Wireless Router RNX-N150RT

User Manual

REV：2.0.0
1910020644

COPYRIGHT & TRADEMARKS

Specifications are subject to change without notice. Rosewill® is a registered trademark of Rosewill Limited. Other brands and product names are trademarks or registered trademarks of their respective holders.

http://www.rosewill.com

FCC STATEMENT

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

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

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

1) This device may not cause harmful interference.

a) 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.”

Limited to local law, only CH1-CH11 can be used in united state and the function of select country code was disabled

CE Mark Warning

CE

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 mWe.i.r.p. within the band 2454-2483.5 MHz	Military Radiolocation use. Refarming of the 2.4 GHz band hasbeen 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 aradius 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

The following items should be found in your package:

- RNX-N150RT 150Mbps Wireless N Router
- Power Adapter for RNX-N150RT 150Mbps Wireless N Router
- Quick Installation Guide
- Resource CD for RNX-N150RT 150Mbps Wireless N Router, including:
  - This Guide
  - Other Helpful Information

☞Note:

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

Chapter 1. Introduction

Thank you for choosing the RNX-N150RT 150Mbps Wireless N Router.

1.1 Overview of the router

The RNX-N150RT 150Mbps Wireless N Router integrates 4-port Switch, Firewall, NAT-Router and Wireless AP. The 150Mbps Wireless N 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.

Incredible

The RNX-N150RT 150Mbps Wireless N Router provides up to 150Mbps wireless connection with other 802.11n wireless clients. The speed makes it ideal for handling multiple data streams at the same time, which ensures your network stable and smooth. It is compatible with all IEEE 802.11g and IEEE 802.11b products.

Multiple Security Protections

With multiple protection measures, including SSID broadcast control and wireless LAN 64/128/152-bit WEP encryption, WiFi protected Access (WPA2- PSK, WPA- PSK), as well as advanced Firewall protections, the RNX-N150RT 150Mbps Wireless N Router provides complete data privacy.

Flexible Access

The RNX-N150RT 150Mbps Wireless N 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 Main Features

- Make use of IEEE 802.11nwireless technology to provide a wireless data rate of up to 150Mbps.
- One 10/100M Auto-Negotiation RJ45 WAN port, four 10/100MAuto-NegotiationRJ45 LAN ports, supporting Auto MDI/MDIX.
- 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 Internet access.
- Supports Virtual Server, Special Application and DMZ host.
- Supports UPnP, Dynamic DNS, Static Routing.
- Provides Automatic-connection and Scheduled Connection on certain time to the Internet.
- Connects Internet on demand and disconnects from the Internet when idle for PPPoE.
- Built-in NAT and DHCP server supporting static IP address distributing.
- Supports Stateful Packet Inspection.
- Supports VPN Passthrough.
- Supports Parental Control and Access Control.
- Provides 64/128/152-bit WEP encryption security and wireless LAN ACL (Access Control List).
- Supports Flow Statistics.
- Supports firmware upgrade and Web management.

1.3 Panel Layout

1.3.1 The Front Panel

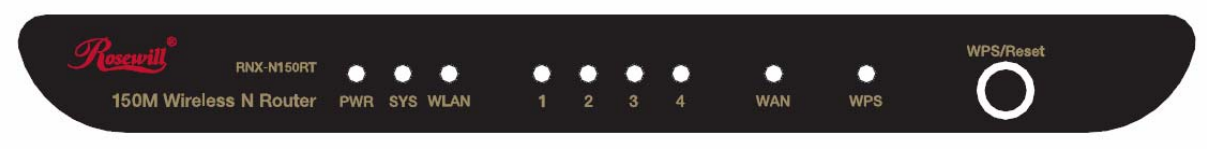


Figure 1-1 Front Panel sketch

The router's LEDs and the WPS/Reset Button are located on the front panel (View from left to right).

Name	Status	Indication
PWR	Off	Power is off.
	On	Power is on.

SYS	Off	The router has a system error.
	On	The router is working properly.
	Flashing	The router is initializing.
WLAN	Off	The Wireless function is disabled.
	Flashing	The Wireless function is enabled.
WAN, 1,2,3,4 (LAN)	Off	There is no device linked to the corresponding port.
	On	There is a device linked to the corresponding port but there is no activity.
	Flashing	There is an active device linked to the corresponding port.
WPS	On	A wireless device has been successfully added to the network by WPS function. The LED will keep on for about 5 minutes.
	Slow Flash	A wireless device is connecting to the network by WPS function. This process will last for about 2 minutes.
	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. When press and hold the WPS/Reset Button for more than 5 seconds, you will reset the router.

1.3.2 The Rear Panel

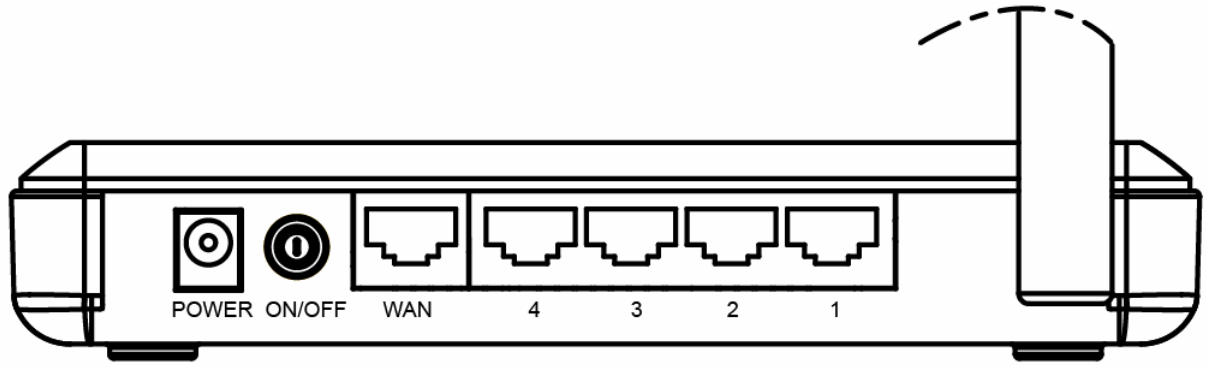


Figure 1-2 Rear Panel sketch

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

- **POWER:** The Power socket is where you will connect the power adapter. Please use the power adapter provided with this RNX-N150RT 150Mbps Wireless N Router.
- **WAN:** This WAN port is where you will connect the DSL/cable Modem, or Ethernet.
- **1,2,3,4 (LAN):** These ports (1, 2, 3, 4) connect the router to the local PC(s).
- **Wireless antenna:** To receive and transmit the wireless data.

Chapter 2. Connecting the router

2.1 System Requirements

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

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

To connect the router, please follow the steps below:

1) Locate an optimum location for the router. The best place is usually at the center of your wireless network. The place must accord with the Installation Environment Requirements.
2) Adjust the direction of the antenna. Normally, upright is a good direction.

After finishing the steps above, please choose the operation mode you need and carry out the corresponding steps. There are five operation mode supported by this router: **Client Router, Router, Multi-SSID, Repeater, Bridge with AP** and **Client**.

a) Client Router Mode

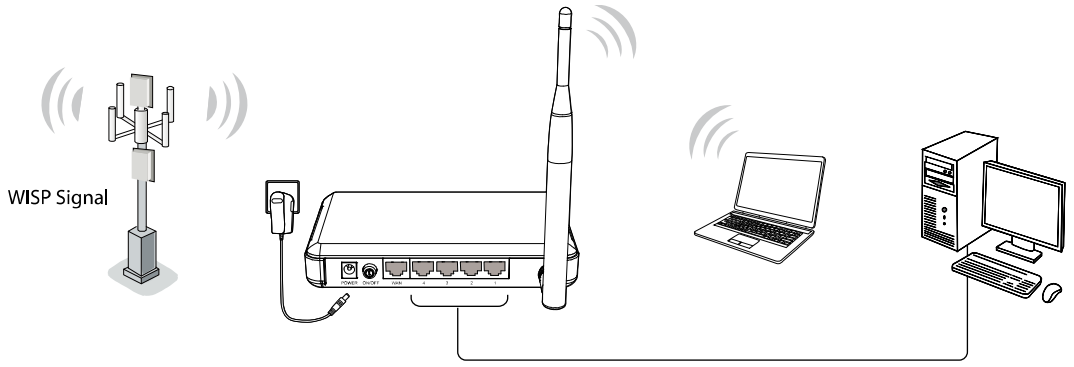


Figure 2-1 Hardware Installation of the RNX-N150RT in Client Router mode

1. Connect the notebook/PC to the LAN port of RNX-N150RT router with an Ethernet cable.
2. Plug one end of the provided power adapter into the POWER jack of the router, and the other end to a standard electrical wall socket.
3. Press the ON/OFF button of the router.

b) Router Mode

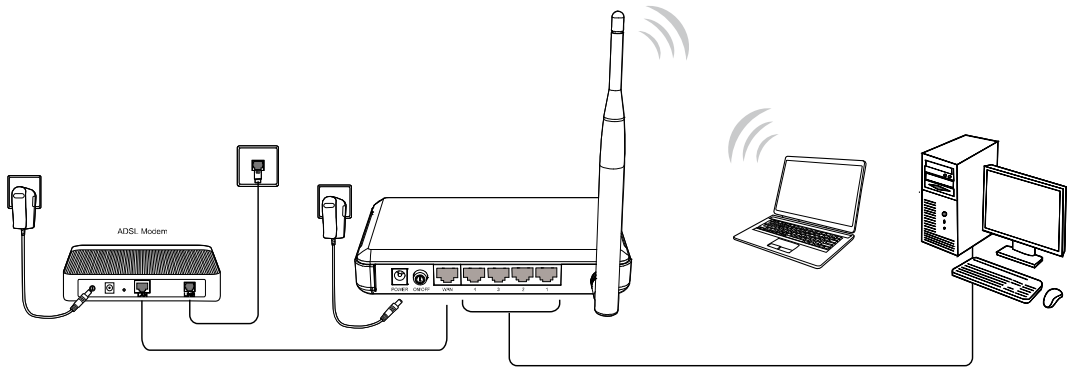


Figure 2-2 Hardware Installation of the RNX-N150RT in Router mode

1. Connect the PC(s)/Switch/Hub in your LAN to the LAN Ports on the router.
2. Connect the DSL/Cable Modem to the INTERNET port on the router.
3. Plug one end of the provided power adapter into the POWER jack of the router, and the other end to a standard electrical wall socket.
4. Press the ON/OFF button of the router.

c) Multi-SSID Mode

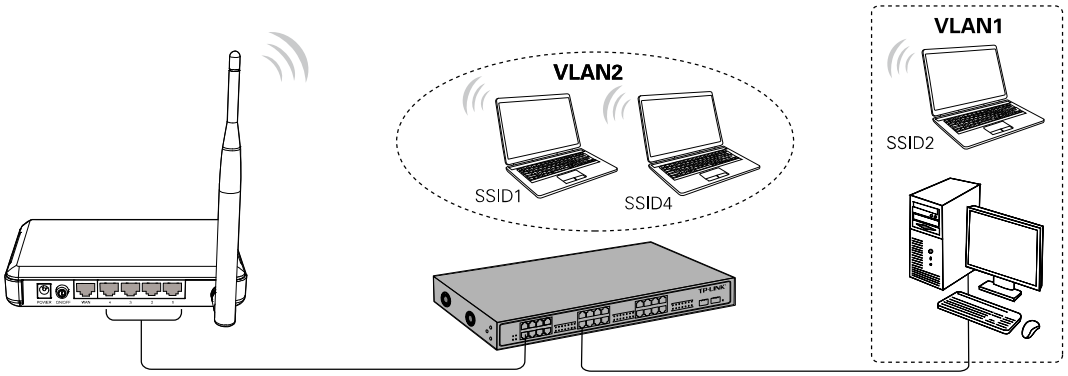


Figure 2-3 Hardware Installation of the RNX-N150RT in Multi-SSID mode

1. Connect the Switch to the LAN Ports of the router.
2. Connect the PC's to the LAN ports of the Switch.
3. Plug one end of the provided power adapter into the POWER jack of the router, and the other end to a standard electrical wall socket.
4. Press the ON/OFF button of the router.

d) Repeater Mode (Range Extender)

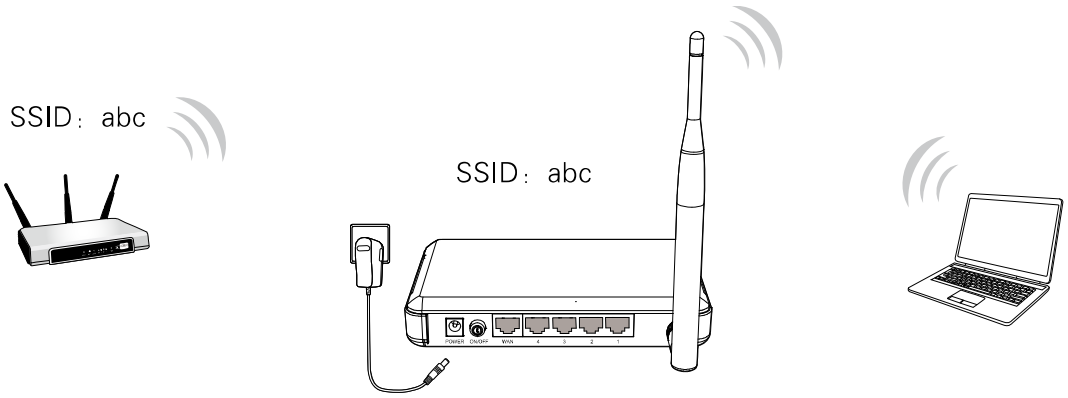


Figure 2-4 Hardware Installation of the RNX-N150RT in Repeater mode

1. Plug one end of the provided power adapter into the POWER jack of the router, and the other end to a standard electrical wall socket.
2. Press the ON/OFF button of the router.

Note:

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

e) Bridge with AP Mode

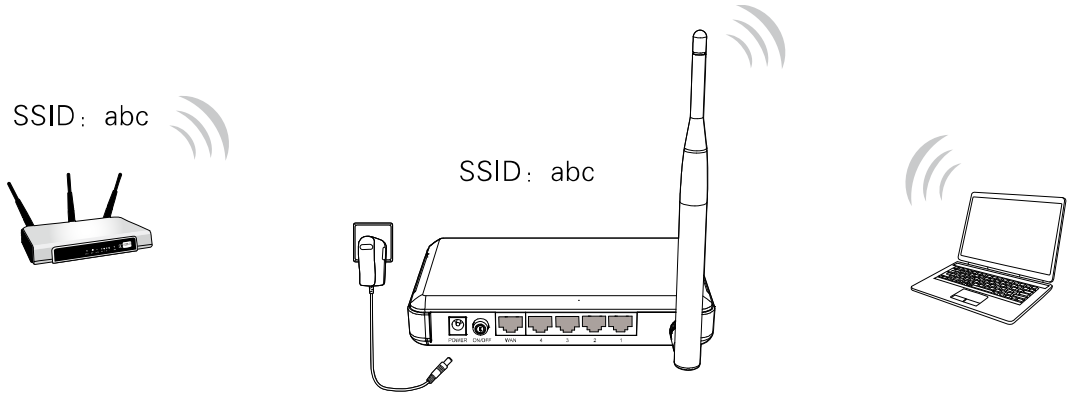


Figure 2-5 Hardware Installation of the RNX-N150RT in Bridge with AP mode

1. Plug one end of the provided power adapter into the POWER jack of the router, and the other end to a standard electrical wall socket.
2. Press the ON/OFF button of the router.

Note:

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

f) Client Mode

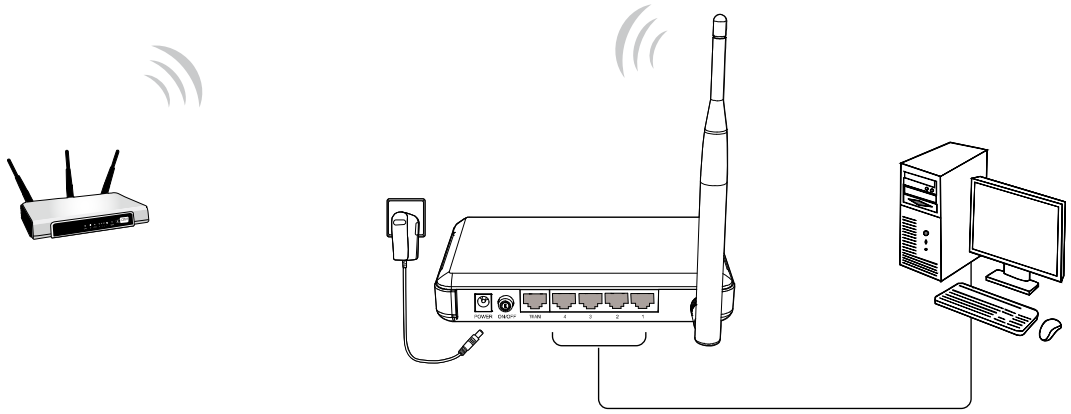


Figure 2-6 Hardware Installation of the RNX-N150RT in Client mode

1. Connect the PC to the LAN port of RNX-N150RT router with an Ethernet cable.
2. Plug one end of the provided power adapter into the POWER jack of the router, and the other end to a standard electrical wall socket.
3. Press the ON/OFF button of the router.

Chapter 3. Quick Installation Guide

This chapter will show you how to configure the basic functions of your RNX-N150RT 150Mbps Wireless N Router using **Quick Setup Wizard** within minutes.

3.1 TCP/IP Configuration

The default IP address of the RNX-N150RT 150Mbps Wireless N 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 in the following two ways.

- Configure the IP address manually

  1) Set up the TCP/IP Protocol for your PC. If you need instructions as to how to do this, please refer to Appendix B: Configuring the PC.

  2) Configure the network parameters. The IP address is 192.168.1.xxx ("xxx" is any number from 2 to 254), Subnet Mask is 255.255.255.0, and Gateway is 192.168.1.1 (The router's default IP address).

- Obtain an IP address automatically

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

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

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 2000 OS.

Open a command prompt, and typing *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.

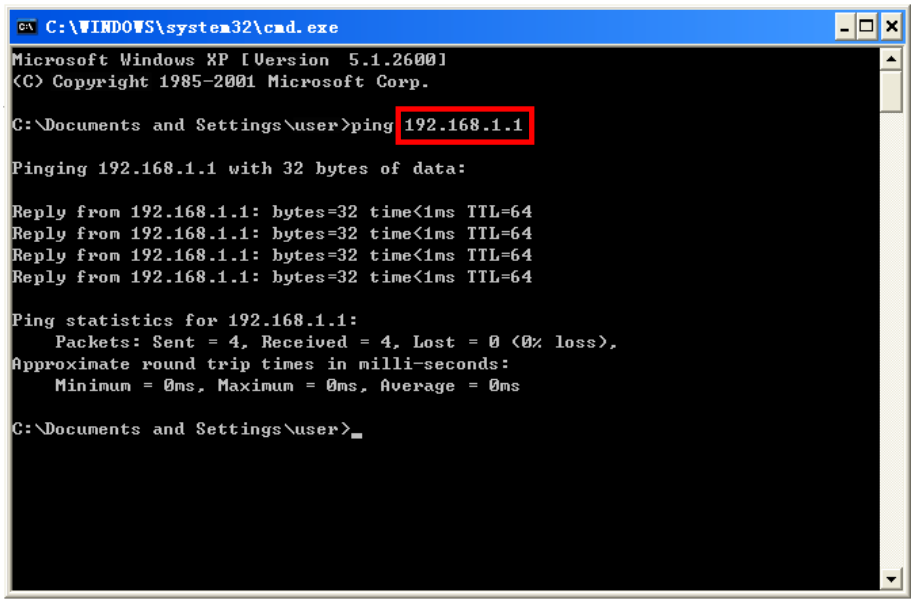


Figure 3-1 Success result of Ping command

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

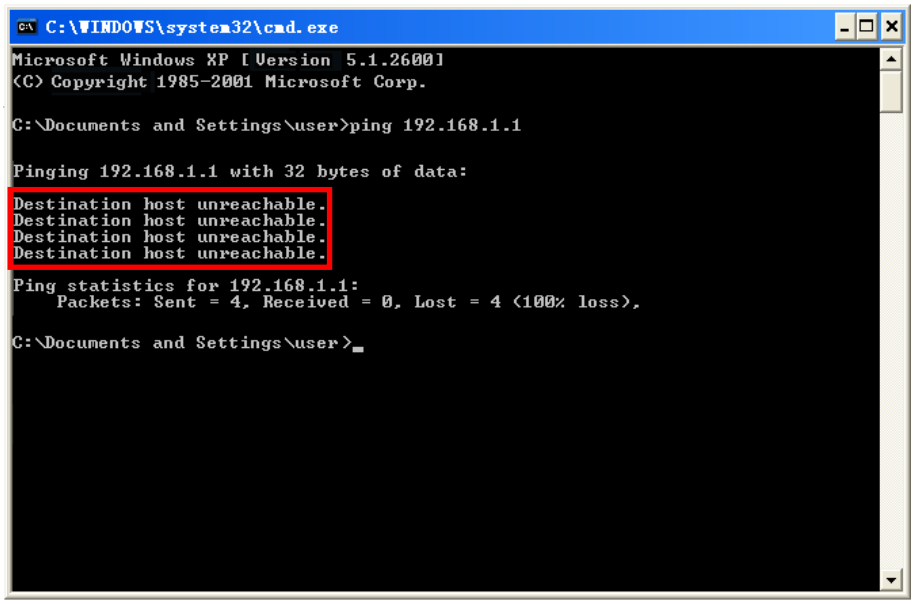


Figure 3-2 Failure result of Ping command

Please check the connection following these steps:

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

☞Note:

The1/2/3/4 LEDs of LAN ports which you link to 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. Please keep in mind that if this is the second layer of your network (eg. Cable RNX-N150RT's WAN port plug into another router's LAN port, you may need to manually adjust the default IP for RNX-N150RT to avoid IP address conflict. Eg. Your current router's IP is already 192.168.1.1, then you will need to change to 192.168.x.1; X can be any number from 2~254.)

3.2 Quick Installation Guide

With a Web-based utility, it is easy to configure and manage the RNX-N150RT 150Mbps Wireless N 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 address http://192.168.1.1 in the address field of the browser.

Figure 3-3 Log in the router

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

Figure 3-4 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 successfully log in, you can click the **Quick Setup** menu to quickly configure your router.

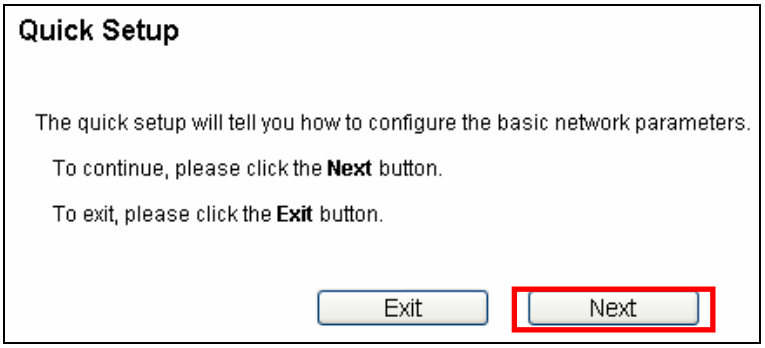


Figure 3-5 Quick Setup

3. Click **Next**, and then **Operation Mode** page will appear, as shown in Figure 3-6.

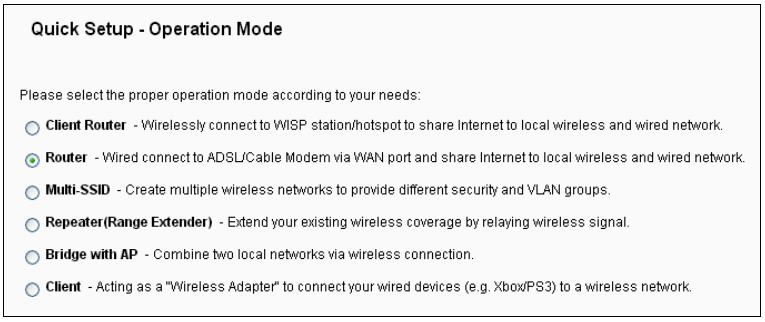


Figure 3-6 Operation Mode

Note:

The router supports six operation modes for multi-user to access the Internet: Client Router, Router, Repeater, Bridge with AP and Client. If you are unsure about which one to select, please refer to **Operation Mode Help** page. You can configure your device quickly by the following steps in different modes.

3.2.1 Configuration for Client Router Mode

When you choose **Client Router** on **Operation Mode** page in Figure 3-6, take the following steps:

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

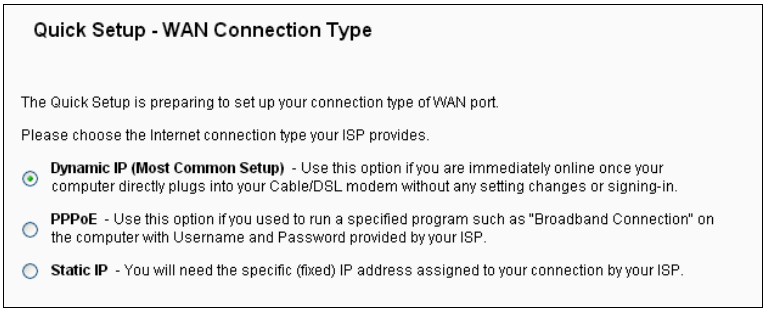


Figure 3-7 Wan Connection Type

The router in Client Router mode supports three popular ways to connect to the Internet. Please select the one compatible with your ISP.

2. Click **Next** to enter the necessary network parameters.

a) If you choose "**Dynamic IP**", the router will automatically receive the IP parameters from your ISP without needing to enter any parameters.

b) If you choose "**PPPoE**", you will see this page shown in Figure 3-8.

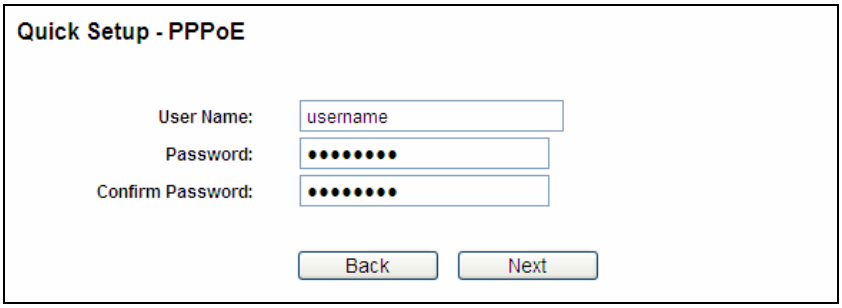


Figure 3-8 PPPoE

- **User Name and Password -** Enter the User Name and Password provided by your ISP. These fields are case-sensitive.
- **Confirm Password -** Enter again the Password provided by your ISP to ensure the password you entered is correct.

c) If you Choose "**Static IP**", the Static IP settings page will appear as shown in Figure 3-9.

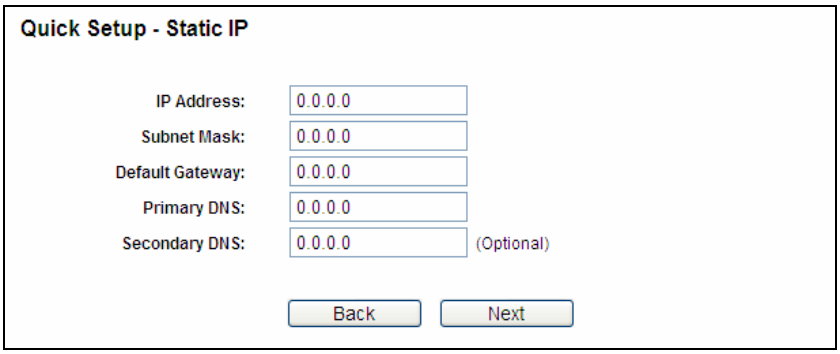


Figure 3-9 Static IP

Note:

The IP parameters should have been provided by your ISP.

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

3. After you have completed the above, click **Next**, the WISP Station Setting page will appear as below.

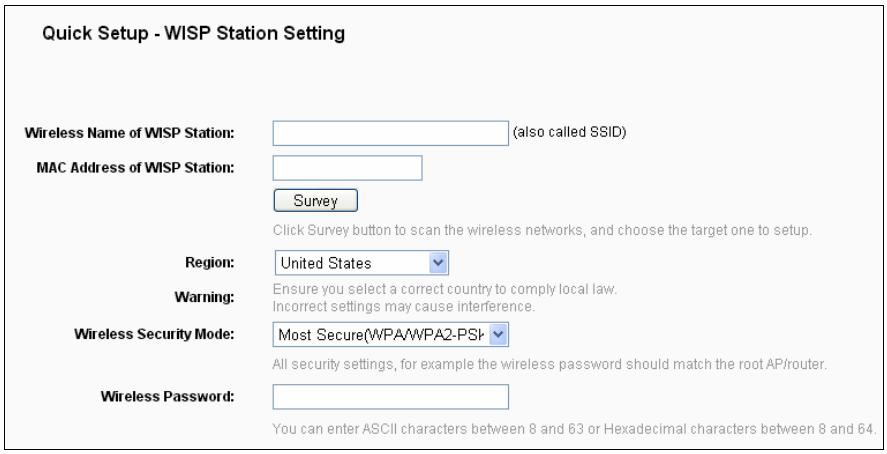


Figure 3-10 WISP Station Setting

- **Wireless Name of WISP Station**（SSID）**-** The SSID of the AP your router is going to connect to as a client. You can also use the search function to select the SSID to join.
- **MAC Address of WISP Station**（BSSID）**-** The BSSID of the AP your router is going to connect to as a client. You can also use the search function to select the BSSID to join.
- **Survey -** Click this button, you can survey the AP which runs in the current channel.
- **Region -** Select your region from the pull-down list. This field specifies the region where the wireless function of the router can be used. It may be illegal to use the wireless function of the router in a region other than one of those specified in this field. If your country or region is not listed, please contact your local government agency for assistance.

When you select your local region from the pull-down list, 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.

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

Click **Survey** button on the Wireless page as shown in Figure 3-10, and then AP List page will appear as shown in Figure 3-11. Find the SSID of the Access Point you want to access, and click **Connect** in the corresponding row. For example, the first item is selected. The target network's SSID will be automatically filled into the corresponding box which is shown as the Figure 3-12.

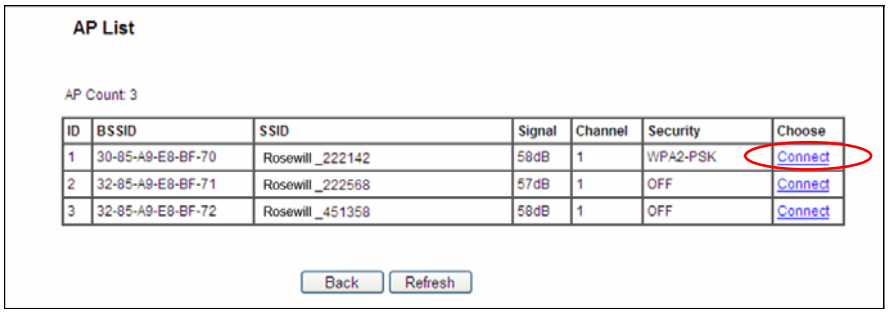


Figure 3-11 AP List

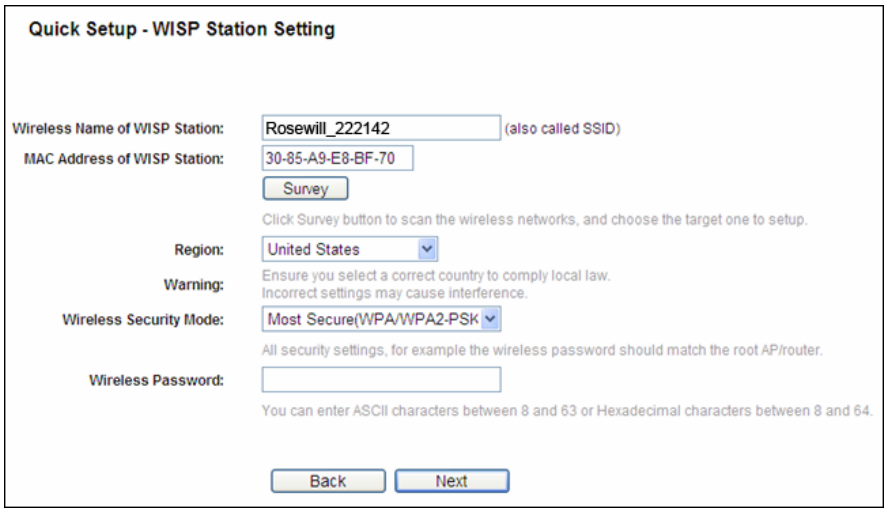


Figure 3-12 WISP Station Setting

Note:

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

4. Click the **Next** button in Figure 3-12, the Local Wireless AP Setting page will appear as below.

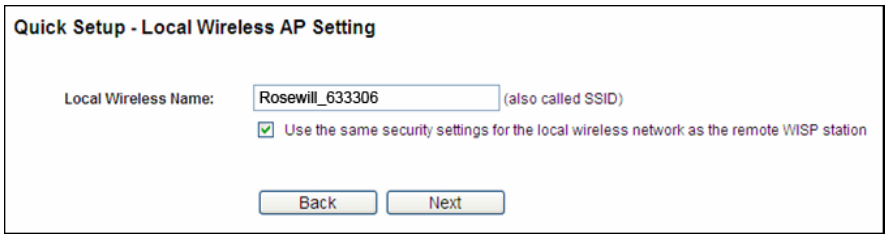


Figure 3-13 Local Wireless AP Setting

- **Local Wireless Name -** Enter a string of up to 32 characters. The same Name (SSID) must be assigned to all wireless devices in your network. The default SSID is set to be **Rosewill_XXXXXX** (xxxxxx indicates the last unique six characters of each Device's MAC address), which can ensure your wireless network security. But it is recommended strongly

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

5. Click the **Next** button in Figure 3-13. You will then see the page as shown in Figure 3-14. Please click the **Reboot** button to make your configuration take effect and finish the **Quick Setup**.

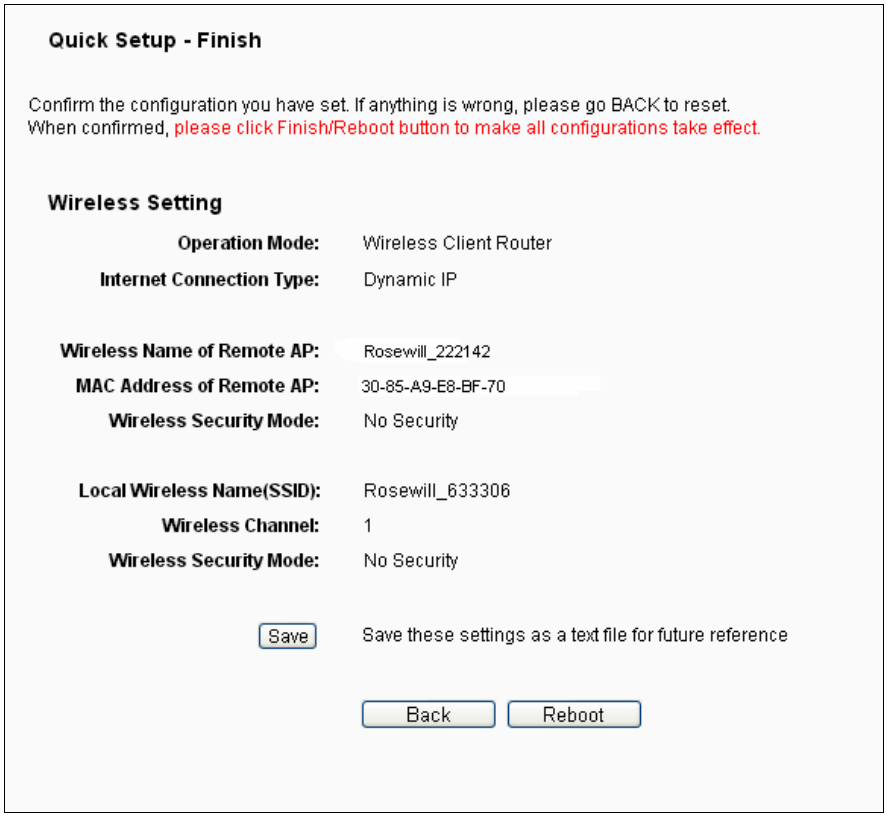


Figure 3-14 Finish

Note:

You may click the **Save** button to save these settings as a text file for future reference.

3.2.2 Configuration for Router Mode

When you choose **Router** on **Operation Mode** page as shown in Figure 3-6, take the following steps:

1. Click **Next**, and then **WAN Connection Type** page will appear, shown in Figure 3-15.

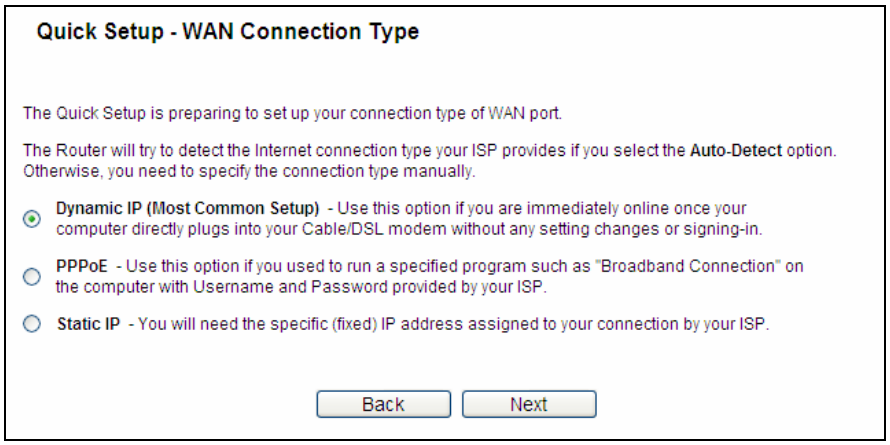


Figure 3-15 WAN Connection Type

The router supports three popular ways **Dynamic IP**, **PPPoE** and **Static IP** to connect to the Internet. Please select the very type and click **Next** to continue configuring.

2. 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.

   1) If the connection type is **Dynamic IP**, the next screen will appear as shown in Figure 3-16. **MAC Clone** is necessary for most users using Cable Modem. It's highly recommended to do this on the **MAIN COMPUTER** that was originally connected to your Cable Modem.

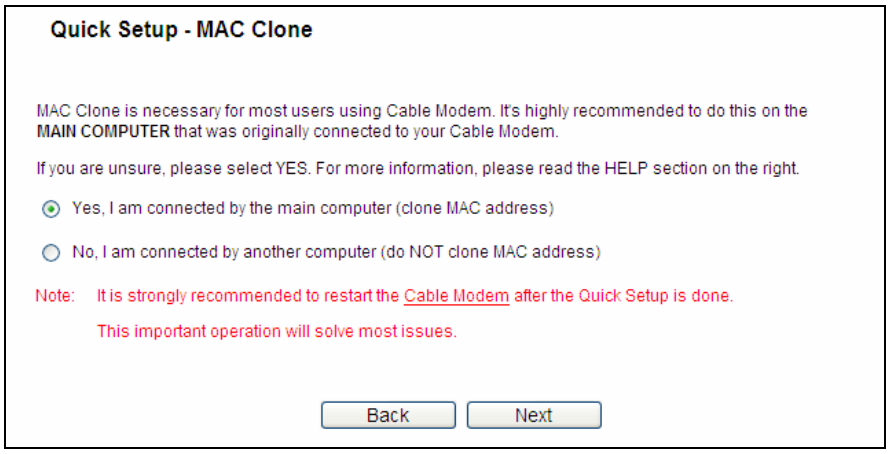


Figure 3-16 MAC Clone

   2) If the connection type is **PPPoE**, the next screen will appear as shown in Figure 3-17.

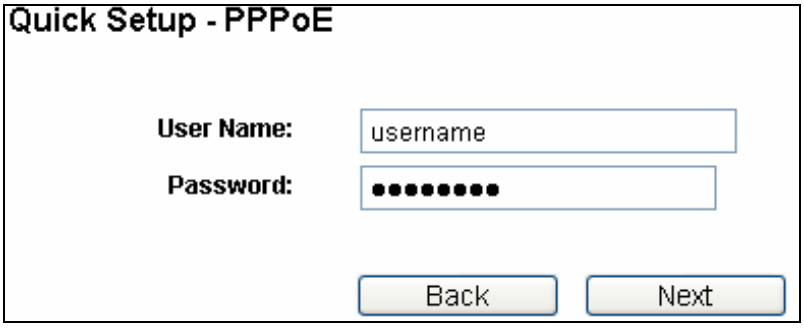


Figure 3-17 Quick Setup - PPPoE

- **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.

3) If the connection type is Static IP, the next screen will appear as shown in Figure 3-18.

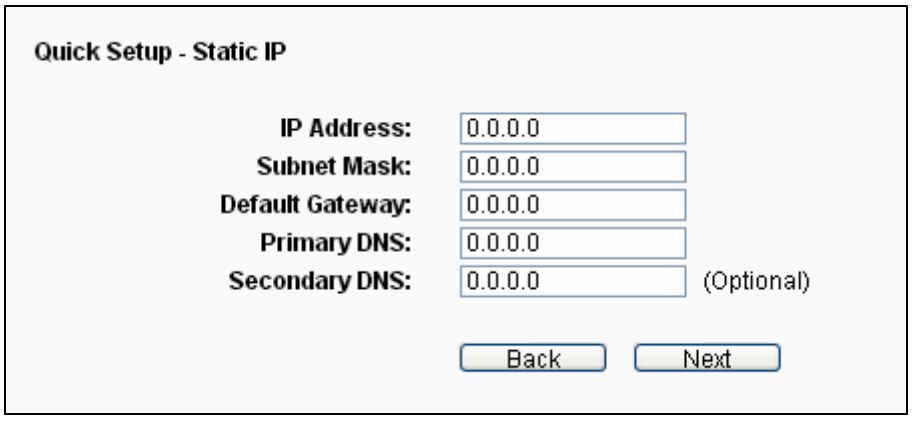


Figure 3-18 Quick Setup - Static IP

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

3. Click **Next** to continue, the Wireless settings page will appear as shown in Figure 3-19.

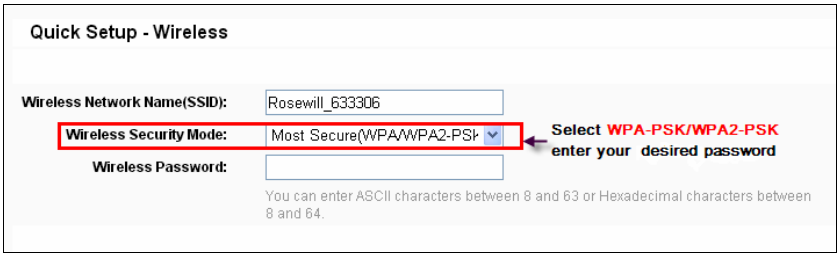


Figure 3-19 Quick Setup –Wireless

- **Wireless Network Name (SSID) -** Enter a value of up to 32 characters. The same name of SSID (Service Set Identification) must be assigned to all wireless devices in your network. Considering your wireless network security, the default SSID is set to be (Rosewill_XXXXXX indicates the last unique six numbers of each router's MAC address). This value is case-sensitive. For example, *TEST* is NOT the same as *test*.
- **Wireless Security Mode -** You can select one of the following security options:
  - **Most Secure (WPA/WPA2-PSK) -** Select WPA based on pre-shared passphrase.
  - **Secure (WEP)-** Select WEP based on none pre-shared passphrase.

- **No Security -** The wireless security function is disabled. The wireless stations will be able to connect the Device without encryption.

➢ **Wireless Password -** Enter an 8 to 63 character alphanumeric pass-phrase. For good security it should be of enough length and should not be a commonly known phrase.

These settings are only for basic wireless parameters. For advanced settings, please refer to Section 4.7 Wireless.

3. Click the **Next** button. You will see the page as shown in Figure 3-20. Please click the **Reboot/Finish** button to make your configuration take effect and finish the **Quick Setup**.

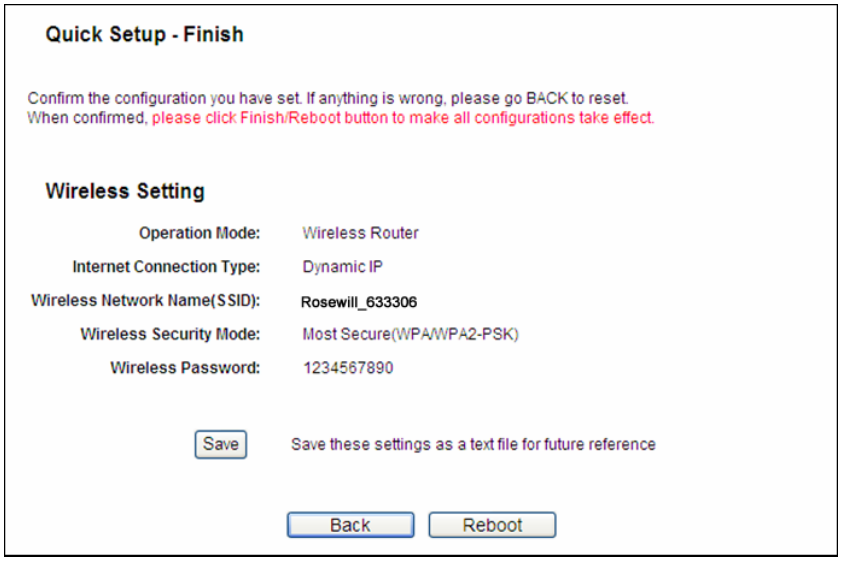


Figure 3-20 Quick Setup – Finish

Note:

You may click the **Save** button to save these settings as a text file for future reference.

3.2.3 Configuration for Multi-SSID

When you choose **Router** on **Operation Mode** page as shown in Figure 3-6, take the following steps:

Click **Next**, and then **WAN Connection Type** page will appear as shown in Figure 3-21.

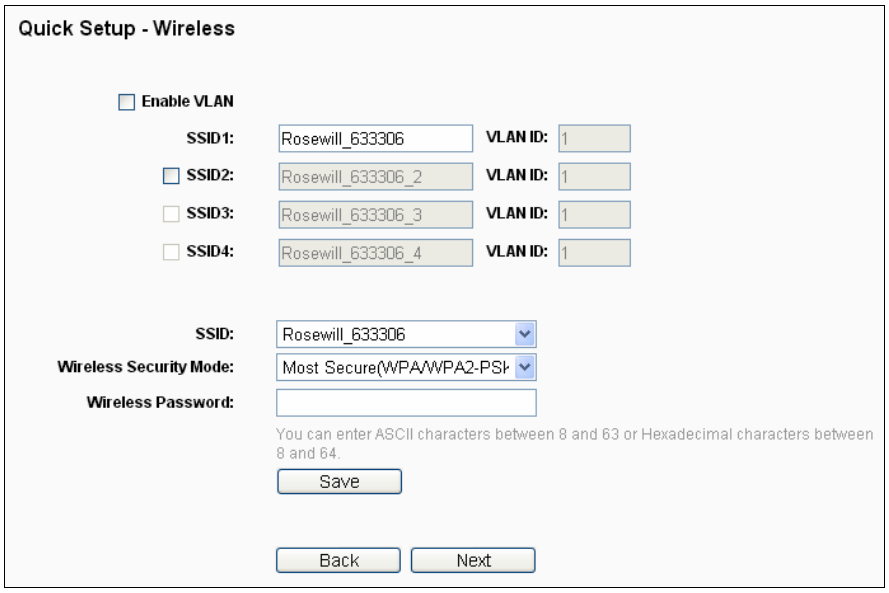


Figure 3-21 Quick Setup – Wireless

You are suggested to implement Multi-SSID function with a switch that supports Tag VLAN feature. For advanced configuration of this step, please refer to explanations of this mode in 4.7.1.3 Wireless Settings in Multi-SSID.

3.2.4 Configuration for Repeater Mode

When you choose Repeater on **Operation Mode** page as shown in Figure 3-6, take the following steps:

1. Click **Next**, and then Wireless page will appear as shown in Figure 3-22.

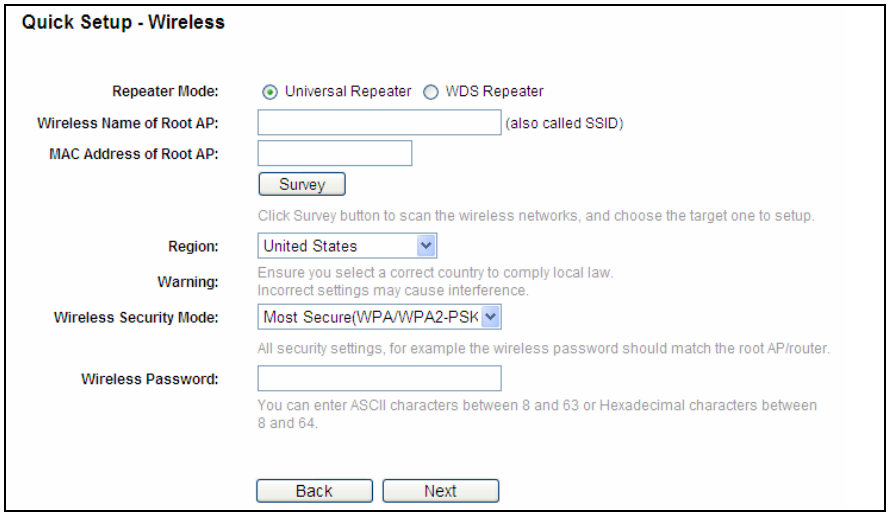


Figure 3-22 Quick Setup – Wireless

- **Repeater Mode -** Choosing WDS Repeater is to enable WDS, while choosing Universal Repeater is to disable WDS. If WDS is enabled, all traffic from wired networks will be forwarded in the format of WDS frames consisting of four address fields. If WDS is disabled, three address frames are used.

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

  When you select your local region from the pull-down list, 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.

- **Wireless Security Mode -** You can select one of the following security options:
  - **Most Secure (WPA/WPA2-PSK) -** Select WPA based on pre-shared passphrase.
  - **Secure (WEP)-** Select WEP based on none pre-shared passphrase.
  - **No Security -** The wireless security function is disabled. The wireless stations will be able to connect the Device without encryption.
- **Wireless Password -** Enter an 8 to 63 character alphanumeric pass-phrase. For good security it should be of enough length and should not be a commonly known phrase.

These settings are only for basic wireless parameters. For advanced settings, please refer to Section 4.7 Wireless.

Click **Survey** button on the Wireless page as shown in Figure 3-22, and then AP List page will appear as shown in Figure 3-23. Find the SSID of the Access Point you want to access, and click **Connect** in the corresponding row. For example, the first item is selected. The target network's SSID will be automatically filled into the corresponding box which is shown as the Figure 3-24.

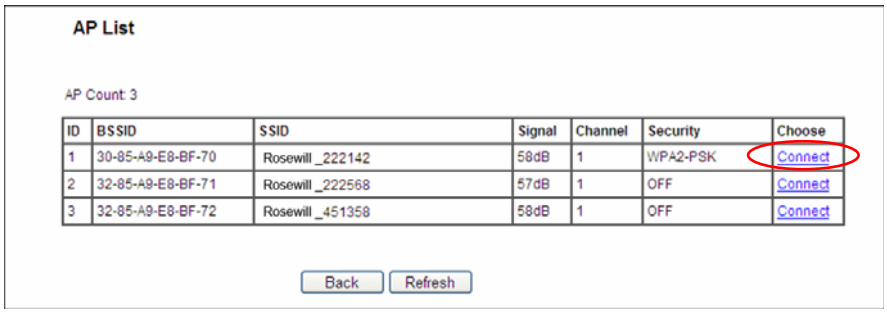


Figure 3-23 AP List

Figure 3-24 Quick Setup – Wireless

Note:

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

2. Click **Next**, and then Network page will appear as shown in Figure 3-25. You can configure the IP parameters of LAN on this page.

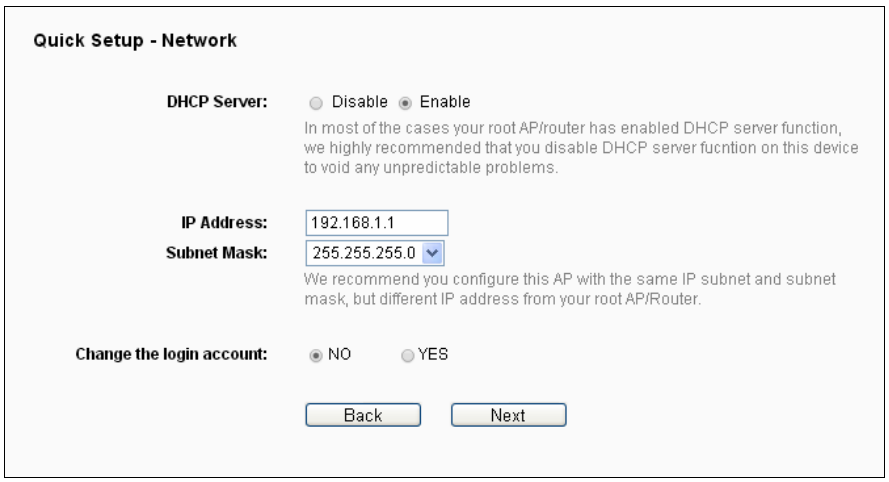


Figure 3-25 Quick Setup – Network

- **DHCP Server - Enable** or **Disable** the server. If you disable the Server, you must have another DHCP server within your network or else you must configure the IP address of the computer manually.
- **IP Address -** Enter the IP address of your system in dotted-decimal notation (factory default: 192.168.1.1).
- **Subnet Mask -** An address code that determines the size of the network. Normally 255.255.255.0 is used as the subnet mask.

Note:
If you change the IP address, you must use the new IP address to login the system.

- **Change the login account -** if you select the **YES** radio, you can modify your login user name and password.

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

4. Click the **Next** button. You will then see the page as shown in Figure 3-26. Please click the **Reboot/Finish** button to make your configuration take effect and finish the **Quick Setup**.

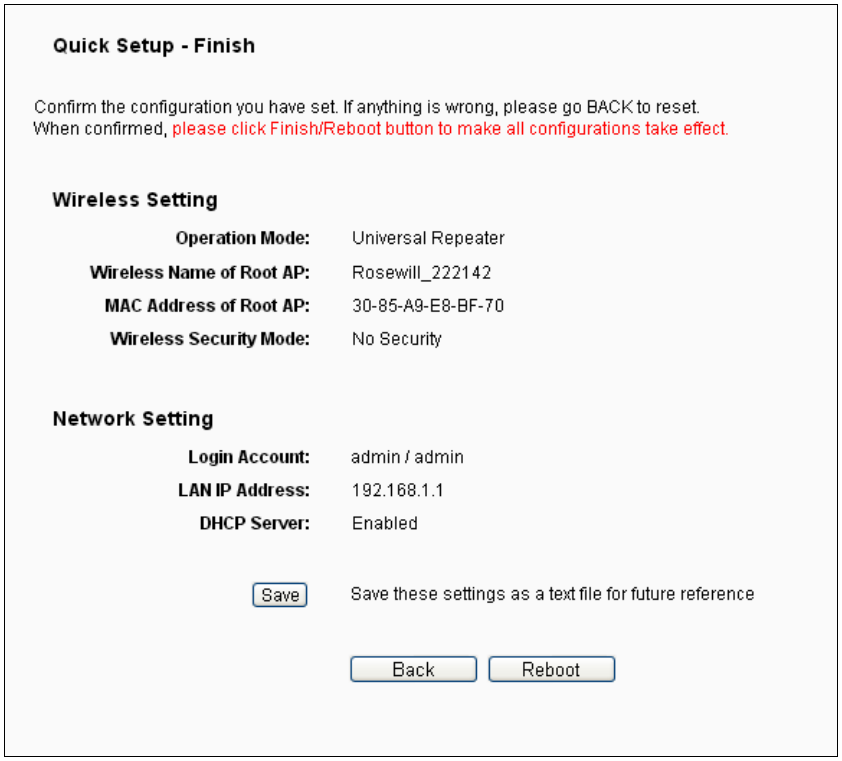


Figure 3-26 Quick Setup – Finish

Note:

You may click the **Save** button to save these settings as a text file for future reference.

3.2.5 Configuration for Bridge with AP Mode

When you choose **Bridge with AP** on **Operation Mode** page in Figure 3-6, the following steps:

1. Click **Next**, and then Wireless Bridge Setting page will appear as shown in Figure 3-27. On this page, please confirm all parameters, and then click **Next**.

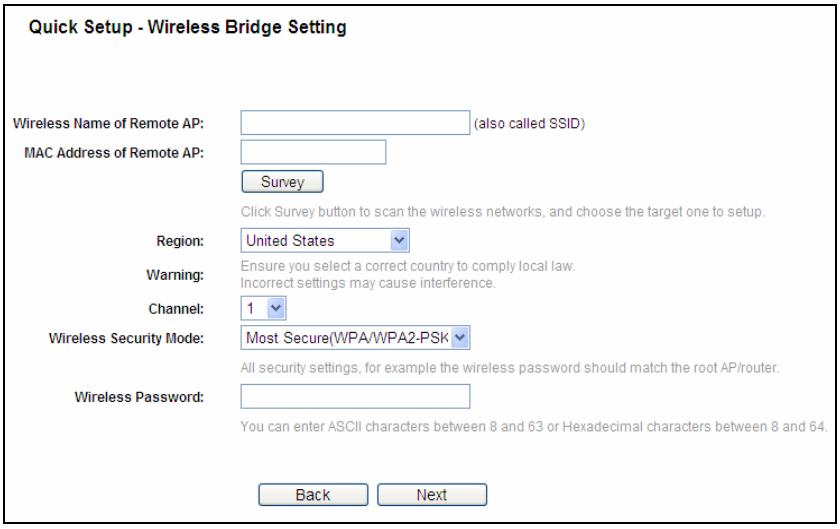


Figure 3-27 Quick Setup – Wireless Bridge Setting

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

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

Note Dialog

Note:

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

- **Channel -** This field determines which operating frequency will be used. The default channel is set to 6. It is not necessary to change the wireless channel unless you notice interference problems with another nearby access point.
- **Wireless Security Mode -** You can select one of the following security options:
  - **Most Secure (WPA/WPA2-PSK) -** Select WPA based on pre-shared passphrase.
  - **Secure (WEP)-** Select WEP based on none pre-shared passphrase.
  - **No Security -** The wireless security function is disabled. The wireless stations will be able to connect the Device without encryption.
- **Wireless Password -** Enter an 8 to 63 character alphanumeric pass-phrase. For good security it should be of enough length and should not be a commonly known phrase.

These settings are only for basic wireless parameters. For advanced settings, please refer to Section 4.7 Wireless.

Click **Survey** button on the Wireless Bridge Setting page as shown in Figure 3-27, and then AP List page will appear as shown in Figure 3-28. Find the SSID of the Access Point you want to access, and click **Connect** in the corresponding row. For example, the first item is selected. The target network's SSID will be automatically filled into the corresponding box which is shown as the Figure 3-29.

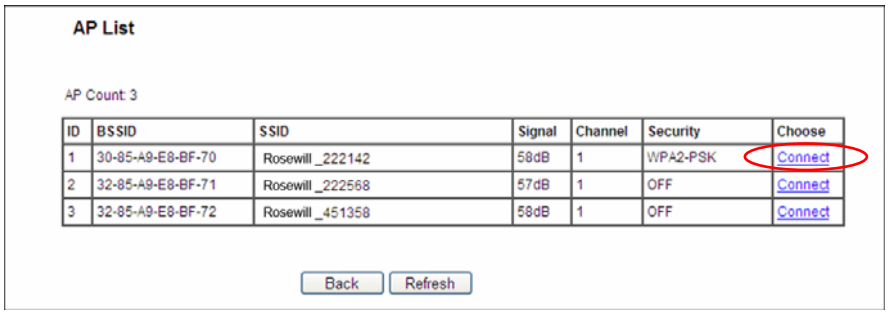


Figure 3-28 AP List

Figure 3-29 Wireless Bridge Setting

Note:

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

2. The Local Wireless AP Setting page will appear as shown in Figure 3-30. Please confirm Local Wireless AP Setting, and then click **Next**.

Figure 3-30 Local Wireless AP Setting

- **Local Wireless Name -** Enter a string of up to 32 characters. The same Name (SSID) must be assigned to all wireless devices in your network. The default SSID is set to be **Rosewill _xxxxxx**(xxxxxx indicates the last unique six characters of each Device's MAC address), which can ensure your wireless network security. But it is recommended strongly that you change your networks name (SSID) to a different value. This value is case-sensitive. For example, **MYSSID** is NOT the same as **MySsid**.

3. You will see the Network page as shown in Figure 3-31. Please configure the IP parameters of LAN on this page, and then click **Next**.

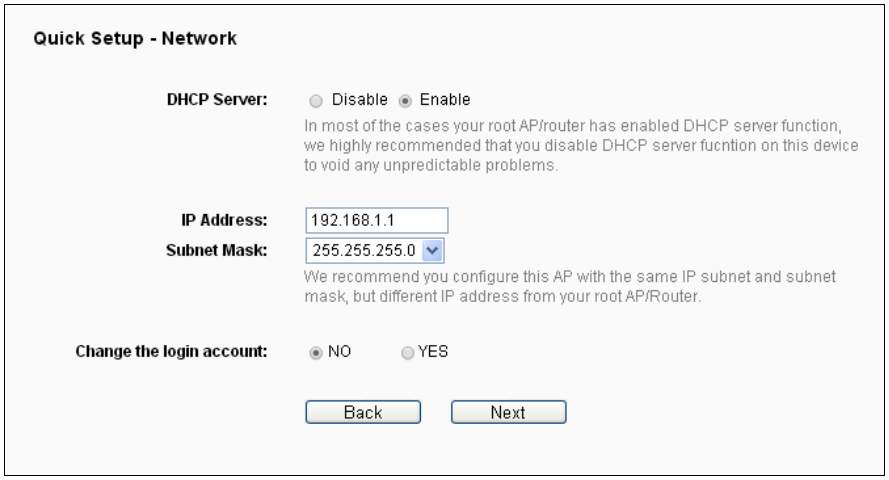


Figure 3-31 Quick Setup – Network

- **DHCP Server - Enable** or **Disable** the server. If you disable the Server, you must have another DHCP server within your network or else you must configure the IP address of the computer manually.
- **IP Address -** Enter the IP address of your system in dotted-decimal notation (factory default: 192.168.1.1).
- **Subnet Mask -** An address code that determines the size of the network. Normally 255.255.255.0 is used as the subnet mask.

Note:
If you change the IP address, you must use the new IP address to login the system.

- **Change the login account -** if you select the **YES** radio, you can modify your login user name and password.

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

4. Click the **Next** button. You will then see the page as shown in Figure 3-32. Please click the **Reboot/Finish** button to make your configuration take effect and finish the **Quick Setup**.

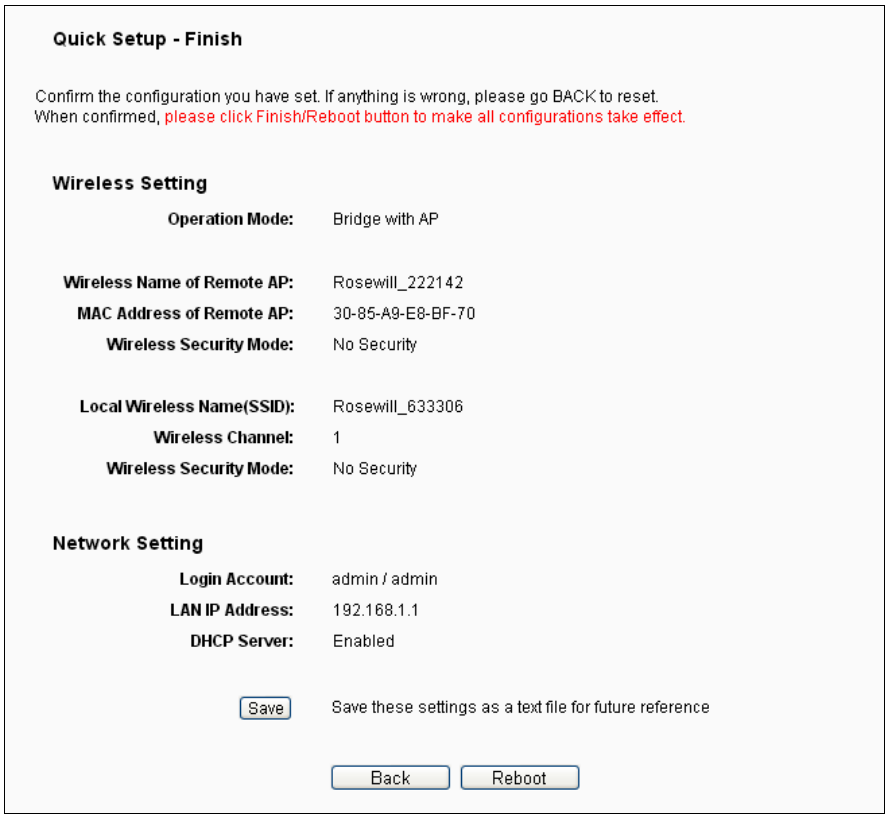


Figure 3-32 Quick Setup – Finish

Note:

You may click the **Save** button to save these settings as a text file for future reference.

3.2.6 Configuration for Client Mode

When you choose **Client** on **Operation Mode** page in Figure 3-6, the following steps:

1. Click **Next**, and then Wireless page will appear as shown in Figure 3-33. On this page, please confirm all parameters, and then click **Next**.

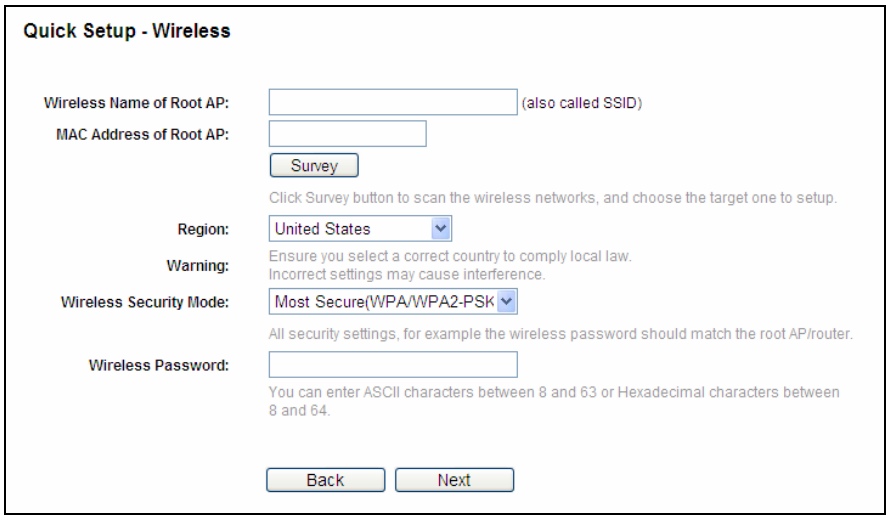


Figure 3-33 Wireless

- **Wireless Name of Root AP**（SSID）**-** The SSID of the AP your router is going to connect to as a client. You can also use the search function to select the SSID to join.
- **MAC Address of Root AP**（BSSID）**-** The BSSID of the AP your router is going to connect to as a client. You can also use the search function to select the BSSID to join.
- **Survey -** Click this button, you can survey the AP which runs in the current channel.
- **Region -** Select your region from the pull-down list. This field specifies the region where the wireless function of the router can be used. It may be illegal to use the wireless function of the router in a region other than one of those specified in this field. If your country or region is not listed, please contact your local government agency for assistance.

  When you select your local region from the pull-down list, 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.

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

Click **Survey** button on the Wireless page as shown in Figure 3-33, and then AP List page will appear as shown in Figure 3-34. Find the SSID of the Access Point you want to access, and click

Connect in the corresponding row. For example, the first item is selected. The target network's SSID will be automatically filled into the corresponding box which is shown as the Figure 3-35.

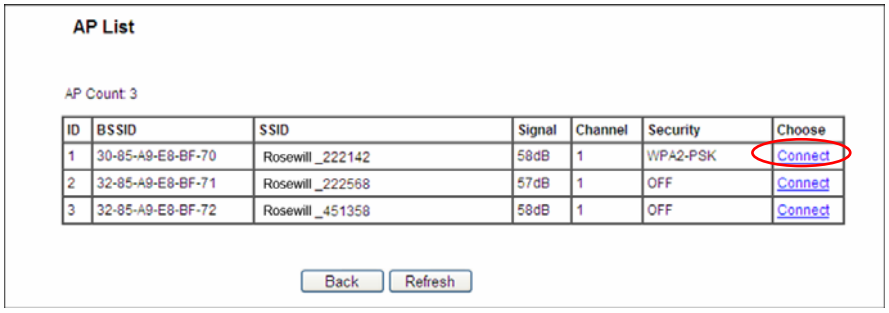


Figure 3-34 AP List

Figure 3-35 Quick Setup - Wireless

Note:

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

2. You will see the Network page as shown in Figure 3-36. Please configure the IP parameters of LAN on this page, and then click **Next**.

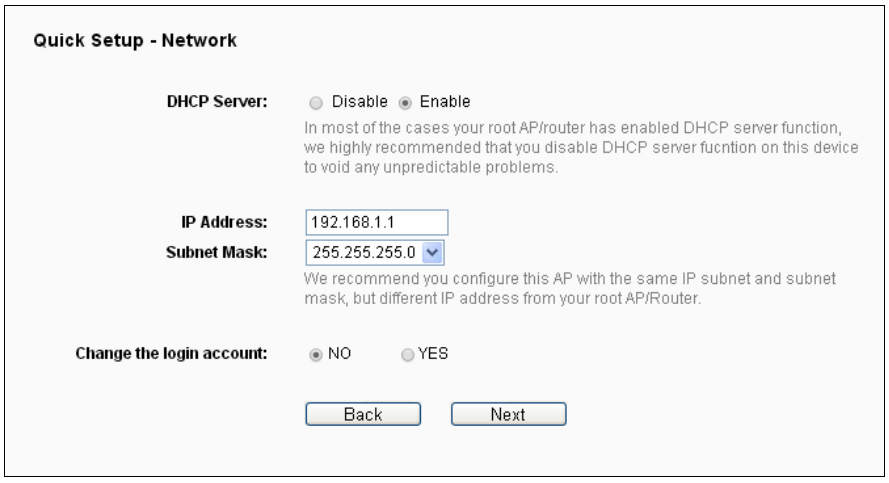


Figure 3-36 Quick Setup – Network

- **DHCP Server - Enable** or **Disable** the server. If you disable the Server, you must have another DHCP server within your network or else you must configure the IP address of the computer manually.
- **IP Address -** Enter the IP address of your system in dotted-decimal notation (factory default: 192.168.1.1).
- **Subnet Mask -** An address code that determines the size of the network. Normally 255.255.255.0 is used as the subnet mask.

Note:
If you change the IP address, you must use the new IP address to login the system.

- **Change the login account -** if you select the **YES** radio, you can modify your login user name and password.

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

5. Click the **Next** button. You will then see the page as shown in Figure 3-37. Please click the **Reboot/Finish** button to make your configuration take effect and finish the **Quick Setup**.

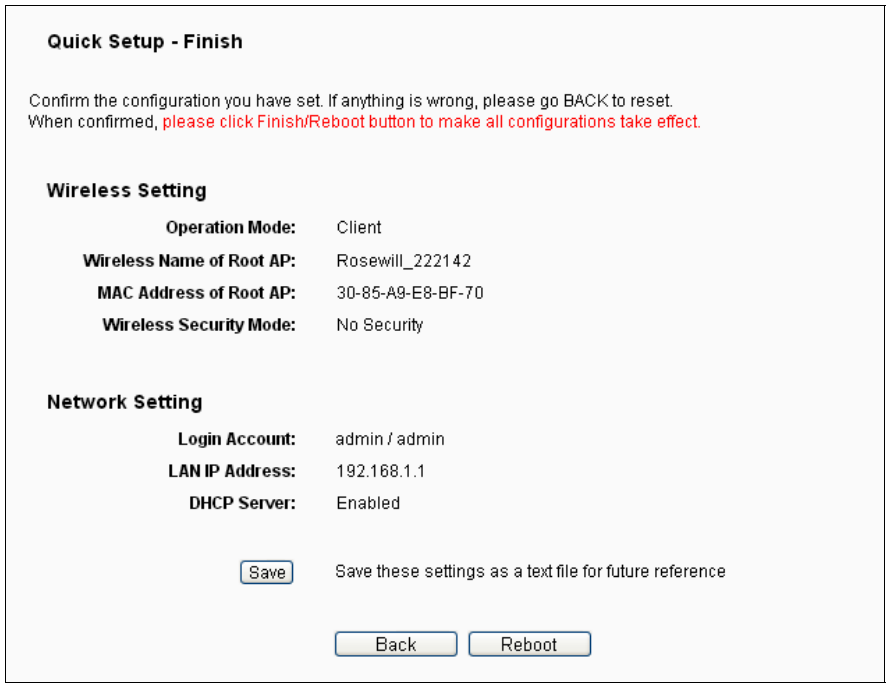


Figure 3-37 Quick Setup – Finish

Note:

You may click the Save button to save these settings as a text file for future reference.

Chapter 4. Configuring the router

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

4.1 Login

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

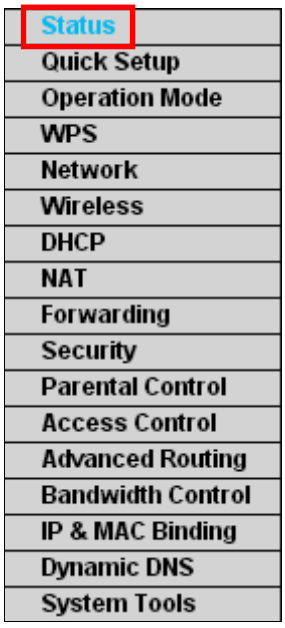


Figure 4-1 the main menu

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

4.2 Status

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

Figure 4-2 router Status

4.3 Quick Setup

Please refer to Section 3.2: "Quick Installation Guide".

4.4 Operation Mode

The router supports five operation mode types: **Client Router, Router, Multi-SSID, Repeater, Bridge with AP** and **Client**. Please select one your want. Click **Save** to save your choice, which is shown as Figure 4-3.

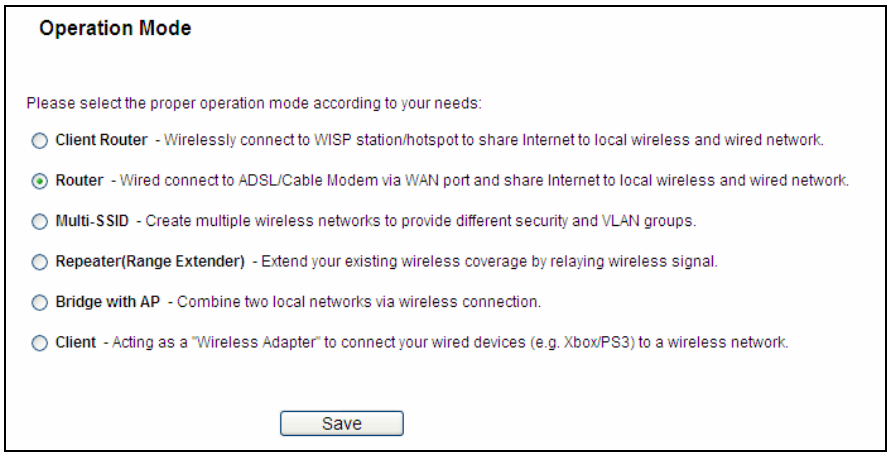


Figure 4-3 Operation Mode

- **Client Router -** In this mode, the device enables multi-users to share Internet from WISP. The LAN port devices share the same IP from WISP through Wireless port. While connecting to WISP, the Wireless port works as a WAN port at Client Router mode. The Ethernet port acts as a LAN port.
- **Router -** In this mode, the device enables multi-users to share Internet via ADSL/Cable Modem. The wireless port share the same IP to ISP through Ethernet WAN port. The Wireless port acts the same as a LAN port while at Router mode.
- **Multi-SSID -** In this mode, the device can create up to 4 wireless networks labeled with different SSIDs and assign each SSID with different security or VLAN, especially for the situation when the various access policies and functions are required.
- **Repeater -** In this mode, the AP will relays data to an associated root AP. AP function is enabled meanwhile. The wireless repeater relays signal between its stations and the root AP for greater wireless range.
- **Bridge with AP -** In this mode, the device bridge to another AP.
- **Client -** In this mode, the device will act as a wireless station to enable wired host(s) to access AP.

4.5 WPS

This section will guide you to add a new wireless device to an existing network quickly by **WPS (Wifi Protect Setup)** function.

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

Figure 4-4 WPS

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

b) To add a new device:

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

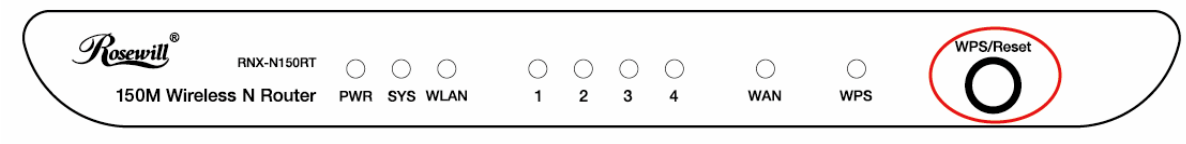
☞Note:

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

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 front panel of the router for one second.



You can also keep the default Status as **Enabled** and click the **Add Device** button in Figure 4-4, then Choose "**Press the button of the new device in two minutes**" and click **Connect**. (Shown in the following figure)

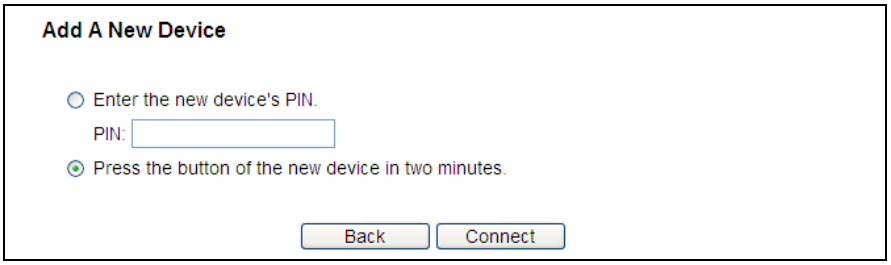


Figure 4-5 Add A New Device

Step 2: Press and hold the 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.

Step 5: Refer back to your client device or its documentation for further instructions.

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

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

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

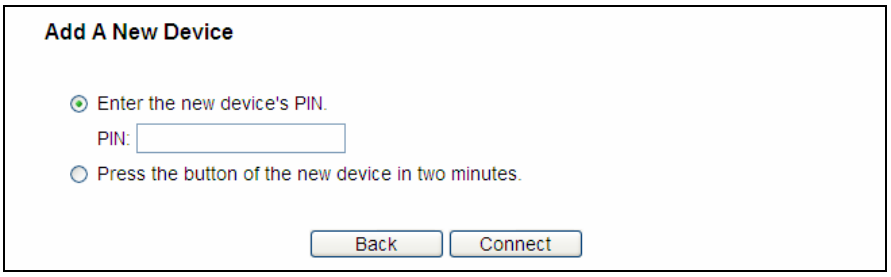


Figure 4-6 Add A New Device

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 4-6, 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. (It is also labeled on the bottom of the router.)

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

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

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

Note:

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

2) The 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 Network

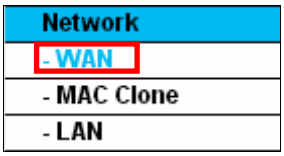


Figure 4-7 the Network menu

There are three submenus under the Network menu (shown in Figure 4-7): **LAN**, **WAN** and **MAC Clone.** Click any of them, and you will be able to configure the corresponding function.

4.6.1 LAN

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

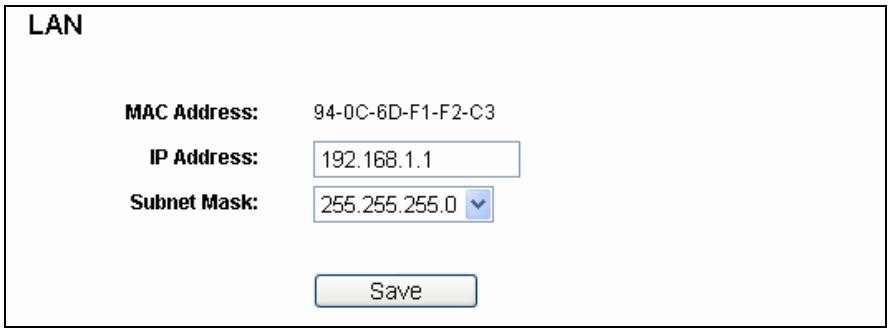


Figure 4-8 LAN

- **MAC Address-**The physical address of the router, as seen from the LAN. The value can't be changed.
- **IP Address -** Enter the IP address of your router or reset it in dotted-decimal notation (factory default: 192.168.1.1).
- **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 login the router.
2. If the new LAN IP Address you set is not in the same subnet, the IP Address pool of the DHCP server will change accordingly at the same time，while the Virtual Server and DMZ Host will not take effect until they are re-configured.

4.6.2 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 4-9):

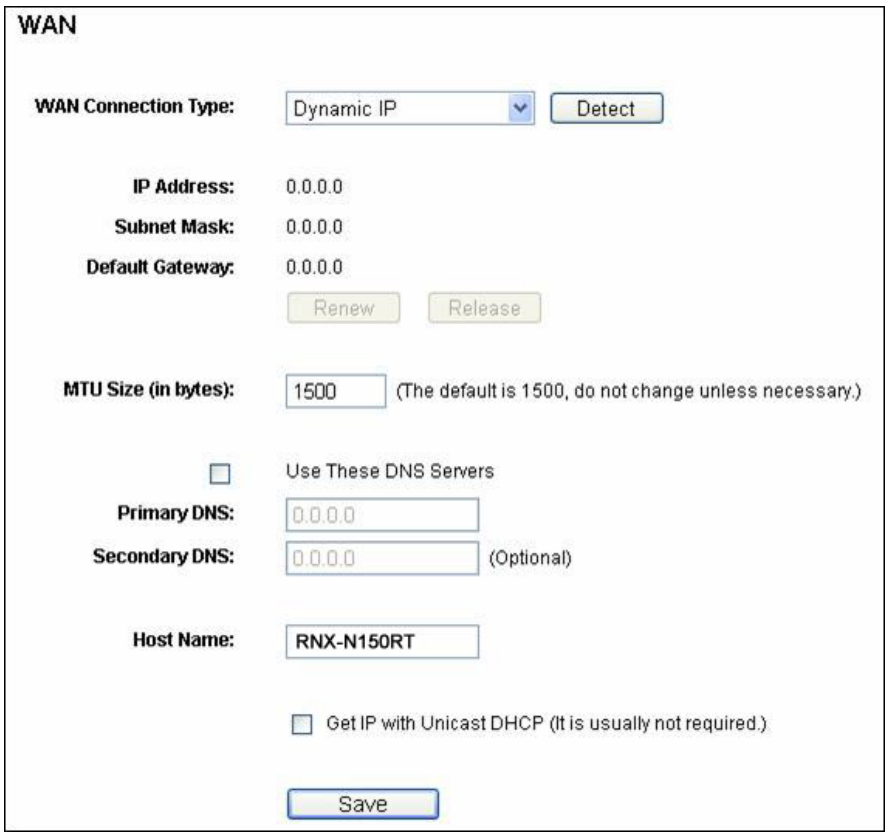


Figure 4-9 WAN – Dynamic IP

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

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

☞**Note:**

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

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

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

2. If your ISP provides a static or fixed IP Address, Subnet Mask, Gateway and DNS setting, select **Static IP**. The Static IP settings page will appear, shown in Figure 4-10.

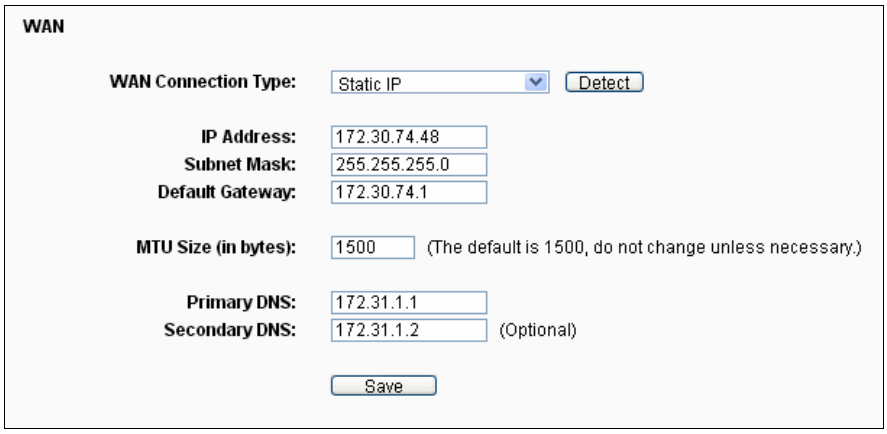


Figure 4-10 WAN - Static IP

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

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

3. If your ISP provides a PPPoE connection, select **PPPoE** option. And you should enter the following parameters (Figure 4-11):

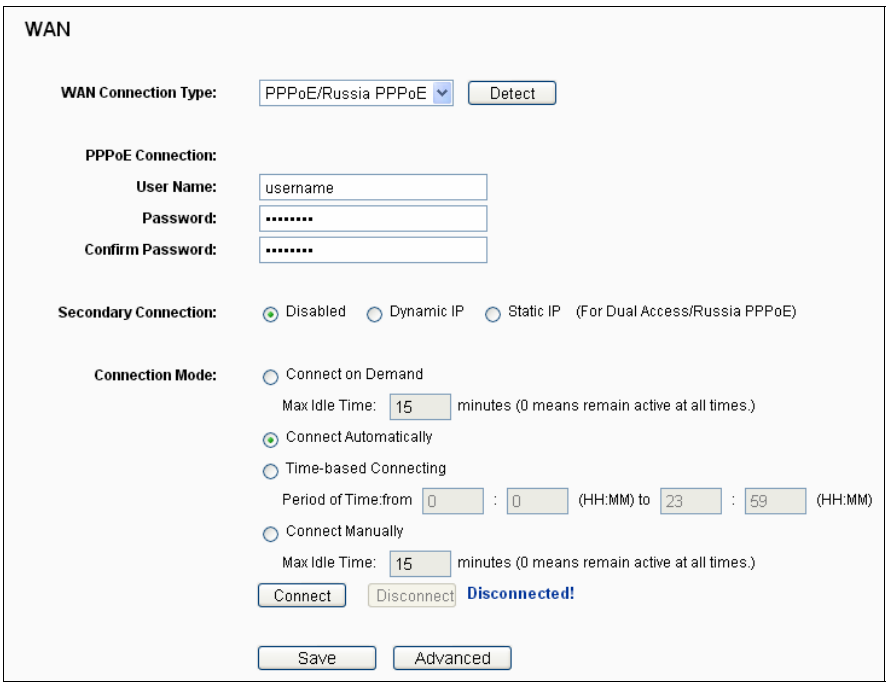


Figure 4-11 WAN - PPPoE

- **User Name/Password -** Enter the User Name and Password provided by your ISP. These fields are case-sensitive.
- **Secondary Connection -** It's available only for PPPoE Connection. If your ISP provides an extra Connection type such as Dynamic/Static IP to connect to a local area network, then you can check the radio button of Dynamic/Static IP to activate this secondary connection.
  - **Disabled -** The Secondary Connection is disabled by default, so there is PPPoE connection only. This is recommended.
  - **Dynamic IP -** You can check this radio button to use Dynamic IP as the secondary connection to connect to the local area network provided by ISP.
  - **Static IP -** You can check this radio button to use Static IP as the secondary connection to connect to the local area network provided by ISP.
- **Connect on Demand -**In this mode, the Internet connection can be terminated automatically after a specified inactivity period (**Max Idle Time**) and be re-established when you attempt to access the Internet again. If you want your Internet connection keeps active all the time, please enter "0" in the **Max Idle Time** field. Otherwise, enter the number of minutes you want to have elapsed before your Internet access disconnects.
- **Connect Automatically -**The connection can be re-established automatically when it was down.
- **Time-based Connecting -**The connection will only be established in the period from the start time to the end time(both are in HH:MM format).

Note:

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

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

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

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

If you want to do some advanced configurations, please click the **Advanced** button, and the page shown in Figure 4-12 will then appear:

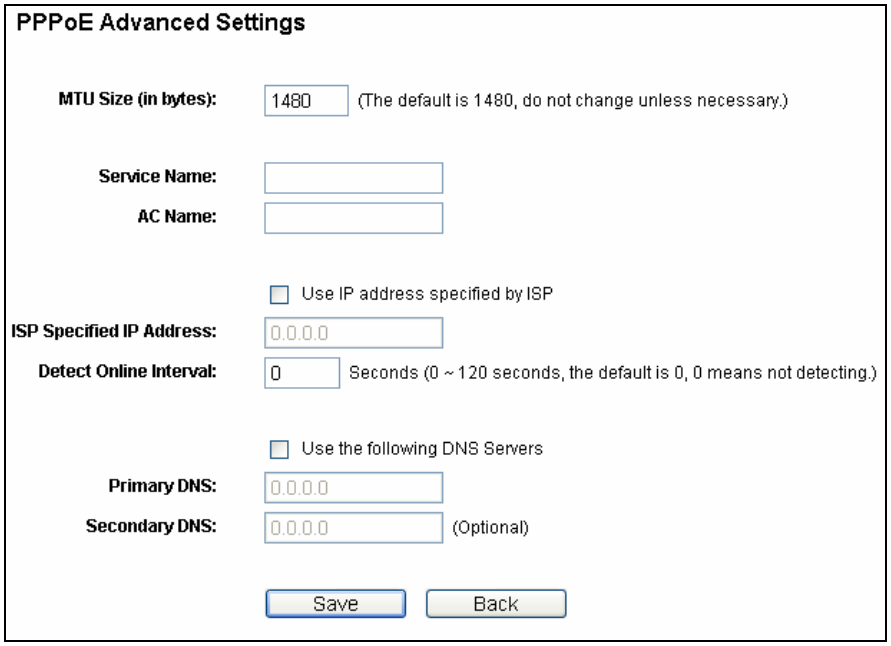


Figure 4-12 PPPoE Advanced Settings

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

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

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

4. If your ISP provides BigPond Cable (or Heart Beat Signal) connection, please select **BigPond Cable**. And you should enter the following parameters (Figure 4-13):

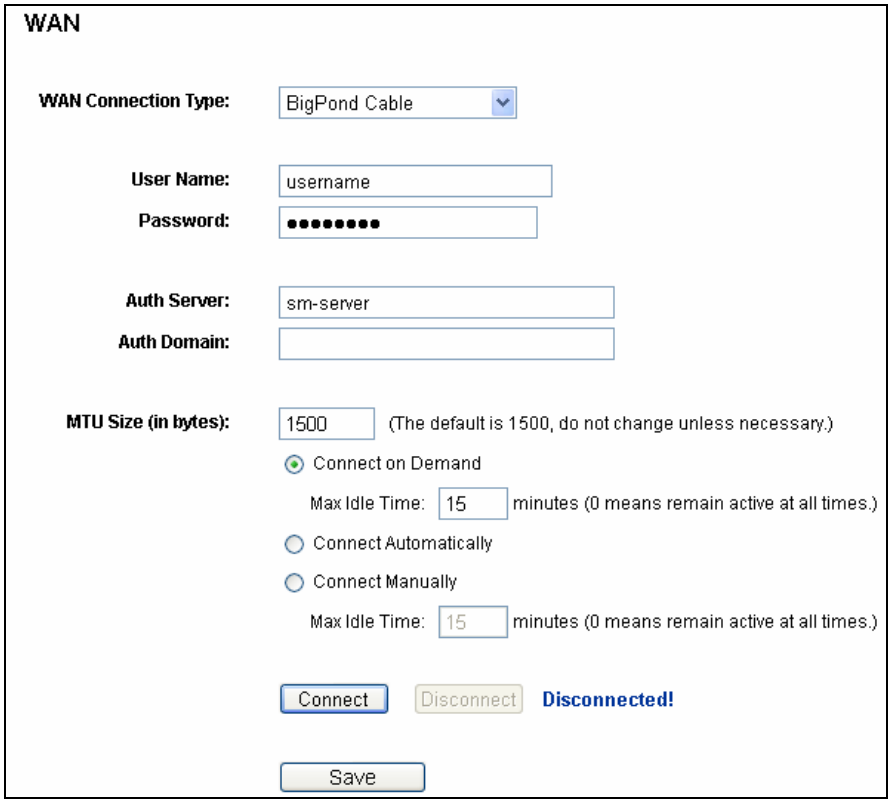


Figure 4-13

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

e.g.

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

- **MTU Size -** The normal **MTU** (Maximum Transmission Unit) value for most Ethernet networks is 1500 Bytes. It is not recommended that you change the default **MTU Size** unless required by your ISP.
- **Connect on Demand -** In this mode, the Internet connection can be terminated automatically after a specified inactivity period (**Max Idle Time**) and be re-established when you attempt to access the Internet again. If you want your Internet connection keeps active all the time, please enter "0" in the **Max Idle Time** field. Otherwise, enter the number of minutes you want to have elapsed before your Internet access disconnects.
- **Connect Automatically -** The connection can be re-established automatically when it was down.
- **Connect Manually -** You can click the **Connect**/**Disconnect** button to connect/disconnect immediately. This mode also supports the **Max Idle Time** function as **Connect on Demand** mode. The Internet connection can be disconnected automatically after a specified inactivity period and re-established when you attempt to access the Internet again.

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

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

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

5. If your ISP provides L2TP connection, please select **L2TP** option. And you should enter the following parameters (Figure 4-14):

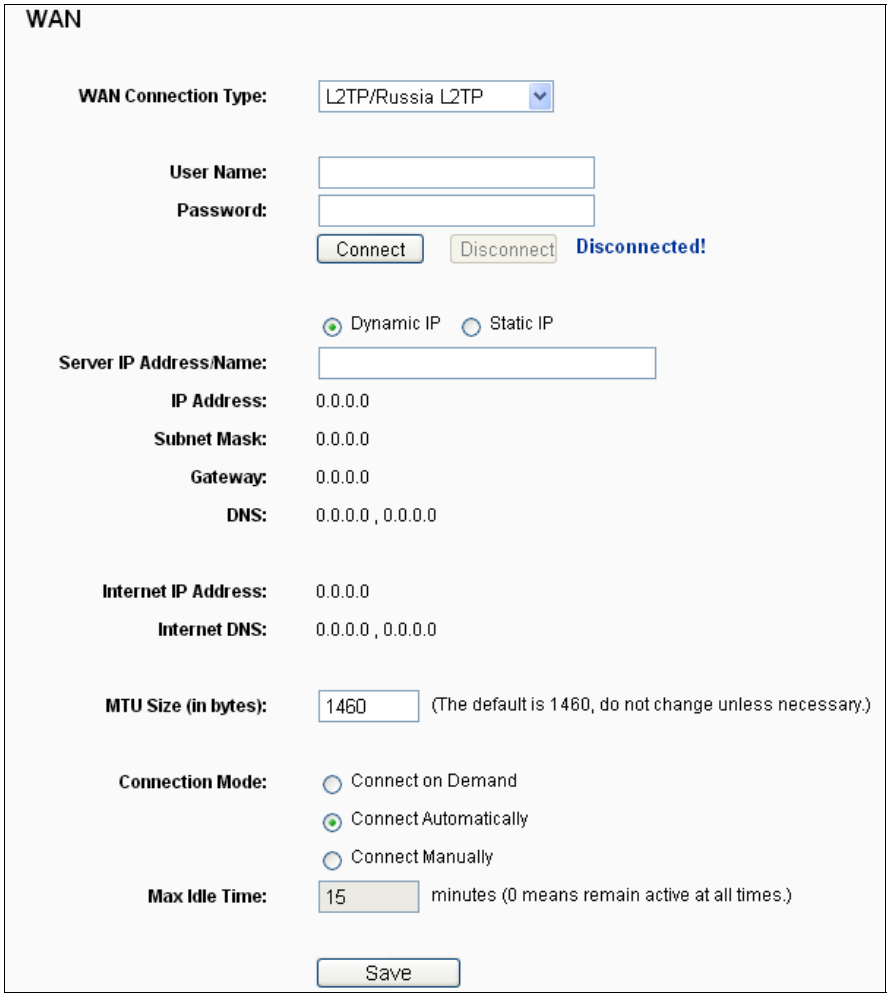


Figure 4-14 L2TP Settings

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

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

☞Note:

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

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

6. If your ISP provides PPTP connection, please select **PPTP** option. And you should enter the following parameters (Figure 4-15):

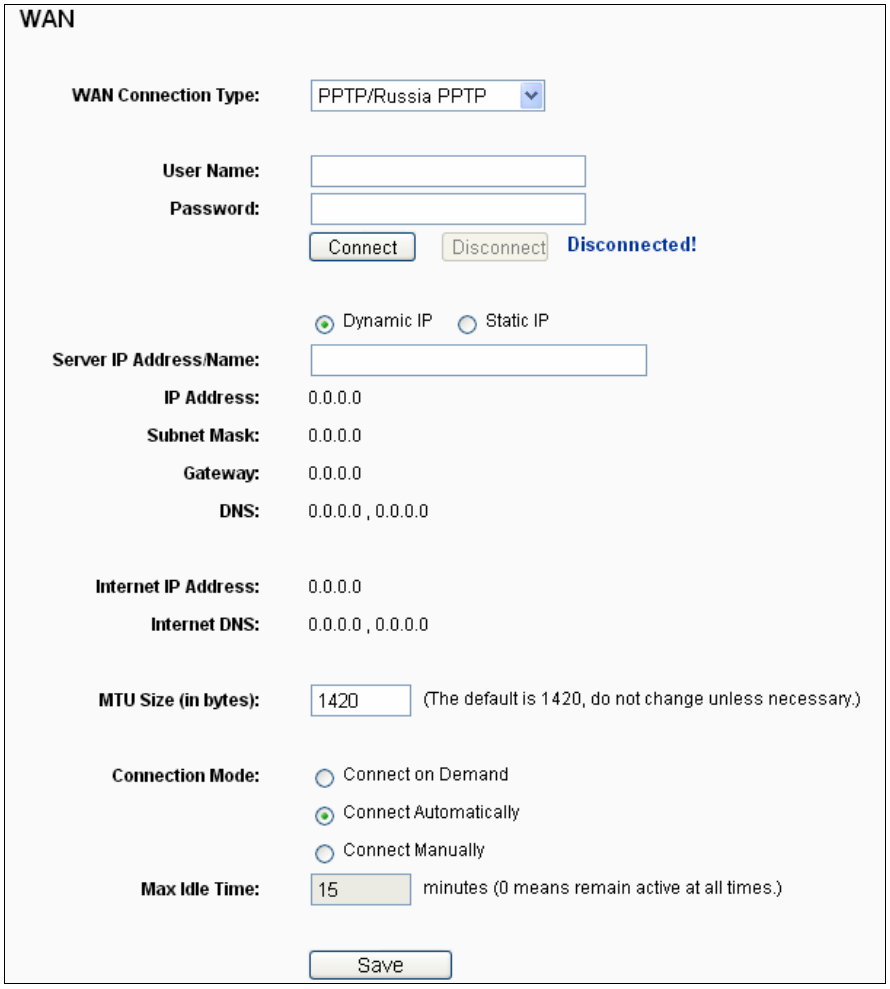


Figure 4-15 PPTP Settings

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

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

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

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

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

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

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

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

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

☞Note:

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

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

- **Static IP-** Connections which use static IP address assignment.

TheRoutercannotdetectPPTP/L2TP/BigPondconnectionswithyourISP.IfyourISPusesone of these protocols, then you must configure your connection manually.

4.6.3 MAC Clone

Choose menu "**Network→MAC Clone**", you can configure the MAC address of the WAN on the screen below, Figure 4-16:

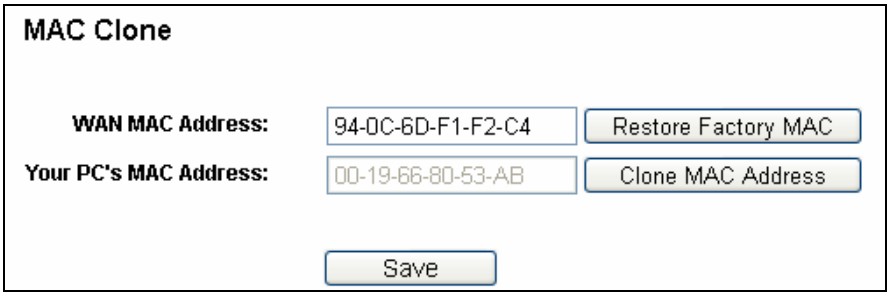


Figure 4-16 MAC Address Clone

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

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

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

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

☞**Note:**

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

4.7 Wireless

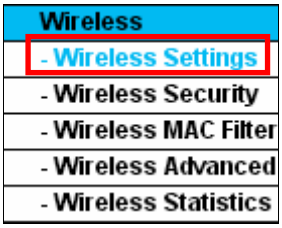


Figure 4-17 Wireless menu

There are five submenus under the Wireless menu (shown in Figure 4-17): **Wireless Settings**, **Wireless Security, Wireless MAC Filtering, Wireless Advanced** and **Wireless Statistics.** Click any of them, and you will be able to configure the corresponding function.

4.7.1 Wireless Settings

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

4.7.1.1. Wireless Settings in Client Router Mode

If you select **Client Router** mode in Figure 3-6 or **Client Router** mode in Figure 4-3, the Wireless Settings page will display as Figure 4-18.

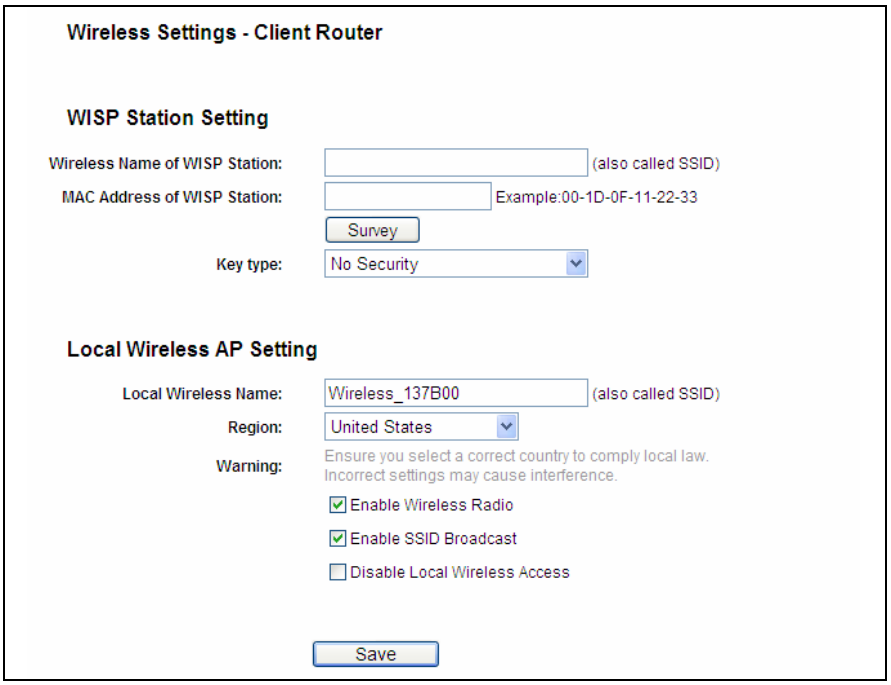


Figure 4-18 Wireless Settings

- **Wireless Name of WISP Station (SSID) -** The SSID of the AP your router is going to connect to as a client. You can also use the search function to select the SSID to join.
- **MAC Address of WISP Station (BSSID) -** The BSSID of the AP your router is going to connect to as a client. You can also use the search function to select the BSSID to join.
- **Survey -** Click this button, you can survey the AP which runs in the current channel.
- **Key type -** This option should be chosen according to the AP's security configuration. It is recommended that the security type is the same as your AP's security type.
- **Auth type -** This option should be chosen if the key type is WEP (ASCII) or WEP (HEX).It indicates the authorization type of the Root AP.

- **WEP Index -** This option should be chosen if the key type is WEP (ASCII) or WEP (HEX). It indicates the index of the WEP key.
- **Password -** If the AP your router is going to connect needs password, you need to fill the password in this blank.
- **Local Wireless Name -** Enter a value of up to 32 characters. The same Name (SSID) must be assigned to all wireless devices in your network.
- **Enable Wireless Router Radio -** The wireless radio of the router can be enabled or disabled to allow wireless stations access. If enabled, the wireless stations will be able to access the router. Otherwise, wireless stations will not be able to access the router.
- **Enable SSID Broadcast -** If you select the **Enable SSID Broadcast** checkbox, the wireless router will broadcast its name (SSID) on the air.
- **Disable Local Wireless Access -** If you select the **Disable Local Wireless Access** checkbox, the wireless router will disable local wireless access; other stations will not be able to access the router by wireless.

Click **Survey** button on the Wireless page shown as Figure 4-18, and then AP List page will appear, as shown in Figure 4-19. Find the SSID of the Access Point you want to access, and click **Connect** in the corresponding row. For example, the desired item is selected. The target network's SSID will be automatically filled into the corresponding box which is shown as the Figure 4-20.

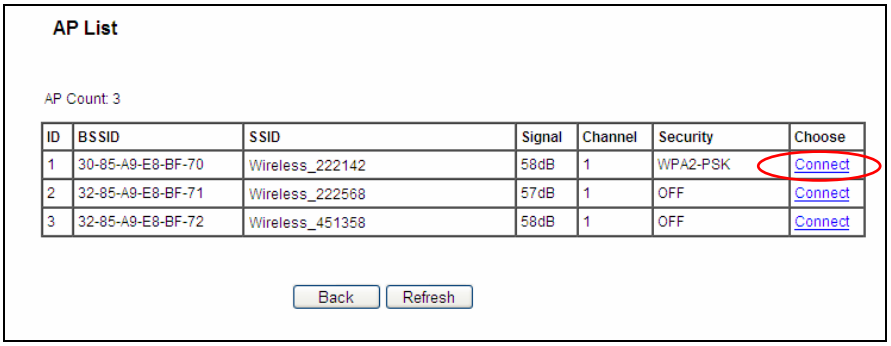


Figure 4-19 AP List

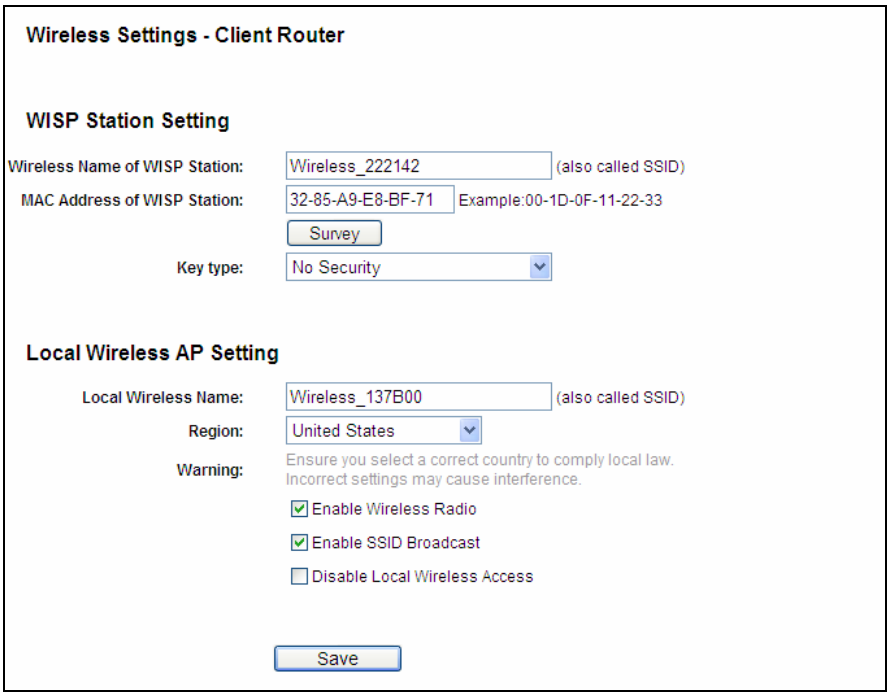


Figure 4-20 Wireless Settings – Client Router

Note:

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

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

Note:

1. The operating distance or range of your wireless connection varies significantly based on the physical placement of the router. For best results, place your router.
   - Near the center of the area in which your wireless stations will operate.
   - In an elevated location such as a high shelf.
   - Away from the potential sources of interference, such as PCs, microwaves, and cordless phones.
   - With the Antenna in the upright position.
   - Away from large metal surfaces.
2. Failure to follow these guidelines can result in significant performance degradation or inability to wirelessly connect to the router.

4.7.1.2. Wireless Settings in Router Mode

If you select **AP Router** mode in Figure 3-6 or **Wireless Router** mode in Figure 4-3, the Wireless Settings page will display as Figure 4-21.

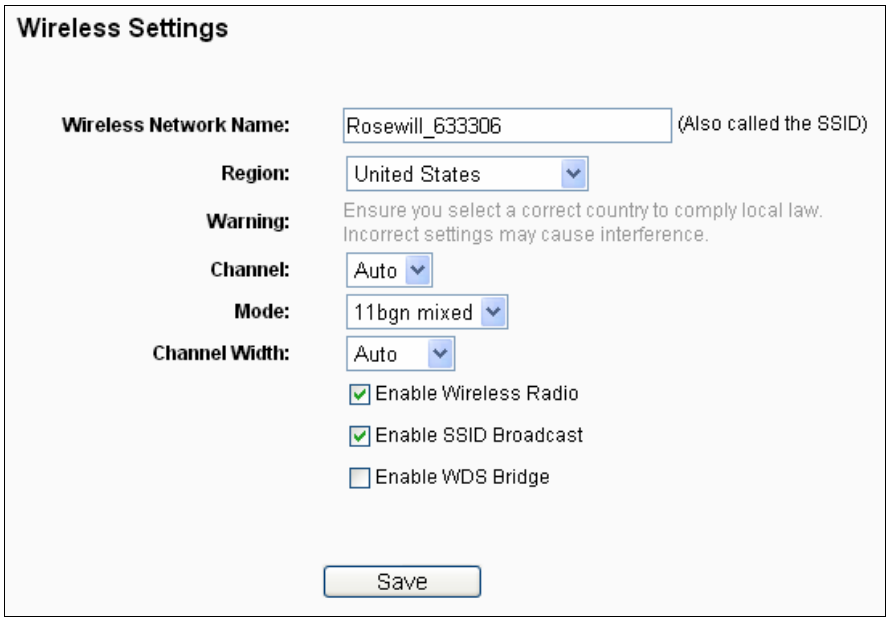


Figure 4-21 Wireless Settings

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

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

Note Dialog

☞Note:

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

- **Channel -** 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.

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

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

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

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

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

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

  Select the desired wireless mode. When802.11g mode is selected, only 802.11g wireless stations can connect to the router. When 802.11n mode is selected, only 802.11n wireless stations can connect to the AP. It is strongly recommended that you set the Mode to **802.11b&g&n**, and all of 802.11b, 802.11g, and 802.11n wireless stations can connect to the router.

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

  ☞Note:

  If **11b only**, **11g only**, or **11bg mixed** is selected in the **Mode** field, the **Channel Width** selecting field will turn grey and the value will become20M, which is unable to be changed.

- **Enable Wireless Router Radio -** The wireless radio of this router can be enabled or disabled to allow wireless stations access.

- **Enable SSID Broadcast -** When wireless clients survey the local area for wireless networks to associate with, they will detect the SSID broadcast by the router. If you select the **Enable SSID Broadcast** checkbox, the Wireless router will broadcast its name (SSID) on the air.

- **Enable WDS Bridge -**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 4-22. Make sure the following settings are correct.

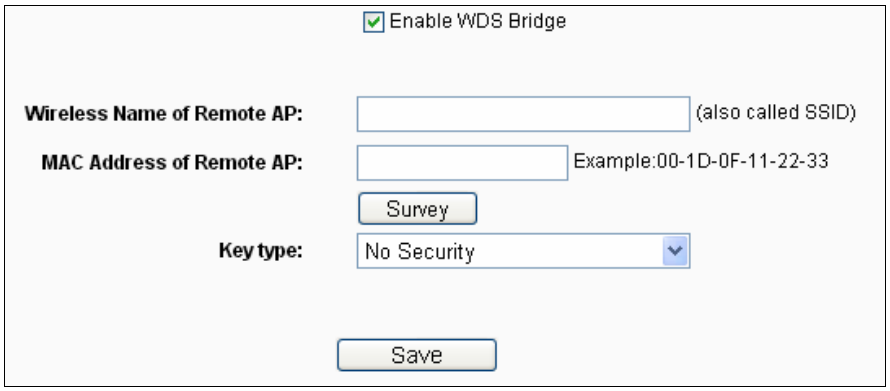


Figure 4-22

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

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

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

☞ **Note:**

1. The operating distance or range of your wireless connection varies significantly based on the physical placement of the router. For best results, place your router.
   - Near the center of the area in which your wireless stations will operate.
   - In an elevated location such as a high shelf.
   - Away from the potential sources of interference, such as PCs, microwaves, and cordless phones.
   - With the Antenna in the upright position.
   - Away from large metal surfaces.
2. Failure to follow these guidelines can result in significant performance degradation or inability to wirelessly connect to the router.

4.7.1.3. Wireless Settings in Multi-SSID

If you select **Multi-SSID** mode in Figure 3-6 or **Multi-SSID** mode in Figure 4-3, the Wireless Settings page will display as Figure 4-23.

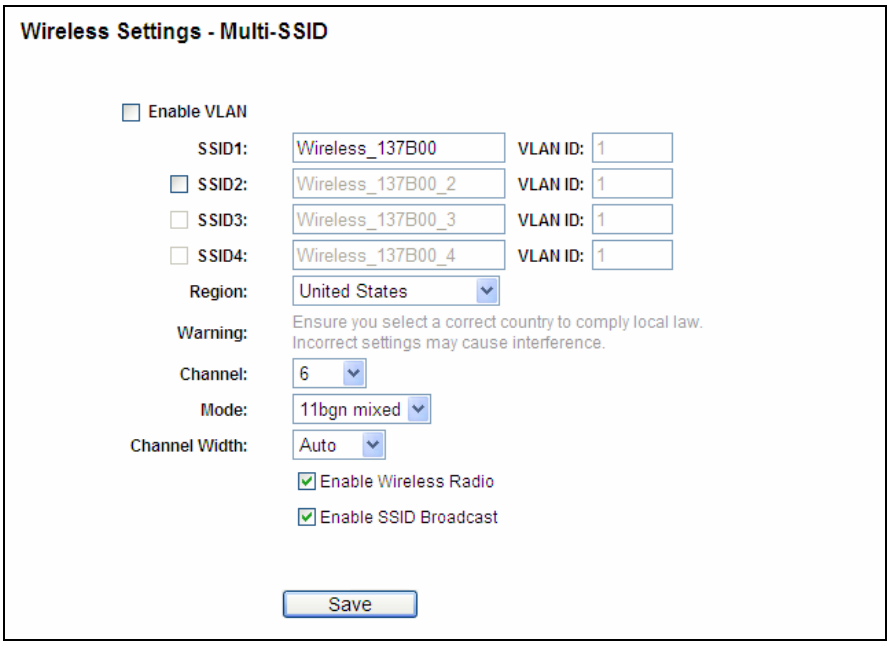


Figure 4-23 Wireless Settings – Multi-SSID

- **Enable VLAN -** Check this box and then you can change the **VLAN ID** of each SSID. If you want to configure the Guest and Internal networks on VLAN, the switch you are using must support VLAN. As a prerequisite step, configure a port on the switch for handling VLAN tagged packets as described in the IEEE802.1Q standard, and enable this field.

- **SSID (1-4) -** Up to four SSIDs for each BSS (Basic Service Set) can be entered in the filed SSID1 ~ SSID4. The name can be up to 32 characters. The same name (SSID) must be assigned to all wireless devices in your network. If **Enable VLAN** is checked, the wireless stations connecting to SSID of different VLANID can not communicate with each other.

- **VLANID (1-4) -** Provide a number between 1 and 4095 for VLAN. This will cause the device to send packets with VLAN tags. The switch connecting with the device must support VLAN IEEE802.1Q frames. The wireless stations connecting to the SSID of a specified VLAN ID can communicate with the PC connecting to the port with the same VLAN ID on the Switch.

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

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

Note Dialog

Note:

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

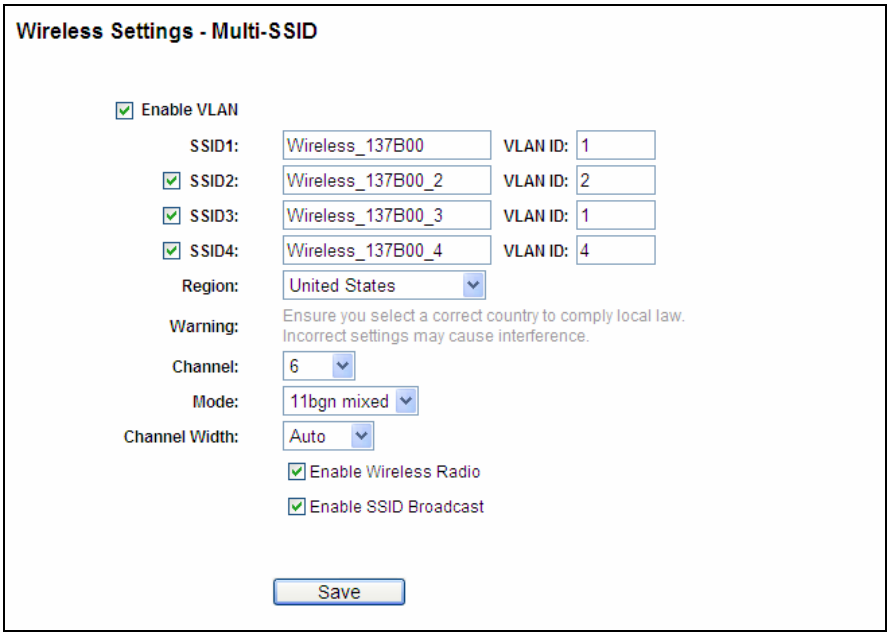
- **Channel -** Determines the operating frequency to be used. It is not necessary to change the wireless channel unless you notice interference problems with another nearby access point.
- **Mode -** This field determines the wireless mode which the device works on.
  - **11b only -** Only 802.11b wireless stations can connect to the device.
  - **11g only -** Only 802.11g wireless stations can connect to the device.
  - **11n only -** Only 802.11n wireless stations can connect to the device.
  - **11bg mixed -** Both 802.11b and 802.11g wireless stations can connect to the device.
  - **11bgn mixed -** All 802.11b, 802.11g and 802.11n wireless stations can connect to the device.
- **Channel Width -** Determines the channel width to be used. It is unnecessary to change the default value unless required.
- **Enable Wireless Radio -** Select or deselect this check box to allow or deny wireless stations to access the device.
- **Enable SSID Broadcast -** Select or deselect this check box to allow or deny the device to broadcast its name (SSID) on the air. If it's allowed, when wireless clients survey the local area for wireless networks to associate with, they will detect the SSID broadcast by the device.

Note:

To apply any settings you have altered on the page, please click the **Save** button, and then you will be reminded to reboot the device.

You are suggested to implement Multi-SSID function with a switch that supports Tag VLAN feature. Here is an example of how to configure Multi-SSID. Please take the following steps:

1. Configure the Access Point



Configure the Access Point

- Select Multi-SSID as the operation mode of RNX-N150RT.
- Select the checkbox before Enable VLAN to enable VLAN function for this access point.
- Configure the SSID and its corresponding VLAN ID. The detailed parameters are shown as the above figure.
- STA1, STA2, STA3 and STA4 join to the wireless network with SSID1, SSID2, SSID3 and SSID4 respectively.
- Click **Save** to apply the current security settings for the selected SSID.

Note:

1. The wireless STAs join to the network with different VLAN IDs cannot communicate with each other, for example, STA1 and STA2.
2. The wireless STAs join to the network with the same VLAN ID can communicate with each other, for example, STA1 and STA3.
3. All wireless STAs can log on to the Web management page of TL-WA701ND and manage the access point, for example, STA1, STA2, STA3 and STA4.
4. All the packets received in the wired network from the wireless STA will be added a corresponding VLAN Tag of the wireless STA, unless the VLAN ID of the wireless network is set to 1.

2. Configure the Switch

- Enable 802.1Q Tag VLAN function on the switch.
- Make sure the Untag frames are forwarded.

The following table shows the detailed configuration for the switch

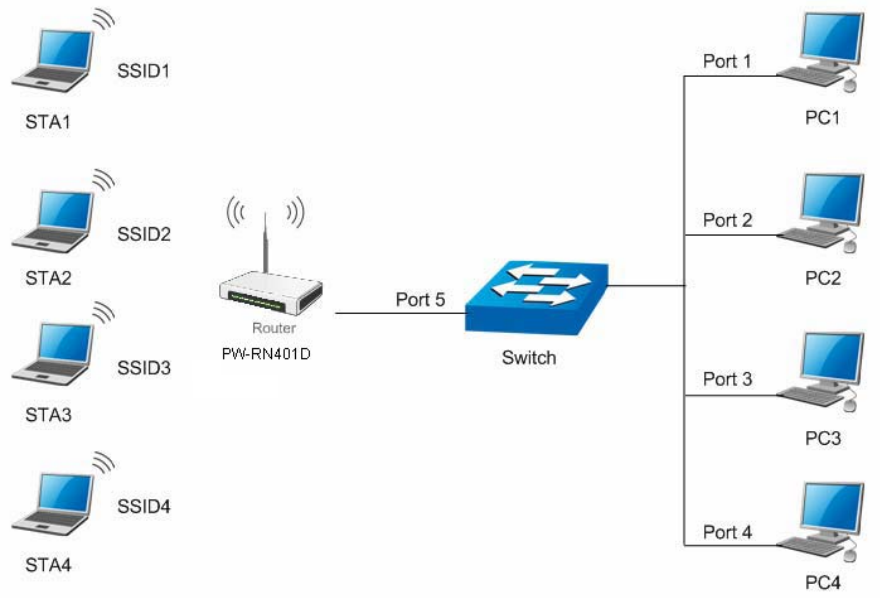
Port	VLAN ID	PVID	Egress Rule	Processing mode of Utag Frames
1	1	1	Untag	Forwarding
2	2	2	Untag	Forwarding
3	3	3	Untag	Forwarding
4	4	4	Untag	Forwarding
5	Port5 belongs to all VLANs	1	Tag	Forwarding

Table 4-1 Configure the Tag VLAN Switch

- Connect PC1, PC2, PC3 and PC4 to port1, port2, port3 and port4 of the switch respectively. The corresponding VLAN IDs of the four ports are 1, 2, 3 and 4.
- Configure port5 of the switch to be the member of VLAN1, VLAN2, VLAN3 and VLAN4 and connect it to the LAN port of TL-WA701ND.
- Configure the VLAN ID of the PC that can log on to the Web management page of RNX-N150RT via the LAN port equal to the PVID of port 5.

3. Verify the communication status after the above configuration is completed.

- If VLAN ID of the PC connected to the switch is different from the VLAN ID of the wireless STA, the two cannot communicate with each other, for example, PC1 and STA2.
- If the PC connected to the switch and the wireless STA have the same VLAN ID, the two can communicate with each other, for example PC2 and STA2.



Multi-SSID+VLAN

Note:

If the LAN port of RNX-N150RT is not connected to a switch but directly to a PC,

1. The PC can directly log on to the Web management page of RNX-N150RT and manage the access point.
2. Only the wireless STA with its VLAN ID set to 1 can communicate with the wired PC.

4.7.1.4. Wireless Settings in Repeater Mode

If you select **Repeater** mode in Figure 3-6 or **Repeater** mode in Figure 4-3, the Wireless Settings page will display as Figure 4-24.

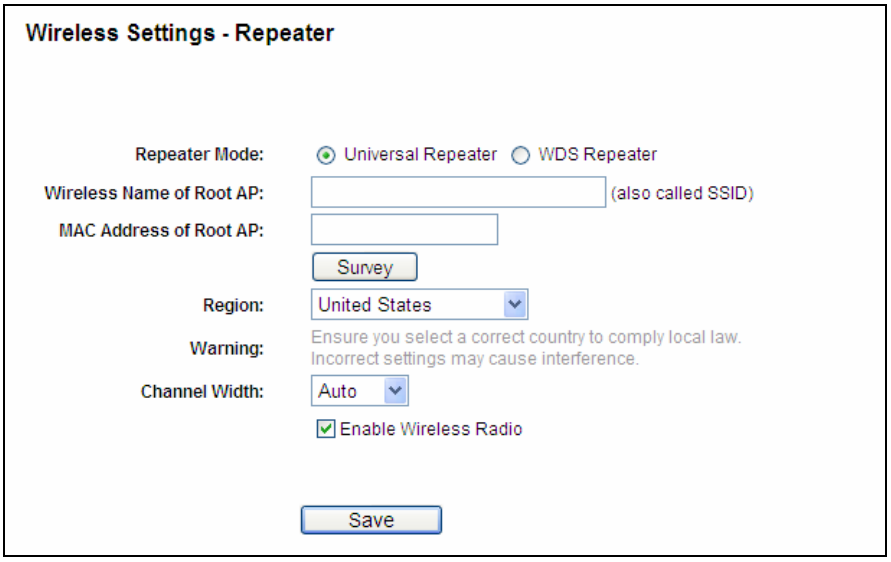


Figure 4-24 Wireless Settings

- **Repeater Mode -** Choosing WDS Repeater is to enable WDS, while choosing Universal Repeater is to disable WDS.
- **Wireless Name of Root AP -** The SSID of the AP your router is going to connect to as a client. You can also use the survey function to select the SSID to join.
- **MAC Address of Root AP -** The BSSID of the AP your router is going to connect to as a client. You can also use the survey function to select the BSSID to join.
- **Survey -** Click this button, you can search the AP which runs in the current channel.
- **Region -** Select your region from the pull-down list. This field specifies the region where the wireless function of the 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.
- **Channel Width -** The bandwidth of the wireless channel.

- **Enable Wireless Radio -** The wireless radio of the router can be enabled or disabled to allow wireless stations access. If enabled, the wireless stations will be able to access the router; otherwise, wireless stations will not be able to access the router.

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

☞ **Note:**

1. The operating distance or range of your wireless connection varies significantly based on the physical placement of the router. For best results, place your router.
   - Near the center of the area in which your wireless stations will operate.
   - In an elevated location such as a high shelf.
   - Away from the potential sources of interference, such as PCs, microwaves, and cordless phones.
   - With the Antenna in the upright position.
   - Away from large metal surfaces.
2. Failure to follow these guidelines can result in significant performance degradation or inability to wirelessly connect to the router.

4.7.1.5. Wireless Settings in Bridge with AP Mode

If you select **Bridge with AP** mode in Figure 3-6 or **Bridge with AP** mode in Figure 4-3, the Wireless Settings page will display as Figure 4-25.

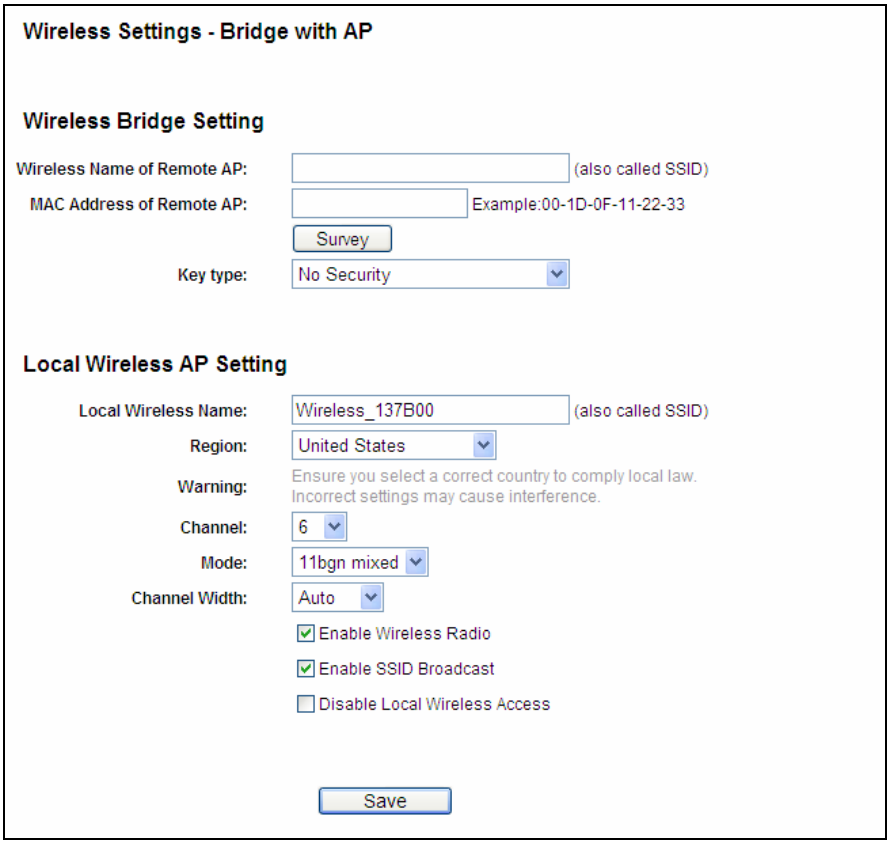


Figure 4-25 Wireless Settings

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

- **Local Wireless Name (SSID) -** Enter a value of up to 32 characters. The same Name (SSID) must be assigned to all wireless devices in your network.
- **Region -** Select your region from the pull-down list. This field specifies the region where the wireless function of the router can be used. It may be illegal to use the wireless function of the router in a region other than one of those specified in this filed. If your country or region is not listed, please contact your local government agency for assistance.
- **Channel -** This field determines which operating frequency will be used. It is not necessary to change the wireless channel unless you notice interference problems with another nearby access point. If you select **Auto**, then the AP will choose the best channel automatically.
- **Mode -** If all of the wireless devices connected with this wireless router can connect in the same transmission mode (e.g. 802.11b), you can choose "Only" mode (e.g. 11b only). If you have some devices that use a different transmission mode, choose the appropriate "Mixed" mode.
- **Channel Width -** The bandwidth of the wireless channel.
- **Enable Wireless Radio -** The wireless radio of the router can be enabled or disabled to allow wireless stations access. If enabled, the wireless stations will be able to access the router; otherwise, wireless stations will not be able to access the router.
- **Enable SSID Broadcast -** If you select the Enable SSID Broadcast checkbox, the wireless router will broadcast its name (SSID) on the air.
- **Disable Local Wireless Access -** If you select the **Disable Local Wireless Access** checkbox, the wireless router will disable local wireless access; other stations will not be able to access the router by wireless.

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

☞ **Note:**

1. The operating distance or range of your wireless connection varies significantly based on the physical placement of the router. For best results, place your router.
   - Near the center of the area in which your wireless stations will operate.
   - In an elevated location such as a high shelf.
   - Away from the potential sources of interference, such as PCs, microwaves, and cordless phones.
   - With the Antenna in the upright position.
   - Away from large metal surfaces.
2. Failure to follow these guidelines can result in significant performance degradation or inability to wirelessly connect to the router.

4.7.1.6. Wireless Settings in Client Mode

If you select **Client** mode in Figure 3-6 or **Client** mode in Figure 4-3, the Wireless Settings page will display as Figure 4-26.

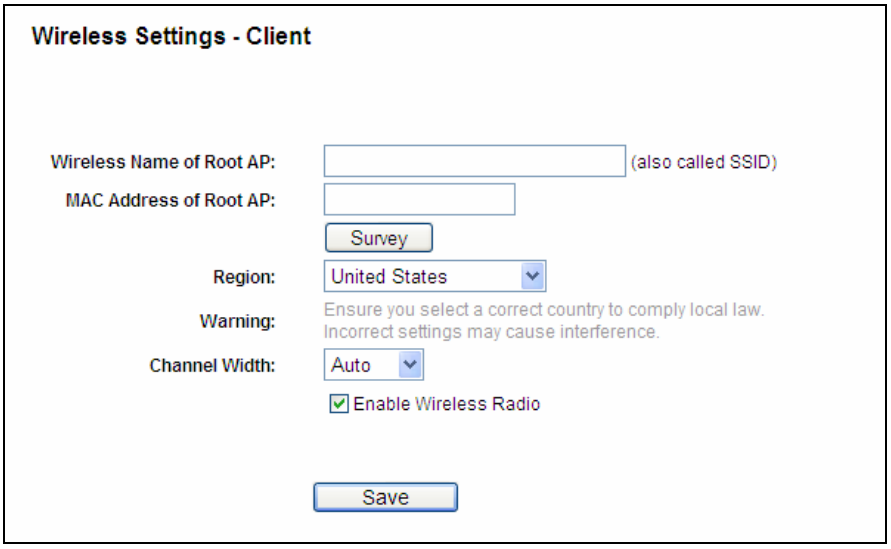


Figure 4-26 Wireless Settings

- **Wireless Name of Root AP** (SSID) **-** The Wireless Name of the AP your router is going to connect to as a client. You can also use the survey function to select the SSID to join.
- **MAC Address of Root AP** (BSSID) **-** The MAC Address of the AP your router is going to connect to as a client. You can also use the survey function to select the BSSID to join.
- **Region -** Select your region from the pull-down list. This field specifies the region where the wireless function of the router can be used. It may be illegal to use the wireless function of the router in a region other than one of those specified in this filed. If your country or region is not listed, please contact your local government agency for assistance.
- **Channel Width -** The bandwidth of the wireless channel.
- **Enable Wireless Radio -** The wireless radio of the router can be enabled or disabled to allow wireless stations access. If enabled, the wireless stations will be able to access the router; otherwise, wireless stations will not be able to access the router.

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

☞ **Note:**

1. The operating distance or range of your wireless connection varies significantly based on the physical placement of the router. For best results, place your router.
   - Near the center of the area in which your wireless stations will operate.
   - In an elevated location such as a high shelf.

- Away from the potential sources of interference, such as PCs, microwaves, and cordless phones.
- With the Antenna in the upright position.
- Away from large metal surfaces.

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

4.7.2 Wireless Security

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

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

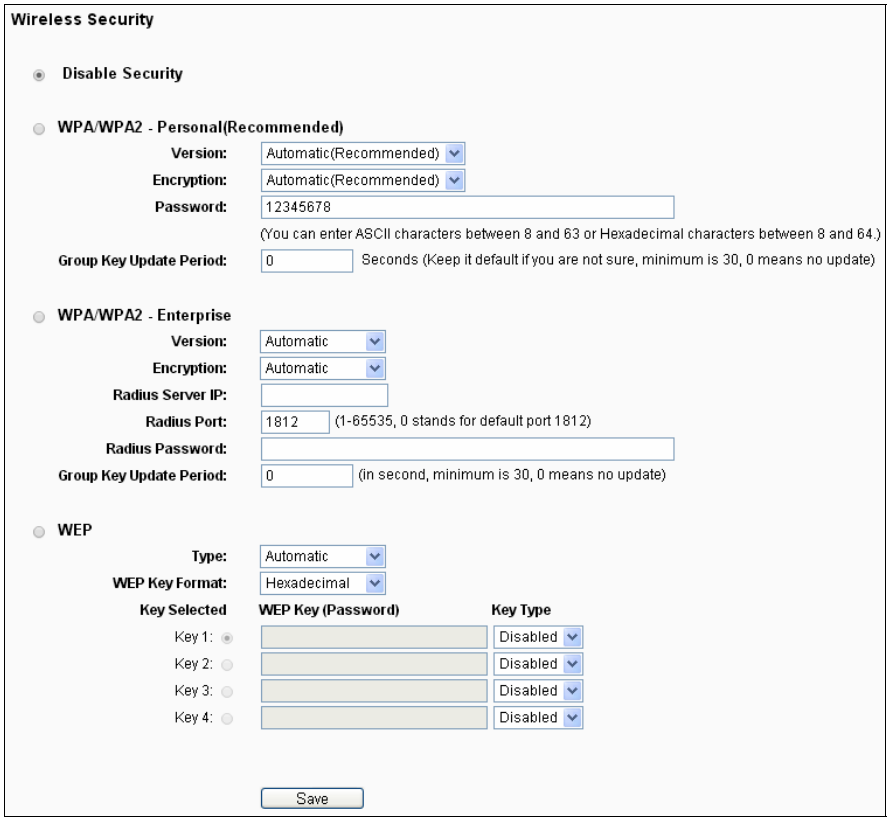


Figure 4-27Wireless Security

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

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

Note:

If you check the **WPA /WPA2 - Personal (Recommended)** radio button and choose **TKIP** encryption then click **save**, and you will find a notice in red as shown in Figure 4-28.

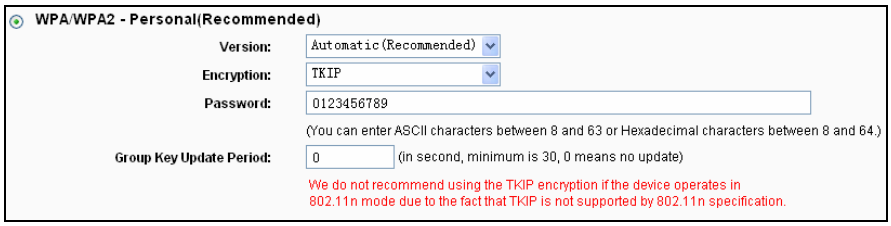


Figure 4-28

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

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 4-29.

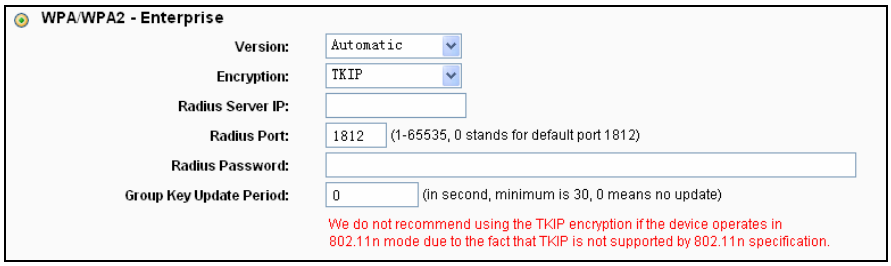


Figure 4-29

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

- **Group Key Update Period -** Specify the group key update interval in seconds. The value should be 30 or above. Enter 0 to disable the update.

➢ **WEP -** It is based on the IEEE 802.11 standard. If you check this radio button, you will find a notice in red as shown in Figure 4-30.

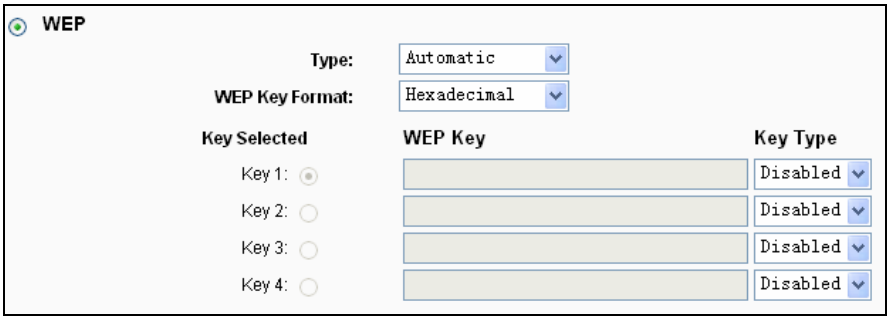


Figure 4-30

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

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

  ☞ **Note:**

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

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

4.7.3 Wireless MAC Filtering

Choose menu "**Wireless → MAC Filtering**", and then you can control the wireless access by configuring the **Wireless MAC Filtering** function, as shown in Figure 4-31.

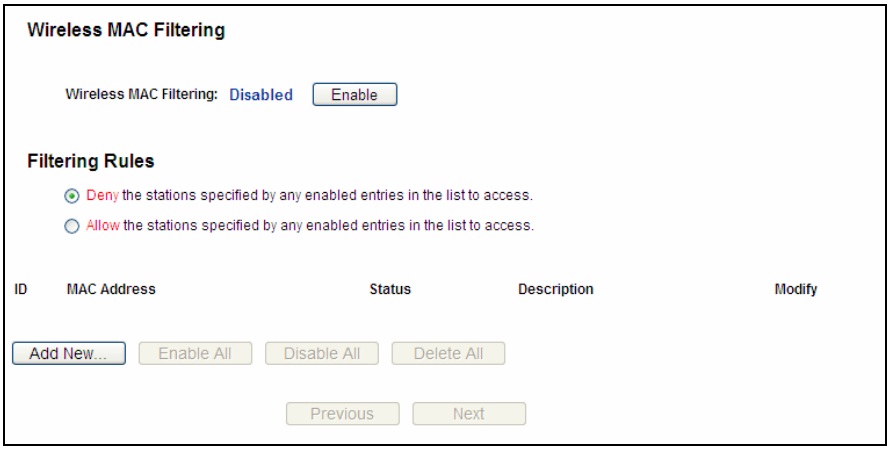


Figure 4-31 Wireless MAC Filtering

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

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

To Add a Wireless MAC Address filtering entry, click the **Add New…** button. The "**Add or Modify Wireless MAC Address Filtering entry**" page will appear, shown in Figure 4-32:

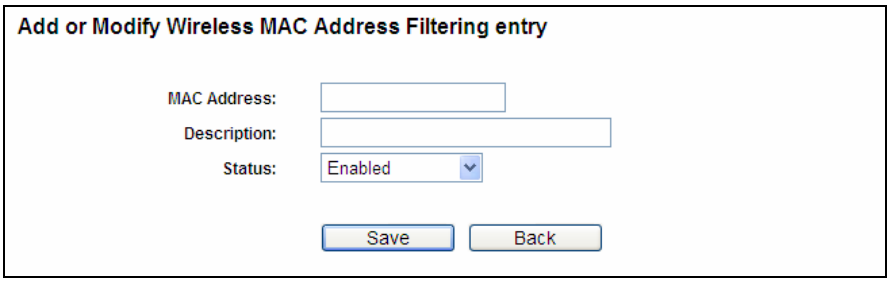


Figure 4-32 Add or Modify Wireless MAC Address Filtering entry

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** pull-down list.
4. Click the **Save** button to save this entry.

To modify or delete an existing entry:

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

2. Modify the information.
3. Click the **Save** button.

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

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

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

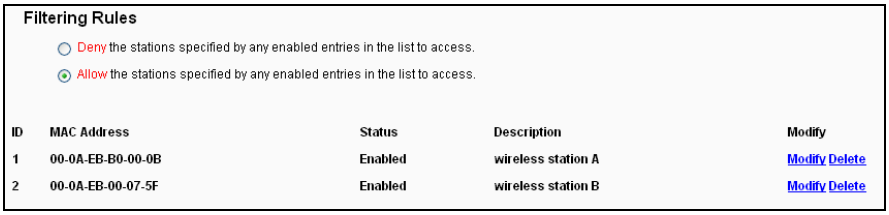
Click the **Next** button to go to the next page.

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

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

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

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



4.7.4 Wireless Advanced

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

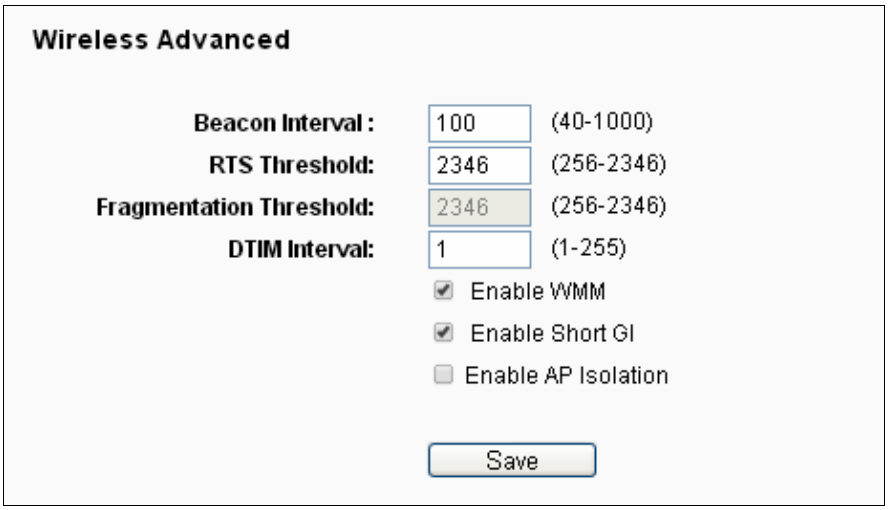


Figure 4-33 Wireless Advanced

- **Beacon Interval -** Enter a value between 20-1000 milliseconds for Beacon Interval here.The beacons are the packets sent by the router to synchronize a wireless network. Beacon Interval value determines the time interval of the beacons. The default value is 100.
- **RTS Threshold -** Here you can specify the RTS (Request to Send) Threshold. If the packet is larger than the specified RTS Threshold size, the router will send RTS frames to a particular receiving station and negotiate the sending of a data frame. The default value is 2346.
- **Fragmentation Threshold -** This value is the maximum size determining whether packets will be fragmented. Setting the Fragmentation Threshold too low may result in poor network performance because of excessive packets. 2346 is the default setting and is recommended.
- **DTIM Interval -** This value determines the interval of the Delivery Traffic Indication Message (DTIM).A DTIM field is a countdown field informing clients of the next window for listening to broadcast and multicast messages. When the router has buffered broadcast or multicast messages for associated clients, it sends the next DTIM with a DTIM Interval value. You can specify the value between 1-255 Beacon Intervals. The default value is 1, which indicates the DTIM Interval is the same as Beacon Interval.
- **Enable WMM - WMM** function can guarantee the packets with high-priority messages being transmitted preferentially. It is strongly recommended.
- **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.

4.7.5 Wireless Statistics

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

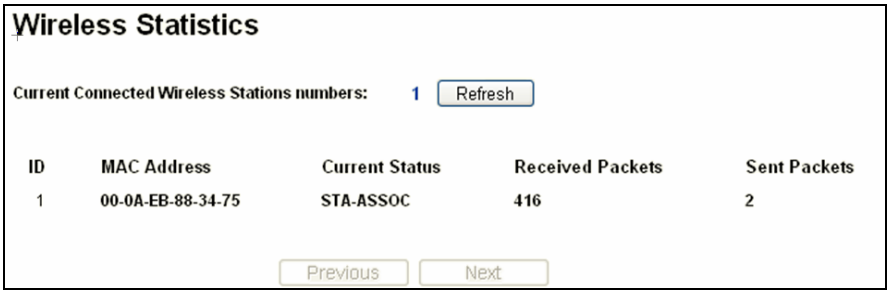


Figure 4-34 Wireless Statistics

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

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

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

Note:

This page will be refreshed automatically every 5 seconds.

4.8 DHCP

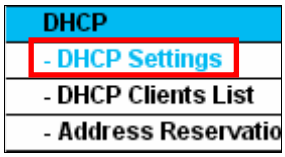


Figure 4-35 The DHCP menu

There are three submenus under the DHCP menu (shown in Figure 4-35), **DHCP Settings**, **DHCP Clients List** and **Address Reservation.** Click any of them, and you will be able to configure the corresponding function.

4.8.1 DHCP Settings

Choose menu "**DHCP→DHCP Settings**", you can configure the DHCP Server on the page as shown in Figure 4-36.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.

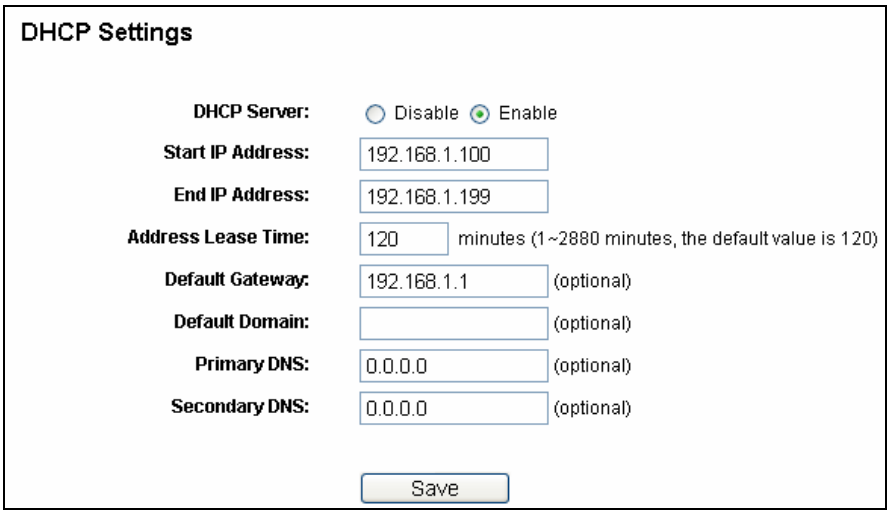


Figure 4-36 DHCP Settings

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

4.8.2 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 4-37.

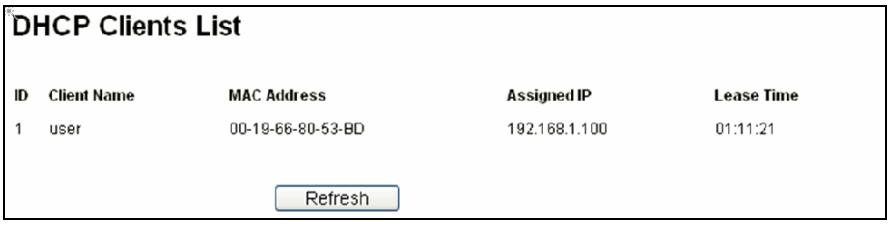


Figure 4-37 DHCP Clients List

- **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.

4.8.3 Address Reservation

Choose menu "**DHCP→Address Reservation**", you can view and add a reserved address for clients via the next screen (shown in Figure 4-38).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 4-38 Address Reservation

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

To Reserve an IP address:

1. Click the **Add New…**button. Then Figure 4-39 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.

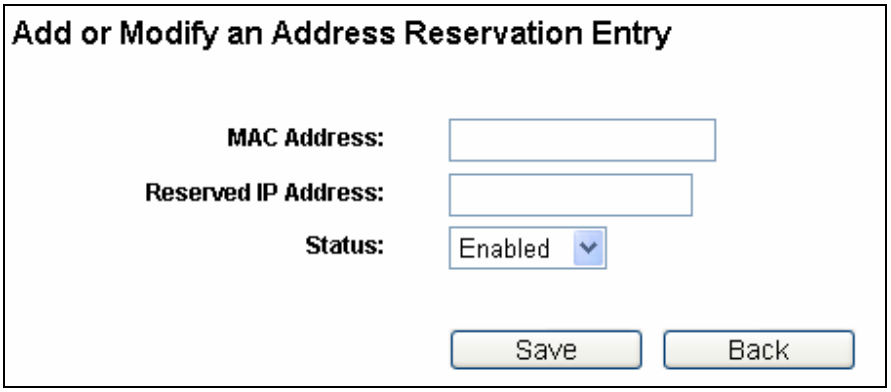


Figure 4-39 Add or Modify an Address Reservation Entry

To modify or delete an existing entry:

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

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

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

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

4.9 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.

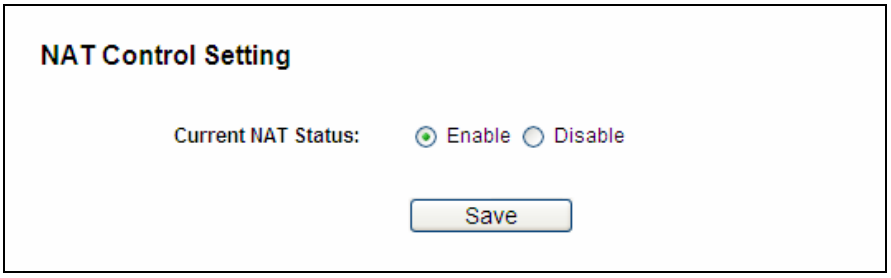


Figure 4-40 NAT Control Setting

- **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.

4.10 Forwarding

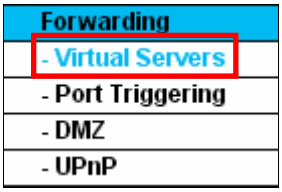


Figure 4-41 The Forwarding menu

There are four submenus under the Forwarding menu (shown in Figure 4-41): **Virtual Servers**, **Port Triggering**, **DMZ** and **UPnP**. Click any of them, and you will be able to configure the corresponding function.

4.10.1 Virtual Servers

Choose menu "**Forwarding→Virtual Servers**", you can view and add virtual servers in the screen as shown in Figure 4-42.Virtual servers can be used for setting up public services on your LAN, such as DNS, Email and FTP. A virtual server is defined as a service port, and all requests from the Internet to this service port will be redirected to the computer specified by the server IP. Any PC that was used for a virtual server must have a static or reserved IP Address because its IP Address may be changed when using the DHCP function.

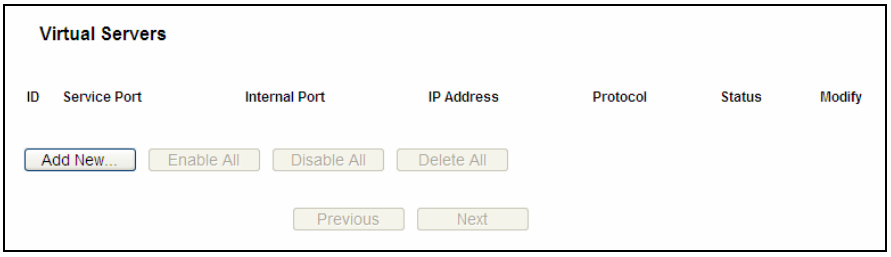


Figure 4-42 Virtual Servers

- **Service Port -** The numbers of External Ports. You can type a service port or a range of service ports (in XXX – YYY format, XXX is the start port number, YYY is the end port number).
- **Internal Port -** The Internal Service Port number of the PC running the service application. You can leave it blank if the **Internal Port** is the same as the **Service Port**, or enter a specific port number when **Service Port** is a single one.
- **IP Address -** The IP Address of the PC providing the service application.

- **Protocol -** The protocol used for this application, either **TCP**, **UDP**, or **All** (all protocols supported by the router).
- **Status -** The status of this entry, either **Enabled** or **Disabled**.

To setup a virtual server entry:

1. Click the **Add New…** button, the next screen will pop-up as shown in Figure 4-43.
2. Select the service port you want to use from the **Common Service Port** list. If the **Common Service Port** list does not have the service that you want to use, type the service port number or service port range in the **Service Port** box. For single Service Port, please enter a specific port number in **Internal Port** box.
3. Type the IP Address of the computer in the **IP Address** box.
4. Select the protocol used for this application, either **TCP**, **UDP**, or **All**.
5. Select the **Enable** to enable the virtual server.
6. Click the **Save** button.

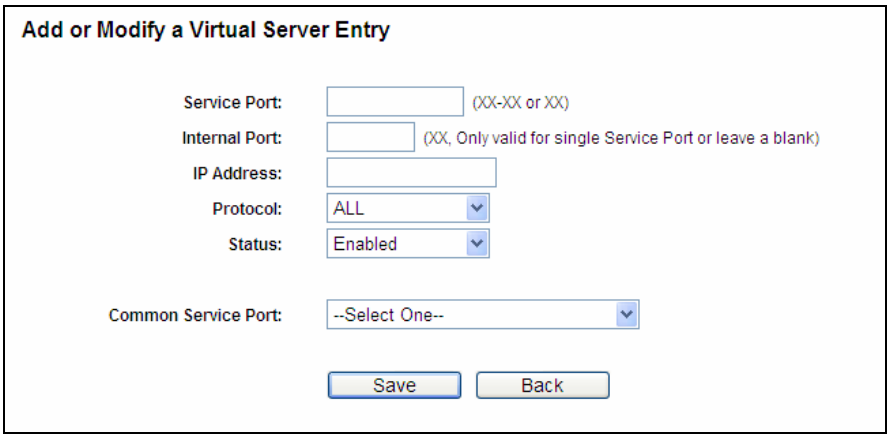


Figure 4-43 Add or Modify a Virtual Server Entry

Note:

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

To modify or delete an existing entry:

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

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

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

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

Note:

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

4.10.2 Port Triggering

Choose menu "**Forwarding → Port Triggering**", and then you can view and add port triggering in the screen as shown in Figure 4-44. Some applications require multiple connections, like Internet games, video conferencing, Internet calling and so on. These applications cannot work with a pure NAT router. Port Triggering is used for some of these applications that can work with an NAT router.

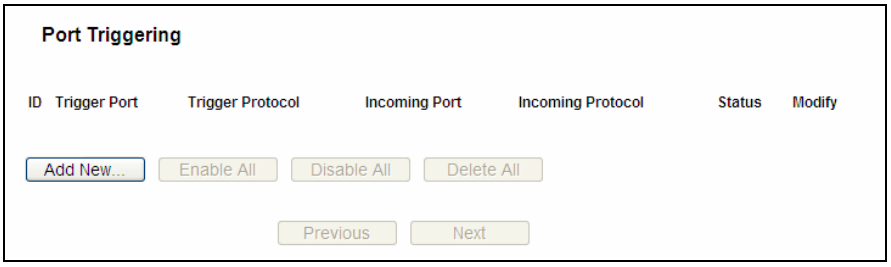


Figure 4-44 Port Triggering

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

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

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

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

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 4-45.
2. Select a common application from the **Common Applications** drop-down list, then the **Trigger Port** field and the **Incoming Ports** field will be automatically filled. If the **Common Applications** do not have the application you need, enter the **Trigger Port** and the **Incoming Ports** manually.
3. Select the protocol used for Trigger Port from the **Trigger Protocol** drop-down list, either **TCP**, **UDP**, or **All**.
4. Select the protocol used for Incoming Ports from the **Incoming Protocol** drop-down list, either **TCP** or **UDP**, or **All.**
5. Select **Enable** in **Status** field.
6. Click the **Save** button to save the new rule.

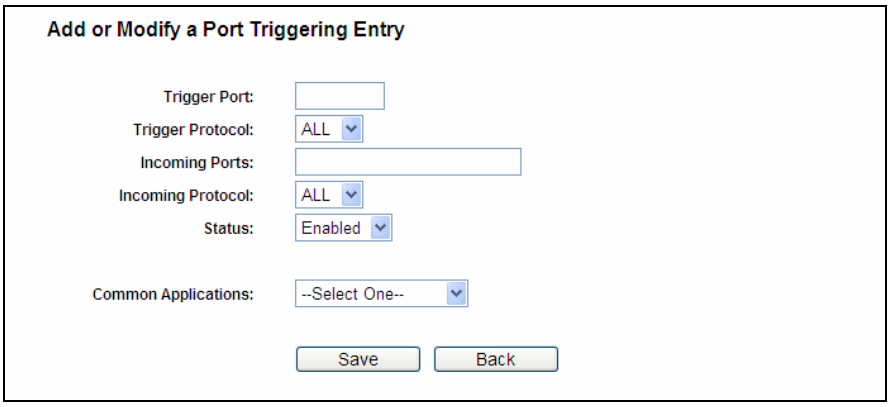


Figure 4-45 Add or Modify a Port Triggering Entry

To modify or delete an existing entry:

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

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

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

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

Note:

1. When the trigger connection is released, the corresponding opening ports will be closed.
2. Each rule is allowed to be used only by one host on LAN synchronously. The trigger connection of other hosts on LAN will be refused.

3. Incoming Port Range cannot overlap each other.

4.10.3 DMZ

Choose menu "**Forwarding → DMZ**", and then you can view and configure DMZ host in the screen as shown in Figure 4-46. The DMZ host feature allows one local host to be exposed to the Internet for a special-purpose service such as Internet gaming or videoconferencing. DMZ host forwards all the ports at the same time. Any PC whose port is being forwarded must have its DHCP client function disabled and should have a new static IP Address assigned to it because its IP Address may be changed when using the DHCP function.

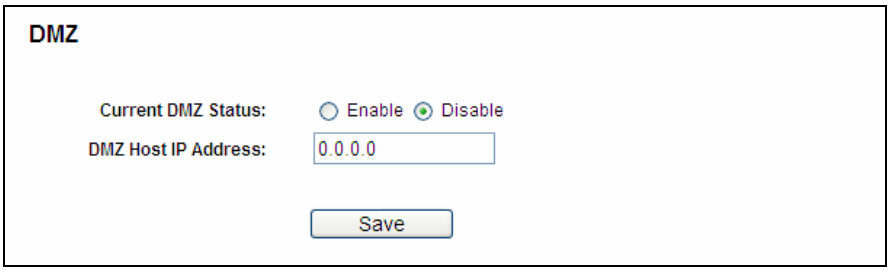


Figure 4-46 DMZ

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

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

☞ **Note:**

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

4.10.4 UPnP

Choose menu "**Forwarding → UPnP**", and then you can view the information about **UPnP** (Universal Plug and Play) in the screen as shown in Figure 4-47. The UPnP feature allows the devices, such as Internet computers, to access the local host resources or devices as needed. UPnP devices can be automatically discovered by the UPnP service application on the LAN.

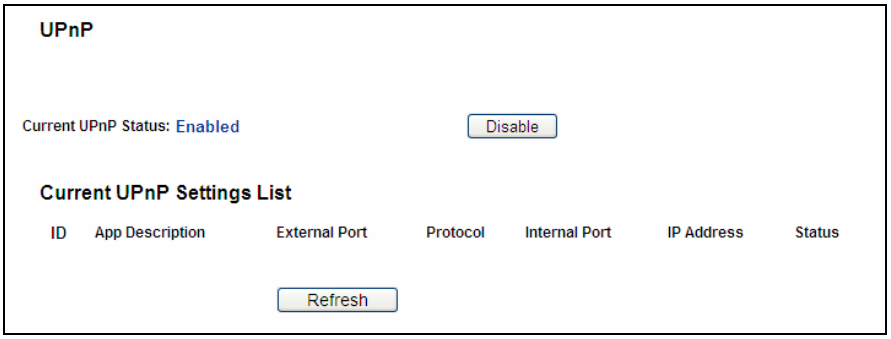


Figure 4-47 UPnP

- **Current UPnP Status -** UPnP can be enabled or disabled by clicking the **Enable** or **Disable** button.

- **Current UPnP Settings List -** This table displays the current UPnP information.
  - **App Description -** The description provided by the application in the UPnP request.
  - **External Port -** The external port the router opens for the application.
  - **Protocol -** The type of protocol the router opens for the application.
  - **Internal Port -** The Internal port the router opens for local host.
  - **IP Address -** The IP address of the UPnP device that is currently accessing the router.
  - **Status -** The status of the port is displayed here. "Enabled" means that the port is still active. Otherwise, the port is inactive.

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

4.11 Security

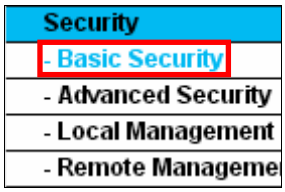


Figure 4-48 The Security menu

There are four submenus under the Security menu as shown in Figure 4-48: **Basic Security**, **Advanced Security**, **Local Management** and **Remote Management.** Click any of them, and you will be able to configure the corresponding function.

4.11.1 Basic Security

Choose menu "**Security→Basic Security**", you can configure the basic security in the screen as shown in Figure 4-49.

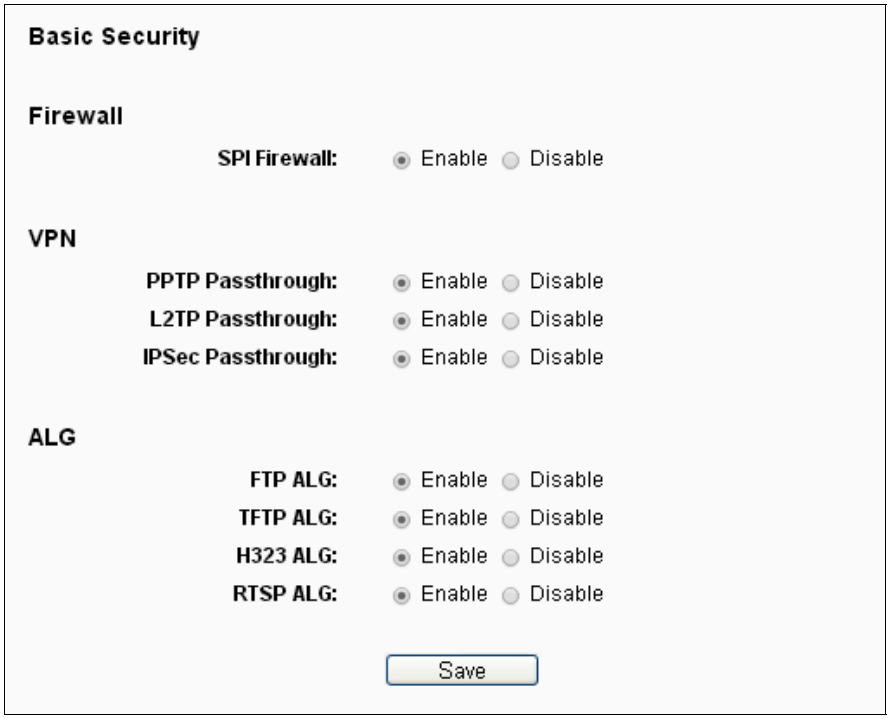


Figure 4-49 Basic Security

- **Firewall -** A firewall protects your network from the outside world. Here you can enable or disable the router's firewall.
  - **SPI Firewall -** SPI (Stateful Packet Inspection, also known as dynamic packet filtering) helps to prevent cyber attacks by tracking more state per session. It validates that the traffic passing through the session conforms to the protocol. SPI Firewall is enabled by factory default. If you want all the computers on the LAN exposed to the outside world, you can disable it.
- **VPN -** VPN Passthrough must be enabled if you want to allow VPN tunnels using IPSec, PPTP, or L2TP protocols to pass through the router's firewall.
  - **PPTP Passthrough -** Point-to-Point Tunneling Protocol (PPTP) allows the Point-to-Point Protocol (PPP) to be tunneled through an IP network. To allow PPTP tunnels to pass through the router, keep the default, **Enabled**.
  - **L2TP Passthrough-** Layer 2 Tunneling Protocol (L2TP) is the method used to enable Point-to-Point sessions via the Internet on the Layer 2 level. To allow L2TP tunnels to pass through the router, keep the default, **Enabled**.
  - **IPSecPassthrough-** Internet Protocol Security (IPSec) is a suite of protocols for ensuring private, secure communications over Internet Protocol (IP) networks, through the use of cryptographic security services. To allow IPSec tunnels to pass through the router, keep the default, **Enabled**.
- **ALG -** It is recommended to enable Application Layer Gateway (ALG) because ALG allows customized Network Address Translation (NAT) traversal filters to be plugged into the

gateway to support address and port translation for certain application layer "control/data" protocols such as FTP, TFTP, H323 etc.

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

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

4.11.2 Advanced Security

Choose menu "**Security→Advanced Security**", you can protect the router from being attacked by TCP-SYN Flood, UDP Flood and ICMP-Flood in the screen as shown in Figure 4-50.

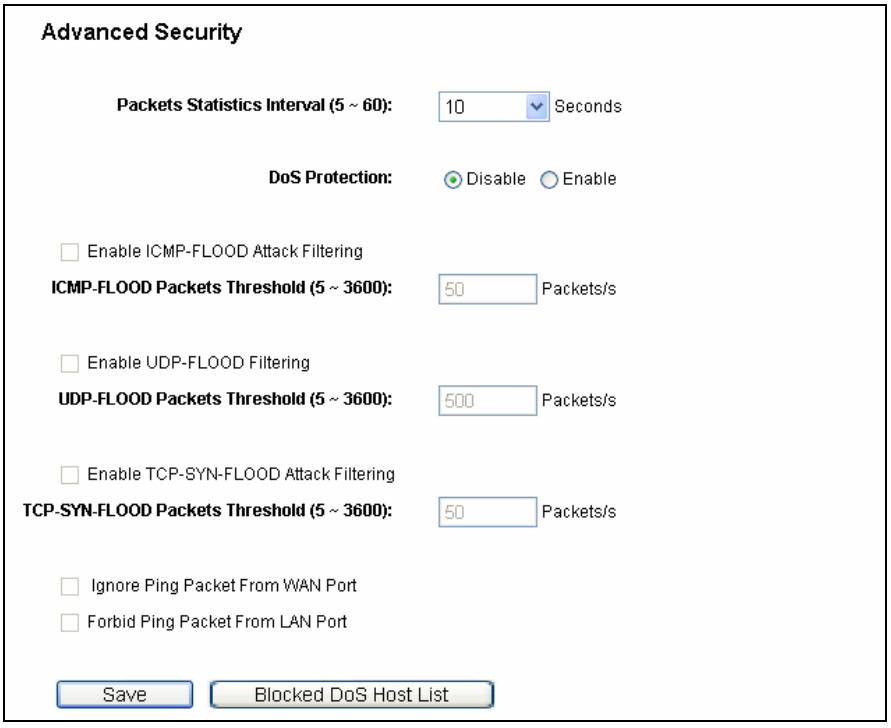


Figure 4-50 Advanced Security

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

☞**Note:**

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

- **Enable ICMP-FLOOD Attack Filtering-** Enable or Disable the ICMP-FLOOD Attack Filtering.
- **ICMP-FLOOD Packets Threshold (5~3600)-** The default value is 50. Enter a value between 5 ~ 3600. When the current ICMP-FLOOD Packets number is beyond the set value, the router will startup the blocking function immediately.
- **Enable UDP-FLOOD Filtering-** Enable or Disable the UDP-FLOOD Filtering.
- **UDP-FLOOD Packets Threshold (5~3600)-** The default value is 500. Enter a value between 5 ~ 3600. When the current UPD-FLOOD Packets number is beyond the set value, the router will startup the blocking function immediately.
- **Enable TCP-SYN-FLOOD Attack Filtering-** Enable or Disable the TCP-SYN-FLOOD Attack Filtering.
- **TCP-SYN-FLOOD Packets Threshold (5~3600)-** The default value is 50. Enter a value between 5 ~ 3600. When the current TCP-SYN-FLOOD Packets numbers is beyond the set value, the router will startup the blocking function immediately.
- **Ignore Ping Packet From WAN Port-** Enable or Disable Ignore Ping Packet From WAN Port. The default setting is disabled. If enabled, the ping packet from the Internet cannot access the router.
- **Forbid Ping Packet From LAN Port-** Enable or Disable Forbid Ping Packet From LAN Port. The default setting is disabled. If enabled, the ping packet from LAN cannot access the router. This function can be used to defend against some viruses.

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

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

4.11.3 Local Management

Choose menu "**Security→Local Management**", you can configure the management rule in the screen as shown in Figure 4-51.The management feature allows you to deny computers in LAN from accessing the router.

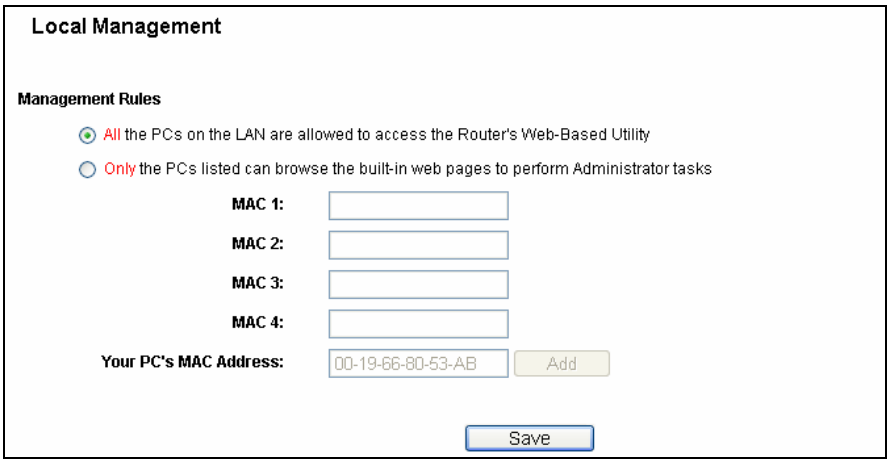


Figure 4-51 Local Management

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

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

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

☞Note:

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

4.11.4 Remote Management

Choose menu "**Security→Remote Management**", you can configure the Remote Management function in the screen as shown in Figure 4-52.This feature allows you to manage your router from a remote location via the Internet.

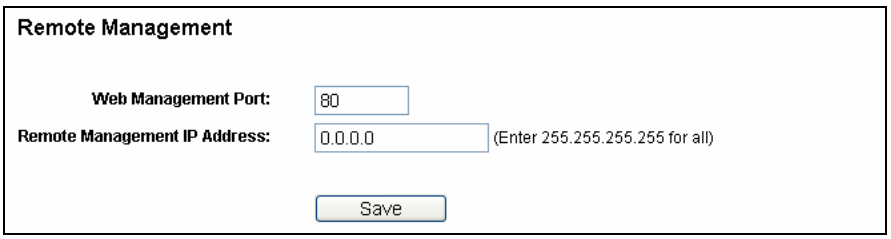


Figure 4-52 Remote Management

- **Web Management Port -** Web browser access normally uses the standard HTTP service port 80. This router's default remote management web port number is 80. For greater security, you can change the remote management web port to a custom port by entering that number

in the box provided. Choose a number between 1 and 65534 but do not use the number of any common service port.

- **Remote Management IP Address-** This is the current address you will use when accessing your router from the Internet. This function is disabled when the IP address is set to the default value of 0.0.0.0. To enable this function change 0.0.0.0 to a valid IP address. If set to 255.255.255.255, then all the hosts can access the router from internet.

☞Note:

1. To access the router, you should type your router's WAN IP address into your browser's address (in IE) or Location (in Navigator) box, followed by a colon and the custom port number. For example, if your router's WAN address is 202.96.12.8, and the port number used is 8080, please enter http://202.96.12.8:8080in 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.

4.12 Parental Control

Choose menu "**Parental Control**", you can configure the parental control in the screen as shown in Figure 4-53. The Parental Control function can be used to control the internet activities of the child, limit the child to access certain websites and restrict the time of surfing.

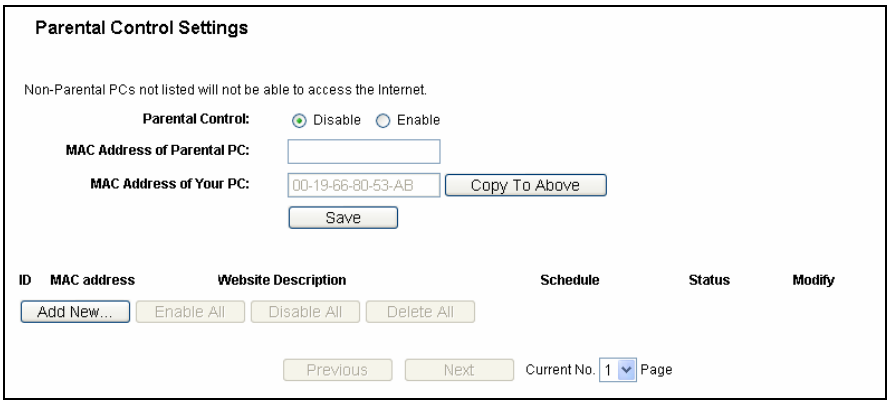


Figure 4-53 Parental Control Settings

- **Parental Control -** Check **Enable** if you want this function to take effect, otherwise check **Disable**.
- **MAC Address of Parental PC -** In this field, enter the MAC address of the controlling PC, or you can make use of the **Copy To Above** button below.
- **MAC Address of Your PC -** This field displays the MAC address of the PC that is managing this router. If the MAC Address of your adapter is registered, you can click the Copy To Above button to fill this address to the MAC Address of Parental PC field above.
- **Website Description -** Description of the allowed website for the PC controlled.

- **Schedule-**The time period allowed for the PC controlled to access the Internet. For detailed information, please go to "**Access Control→Schedule**".
- **Modify-** Here you can edit or delete an existing entry.

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

1. Click the **Add New…**button and the next screen will pop-up as shown in Figure 4-54.
2. Enter the MAC address of the PC (e.g.00-11-22-33-44-AA) you'd like to control in the MAC Address of Child PC field. Or you can choose the MAC address from the All Address in Current LAN drop-down list.
3. Give a description (e.g. Allow Google) for the website allowed to be accessed in the Website Description field.
4. Enter the domain name of the website (e.g. www.google.com) in the Allowed Domain Name field.
5. Select from the Effective Time drop-down list the schedule (e.g. Schedule_1) you want the entry to take effect. If there are not suitable schedules for you, click the **Schedule** in red below to go to the Advance Schedule Settings page and create the schedule you need.
6. In the Status field, you can select **Enabled** or **Disabled** to enable or disable your entry.
7. Click the **Save** button.

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

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

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

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

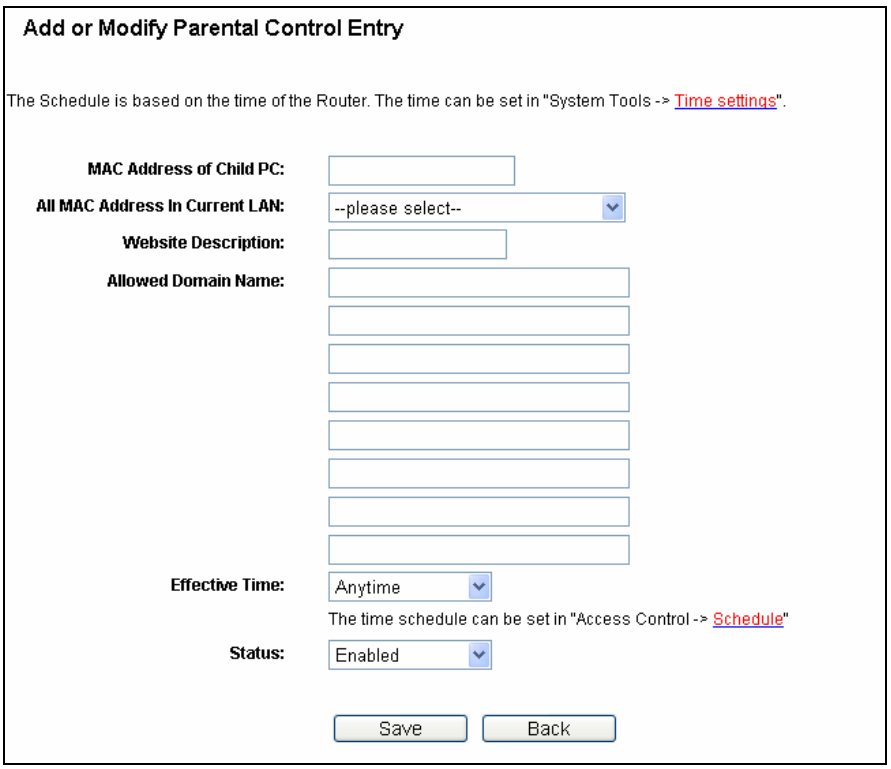


Figure 4-54 Add or Modify Parental Control Entry

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

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

Then you will go back to the Parental Control Settings page and see the following list, as shown in Figure 4-55.

Figure 4-55 Parental Control Settings

4.13 Access Control

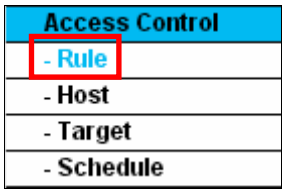


Figure 4-56 Access Control

There are four submenus under the Access Control menu as shown in Figure 4-56: **Rule**, **Host**, **Target** and **Schedule**. Click any of them, and you will be able to configure the corresponding function.

4.13.1 Rule

Choose menu "**Access Control→Rule**", you can view and set Access Control rules in the screen as shown in Figure 4-57.

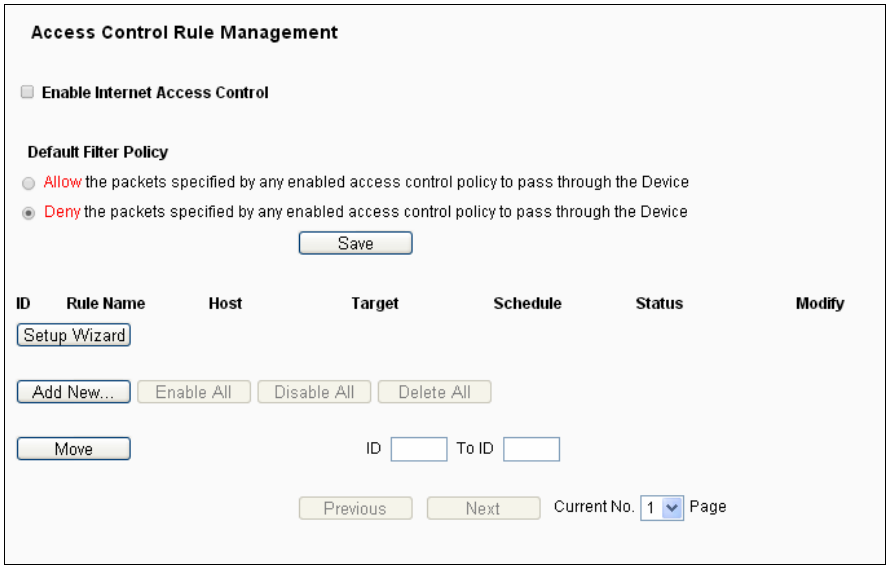


Figure 4-57 Access Control Rule Management

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

- **Schedule -** Here displays the schedule selected in the corresponding rule.
- **Status -** This field displays the status of the rule. **Enabled** means the rule will take effect, **Disabled** means the rule will not take effect.
- **Modify -** Here you can edit or delete an existing rule.

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

1. Click the **Add New…** button and the next screen will pop-up as shown in Figure 4-58.
2. Give a name (e.g. Rule_1) for the rule in the **Rule Name** field.
3. Select a host from the **Host** drop-down list or choose "**Click Here To Add New Host List**".
4. Select a target from the **Target** drop-sown list or choose "**Click Here To Add New Target List**".
5. Select a schedule from the **Schedule** drop-down list or choose "**Click Here To Add New Schedule**".
6. In the **Status** field, select **Enabled** or **Disabled** to enable or disable your entry.
8. Click the **Save** button.

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

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

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

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

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

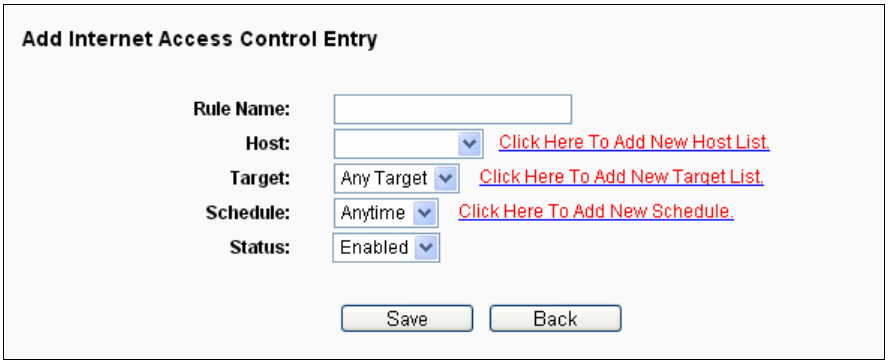


Figure 4-58 Add or Modify Internet Access Control Entry

For example: If you desire to allow the host with MAC address00-11-22-33-44-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 "**Access Control→Host**" in the left to enter the Host Settings page. Add a new entry with the Host Description is Host_1 and MAC Address is 00-11-22-33-44-AA.
2. Click "**Access Control→Target**" in the left to enter the Target Settings page. Add a new entry with the Target Description is Target_1 and Domain Name is www.google.com.
3. Click "**Access Control→Schedule**" in the left to enter the Schedule Settings page. Add a new entry with the Schedule Description is Schedule_1, Day is Sat and Sun, Start Time is 1800 and Stop Time is 2000.
4. Click "**Access Control→Rule**" in the left to return to the Access Control Rule Management page. Select "**Enable Internet Access Control**" and choose "Deny the packets not specified by any access control policy to pass through the router".
5. Click **Add New...** button to add a new rule as follows:
   - In **Rule Name** field, create a name for the rule. Note that this name should be unique, for example Rule_1.
   - In **Host** field, select Host_1.
   - In **Target** field, select Target_1.
   - In **Schedule** field, select Schedule_1.
   - In **Action** field, select Allow.
   - In **Status** field, select Enable.
   - Click **Save** to complete the settings.

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

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

4.13.2 Host

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

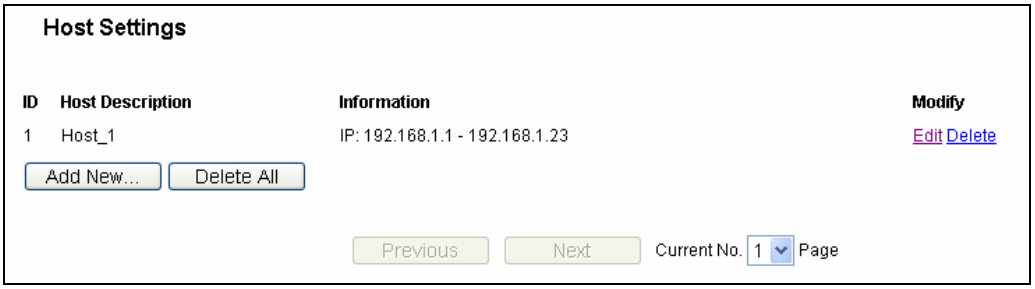


Figure 4-59 Host Settings

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

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

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

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

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

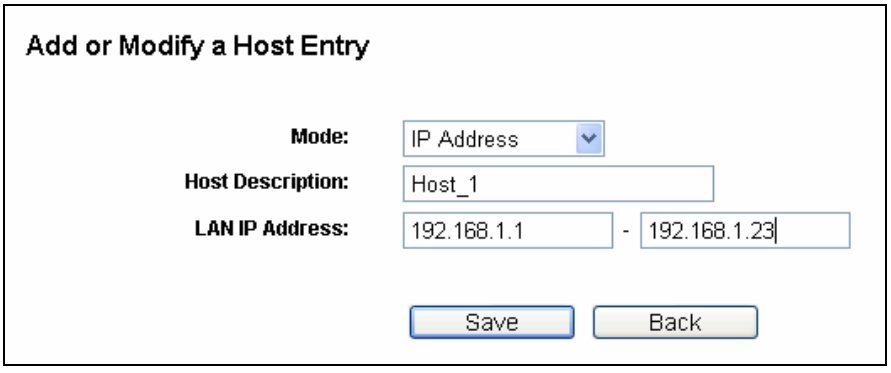


Figure 4-60 Add or Modify a Host Entry

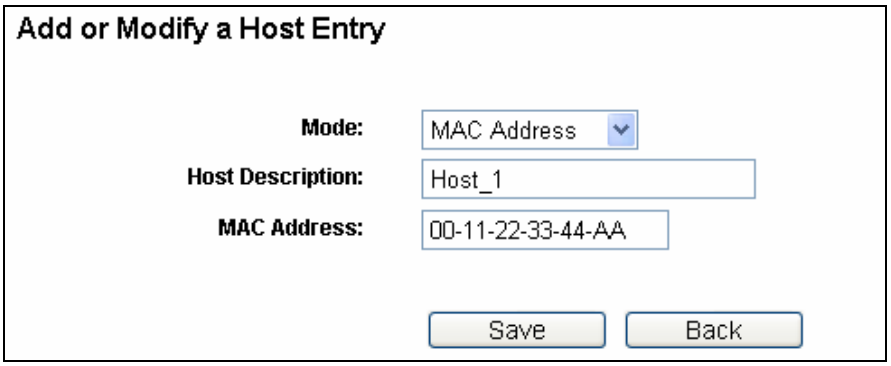
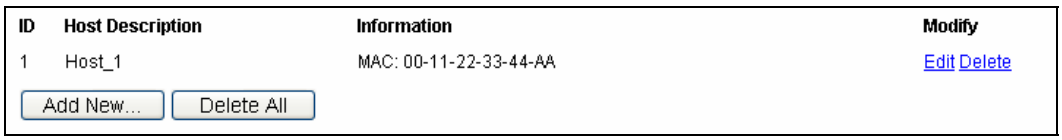


Figure 4-61 Add or Modify a Host Entry

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

1. Click **Add New...** button in Figure 4-59to enter the Add or Modify a Host Entry page.
2. In **Mode** field, select MAC Address from the drop-down list.
3. In **Host Description** field, create a **unique** description for the host (e.g. Host_1).
4. In **MAC Address** field, enter 00-11-22-33-44-AA.
5. Click **Save** to complete the settings.

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



4.13.3 Target

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

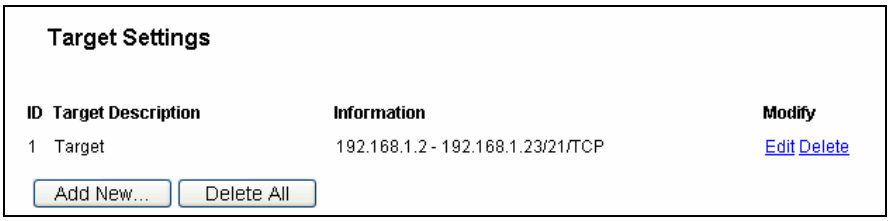


Figure 4-62 Target Settings

- **Target Description -** Here displays the description about the target and this description is unique.
- **Information -** The target can be an IP address, a port, or a domain name.
- **Modify -** To modify or delete an existing entry.

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

1. Click the **Add New…** button.
2. In **Mode** field, select IP Address or Domain Name.

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

3. Click the **Save** button.

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

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

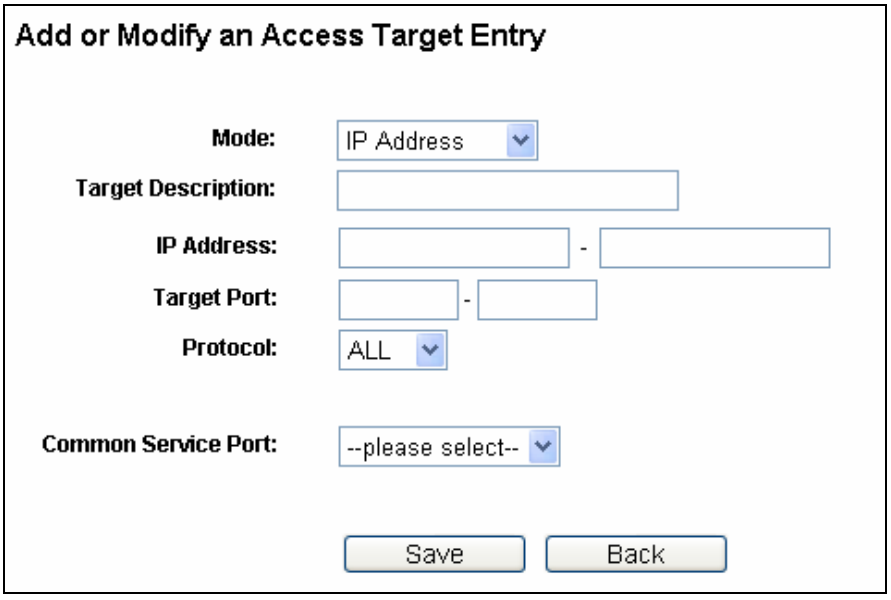


Figure 4-63 Add or Modify an Access Target Entry

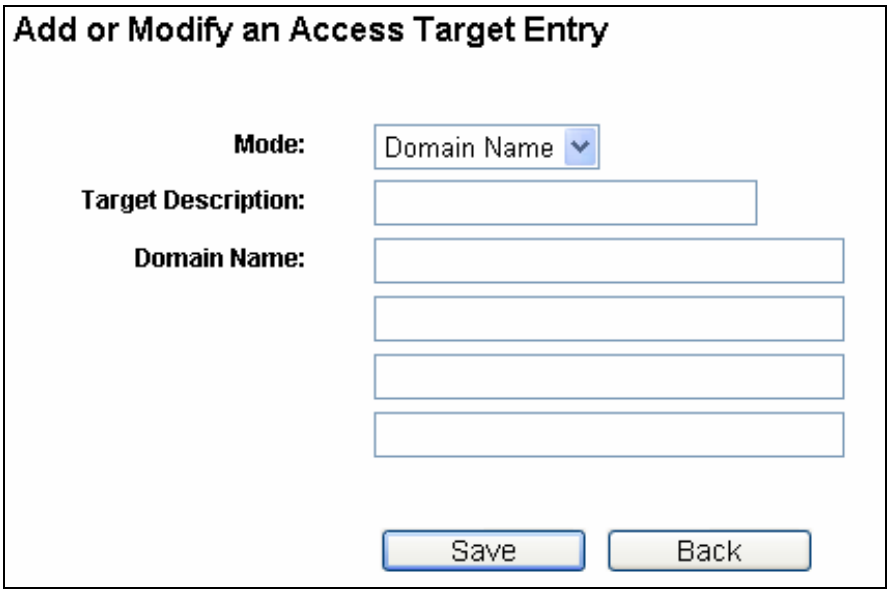


Figure 4-64 Add or Modify an Access Target Entry

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

1. Click **Add New…** button in Figure 4-62 to enter the Add or Modify an Access Target Entry page.
2. In **Mode** field, select Domain Name from the drop-down list.
3. In **Target Description** field, create a unique description for the target (e.g. Target_1).
4. In **Domain Name** field, enter www.google.com.
5. Click **Save** to complete the settings.

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

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

4.13.4 Schedule

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

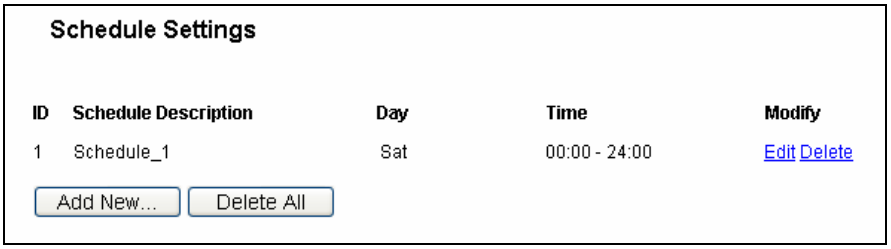


Figure 4-65 Schedule Settings

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

To add a new schedule, follow the steps below.

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

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

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

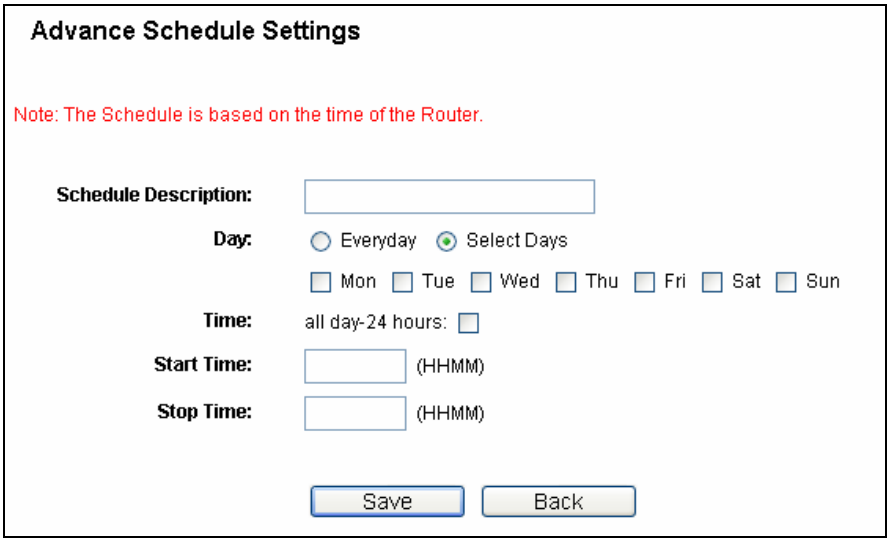


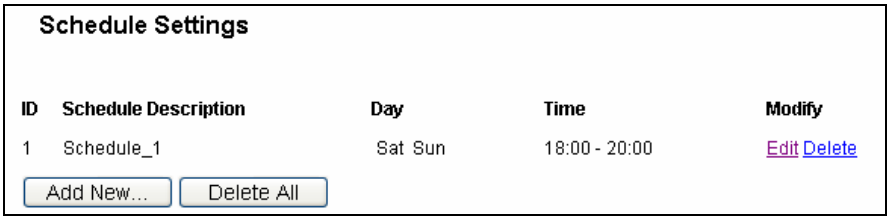
Figure 4-66 Advanced Schedule Settings

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

1. Click **Add New...** button shown in Figure 4-65 to enter the Advanced Schedule Settings page.

2. In **Schedule Description** field, create a unique description for the schedule (e.g. Schedule_1).
3. In **Day** field, check the Select Days radio button and then select Sat and Sun.
4. In **Time** field, enter1800 in Start Time field and 2000 in Stop Time field.
5. Click **Save** to complete the settings.

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



4.14 Advanced Routing

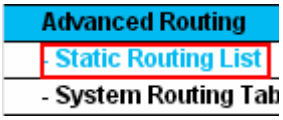


Figure 4-67 Advanced Routing

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

4.14.1 Static Routing List

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

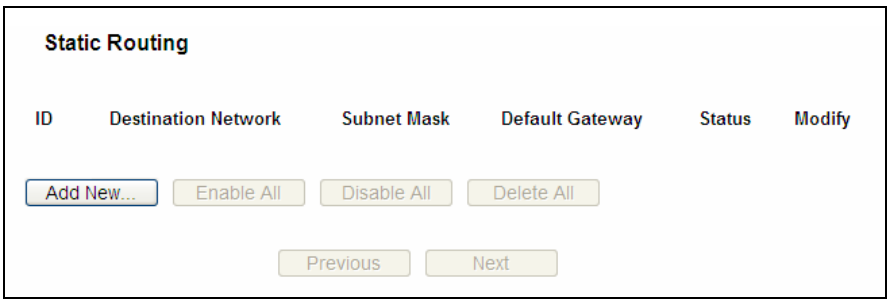


Figure 4-68 Static Routing

To add static routing entries:

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

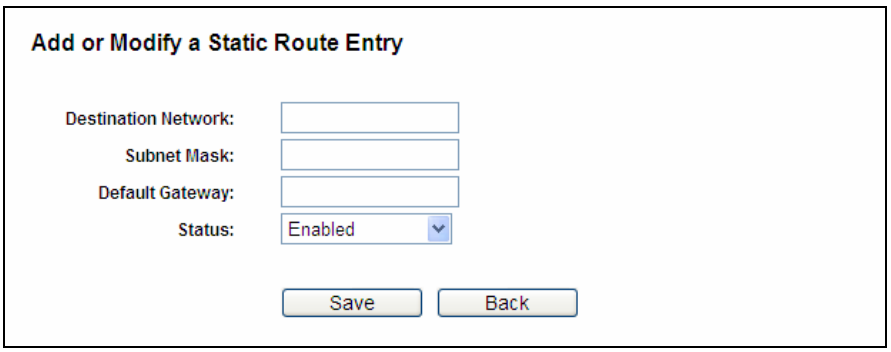


Figure 4-69 Add or Modify a Static Route Entry

2. Enter the following data:

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

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

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

Other configurations for the entries:

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

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

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

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

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

4.14.2 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 4-70). System routing table views all of the valid route entries in use. The Destination IP address, Subnet Mask, Gateway, and Interface will be displayed for each entry.

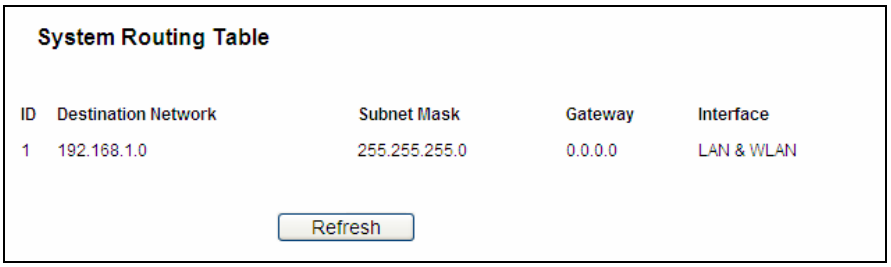


Figure 4-70 System Routing Table

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

4.15 Bandwidth Control

Figure 4-71

There are two submenus under the Bandwidth Control menu as shown in Figure 4-71. Click any of them, and you will be able to configure the corresponding function. The detailed explanations for each submenu are provided below.

4.15.1 Control Settings

Choose menu "**Bandwidth Control→Control Settings**", you can configure the Egress Bandwidth and Ingress Bandwidth in the next screen. Their values you configure should be less than 1000000Kbps.

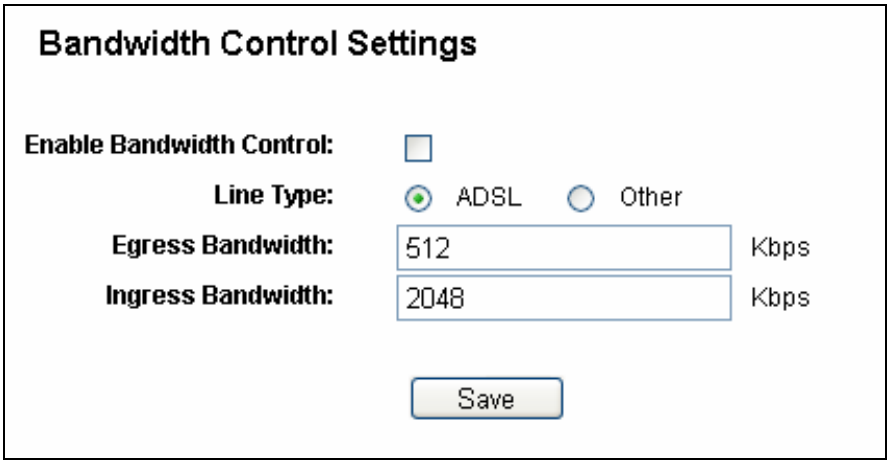


Figure 4-72 Bandwidth Control Settings

☞Note:

For optimal control of the bandwidth, please select the right bandwidth type and ask your ISP for the total bandwidth of the egress and ingress.

4.15.2 Rules List

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

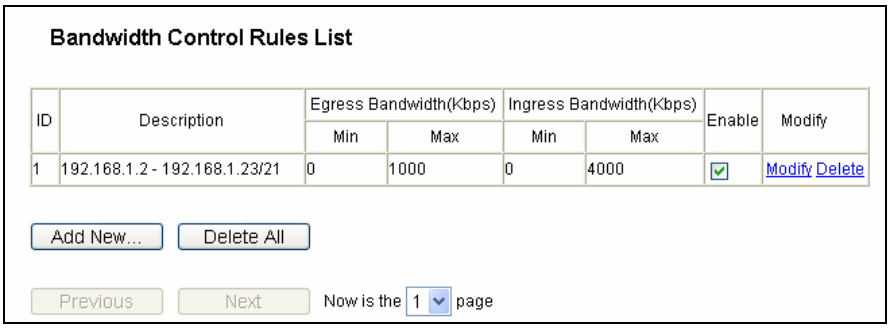


Figure 4-73 Bandwidth Control Rules List

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

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

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

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

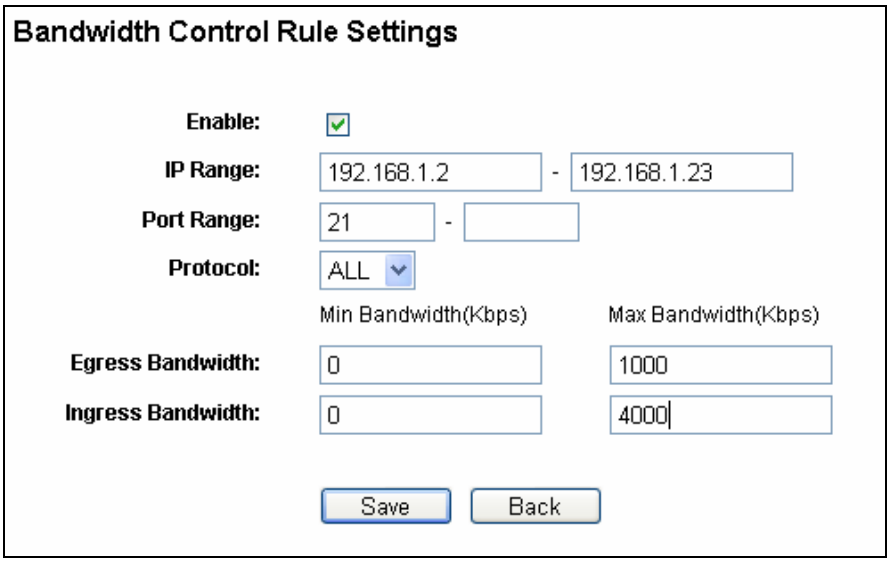


Figure 4-74 Bandwidth Control Rule Settings

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

4.16 IP& MAC Binding

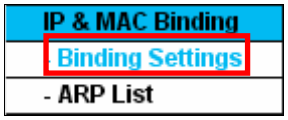


Figure 4-75 the IP & MAC Binding menu

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

4.16.1 Binding Settings

This page displays the **IP & MAC Binding Setting** table; you can operate it in accord with your desire as shown in Figure 4-76.

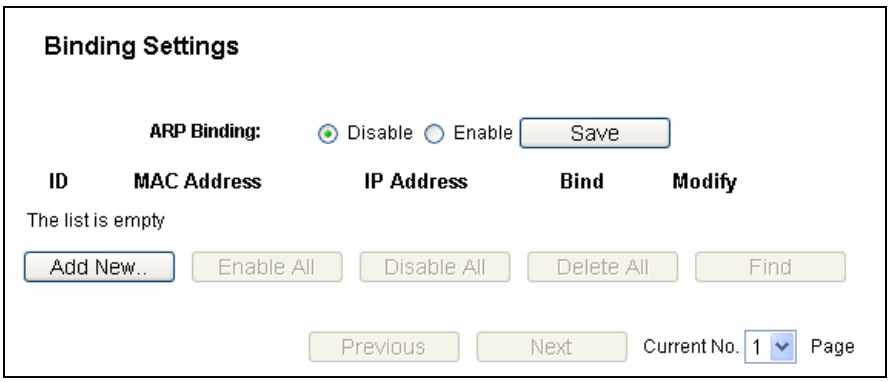


Figure 4-76 Binding Settings

- **MAC Address-** The MAC address of the controlled computer in the LAN.
- **IP Address -** The assigned IP address of the controlled computer in the LAN.

- **Bind-**Check this option to enable ARP binding for a specific device.
- **Modify-**To modify or delete an existing entry.

When you want to add or modify an IP & MAC Binding entry, you can click the **Add New…** button or **Modify** button, and then you will go to the next page. This page is used for adding or modifying an IP & MAC Binding entry, shown in Figure 4-77.

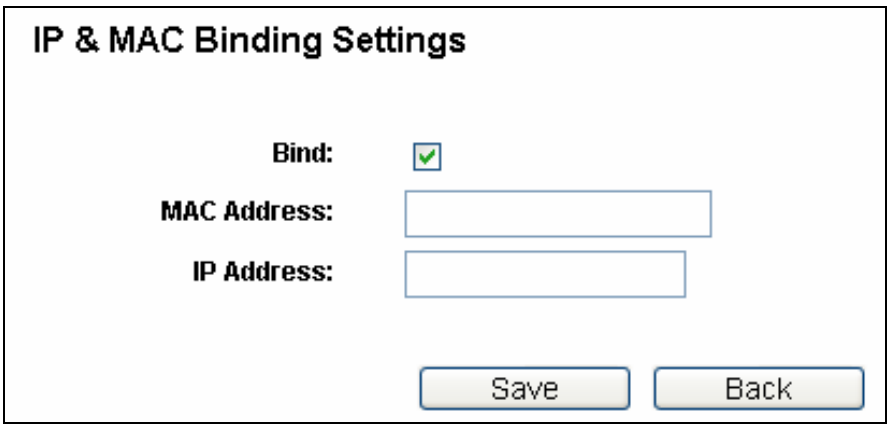


Figure 4-77 IP & MAC Binding Settings

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

1. Click the **Add New...** button as shown in Figure 4-76.
2. Enter the MAC Address and IP Address.
3. Select the Bind checkbox.
4. Click the **Save** button to save it.

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

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

To find an existing entry, follow the steps below.

1. Click the **Find** button as shown in Figure 4-76.
2. Enter the MAC Address or IP Address.
3. Click the **Find** button in the page as shown in Figure 4-78.

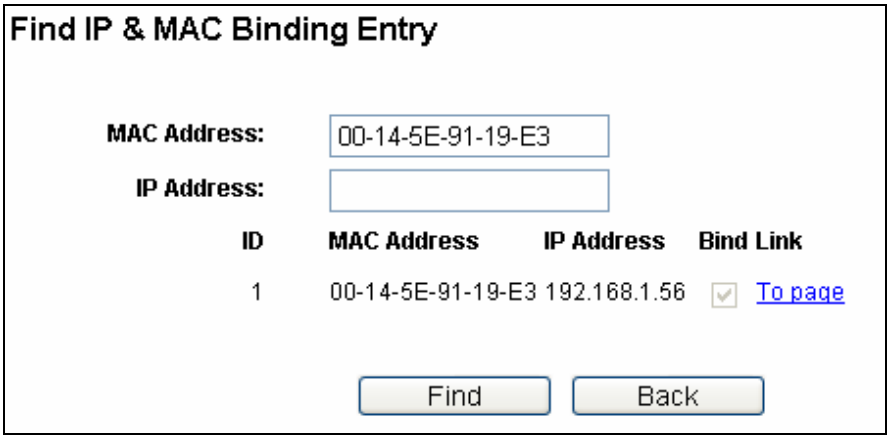


Figure 4-78 Find IP & MAC Binding Entry

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

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

4.16.2 ARP List

To manage the computer, you could observe the computers in the LAN by checking the relationship of MAC address and IP address on the ARP list, and you could configure the items on the ARP list also. This page displays the ARP List; it shows all the existing IP & MAC Binding entries as shown in Figure 4-79.

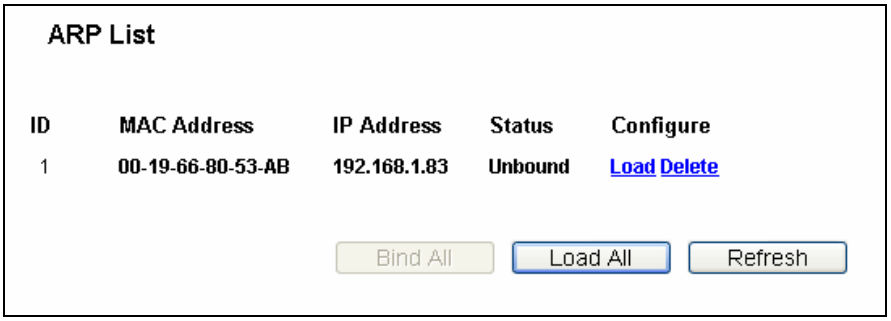


Figure 4-79 ARP List

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

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

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

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

☞Note:

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

4.17 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.

4.17.1 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 4-68.

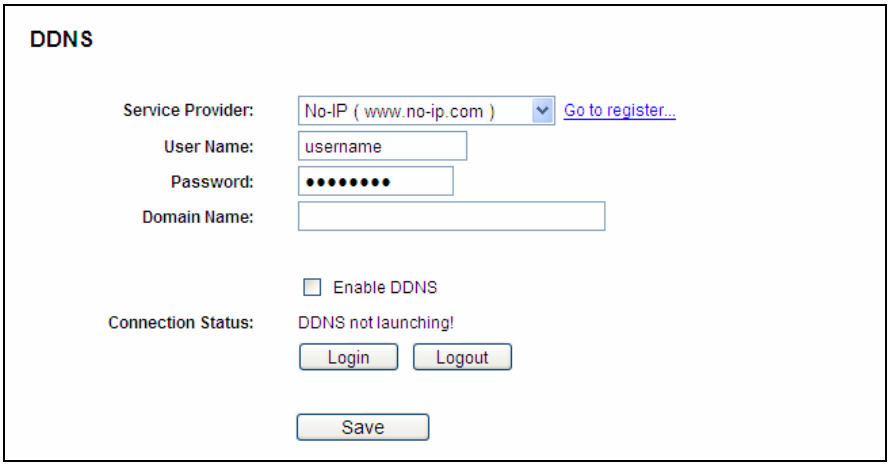


Figure 4-80 No-ip.com DDNS Settings

To set up for DDNS, follow these instructions:

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

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

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

4.17.2 Dyndns.org DDNS

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

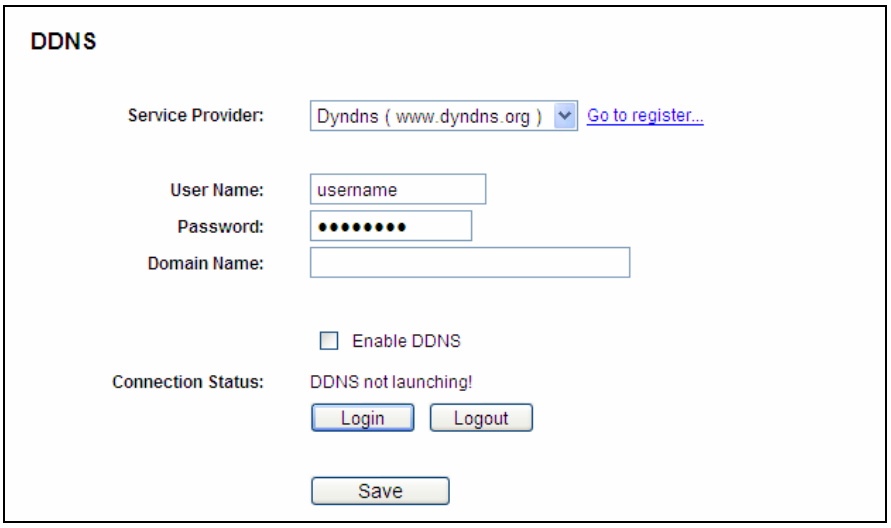


Figure 4-81 Dyndns.org DDNS Settings

To set up for DDNS, follow these instructions:

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

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

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

4.17.3 Comexe.cn DDNS

If the dynamic DNS **Service Provider** you select is www.comexe.cn, the page will appear as shown in Figure 4-82.

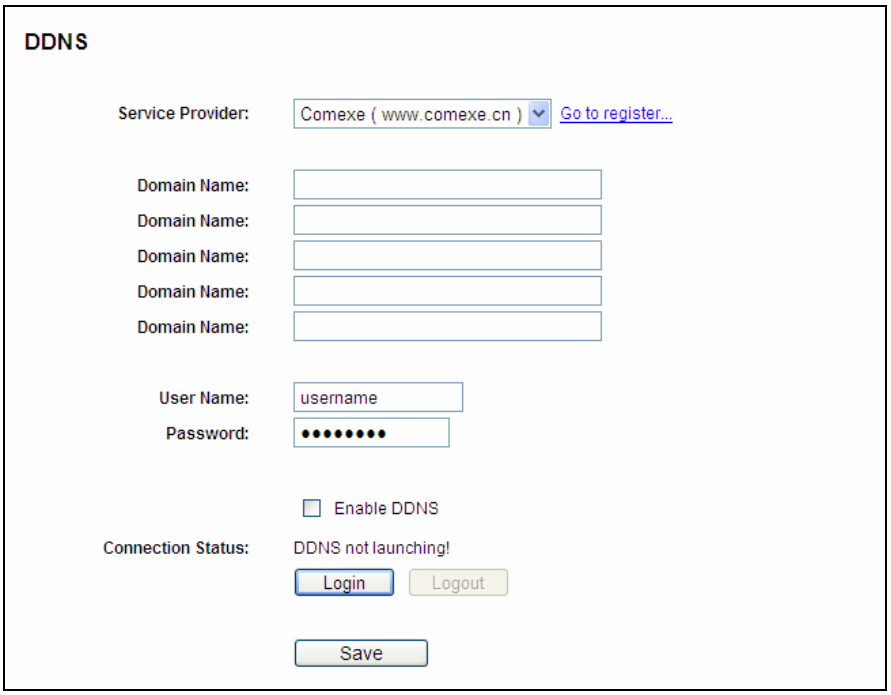


Figure 4-82 Comexe.cn DDNS Settings

To set up for DDNS, follow these instructions:

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

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

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

4.18 System Tools

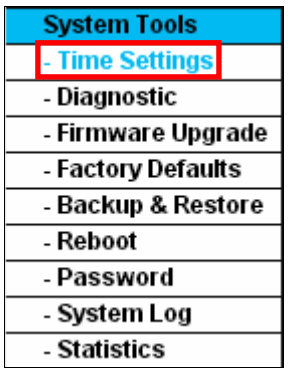


Figure 4-83 The System Tools menu

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

4.18.1 Time Settings

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

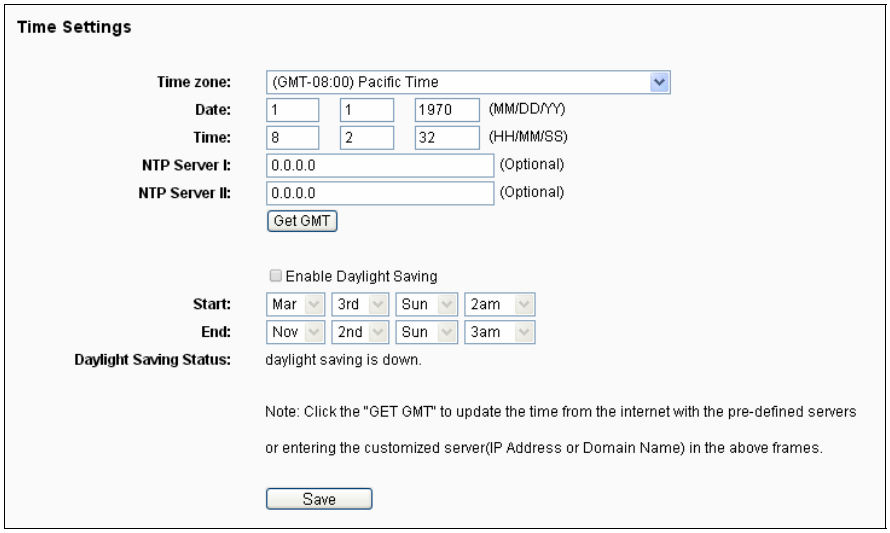


Figure 4-84 Time settings

- **Time Zone -** Select your local time zone from this pull down list.
- **Date -** Enter your local date in MM/DD/YY into the right blanks.
- **Time -** Enter your local time in HH/MM/SS into the right blanks.
- **NTP Server Prior -** Enter the address for the NTP Server, then the router will get the time from the NTP Server preferentially. In addition, for some built-in common NTP Servers, the router can get time automatically once it connects the Internet.

To configure the system manually:

1. Select your local time zone.
2. Enter date and time in the right blanks.
3. Click **Save** to save the configuration.

To configure the system automatically:

1. Select your local time zone.
2. Enter the IP address for **NTP Server Prior**.
3. Click the **Get GMT** button to get system time from Internet if you have connected to the Internet.

☞Note:

1. This setting will be used for some time-based functions such as firewall. You must specify your time zone once you log in 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 obtain GMT automatically from Internet if it has already connected to Internet.

4.18.2 Diagnostic

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

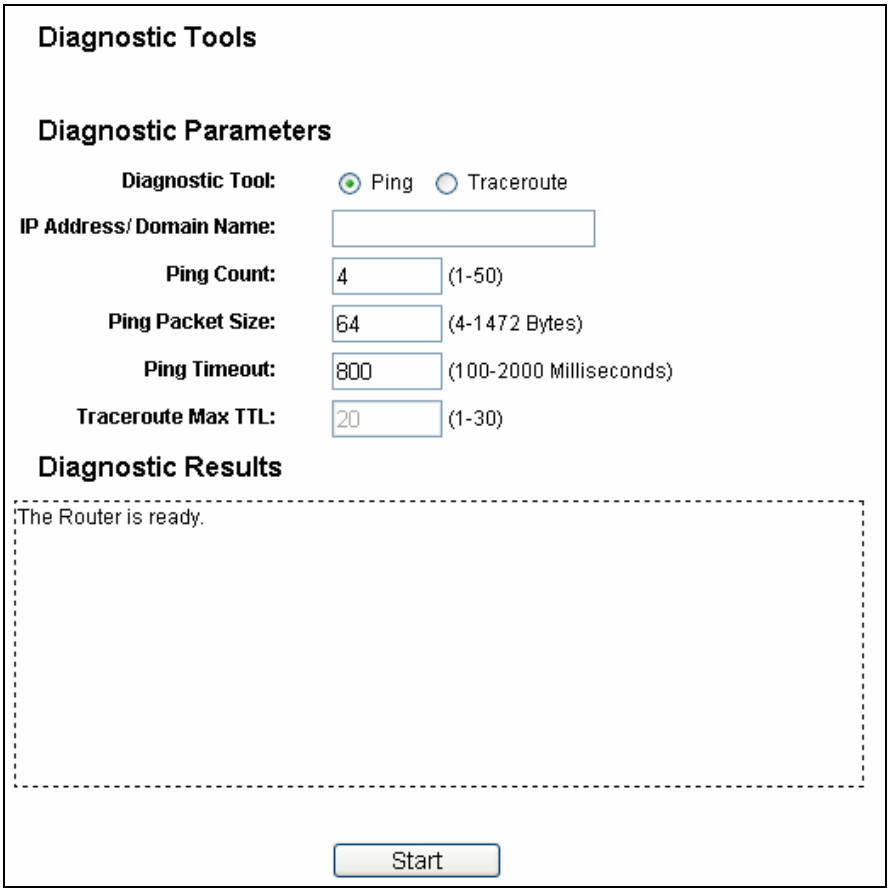


Figure 4-85 Diagnostic Tools

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

  ☞Note:

  You can use ping/traceroute to test both numeric IP address or domain name. If pinging/tracerouting the IP address is successful, but pinging/tracerouting the domain name is

not, you might have a name resolution problem. In this case, ensure that the domain name you are specifying can be resolved by using Domain Name System (DNS) queries.

- **IP Address/Domain Name –**Type the destination IP address (such as 202.108.22.5) or Domain name.
- **Pings Count -**The number of Ping packets for a Ping connection.
- **Ping Packet Size -**The size of Ping packet.
- **Ping Timeout -**Set the waiting time for the reply of each Ping packet. If there is no reply in the specified time, the connection is overtime.
- **Traceroute Max TM-**The max number of hops for a Traceroute connection.

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

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

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

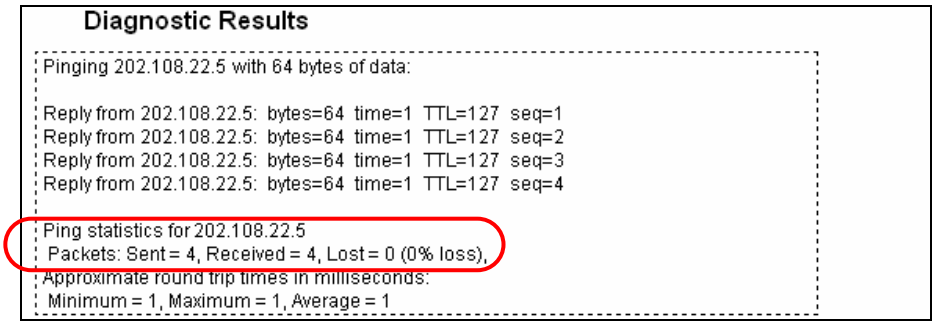


Figure 4-86 Diagnostic Results

Note:

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

4.18.3 Firmware Upgrade

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

Figure 4-87 Firmware Upgrade

- **Firmware Version-**This displays the current firmware version.

- **Hardware Version**-This displays the current hardware version. The hardware version of the upgrade file must accord with the router's current hardware version.

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

1. Download a more recent firmware upgrade file from our website.
2. Type the path and file name of the update file into the **File** field. Or click the **Browse** button to locate the update file.
3. Click the **Upgrade** button.

Note:

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

4.18.4 Factory Defaults

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

Figure 4-88 Restore Factory Default

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

- The default **User Name**: admin
- The default **Password**: admin
- The default **IP Address**: 192.168.1.1
- The default **Subnet Mask**: 255.255.255.0

Note:

1. Any settings you have saved will be lost when the default settings are restored.
2. Press and hold the WPS/Reset button for more than 5 seconds, you can reset the router, too.

4.18.5 Backup & Restore

Choose menu "**System Tools→Backup &Restore**", you can save the current configuration of the router as a backup file and restore the configuration via a backup file as shown in Figure 4-89.

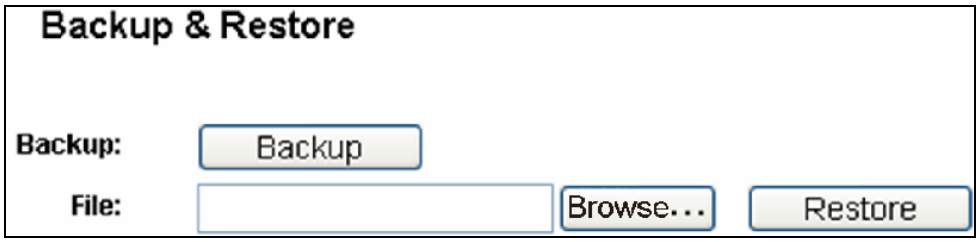


Figure 4-89 Backup & Restore Configuration

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

☞Note:

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

4.18.6 Reboot

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

Figure 4-90 Reboot the router

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

- Change the LAN IP Address (system will reboot automatically).
- Change the DHCP Settings.
- Change the Wireless configurations.
- Change the Web Management Port.
- Upgrade the firmware of the router (system will reboot automatically).

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

4.18.7 Password

Choose menu "**System Tools→Password**", you can change the factory default user name and password of the router in the next screen as shown in Figure 4-91.

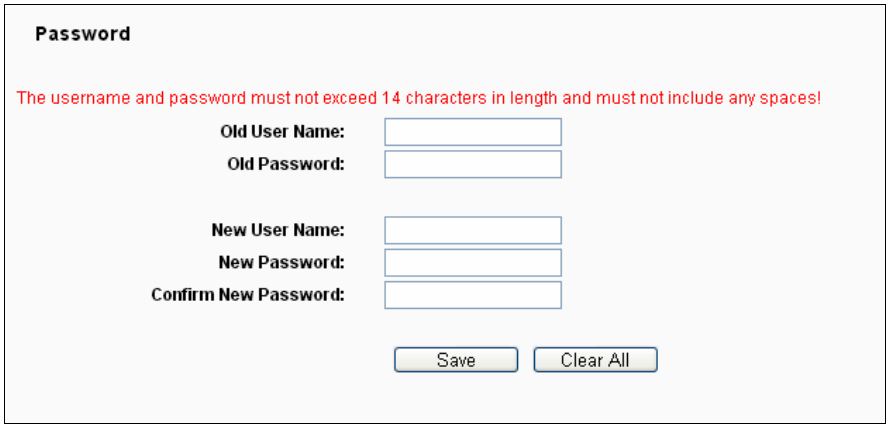


Figure 4-91 Password

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

☞**Note:**

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

Click the **Save** button when finished.

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

4.18.8 System log

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

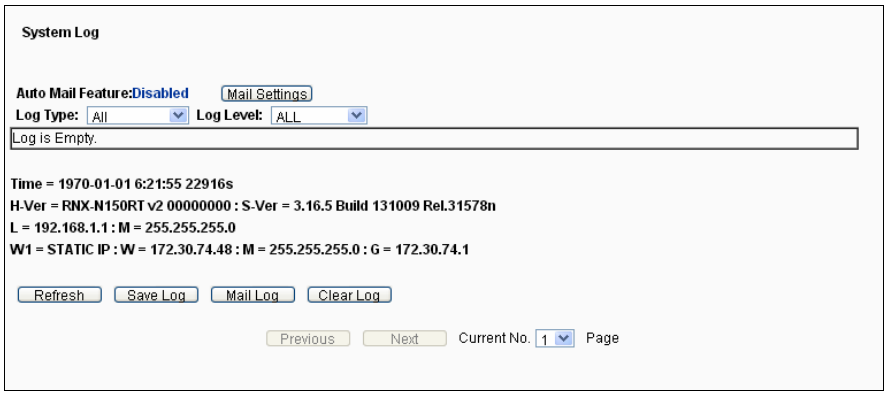


Figure 4-92 System Log

- **Auto Mail Feature -** Indicates whether auto mail feature is enabled or not.
- **Mail Settings -** Set the receiving and sending mailbox address, server address, validation information as well as the timetable for Auto Mail Feature, as shown in Figure 4-93.

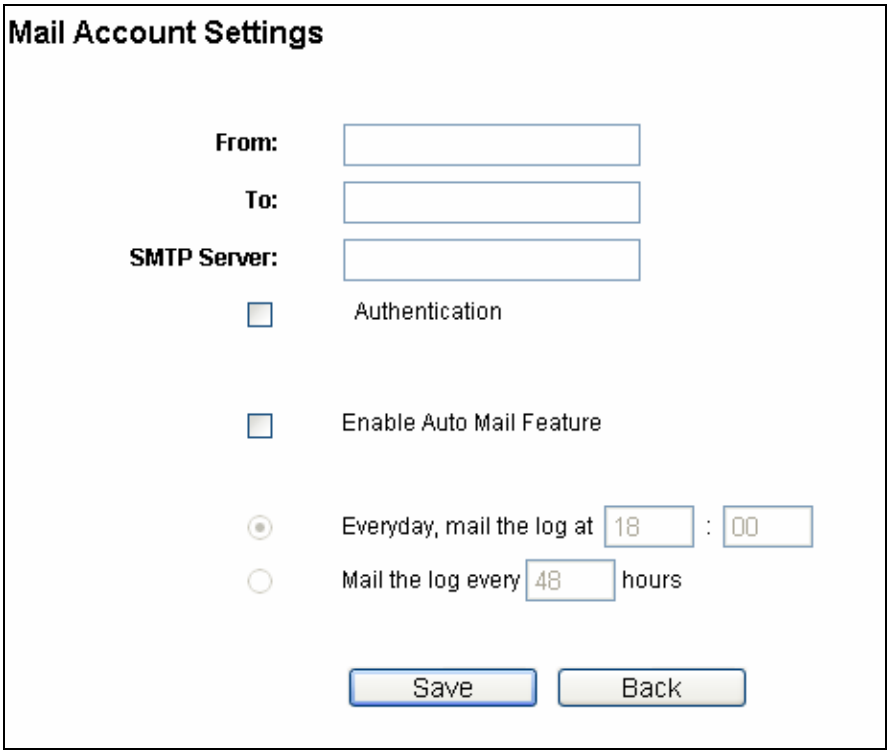


Figure 4-93 Mail Account Settings

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

☞**Note:**

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

- **User Name -** Your mail account name filled in the From field. The part behind @ is excluded.
- **Password -** Your mail account password.
- **Confirm The Password -** Enter the password again to confirm.
- **Enable Auto Mail Feature -** Select it to mail logs automatically. You could mail the current logs either at a specified time everyday or by intervals, but only one could be the current effective rule. Enter the desired time or intervals in the corresponding field as shown in Figure 4-93.

Click **Save** to keep your settings.

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

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

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

4.18.9 Statistics

Choose menu "**System Tools→Statistics**", you can view the network traffic of each PC on the LAN, including total traffic and the value of the last **Packets Statistic interval** in seconds.

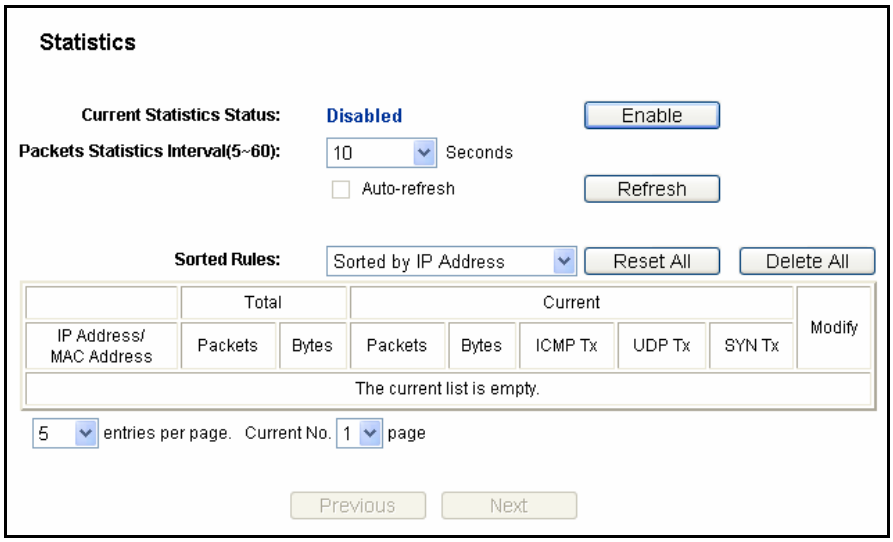


Figure 4-94 Statistics

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

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

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

- **Sorted Rules -**Choose how displayed statistics are sorted.

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

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

Statistics Table:

IP Address/ MAC Address		The IP Address and MAC address are displayed with related statistics
Total	**Packets**	The total number of packets received and transmitted by the 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 ICMP packets transmitted to the WAN per second at the specified **Packets Statistics interval**. It is shown like "current transmitting rate / Max transmitting rate".
	UDP Tx	The number of UDP packets transmitted to the WAN per second at the

		specified **Packets Statistics interval**. It is shown like "current transmitting rate / Max transmitting rate".
	TCP SYN Tx	The number of TCP SYN packets transmitted to the WAN per second at the specified **Packets Statistics interval**. It is shown like "current transmitting rate / Max transmitting rate".

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

Appendix A: FAQ

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

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

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

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

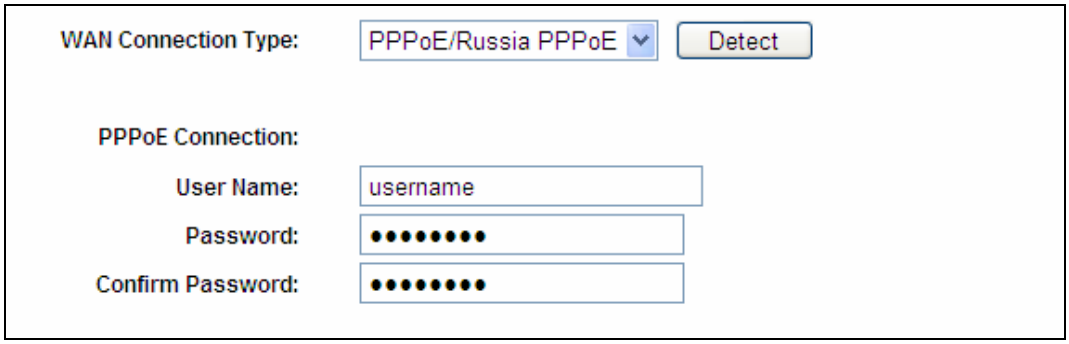


Figure A-1 PPPoE Connection Type

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

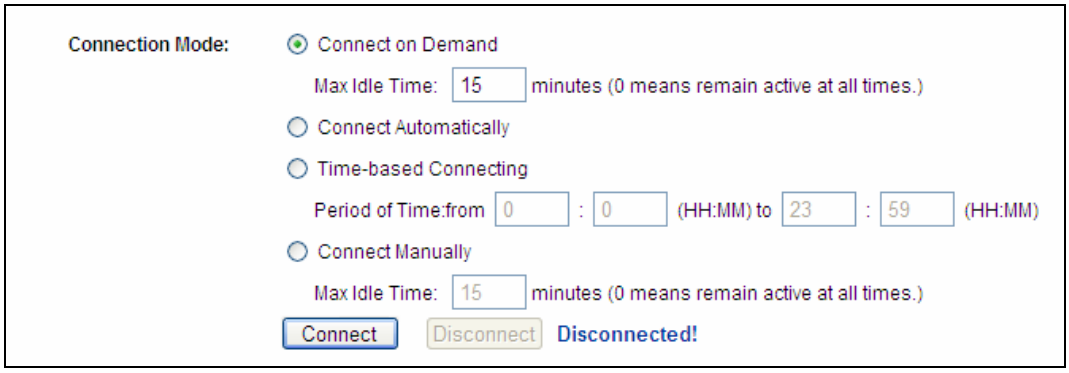


Figure A-2 PPPoE Connection Mode

Note:

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

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

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

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

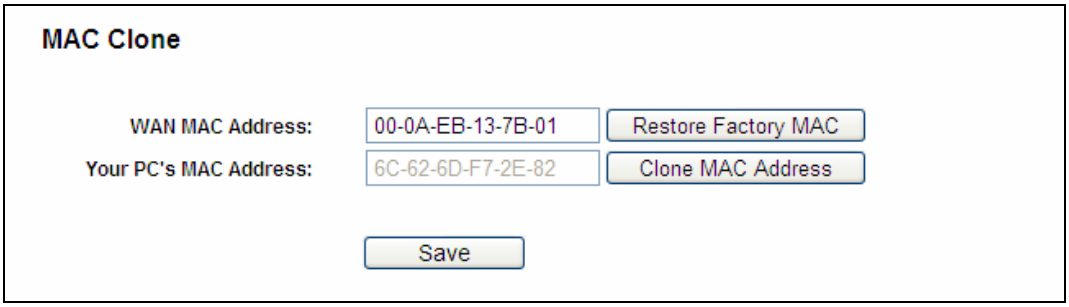


Figure A-3 MAC Clone

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

1) If you start NetMeeting as a sponsor, you don't need to do anything with the router.

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

3) How to configure Virtual Server: Log in to the router, click the "**Forwarding**" menu on the left of your browser, and click "**Virtual Servers**" submenu. On the "**Virtual Servers**" page, click **Add New…**. Then on the "**Add or Modify a Virtual Server Entry**" page, enter "1720" for the "Service Port" blank, and your IP address for the "IP Address" blank, taking 192.168.1.175 for an example, remember to **Enable** and **Save**.

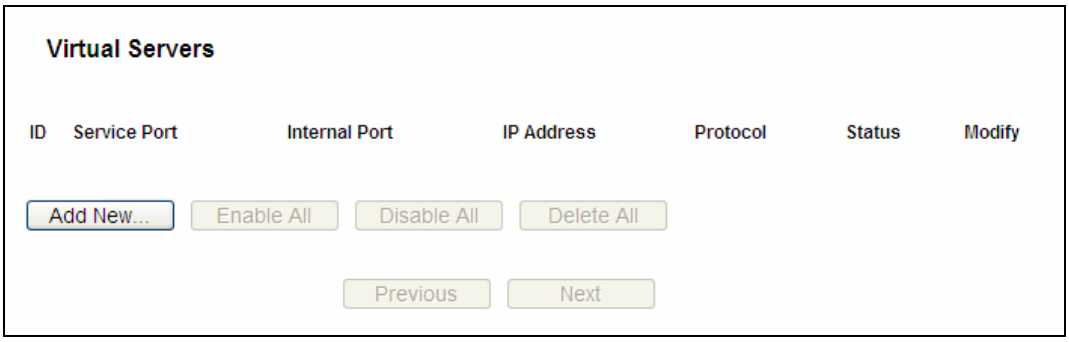


Figure A-4 Virtual Servers

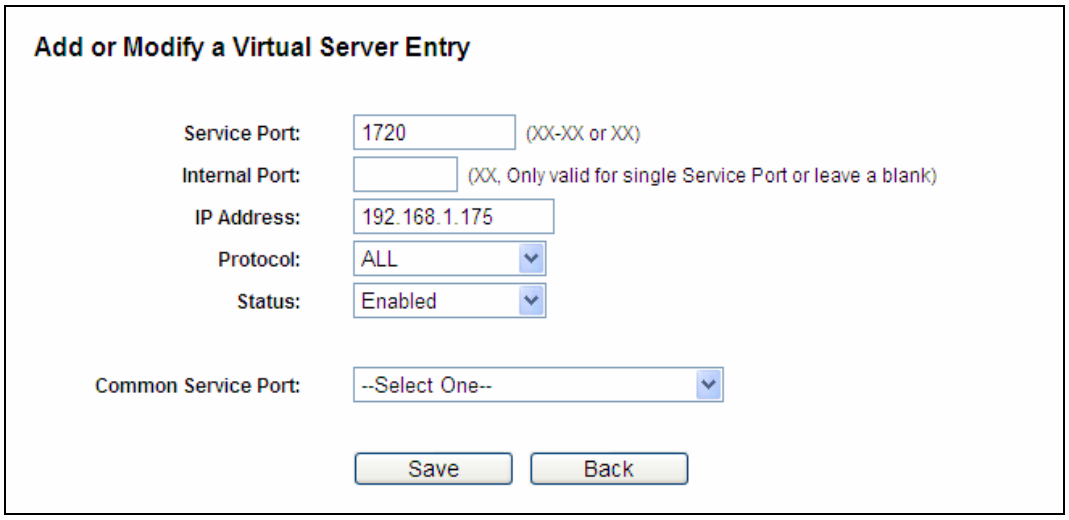


Figure A-5 Add or Modify a Virtual server Entry

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.

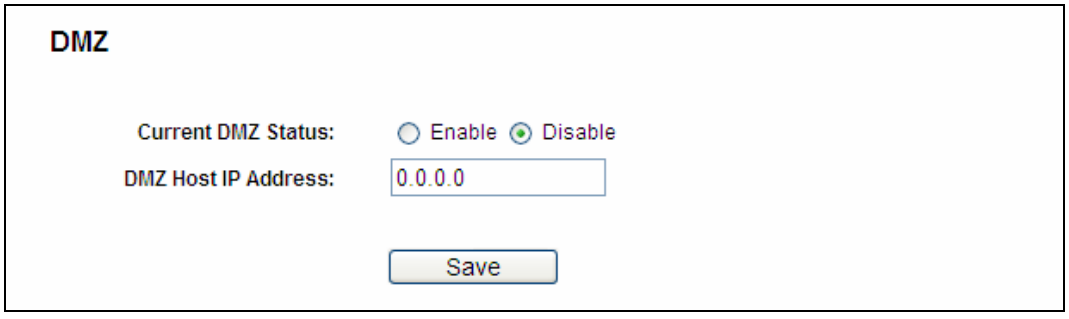


Figure A-6 DMZ

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.

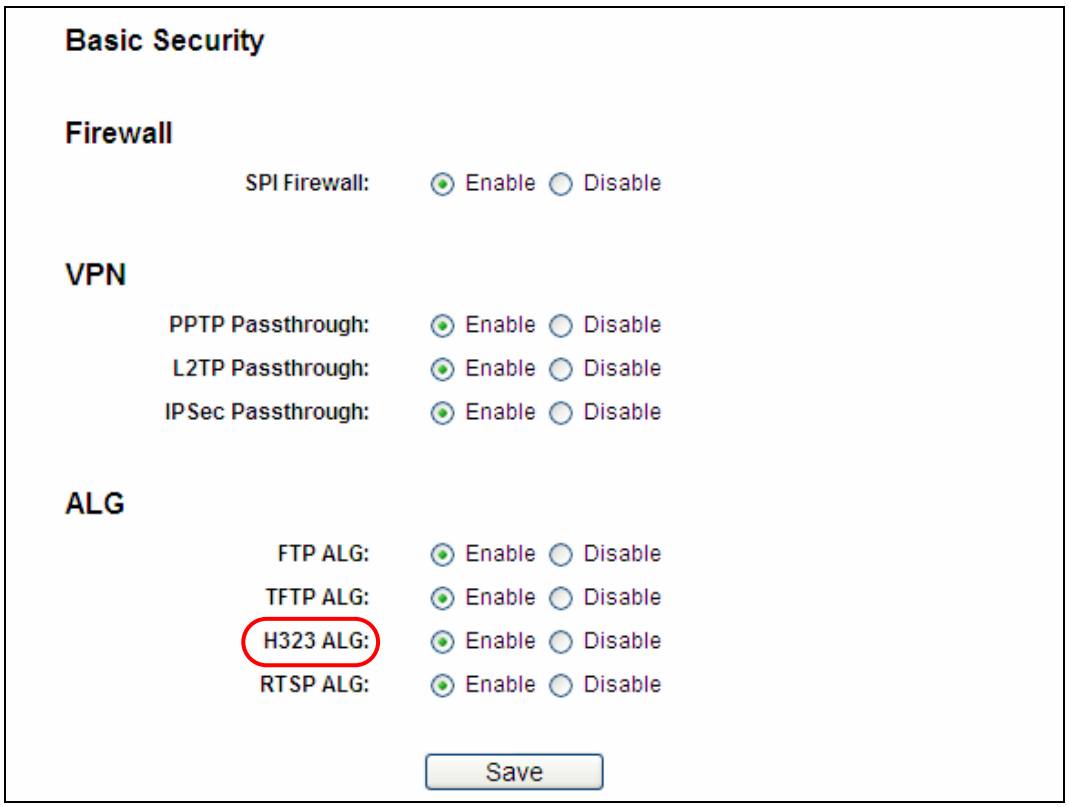


Figure A-7 Basic Security

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

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

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

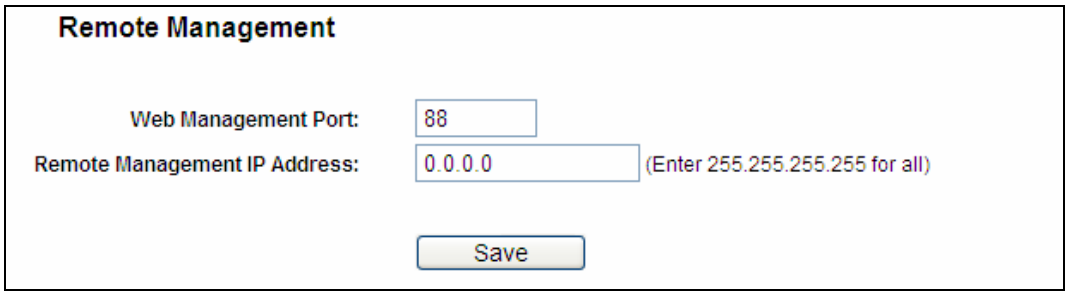


Figure A-8 Remote Management

☞ **Note:**

If the above configuration takes effect, configure to the router by typing 192.168.1.188 (the router's LAN IP address: Web Management Port) in the address field of the Web browser.

3) Log in to the router, click the "**Forwarding**" menu on the left of your browser, and click the "**Virtual Servers**" submenu. On the "**Virtual Servers**" page, click **Add New…**, then on the "**Add or Modify a Virtual Server**" page, enter "80" into the blank next to the "**Service Port**", and your IP address next to the "**IP Address**", assuming 192.168.1.188 for an example, remember to **Enable** and **Save**.

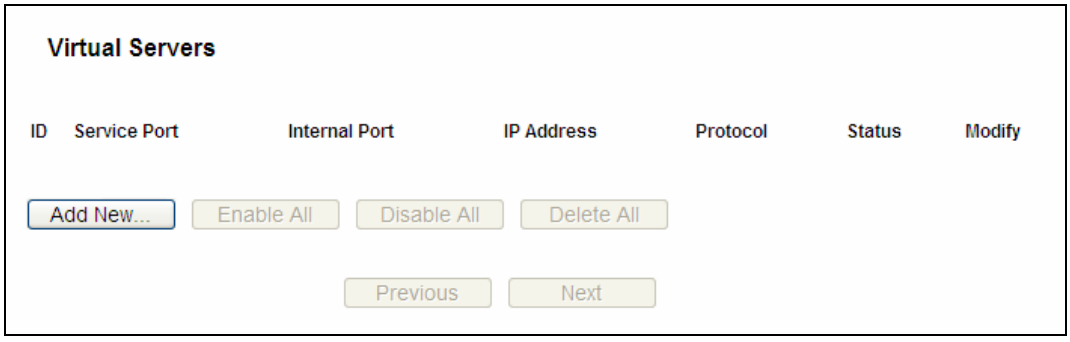


Figure A-9 Virtual Servers

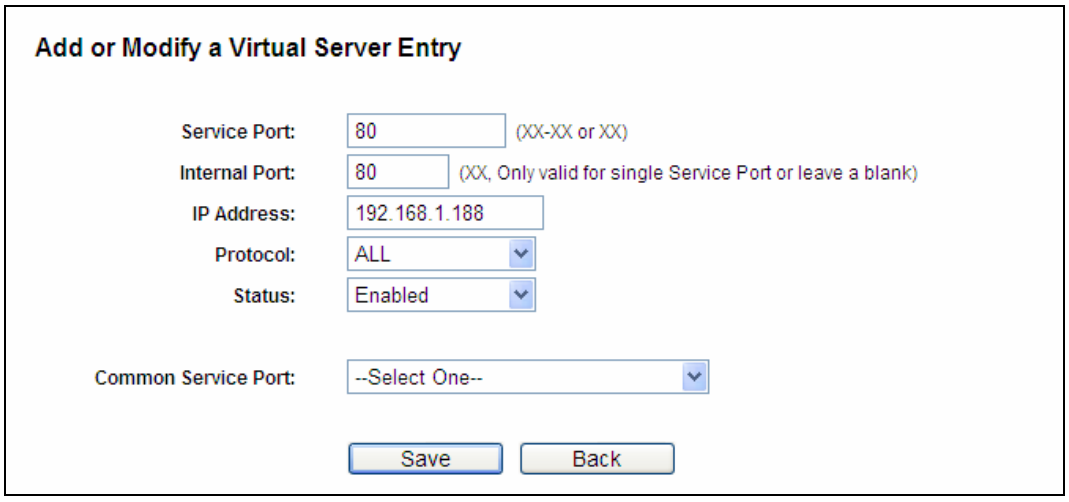


Figure A-10 Add or Modify a Virtual server Entry

5. The wireless stations cannot connect to the router.

1) Make sure the "**Enable Wireless Router Radio**" is checked.

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

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

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

Appendix B: Configuring the PC

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

1. Configure TCP/IP component

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

2) Click the **Network and Internet Connections** icon, and then click on the **Network Connections** tab in the appearing window.

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

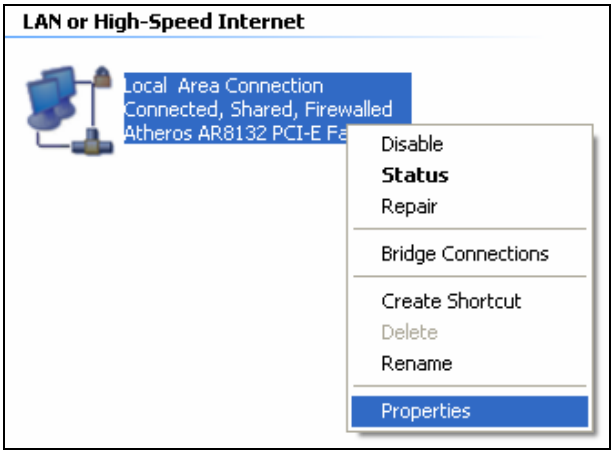


Figure B-1

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

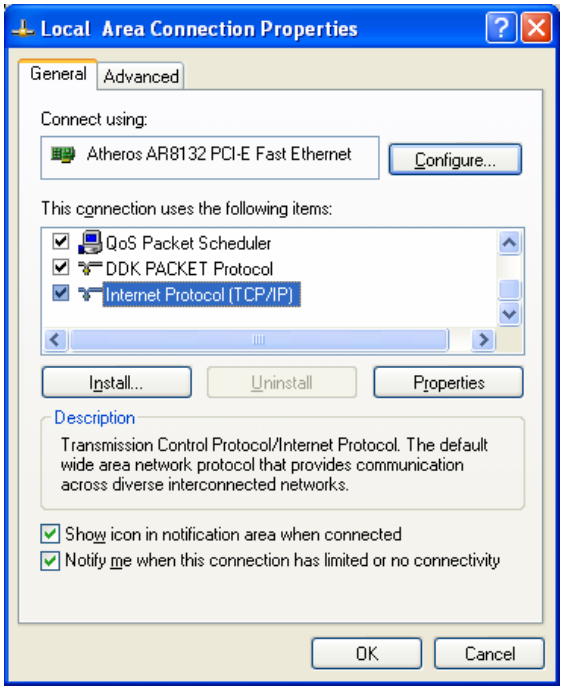


Figure B-2

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

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

➢ **Setting IP address automatically**

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

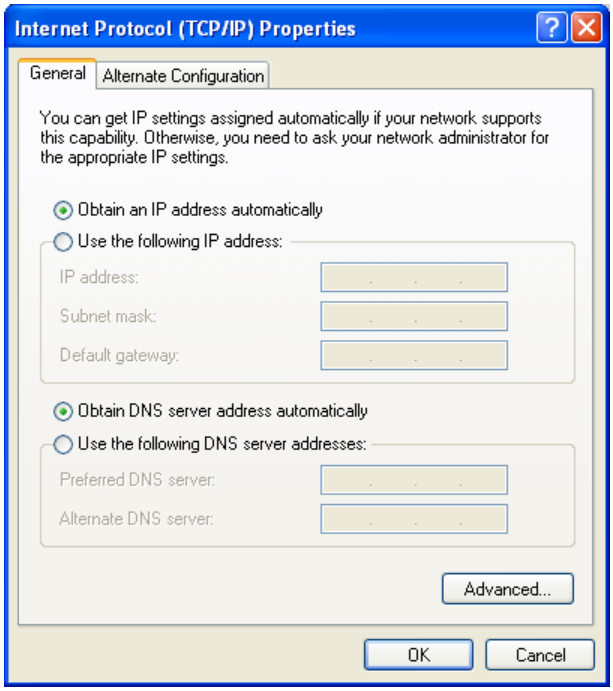


Figure B-3

☞ **Note:**

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

➢ **Setting IP address manually**

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

3 If the router's LAN IP address is 192.168.1.1, specify the **IP address** as 192.168.1.x (x is from 2 to 254), and the **Subnet mask** as 255.255.255.0.

4 Type the router's LAN IP address (the default IP is 192.168.1.1) into the **Default gateway** field.

5 Select **Use the following DNS server addresses**. In the **Preferred DNS Server** field you can enter the same value as the **Default gateway** or type the local DNS server IP address.

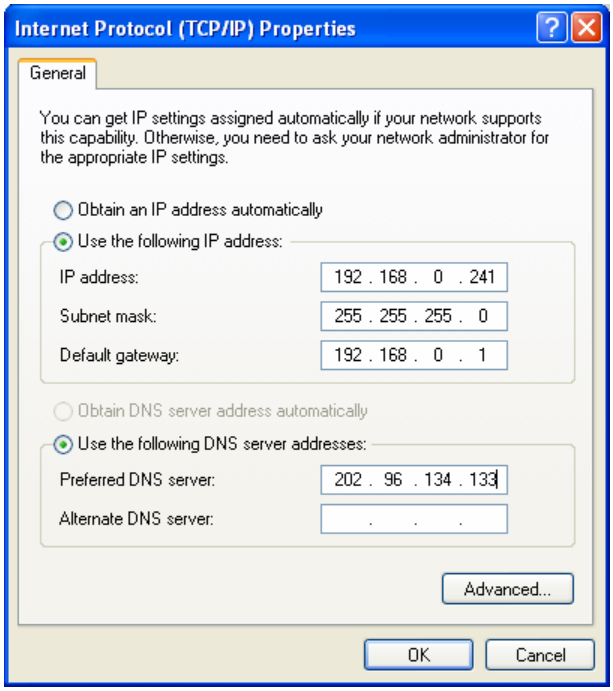


Figure B-4

Now:

Click **OK** to keep your settings.

Appendix C: Specifications

General	
Standards	IEEE 802.3, 802.3u, 802.3x, 802.1x, 802.11n, 802.11b, 802.11g, 802.11e, 802.11i
Protocols	TCP/IP, PPPoE, DHCP, ICMP, NAT, SNTP
Ports	One 10/100M Auto-Negotiation INTERNET RJ45 port; Four 10/100M Auto-Negotiation LAN RJ45 ports supporting Auto MDI/MDIX
Cabling Type	10BASE-T: UTP category 3, 4, 5 cable (maximum 100m) EIA/TIA-568 100Ω STP (maximum 100m)
	100BASE-TX: UTP category 5, 5e cable (maximum 100m) EIA/TIA-568 100Ω STP (maximum 100m)
LEDs	PWR, SYS, WLAN, LAN 1-4, WAN, WPS
Safety & Emissions	FCC, CE
Wireless	
Frequency Band	2.4~2.4835GHz
Radio Data Rate	11n：up to 150Mbps（Automatic） 11g：54/48/36/24/18/12/9/6M（Automatic） 11b：11/5.5/2/1M（Automatic）
Frequency Expansion	DSSS(Direct Sequence Spread Spectrum)
Modulation	DBPSK, DQPSK, CCK, OFDM, 16-QAM, 64-QAM
Security	WEP/WPA/WPA2/WPA2-PSK/WPA-PSK
Sensitivity @PER	130M: -68dBm@10% PER 108M: -68dBm@10% PER; 54M: -68dBm@10% PER 11M: -85dBm@8% PER; 6M: -88dBm@10% PER 1M: -90dBm@8% PER
Antenna Gain	5dBi
Environmental and Physical	
Temperature.	Operating : 0℃~40℃ (32℉~104℉)
	Storage: -40℃~70℃(-40℉~158℉)
Humidity	Operating: 10% - 90% RH, Non-condensing
	Storage: 5% - 95% RH, Non-condensing

Appendix D: Glossary

- **802.11n -** 802.11n builds upon previous 802.11 standards by adding MIMO (multiple-input multiple-output). MIMO uses multiple transmitter and receiver antennas to allow for increased data throughput via spatial multiplexing and increased range by exploiting the spatial diversity, perhaps through coding schemes like Alamouti coding. The Enhanced Wireless Consortium (EWC) [3] was formed to help accelerate the IEEE 802.11n development process and promote a technology specification for interoperability of next-generation wireless local area networking (WLAN) products.
- **802.11b -** The 802.11b standard specifies a wireless networking at 11 Mbps using direct-sequence spread-spectrum (DSSS) technology and operating in the unlicensed radio spectrum at 2.4GHz, and WEP encryption for security. 802.11b networks are also referred to as Wi-Fi networks.
- **802.11g -** specification for wireless networking at 54 Mbps using direct-sequence spread-spectrum (DSSS) technology, using OFDM modulation and operating in the unlicensed radio spectrum at 2.4GHz, and backward compatibility with IEEE 802.11b devices, and WEP encryption for security.
- **DDNS** (**D**ynamic **D**omain **N**ame **S**ystem) **-** The capability of assigning a fixed host and domain name to a dynamic Internet IP Address.
- **DHCP** (**D**ynamic **H**ost **C**onfiguration **P**rotocol) **-** A protocol that automatically configure the TCP/IP parameters for the all the PC(s) that are connected to a DHCP server.
- **DMZ** (**Dem**ilitarized **Z**one) **-** A Demilitarized Zone allows one local host to be exposed to the Internet for a special-purpose service such as Internet gaming or videoconferencing.
- **DNS** (**D**omain **N**ame **S**ystem) **–** An Internet Service that translates the names of websites into IP addresses.
- **Domain Name -** A descriptive name for an address or group of addresses on the Internet.
- **DSL** (**D**igital **S**ubscriber **L**ine) **-** A technology that allows data to be sent or received over existing traditional phone lines.
- **ISP** (**I**nternet **S**ervice **P**rovider) **-** A company that provides access to the Internet.
- **MTU** (**Maximum Transmission Unit**) **-** The size in bytes of the largest packet that can be transmitted.
- **NAT** (**N**etwork **A**ddress **T**ranslation) **-** NAT technology translates IP addresses of a local area network to a different IP address for the Internet.

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

Thank you for purchasing a quality Rosewill Product.

Please register your product at: www.rosewill.com for complete warranty information and future support for your product.

Rosewill Customer Service Hotline: 1-800-575-9885

Rosewill Customer Service Support: techsupport@rosewill.com