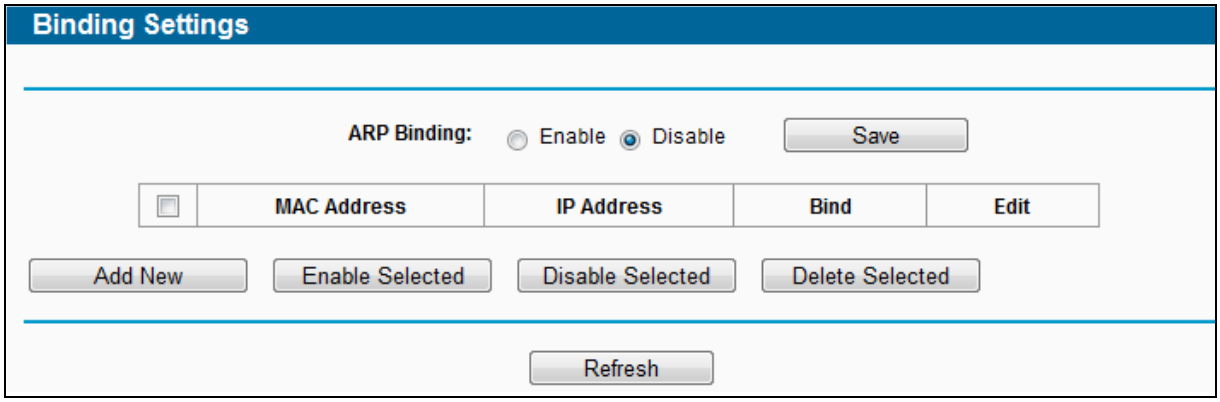


Figure 4-92 Binding Setting

- **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.
- **Edit -** To edit 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 **Edit** button, and then you will go to the next page. This page is used for adding or modifying an IP & MAC Binding entry (shown in Figure 4-93).

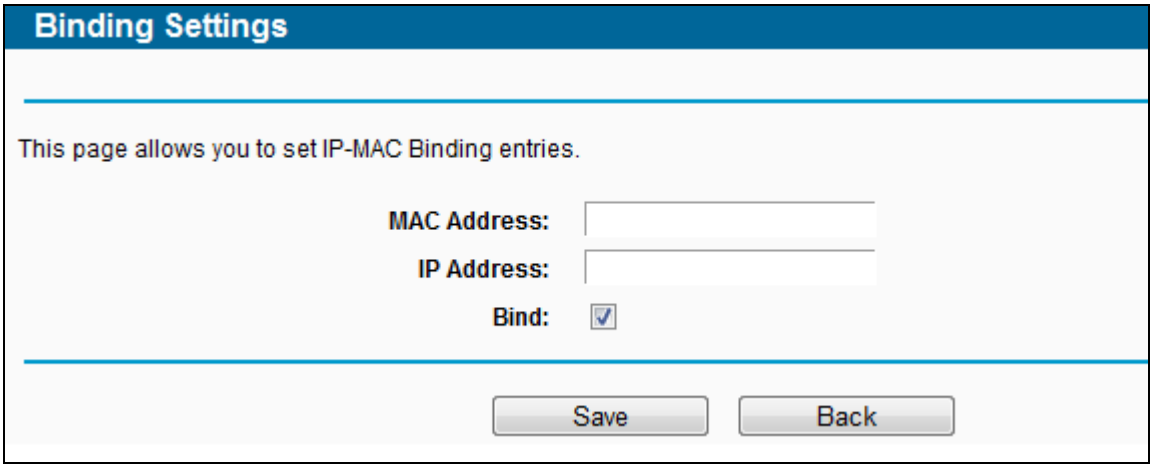


Figure 4-93 IP & MAC Binding Setting (Add & Modify)

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

1. Click the **Add New** button as shown in Figure 4-92.
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 **Edit** or **Delete** as desired on the **Edit** column.

4.18.2 ARP List

To manage the computer, you could observe the computers in the LAN by checking the relationship of MAC address and IP address on the ARP list, and you could also configure the items on the ARP list. This page displays the ARP List; it shows all the existing IP & MAC Binding entries (shown in Figure 4-94).

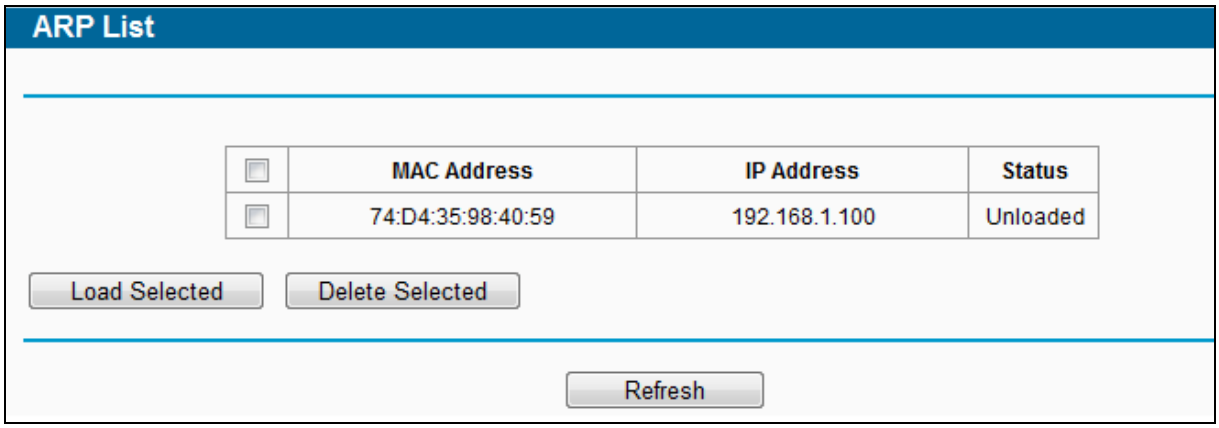


Figure 4-94 ARP List

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.

Click the **Load Selected** button to load the selected items to the IP & MAC Binding list.

Click the **Delete Selected** button to delete the selected items to the IP & MAC Binding list.

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

☞ **Note:**

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

4.19 Dynamic DNS

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

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

4.19.1 No-ip.com DDNS

If the dynamic DNS **Service Provider** you select is www.no-ip.com, the page will appear as shown in. Figure 4-95

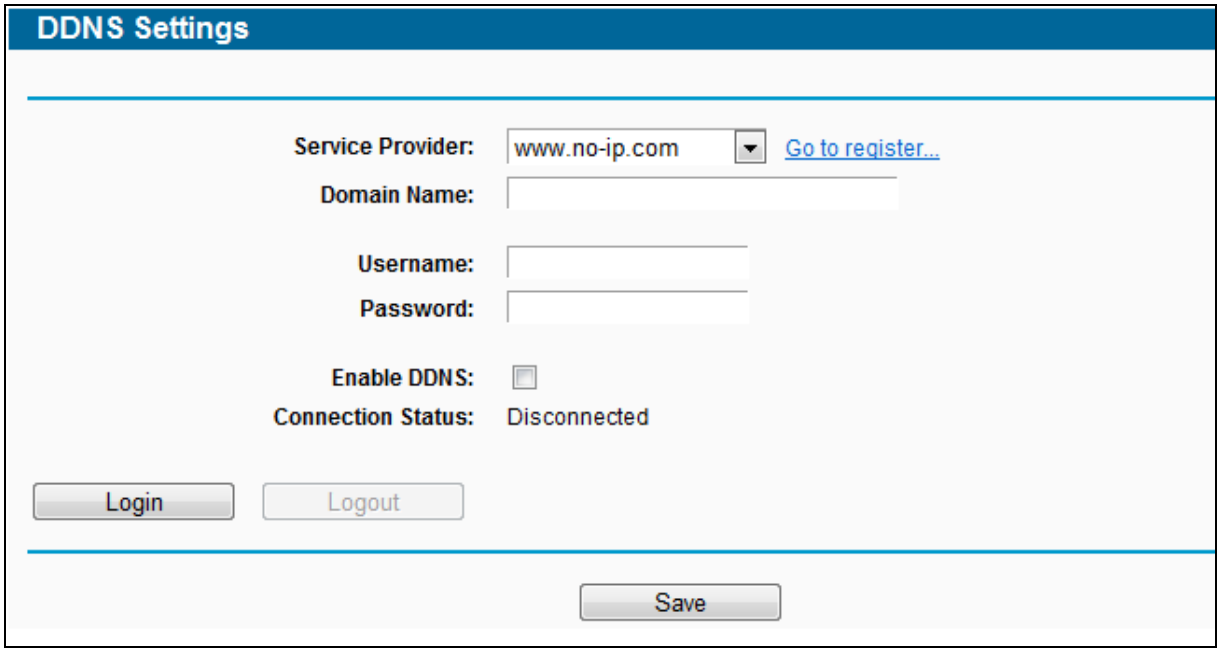


Figure 4-95 No-ip.com DDNS Settings

To set up for DDNS, follow these instructions:

1. Enter the **Domain Name** you received from dynamic DNS service provider.
2. Enter the **Username** for your DDNS account.
3. Enter the **Password** for your DDNS account.
4. Enable DDNS.
5. 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.

4.19.2 Comexe.cn DDNS

If the dynamic DNS **Service Provider** you select is www.comexe.cn, the page will appear as shown in Figure 4-96.

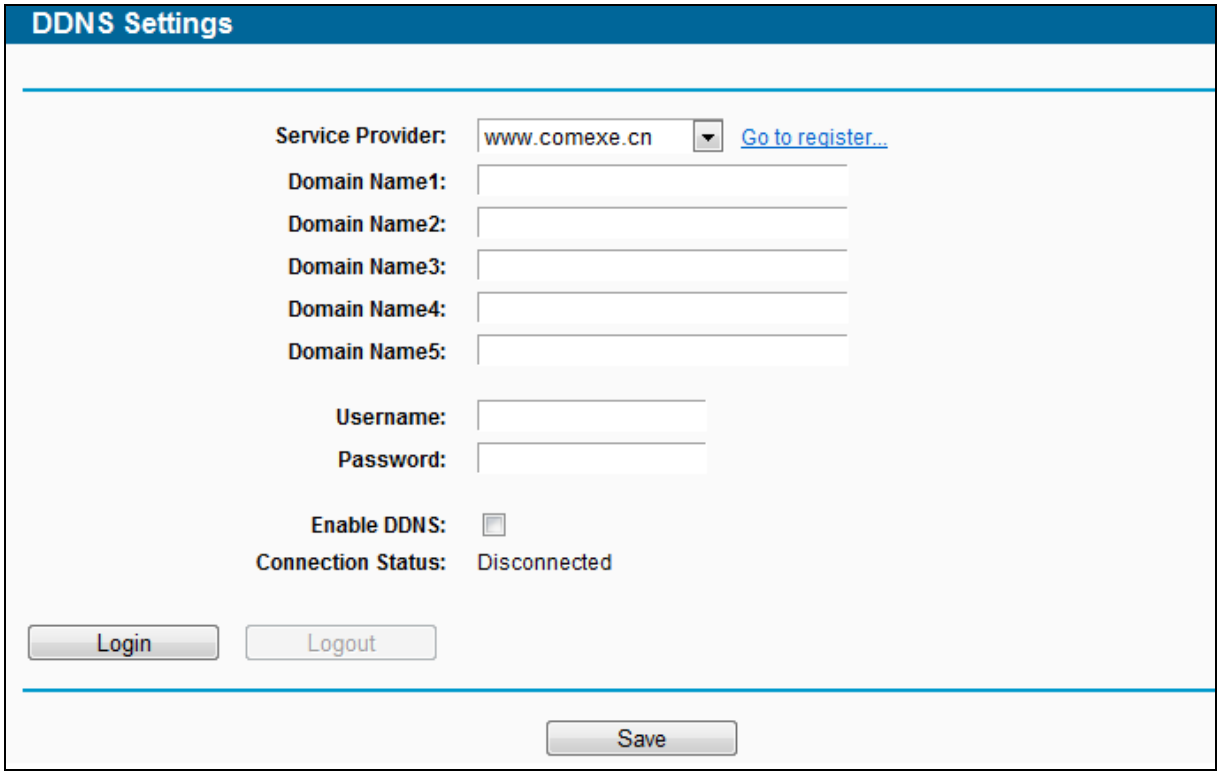


Figure 4-96 Comexe.cn DDNS Settings

To set up for DDNS, follow these instructions:

1. Enter the **Domain Name** your dynamic DNS service provider gave.
2. Enter the **Username** for your DDNS account.
3. Enter the **Password** for your DDNS account.
4. Enable DDNS.
5. 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.

4.19.3 Dyndns.com DDNS

If the dynamic DNS **Service Provider** you select is www.dyndns.com, the page will appear as shown in Figure 4-97.

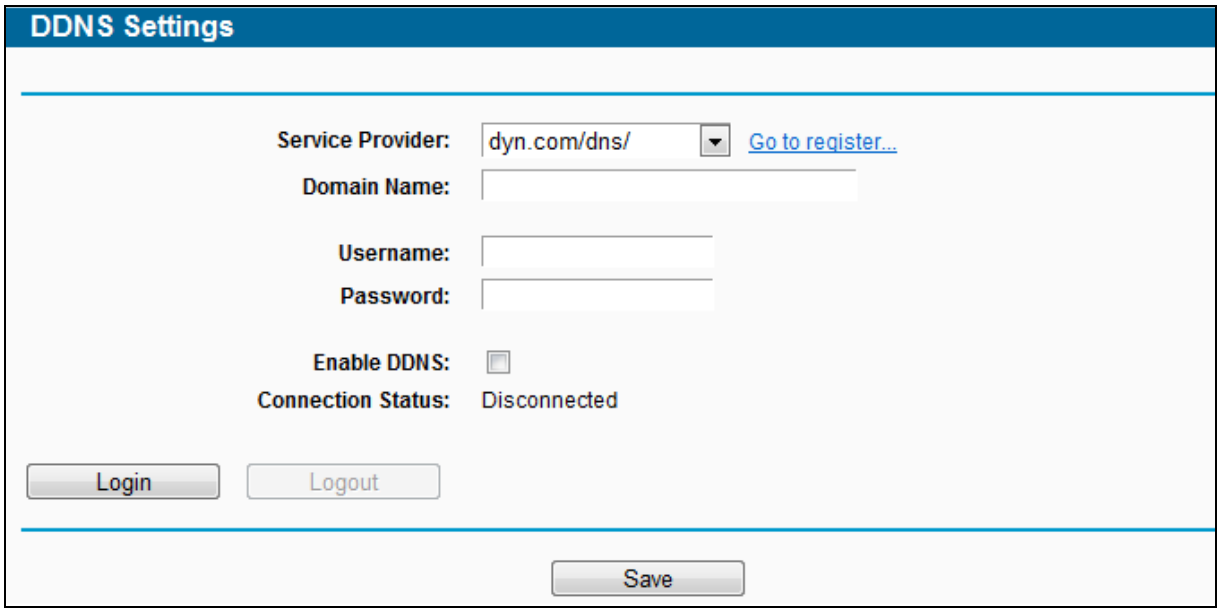


Figure 4-97 Dyndns.org DDNS Settings

To set up for DDNS, follow these instructions:

1. Enter the **Domain Name** you received from dynamic DNS service provider.
2. Enter the **Username** for your DDNS account.
3. Enter the **Password** for your DDNS account.
4. Enable DDNS.
5. 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.

4.20 IPv6

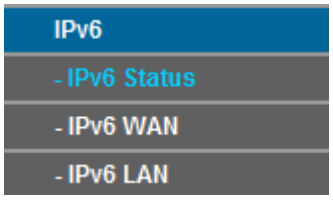


Figure 4-98 IPv6 Support

There are three submenus under the IPv6 Support menu (shown in Figure 4-98): **IPv6 Status**, **IPv6 WAN and IPv6 LAN**. 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.

4.20.1 IPv6 Status

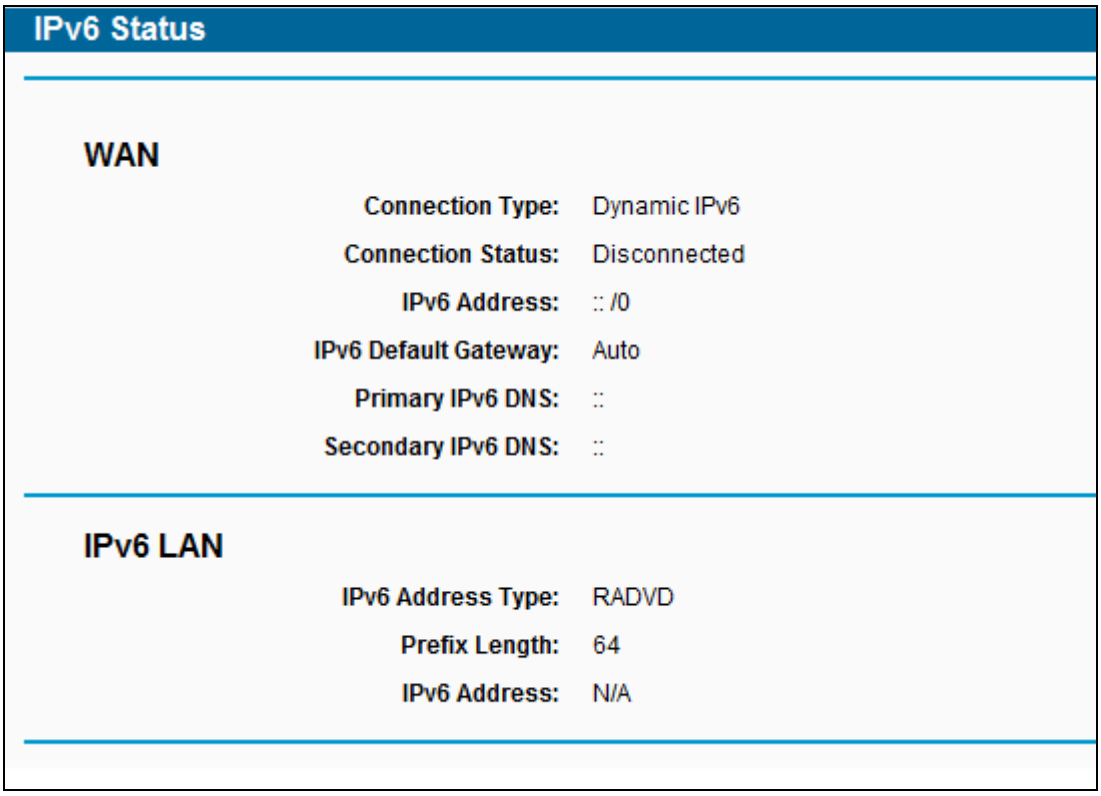


Figure 4-99 IPv6 Status

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
  - **Connection Status** - The status of IPv6 connection
  - **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 Type** - There are two types of assignation for IPv6 address: RADVD (Stateless address auto-configuration) and DHCPv6 (Dynamic Host Configuration Protocol for IPv6) Server.
  - **Prefix Length** - The prefix length of IPv6 address
  - **IPv6 Address** - The LAN IPv6 address

4.20.2 IPv6 WAN

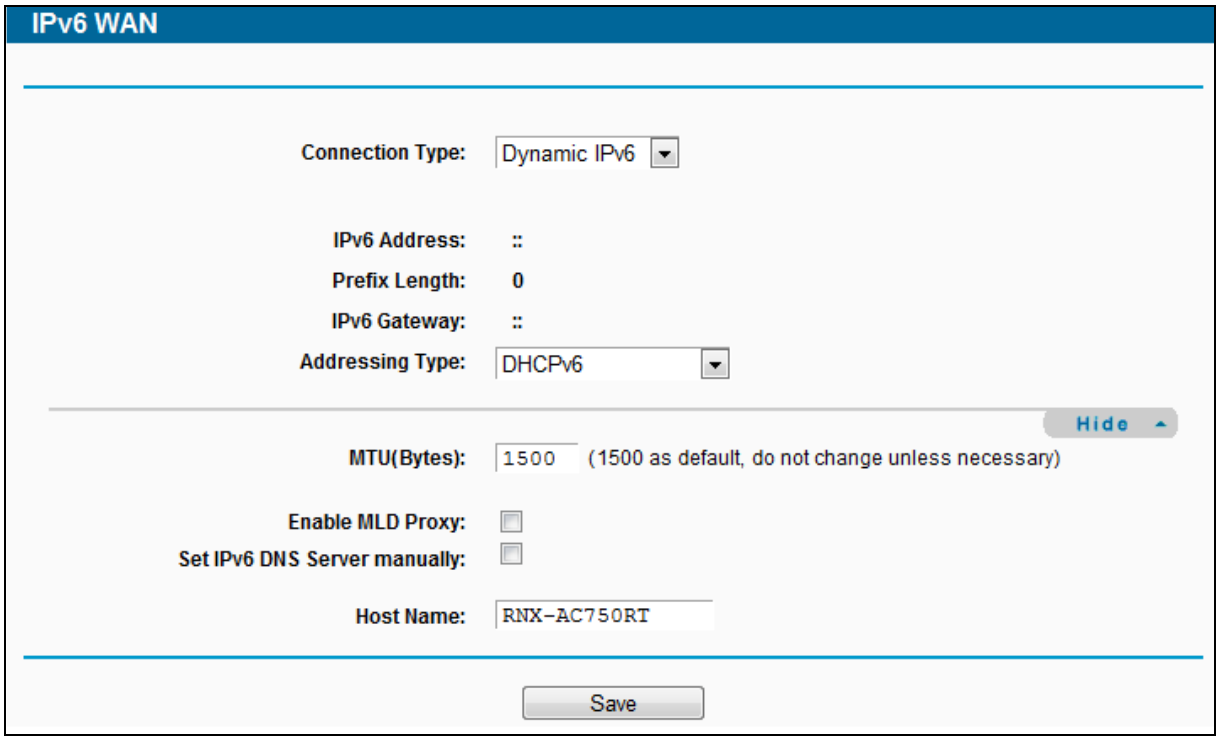


Figure 4-100 Enable/Disable IPv6

- **Connection Type** - Choose the correct WAN connection type based on your ISP network topology.
  - **Dynamic IPv6** - 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) Dynamic IPv6

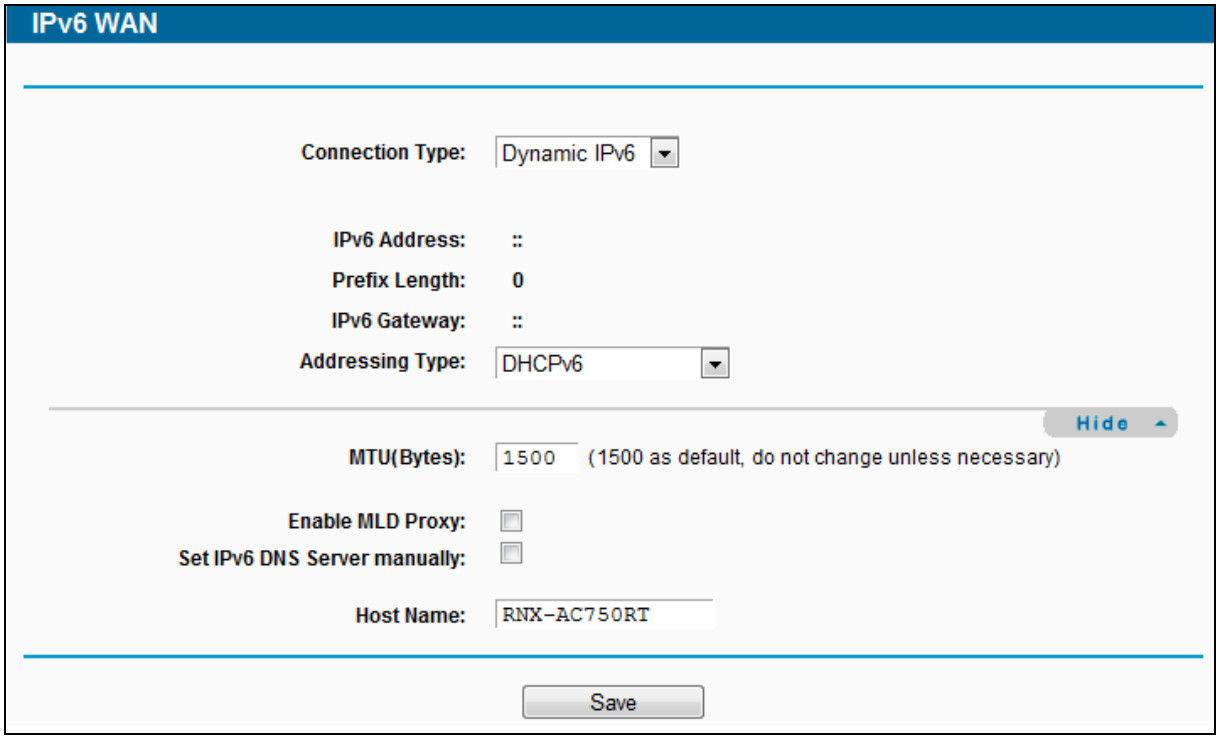


Figure 4-101 Dynamic IPv6

- **IPv6 Address** - The IPv6 address assigned by your ISP dynamically.
- **Prefix Length** - The length of IPv6 address prefix.
- **IPv6 Gateway** - Enter the default gateway provided by your ISP.
- **Addressing Type** - There are two types of assignation for IPv6 address: SLAAC (Stateless address auto-configuration) and DHCPv6 (Dynamic Host Configuration Protocol for IPv6) Server.
- **MTU(Bytes)** - 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.

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

- **Enable MLD Proxy** - Enable the Multicast Listener Discovery (MLD) Proxy function if you need.
- **IPv6 DNS Server** - Enter the DNS IPv6 address provided by your ISP.
- **Secondary IPv6 DNS Server** - Enter another DNS IPv6 address 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.

2) Static IPv6

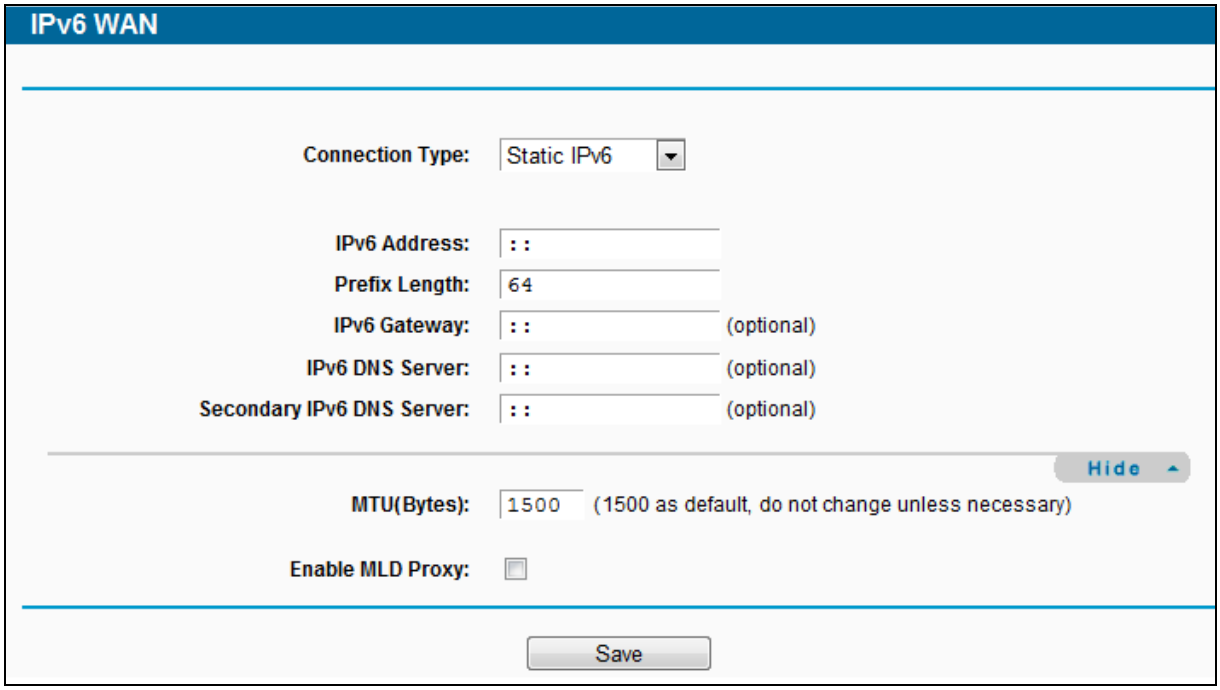


Figure 4-102 Static IPv6

- **IPv6 Address** - Enter the IPv6 address provided by your ISP.
- **Prefix Length** - The length of IPv6 address prefix.
- **IPv6 Gateway** - Enter the default gateway provided by your ISP.
- **IPv6 DNS Server**- Enter the DNS IPv6 address provided by your ISP.
- **Secondary IPv6 DNS Server** - Enter another DNS IPv6 address provided by your ISP.
- **MTU(Bytes)** - 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.
- **Enable MLD Proxy** - Enable the Multicast Listener Discovery (MLD) Proxy function if you need.

3) PPPoEv6

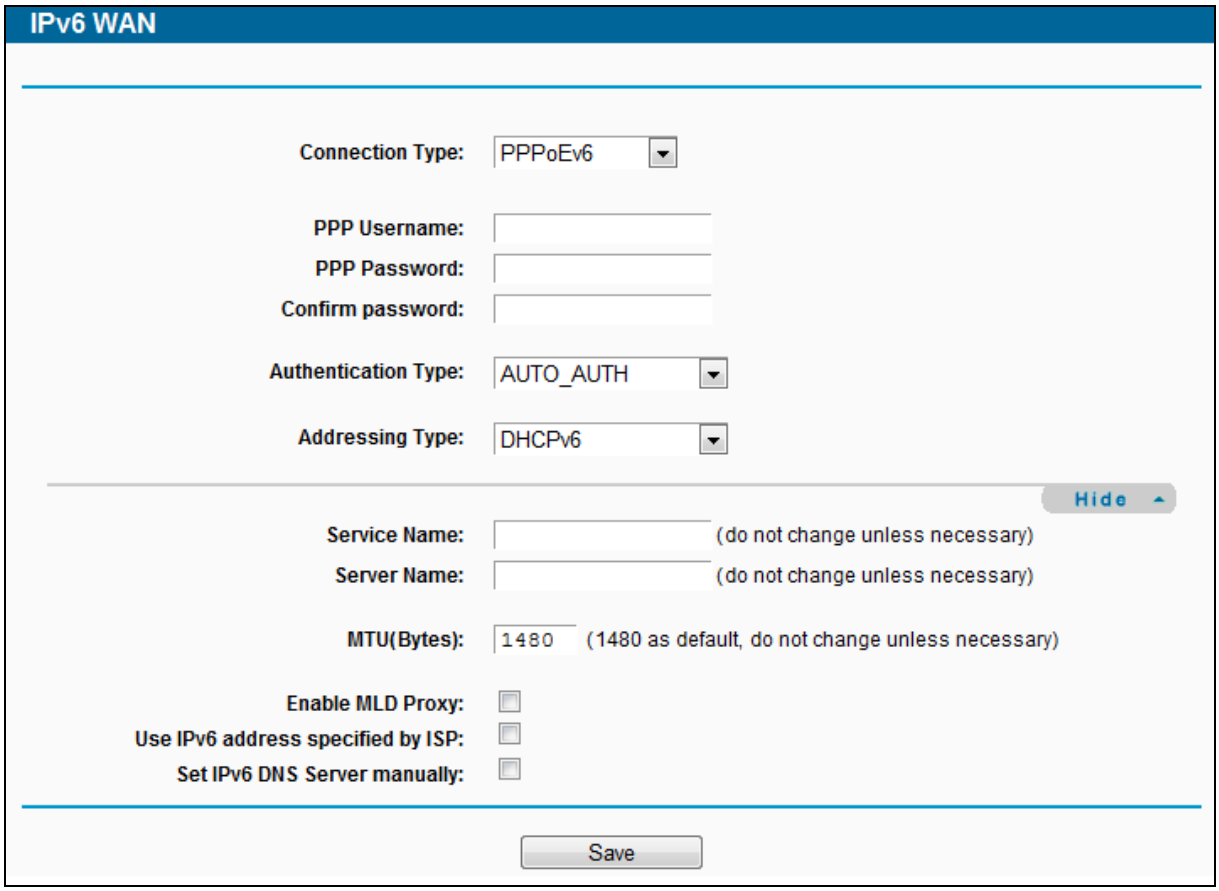


Figure 4-103 PPPoEv6

- **PPP Username/Password** - Enter the User Name and Password provided by your ISP. These fields are case-sensitive.
- **Authentication Type** – Choose one authentication type from **AUTO-AUTH**, **PAP**, **CHAP** and **MS-CHAP**.
- **Addressing Type** - There are two types of assignation for IPv6 address: SLAAC (Stateless address auto-configuration) and DHCPv6 (Dynamic Host Configuration Protocol for IPv6) Server.
- **MTU(Bytes)** - 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.
- **Enable MLD Proxy** - Enable the Multicast Listener Discovery (MLD) Proxy function if you need.
- **Use IP address specified by ISP** - Input a static IPv6 address from the ISP.
- **Set IPv6 DNS Server manually** - Enter the IP address of the IPv6 DNS server and secondary IPv6 DNS server.

4) Tunnel 6to4

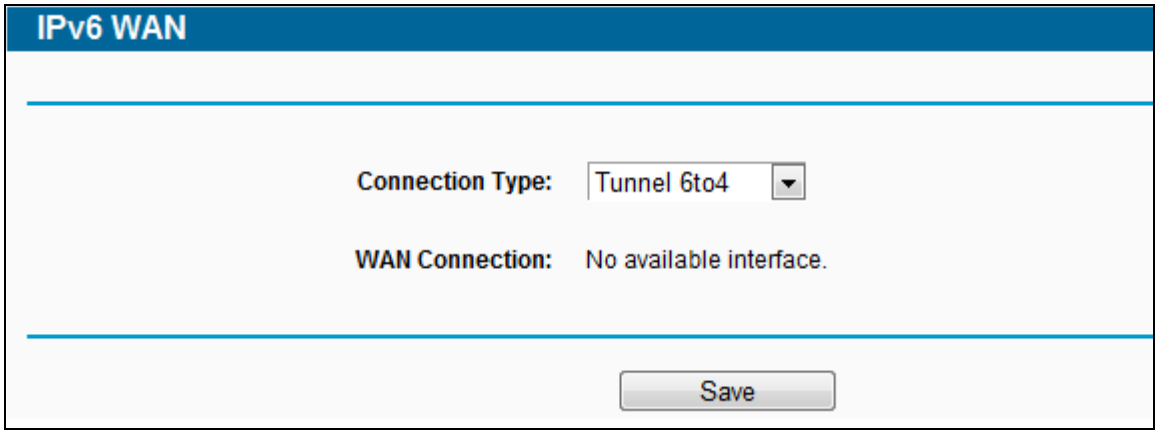


Figure 4-104 Tunnel 6to4

This type is used in the situation that your WAN connection is IPv4 while LAN connection is IPv6.

- **WAN Connection** - Display the available wan connection.

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

4.20.3 IPv6 LAN

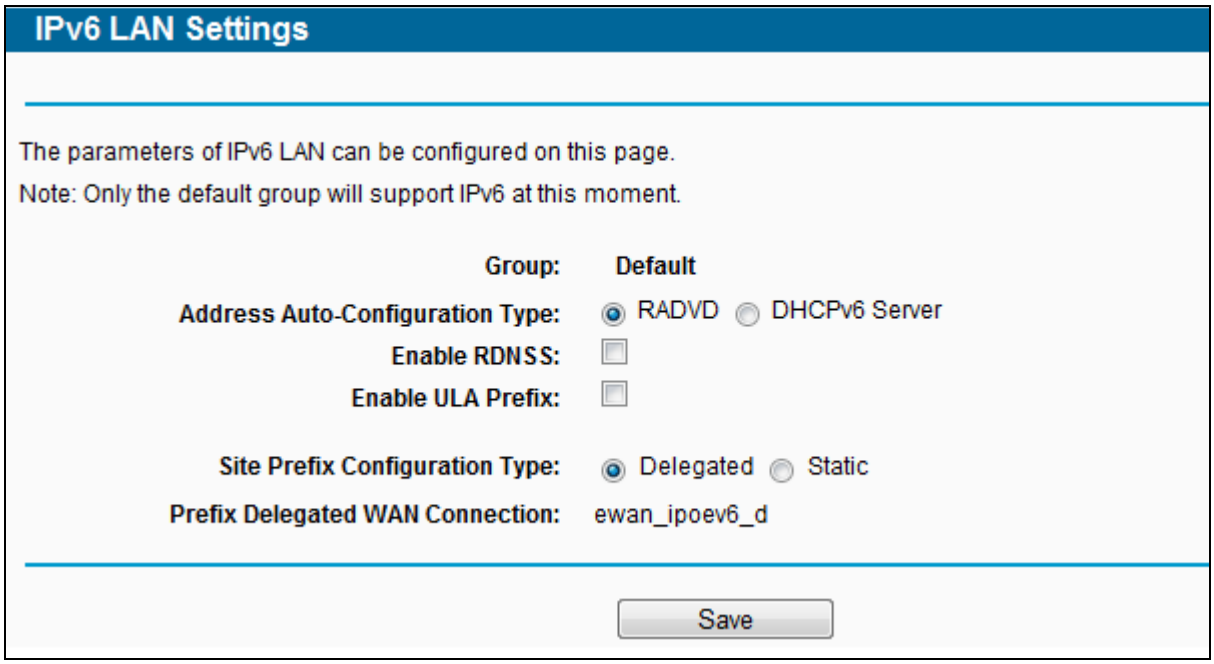


Figure 4-105 IPv6 LAN

- **Address Auto-Configuration Type** - Choose the IPv6 address auto-configuration type, either **RADVD** or **DHCPv6 Server**.
- **Site Prefix Configuration Type** - Choose the site prefix configuration type, either **Delegated** or **Static**.

4.21 System Tools

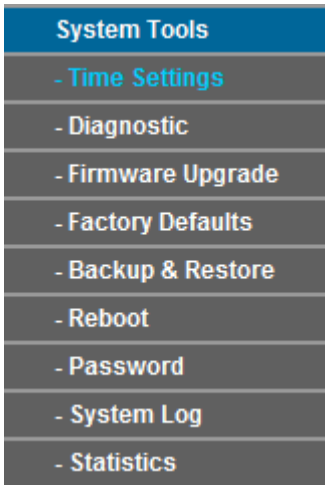


Figure 4-106 The System Tools menu

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.

4.21.1 Time Settings

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

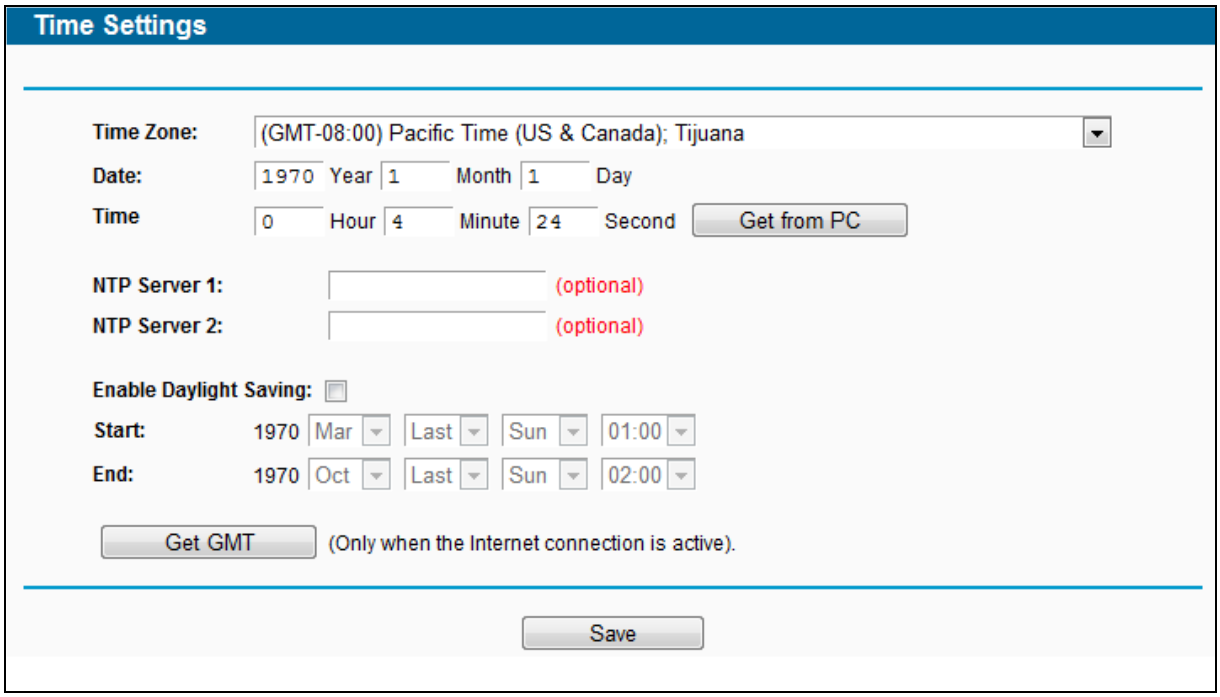


Figure 4-107 Time settings

- **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.
- **Get From PC -** Enter your PC's current time into the right blanks.
- **NTP Server 1 / NTP Server 2 -** Enter the address or domain of the **NTP Server 1** or **NTP Server 2**, 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.

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

To set Daylight Saving:

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

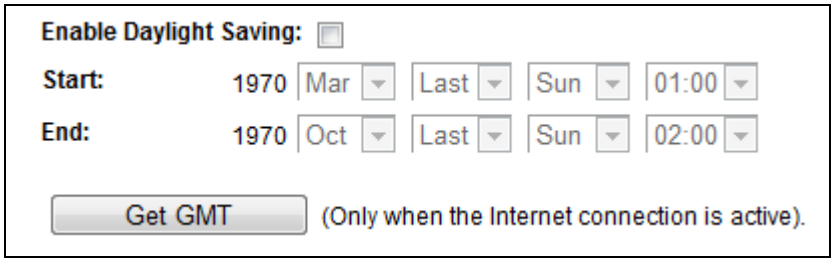


Figure 4-108 Time settings

Note:

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

4.21.2 Diagnostic

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

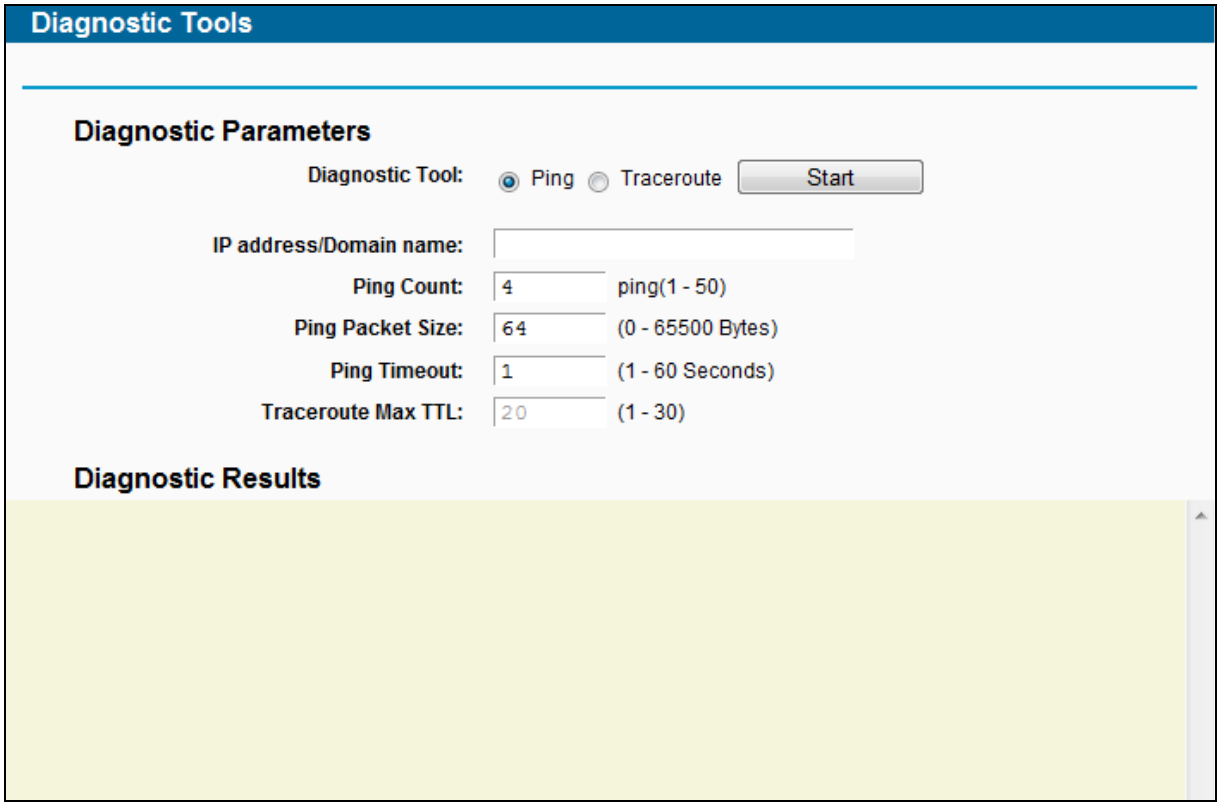


Figure 4-109 Diagnostic Tools

- **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.
- **Ping Count -** Specifies the number of Echo Request messages sent. The default is 4.
- **Ping Packet Size -** Specifies the number of data bytes to be sent. The default is 64.
- **Ping Timeout -** Time to wait for a response, in milliseconds. The default is 800.
- **Traceroute Max TTL -** Set the maximum number of hops (max TTL to be reached) in the path to search for the target (destination). The default is 20.

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

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

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

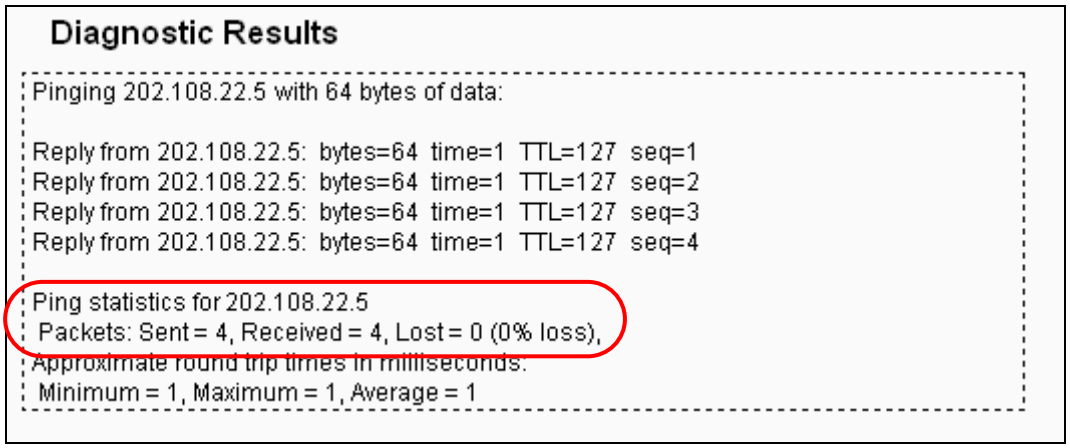


Figure 4-110 Diagnostic Results

☞ **Note:**

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

4.21.3 Firmware Upgrade

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

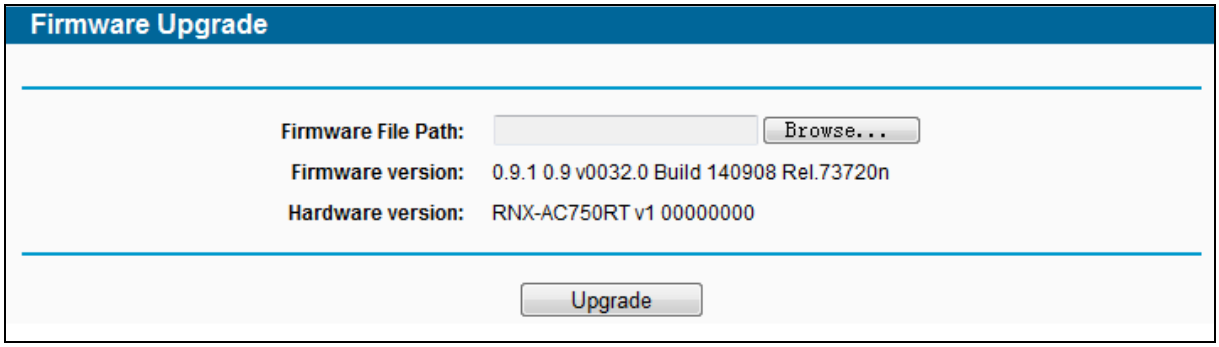


Figure 4-111 Firmware Upgrade

- **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. Enter or select the path name where you save the upgrade file on the computer into the **Firmware File Path** blank.
2. Click the **Upgrade** button.
3. The router will reboot while the upgrading has been finished.

☞ **Note:**

1) 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.
2) 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.
3) The firmware version must correspond to the hardware.
4) The upgrade process takes a few moments and the router restarts automatically when the upgrade is complete.

4.21.4 Factory Defaults

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

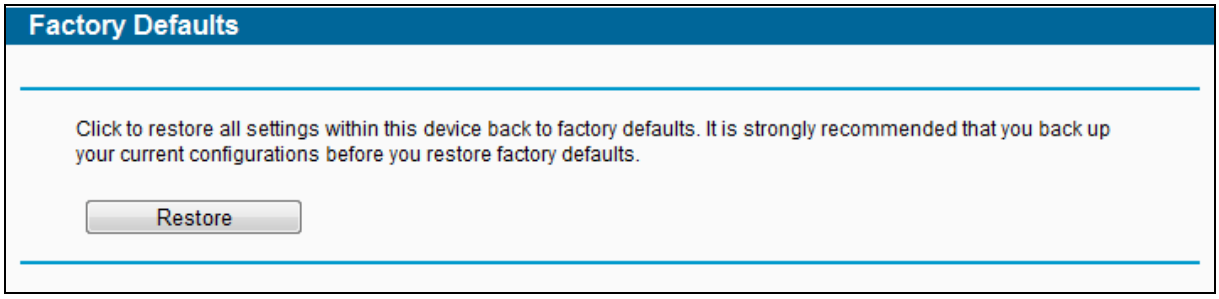


Figure 4-112 Restore Factory Default

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.

4.21.5 Backup & Restore

Choose menu "**System Tools → Backup & Restore**", and then you can save the current configuration of the router as a backup file and restore the configuration via a backup file as shown in Figure 4-113.

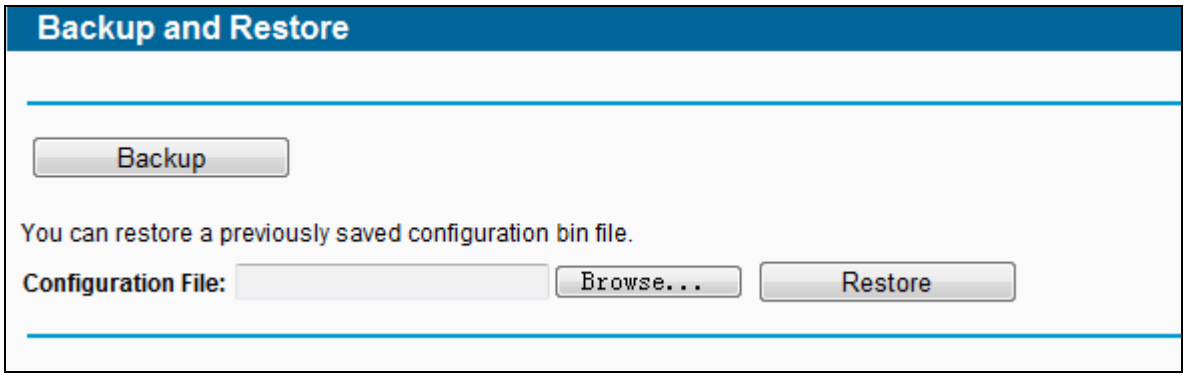


Figure 4-113 Backup & Restore Configuration

- 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.

4.21.6 Reboot

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

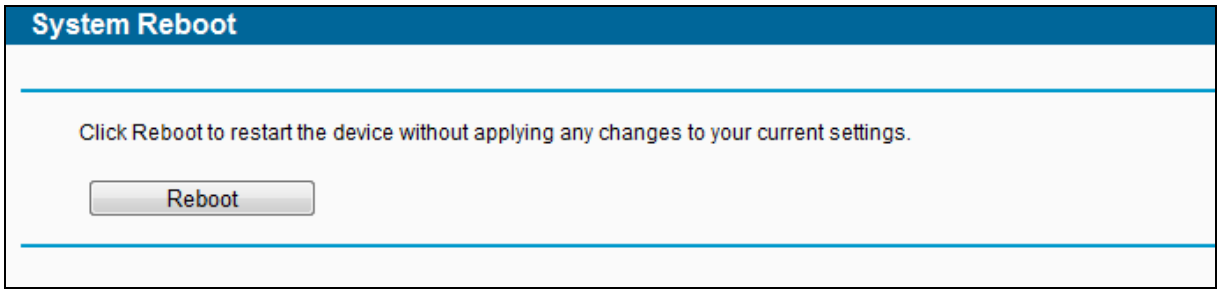


Figure 4-114 Reboot the router

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

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

4.21.7 Password

Choose menu "**System Tools → Password**", and then you can change the factory default user name and password of the router in the next screen as shown in Figure 4-115.

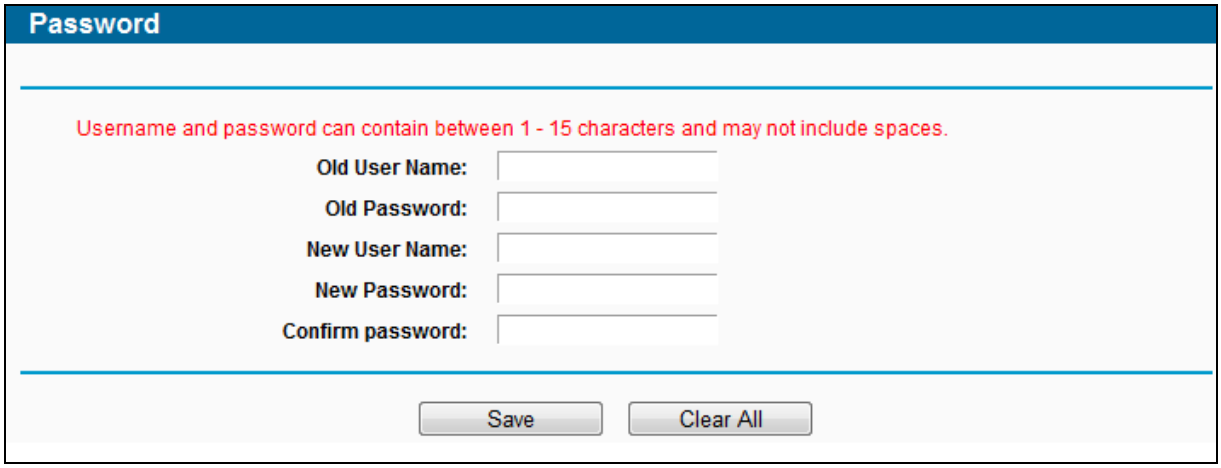


Figure 4-115 Password

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

Note:

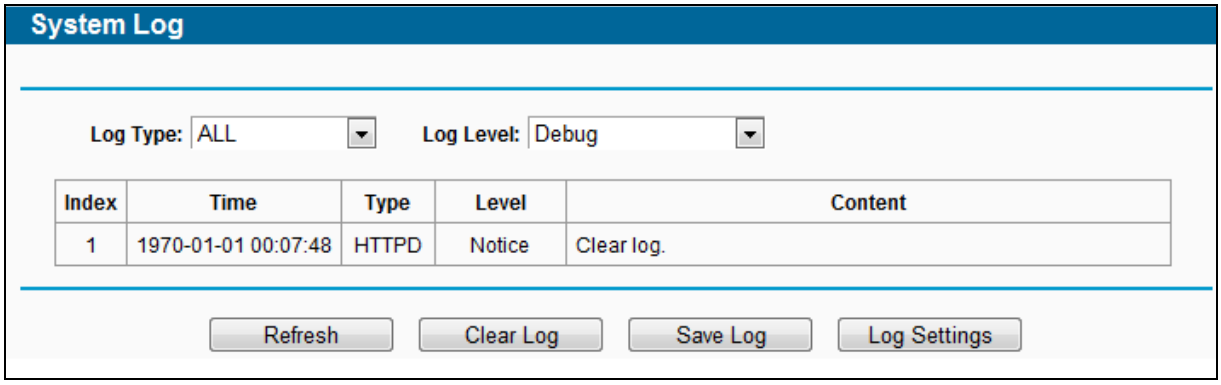
The new user name and password must not exceed 14 characters in length and not include any spaces. Enter the new Password twice to confirm it.

Click the **Save** button when finished.

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

4.21.8 System Log

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



- **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.
- **Clear Log -** All the logs will be deleted from the router permanently, not just from the page.
- **Save Log -** Click to save all the logs in a txt file.
- **Log Settings -** Click to change the log settings.

4.21.9 Statistics

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

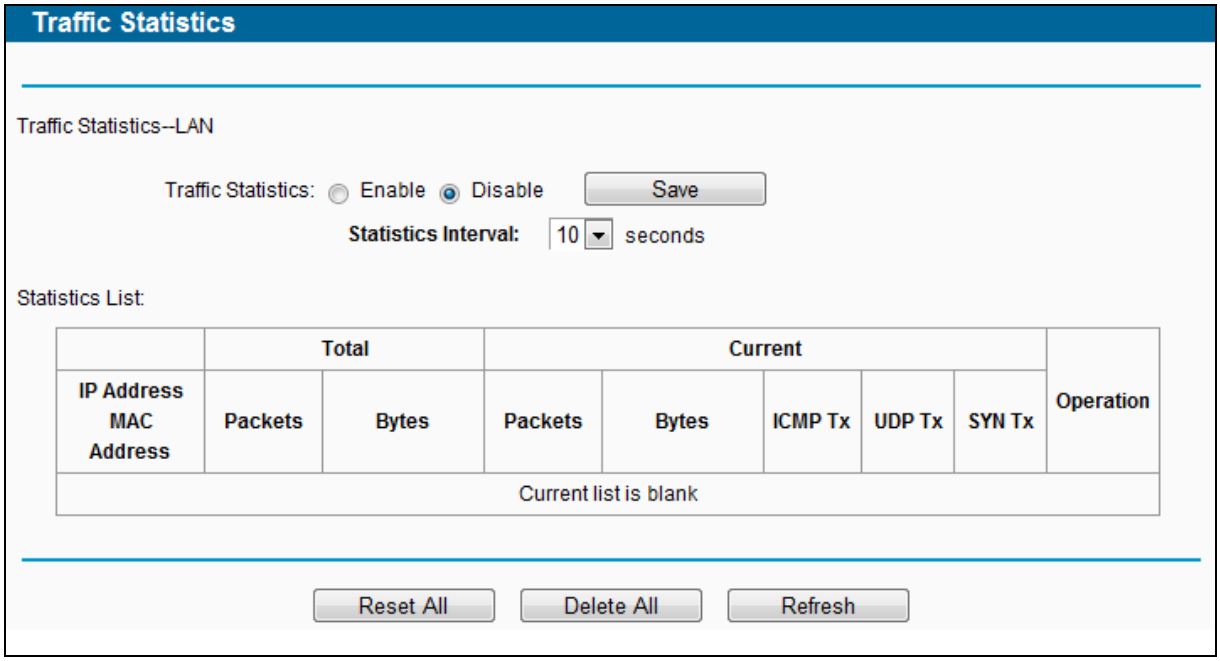


Figure 4-116 Statistics

- **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.
- **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.

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

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

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

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”.
Operation	**Reset**	Reset the value of he entry to zero.
	Delete	Delete the existing entry in the table.

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

4.22 Logout

Choose ”**Logout**”, and you will be back to the login screen as shown in Figure 4-117.

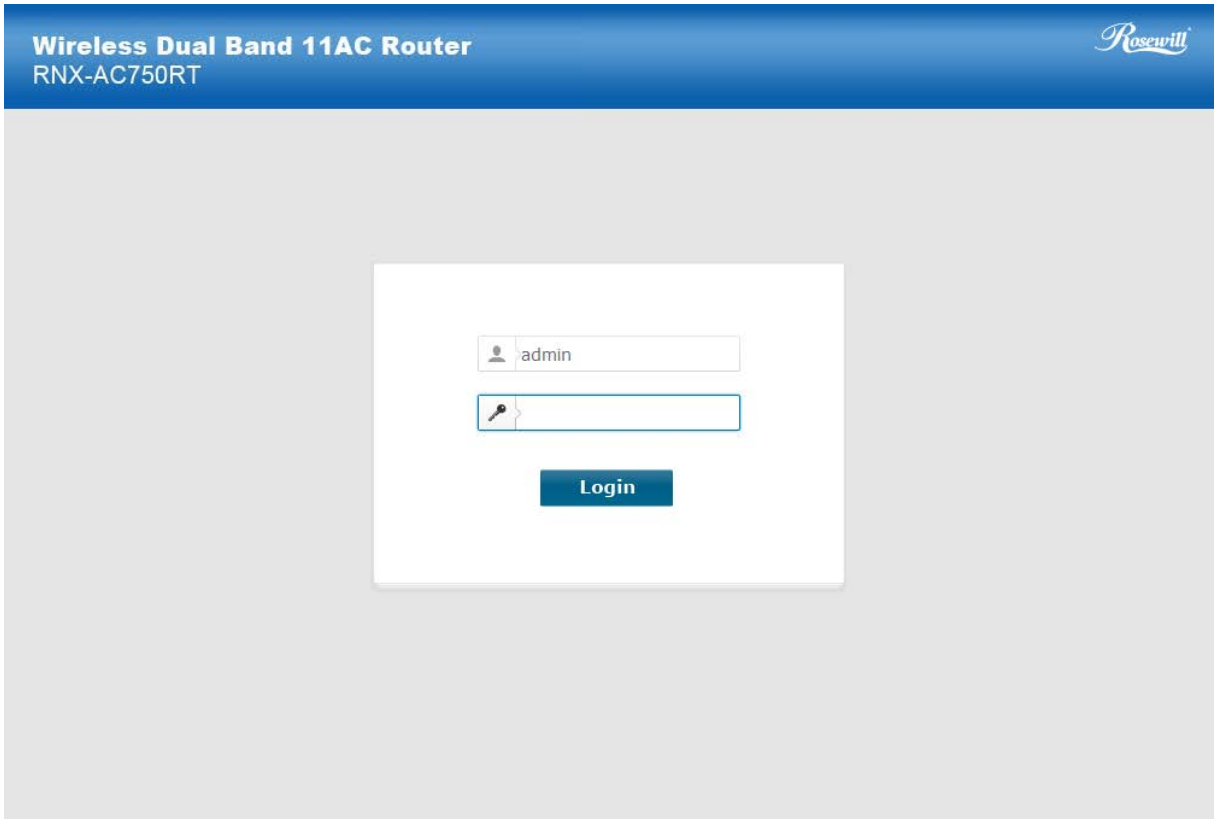


Figure 4-117 Logout

Appendix A: FAQ

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

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

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

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

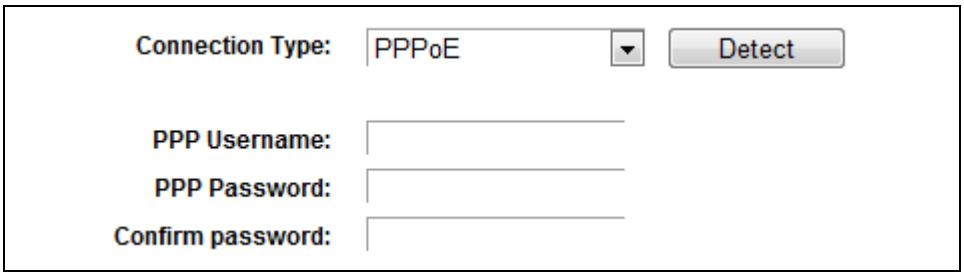


Figure A-1 PPPoE Connection Type

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 “Always on” for Internet connection mode.

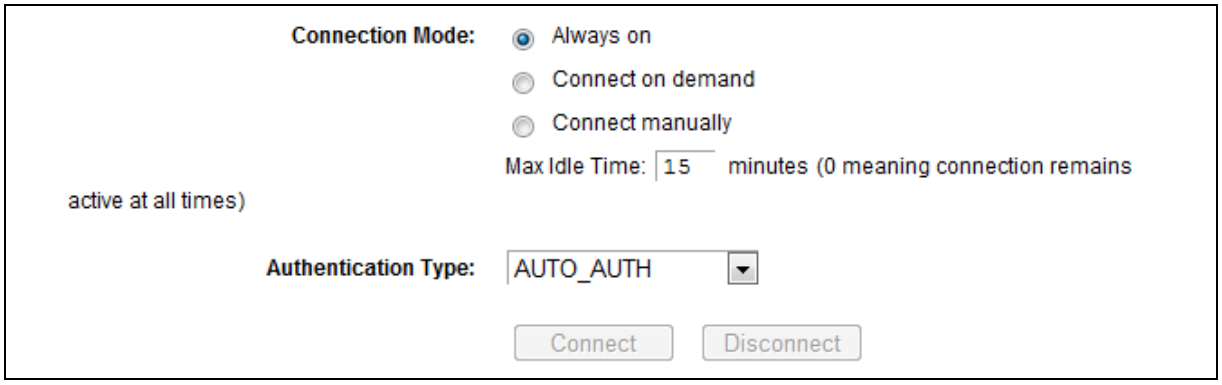


Figure A-2 PPPoE Connection Mode

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.

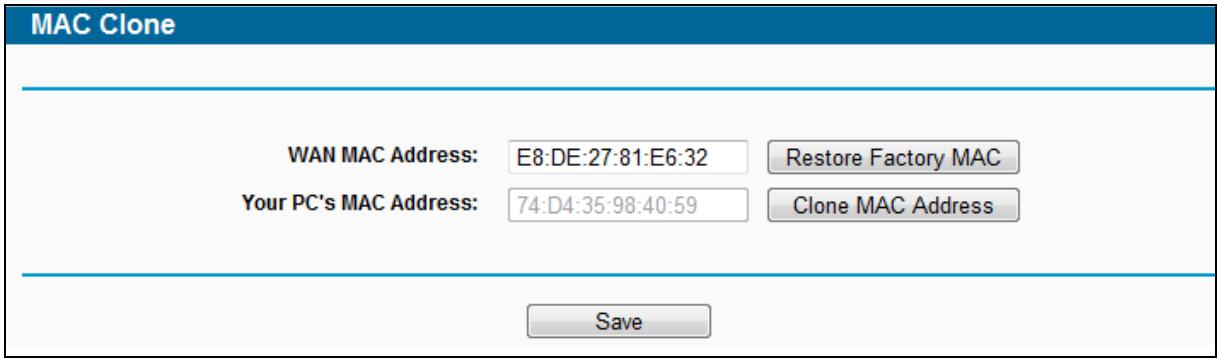


Figure A-3 MAC Clone

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 Server**" submenu. On the "**Virtual Server**" page, click **Add New**. Then enter “1720” for the “Service Port” blank, and your IP address for the “IP Address” blank, taking 192.168.1.169 for an example, remember to **Enable** and **Save**.

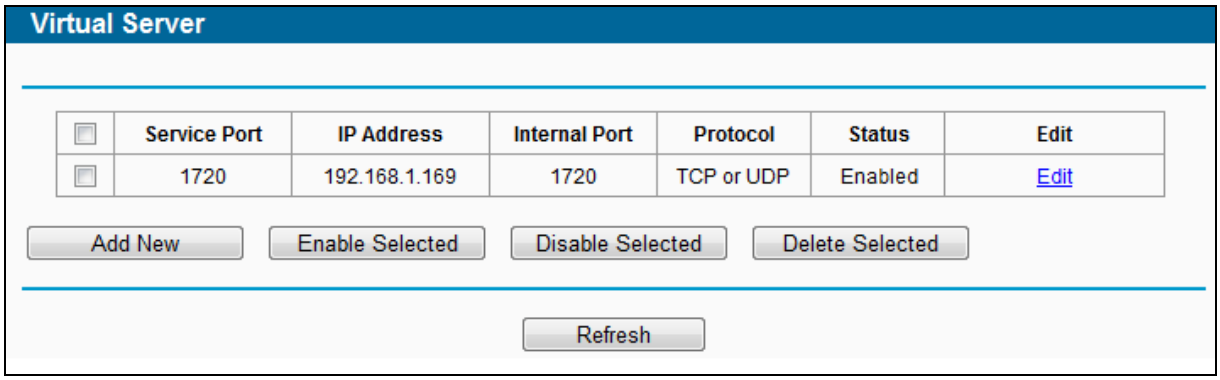


Figure A-4 Virtual Servers

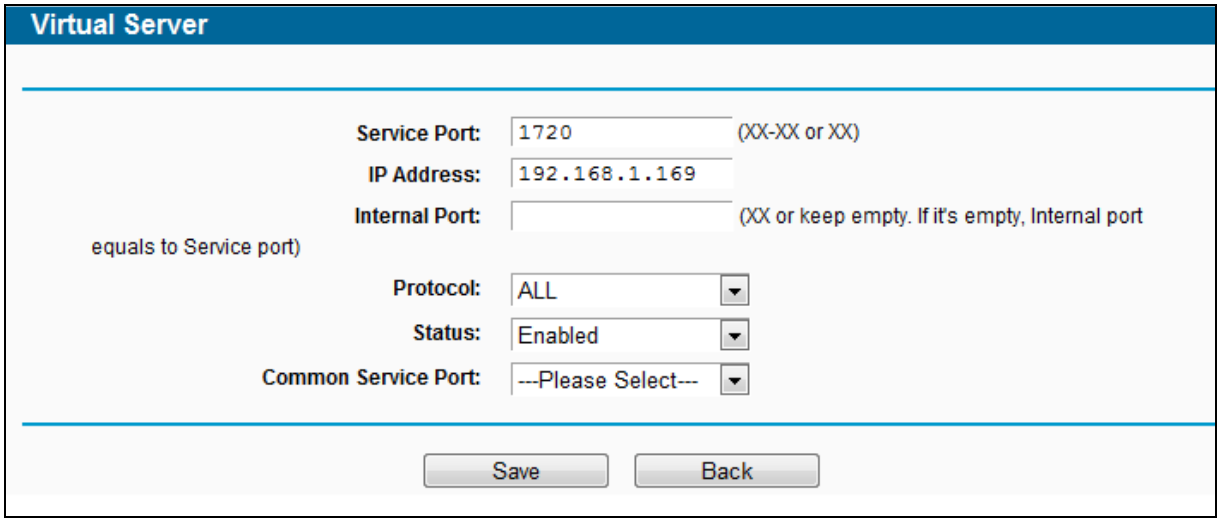


Figure A-5 Add or Modify a Virtual server Entry

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 192.168.1.169 as an example, remember to click the **Save** button.

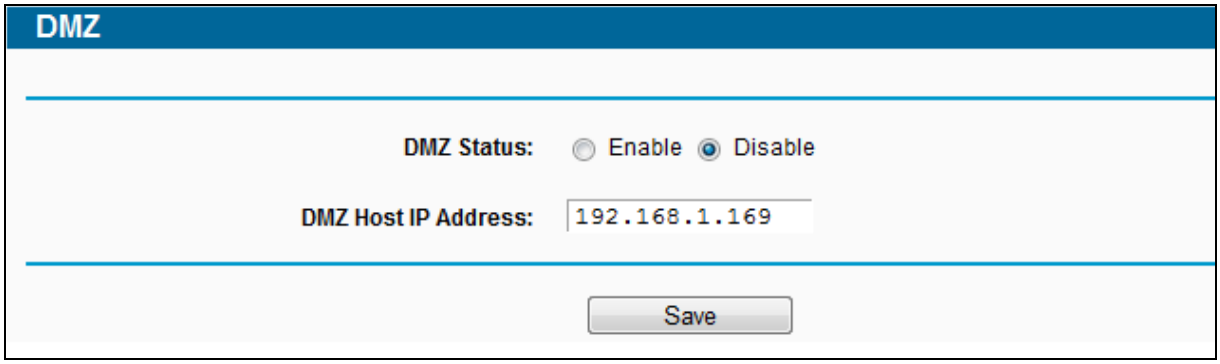


Figure A-6 DMZ

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.

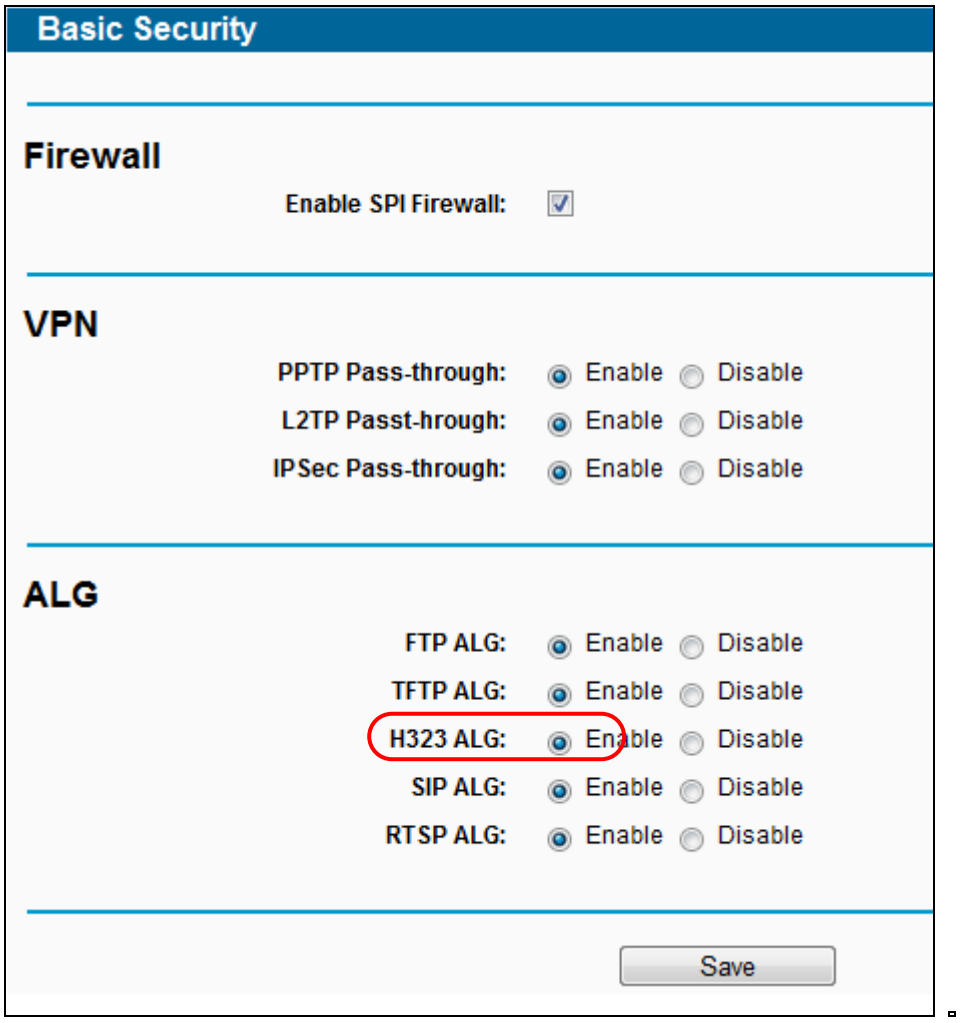


Figure A-7 Basic Security

4. The wireless stations cannot connect to the router.

1) Make sure the "**Wireless Radio Band**" 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 XP. First make sure your Ethernet Adapter is working, refer to the adapter's manual if needed.

1. Install TCP/IP component

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

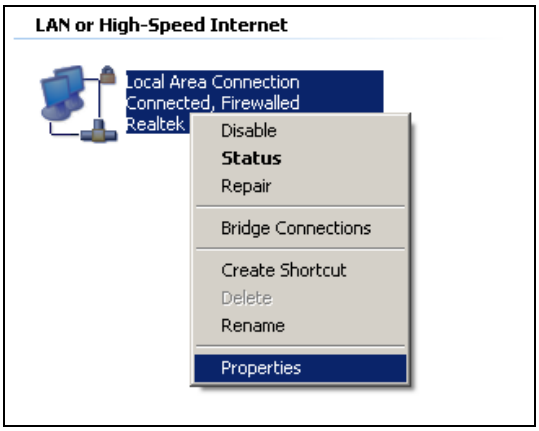


Figure B-1

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

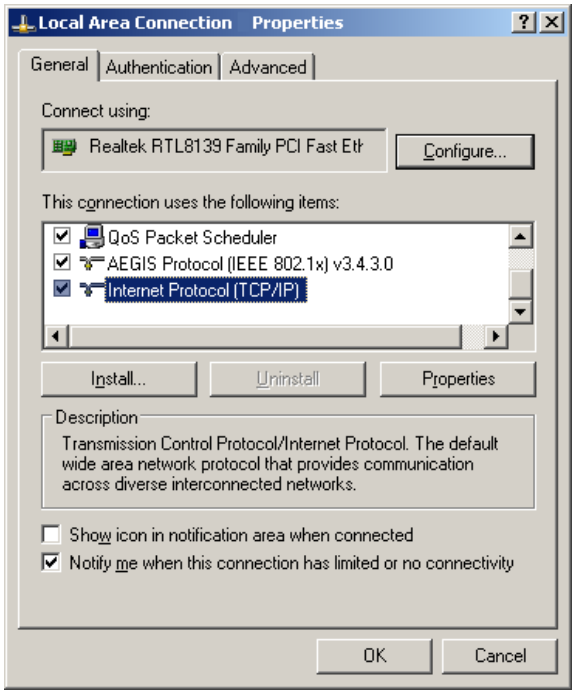


Figure B-2

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

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

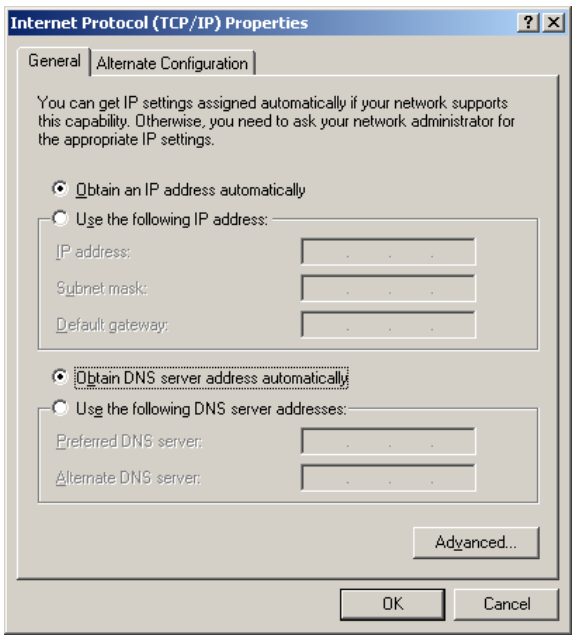


Figure B-3

Appendix C: Specifications

General	
Standards	IEEE 802.11ac, IEEE 802.11n, IEEE 802.11g, IEEE 802.11b, IEEE 802.11a, IEEE 802.11e, IEEE 802.11i, IEEE 802.1X, IEEE 802.3X, IEEE 802.3, IEEE 802.3u, IEEE 802.3ab
Protocols	TCP/IP, PPPoE, DHCP, ICMP, NAT, SNTP, IGMPv3, L2TP, PPTP, IPv6, MLD
Ports	1 10/100/1000M Auto-Negotiation Internet RJ45 port; 4 10/100/1000M Auto-Negotiation LAN RJ45 ports supporting Auto MDI/MDIX; 1 USB port supporting storage/FTP/Media;
Cabling Type	10BASE-T: UTP category 3, 4, 5 cable (maximum 100m) EIA/TIA-568 100Ω STP (maximum 100m)
	100BASE-TX: UTP category 5, 5e cable (maximum 100m) EIA/TIA-568 100Ω STP (maximum 100m)
	1000BASE-TX: UTP category 5, 5e cable (maximum 100m) EIA/TIA-568 100Ω STP (maximum 100m)
LEDs	Power, Wireless, Ethernet, Internet, WPS, USB
Safety & Emissions	FCC, CE
Wireless	
Frequency Band*	2.4GHz, 5GHz
Radio Data Rate	11b: 1/2/5.5/11Mbps 11a/g: 6/9/12/18/24/36/48/54/Mbps 11n: up to 300Mbps 11ac: up to 450Mbps
Frequency Expansion	DSSS (Direct Sequence Spread Spectrum)
Modulation	11ac: 256-QAM for OFDM 11n/g/a: QPSK,BPSK,16-QAM, 64-QAM for OFDM 11b: CCK,DQPSK,DBPSK
Security	WEP, WPA/WPA2, WPA2-PSK/WPA-PSK
Sensitivity @PER	5G： 11a 6Mbps：-91dBm 11a 54Mbps：-74dBm 11ac HT20：-66dBm 11ac HT40：-64dBm 11ac HT80：-61dBm 2.4G： 11g 54M：-74dBm 11n HT20：-72dmB 11n HT40：-69dBm
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

* Only 2.412GHz~2.462GHz is allowed to be used in USA, which means only channel 1~11 is available for American users to choose.

Appendix D: Glossary

- **802.11ac** - IEEE 802.11ac is a wireless computer networking standard of 802.11.This specification will enable multi-station WLAN throughput of at least 1 gigabit per second .This is accomplished by extending the air interface concepts embraced by 802.11n: wider RF bandwidth, more MIMO spatial streams, multi-user MIMO, and high-density modulation (up to 256 QAM).
- **802.11n -** 802.11n builds upon previous 802.11 standards by adding MIMO (multiple-input multiple-output). MIMO uses multiple transmitter and receiver antennas to allow for increased data throughput via spatial multiplexing and increased range by exploiting the spatial diversity, perhaps through coding schemes like Alamouti coding. The Enhanced Wireless Consortium (EWC) [3] was formed to help accelerate the IEEE 802.11n development process and promote a technology specification for interoperability of next-generation wireless local area networking (WLAN) products.
- **802.11b -** The 802.11b standard specifies a wireless networking at 11 Mbps using direct-sequence spread-spectrum (DSSS) technology and operating in the unlicensed radio spectrum at 2.4GHz, and WEP encryption for security. 802.11b networks are also referred to as Wi-Fi networks.
- **802.11g -** specification for wireless networking at 54 Mbps using direct-sequence spread-spectrum (DSSS) technology, using OFDM modulation and operating in the unlicensed radio spectrum at 2.4GHz, and backward compatibility with IEEE 802.11b devices, and WEP encryption for security.
- **DDNS** (**D**ynamic **D**omain **N**ame **S**ystem) **-** The capability of assigning a fixed host and domain name to a dynamic Internet IP Address.
- **DHCP** (**D**ynamic **H**ost **C**onfiguration **P**rotocol) **-** A protocol that automatically configure the TCP/IP parameters for the all the PC(s) that are connected to a DHCP server.
- **DMZ** (**De**militarized **Z**one) **-** A Demilitarized Zone allows one local host to be exposed to the Internet for a special-purpose service such as Internet gaming or videoconferencing.
- **DNS** (**D**omain **N**ame **S**ystem) **-** An Internet Service that translates the names of websites into IP addresses.
- **Domain Name -** A descriptive name for an address or group of addresses on the Internet.
- **DSL** (**D**igital **S**ubscriber **L**ine) **-** A technology that allows data to be sent or received over existing traditional phone lines.
- **ISP** (**I**nternet **S**ervice **P**rovider) **-** A company that provides access to the Internet.

- **MTU** (**Maximum Transmission Unit**) **-** The size in bytes of the largest packet that can be transmitted.
- **NAT** (**N**etwork **A**ddress **T**ranslation) **-** NAT technology translates IP addresses of a local area network to a different IP address for the Internet.
- **PPPoE** (**P**oint to **P**oint **P**rotocol **o**ver **E**thernet) **-** PPPoE is a protocol for connecting remote hosts to the Internet over an always-on connection by simulating a dial-up connection.
- **SSID -** A **S**ervice **S**et **Id**entification is a thirty-two character (maximum) alphanumeric key identifying a wireless local area network. For the wireless devices in a network to communicate with each other, all devices must be configured with the same SSID. This is typically the configuration parameter for a wireless PC card. It corresponds to the ESSID in the wireless Access Point and to the wireless network name.
- **WEP** (**W**ired **E**quivalent **P**rivacy) **-** A data privacy mechanism based on a 64-bit or 128-bit or 152-bit shared key algorithm, as described in the IEEE 802.11 standard.
- **Wi-Fi -** A trade name for the 802.11b wireless networking standard, given by the Wireless Ethernet Compatibility Alliance (WECA, see http://www.wi-fi.net), an industry standards group promoting interoperability among 802.11b devices.
- **WLAN** (**W**ireless **L**ocal **A**rea **N**etwork) **-** A group of computers and associated devices communicate with each other wirelessly, which network serving users are limited in a local area.