UTT™

AC750W Wireless Router

Advanced Configuration Guide

V1.0

UTT Technologies Co., Ltd.
http://www.uttglobal.com

Copyright Notice

Product Number (PN): 0904-0003-008

Document Number (DN): PR-PMMU-1150.50-PPR-EN-1.0A

Table of Contents

About This Manual

0.1 Scope

This guide mainly describes how to install and configure the AC750W Wireless Router offered by UTT Technologies Co., Ltd. For more information, please visit our website at www.uttglobal.com.

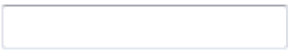
0.2 Web UI Style

The Web UI style complies with the browser standard, which is as follows:

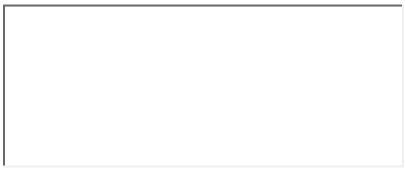
Radio Button: It allows you to choose only one of a predefined set of options.

Check Box: It allows you to choose one or more options.

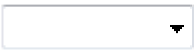
Button: It allows you to click to perform an action.



Text Box: It allows you to enter text information.



List Box: It allows you to select one or more items from a list contained within a static, multiple line text box.



Drop-down List: It allows you to choose one item from a list. When a drop-down list is inactive, it displays a single item. When activated, it drops down a list of items, from which you may select one.

0.3 Documents Conventions

0.3.1 Symbol Conventions

◆: It represents a configuration parameter. Parameters may be optional or required. Required parameters are indicated by a red asterisk (*).

▶: It represents a button.

✓: It represents one or more notes.

0.3.2 Other Conventions

0.3.2.1 Convention for a Page Path

First Level Menu Item > Second Level Menu Item (bold font) means the menu path to open a page. For example, **Wireless > MAC Filtering** means that in the Web UI, click the first level menu item **Wireless** firstly, and then click the second level menu item **MAC Filtering** to open the corresponding page.

0.3.2.2 Convention for Clicking a Button

Click the **XXX** button (**XXX** is the name of the button, bold font) means performing the corresponding operation. E.g., click the **Delete** button means performing the delete operation, the **Delete** button is shown as Delete.

0.3.3 Common Button Descriptions

The following table describes the commonly-used buttons in the Web UI.

Button	Description
Save	Click to save your changes.

Cancel	Click to revert to the last saved settings.
Delete	Click to delete the selected entry(s).
Refresh	Click to display the latest information on the page.
Clear	Click to clear all the statistics on the page.
Back	Click to go back to the previous page.

Table 0-1 Common Button Descriptions

0.3.4 Detailed Description of List

0.3.4.1 Basic Elements and Features

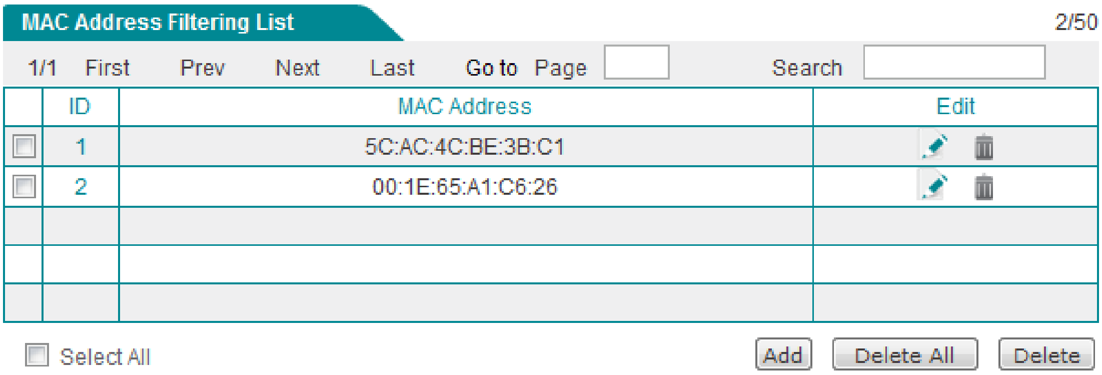
The Web UI contains two kinds of lists: editable list and read-only list.

- An editable list is used to add, display, modify and delete the configuration entries.
- A read-only list is used to display the system status information which is not editable.

Let’s take the editable **MAC Address Filtering List** (see Figure 0-1) as an example to explain the basic elements and features of the list.

Note

Only the editable lists support Add, Modify, and Delete operations. The read-only lists don’t support them.



MAC Address Filtering List 2/50

1/1 First Prev Next Last Go to Page □ Search □

	ID	MAC Address	Edit
□	1	5C:AC:4C:BE:3B:C1	✎ 🗑
□	2	00:1E:65:A1:C6:26	✎ 🗑

□ Select All Add Delete All Delete

Figure 0-1 MAC Address Filtering List

The following table describes the basic elements and features of the list.

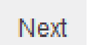
Element	Description
1/1	Current page number/ total pages, the example means that the current page is the first page, and total one page.
First	Click to jump to the first page.
Prev	Click to jump to the previous page.
 Next	Click to jump to the next page.
Last	Click to jump to the last page.
Go to Page	Enter page number in text field, then click **Go to** or press **<Enter>** key to jump to that page.
Search	Enter the text string you want to search for in this text box, then press **<Enter>** key to display all the matched entries. In addition, you can do the search within the displayed results. If you want to display all the entries, you only need clear the text box and then press **<Enter>** key. Note that the matching rule is substring matching, that is, it will search for and display those entries that contain the specified text string.
2/50	Configured number / maximum number, the example means that there are 2 configured MAC address filtering entries, and the maximum number of MAC address filtering allowed is 50.
	Click to go to the setup page to modify the corresponding entry.
	Click to delete the corresponding entry.
☐ Select All	Click (add the check mark) to select all the entries in the current page. Click again (remove the check mark) to unselect all the entries in the current page.
Add	Click to go to the setup page to add a new entry to the list.
Delete All	Click to delete all the entries in the list.
Delete	To delete one or more entries, select the leftmost check boxes of them, and then click the **Delete** button.

Table 0- 2 Basic Elements and Features of the List

0.3.4.2 Sorting Function

All the lists in the Web UI support sorting function. The operation is as follows: You can click any column header to sort the entries in a list by that column. Click once to sort the entries in descending order, click again to sort them in ascending order. Click a third time to sort them in descending order, and so forth. After sorted, the list will be displayed from the first page.

0.4 Factory Default Settings

The following table lists the default values of several important parameters.

Parameter	Default Value	Description
Administrator User Name	admin	You can use the administrator account to login to the Wireless Router's Web UI. **Note:** Both the User Name and Password are case sensitive.
Administrator Password	admin	
LAN IP Address	192.168.1.1	They are the IP address and subnet mask of the Wireless Router's LAN interface. You can use this IP address to access and manage the Wireless Router.
LAN Subnet Mask	255.255.255.0	
SSID	UTT-HIPER_XXXXXX	To connect to the Wireless Router, wireless clients must use the same SSID as the Wireless Router. Therein, "XXXXXX" is the Wireless Router's serial number in hexadecimal format.

Table 0- 3 Factory Default Settings

0.5 Document Organization

This guide mainly describes the settings and applications of the AC750W Wireless Router, which include product overview, hardware installation, quick setup, start menu, network, wireless, advanced, user management, firewall, VPN, system administration, status and support.

Chapter 1 Product Overview

This chapter describes functions and features of the Wireless Router.

Chapter 2 Hardware Installation

This chapter describes how to install the Wireless Router.

Chapter 3 Quick Setup

This chapter describes the following contents:

- How to install and configure TCP/IP properties on your PC.
- How to login to the Wireless Router; and introduction to the WEB UI layout.
- How to use the **Setup Wizard** to quickly configure the basic parameters for the Wireless Router to operate properly.

Chapter 4 Start Menu

This chapter describes how to quickly go to the following pages to configure the related features via the **Start** menu items:

- **Setup Wizard:** How to configure the basic parameters for the Wireless Router to operate properly.
- **System Status:** How to view wired and wireless status of the Wireless Router.
- **Interface Traffic:** How to view the real-time traffic chart for each interface, and the ingress and egress traffic statistics for each interface.
- **Restart:** How to restart the Wireless Router.

Chapter 5 Network

This chapter describes how to configure the basic network parameters of the Wireless Router, including:

- **WAN:** How to configure Internet connections and view their configuration and status.
- **Load Balancing:** How to configure the load balancing feature which includes detection and weight settings, global settings; and how to view the load balancing list.
- **LAN Settings:** How to configure the parameters of the LAN interface, such as IP address, subnet mask, MAC address, and so on.
- **DHCP Server:** How to configure DHCP server, DNS proxy, static DHCP; how to view the static DHCP list and DHCP client list.
- **DDNS:** How to apply for DDNS account and configure DDNS service, and view DDNS status.
- **UPnP:** How to enable or disable UPnP, and view the UPnP port forwarding list.

Chapter 6 Wireless

This chapter describes how to configure the wireless features of the Wireless Router, including:

- **Basic Wireless Settings:** How to configure basic wireless settings.
- **Wireless Security Settings:** How to configure wireless security settings.
- **Wireless MAC Address Filtering:** How to filter the wireless clients based on their MAC addresses.
- **Advanced Wireless Settings:** How to configure advanced wireless settings.
- **Wireless Client List:** How to view the status of the wireless clients, and easily configure MAC address filtering entries via the list.

Chapter 7 Advanced

This chapter describes how to configure the advanced features of the Wireless Router, including:

- **NAT and DMZ:** How to configure and view NAT rules, port forwarding entries and DMZ host.
- **IP/MAC Binding:** How to configure IP/MAC bindings to prevent IP address spoofing. How to configure an Internet whitelist or blacklist for the LAN users.
- **Static Route:** How to configure and view the static routes.
- **PPPoE Server:** How to configure PPPoE server global settings and PPPoE account settings, and view PPPoE user status.

Chapter 8 User Management

This chapter describes how to control and manage the Internet behaviors of the LAN users based on schedule, including:

- **Global Management:** How to allow or block the LAN users from using popular IM (e.g., QQ, MSN) and P2P applications (e.g., Bit Comet, Bit Spirit, Thunder Search) based on schedule.
- **Group Management:** How to allow or block the LAN users from using popular IM and P2P applications based on user group and schedule.

Chapter 9 Firewall

This chapter describes how to configure firewall features, including:

- **Access Control:** How to configure access control rules to assign Internet access privileges to the LAN users based on schedule, and to prevent external attacks.
- **Domain Filtering:** How to configure domain filtering feature to block access to the specified websites.
- **Attack Prevention:** How to configure attack prevention features.

Chapter 10 VPN

This chapter describes the PPTP implementation, and how to configure the Wireless Router as a PPTP client.

Chapter 11 System Administration

This chapter describes how to perform maintenance activities on the Wireless Router, including:

- **Administrator:** How to add, view, modify and delete the administrator accounts.
- **System Time:** How to set the system date and time manually or automatically.
- **Configuration:** How to backup and restore the system configuration, and reset the Wireless Router to factory default settings.
- **Firmware upgrade:** How to backup, download and upgrade firmware.
- **Remote Access:** How to enable HTTP remote management feature to remotely configure and manage the Wireless Router via Internet.
- **Scheduled Task:** How to create and view the scheduled tasks. Now the Wireless Router only supports one scheduled task: Restart.

Chapter 12 Status

This chapter describes how to view the system status information and statistics, including:

- **System Status:** It displays wired and wireless status of the Wireless Router.
- **Traffic Statistics:** It displays wired and wireless data traffic statistics of the Wireless Router.
- **System Information:** It displays the current system time, system up time, system resources usage information, SN, firmware version, and system log messages.

Chapter 13 Support

This chapter describes how to link to the UTTCare, Forum, Knowledge and Reservation page of the UTT website, which can help you quickly learn the UTT Technologies service system and enjoy the most intimate and professional services.

Appendix

This guide provides six appendixes, including:

- **Appendix A How to Configure Your PC:** How to configure TCP/IP settings on a Windows XP-based computer.
- **Appendix B FAQ:** Frequent questions and answers.
- **Appendix C Common IP Protocols:** Provides the list of common IP protocols and their protocol numbers.
- **Appendix D Common Service Ports:** Provides the list of common services and their port numbers.

- **Appendix E Figure Index:** Provides a figure index directory.
- **Appendix F Table Index:** Provides a table index directory.

0.6 Contact Information

If you have any questions regarding the operation or installation of the AC750W Wireless Router, please contact us in any of the following ways.

- **Technical Support Phone:** +86-4006-120-780, +86-4006-880-780
- **UTT Forum**: http://www.uttglobal.com/forum/
- **E-mail**: uttglobal@utt.com.cn

Chapter 1 Product Overview

Thanks for choosing the AC750W Wireless Router from UTT Technologies Co., Ltd.

This chapter describes the functions and features of the AC750W Wireless Router in brief.

1.1 Product Brief

The AC750W Wireless Router is designed for small-sized businesses and branch offices, integrating wired networks with 3G and 802.11 wireless networks. In addition, it adheres to the characteristics of UTT Technologies products: open, easy-to-use, safe, smooth, and so on.

The AC750W is based on IEEE 802.11n standard and is compatible with IEEE 802.11b and IEEE 802.11g standards. It provides maximum wireless transfer rate up to 300Mbps, wide wireless coverage, and stable wireless data transmission.

The AC750W supports multiple security modes which include WEP, WPA-Enterprise, WPA2-Enterprise, WPA-PSK and WPA2-PSK. What's more, it provides simple and efficient wireless MAC address filtering to improve the security of your wireless network.

The AC750W supports DHCP server, NAT, static route, DDNS, IP/MAC binding, PPPoE server and other advanced features. Furthermore, it provides feature-rich user management, which can help you control and manage the Internet behaviors of the LAN users based on schedule and address group, including QQ, MSN and P2P applications (e.g., Bit Comet, Bit Spirit, and Thunder Search) control, the maximum upload and download rate limiting.

The AC750W supports flexible firewall features like access control and domain filtering to effectively prevent network attacks, and provide security for the LAN users.

The AC750W provides a concise, intuitive, and feature-rich Web User Interface. The Setup Wizard can help you quickly configure the basic parameters for the Wireless Router to operate properly. The status information (System Status, Wireless Client List, Traffic Statistics, etc.) can help you identify and diagnose the source of current system problems, or predict potential system problems. In addition, the Support page provides links to the UTT website to help you quickly learn the UTT Technologies service system and enjoy the most intimate and professional services.

1.2 Key Features

- Supports multiple Internet connection types: 3G, PPPoE, Static IP, DHCP and Wi-Fi AP
- Provides two wired WAN interfaces (WAN1 and WAN2), two wireless WAN interfaces (3G and APClient), and three 10M/100M LAN ports
- Supports multiple Internet connections that provide intelligent load balancing and automatic failover
- Supports 6kV lightning protection
- Conforms to IEEE 802.11n (802.11g and 802.11b Compatible).
- Provides maximum wireless transfer rate up to 300Mbps
- Supports multiple wireless security modes which include WEP, WPA-Enterprise, WPA2-Enterprise, WPA-PSK and WPA2-PSK
- Supports hidden SSID
- Supports VPN pass-through (IPSec, PPTP and L2TP)
- Supports PPTP client
- Supports WMM (Wi-Fi Multimedia)
- Supports wireless MAC address filtering feature, whitelist, blacklist, one-click filtering of MAC addresses
- Supports DHCP server
- Supports DNS proxy
- Supports DDNS (Dynamic Domain Name System)
- Supports IP/MAC binding
- Supports feature-rich PPPoE server
- Supports upload and download rate limiting for the LAN users
- Supports Internet behavior management for the LAN users, such as block or allow QQ, MSN and P2P applications (e.g., Bit Comet, Bit Spirit, and Thunder Search)
- Supports flexible and strong firewall features
- Supports IP packet filtering based on IP address, protocol and TCP/UDP port
- Supports URL and keyword filtering
- Supports DNS request filtering
- Supports HTTP remote management
- Provides the Web User Interface (Web UI) for ease of use
- Supports firmware upgrade via the Web UI
- Supports configuration backup and restore

- Provides wireless client list and system status

1.3 Physical Specification

- Conforms to IEEE 802.11n, IEEE 802.11b and IEEE 802.11g standards
- Conforms to IEEE 802.3 Ethernet and IEEE 802.3u Fast Ethernet standards
- Supports TCP/IP, PPPoE, DHCP, ICMP, NAT, Static Route, etc.
- Each physical port supports auto-negotiation for the port speed and duplex mode
- Each physical port supports auto MDI/MDI-X
- Provides system and port LEDs
- Operating Environment:

  Temperature: 32° to 104° F (0° to 40° C)

  Relative Humidity: 10% to 90%, Non-condensing

  Height: 0m to 4000m

Chapter 2 Hardware Installation

2.1 Physical Characteristics

2.1.1 Front Panel

As shown in Figure 2-1, the LEDs are located on the front panel of the Wireless Router. The LEDs indicate the status of the system and each port. Table 2-1 describes these LEDs.

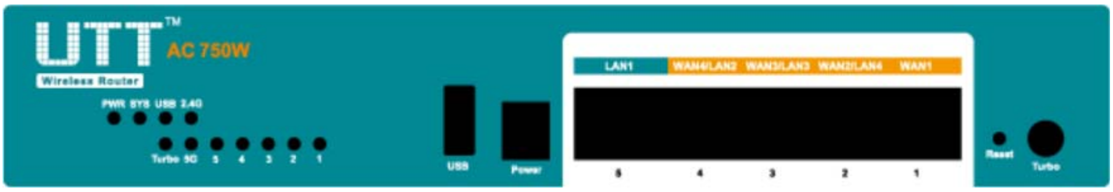


Figure 2-1 Front Panel of the Wireless Router

LED	Full Name	State	Description
PWR	Power LED	On	The Wireless Router is powered on.
		Off	The Wireless Router is powered off.
SYS	System LED	Blinking	The system is operating properly.
		On	The system is not operating properly.
		Off	The system is not operating properly.
USB	3G USB Modem Status LED	On	A 3G USB modem is connected to the USB port.
		Off	No 3G USB modem is connected.
WLAN	Wireless LAN Status LED	On	The wireless function is enabled.
		Blinking	The Wireless Router is sending or receiving data over the wireless network.

		Off	The wireless function is disabled.
WAN1/ WAN2	WAN1/WAN2 Port Status LED	On	A valid link is established on the corresponding port.
		Blinking	The corresponding port is sending or receiving data.
		Off	No link is established on the corresponding port.
1, 2, 3	LAN Port Status LED	On	A valid link is established on the corresponding port.
		Blinking	The corresponding port is sending or receiving data.
		Off	No link is established on the corresponding port.
Note: The Wireless Router doesn’t support WPS feature at present.			

Table 2-1 Description of LEDs on the Front Panel

2.1.2 Rear Panel

As shown in Figure 2-2, the rear panel of the Wireless Router contains a POWER connector, a RESET button, a USB port, two wired WAN ports (WAN1 and WAN2), three LAN ports, a WPS button, and two Antenna ports. Note that the Wireless Router doesn’t support WPS feature at present.

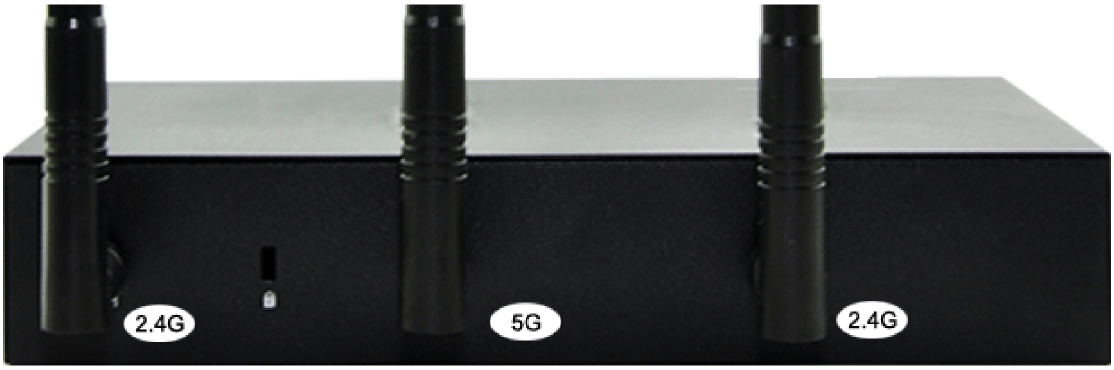


Figure 2-2 Back Panel of the Wireless Router

1. RESET Button

If you forget the administrator password, you need to use the RESET button to reset the Wireless Router to factory default settings. The operation is as follows: While the Wireless Router is powered on, use a pin or paper clip to press and hold the RESET button for more than 5 seconds, and then release the button. After that, the Wireless Router will restart with factory default settings.

✓ **Note**

This operation will clear all the custom settings on the Wireless Router. If you remember the administrator account, it is strongly recommended that you go to **Administration > Configuration** page to backup the current configuration firstly, and then reset the Wireless Router to factory default settings.

2. Ports

The Wireless Router provides three LAN ports, two WAN ports, and a USB port. Table 2-2 describes these ports.

Port	Description
LAN (1, 2, 3)	They are used to connect the wired computers, hubs, switches, and other Ethernet network devices on the LAN to the Wireless Router.
WAN1/WAN2	They are used to connect the Wireless Router to the Internet.
USB	The Wireless Router provides a USB port for connecting a 3G USB Modem, which is used to connect the Wireless Router to the Internet.

Table 2-2 Description of Ports on the Rear Panel

3. Components

Component	Number	Description
Antenna	2	They are used to receive and transmit wireless signals.
Power	1	It is used to connect the power adapter.

Table 2-3 Description of Components on the Rear Panel

2.2 Installation Procedure

1. Selecting a Proper Location

Please make sure that the Wireless Router is powered off before installing it. Then you need to select a proper location to install the Wireless Router. In most cases, you can install it on a level surface such as a desktop or shelf.

✓ **Note**

Please ensure that the desktop or shelf is stable and the power outlet is grounded properly, and do not place heavy objects on the Wireless Router.

2. Attach the Antennas

When shipped, the two antennas are not connected to the Wireless Router. To attach the antennas to the Wireless Router, follow these steps:

1) Remove one antenna from the box.
2) Locate one antenna port (threaded knob) on the back panel of the Wireless Router, see Figure 2- 2.
3) Screw the antenna in a clockwise direction to the threaded knob until firmly seated. Don’t over-tighten.
4) Repeat the above steps to attach the other antenna.

✓ **Note**

Please make sure that you have attached the two antennas to the Wireless Router properly. The antennas will greatly enhance wireless communication capacity of the Wireless Router.

3. Connecting the Wireless Router to the LAN

Connect a standard network cable from a PC or switch to a LAN port of the Wireless Router, or connect a PC to the Wireless Router wirelessly. The Wireless Router will automatically adapt to any network device operating at 10Mbps or 100Mbps.

4. Connecting the Wireless Router to the Internet

Connect the network cable provided by the manufacturer from the DSL, cable or fiber optic modem to a WAN port of the Wireless Router, or insert your 3G USB modem to the USB port of the Wireless Router.

5. Powering On the Wireless Router

Connect the supplied power cord to the power connector on the rear panel of the Wireless Router, and then plug the other end of the power cord to a grounded power outlet. The Wireless Router will start automatically.

✓ **Note**

To prevent the Wireless Router from working abnormally or being damaged, please make sure that the power supply and connectivity are normal, and the power outlet is grounded properly before powering on the Wireless Router.

6. Checking the LEDs

Verify that the Wireless Router starts up properly and the network connections are operational by checking the LED states, as described in Table 2- 1.

Chapter 3 Quick Setup

This chapter describes how to properly configure TCP/IP settings on your computer, how to login to the Wireless Router, and how to configure the basic parameters to quickly connect the Wireless Router to the Internet via the **Start > Setup Wizard**. In addition, it also briefly describes the layout and style of the Wireless Router's Web UI.

3.1 Configuring Your Computer

Before configuring the Wireless Router via the Web UI, you should properly configure TCP/IP settings on the computer that you use to administer the Wireless Router. To do this, follow these steps:

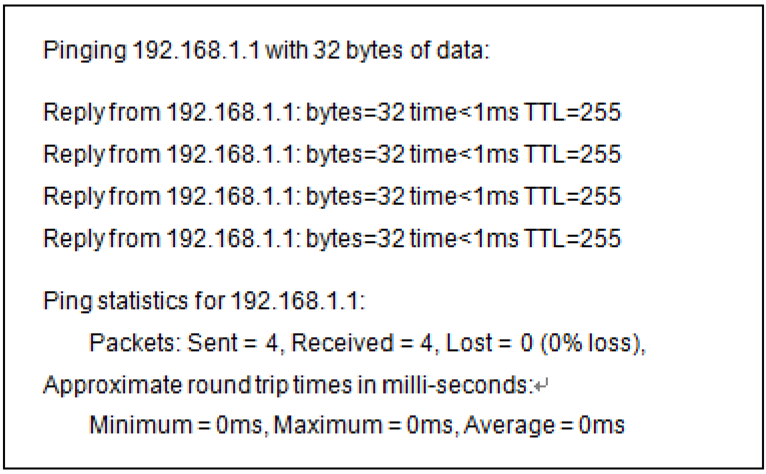
Step 1 Connect the computer to a LAN port of the Wireless Router.

Step 2 Install TCP/IP protocol on your computer. If it has been installed, please ignore it.

Step 3 Configure TCP/IP settings on your computer: set the computer's IP address to an IP address in the range of 192.168.1.2 through 192.168.1.254, set its subnet mask to 255.255.255.0, set its default gateway to 192.168.16.1 (the Wireless Router's default LAN IP address is 192.168.1.1 with a subnet mask of 255.255.255.0), and set its DNS server to an available IP address provided by your ISP.

Step 4 To verify the network connection between your computer and the Wireless Router, you can use the ping command at the command prompt on the computer: **Ping 192.168.1.1**

- If the displayed page is similar to the screenshot below, the connection between your computer and the Wireless Router has been established.

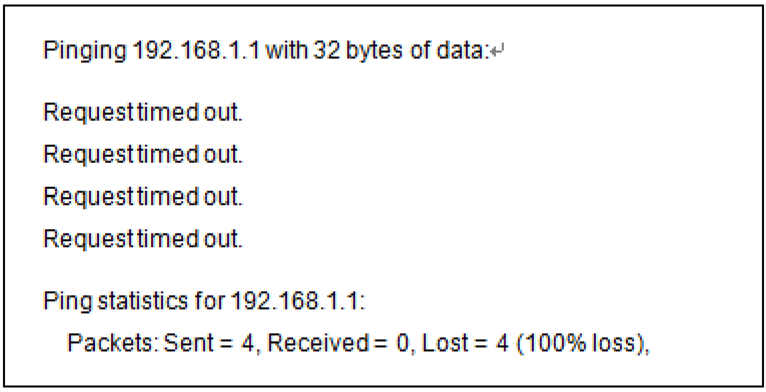


```
Pinging 192.168.1.1 with 32 bytes of data:

Reply from 192.168.1.1: bytes=32 time<1ms TTL=255
Reply from 192.168.1.1: bytes=32 time<1ms TTL=255
Reply from 192.168.1.1: bytes=32 time<1ms TTL=255
Reply from 192.168.1.1: bytes=32 time<1ms TTL=255

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

- If the displayed page is similar to the screenshot below, the connection between your computer and the Wireless Router hasn't been established yet.



```
Pinging 192.168.1.1 with 32 bytes of data:

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

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

If the connection hasn't been established, please take the following steps to resolve the problem:

1. Is the physical link between your computer and the Wireless Router connected properly?

Verify that the LED corresponding to the Wireless Router’s LAN port and the LED on your computer’s adapter are lit.

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

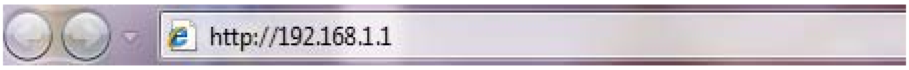
Verify that your computer is on the same subnet as the Wireless Router’s LAN interface. For example, if the Wireless Router’s LAN IP address is 192.168.1.1/24 (default value), your computer’s IP address must be an IP address in the range of 192.168.1.2 through 192.168.1.254, which is not being used by another network device; and its default gateway must be 192.168.1.1.

3.2 Logging in to the Wireless Router

This section describes how to login to the Wireless Router.

No matter what operating system is installed on your computer, such as, MS Windows, Macintosh, UNIX, or Linux, and so on, you can login to and configure the Wireless Router through the Web browser (for example, Internet Explorer).

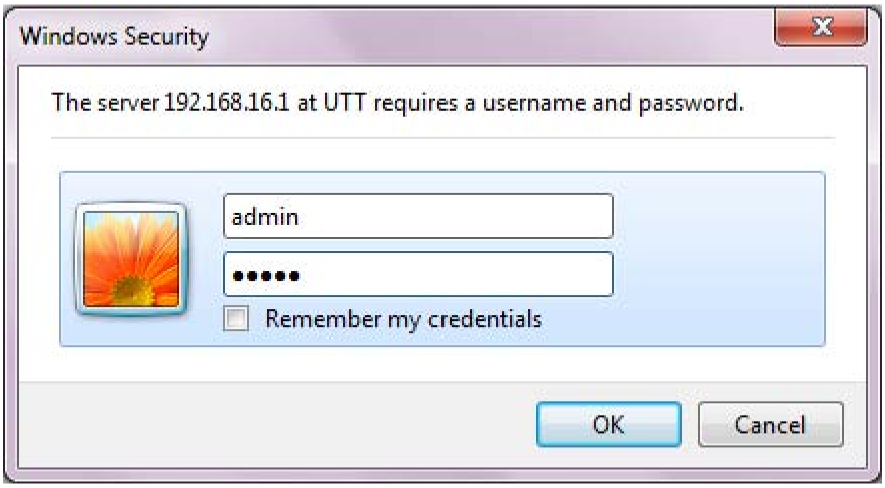
To login to the Wireless Router, do the following: Open a Web browser, enter the Wireless Router's LAN interface IP address (the default is **192.168.1.1**) in the address bar, and then press **<Enter>** key, see Figure 3- 1.



http://192.168.1.1

Figure 3- 1 Entering IP address in the Address Bar

A login screen prompts you for your user name and password, see Figure 3- 2. When you first login to the Wireless Router, please use the default administrator account: Enter **admin** in both the **User name** and **Password** boxes (the default user name and password both are **admin**), lastly click **OK**.



Windows Security

The server 192.168.16.1 at UTT requires a username and password.

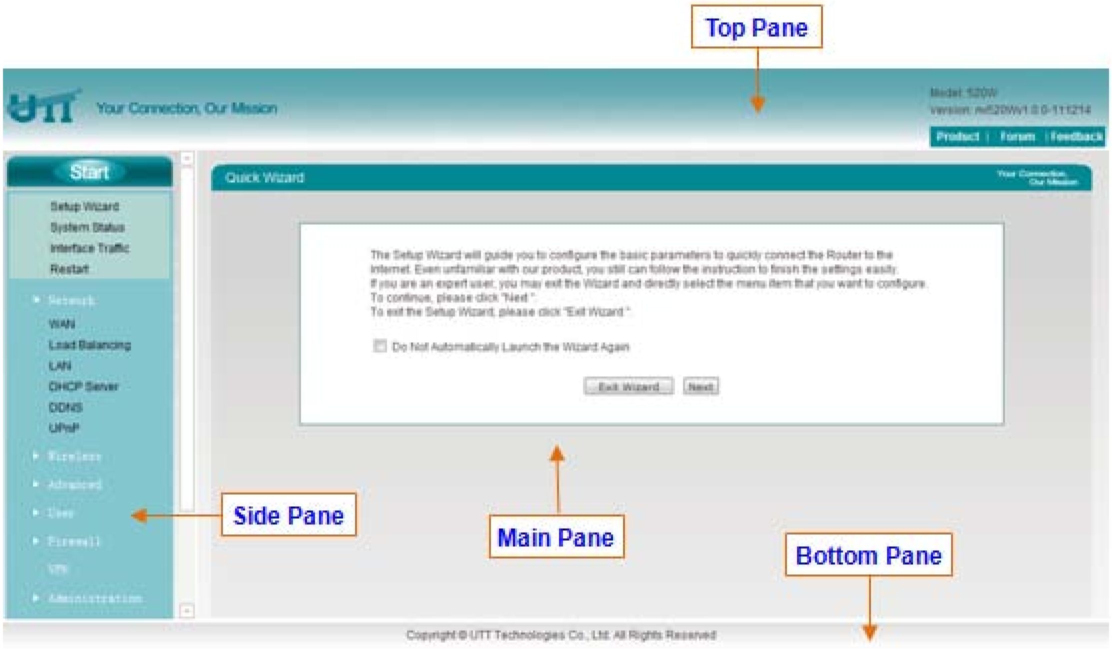
admin

●●●●●

□ Remember my credentials

Figure 3- 2 Login Screen

If your user name and password are correct, it will display the homepage, see Figure 3- 3.



The Setup Wizard will guide you to configure the basic parameters to quickly connect the Router to the Internet. Even unfamiliar with our product, you still can follow the instruction to finish the settings easily.
If you are an expert user, you may exit the Wizard and directly select the menu item that you want to configure.
To continue, please click "Next".
To exit the Setup Wizard, please click "Exit Wizard".

□ Do Not Automatically Launch the Wizard Again

Figure 3- 3 Homepage

Each page of the Wireless Router's Web UI consists of four panes:

1. **Top Pane:** It displays UTT logo, model and version, and three shortcut icons.

   1) **UTT Logo:** Click to link to the homepage of the UTT website.

   2) **Model** and **Version:** The product model and firmware version of the Wireless Router.

   3) **Short Icons:** They are used for fast link to the corresponding pages on the website of UTT Technologies Co., Ltd.

      - **Product:** Click to link to the products page of the UTT website to find more products.
      - **Forum:** Click to link to the forum homepage of the UTT website to participate in product discussions.
      - **Feedback:** Click to link to send us your feedback by E-mail.

2. **Main Pane:** It is the location where you can configure each feature of the Wireless Router, view configuration, status and statistics.

3. **Side Pane:** It displays the two-level main menu bar (i.e., navigation bar). The first level menu is always visible. The second level menu is hidden by default. You can click a first level menu item to reveal its submenu items, click again to hide them.

4. **Bottom Pane:** It displays copyright information.

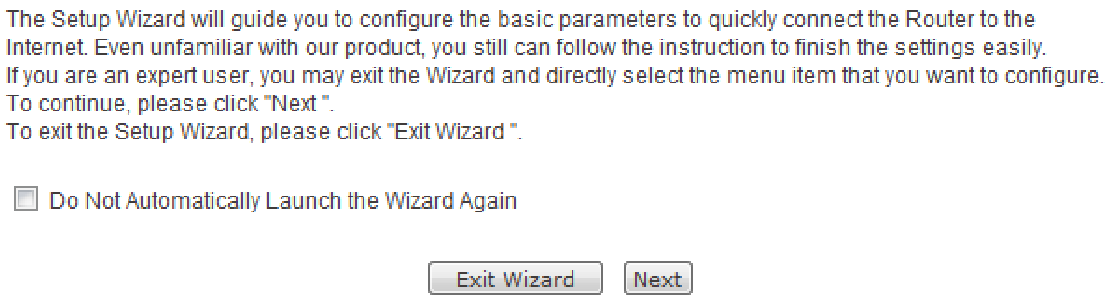
If this is the first time that you login to the Wireless Router, the first page of the **Setup Wizard** appears. In the next section we will describe how to use the **Setup Wizard** to configure the basic parameters for the Wireless Router to operate properly.

3.3 Setup Wizard

This section describes the **Start > Setup Wizard** page.

3.3.1 Running the Setup Wizard

As mentioned earlier, the first page of the **Setup Wizard** appears immediately after your first login, see the following figure.



The Setup Wizard will guide you to configure the basic parameters to quickly connect the Router to the Internet. Even unfamiliar with our product, you still can follow the instruction to finish the settings easily.
If you are an expert user, you may exit the Wizard and directly select the menu item that you want to configure.
To continue, please click "Next ".
To exit the Setup Wizard, please click "Exit Wizard ".

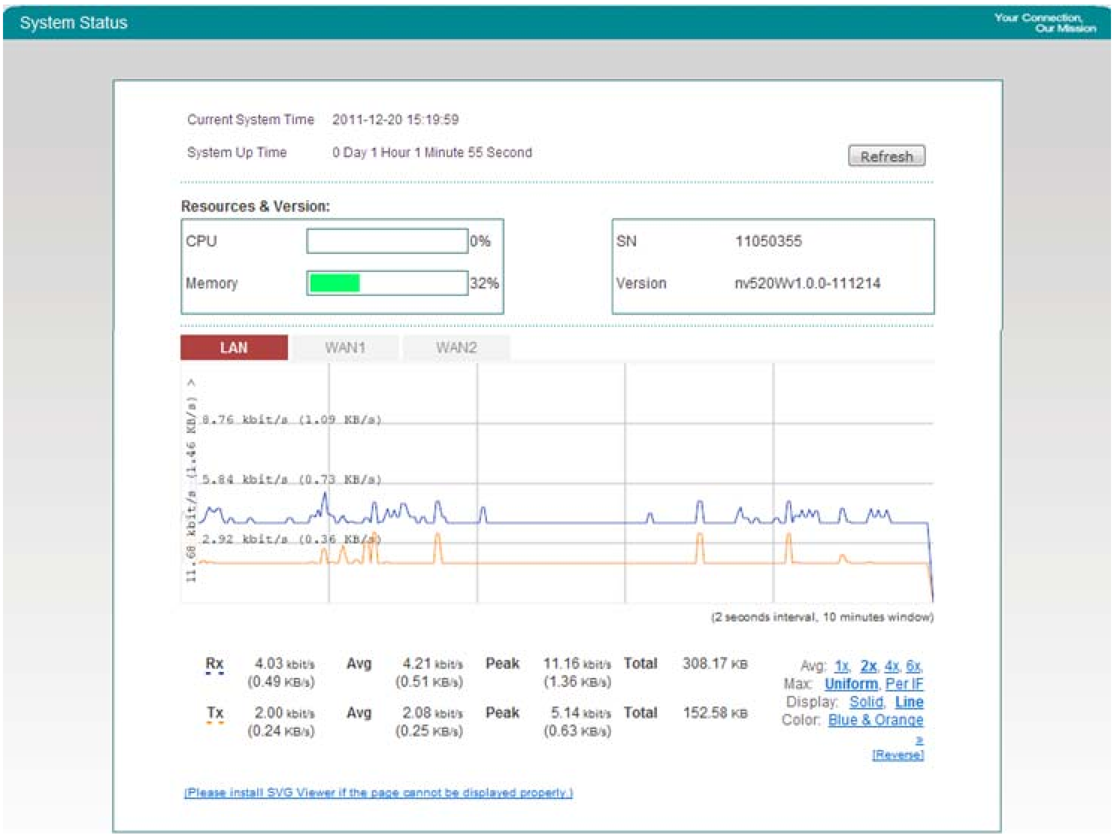
□ Do Not Automatically Launch the Wizard Again

Figure 3- 4 Running the Setup Wizard

- **Do Not Automatically Launch the Wizard Again:** If you select this check box, the system don't automatically launch the **Setup Wizard** the next time you login to the Wireless Router, instead directly open the **Welcome** page shown in Figure 3- 5. Else, the system will still launch the **Setup Wizard** automatically.

- **Exit Wizard:** Click to exit the **Setup Wizard** and go to the **Welcome** page (see Figure 3- 5). The changes made in the **Setup Wizard** will be discarded.

- **Next:** Click to go to the next page of the **Setup Wizard**, that is, the **Setup Wizard - Internet Access Mode** page shown in Figure 3- 6.



Current System Time 2011-12-20 15:19:59

System Up Time 0 Day 1 Hour 1 Minute 55 Second

Resources & Version:

CPU 0%

Memory 32%

SN 11050355

Version nv520Wv1.0.0-111214

(2 seconds interval, 10 minutes window)

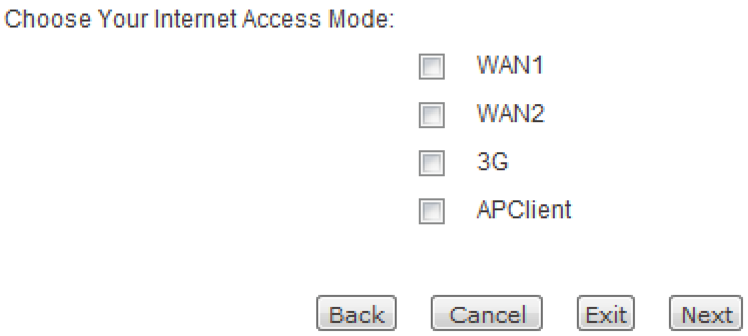
Rx	4.03 kbit/s (0.49 KB/s)	Avg	4.21 kbit/s (0.51 KB/s)	Peak	11.16 kbit/s (1.36 KB/s)	Total	308.17 KB
Tx	2.00 kbit/s (0.24 KB/s)	Avg	2.08 kbit/s (0.25 KB/s)	Peak	5.14 kbit/s (0.63 KB/s)	Total	152.58 KB

[Please install SVG Viewer if the page cannot be displayed properly.]

Figure 3- 5 Welcome Page

3.3.2 Setup Wizard - Internet Access Mode

In this page, you can choose one or more Internet connections that you want to configure via the **Setup Wizard**, see Figure 3- 6.



Choose Your Internet Access Mode:

□ WAN1

□ WAN2

□ 3G

□ APClient

Figure 3- 6 Setup Wizard - Internet Access Mode

- **WAN1:** If you want to configure a wired Internet connection on the WAN1 interface via the **Setup Wizard**, select this check box.
- **WAN2:** If you want to configure a wired Internet connection on the WAN2 interface

via the **Setup Wizard**, select this check box.

- **3G Client:** If you want to configure a 3G Internet connection via the **Setup Wizard**, select this check box. Here the Wireless Router acts as a 3G client.
- **AP Client:** If you want to configure a wireless Internet connection via the **Setup Wizard**, select this check box. Here the Wireless Router acts as an AP client.
- **Back:** Click to go back to the previous page of the **Setup Wizard**.
- **Cancel:** Click to revert to the last saved settings.
- **Exit Wizard:** Click to exit the **Setup Wizard** and go to the **Welcome** page (see Figure 3- 5). The changes made in the **Setup Wizard** will be discarded.
- **Next:** Click to go to the next page of the **Setup Wizard**.

3.3.3 Setup Wizard - Internet Connection Settings

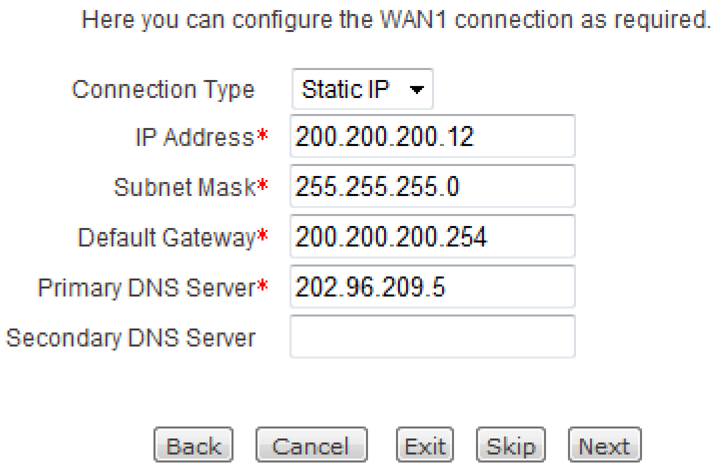
In the **Setup Wizard**, you can configure each Internet connection respectively. For each Internet access mode, the Internet connection settings are different.

3.3.3.1 WAN1/WAN2 Internet Connection Settings

For the WAN1 or WAN2 Internet connection, there are three connection types: PPPoE, Static IP and DHCP.

3.3.3.1.1 Static IP Internet Connection Settings

If you are required to use a static IP address, please select **Static IP** from the **Connection Type** drop-down list. Then the following page will be shown.



Here you can configure the WAN1 connection as required.

Connection Type	Static IP
IP Address*	200.200.200.12
Subnet Mask*	255.255.255.0
Default Gateway*	200.200.200.254
Primary DNS Server*	202.96.209.5
Secondary DNS Server	

Figure 3- 7 Setup Wizard - WAN1/WAN2 Internet Connection Settings (Static IP)

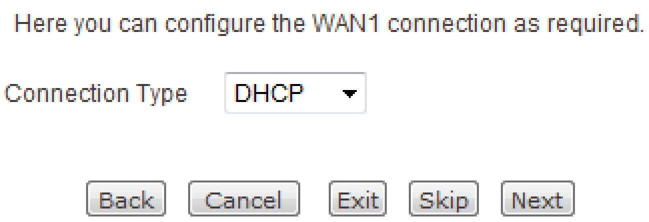
- **Connection Type:** It specifies the type of the Internet connection. Here please select **Static IP**. You need to manually configure IP address, subnet mask, default gateway and DNS server addresses, which are provided by your ISP.
- **IP Address:** It specifies the IP address of the WAN interface, which is provided by your ISP.
- **Subnet Mask:** It specifies the subnet mask of the WAN interface, which is provided by your ISP.
- **Default Gateway:** It specifies the IP address of the default gateway, which is provided by your ISP.
- **Primary DNS Server:** It specifies the IP address of your ISP's primary DNS server.
- **Secondary DNS Server:** It specifies the IP address of your ISP's secondary DNS server. If it is available, you may set it. Else, please leave it blank.
- **Back:** Click to go back to the previous page of the **Setup Wizard**.
- **Cancel:** Click to revert to the last saved settings.
- **Exit:** Click to exit the **Setup Wizard** and go to the **Welcome** page (see Figure 3- 5). The changes made in the **Setup Wizard** will be discarded.
- **Skip:** Click to go directly to the next page of the **Setup Wizard**. The changes made on the current page will be discarded.
- **Next:** Click to go to the next page of the **Setup Wizard**.

✓ **Note**

The WAN IP address and default gateway IP address must be on the same subnet. If not, please modify the **Subnet Mask** to make them be on the same subnet. If you don't have the subnet related knowledge, please ask a professional or UTT customer engineer for help.

3.3.3.1.2 DHCP Internet Connection Settings

If your ISP automatically assigns an IP address to the Wireless Router via DHCP, please select **DHCP** from the **Connection Type** drop-down list. Then the following page will be shown.


Here you can configure the WAN1 connection as required.

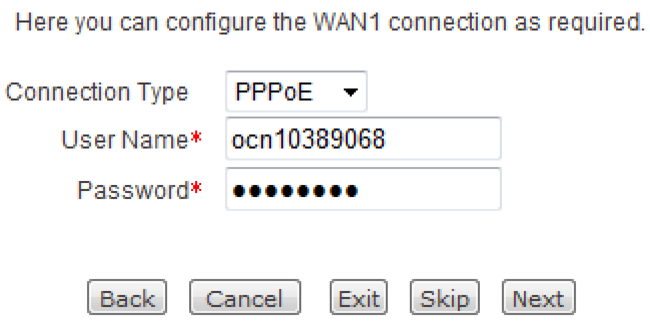
Connection Type DHCP

Figure 3- 8 Setup Wizard - WAN1/WAN2 Settings (DHCP)

- **Connection Type:** It specifies the type of the Internet connection. Here please select **DHCP**. The Wireless Router will automatically obtain the WAN IP address, subnet mask and gateway and DNS server addresses from your ISP's DHCP server.
- **Back:** Click to go back to the previous page of the **Setup Wizard**.
- **Cancel:** Click to revert to the last saved settings.
- **Exit:** Click to exit the **Setup Wizard** and go to the **Welcome** page (see Figure 3- 5). The changes made in the **Setup Wizard** will be discarded.
- **Skip:** Click to go directly to the next page of the **Setup Wizard**. The changes made on the current page will be discarded.
- **Next:** Click to go to the next page of the **Setup Wizard**.

3.3.3.1.3 PPPoE Internet Connection Settings

Please select **PPPoE** from the **Connection Type** drop-down list if your ISP uses PPPoE to establish the Internet connection for you. Then the following page will be shown.


Here you can configure the WAN1 connection as required.

Connection Type PPPoE

User Name* ocn10389068

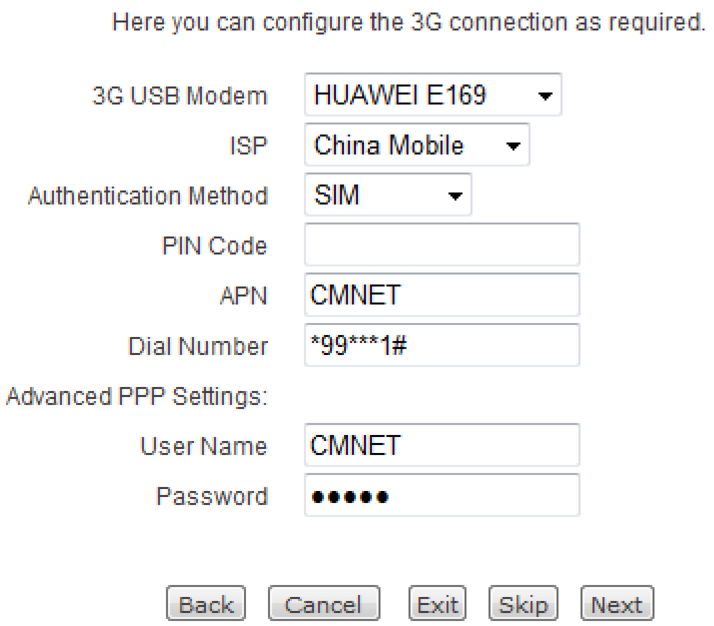
Password* ●●●●●●●●●

Figure 3- 9 Setup Wizard - WAN1/WAN2 Settings (PPPoE)

- **Connection Type:** It specifies the type of the Internet connection. Here please select **PPPoE**. The Wireless Router will automatically obtain the WAN IP address, subnet mask and gateway IP address from your ISP's PPPoE server.
- **User Name** and **Password:** They specify the PPPoE login user name and password provided by your ISP. Please ask your ISP if you have any questions.
- **Back:** Click to go back to the previous page of the **Setup Wizard**.

- **Cancel:** Click to revert to the last saved settings.
- **Exit:** Click to exit the **Setup Wizard** and go to the **Welcome** page (see Figure 3-5). The changes made in the **Setup Wizard** will be discarded.
- **Skip:** Click to go directly to the next page of the **Setup Wizard**. The changes made on the current page will be discarded.
- **Next:** Click to go to the next page of the **Setup Wizard**.

3.3.3.2 3G Internet Connection Settings



Here you can configure the 3G connection as required.

3G USB Modem	HUAWEI E169
ISP	China Mobile
Authentication Method	SIM
PIN Code	
APN	CMNET
Dial Number	*99***1#
Advanced PPP Settings:	
User Name	CMNET
Password	●●●●●

Figure 3-10 Setup Wizard - 3G Internet Connection Settings

- **3G USB Modem:** It specifies the model of the 3G USB modem. Now the Wireless Router supports five models: **HUAWEI E169**, **HUEWEI E1750**, **HUAWEI EC1260**, **HUAWEI ET128**, and **ZTE MF637U**.
- **ISP:** It is short for Internet Service Provider, a company that provides 3G wireless Internet access service for you. Now the Wireless Router supports three ISPs: **China Mobile**, **China Unicom** and **China Telecom**.
- **Authentication Method:** It specifies the authentication method used by your ISP. The options are **SIM** and **Password**.
- **PIN Code:** It specifies the PIN code of your 3G SIM card. PIN is short for Personal Identification Number.
- **APN:** It is short for Access Point Name, which is provided by your ISP.
- **Dial Number:** It specifies the dial number provided by your ISP.

- **User Name:** It specifies the user name used for PPP authentication.
- **Password:** It specifies the password used for PPP authentication.
- **Back:** Click to go back to the previous page of the **Setup Wizard**.
- **Cancel:** Click to revert to the last saved settings.
- **Exit:** Click to exit the **Setup Wizard** and go to the **Welcome** page (see Figure 3-5). The changes made in the **Setup Wizard** will be discarded.
- **Skip:** Click to go directly to the next page of the **Setup Wizard**. The changes made on the current page will be discarded.
- **Next:** Click to go to the next page of the **Setup Wizard**.

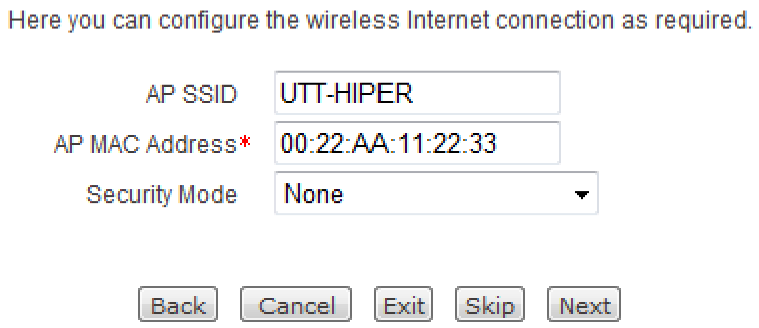
✓ **Note**

It is strongly recommended that you configure only the **3G USB Modem** and **ISP** of the 3G Internet connection, and leave the other parameters at their default values. If necessary, please change them under the guidance of a professional.

3.3.3.3 APClient Internet Connection Settings

In the **Setup Wizard - APClient Connection Settings** page, the security settings depend on the value of **Security Mode**. The following sections describe the APClient connection settings under each security mode respectively.

3.3.3.3.1 APClient Connection Settings - Disabling Wireless Security



Here you can configure the wireless Internet connection as required.

AP SSID: UTT-HIPER

AP MAC Address*: 00:22:AA:11:22:33

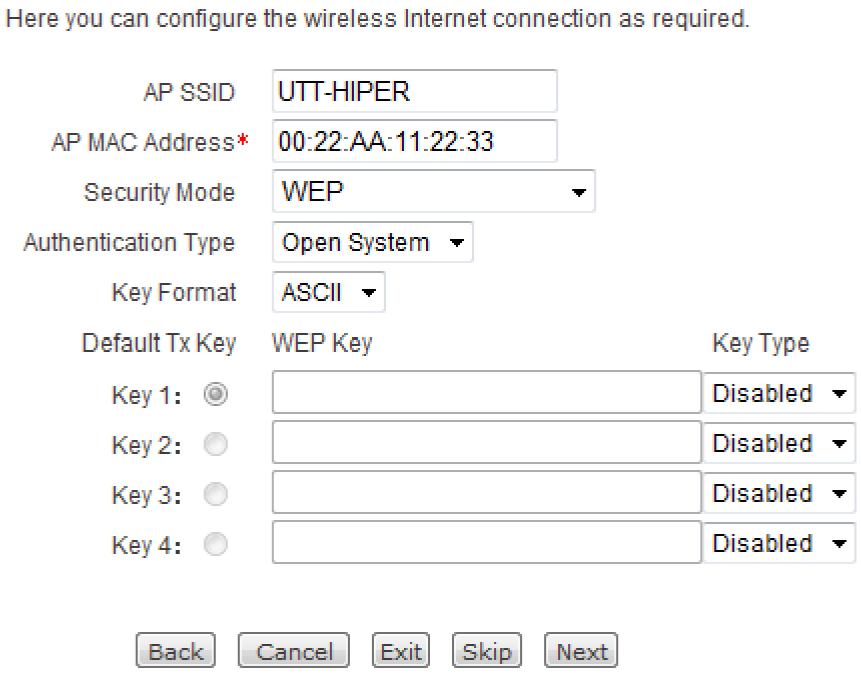
Security Mode: None

Figure 3-11 Setup Wizard - APClient Connection Settings (Disabling Wireless Security)

- **AP SSID:** It specifies the SSID of the remote AP. It must be between 1 and 32 characters long, and it is case sensitive.
- **AP MAC Address:** It specifies the MAC address of the remote AP.

- **Security Mode:** It specifies the security mode to be used by the Wireless Router. Here please select **None**.
- **Back:** Click to go back to the previous page of the **Setup Wizard**.
- **Cancel:** Click to revert to the last saved settings.
- **Exit:** Click to exit the **Setup Wizard** and go to the **Welcome** page (see Figure 3-5). The changes made in the **Setup Wizard** will be discarded.
- **Skip:** Click to go directly to the next page of the **Setup Wizard**. The changes made on the current page will be discarded.
- **Next:** Click to go to the next page of the **Setup Wizard**.

3.3.3.3.2 APClient Connection Settings - WEP



Here you can configure the wireless Internet connection as required.

AP SSID: UTT-HIPER
AP MAC Address*: 00:22:AA:11:22:33
Security Mode: WEP
Authentication Type: Open System
Key Format: ASCII

Default Tx Key		WEP Key	Key Type
Key 1:	●		Disabled
Key 2:	○		Disabled
Key 3:	○		Disabled
Key 4:	○		Disabled

Figure 3-12 Setup Wizard - APClient Connection Settings (WEP)

- **AP SSID:** It specifies the SSID of the remote AP. It must be between 1 and 32 characters long, and it is case sensitive.
- **AP MAC Address:** It specifies the MAC address of the remote AP.
- **Security Mode:** It specifies the security mode to be used by the Wireless Router. Here please select **WEP**. WEP is the basic encryption mode which is not as secure as WPA.
- **Authentication Type:** It allows you to select the authentication type under **WEP** security mode. The options are **Open System** and **Shared Key**.

- **Open System:** It allows the Wireless Router regardless of its WEP keys to authenticate and attempt to associate with the remote AP. However, even if the Wireless Router can complete authentication and associate with the remote AP, the Wireless Router cannot send or receive data from the remote AP unless it has the correct WEP key.
- **Shared Key:** It requires that the Wireless Router and remote AP have the same WEP key to authenticate. Without the correct key, authentication will fail and the Wireless Router won't be allowed to associate with the remote AP.

◆ **Key Format:** It specifies the format for entering the WEP keys. The options are **Hex** and **ASCII**.

- **Hex:** Select this option if you want to enter the WEP keys in hexadecimal format. Hexadecimal digits are a set of characters that includes numbers 0 through 9 and letters A through F (or a through f). Hex WEP keys are case insensitive.
- **ASCII:** Select this option if you want to enter the WEP keys in ASCII format. ASCII WEP keys are case sensitive.

◆ **Default Tx Key:** It allows you to select one of the WEP keys as the default transmit key to transmit data. All keys can be used to receive data.

◆ **WEP Key:** It allows you to enter a key in one of the **WEP Key** boxes. You can enter up to four WEP keys. You should enter a key according to the **Key Format** and **Key Type** selected.

- For 64-bit encryption, enter 10 hex characters or 5 ASCII characters.
- For 128-bit encryption, enter 26 hex characters or 13 ASCII characters.

◆ **Key Type:** It allows you to select the size of each key, and it also allows you to disable or enable each key. The options are **Disabled**, **64-bit** and **128-bit**. By default, **Disabled** is selected, which means the key is of no effect.

▶ **Back:** Click to go back to the previous page of the **Setup Wizard**.

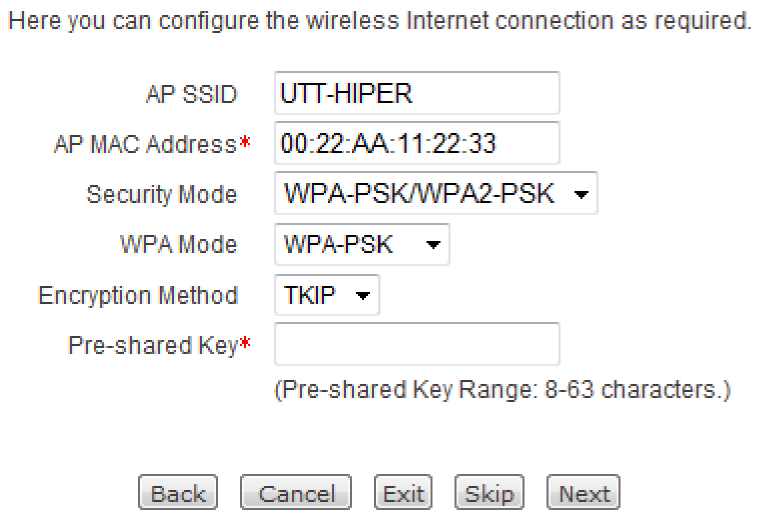
▶ **Cancel:** Click to revert to the last saved settings.

▶ **Exit:** Click to exit the **Setup Wizard** and go to the **Welcome** page (see Figure 3-5). The changes made in the **Setup Wizard** will be discarded.

▶ **Skip:** Click to go directly to the next page of the **Setup Wizard**. The changes made on the current page will be discarded.

▶ **Next:** Click to go to the next page of the **Setup Wizard**.

3.3.3.3.3 APClient Connection Settings - WPA-PSK/WAP2-PSK



Here you can configure the wireless Internet connection as required.

AP SSID: UTT-HIPER

AP MAC Address*: 00:22:AA:11:22:33

Security Mode: WPA-PSK/WPA2-PSK

WPA Mode: WPA-PSK

Encryption Method: TKIP

Pre-shared Key*:

(Pre-shared Key Range: 8-63 characters.)

Figure 3- 13 Setup Wizard - APClient Connection Settings (WPA-PSK/WAP2-PSK)

- **AP SSID:** It specifies the SSID of the remote AP. It must be between 1 and 32 characters long, and it is case sensitive.

- **AP MAC Address:** It specifies the MAC address of the remote AP.

- **Security Mode:** It specifies the security mode to be used by the Wireless Router. Here please select **WPA-PSK/WPA2-PSK** to use WPA-PSK mode or WPA2-PSK mode. In WPA-PSK or WPA2-PSK mode, the Wireless Router uses the pre-shared key that is manulally entered to generate encryption keys.

- **WPA Mode:** It specifies the WPA mode to be used by the Wireless Router. The options are **WPA-PSK** and **WPA2-PSK**.
  - **WPA-PSK:** It means that the Wireless Router will use WAP-PSK security mode.
  - **WPA2-PSK:** It means that the Wireless Router will use WAP2-PSK security mode.

- **Encrption Method:** It specifies the encrytion method used for data encryption. The options are **TKIP** and **AES**.
  - **TKIP:** It means that the Wireless Router will use TKIP for data encryption.
  - **AES:** It means that the Wireless Router will use AES for data encryption.

- **Pre-shared Key:** This key serves as seed for generating encryption keys. It must be identical to the remote AP's. It must be between 8 and 63 characters long.

- **Back:** Click to go back to the previous page of the **Setup Wizard**.

- **Cancel:** Click to revert to the last saved settings.

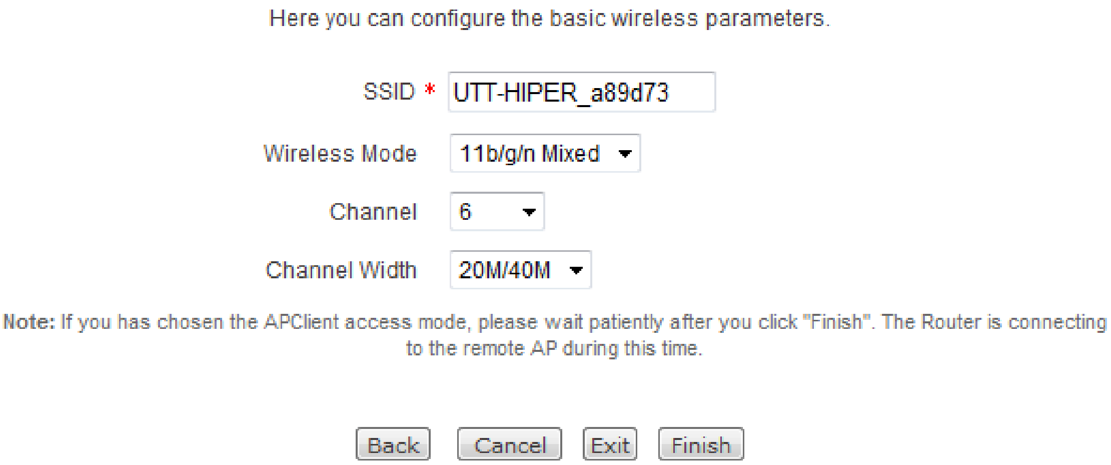
- **Exit:** Click to exit the **Setup Wizard** and go to the **Welcome** page (see Figure 3- 5).

The changes made in the **Setup Wizard** will be discarded.

- **Skip:** Click to go directly to the next page of the **Setup Wizard**. The changes made on the current page will be discarded.
- **Next:** Click to go to the next page of the **Setup Wizard**.

3.3.4 Setup Wizard - Wireless Settings

In this page, you can configure basic wireless settings of the Wireless Router.



Here you can configure the basic wireless parameters.

SSID * UTT-HIPER_a89d73

Wireless Mode 11b/g/n Mixed

Channel 6

Channel Width 20M/40M

Note: If you has chosen the APClient access mode, please wait patiently after you click "Finish". The Router is connecting to the remote AP during this time.

Figure 3- 14 Setup Wizard - Wireless Settings

- **SSID:** The SSID (Service Set Identification) is also known as the wireless network name, which is used to uniquely identify a wireless network. It must be between 1 and 32 characters long, and it is case sensitive.
- **Wireless Mode:** It specifies the wireless standards running on your wireless network. The options are **11g Only**, **11n Only** and **11b/g/n Mixed**.
  - **11g Only:** In allows both 802.11g and 802.11n wireless clients to connect to the Wireless Router at 802.11g data rates with a maximum speed of 54Mbps.
  - **11n Only:** It only allows 802.11n wireless clients to connect to the Wireless Router at 802.11n data rates with a maximum speed of 300Mbps.
  - **11b/g/n Mixed:** It allows 802.11b, 802.11g and 802.11n wireless clients to connect to the Wireless Router at their respective data rates. The maximum speeds are 11Mbps, 54Mbps and 300Mbps respectively.
- **Channel:** It specifies the wireless channel used between the Wireless Router and wireless clients. The valid range is 1 through 11. You can also select **Auto** to let the Wireless Router automatically select the best channel. If there are multiple wireless routers in your area, please make sure that their channels don’t interfere with each

other.

- **Channel Width:** It specifies the range of frequecies used by your wireless network. The options are **20/40M** and **20M**. Note that this parameter can only act on 802.11n wireless clients. 802.11b and 802.11g wireless clients can only use 20MHz channel.
  - **20M/40M:** If you select this option, 802.11n wireless clients will negotiate the channel width with the Wireless Router.
  - **20M:** It you select this option, 802.11n wireless clients will use 20MHz channel.

- **Back:** Click to go back to the previous page of the **Setup Wizard**.
- **Cancel:** Click to revert to the last saved settings.
- **Exit:** Click to exit the **Setup Wizard** and go to the **Welcome** page (see Figure 3-5). The changes made in the **Setup Wizard** will be discarded.
- **Finish:** Click to save the changes you have made in the **Setup Wizard** and close the **Setup Wizard**.

✓ **Note**

Do not forget to click the **Finish** button to save the changes you have made in the **Setup Wizard**, else these changes will be discarded.

Chapter 4 Start Menu

The **Start** menu item is the first one under the top-level menu. It provides links to several commonly used pages including **Setup Wizard**, **System Status**, **Interface Traffic** and **Restart**, where you can quickly configure the basic parameters for the Wireless Router to operate properly, view system status, view interface traffic statistics, and restart the Wireless Router.

4.1 Setup Wizard

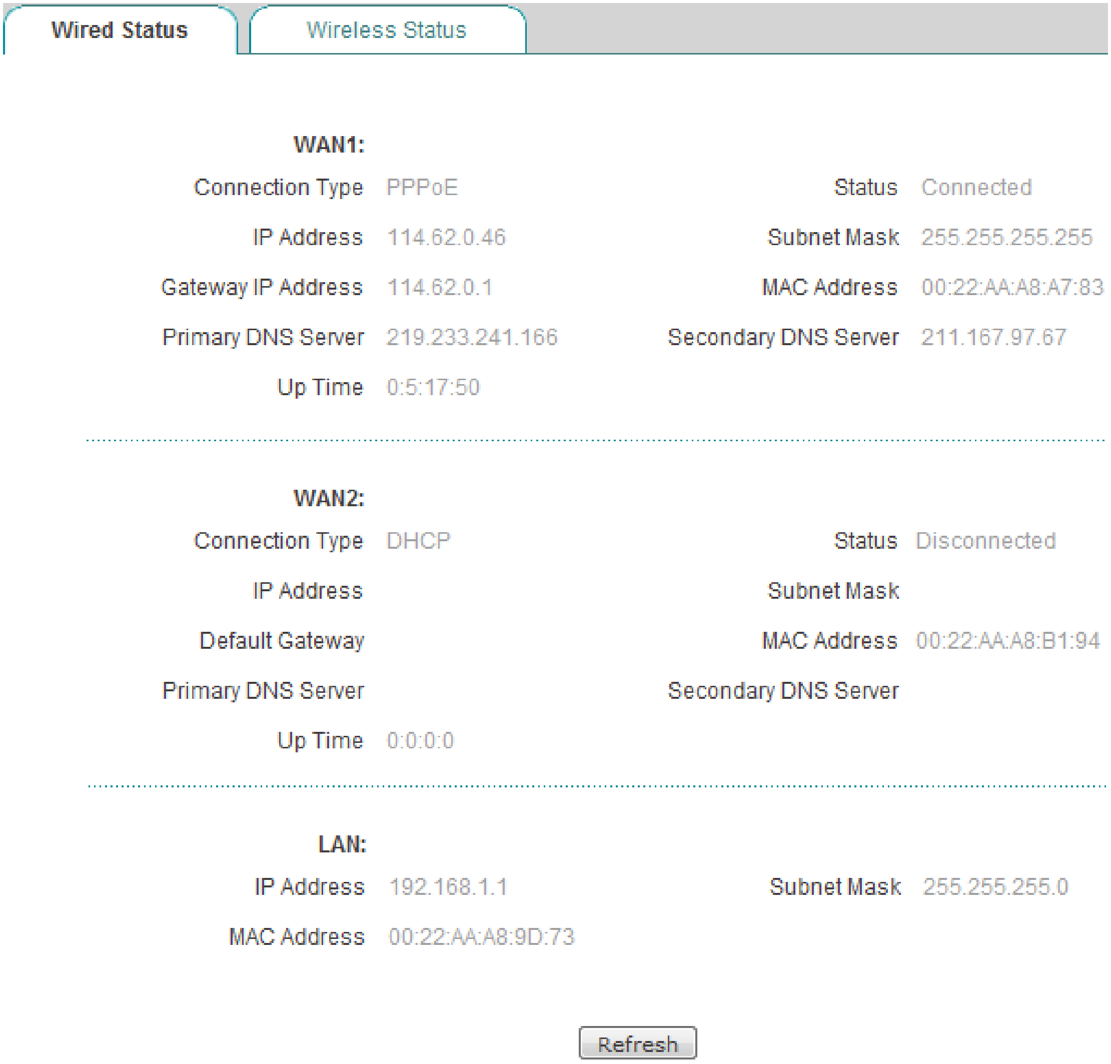
The **Start > Setup Wizard** can help you configure the basic parameters for the Wireless Router to operate properly. Refer to **Section 3.3 Setup Wizard** for detailed information.

4.2 System Status

This section describes the **Start > System Status** page, where you can view the current status information of the Wireless Router.

4.2.1 Wired Status

This page displays the current status information of the wired interfaces, which include WAN1, WAN2 and LAN.



WAN1:

Connection Type	PPPoE	Status	Connected
IP Address	114.62.0.46	Subnet Mask	255.255.255.255
Gateway IP Address	114.62.0.1	MAC Address	00:22:AA:A8:A7:83
Primary DNS Server	219.233.241.166	Secondary DNS Server	211.167.97.67
Up Time	0:5:17:50		

WAN2:

Connection Type	DHCP	Status	Disconnected
IP Address		Subnet Mask	
Default Gateway		MAC Address	00:22:AA:A8:B1:94
Primary DNS Server		Secondary DNS Server	
Up Time	0:0:0:0		

LAN:

IP Address	192.168.1.1	Subnet Mask	255.255.255.0
MAC Address	00:22:AA:A8:9D:73		

Figure 4- 1 System Status - Wired Status

- **WAN1**: It displays the current status and basic configuration of the WAN1 Internet connection, which include connection type, status, IP address, subnet mask, MAC address, default gateway and DNS server addresses, and up time.

- **WAN2:** It displays the current status and basic configuration of the WAN2 Internet connection, which are the same as those of the WAN1 Internet connection.

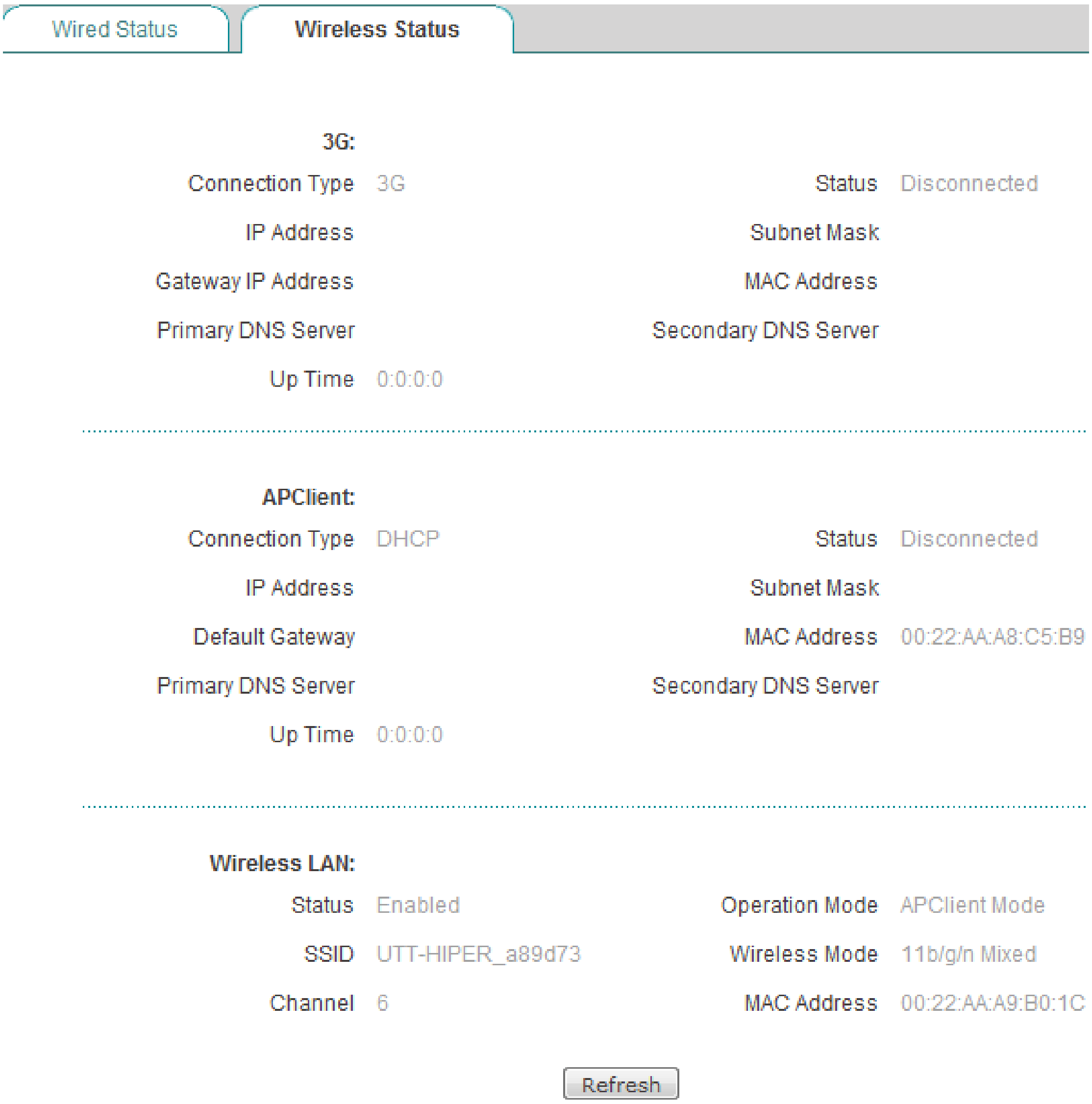
- **LAN:** It displays the basic configuration of the LAN inteface, which include IP address, subnet mask and MAC address.

- **Refresh:** Click to view the latest wired status information.

4.2.2 Wireless Status

This page displays the current status information of the wireless interfaces, which include

3G, APClient and Wireless LAN.



3G:

Connection Type	3G	Status	Disconnected
IP Address		Subnet Mask	
Gateway IP Address		MAC Address	
Primary DNS Server		Secondary DNS Server	
Up Time	0:0:0:0		

APClient:

Connection Type	DHCP	Status	Disconnected
IP Address		Subnet Mask	
Default Gateway		MAC Address	00:22:AA:A8:C5:B9
Primary DNS Server		Secondary DNS Server	
Up Time	0:0:0:0		

Wireless LAN:

Status	Enabled	Operation Mode	APClient Mode
SSID	UTT-HIPER_a89d73	Wireless Mode	11b/g/n Mixed
Channel	6	MAC Address	00:22:AA:A9:B0:1C

Figure 4- 2 System Status - Wireless Status

- **3G:** It displays the current status and basic configuration of the 3G Internet connection, which include connection type, status, IP address, subnet mask, MAC address, default gateway and DNS server addresses, and up time.
- **APClient:** It displays the current status and basic configuration of the APClient Internet connection, which are the same as those of the 3G Internection connection.
- **Wireless LAN:** It displays the current status and basic configuration of the Wireless LAN, which include status, operation mode, SSID, wireless mode, channel and MAC address.

- **Refresh:** Click to view the latest wireless status information.

✓ **Note**

The **Wired Status** page and **Wireless Status** page only display the status information of the interfaces that have been configured.

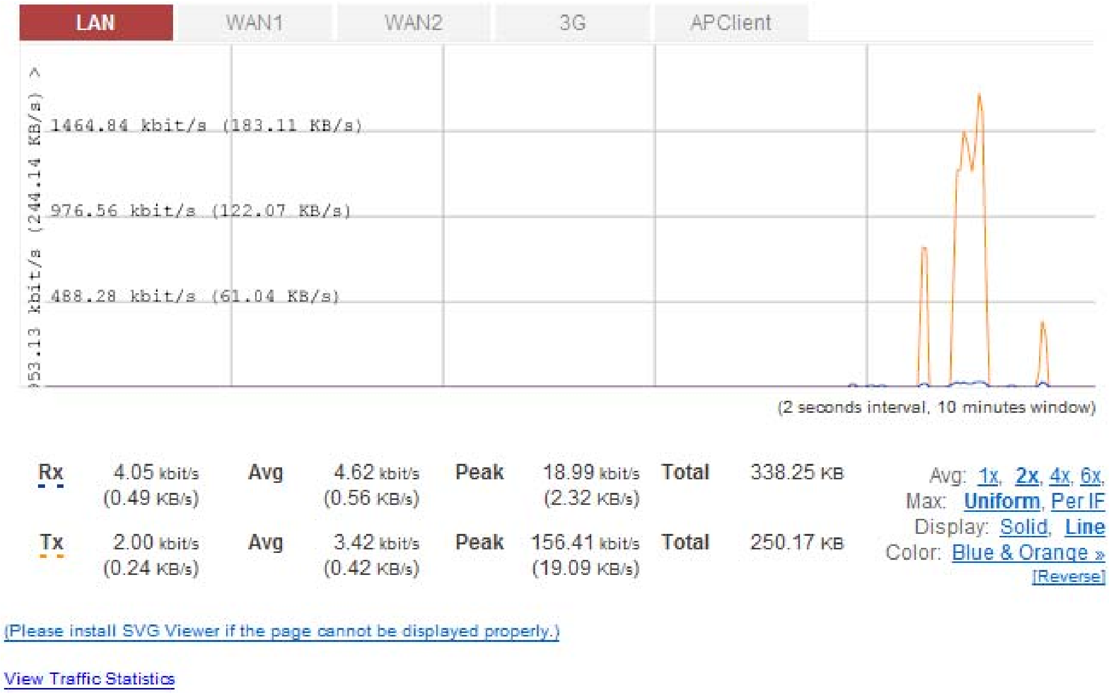
4.3 Interface Traffic

This section describes the **Start > Interface Traffic** page.

This page provides the real-time traffic chart for each interface that has been configured, which displays the real-time Rx/Tx rate, average Rx/Tx rate, maximum Rx/Tx rate and total Rx/Tx traffic of each interface. For example, as shown in Figure 4-3, all of the Wireless Router’s interfaces (LAN, WAN1, WAN2, 3G and APClient) have been configured.

Note

If the SVG Viewer plug-in isn’t installed on your web browser, the port traffic chart cannot be displayed properly. Please click the **(Please install SVG Viewer if the page cannot be displayed properly.)** hyperlink to download and install the SVG Viewer to view the traffic chart.


LAN
WAN1
WAN2
3G
APClient
1953.13 kbit/s (244.14 KB/s) >
1464.84 kbit/s (183.11 KB/s)
976.56 kbit/s (122.07 KB/s)
488.28 kbit/s (61.04 KB/s)

(2 seconds interval, 10 minutes window)

Rx	4.05 kbit/s (0.49 KB/s)	Avg	4.62 kbit/s (0.56 KB/s)	Peak	18.99 kbit/s (2.32 KB/s)	Total	338.25 KB
Tx	2.00 kbit/s (0.24 KB/s)	Avg	3.42 kbit/s (0.42 KB/s)	Peak	156.41 kbit/s (19.09 KB/s)	Total	250.17 KB

Avg: 1x, 2x, 4x, 6x,
Max: Uniform, Per IF
Display: Solid, Line
Color: Blue & Orange »
[Reverse]

(Please install SVG Viewer if the page cannot be displayed properly.)

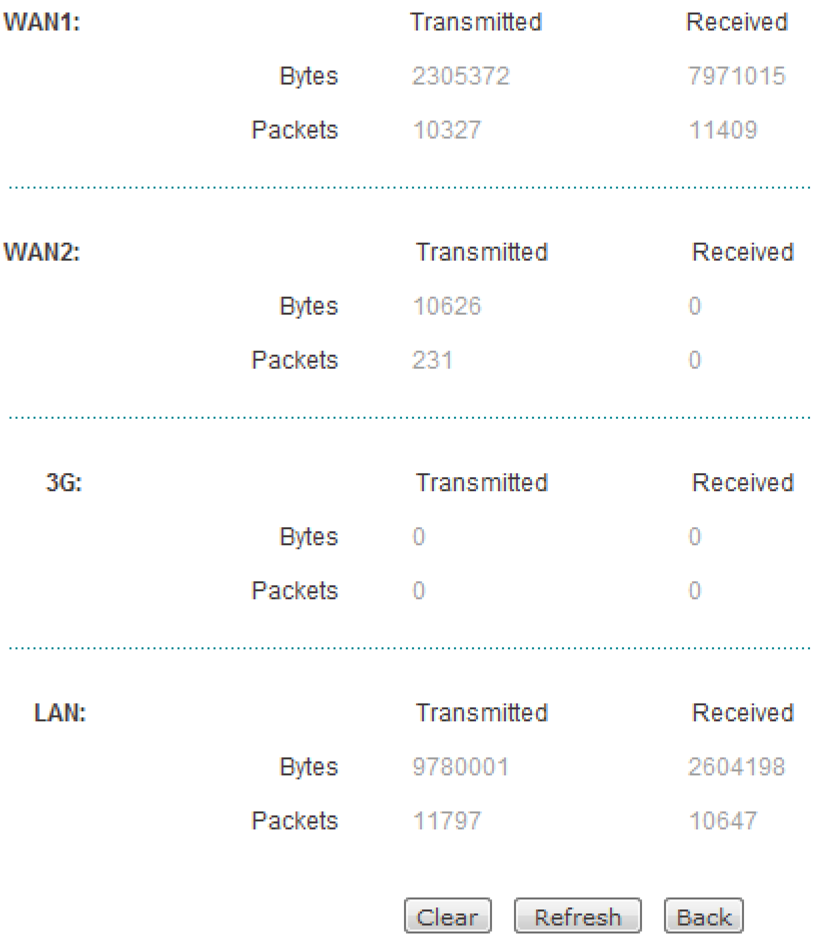
View Traffic Statistics

Figure 4-3 Interface Traffic Chart

- **Avg: 1x, 2x, 4x, 6x:** It specifies the number of samples to average, or no averaging.
- **Max:** It determines that the charts are scaled uniformly to the max traffic value of all interfaces or individually per interface.

- **Display:** It allows you to change the type of chart displayed. The options are **Line** and **Solid**.
  - **Line:** Select this option to display a line chart. The chart includes two lines with different colors, which represent the real-time Rx rate and Tx rate resectively.
  - **Solid:** Select this option to display an area chart. The area chart is like the line chart except that the area between the axis the plot line is solid.
- **Color:** It specifies the colors of the two lines (or filled areas), such as red, blue, black, etc.
- **Reverse:** Click to toggle the colors of the two lines (or filled areas).

- **LAN**, **WAN1**, **WAN2**, **APClient** and **3G:** You can select an interface name at the top to view the traffic chart for that interface.
- **View Traffic Statistics:** Click to view the ingress and egress traffic statistics for the interfaces that have been configured, see Figure 4-4.



WAN1:		Transmitted	Received
	Bytes	2305372	7971015
	Packets	10327	11409

WAN2:		Transmitted	Received
	Bytes	10626	0
	Packets	231	0

3G:		Transmitted	Received
	Bytes	0	0
	Packets	0	0

LAN:		Transmitted	Received
	Bytes	9780001	2604198
	Packets	11797	10647

Figure 4-4 Traffic Statistics

- **WAN1**, **WAN2**, **3G**, **APClient** and **LAN**: You can view the traffic statistics for each interface, including the number of bytes received and transmitted, and the number of packets received and transmitted.

- **Clear:** Click to clear all traffic statistics.
- **Refresh:** Click to view the latest traffic statistics.
- **Back:** Click to go back to the **Start > Interface Traffic** page.

Note

This page only displays the traffic statistics for the interfaces that have been configured.

4.4 Restart

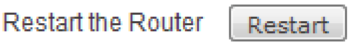
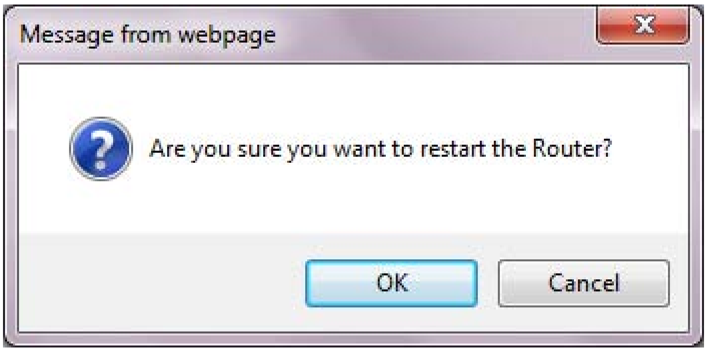

Restart the Router

Figure 4- 5 Restart the Wireless Router

- **Restart:** Click to restart the Wireless Router.

If you click the **Restart** button, the system will pop up a prompt dialog box (see Figure 4- 6). Then you can click **OK** to restart the Wireless Router, or click **Cancel** to cancel the operation.


Message from webpage

Are you sure you want to restart the Router?

Figure 4- 6 Prompt Dialog Box - Restart the Wireless Router

Note

Restarting the Wireless Router will disconnect all the sessions, so please do it with caution.

Chapter 5 Network

This chapter describes how to configure the basic network parameters of the Wireless Router, which include WAN settings, load balancing, LAN settings, DHCP server, DDNS, and UPnP.

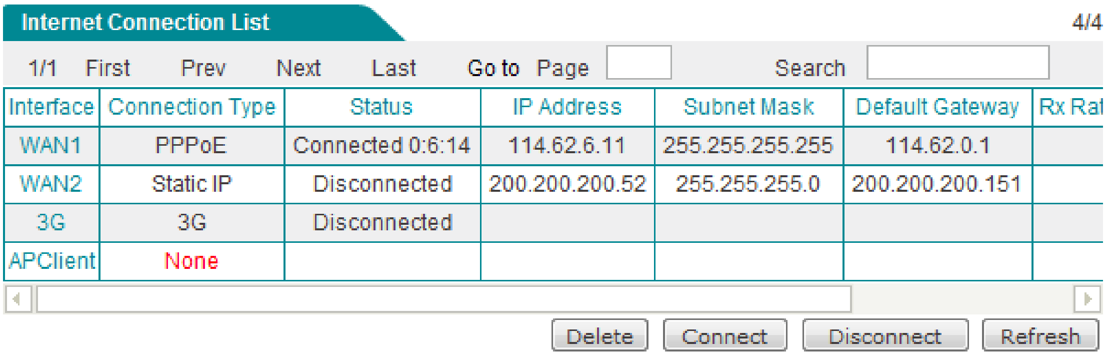
5.1 WAN Settings

This section describes the **Network > WAN** page.

If you have configured one or more Internet connections in the **Start > Quick Wizard**, you can view their configuration and status in this page, and modify or delete them if needed. You also can directly configure one or more Internet connections in this page.

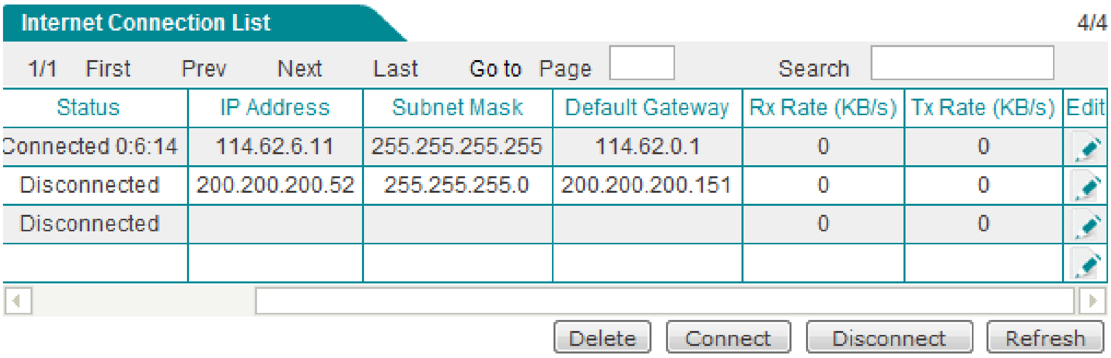
5.1.1 Internet Connection List

You can view the configuration and status of each Internet connection in the **Internet Connection List**, see Figure 5-1.



Interface	Connection Type	Status	IP Address	Subnet Mask	Default Gateway	Rx Rat
WAN1	PPPoE	Connected 0:6:14	114.62.6.11	255.255.255.255	114.62.0.1	
WAN2	Static IP	Disconnected	200.200.200.52	255.255.255.0	200.200.200.151	
3G	3G	Disconnected				
APClient	None					

Figure 5-1 Internet Connection List



Status	IP Address	Subnet Mask	Default Gateway	Rx Rate (KB/s)	Tx Rate (KB/s)	Edit
Connected 0:6:14	114.62.6.11	255.255.255.255	114.62.0.1	0	0	✎
Disconnected	200.200.200.52	255.255.255.0	200.200.200.151	0	0	✎
Disconnected				0	0	✎
						✎

Figure 5-2 Internet Connection List (Continue)

5.1.1.1 Parameter Definitions

- **Interface:** It displays the name of the WAN interface. The Wireless Router has four WAN interfaces: WAN1, WAN2, 3G, and APClient. Therein, WAN1 and WAN2 are wired interfaces, and 3G and APClient are wireless interfaces.
- **Connection Type:** It displays the type of the Internet connection. There are four connection types: Static IP, PPPoE, DHCP and 3G.
- **Status:** It displays current status of the connection. There are four cases:

1. PPPoE Connection Status

For the PPPoE connection, there are two kinds of status, see Table 5-1. When it is connected, it will also display the elapsed time (days: hours: minutes: seconds) since connected.

Status	Description
Disconnected	The connection is disconnected due to that the interface is disabled or not connected, or the Wireless Router doesn't dial up yet, or wrong user name or password, etc.
Connected	Authentication succeeded, and the connection is established and ready for data transmission.

Table 5-1 Description of PPPoE Connection Status

2. Static IP Connection Status

For the static IP connection, there are two kinds of status, see Table 5-2.

Status	Description

Disconnected	The connection is disconnected due to that the interface is disabled or not connected, etc.
Connected	The connection is established between the Wireless Router and peer device.

Table 5- 2 Description of Static IP Connection Status

3. DHCP Connection Status

For the DHCP connection, there are two kinds of status, see Table 5- 3. When it is connected, it will also display the elapsed time (days: hours: minutes: seconds) since connected.

Status	Description
Disconnected	The connection is disconnected due to that the interface is disabled or not connected, or the Wireless Router has released the IP address but hasn't obtained a new one yet, etc.
Connected	The Wireless Router has obtained an IP address, and the connection is established successfully.

Table 5- 3 Description of DHCP Connection Status

4. 3G Connection Status

For the 3G connection, there are two kinds of status, see Table 5- 4. When it is connected, it will also display the elapsed time (days: hours: minutes: seconds) since connected.

Status	Description
Disconnected	The connection is disconnected due to that the 3G USB modem isn't inserted properly, or wrong ISP, 3G USB modem settings, etc.
Connected	The Wireless Router has obtained an IP address, and the connection is established successfully.

Table 5- 4 Description of 3G Connection Status

- **IP Address, Subnet Mask** and **Default Gateway:** They display the current IP settings of the connection. There are two cases:
  - For the PPPoE, DHCP or 3G Internet connection, it will show the current WAN IP address, subnet mask and gateway IP address which are assigned by your ISP.
  - For the static IP Internet connection, it will show the information you have entered manually.

- **Rx Rate:** It displays the average download speed (in kilobytes per second) of the Internet connection during the time interval between two refresh operations.

- **Tx Rate:** It displays the average upload speed (in kilobytes per second) of the Internet connection during the time interval between two refresh operations.

5.1.1.2 How to Add, View, Modify and Delete Internet Connections

- **Add an Internet Connection:** To add a new Internet connection, first click its **Interface** hyperlink or ✎ icon, and then configure it, lastly click the **Save** button.

- **View Internet Connection(s):** When you have configured one or more Internet connections, you can view them in the **Internet Connection List**.

- **Modify an Internet Connection:** To modify a configured Internet connection, click its **Interface** hyperlink or ✎ icon, the related information will be displayed in the setup fields. Then modify it, and click the **Save** button.

- **Delete an Internet Connection:** To delete an Internet connection, click its **Interface** hyperlink or ✎ icon to select the connection, and then click the **Delete** button below the list.

- **Refresh Internet Connection List:** To view the latest status of the Internet connections, click the **Refresh** button below the list.

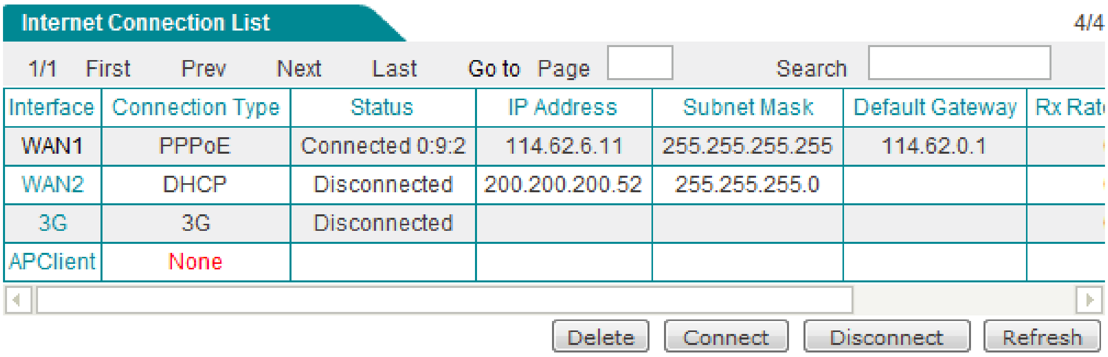
5.1.1.3 How to Connect and Disconnect a PPPoE/3G Connection

If you click the **Interface** hyperlink or ✎ icon of a PPPoE or 3G connection, the **Connect** and **Disconnect** button will appear below the list, see Figure 5-3.

If the PPPoE connection's **Dial Type** is set to **Manual** (see **Section 5.1.2.1.3 PPPoE Internet Connection Settings**), you need to click the **Connect** button to connect it, and click the **Disconnect** button to disconnect it.

- **Connect:** Click to connect the PPPoE or 3G Internet connection manually.

- **Disconnect:** Click to disconnect the PPPoE or 3G Internet connection manually.

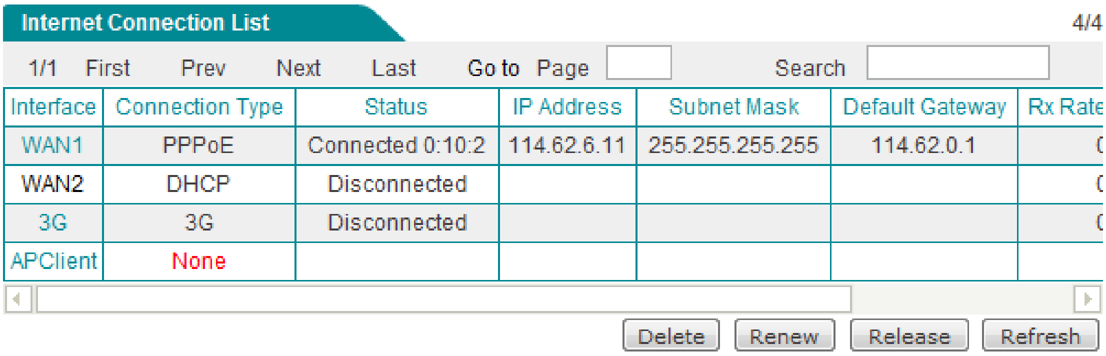


Interface	Connection Type	Status	IP Address	Subnet Mask	Default Gateway	Rx Rat
WAN1	PPPoE	Connected 0:9:2	114.62.6.11	255.255.255.255	114.62.0.1	
WAN2	DHCP	Disconnected	200.200.200.52	255.255.255.0		
3G	3G	Disconnected				
APClient	None					

Figure 5- 3 Internet Connection List - PPPoE/3G Connection

5.1.1.4 How to Renew and Release a DHCP Connection

If you click the **Interface** hyperlink or ✎ icon of a DHCP connection, the **Renew** button and **Release** button will appear below the list, see Figure 5- 4.



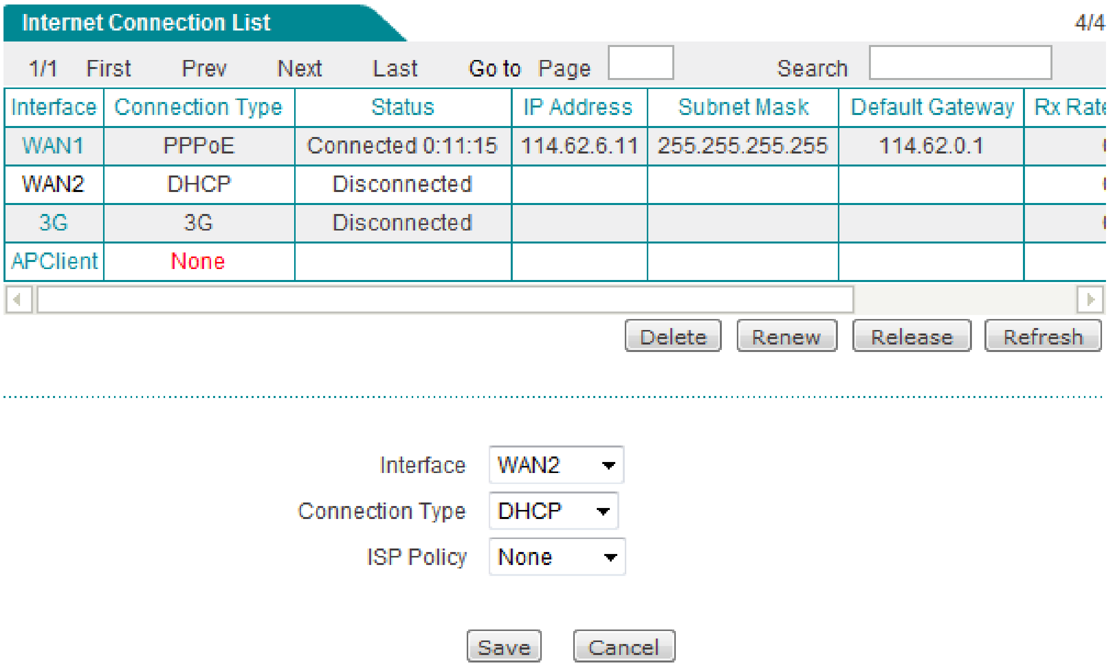
Interface	Connection Type	Status	IP Address	Subnet Mask	Default Gateway	Rx Rate
WAN1	PPPoE	Connected 0:10:2	114.62.6.11	255.255.255.255	114.62.0.1	
WAN2	DHCP	Disconnected				
3G	3G	Disconnected				
APClient	None					

Figure 5- 4 Internet Connection List - DHCP Connection

- **Renew:** Click to re-obtain an IP address from the ISP's DHCP server. The Wireless Router will automatically release the assigned IP address firstly, and then obtain a new IP address from the DHCP server.
- **Release:** Click to release the IP address obtained from the ISP's DHCP server.

5.1.2 Internet Connection Settings

If you want to configure an Internet connection, please click its **Interface** hyperlink or ✎ icon in the **Internet Connection List**. The setup page is shown in Figure 5- 5.



Interface	Connection Type	Status	IP Address	Subnet Mask	Default Gateway	Rx Rate
WAN1	PPPoE	Connected 0:11:15	114.62.6.11	255.255.255.255	114.62.0.1	
WAN2	DHCP	Disconnected				
3G	3G	Disconnected				
APClient	None					

Interface WAN2

Connection Type DHCP

ISP Policy None

Figure 5- 5 Network - WAN Settings

Note

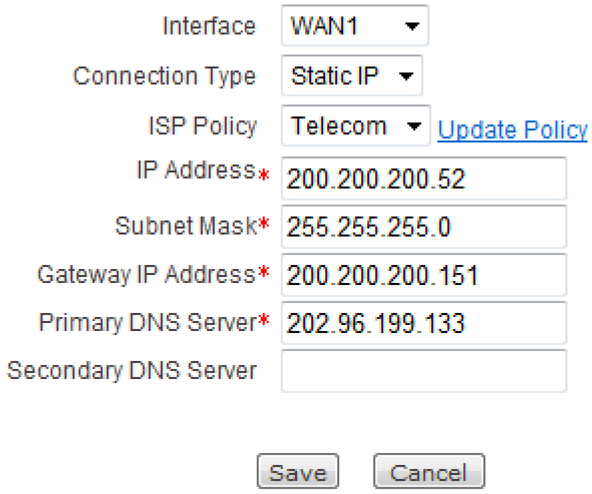
1. It allows you to choose the **ISP Policy** (i.e., route policy database) for each Internet connection. The system will automatically create the associated static routes according to your selection. Thus all traffic destined for one ISP's servers will be forwarded through this ISP's connection.

2. If you want to configure and use an APClient Internet connection, please choose **APClient Mode** as the **Operation Mode** in the **Wireless > Basic** page.

5.1.2.1 WAN1/WAN2/APClient Internet Connection Settings

For the WAN1, WAN2 or APClient Internet connection, there are three connection types which include PPPoE, Static IP and DHCP. The following subsections describe how to configure the PPPoE, Static IP and DHCP Internet connection respectively.

5.1.2.1.1 Static IP Internet Connection Settings



Interface	WAN1
Connection Type	Static IP
ISP Policy	Telecom Update Policy
IP Address*	200.200.200.52
Subnet Mask*	255.255.255.0
Gateway IP Address*	200.200.200.151
Primary DNS Server*	202.96.199.133
Secondary DNS Server	

Figure 5- 6 Static IP Internet Connection

- **Interface:** It specifies the name of the WAN interface. Here please select **WAN1**, **WAN2** or **APClient**.

- **Connection Type:** It specifies the type of the Internet connection. Here please select **Static IP**. You need to manually configure IP address, subnet mask, default gateway and DNS server addresses, which are provided by your ISP.

- **ISP Policy:** It specifies the route policy database used for the Interent connection. There are four options: None, Telecom, Unicom and Mobile.
  - **None:** It means that no route policy database is used. This option is selected by default.
  - **Telecom:** If your ISP is China Telecom, you may select this option. Then the traffic destined for China Telecom servers will be forwarded through the connection.
  - **Unicom:** If your ISP is China Unicom, you may select this option. Then the traffic destined for China Unicom servers will be forwarded through the connection.
  - **Mobile:** If your ISP is China Mobile, you may select this option. Then the traffic destined for China Mobile servers will be forwarded through the connection.

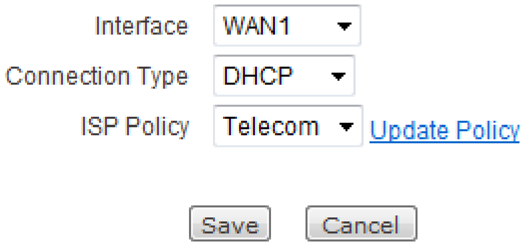
- **Update Policy:** Click to update the corresponding route policy database.

- **IP Address**, **Subnet Mask**, **Default Gateway**, **Primary DNS Server** and **Secondary DNS Server:** Refer to **Section 3.3.3.1.1 Static IP Internet Connection Settings** for detailed information.

- **Save:** Click to save your changes.

- **Cancel:** Click to revert to the last saved settings.

5.1.2.1.2 DHCP Internet Connection Settings

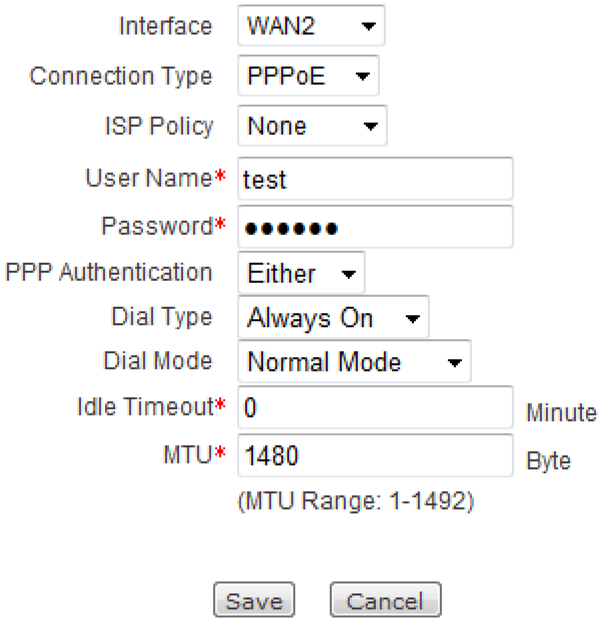


Interface	WAN1
Connection Type	DHCP
ISP Policy	Telecom

Figure 5- 7 DHCP Internet Connection Settings

- **Interface:** It specifies the name of the WAN interface. Here please select **WAN1**, **WAN2** or **APClient**.
- **Connection Type:** It specifies the type of the Internet connection. Here please select **DHCP**. The Wireless Router will automatically obtain the WAN IP address, subnet mask and gateway and DNS server addresses from your ISP's DHCP server.
- **ISP Policy** and **Update Policy:** Refer to **Section 5.1.2.1.1 Static IP Internet Connection Settings** for detailed information.
- **Save:** Click to save your changes.
- **Cancel:** Click to revert to the last saved settings.

5.1.2.1.3 PPPoE Internet Connection Settings



Interface	WAN2
Connection Type	PPPoE
ISP Policy	None
User Name*	test
Password*	●●●●●●
PPP Authentication	Either
Dial Type	Always On
Dial Mode	Normal Mode
Idle Timeout*	0 Minute
MTU*	1480 Byte (MTU Range: 1-1492)

Figure 5- 8 PPPoE Internet Connection Settings

- **Interface:** It specifies the name of the WAN interface. Here please select **WAN1**,

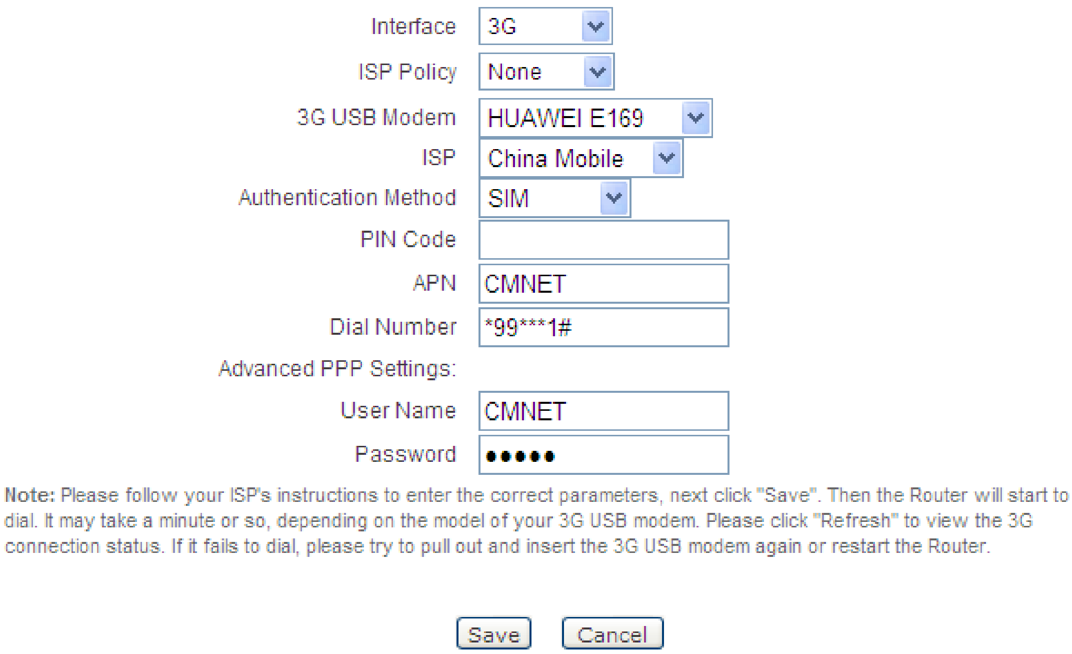
WAN2 or **APClient**.

- **Connection Type:** It specifies the type of the Internet connection. Here please select **PPPoE**. The Wireless Router will automatically obtain the WAN IP address, subnet mask and gateway IP address from your ISP's PPPoE server.
- **ISP Policy** and **Update Policy:** Refer to **Section 5.1.2.1.1 Static IP Internet Connection Settings** for detailed information.
- **User Name** and **Password:** They specify the PPPoE login user name and password provided by your ISP. Please ask your ISP if you have any questions.
- **PPP Authentication:** It specifies the PPP authentication mode of the PPPoE connection. The available options are **Either**, **PAP**, **CHAP** and **NONE**. The default value is **Either**, which means that the Wireless Router will automatically negotiate it with the remote PPPoE Server. **NONE** means that no authentication is performed.
- **Dial Type:** It specifies the dial type of the PPPoE connection. The available options are **Always On**, **Manual** and **On Demand**.
  - **Always On:** If you want the Wireless Router to establish the PPPoE connection when starting up and to automatically re-establish the PPPoE connection once disconnected, please select this option.
  - **Manual:** If you want to connect and disconnect the PPPoE connection manually in the **Internet connection List** (see **Section 5.1.1.3 How to Connect and Disconnect a PPPoE/3G Connection**), please select this option.
  - **On Demand:** If you want the Wireless Router to establish the PPPoE connection only when it listens for packets destined for the Internet, please select this option.
- **Dial Mode:** It specifies the dial mode of the PPPoE Internet connection. The default value is **Normal mode**. If the PPPoE connection isn't established successfully even using correct user name and password, you may try to use another mode.
- **Idle Timeout:** It specifies how long the PPPoE connection keeps connected since no Internet activity. The Wireless Router will automatically terminate the connection after it has been inactive for the specified period of time. The default value is zero, which means that the Wireless Router will not terminate it.
- **MTU:** It the maximum packet size that can be transmitted over a network. When dialing, the Wireless Router will automatically negotiate it with the peer device. Please leave the default value of 1480 bytes, unless you have a special application.

- **Save:** Click to save your changes.
- **Cancel:** Click to revert to the last saved settings.

5.1.2.2 3G Internet Connection Settings

To configure a 3G Internet connection, select **3G** from the Interface drop-down list. Then the following page will be shown.



Interface	3G
ISP Policy	None
3G USB Modem	HUAWEI E169
ISP	China Mobile
Authentication Method	SIM
PIN Code	
APN	CMNET
Dial Number	*99***1#
Advanced PPP Settings:	
User Name	CMNET
Password	●●●●●

Note: Please follow your ISP's instructions to enter the correct parameters, next click "Save". Then the Router will start to dial. It may take a minute or so, depending on the model of your 3G USB modem. Please click "Refresh" to view the 3G connection status. If it fails to dial, please try to pull out and insert the 3G USB modem again or restart the Router.

Figure 5- 9 3G Internet Connection Settings

- **Interface:** It specifies the name of the WAN interface. Here please select **3G**.
- **ISP Policy** and **Update Policy:** Refer to **Section 5.1.2.1.1 Static IP Internet Connection** for detailed information.
- **3G USB Modem**, **ISP**, **Authentication Method**, **PIN Code**, **APN**, **Dial Number**, **User Name**, and **Password:** Refer to **Section 3.3.3.2 3G Internet Connection Settings** for detailed information.
- **Save:** Click to save your changes.
- **Cancel:** Click to revert to the last saved settings.

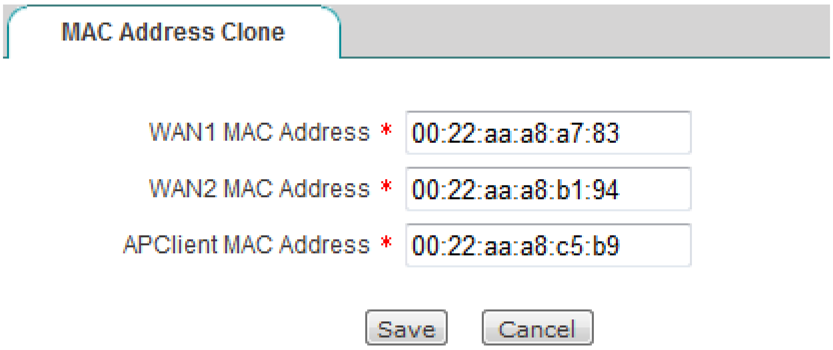
Note

It is strongly recommended that you configure only the **3G USB Modem** and **ISP** of the 3G Internet connection, and leave the other parameters at their default values. If necessary, please follow your ISP's instructions to change them. After you click the **Save** button, the Wireless Router will start to dial. It may take a minute or so, depending on the model of your 3G USB modem. Please click the **Refresh** button to view the 3G connection status. If it fails to dial, please try to pull out and insert the 3G USB modem again or restart the Wireless Router.

5.1.3 MAC Address Clone

Some ISPs register the MAC address of your network device (usually a computer) when your account is first opened, and they will only accept traffic from that MAC address. With MAC address clone feature, you may assign the registered MAC address to the Wireless Router's external interface if you don't want to re-register the MAC address with your ISP.

To configure MAC address clone, go to the **Network > WAN** page, and then select the **MAC Address Clone** tab to go to the setup page shown in Figure 5-10 MAC Address CloneFigure 5-10. In this page, you can change the MAC address of each external interface (WAN1, WAN2, or APClient interface) as required.



WAN1 MAC Address * 00:22:aa:a8:a7:83

WAN2 MAC Address * 00:22:aa:a8:b1:94

APClient MAC Address * 00:22:aa:a8:c5:b9

Figure 5-10 MAC Address Clone

- **WAN1 MAC Address:** It specifies the MAC address of the Wireless Router's WAN1 interface.
- **WAN2 MAC Address:** It specifies the MAC address of the Wireless Router's WAN2 interface.
- **APClient MAC Address:** It specifies the MAC address of the Wireless Router's APClient interface.
- **Save:** Click to save your changes.
- **Cancel:** Click to revert to the last saved settings.

5.2 Load Balancing

This section describes the **Network > Load Balancing** page.

In this page, you can configure load balancing global parameters, the connection detection parameters (including detection target IP, detection interval, retry times, etc.) for each Internet connection, and view the status and configuration of them.

5.2.1 Introduction to Load Balancing and Failover

5.2.1.1 Internet Connection Detection Mechanism

When using multiple Internet connections, to ensure that the network will not be interrupted when a connection is faulty, the Wireless Router should have the ability of real-time monitoring each Internet connection. To this end, we design flexible automatic detection mechanism on the Wireless Router, and provide multiple detection methods to meet the actual requirements.

For the sake of convenience, we firstly introduce several related parameters including **Detection Target IP**, **Detection Interval**, **Retry Times**, and **Detection Period**.

- **Detection Target IP:** It indicates the IP address of a target device. The Wireless Router will monitor an Internet connection by sending detection packets to the specified target IP address.
- **Detection Interval:** It indicates the time interval at which the Wireless Router periodically sends detection packets, one packet at a time. The default value is 0, which means that connection detection is disabled.
- **Retry Times:** It indicates the number of retries per detection period.
- **Detection Period:** It indicates a period of time during which the Wireless Router detects whether the Internet connection is available or not. Its value is the product of **Detection Interval** and **Retry Times**. For example, if the **Detection Interval** is set to 10 seconds and the **Retry Times** is set to 3, then the **Detection Period** is 30 (10 × 3 = 30) seconds.

For a normal Internet connection and a faulty Internet connection, the detection mechanisms are different, the following describes them respectively.

For a normal Internet connection, the detection mechanism is as follows: The Wireless Router periodically sends a detection packet at the specified time interval to the target IP address. Once no response packet received during a detection period, the Wireless Router will consider that the connection is faulty and shield it immediately. For example, when the **Retry Times** is set to 5, if the Wireless Router has sent five consecutive detection packets but not received any response packet during a detection period, it will consider that the connection is faulty.

For a faulty Internet connection, the detection mechanism is as follows: Similarly, the Wireless Router also periodically sends a detection packet at the specified time interval to the target IP address. Once more than half of the response packets received during a detection period, the Wireless Router will consider that the connection is back to normal and enable it immediately. For example, when the **Retry Times** is set to 5, if the Wireless Router has sent five consecutive detection packets and received three or more packets during a detection period, it will consider that the connection is back to normal.

On the Wireless Router, you can assign a preferential Internet connection to some local computers in advance by setting the connection's **Start Internal IP** and **End Internal IP**, thus the computers in the specified address range will preferentially use the assigned Internet connection to access the Internet. If the assigned Internet connection is normal, those computers can only use it to access the Internet. Else, they will use other normal Internet connections to access the Internet.

✓ **Note**

If you don't want to monitor an Internet connection, please leave its **Detection Interval** at the default value of 0.

5.2.1.2 Load Balancing Mode

The Wireless Router provides two connection groups: primary connection group and backup connection group. An Internet connection in the primary connection group is a primary connection, while an Internet connection in the backup connection group is a backup connection. By default, all the Internet connections are primary connections. You can move one or more connections into the backup connection group if needed.

The Wireless Router provides two load balancing modes: **Full Load Balancing** and **Partial Load Balancing**.

If you choose to use **Full Load Balancing**, all the Internet connections are used as primary connections. The working principle is as follows:

1. If all the Internet connections are normal, the LAN users will use these connections to access the Internet.

2. If an Internet connection is faulty, the Wireless Router will shield it immediately, and the traffic through the faulty connection will be distributed to other normal connections automatically.

3. Once the faulty connection is back to normal, the Wireless Router will enable it immediately, and the traffic will be redistributed automatically.

If you choose to use **Partial Load Balancing**, some Internet connections are used as primary connections, and others are used as backup connections. The working principle is as follows:

1. As long as one or more primary connections are normal, the LAN users will use the primary connection(s) to access the Internet.
2. If all the primary connections are faulty, it will automatically switch to the backup connection(s) to let the LAN users use them to access the Internet.
3. Once one or more faulty primary connections are back to normal, it will automatically switch back to the primary connection.

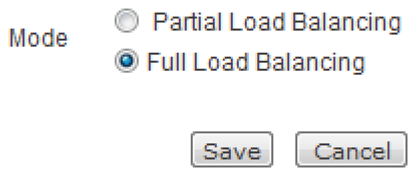
✓ **Note**

During connections switching, some user applications (such as some online games) may be interrupted unexpectedly due to the nature of TCP connection.

5.2.2 Load Balancing Global Settings

The following sections describe the global settings related to **Full Load Balancing** and **Partial Load Balancing** respectively. For more information, please refer to **Section 5.2.1.2 Load Balancing Mode**.

5.2.2.1 Global Settings - Full Load Balancing

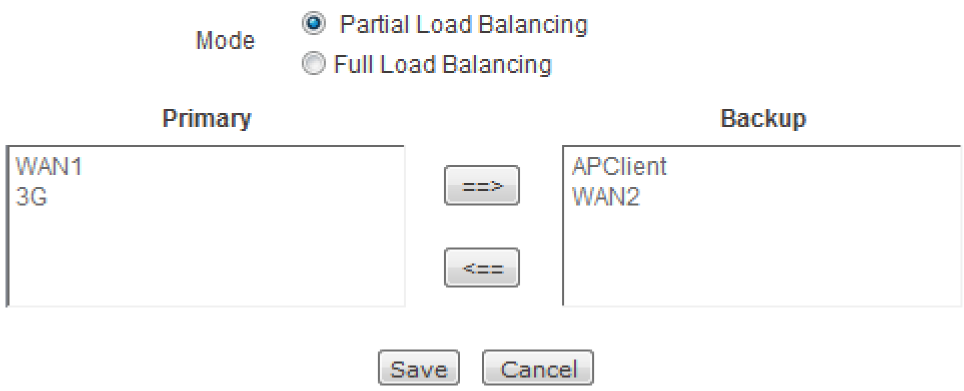


Mode ○ Partial Load Balancing ● Full Load Balancing

Figure 5-11 Global Settings - Full Load Balancing

- **Mode:** It specifies the mode of load balancing. Here please leave the default value of **Full Load Balancing**.
- **Save:** Click to save your changes.
- **Cancel:** Click to revert to the last saved settings.

5.2.2.2 Global Settings - Partial Load Balancing



Mode ● Partial Load Balancing ○ Full Load Balancing

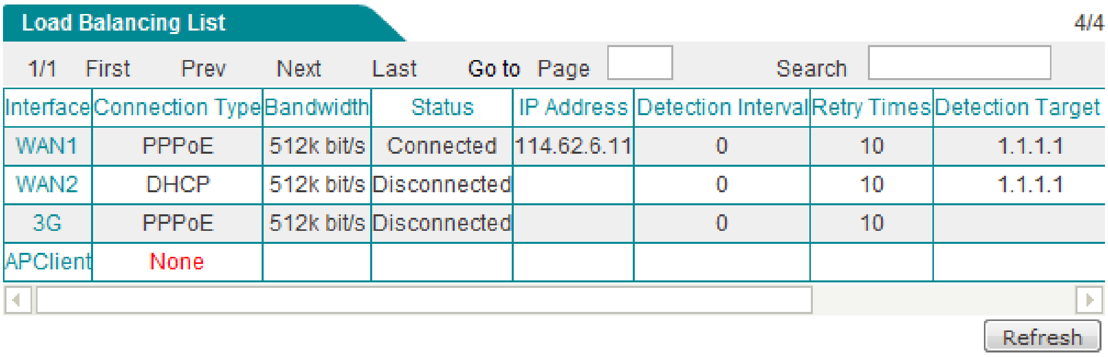
Primary: WAN1, 3G

Backup: APClient, WAN2

Figure 5- 12 Global Settings - Partial Load Balancing

- **Mode:** It specifies the mode of load balancing. Here please select **Partial Load Balancing**.
- **Primary:** It specifies the primary connection group. An Internet connection in the **Primary** list box is a primary connection.
- **Backup:** It specifies the backup connection group. An Internet connection in the **Backup** list box is a backup connection.
- **==>:** Select one or more Internet connections in the **Primary** list box, and then click **==>** to move the selected connection(s) to the **Backup** list box.
- **<==:** Select one or more Internet connections in the **Backup** list box, and then click **==>** to move the selected connection(s) to the **Primary** list box.
- **Save:** Click to save your changes.
- **Cancel:** Click to revert to the last saved settings.

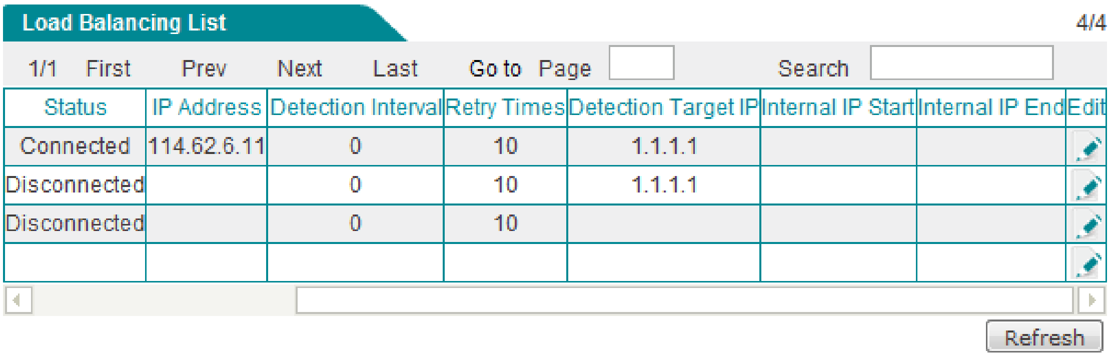
5.2.3 Load Balancing List



Load Balancing List 4/4

Interface	Connection Type	Bandwidth	Status	IP Address	Detection Interval	Retry Times	Detection Target
WAN1	PPPoE	512k bit/s	Connected	114.62.6.11	0	10	1.1.1.1
WAN2	DHCP	512k bit/s	Disconnected		0	10	1.1.1.1
3G	PPPoE	512k bit/s	Disconnected		0	10	
APClient	None						

Figure 5- 13 Load Balancing List



Status	IP Address	Detection Interval	Retry Times	Detection Target IP	Internal IP Start	Internal IP End	Edit
Connected	114.62.6.11	0	10	1.1.1.1			✎
Disconnected		0	10	1.1.1.1			✎
Disconnected		0	10				✎
							✎

Figure 5- 14 Load Balancing List (Continue)

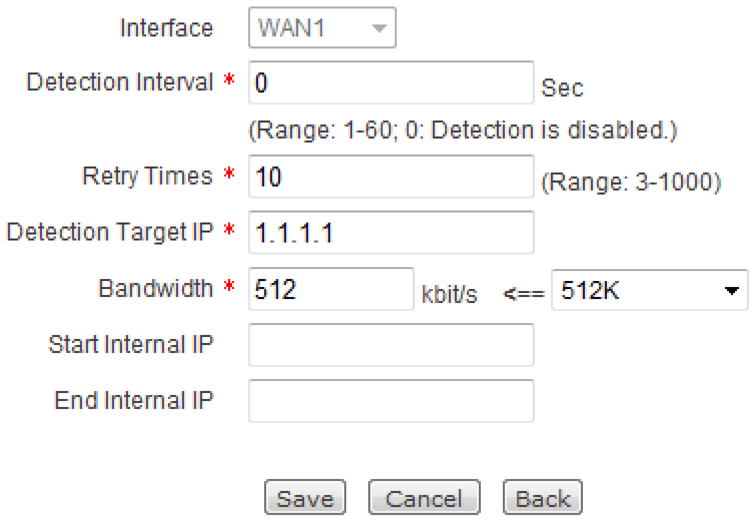
- **Edit an Internet Connection:** To configure or modify the detection related parameters of an Internet connection, click its **Interface** hyperlink or ✎ icon, the related information will be displayed in the **Connection Detection Settings** page. Then configure or modify it, and click the **Save** button.

- **View Load Balancing List:** When you have configured load balancing global settings and connection detection settings, you can view the related configuration and status in the **Load Balancing List**.

- **Refresh Load Balancing List:** Click the **Refresh** button to view the latest information in the list.

5.2.4 Connection Detection Settings

You can configure the connection detection related parameters for each Internet connection as required. The operation is as follows: Go to the **Network > Load Balancing > Load Balancing List** page, and click an Internet connection's **Interface** hyperlink or ✎ icon to go the **Connection Detection Settings** page to configure them.



Interface: WAN1

Detection Interval *: 0 Sec

(Range: 1-60; 0: Detection is disabled.)

Retry Times *: 10 (Range: 3-1000)

Detection Target IP *: 1.1.1.1

Bandwidth *: 512 kbit/s <== 512K

Start Internal IP:

End Internal IP:

Figure 5-15 Connection Detection Settings

- **Interface:** It indicates the name of the WAN interface. It is non-editable.
- **Detection Interval:** It specifies the time interval at which the Wireless Router periodically sends detection packets, one packet at a time. It must be between 1 and 60 seconds, or 0. The default value is 0, which means that connection detection is disabled on the Internet connection.
- **Retry Times:** It specifies the number of retries per detection period. The default value is 3.
- **Detection Target IP:** It specifies the IP address of a detection target device. The Wireless Router will monitor the Internet connection by sending the detection packets to the detection target IP address.
- **Bandwidth:** It specifies the Internet connection's bandwidth, which is provided by your ISP.
- **Start Internal IP** and **End Internal IP:** They specify a range of internal IP addresses. The local computers within the specified range will preferentially use the Internet connection. Refer to **Section 5.2.1.1 Internet Connection Detection Mechanism** for more information.

- **Save:** Click to save your changes.
- **Cancel:** Click to revert to the last saved settings.
- **Back:** Click to go back to the **Load Balancing List** page.

Note

The **Detection Target IP**, **Detection Interval**, and **Retry Times** are connection detection related parameters. Please refer to **Section 5.2.1.1 Internet Connection Detection Mechanism** for more information.

5.2.5 How to Configure Connection Detection Settings

To configure connection detection settings, follow these steps:

Step 1 Go to the **Network > Load Balancing > Load Balancing List** page.

Step 2 Click an Internet connection’s **Interface** hyperlink or ✎ icon to go the **Connection Detection Settings** page.

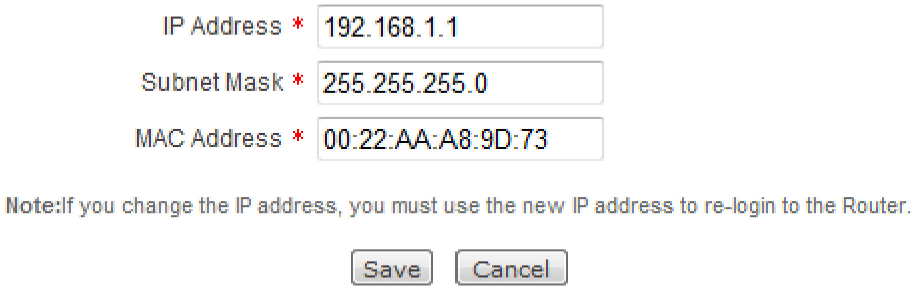
Step 3 Configure detection related parameters (**Detection Target IP**, **Detection Interval**, **Retry Times**, etc.) for the selected Internet connection as required.

Step 4 Click the **Save** button to save your changes.

Step 5 To configure the detection settings for another Internet connection, please repeat the above steps.

5.3 LAN Settings

This section describes the **Network > LAN** page, where you can configure the IP address, subnet mask and MAC address of the Wireless Router's LAN interface.



IP Address * 192.168.1.1

Subnet Mask * 255.255.255.0

MAC Address * 00:22:AA:A8:9D:73

Note: If you change the IP address, you must use the new IP address to re-login to the Router.

Figure 5- 16 LAN Interface Settings

- **IP Address:** It specifies the IP address of the LAN interface.
- **Subnet Mask:** It specifies the subnet mask that defines the range of the LAN.
- **MAC Address:** It specifies the MAC address of the LAN interface. In most cases, please leave the default value.
- **Save:** Click to save your changes.
- **Cancel:** Click to revert to the last saved settings.

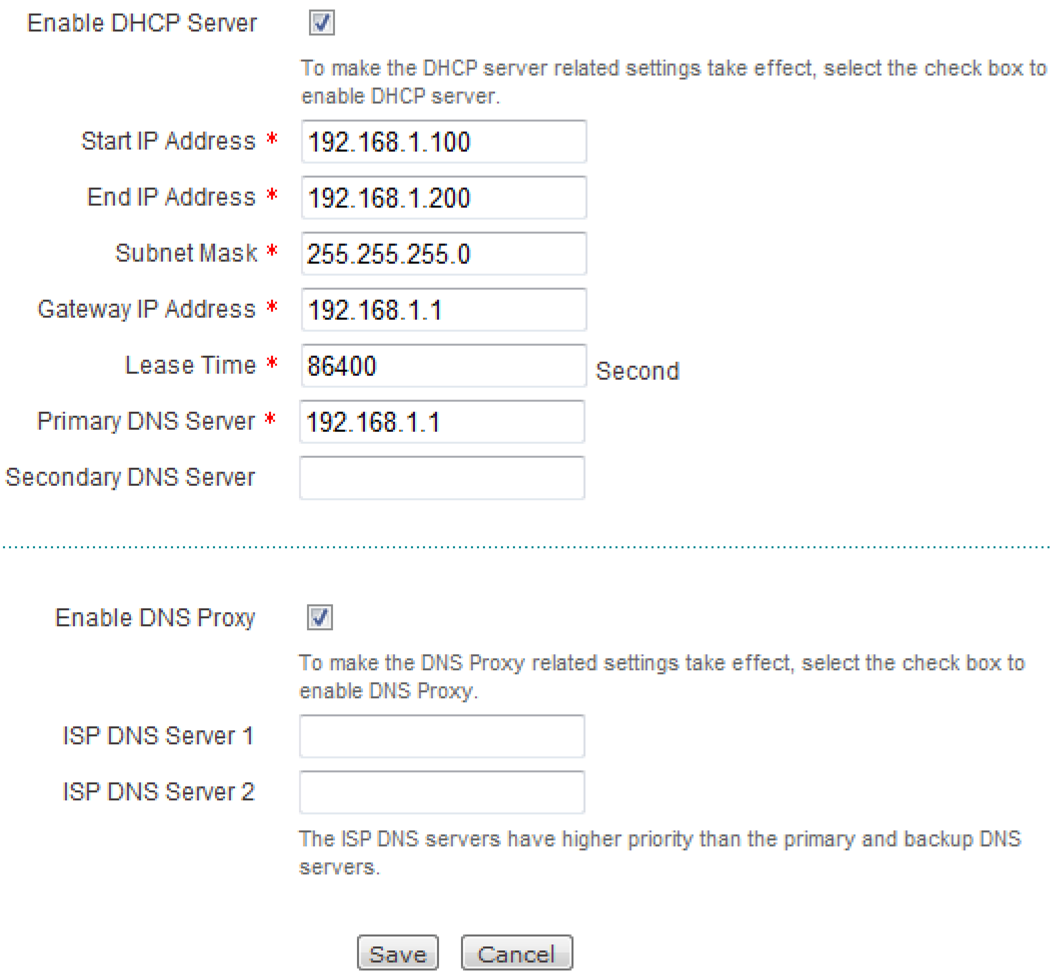
✓ **Note**

If you have changed the IP address of the LAN interface and saved the change, you must use the new IP address to re-login to the Wireless Router.

5.4 DHCP Server

This section describes the **Network > DHCP Server** page, which includes DHCP server settings, static DHCP and DHCP client list.

5.4.1 DHCP Server Settings



Enable DHCP Server ☑

To make the DHCP server related settings take effect, select the check box to enable DHCP server.

Start IP Address *	192.168.1.100	
End IP Address *	192.168.1.200	
Subnet Mask *	255.255.255.0	
Gateway IP Address *	192.168.1.1	
Lease Time *	86400	Second
Primary DNS Server *	192.168.1.1	
Secondary DNS Server		

Enable DNS Proxy ☑

To make the DNS Proxy related settings take effect, select the check box to enable DNS Proxy.

ISP DNS Server 1	
ISP DNS Server 2	

The ISP DNS servers have higher priority than the primary and backup DNS servers.

Figure 5-17 DHCP Server Settings

- **Enable DHCP Server:** It allows you to enable or disable DHCP server. If you want to enable DHCP server on the Wireless Router, please select this check box.
- **Start IP Address:** It specifies the first IP address assigned by the DHCP server. In most cases, this address must be on the same subnet as the Wireless Router’s LAN IP address.
- **End IP Address:** It specifies the last IP address assigned by the DHCP server. In

most cases, this address must be on the same subnet as the Wireless Router’s LAN IP address.

- **Subnet Mask:** It specifies the subnet mask of the IP addresses assigned by the DHCP server. In most cases, this subnet mask must be identical to the Wireless Router’s LAN subnet mask.
- **Default Gateway:** It specifies the IP address of the default gateway for a DHCP client. In most cases, this address must be identical to the Wireless Router’s LAN IP address, that is, the Wireless Router is used as the default gateway for the local computers.
- **Lease Time:** It specifies the length of time (in seconds) during which a DHCP client can use an assigned IP address.
- **Primary DNS Server:** It specifies the IP address of the primary DNS server that is available to a DHCP client.
- **Secondary DNS Server:** It specifies the IP address of the secondary DNS server that is available to a DHCP client.
- **Enable DNS Proxy:** It allows you to enable or disable DNS proxy. If you want to enable DNS proxy on the Wireless Router, please select this check box. When acting as a DNS proxy, the Wireless Router listens for incoming DNS requests on the LAN interface, relays the DNS requests to the current public DNS servers, and replies as a DNS resolver to the requesting local computers.
- **ISP DNS Server 1** and **ISP DNS Server 2:** They specify the IP addresses of the ISP DNS servers.

- **Save:** Click to save your changes.
- **Cancel:** Click to revert to the last saved settings.

✓ **Note**

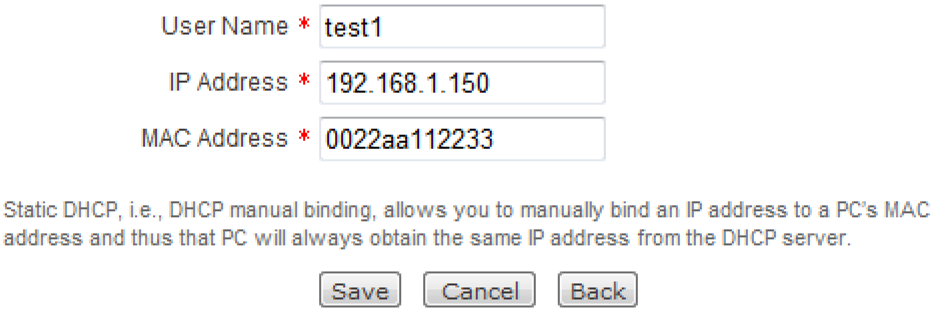
1. If you want a local computer to obtain an IP address and other TCP/IP parameters from the Wireless Router’s built-in DHCP server, please configure the computer to obtain an IP address automatically.
2. If the DNS proxy is enabled on the Wireless Router, in order to use DNS proxy service normally, you need to set the local computers’ primary DNS server to the Wireless Router’s LAN IP address. In addition, if the DHCP server is also enabled on the Wireless Router, the Wireless Router will assign its LAN IP address as the primary DNS server address to the local computers automatically.
3. To ensure that the DNS proxy works well, you must at least specify the primary DNS server provided by your ISP on the Wireless Router.
4. The Wireless Router can act as a DNS proxy server to all local computers. This greatly simplifies configuration of your local computers. For example, there is a LAN

DNS proxy server on which a DNS proxy software is installed (e.g., Wingate), and the local computers use this server as the primary DNS server. Now, the Wireless Router will be used as a new gateway for the local computers. In this case, in order to use DNS proxy service normally, the administrator only need to change the Wireless Router's LAN IP address to the old proxy DNS server's IP address, and enable DNS proxy on the Wireless Router, without having to change each computer.

5.4.2 Static DHCP

The Wireless Router offers static DHCP feature which allows you to manually bind an IP address to a computer's MAC address and thus that computer will always obtain the same IP address from the DHCP server. More specifically, each time the specified computer boots and requests its IP address from the Wireless Router's DHCP server, the DHCP server will recognize the computer's MAC address and always assign the reserved IP address to it.

5.4.2.1 Static DHCP Settings



User Name *	test1
IP Address *	192.168.1.150
MAC Address *	0022aa112233

Static DHCP, i.e., DHCP manual binding, allows you to manually bind an IP address to a PC's MAC address and thus that PC will always obtain the same IP address from the DHCP server.

Figure 5- 18 Static DHCP Settings

- **User Name:** It specifies a unique user name of the DHCP client that wants to be assigned a static IP address.
- **IP Address:** It specifies the IP address that you want to reserve for the DHCP client. It must be a valid IP address within the range of IP addresses assigned by the DHCP server.
- **MAC Address:** It specifies the MAC address of the DHCP client.

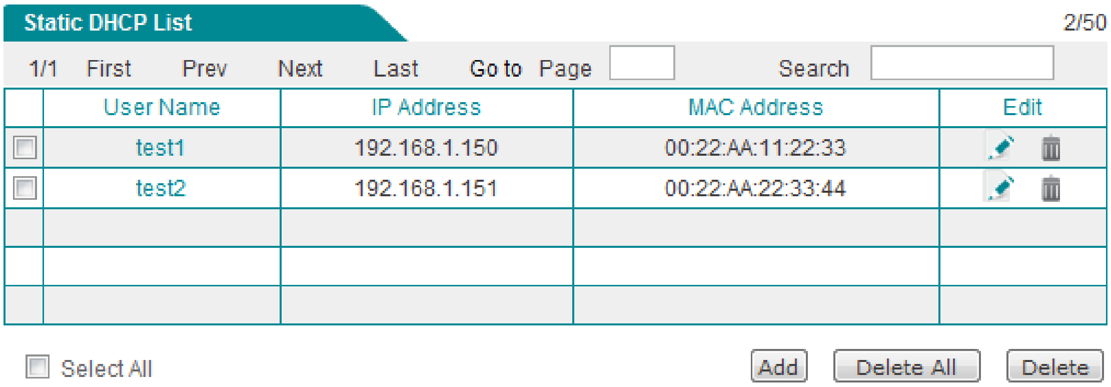
- **Save:** Click to save your changes.
- **Cancel:** Click to revert to the last saved settings.
- **Back:** Click to go back to the **Network > DHCP Server > Static DHCP** page.

Note

1. The reserved IP address must be a valid IP address within the range of IP addresses assigned by the DHCP server.

2. After you have added the static DHCP entry successfully, the Wireless Router will always assign the reserved IP address to the specified computer.

5.4.2.2 Static DHCP List



Static DHCP List 2/50

1/1 First Prev Next Last Go to Page Search

	User Name	IP Address	MAC Address	Edit
□	test1	192.168.1.150	00:22:AA:11:22:33	✎ 🗑
□	test2	192.168.1.151	00:22:AA:22:33:44	✎ 🗑

□ Select All

Figure 5-19 Static DHCP List

- **Add a Static DHCP Entry:** To add a new static DHCP entry, first click the **Add** button to go to the **Static DHCP Settings** page, next configure it, lastly click the **Save** button.

- **View Static DHCP Entry(s):** When you have configured one or more static DHCP entries, you can view them in the **Static DHCP List**.

- **Modify a Static DHCP Entry:** To modify a configured static DHCP entry, click its **User Name** hyperlink or ✎ icon, the related information will be displayed in the **Static DHCP Settings** page. Then modify it, and click the **Save** button.

- **Delete Static DHCP Entry(s):** There are three ways to delete static DHCP entry(s).

  1. To delete a static DHCP entry, directly click its 🗑 icon.

  2. To delete more than one static DHCP entry at a time, select the leftmost check boxes of the static DHCP entries that you want to delete, and then click the **Delete** button.

  3. To delete all the static DHCP entries at a time, directly click the **Delete All** button.

5.4.2.3 How to Add Static DHCP Entries

To add one or more static DHCP entries, follow these steps:

Step 1 Go to the **Network > DHCP Server > Static DHCP** page.

Step 2 Click the **Add** button to go to the **Static DHCP Settings** page, and then specify the **User Name**, **IP Address** and **MAC Address**, lastly click the **Save** button.

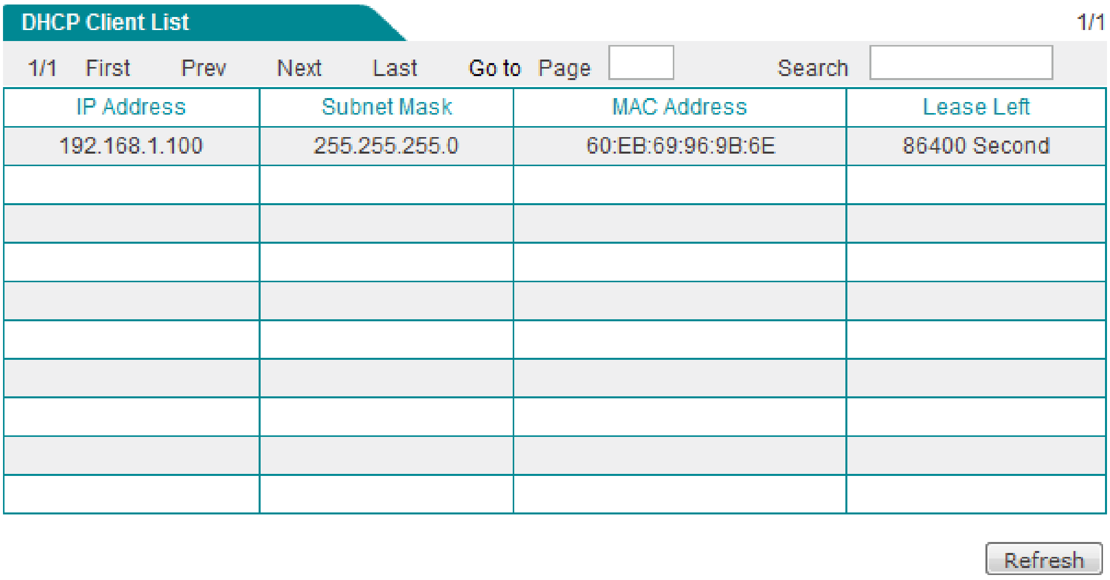
Step 3 Now you can view the static DHCP entry in the **Static DHCP List**.

Step 4 To add another static DHCP entry, please repeat the above steps.

Note

If you want to delete static DHCP entry(s), please follow the ways described in **Section 5.4.2.2 Static DHCP List**.

5.4.3 DHCP Client List



IP Address	Subnet Mask	MAC Address	Lease Left
192.168.1.100	255.255.255.0	60:EB:69:96:9B:6E	86400 Second

Figure 5- 20 DHCP Client List

- **IP Address:** It displays the IP address assigned to the DHCP client.
- **Subnet Mask:** It displays the subnet mask of the current IP address.
- **MAC Address:** It displays the MAC address of the DHCP client.
- **Lease Left:** It displays the time remaining (in seconds) until the current IP address lease expires.

- **Refresh:** Click to view the latest information in the list.

✓ **Note**

The **DHCP Client List** only displays the DHCP clients with dynamically assigned IP addresses. It doesn’t display the DHCP clients specified by the static DHCP entries.

5.4.4 Configuration Example for DHCP

1. Requirements

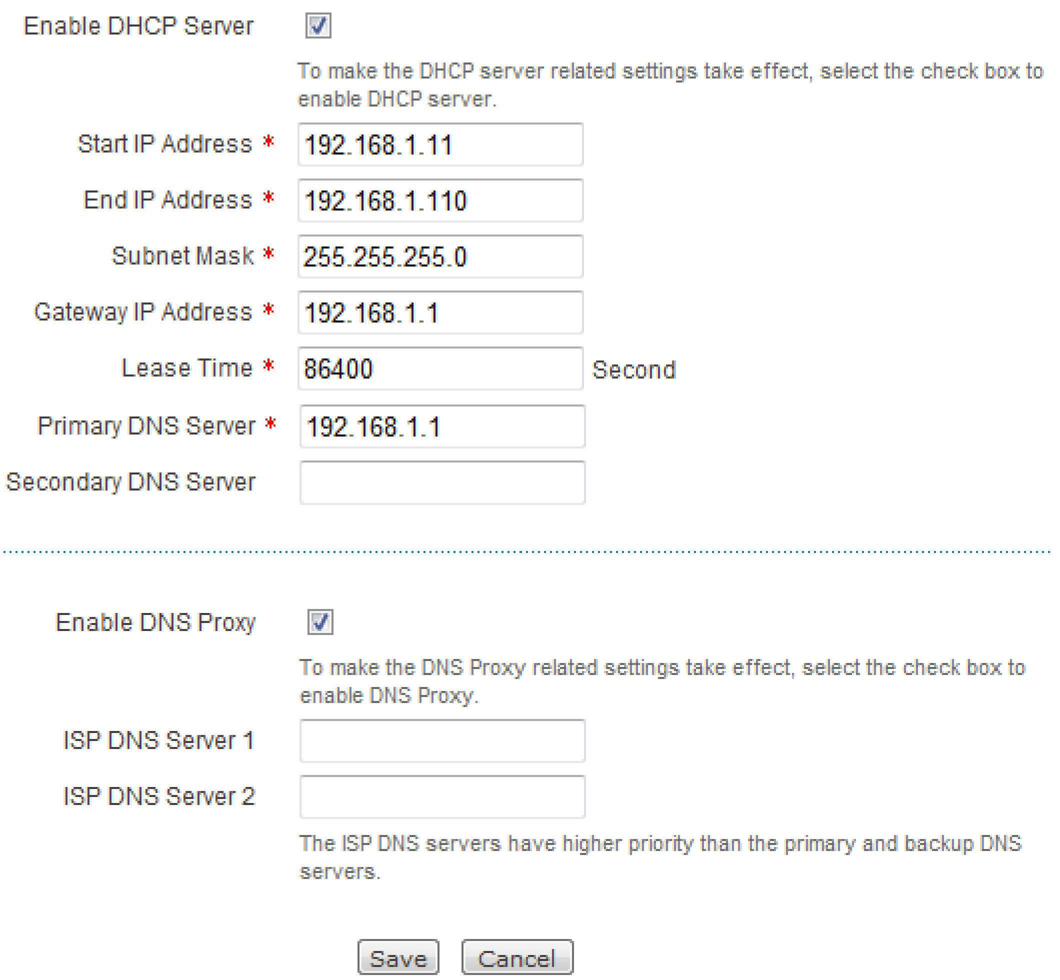
In this example, the Wireless Router acts as a DHCP server to dynamically assign the IP addresses to the clients that reside on the same subnet. The Wireless Router's LAN IP address is 192.168.1.1/24. The start IP address of the DHCP address pool is 192.168.1.11, and the number of addresses is 100.

Besides, there are two computers that must always have the same IP address: one's MAC address is 00:21:85:9B:45:46 and IP address is 192.168.1.15, the other's MAC address is 00:1f:3c:0f:07:f4 and IP address is 192.168.1.16.

2. Configuration Steps

Step 1 Go to the **Network > DHCP Server > DHCP Server Settings** page.

Step 2 As shown in the following figure, select the **Enable DHCP Server** check box, and enter **192.168.1.11** and **192.168.1.110** in the **Start IP Address** and **End IP Address** text boxes respectively. Leave the other parameters at their default values. Then click the **Save** button to save the settings.



Enable DHCP Server ☑

To make the DHCP server related settings take effect, select the check box to enable DHCP server.

Start IP Address * 192.168.1.11

End IP Address * 192.168.1.110

Subnet Mask * 255.255.255.0

Gateway IP Address * 192.168.1.1

Lease Time * 86400 Second

Primary DNS Server * 192.168.1.1

Secondary DNS Server

Enable DNS Proxy ☑

To make the DNS Proxy related settings take effect, select the check box to enable DNS Proxy.

ISP DNS Server 1

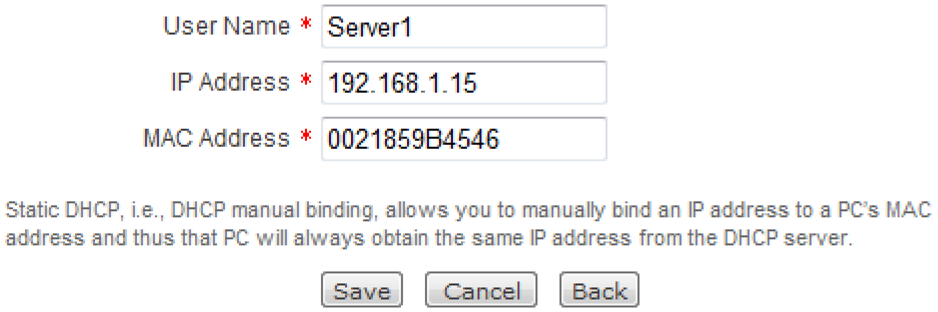
ISP DNS Server 2

The ISP DNS servers have higher priority than the primary and backup DNS servers.

Figure 5- 21 DHCP Server Settings - Example

Step 3 Go to the **Network > DHCP Server > Static DHCP** page.

Step 4 Add the static DHCP entry 1: Click the **Add** button to go to the **Static DHCP Settings** page (see Figure 5- 22), enter **Server1** in the **User Name** text box, **192.168.1.15** in the **IP Address** text box, and **0021859B4546** in the **MAC Address** text box, and then click the **Save** button.



User Name * Server1

IP Address * 192.168.1.15

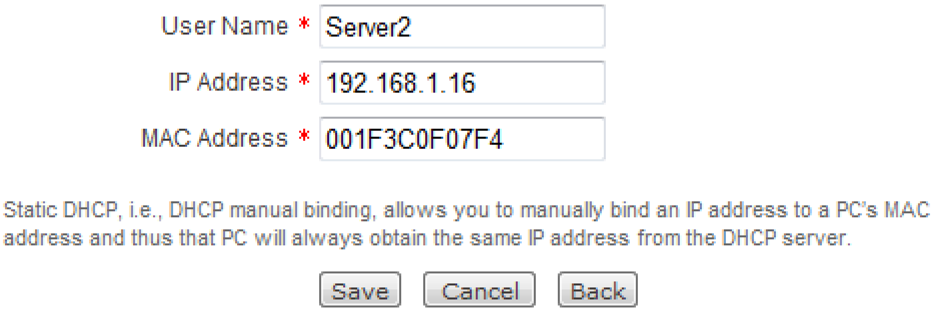
MAC Address * 0021859B4546

Static DHCP, i.e., DHCP manual binding, allows you to manually bind an IP address to a PC's MAC address and thus that PC will always obtain the same IP address from the DHCP server.

Figure 5- 22 Adding the Static DHCP Entry 1 - Example

Step 5 Add the static DHCP entry 2: Click the **Add** button to go to the **Static DHCP Settings** page (see Figure 5- 23), enter **Server2** in the **User Name** text box,

192.168.1.16 in the **IP Address** text box, and **001f3c0f07f4** in the **MAC Address** text box, and then click the **Save** button.



User Name * Server2

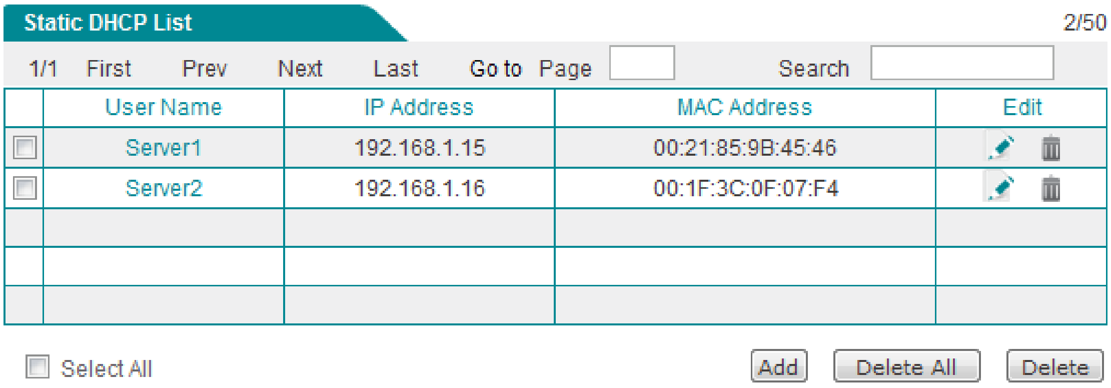
IP Address * 192.168.1.16

MAC Address * 001F3C0F07F4

Static DHCP, i.e., DHCP manual binding, allows you to manually bind an IP address to a PC's MAC address and thus that PC will always obtain the same IP address from the DHCP server.

Figure 5- 23 Adding the Static DHCP Entry 2 - Example

Now you have configured the two static DHCP entries. You can view them in the **Static DHCP List** (see Figure 5- 24), and you can directly click the ✎ icon to modify either of them if desired.



	User Name	IP Address	MAC Address	Edit
□	Server1	192.168.1.15	00:21:85:9B:45:46	✎ 🗑
□	Server2	192.168.1.16	00:1F:3C:0F:07:F4	✎ 🗑

Figure 5- 24 Static DHCP List - Example

5.5 DDNS

This section describes the **Network > DDNS** page. In this page, you can not only configure DDNS parameters, but also view and update DDNS status.

5.5.1 Introduction to DDNS

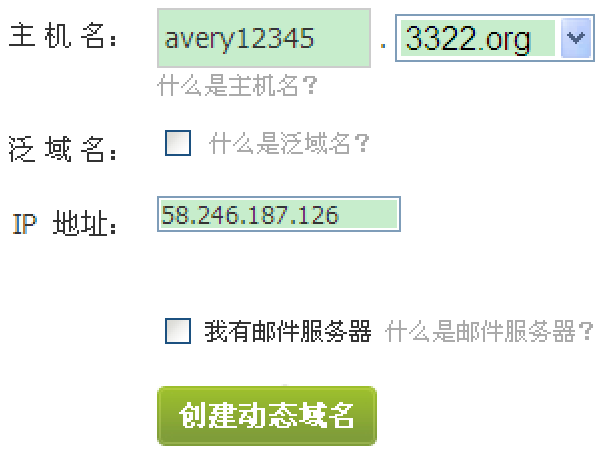
Dynamic Domain Name Service (DDNS) is a service used to map a domain name which never changes to a dynamic IP address which can change quite often. For example, if you have applied for a PPPoE connection with a dynamically assigned IP address from the ISP's PPPoE server, you can use DDNS to allow the external computers to access the Wireless Router by a constant domain name.

In order to use DDNS service, you should apply for a DDNS account from a DDNS service provider. Each DDNS provider offers its own specific network services. The DDNS service provider reserves the right to change, suspend or terminate your use of some or all network services at any time for any reason. The DDNS service providers supported by UTT Technologies Co., Ltd. currently provide free DDNS services, but they may charge for the DDNS services in the future. In this case, UTT Technologies Co., Ltd. will notify you as soon as possible; if you refuse to pay for the services, you will no longer be able to use them. During the free phase, UTT Technologies Co., Ltd. does not guarantee that the DDNS services can meet your requirements and will be uninterrupted, and UTT does not guarantee the timeliness, security and accuracy of the services.

So far, UTT Technologies Co., Ltd. supports only two DDNS service providers: iplink.com.cn and 3322.org. It will successively support other DDNS service providers in the future.

5.5.2 Apply for a DDNS Account

Please login to http://www.3322.org or http://www.utt.com.cn/ddns to apply for a fully qualified domain name (FQDN). This section describes how to apply for a FQDN with suffix of 3322.org from http://www.3322.org.



主 机 名： avery12345 . 3322.org

什么是主机名？

泛 域 名： □ 什么是泛域名？

IP 地址： 58.246.187.126

□ 我有邮件服务器 什么是邮件服务器？

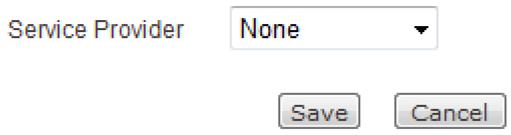
Figure 5- 25 Apply for a DDNS Account from 3322.org

- **Host Name:** It specifies a unique host name of the Wireless Router. The suffix of 3322.org will be appended to the host name to create a fully qualified domain name (FQDN) for the Wireless Router. For example, if the Wireless Router's host name is **test**, then its FQDN is **test.3322.org**; and it allows you to use **test.3322.org** to access the Wireless Router.
- **IP Address:** It specifies the IP address mapped to the registered domain name of the Wireless Router.
- **Register:** Click to register the domain name.

5.5.3 DDNS Settings

5.5.3.1 Disabling DDNS Service

If you want to disable DDNS service, please leave the **Service Provider** at its default value of **None**, see Figure 5- 26.



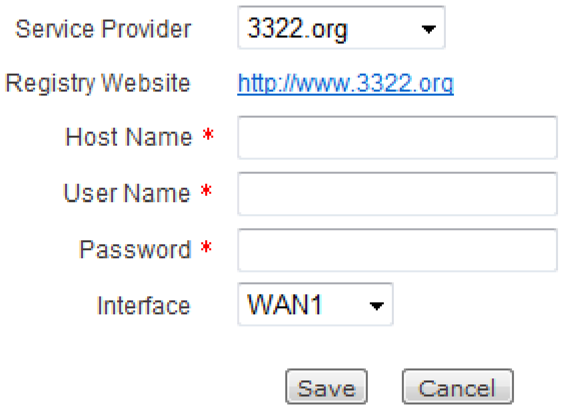
Service Provider None

Figure 5- 26 Disabling DDNS Service

- **Service Provider:** It specifies the DDNS service provider who offers services to the Wireless Router. Here please select **None** to disable DDNS service.
- **Save:** Click to save your changes.

- **Cancel:** Click to revert to the last saved settings.

5.5.3.2 DDNS Service Offered by 3322.org

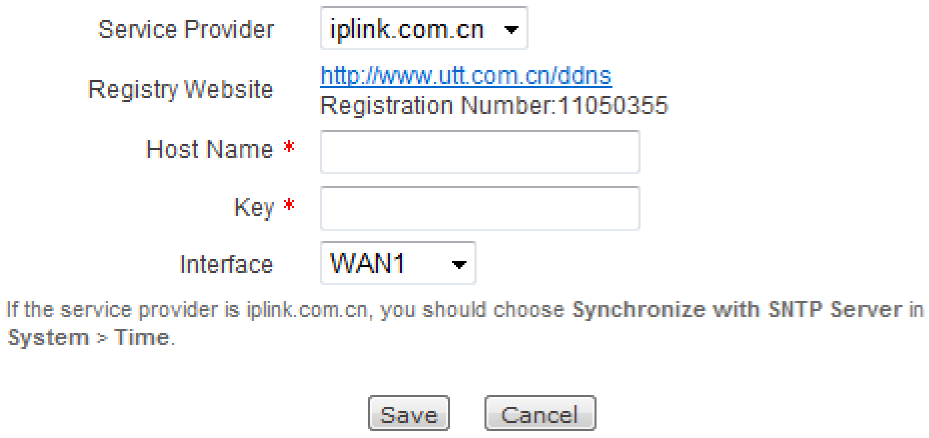


Service Provider	3322.org
Registry Website	http://www.3322.org
Host Name *	
User Name *	
Password *	
Interface	WAN1

Figure 5-27 DDNS Settings Related to 3322.org

- **Service Provider:** It specifies the DDNS service provider who offers services to the Wireless Router. Now the Wireless Router only supports two DDNS service providers: **iplink.com.cn** and **3322.org**. Here please select **3322.org**.
- **Registry Website:** It allows you to click http://www.3322.org to go to this website to register a DDNS account for the Wireless Router.
- **Host Name:** It specifies the host name of the Wireless Router. It must be identical to the host name that you entered when registering the DDNS account on the website http://www.3322.org.
- **User Name:** It specifies the user name that you entered when registering your user account on the website http://www.3322.org.
- **Password:** It specifies the password that you entered when registering your user account on the website http://www.3322.org.
- **Interface:** It specifies the interface on which DDNS service is applied.
- **Save:** Click to save your changes.
- **Cancel:** Click to revert to the last saved settings.

5.5.3.3 DDNS Service Offered by IPLink



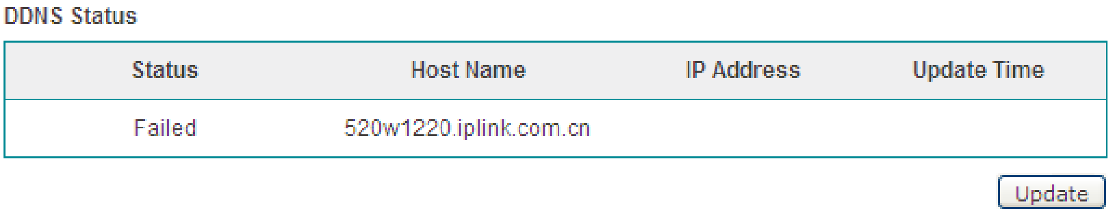
Service Provider	iplink.com.cn ▾
Registry Website	http://www.utt.com.cn/ddns Registration Number:11050355
Host Name *	
Key *	
Interface	WAN1 ▾

If the service provider is iplink.com.cn, you should choose **Synchronize with SNTP Server** in **System > Time**.

Figure 5- 28 DDNS Settings Related to iplink.com.cn

- **Service Provider:** It specifies the DDNS service provider who offers services to the Wireless Router. Now the Wireless Router only supports two DDNS service providers: **iplink.com.cn** and **3322.org**. Here please select **iplink.com.cn**.
- **Registry Website:** It allows you to click   to go to this website to register a DDNS account for the Wireless Router.
- **Registration Number:** It specifies the registration number of the Wireless Router.
- **Host Name:** It specifies the host name of the Wireless Router. It must be identical to the host name that you entered when registering the DDNS account on the website http://www.utt.com.cn/ddns.
- **Key:** It specifies the key that you got when registering the DDNS account on the website http://www.utt.com.cn/ddns.
- **Interface:** It specifies the interface on which DDNS service is applied.
- **Save:** Click to save your changes.
- **Cancel:** Click to revert to the last saved settings.

5.5.4 DDNS Status



DDNS Status

Status	Host Name	IP Address	Update Time
Failed	520w1220.iplink.com.cn		

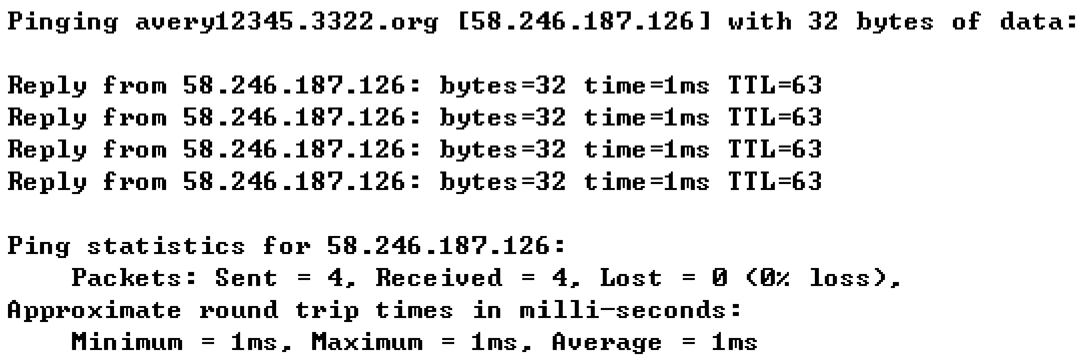
Figure 5- 29 DDNS Status

- **Update:** Click to update DDNS status.

5.5.5 DDNS Verification

To verify whether DDNS is updated successfully, you can use the ping command at the command prompt on the PC, for example: **ping avery12345.3322.org**

If the displayed page is similar to the screenshot below: the domain name is resolved to an IP address successfully (58.246.187.126 in this example), DDNS is updated successfully.



```
Pinging avery12345.3322.org [58.246.187.126] with 32 bytes of data:

Reply from 58.246.187.126: bytes=32 time=1ms TTL=63
Reply from 58.246.187.126: bytes=32 time=1ms TTL=63
Reply from 58.246.187.126: bytes=32 time=1ms TTL=63
Reply from 58.246.187.126: bytes=32 time=1ms TTL=63

Ping statistics for 58.246.187.126:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 1ms, Average = 1ms
```

Note

1. Only when the WAN interface IP address is a public IP address, the Internet users can use its mapped domain name to access the Wireless Router normally.

2. DDNS feature can help you implement VPN tunnels using dynamic IP addresses on the Wireless Router.

5.6 UPnP

This section describes the **Network > UPnP** page.

The Universal Plug and Play (UPnP) is architecture that implements zero configuration networking, that is, it provides automatic IP configuration and dynamic discovery of the UPnP compatible devices from various vendors. A UPnP compatible device can dynamically join a network and work properly.

When you enable UPnP, the Wireless Router allows any local UPnP-enabled device to perform a variety of actions, including retrieving the public IP address, enumerating existing port mappings, and adding or removing port mappings. By adding a port mapping, a UPnP-enabled device opens the related service ports on the Wireless Router to allow outside computers to access.

5.6.1 Enable UPnP

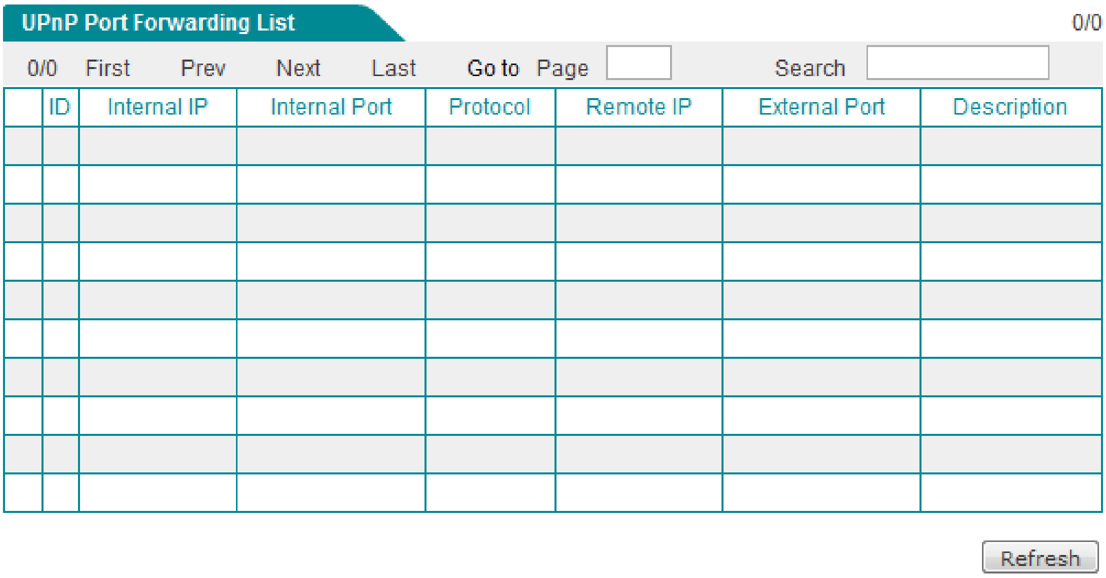
Enable UPnP □ Save

Figure 5- 30 Enable UPnP

- **Enable UPnP:** It allows you to enable or disable UPnP. If you want to enable UPnP, please select this check box.
- **Save:** Click to save your changes.

5.6.2 UPnP Port Forwarding List

The **UPnP Port Forwarding List** lists all the port forwarding entries established using UPnP, see the following figure.



UPnP Port Forwarding List 0/0

0/0 First Prev Next Last Go to Page Search

	ID	Internal IP	Internal Port	Protocol	Remote IP	External Port	Description

Figure 5- 31 UPnP Port Forwarding List

- **ID:** It is used to identify each UPnP port forwarding entry in the list.
- **Internal IP:** It displays the IP address of the local computer.
- **Internal Port:** It displays the service port provided by the local computer.
- **Protocol:** It displays the transport protocol used by the service.
- **Remote IP:** It displays the IP address of the remote computer.
- **External Port:** It displays the external port of the UPnP port forwarding, which is opened for outside user to access.
- **Description:** It displays the description of the UPnP port forwarding entry.
- **Refresh:** Click to view the latest information in the list.

Chapter 6 Wireless

This chapter describes how to configure and use the wireless features of the Wireless Router, which include: basic wireless settings, wireless security settings, wireless MAC address filtering, and advanced wireless settings; and how to view the status of the wireless clients.

6.1 Basic Wireless Settings

This section describes the **Wireless > Basic** page. In this page, you can configure the basic wireless settings of the Wireless Router, which include: enable or disable wireless function, operation mode, SSID, wireless mode, channel, channel width, enable or disable SSID broadcast, and so on.

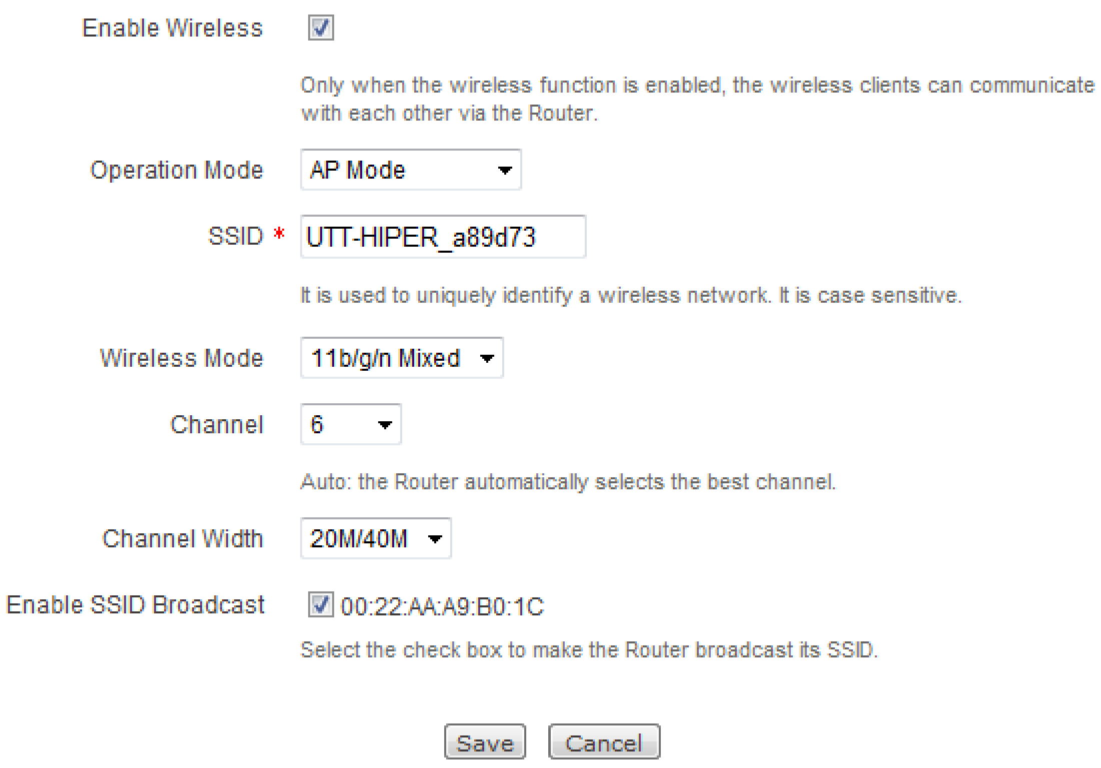
The Wireless Router supports multiple operation modes: AP mode, AP Client mode, and three WDS modes including Repeater mode, Bridge mode and Lazy mode. The following sections describe the basic wireless settings under each operation mode.

✓ **Note**

1. The Wireless Router functions differently under each operation mode. Please select the one that best meets your needs.
2. After you modify the wireless parameters and save the changes, the wireless module will automatically restart. This will disconnect all wireless connections, but won't affect the wired connections.

6.1.1 AP Mode

If you want the Wireless Router to operate in AP mode, please select **AP Mode** from the **Opeartion Mode** drop-down list, see Figure 6-1. In this mode, the Wireless Router can connect to other wireless network devices in AP Client mode, and at at same time it can provide connectivity for wireless clients.



Enable Wireless ☑

Only when the wireless function is enabled, the wireless clients can communicate with each other via the Router.

Operation Mode: AP Mode

SSID *: UTT-HIPER_a89d73

It is used to uniquely identify a wireless network. It is case sensitive.

Wireless Mode: 11b/g/n Mixed

Channel: 6

Auto: the Router automatically selects the best channel.

Channel Width: 20M/40M

Enable SSID Broadcast ☑ 00:22:AA:A9:B0:1C

Select the check box to make the Router broadcast its SSID.

Figure 6-1 Basic Wireless Settings - AP Mode

- **Enable Wireless:** It allows you to enable or disable wireless function. If you select the check box to enable wireless function, wireless clients can connect to the Wireless Router to access the Internet, commnuicate with each other via the Wireless Router, and access the wired network connected to the Wireless Router. Else, the Wireless Router accepts only wired computers and other wired network devices.

- **Operation Mode:** Here please select **AP Mode**.

- **SSID:** The SSID (Service Set Identification) is also known as the wireless network name, which is used to uniquely identify a wireless network. It is case sensitive. It must be identical for all wireless devices in the wireless network.

- **Wireless Mode:** It specifies the wireless standards running on your wireless network. The options are **11g Only**, **11n Only** and **11b/g/n Mixed**.

  - **11g Only:** In allows both 802.11g and 802.11n wireless clients to connect to the Wireless Router at 802.11g data rates with a maximum speed of 54Mbps.
  - **11n Only:** It only allows 802.11n wireless clients to connect to the Wireless Router at 802.11n data rates with a maximum speed of 300Mbps.
  - **11b/g/n Mixed:** It allows 802.11b, 802.11g and 802.11n wireless clients to connect to the Wireless Router at their respective data rates. The maximum speeds are 11Mbps, 54Mbps and 300Mbps respectively.

- **Channel:** It specifies the wireless channel used between the Wireless Router and wireless clients. The valid range is 1 through 11. You can also select **Auto** to let the

Wireless Router automatically select the best channel. If there are multiple wireless routers in your area, please make sure that their channels don't interfere with each other.

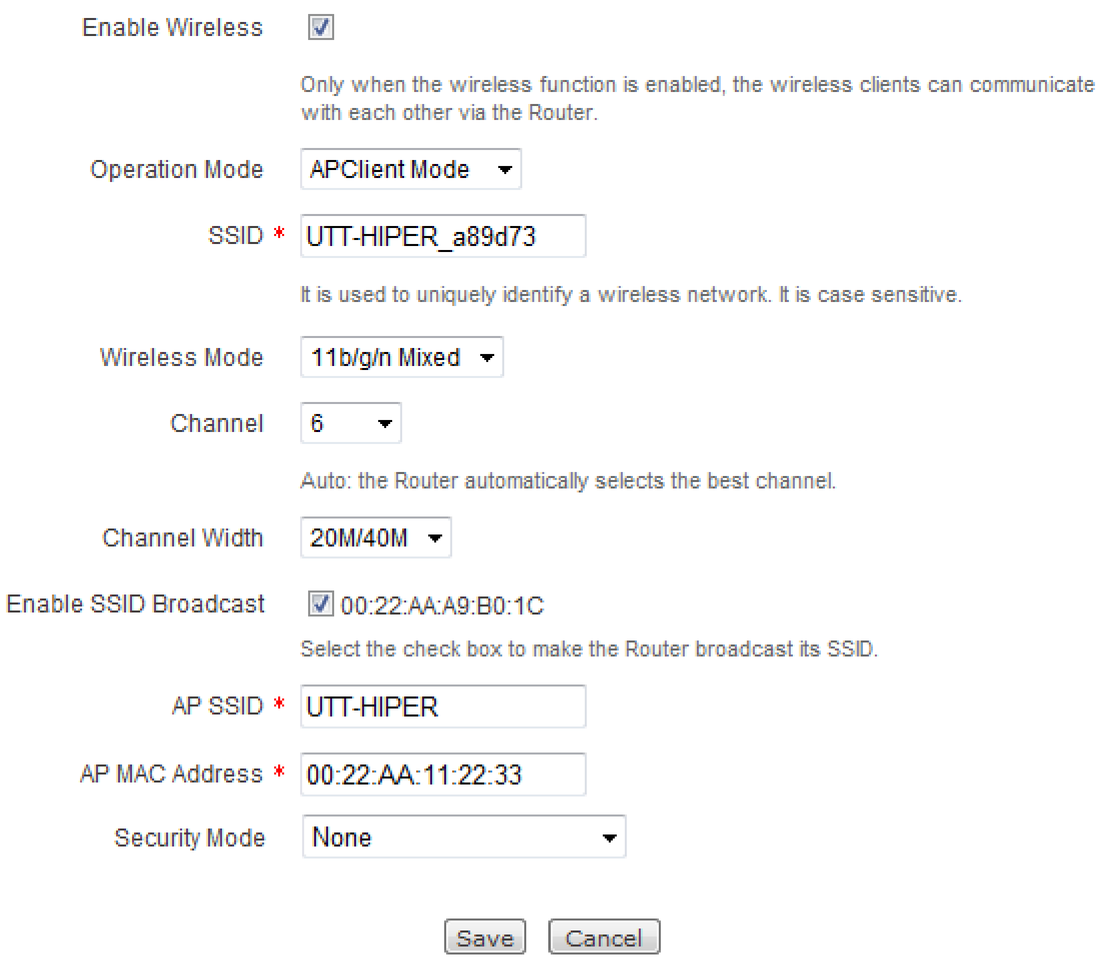
- **Channel Width:** It specifies the range of frequecies used by your wireless network. The options are **20/40M** and **20M**. Note that this parameter can only act on 802.11n wireless clients. 802.11b and 802.11g wireless clients can only use 20MHz channel.
  - **20M/40M:** If you select this option, 802.11n wireless clients will negotiate the channel width with the Wireless Router.
  - **20M:** It you select this option, 802.11n wireless clients will use 20MHz channel.
- **Enable SSID Broadcast:** It allows you to enable or disable SSID broadcast. If you select the check box to enable this feaute, the Wireless Router will periodically broadcast its SSID, so that wireless clients can automatically find it to connect to the Wireless Router and join the wireless network identified by the SSID. However, this feature also makes it easier for hackers to know your SSID and break into your WLAN. It is suggested that you disable this feature to improve security of your WLAN. In this case, you need to manually configure the right SSID for your wireless clients.

- **Save:** Click to save your changes.
- **Cancel:** Click to revert to the last saved settings.

6.1.2 APClient Mode

If you want the Wireless Router to operate in APClient mode, please select **APClient Mode** from the **Opeartion Mode** drop-down list, see Figure 6-2. In this mode, the Wireless Router can connect to a remote network device in AP mode, and at same time it can provide connectivity for wireless clients.

If you configure the APClient Internet connection in the **Start > Setup Wizard**, the system will automatically choose **APClient Mode** as the **Operation Mode**.



Enable Wireless	☑
	Only when the wireless function is enabled, the wireless clients can communicate with each other via the Router.
Operation Mode	APClient Mode
SSID *	UTT-HIPER_a89d73
	It is used to uniquely identify a wireless network. It is case sensitive.
Wireless Mode	11b/g/n Mixed
Channel	6
	Auto: the Router automatically selects the best channel.
Channel Width	20M/40M
Enable SSID Broadcast	☑ 00:22:AA:A9:B0:1C
	Select the check box to make the Router broadcast its SSID.
AP SSID *	UTT-HIPER
AP MAC Address *	00:22:AA:11:22:33
Security Mode	None

Figure 6- 2 Basic Wireless Settings - APClient Mode

- **Operation Mode:** Here please select **APClient Mode**.
- **Enable Wireless**, **SSID**, **Wireless Mode**, **Channel**, **Channel Width**, and **Enable SSID Broadcast**: Refer to **Section 6.1.1 AP Mode** for detailed information.
- **AP SSID**, **AP MAC Address** and **Security Mode:** Refer to **Section 3.3.3.3 APClient Internet Connection Settings** for detailed information.
- **Save:** Click to save your changes.
- **Cancel:** Click to revert to the last saved settings.

Note

In APClient Mode, the **Securtiy Mode**, **Channel** and **Channel Width** configured on the Wireless Router must match those on the remote AP. Otherwise, the Wirelesss Router is unable to connect to the remote AP.

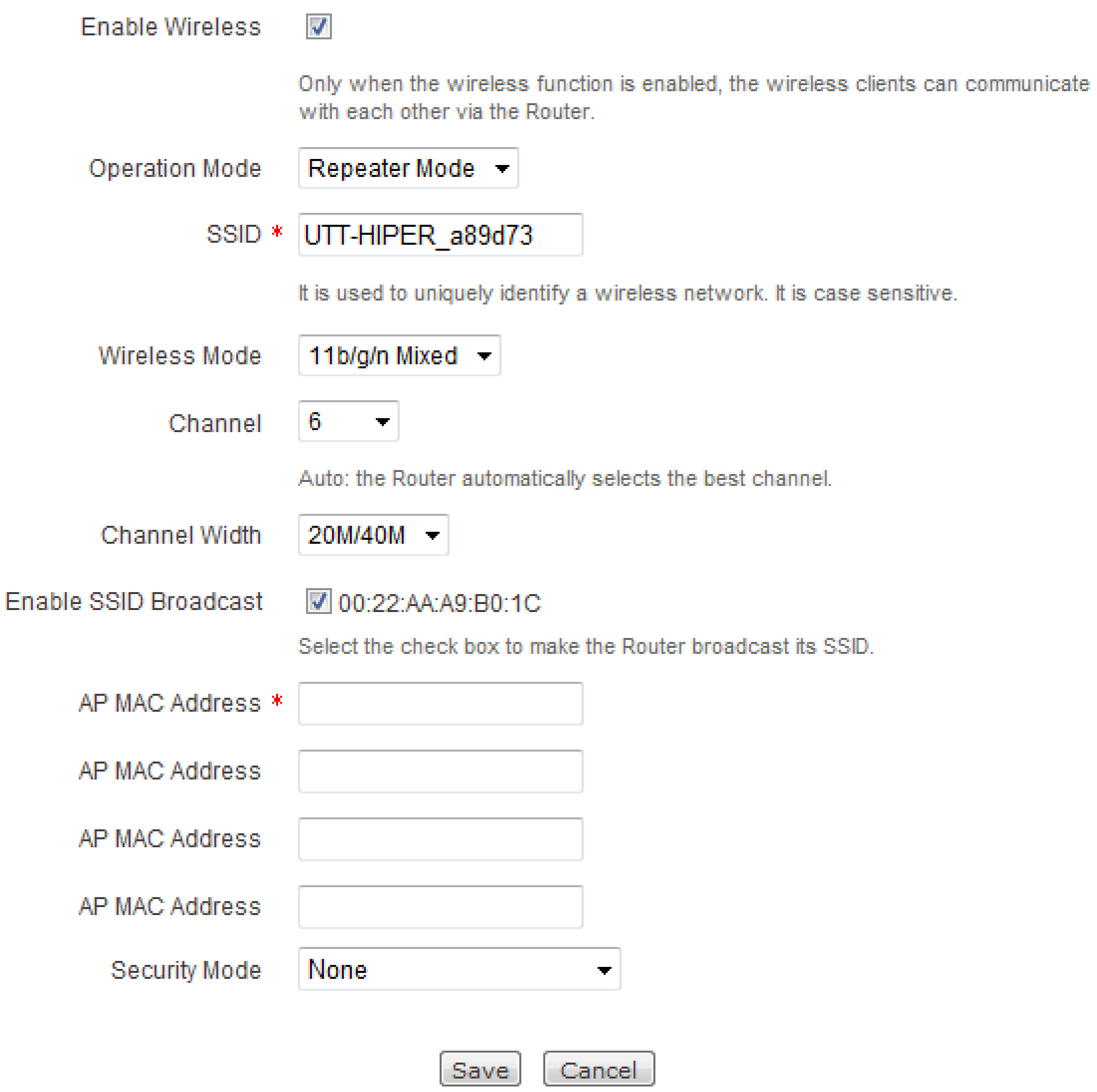
6.1.3 WDS

A Wireless Distribution System (WDS) is a method of interconnecting access points (AP) in a wireless local area network (WLAN) without requiring that they connect through a wired backbone. This feature is usually used to extend the range of the wireless network to reach remote clients.

The Wireless Router can be configured to operate in a WDS mode (**Repeater Mode**, **Bridge Mode** or **Lazy Mode**) that allows it to forward traffic directly to other wireless access points, repeaters or routers. Note that the **Securtiy Mode**, **Channel** and **Channel Width** configured on the Wireless Router must match those on the remote AP, and their LAN IP addresses must be on the same subnet.

6.1.3.1 Repeater Mode

If you want the Wireless Router to operate in repeater mode, please select **Repeater Mode** from the **Opeartion Mode** drop-down list, see Figure 6-3. In this mode, the Wireless Router can connect to other wireless network devices in bridge mode, repeater mode or lazy mode, and at the same time it can provide connectivity for wireless clients.



Enable Wireless ☑

Only when the wireless function is enabled, the wireless clients can communicate with each other via the Router.

Operation Mode: Repeater Mode

SSID *: UTT-HIPER_a89d73

It is used to uniquely identify a wireless network. It is case sensitive.

Wireless Mode: 11b/g/n Mixed

Channel: 6

Auto: the Router automatically selects the best channel.

Channel Width: 20M/40M

Enable SSID Broadcast ☑ 00:22:AA:A9:B0:1C

Select the check box to make the Router broadcast its SSID.

AP MAC Address *:

AP MAC Address:

AP MAC Address:

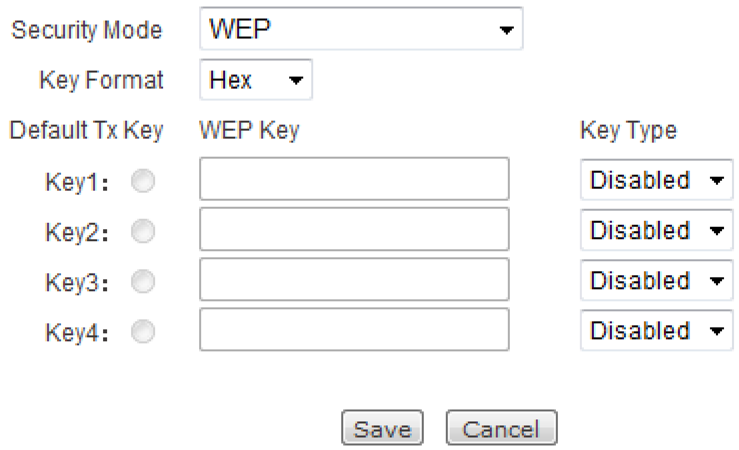
AP MAC Address:

Security Mode: None

Figure 6-3 Basic Wireless Settings - Repeater Mode

- **Operation Mode:** Here please select **Repeater Mode**.
- **Enable Wireless**, **SSID**, **Wireless Mode**, **Channel**, **Channel Width**, and **Enable SSID Broadcast**: Refer to **Section 6.1.1 AP Mode** for detailed information.
- **AP MAC Address:** It specifies the MAC address of the remote AP.
- **Security Mode:** It specifies the security mode to be used by the Wireless Router. There are four options: None, WEP, TKIP and AES.
  - **None:** It means that no security mode will be used.
  - **WEP:** It means that the Wireless Router will use WEP for data encryption, see Figure 6-4.
  - **TKIP:** It means that the Wireless Router will use TKIP for data encryption, see Figure 6-6.
  - **AES:** It means that the Wireless Router will use AES for data encryption, see Figure 6-7.

- **Save:** Click to save your changes.
- **Cancel:** Click to revert to the last saved settings.



Security Mode: WEP

Key Format: Hex

Default Tx Key		WEP Key	Key Type
Key1:	○		Disabled
Key2:	○		Disabled
Key3:	○		Disabled
Key4:	○		Disabled

Figure 6-4 Security Settings - WEP Mode

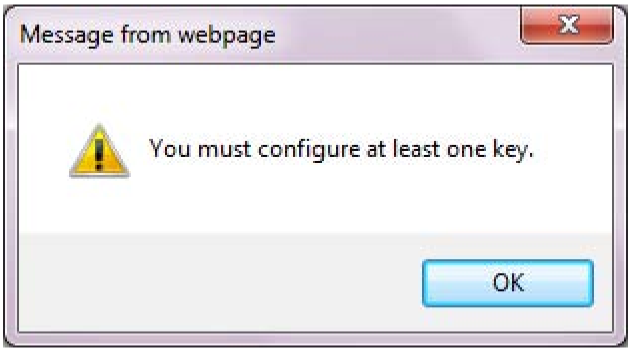
- **Security Mode:** It specifies the security mode to be used by the Wireless Router. Here please select **WEP**.
- **Key Format:** It specifies the format for entering the WEP keys. The options are **Hex** and **ASCII**.
  - **Hex:** Select this option if you want to enter the WEP keys in hexadecimal format. Hexadecimal digits are a set of characters that includes numbers 0 through 9 and letters A through F (or a through f). Hex WEP keys are case insensitive.
  - **ASCII:** Select this option if you want to enter the WEP keys in ASCII format. ASCII WEP keys are case sensitive.
- **Default Tx Key:** It allows you to select one of the WEP keys as the default transmit key to transmit data. All keys can be used to receive data.
- **Key Type:** It allows you to select the size of each key, and it also allows you to disable or enable each key. The options are **Disabled**, **64-bit** and **128-bit**. By default, **Disabled** is selected, which means the key is of no effect.
- **WEP Key:** It allows you to enter a key in one of the **WEP Key** boxes. You can enter up to four WEP keys. You should enter a key according to the **Key Format** and **Key Type** selected.
  - For 64-bit encryption, enter 10 hex characters or 5 ASCII characters.
  - For 128-bit encryption, enter 26 hex characters or 13 ASCII characters.

Note

1. The WEP keys on the Wireless Router must match the WEP keys on the remote wireless device in the same order. That is, WEP Key 1 on the Wireless Router must

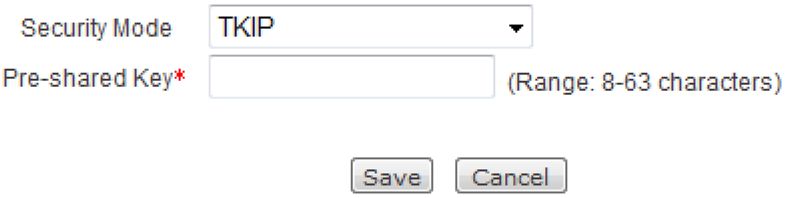
match WEP Key 1 on the remote wireless device, and WEP Key 2, 3 and 4 must match in a similar fashion. However, the two devices can have different Default Tx Keys as long as the keys are in the same order. For example, the Wireless Router can use WEP Key 1 as its Default Tx Key, while the remote wireless device can use WEP Key 3 as its Default Tx Key. The two devices will communicate as long as the Wireless Router's WEP Key 1 is identical to the remote wireless device's WEP Key 1, and the Wireless Router's WEP Key 3 is identical to the remote wireless device's WEP Key 3.

2. You must configure at least one WEP key. Otherwise, the system will pop up a prompt dialog box after you click the **Save** button, see Figure 6- 5.


Message from webpage

You must configure at least one key.

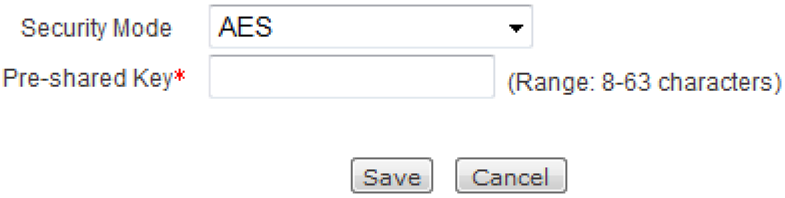
Figure 6- 5 Key Settings Prompt Dialog Box


Security Mode: TKIP

Pre-shared Key*: (Range: 8-63 characters)

Figure 6- 6 Security Settings - TKIP Mode

- **Security Mode:** It specifies the security mode to be used by the Wireless Router. Here please select **TKIP**.
- **Pre-shared Key:** This key serves as seed for generating encryption keys. It must be identical to the remote wireless network device's. It must be between 8 and 63 characters long.


Security Mode: AES

Pre-shared Key*: (Range: 8-63 characters)

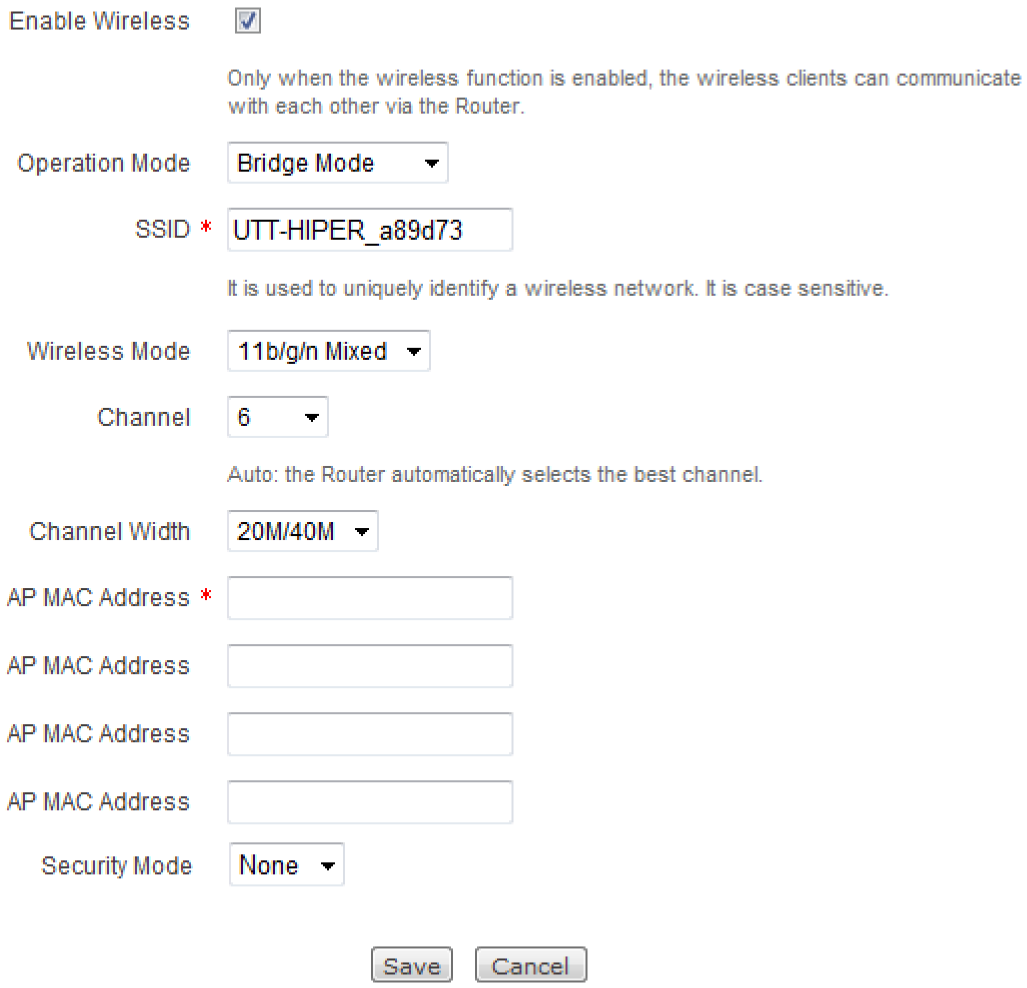
Figure 6- 7 Security Settings - AES Mode

- **Security Mode:** It specifies the security mode to be used by the Wireless Router. Here please select **AES**.

- **Pre-shared Key:** This key serves as seed for generating encryption keys. It must be identical to the remote wireless network device's. It must be between 8 and 63 characters long.

6.1.3.2 Bridge Mode

If you want the Wireless Router to operate in bridge mode, please select **Bridge Mode** from the **Opeartion Mode** drop-down list, see Figure 6-8. In this mode, the Wireless Router can connect to other wireless network devices in repeater mode or lazy mode. However, in this mode wireless clients are unable to connect to the Wireless Router directly.



Enable Wireless ☑

Only when the wireless function is enabled, the wireless clients can communicate with each other via the Router.

Operation Mode: Bridge Mode

SSID *: UTT-HIPER_a89d73

It is used to uniquely identify a wireless network. It is case sensitive.

Wireless Mode: 11b/g/n Mixed

Channel: 6

Auto: the Router automatically selects the best channel.

Channel Width: 20M/40M

AP MAC Address *:

AP MAC Address:

AP MAC Address:

AP MAC Address:

Security Mode: None

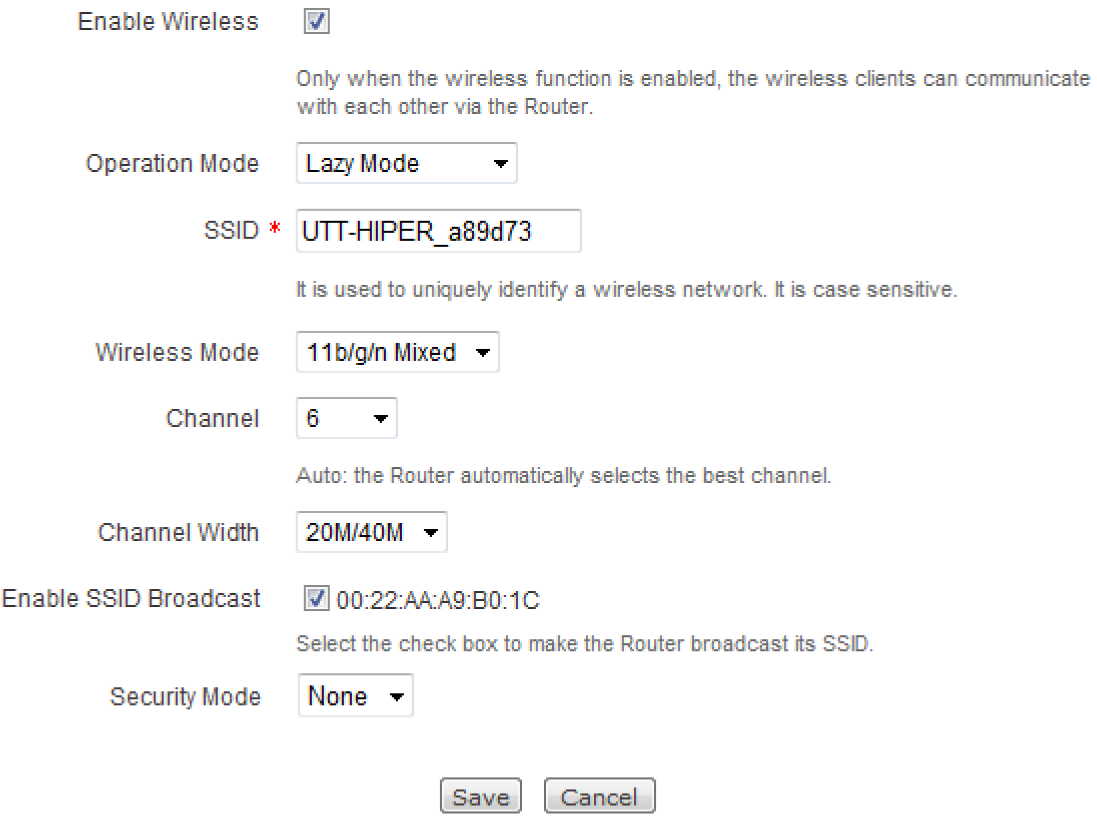
Figure 6-8 Basic Wireless Settings - Bridge Mode

- **Operation Mode:** Here please select **Bridge Mode**.

The other paramters are the same as those of **Repeater Mode**. Please refer to **Section 6.1.3.1 Repeater Mode** for detailed information.

6.1.3.3 Lazy Mode

If you want the Wireless Router to operate in lazy mode, please select **Lazy Mode** from the **Opeartion Mode** drop-down list, see Figure 6- 9. In this mode, the Wireless Router can connect to other wireless network devices in bridge mode or repearter mode; and at the same time it can provide connectivity for wilreless clients.



Enable Wireless ☑

Only when the wireless function is enabled, the wireless clients can communicate with each other via the Router.

Operation Mode: Lazy Mode

SSID *: UTT-HIPER_a89d73

It is used to uniquely identify a wireless network. It is case sensitive.

Wireless Mode: 11b/g/n Mixed

Channel: 6

Auto: the Router automatically selects the best channel.

Channel Width: 20M/40M

Enable SSID Broadcast ☑ 00:22:AA:A9:B0:1C

Select the check box to make the Router broadcast its SSID.

Security Mode: None

Figure 6- 9 Basic Wireless Settings - Lazy Mode

- **Operation Mode:** Here please select **Laze Mode**.

  The other paramters are the same as those of **Repeater Mode**. Please refer to **Section 6.1.3.1 Repeater Mode** for detailed information.

6.1.4 Configuration Example for WDS

1. Requirements

In this example (see Figure 6- 10), there are two Wireless Routers: Router A and Router B. The Wireless Router A operates in Bridge Mode, its SSID is UTT123, security mode is TKIP, pre-shared key is 123456789 and LAN IP address is 192.168.1.1/25. The Wireless Router B's IP address is 192.168.1.2/25. We want the two Routers to communicate with each other wirelessly.

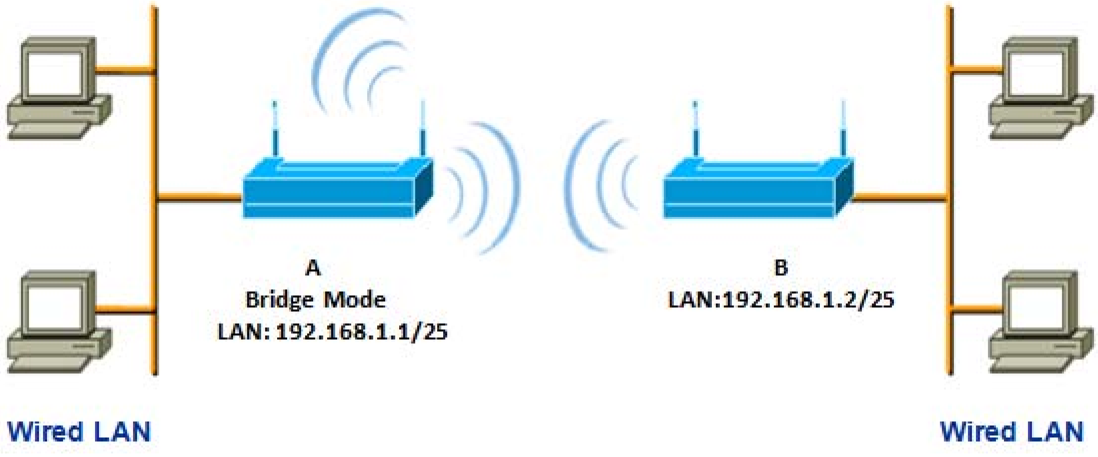


Figure 6- 10 Configuration Example for WDS - Network Topology

2. Configuration and Verification

To connect the Wireless Router A to the Wireless Router B properly, the Wireless Router B's operation mode may be Lazy Mode or Repeater Mode (here we take Lazy Mode for example), its SSID, security mode and pre-shared key must be the same as those of the Wireless Router A.

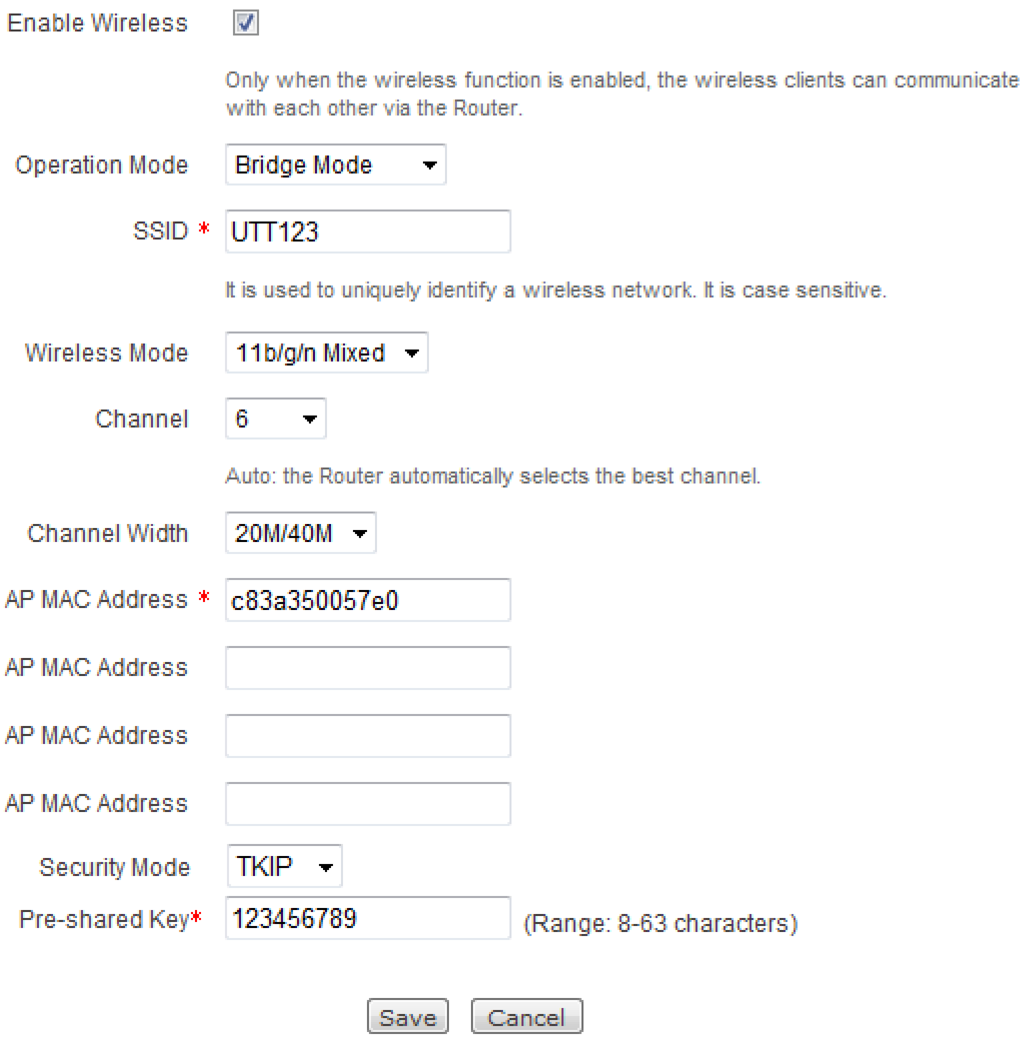
Besides, we leave the other parameters at their default values on both Routers.

1） Configuring the Wireless Router A

The following figure shows the detailed settings on the Wireless Router A.

✓ **Note**

Please enter the Wireless Router B's MAC address (c83a350057e0 in this example) in the first **AP MAC Address** text box on the Wireless Router A.



Enable Wireless ☑

Only when the wireless function is enabled, the wireless clients can communicate with each other via the Router.

Operation Mode: Bridge Mode

SSID *: UTT123

It is used to uniquely identify a wireless network. It is case sensitive.

Wireless Mode: 11b/g/n Mixed

Channel: 6

Auto: the Router automatically selects the best channel.

Channel Width: 20M/40M

AP MAC Address *: c83a350057e0

AP MAC Address:

AP MAC Address:

AP MAC Address:

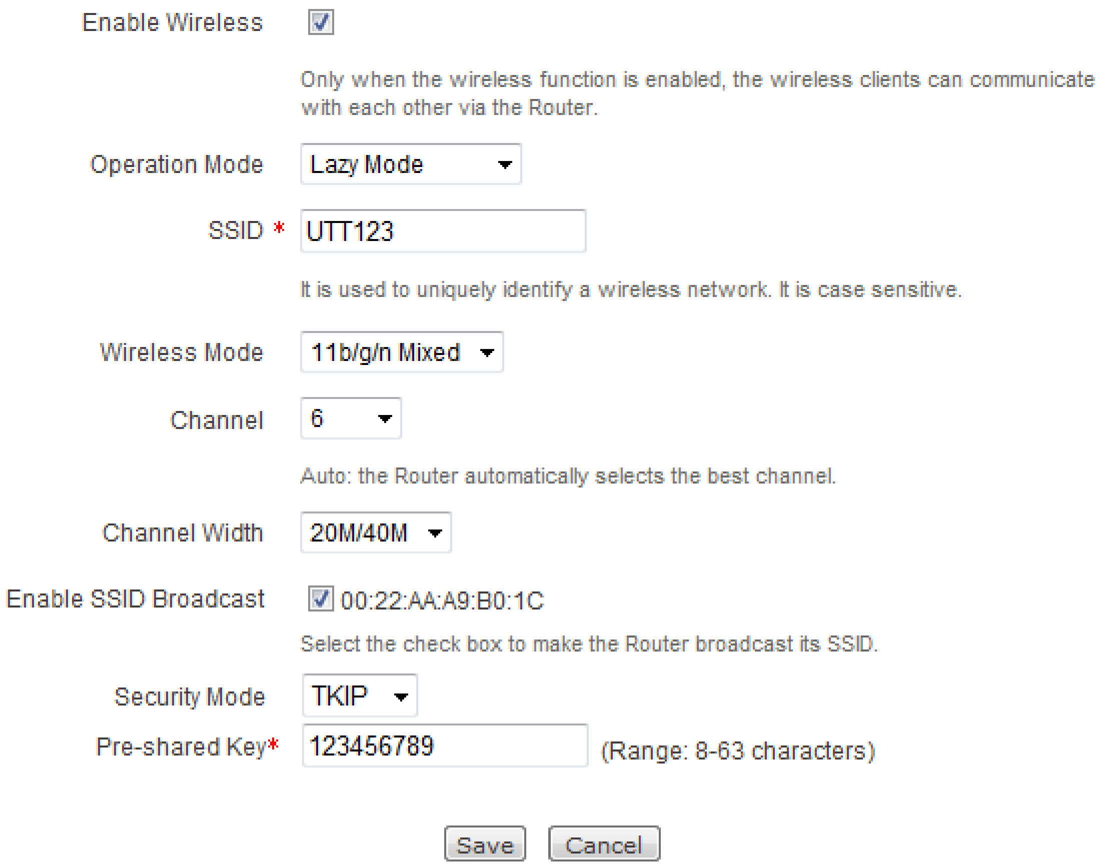
Security Mode: TKIP

Pre-shared Key*: 123456789 (Range: 8-63 characters)

Figure 6- 11 Configuration Example for WDS - Configuring the Wireless Router A

2） Configuring the Wireless Router B

The following figure shows the detailed settings on the Wireless Router B.



Enable Wireless ☑

Only when the wireless function is enabled, the wireless clients can communicate with each other via the Router.

Operation Mode: Lazy Mode

SSID *: UTT123

It is used to uniquely identify a wireless network. It is case sensitive.

Wireless Mode: 11b/g/n Mixed

Channel: 6

Auto: the Router automatically selects the best channel.

Channel Width: 20M/40M

Enable SSID Broadcast ☑ 00:22:AA:A9:B0:1C

Select the check box to make the Router broadcast its SSID.

Security Mode: TKIP

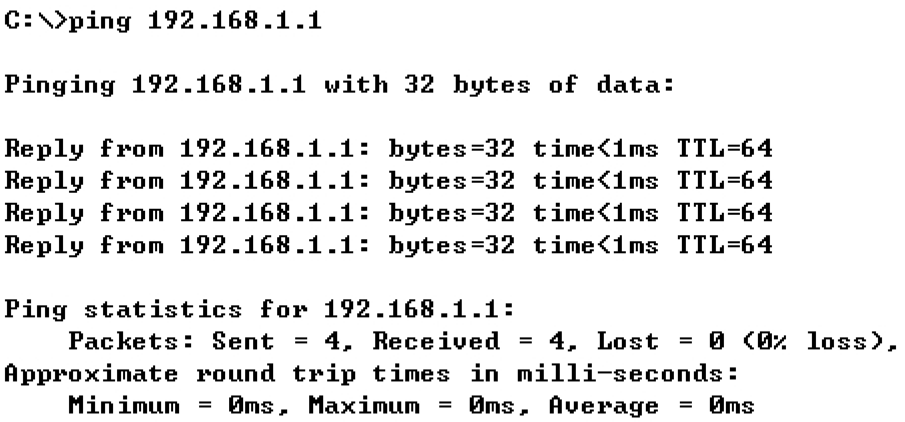
Pre-shared Key*: 123456789 (Range: 8-63 characters)

Figure 6- 12 Configuration Example for WDS - Configuring the Wireless Router B

3） Verifying Connectivity between the Two Routers

To verify connectivity between the two Routers, you can use the ping command at the command prompt on the Wireless Router B: **Ping 192.168.1.1**

If the displayed page is similar to the screenshot below, the connection between the two Routers has been established.



```
C:\>ping 192.168.1.1

Pinging 192.168.1.1 with 32 bytes of data:

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

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

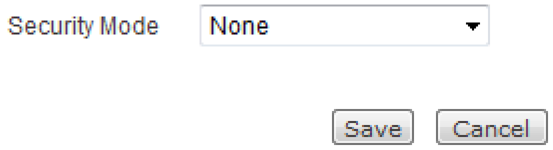
Figure 6- 13 Configuration Example for WDS - Verifying Connectivity

6.2 Wireless Security Settings

This section describes the **Wireless > Security** page.

The Wireless Router provides four security mode options including **None**, **WEP**, **WPA/WPA2**, and **WPA-PSK/WPA2-PSK**. If you want an open network without wireless security, keep the default value of **None**.

6.2.1 Disabling Wireless Security

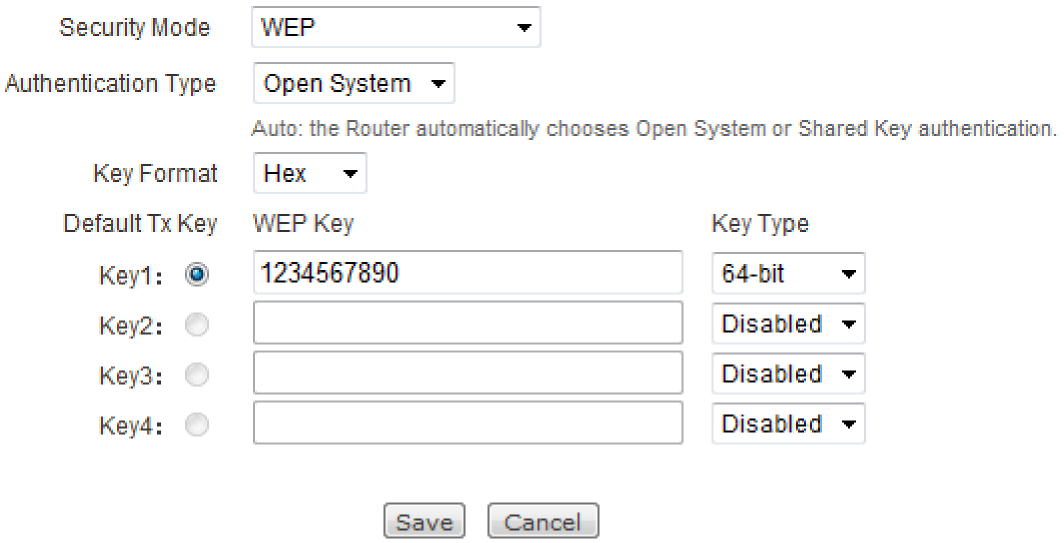


Security Mode: None

Figure 6- 14 Disabling Wireless Security

- **Security Mode:** It specifies the security mode that you want to use on your wireless network. Here please select **None** to disable wireless securtiy.
- **Save:** Click to save you changes.
- **Cancel:** Click to revert to the last saved settings.

6.2.2 Wireless Security Settings – WEP



Security Mode: WEP

Authentication Type: Open System

Auto: the Router automatically chooses Open System or Shared Key authentication.

Key Format: Hex

Default Tx Key		WEP Key	Key Type
Key1:	●	1234567890	64-bit
Key2:	○		Disabled
Key3:	○		Disabled
Key4:	○		Disabled

Figure 6- 15 Wireless Security Settings - WEP

- **Security Mode:** It specifies the security mode that you want to use on your wireless network. Here please select **WEP**. WEP is the basic encryption mode which is not as secure as WPA.

- **Authentication Type:** It allows you to select the authentication type under **WEP** security mode. The Wireless Router must authenticate a wireless client before the client can join the wireless network. There are three options: **Auto**, **Open System** and **Shared Key**.

  - **Auto:** It allows either **Open System** or **Shared Key** authentication to be used. The Wireless Router will automatically choose the authentication type.
  - **Open System:** It allows any wireless client regardless of its WEP keys to authenticate and attempt to associate with the Wireless Router. However, even if a client can complete authentication and associate with the Wireless Router, the client cannot send or receive data from the Wireless Router unless the client has the correct WEP key.
  - **Shared Key:** It requires that the wireless client and the Wireless Router have the same WEP key to authenticate. Without the correct key, authentication will fail and the client won't be allowed to associate with the Wireless Router.

- **Key Format:** It specifies the format for entering the WEP keys. The options are **Hex** and **ASCII**.

  - **Hex:** Select this option if you want to enter the WEP keys in hexadecimal format. Hexadecimal digits are a set of characters that includes numbers 0 through 9 and letters A through F (or a through f). Hex WEP keys are case insensitive.
  - **ASCII:** Select this option if you want to enter the WEP keys in ASCII format. ASCII WEP keys are case sensitive.

- **Default Tx Key:** It allows you to select one of the WEP keys as the default transmit key to transmit data. All keys can be used to receive data.

- **WEP Key:** It allows you to enter a key in one of the **WEP Key** boxes. You can enter up to four WEP keys. You should enter a key according to the **Key Format** and **Key Type** selected.

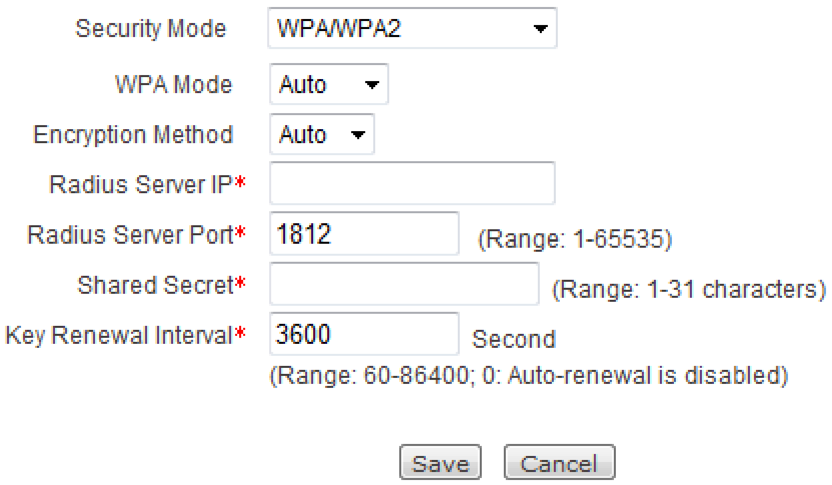
  - For 64-bit encryption, enter 10 hex characters or 5 ASCII characters.
  - For 128-bit encryption, enter 26 hex characters or 13 ASCII characters.

- **Key Type:** It allows you to select the size of each key, and it also allows you to disable or enable each key. The options are **Disabled**, **64-bit** and **128-bit**. By default, **Disabled** is selected, which means the key is of no effect.

- **Save:** Click to save your changes.

- **Cancel:** Click to revert to the last saved settings.

6.2.3 Wireless Security Settings - WPA/WPA2



Security Mode	WPA/WPA2	
WPA Mode	Auto	
Encryption Method	Auto	
Radius Server IP*		
Radius Server Port*	1812	(Range: 1-65535)
Shared Secret*		(Range: 1-31 characters)
Key Renewal Interval*	3600	Second
	(Range: 60-86400; 0: Auto-renewal is disabled)	

Figure 6- 16 Wireless Security Settings - WPA/WPA2

- **Security Mode:** It specifies the security mode that you want to use on your wireless network. Here please select **WPA/WPA2** to use WPA mode, WPA2 mode or both. In WPA or WPA2 mode, the Wireless Router uses an external RADIUS server to authenticate wireless clients.

- **WPA Mode:** It specifies the WPA mode that you want to use on your wireless network. The options are **Auto**, **WPA** and **WPA2**.
  - **Auto:** It allows both WPA and WPA2 clients to connect to the Wireless Router.
  - **WPA:** It only allows WPA clients to connect to the Wireless Router.
  - **WPA2:** It only allows WPA2 clients to connect to the Wireless Router.

- **Encrption Method:** It specifies the encrytion method used for data encryption. The options are **Auto**, **TKIP** and **AES**.
  - **Auto:** It means that the Wireless Router will automatically choose to use TKIP or AES for data encryption.
  - **TKIP:** It means that the Wireless Router will use TKIP for data encryption.
  - **AES:** It means that the Wireless Router will use AES for data encryption.

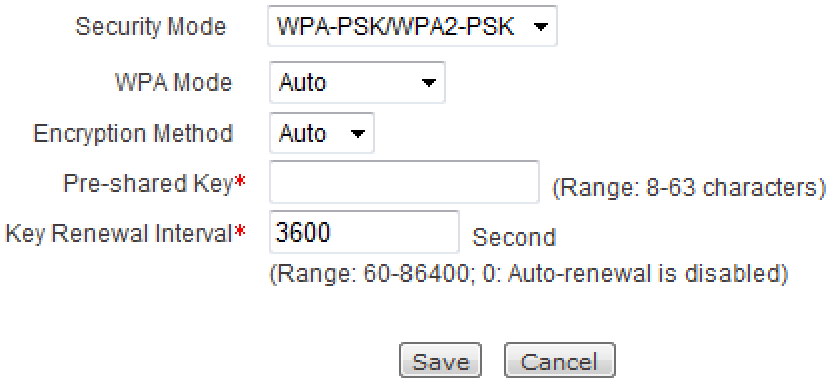
- **RADIUS Server IP:** It specifies the IP address of the RADIUS server, which is used to authenticate the wireless clients.

- **RADIUS Server Port:** It specifies the UPD port number of the RADIUS server. The vaild range is 1 to 65535, and the default value is 1812.

- **Shared Secret:** It specifies the shared secret key to be used for authentication between the Wireless Router and the RADIUS server. It must be the same on both the Wireless Router and the RADIUS server.

- **Key Renewal Interval:** It specifies how often the WPA group key changes. The valid range is 60-86400 or 0, and the default value is 3600 seconds. Enter 0 to disable automatic renewal.
- **Save:** Click to save your changes.
- **Cancel:** Click to revert to the last saved settings.

6.2.4 Wireless Security Settings - WPA-PSK/WPA2-PSK



Security Mode: WPA-PSK/WPA2-PSK

WPA Mode: Auto

Encryption Method: Auto

Pre-shared Key*: (Range: 8-63 characters)

Key Renewal Interval*: 3600 Second

(Range: 60-86400; 0: Auto-renewal is disabled)

Figure 6- 17 Wireless Security Settings - WPA-PSK/WPA2-PSK

- **Security Mode:** It specifies the security mode that you want to use on your wireless network. Here please select **WPA-PSK/WPA2-PSK** to use WPA-PSK mode, WPA2-PSK mode or both. This mode intends for the wireless network that doesn't have a RADIUS server. In this mode, the Wireless Router uses the pre-shared key that is manulally entered to generate encryption keys.
- **WPA Mode:** It specifies the WPA mode that you want to use on your wireless network. The options are **Auto**, **WPA-PSK** and **WPA2-PSK**.
  - **Auto:** It allows both WPA and WPA2 clients to connect to the Wireless Router.
  - **WPA-PSK:** It only allows WPA clients to connect to the Wireless Router.
  - **WPA2-PSK:** It only allows WPA2 clients to connect to the Wireless Router.
- **Encrption Method:** It specifies the encrytion method used for data encryption. The options are **Auto**, **TKIP** and **AES**.
  - **Auto:** It means that the Wireless Router will automatically choose encryption method for each wireless client.
  - **TKIP:** It means that the Wireless Router will use TKIP for data encryption.
  - **AES:** It means that the Wireless Router will use AES for data encryption.
- **Pre-shared Key:** This key serves as seed for generating encryption keys. The

wireless clients also need to be configurd with the same pre-shared key. It must be between 8 and 63 characters long.

- **Key Renewal Interval:** It specifies how often the WPA group key changes. The valid range is 60-86400 or 0, and the default value is 3600 seconds. Enter 0 to disable automatic renewal.

- **Save:** Click to save your changes.

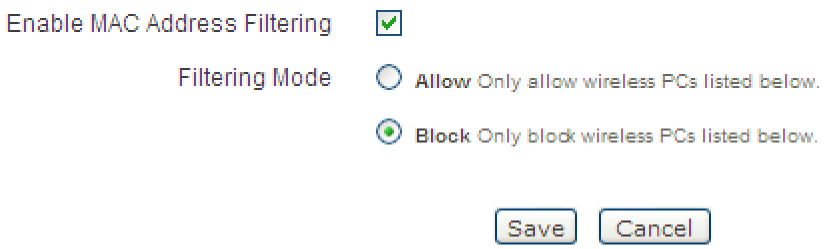
- **Cancel:** Click to revert to the last saved settings.

6.3 Wireless MAC Address Filtering

This section describes the **Wireless > MAC Filtering** page.

The MAC address filtering is used to filter the wireless clients based on their MAC addresses. With this feature, you can either allow or block specific wireless clients to connect to the Wireless Router.

6.3.1 MAC Address Filtering Global Settings



Enable MAC Address Filtering ☑

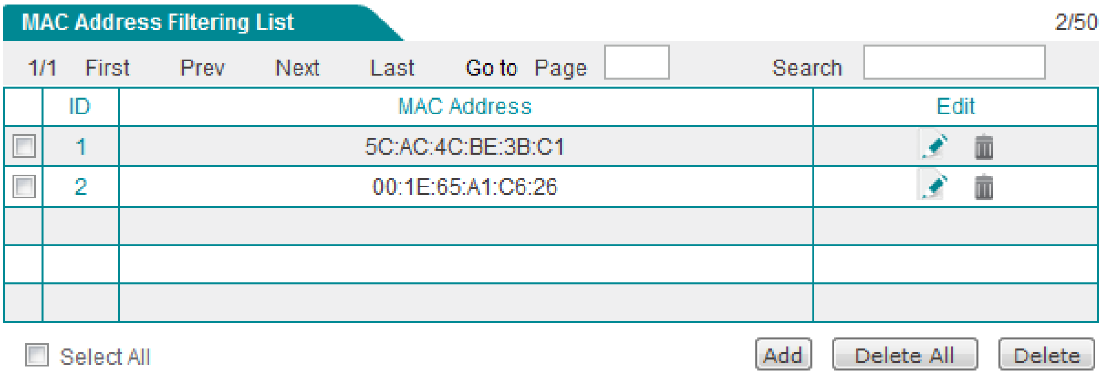
Filtering Mode ○ **Allow** Only allow wireless PCs listed below.

● **Block** Only block wireless PCs listed below.

Figure 6-18 MAC Address Filtering Global Settings

- **Enable MAC Address Filtering:** It allows you to enable or disable MAC address filtering. If you want to enable MAC address filtering, please select the check box.
- **Filtering Mode:** It specifies the mode of MAC address filtering.
  - **Allow:** Choose this option to allow the wireless clients with the MAC addresses listed in the **MAC Address Filtering List** to connect to the Wireless Router, but block all other wireless clients.
  - **Deny:** Choose this option to block the wireless clients with the MAC addresses listed in the **MAC Address Filtering List** from connecting to the Wireless Router, but allow all other wireless clients.
- **Save:** Click to save your changes.
- **Cancel:** Click to revert to the last saved settings.

6.3.2 MAC Address Filtering List



MAC Address Filtering List 2/50

1/1 First Prev Next Last Go to Page □ Search □

	ID	MAC Address	Edit
□	1	5C:AC:4C:BE:3B:C1	✎ 🗑
□	2	00:1E:65:A1:C6:26	✎ 🗑

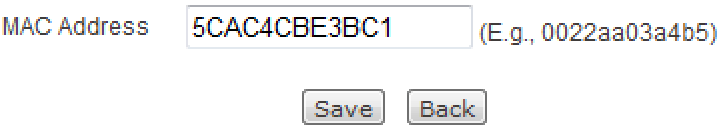
□ Select All

Figure 6-19 MAC Address Filtering List

- **Add a MAC Address Filtering Entry:** To add a new MAC address filtering entry, first click the **Add** button to go to the **MAC Address Filtering Settings** page, next configure it, lastly click the **Save** button.
- **View MAC Address Filtering Entry(s):** When you have configured one or more MAC address filtering entries, you can view them in the **MAC Address Filtering List**.
- **Modify a MAC Address Filtering Entry:** To modify a configured MAC address filtering entry, click its **ID** hyperlink or ✎ icon, the related information will be displayed in the setup page. Then modify it, and click the **Save** button.
- **Delete MAC Address Filtering Entry(s):** There are three ways to delete MAC address filtering entry(s).

  1. To delete a MAC address filtering entry, directly click its 🗑 icon.
  2. To delete more than one MAC address filtering entry at a time, select the leftmost check boxes of the entries that you want to delete, and then click the **Delete** button.
  3. To delete all the MAC address filtering entries at a time, directly click the **Delete All** button.

6.3.3 MAC Address Filtering Settings



MAC Address 5CAC4CBE3BC1 (E.g., 0022aa03a4b5)

Figure 6-20 MAC Address Filtering Settings

- **MAC Address:** It specifies the MAC address of the wireless client that you want to allow or block.
- **Save:** Click to save your changes.
- **Back:** Click to go back to the **Wireless > MAC Filtering** page.

6.3.4 How to Configure MAC Address Filtering

To configure MAC address filtering, follow these steps:

Step 1 Go to the **Wireless > MAC Filtering** page.

Step 2 Click the **Add** button to go to **MAC Address Filtering Settings** page, next enter the MAC address of the wireless client that you want to control in the **MAC Address** text box.

Step 3 Now you can view the MAC address filtering entry in the **MAC Address Filtering List**.

Step 4 Continue to configure other MAC address filtering entries.

Step 5 If you want to allow the wireless clients with the MAC addresses listed in the **MAC Address Filtering List** to connect to the Wireless Router, but block all other wireless clients, select the **Enable MAC Address Filtering** check box, and choose **Allow** as the **Filtering Mode**. If you want to block the specified wireless clients from connecting to the Wireless Router, but allow all other wireless clients, select the **Enable MAC Address Filtering** check box, and choose **Block** as the **Filtering Mode**.

After you have configured MAC address filtering, the Wireless Router will allow or block wireless clients based on their MAC addresses.

To temporarily disable MAC address filtering, clear the **Enable MAC Address Filtering** check box.

6.3.5 Configuration Example for MAC Address Filtering

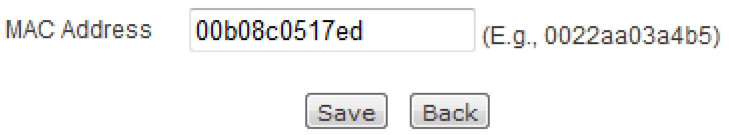
1. Requirements

In this example, we want to block the wireless clients with the MAC addresses 00b08c0517ed, 001f3c47f481 and 001f3c0f07f4 accessing the Wireless Router, and allow all other wireless clients to access the Wireless Router.

2. Configuration Steps

Step 1 Go to the **Wireless > MAC Filtering** page.

Step 2 Click the **Add** button to go to **MAC Address Filtering Settings** page (see Figure 6-21), enter **00b08c0517ed** in the **MAC Address** text box, and then click the **Save** button.

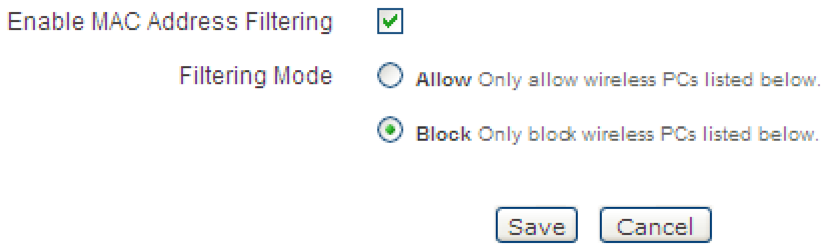


MAC Address: 00b08c0517ed (E.g., 0022aa03a4b5)

Figure 6-21 Adding a MAC Address Filtering Entry - Example

Step 3 Continue to add the other two MAC addresses (001f3c47f481 and 001f3c0f07f4) to the **MAC Address Filtering List**.

Step 4 Select the **Enable MAC Address Filtering** check box, choose **Block** as the **Filtering Mode**, and then click the **Save** button.



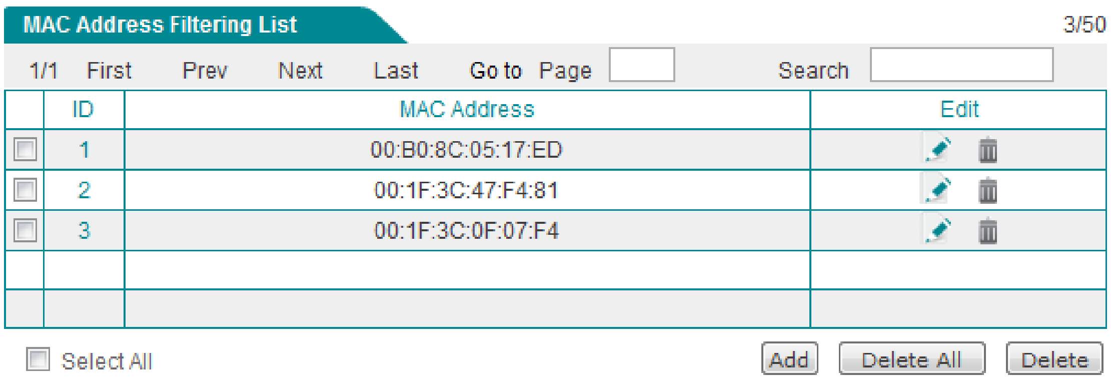
Enable MAC Address Filtering ☑

Filtering Mode ○ **Allow** Only allow wireless PCs listed below.

● **Block** Only block wireless PCs listed below.

Figure 6-22 MAC Address Filtering Global Settings - Example

Now the configuration is complete, and you can view the three MAC address filtering entries in the **MAC Address Filtering List**. If you have entered an incorrect MAC address, directly click its ✎ icon to go to the **MAC Address Filtering Settings** page to modify it, and click the **Save** button to save the change.



MAC Address Filtering List 3/50

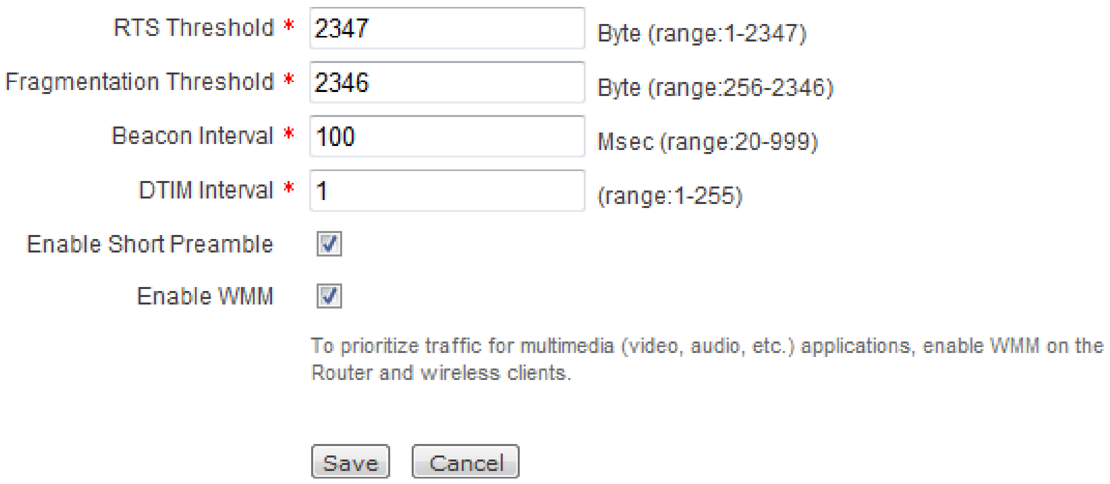
	ID	MAC Address	Edit
□	1	00:B0:8C:05:17:ED	✎ 🗑
□	2	00:1F:3C:47:F4:81	✎ 🗑
□	3	00:1F:3C:0F:07:F4	✎ 🗑

Figure 6-23 MAC Address Filtering List - Example

6.4 Advanced Wireless Settings

This section describes the **Wireless > Advanced Wireless Settings** page.

In this page, you can configure advanced wireless settings for your wireless connection. We suggest that you don’t adjust these settings unless you are an expert user. Incorrect settings will reduce the performance of your wireless network.



RTS Threshold * 2347 Byte (range:1-2347)

Fragmentation Threshold * 2346 Byte (range:256-2346)

Beacon Interval * 100 Msec (range:20-999)

DTIM Interval * 1 (range:1-255)

Enable Short Preamble ☑

Enable WMM ☑

To prioritize traffic for multimedia (video, audio, etc.) applications, enable WMM on the Router and wireless clients.

Figure 6- 24 Advanced Wireless Settings

- **RTS Threshold:** It specifies the packet size above which an RTS/CTS handshake will be performed before sending the packet. It must be between 1 and 2347, and the default value is 2347 bytes.

  RTS/CTS handshake is used to reduce collisions introduced by hidden nodes in the WLAN. A low threshold causes RTS packts to be sent more frequently, which consume more available bandwidth and reduce the throughput of other network packets. However, frequent RTS packets can help the network to recover from interference or collisions.

- **Fragmentation Threshold:** It speicifies the maximum size of a packet that can be transmitted. The packets larger than the specified size will be fragmented before transmission. It must be between 256 and 2346, and the default value is 2346 bytes.

  Reducing this value will decrease network performance. In most cases, please leave the default value. However, to ensure data transmission, you may decrease this value in areas where communication is poor, or in areas where there is a great deal of radio interference.

- **Beacon Interval:** It specifies the time interval between beacons. The Wireless Router periodically broadcasts beacons at the specified interval to synchronize the wireless network. It must be between 20 and 999, and the default value is 100 milliseconds.

- **DTIM Interval:** It determines how often the beacon contains a Delivery Traffic

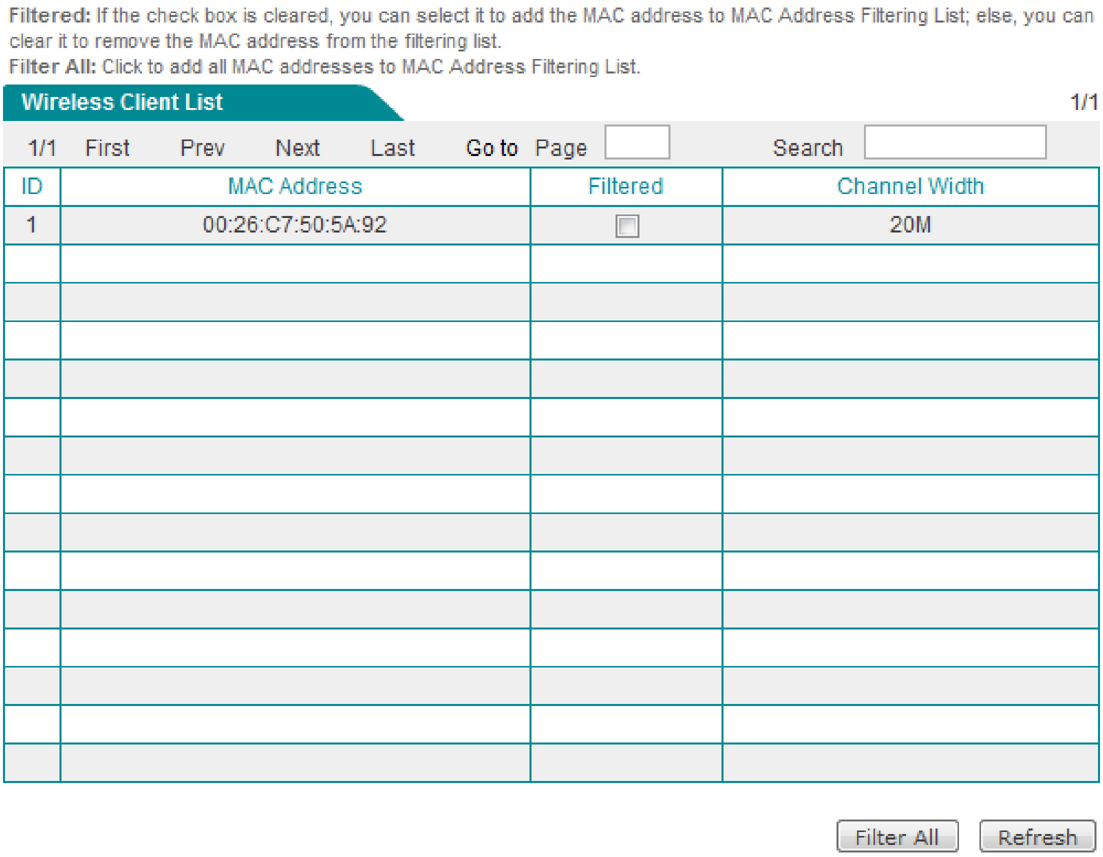
Indication Message (DTIM). The DTIM notifies wireless clients in power-save mode that a packet is waiting for them. The DTIM interval is a multiple of the **Beacon Interval**. For example, if it is set to 4, a DTIM message will be sent with every fourth beacon. It must be between 1 and 255, and the default value is 1.

- **Enable Short Preamble:** It allows you to enable short preamble or long preamble.
  - Select the check box to enable short preamble. The short preamble can improve network performance.
  - Clear the check box to enable long preamble. The long preamble ensures compatibilities with some old 802.11b devices that require the long preamble, but it can slightly reduce throughout at high data rate.
- **Enable WMM:** It allows you to enable or disable WMM (Wi-Fi Multimedia). WMM is a subset of the 802.11e standard. Enable this feature to improve the quality of multimedia (video, audio, etc.) applications by prioritizing traffic for them. To use this feature, your wireless clients must also support WMM.
- **Save:** Click to save your changes.
- **Cancel:** Click to revert to the last saved settings.

6.5 Wireless Client List

This section describes the **Wireless > Client List** page.

In the **Wireless Client List**, you can view the status of all wireless clients which are connected to the Wireless Router. In addition, you can also easily configure MAC address filtering entries via the list.



Filtered: If the check box is cleared, you can select it to add the MAC address to MAC Address Filtering List; else, you can clear it to remove the MAC address from the filtering list.
Filter All: Click to add all MAC addresses to MAC Address Filtering List.

Wireless Client List 1/1

ID	MAC Address	Filtered	Channel Width
1	00:26:C7:50:5A:92	□	20M

Figure 6- 25 Wireless Client List

- **ID:** It is used to identify each wireless client entry in the list.
- **MAC Address:** It displays the MAC address of the wireless client.
- **Filtered:** It indicates whether the corresponding MAC address has been added to the **MAC Address Filtering List** in the **Wireless > MAC Filtering** page. If the MAC address has been added to the **MAC Address Filtering List**, the **Filtered** check box is checked. Else, the **Filtered** check box is cleared; and in this case, you can click the check box to add the MAC address to the **MAC Address Filtering List**.
- **Channel Width:** It displays the current channel width in MHz.
- **Filter All:** Click to select the **Filtered** check boxes of all MAC addresses and add them into the **MAC Address Filtering List**, except those already added.
- **Refresh:** Click to view the latest information in the list.

Chapter 7 Advanced

This chapter describes how to configure and use the advanced features of the Wireless Router, which include NAT and DMZ, IP/MAC binding, static route, and PPPoE server.

7.1 NAT and DMZ

This section describes the **Advanced > NAT&DMZ** page.

7.1.1 Introduction to NAT Features

7.1.1.1 NAT Overview

The NAT (Network Address Translation) is an Internet standard that is used to map one IP address space (i.e., Intranet) to another IP address space (i.e., Internet). The NAT is designed to alleviate the shortage of IP addresses, that is, it allows all the local computers to share a single or a small group of IP addresses: On the Internet, there is only a single network device using a single or a small group of public IP addresses; but the local computers can use any range of private IP addresses, and these IP addresses are not visible from the Internet. As the internal network can be effectively isolated from the outside world, the NAT can also provide the benefit of network security assurance.

The Wireless Router provides flexible NAT features. The following sections describe them in detail.

7.1.1.2 NAT Address Space Definitions

To ensure that NAT operates properly, the Wireless Router uses and maintains two address spaces:

- **Internal IP address:** It indicates the IP address assigned to a local computer by the administrator. It is usually a private IP address.

- **External IP address:** It indicates the IP address assigned to the Wireless Router's Internet connection by the ISP. It is a legal public IP address that can represent one or more internal IP addresses to the outside world.

7.1.1.3 NAT Types

The Wireless Router provides two types of NAT: **One2One** and **EasyIP**.

- **One2One (One to One):** It indicates static network address translation. It is always referred to as Basic NAT, which provides a one to one mapping between an internal and an external IP address. In this type of NAT, IP address needs to be changed, but port needn't.

  One to One NAT can be used to allow the outside users to access a LAN server: In the local network, the LAN server still use the private IP address, which is provided to the local computers to access; and on the Internet, the Wireless Router will assign an external IP address to the local server, then the outside users can using this external IP address to access the server through the Wireless Router.

- **EasyIP:** It indicates network address and port translation (NAPT). Since it is the most common type of NAT, it is often simply referred to as NAT. NAPT provides many-to-one mappings between multiple internal IP addresses and a single external IP addresses, that is, these multiple internal IP addresses will be translated to the same external IP address. In this type of NAT, to avoid ambiguity in the handling of returned packets, it must dynamically assign a TCP/UDP port to an outgoing session and change the packets' source port to the assigned port before forwarding them. Besides, the Wireless Router must maintain a translation table so that return packets can be correctly translated back.

When you obtain multiple public IP addresses from your ISP, you can create more than one NAT rule for either type of NAT. In actual network environment, the two types of NAT rules are often used together.

7.1.1.4 Port Forwarding and DMZ Host

When NAT is enabled on the Wireless Router, the Wireless Router will block all the requests initiated from outside users. However, in some cases, the outside users want to access the LAN internal servers through the Wireless Router. To achieve this purpose, you need to configure port forwarding entries or DMZ host on the Wireless Router.

1. Port Forwarding

Port forwarding feature allows you to create the mapping between <external IP address: external port> and <internal IP address: internal port>, then all the requests from outside users to the specified external IP address: port on the Wireless Router will be forwarded to the mapped local server, so the outside users can access the service offered by the server.

For example, if you want to allow the local SMTP server (IP address: 192.168.1.88) to be available to the outside users, you can create a port forwarding entry: external IP address is WAN1 IP address (200.200.201.88 in this example), external port is 2100, internal IP address is 192.168.1.88, and internal port is 25. Then all the requests to SMTP service from outside users to 200.200.201.88:2100 will be forwarded to 192.168.1.88:25.

2. DMZ Host

The DMZ (Demilitarized Zone) feature allows one local computer to be exposed to the Internet for the use of a special service such as online game or video conferencing. When receiving the requests initiated from outside users, the Wireless Router will directly forward these requests to the specified DMZ host.

✓ **Note**

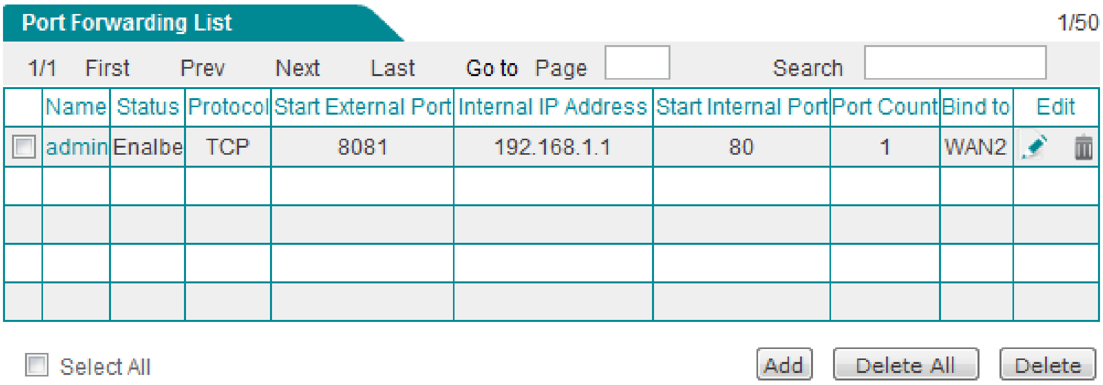
When a local computer is designated as the DMZ host, it loses firewall protection provided by the Wireless Router. As the DMZ host is exposed to many exploits from the Internet, it may be used to attack your network.

3. The Priorities of Port Forwarding Entries and DMZ Host

The port forwarding entries take priority over the DMZ host. When receiving a request packet initiated from an outside user, the Wireless Router will firstly search the **Port Forwarding List** to find out if there is a port forwarding entry matching the destination IP address and port of the packet. If a match is found, the Wireless Router will forward the packet to the mapped local computer. Else, the Wireless Router will try to find out if there is an available DMZ host.

7.1.2 Port Forwarding

7.1.2.1 Port Forwarding List



Port Forwarding List 1/50

1/1 First Prev Next Last Go to Page Search

	Name	Status	Protocol	Start External Port	Internal IP Address	Start Internal Port	Port Count	Bind to	Edit
□	admin	Enalbe	TCP	8081	192.168.1.1	80	1	WAN2	

□ Select All

Figure 7-1 Port Forwarding List

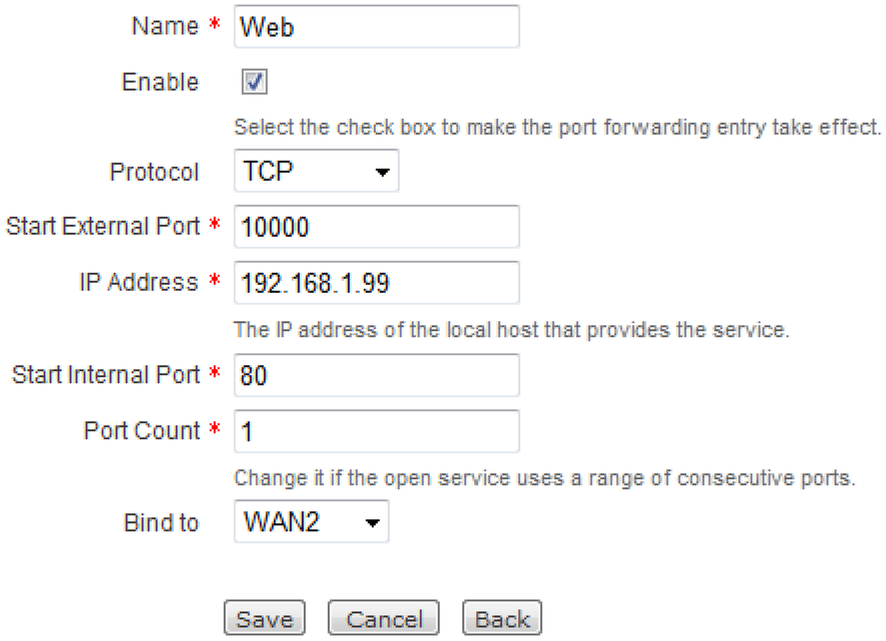
- **Add a Port Forwarding Entry:** To add a new port forwarding entry, first click the **Add** button to go to the **Port Forwarding Settings** page, next configure it, lastly click the **Save** button.
- **View Port Forwarding Entry(s):** When you have configured one or more port forwarding entries, you can view them in the **Port Forwarding List**.
- **Modify a Port Forwarding Entry:** To modify a configured port forwarding entry, click its **Name** hyperlink or ✎ icon, the related information will be displayed in the setup page. Then modify it, and click the **Save** button.
- **Delete Port Forwarding Entry(s):** There are three ways to delete port forwarding entry(s).

  1. To delete a port forwarding entry, directly click its 🗑 icon.
  2. To delete more than one port forwarding entry at a time, select the leftmost check boxes of the entries that you want to delete, and then click the **Delete** button.
  3. To delete all the port forwarding entries at a time, directly click the **Delete All** button.

Note

After you enable HTTP remote management in the **Administration > Remote Access** page, the system will automatically create a port forwarding entry for it. You cannot modify or delete it in this page.

7.1.2.2 Port Forwarding Settings



Name * Web

Enable ☑

Select the check box to make the port forwarding entry take effect.

Protocol TCP

Start External Port * 10000

IP Address * 192.168.1.99

The IP address of the local host that provides the service.

Start Internal Port * 80

Port Count * 1

Change it if the open service uses a range of consecutive ports.

Bind to WAN2

Figure 7-2 Port Forwarding Settings

- **Name:** It specifies a unique name of the port forwarding entry.
- **Enable:** It allows you to enable or disable the port forwarding entry. The default value is checked, which means the port forwarding entry is in effect. If you want to disable the entry temporarily instead of deleting it, please clear the check box.
- **Protocol:** It specifies the transport protocol used by the service. The available options are **TCP**, **UDP** and **TCP/UDP**. If you are not sure, select **TCP/UDP**.
- **Start External Port:** It specifies the lowest port number provided by the Wireless Router. The external ports are opened for outside users to access.
- **Internal IP Address:** It specifies the IP address of the local computer that provides the service.
- **Start Internal Port:** It specifies the lowest port number of the service provided by the local computer. The **Start External Port** and **Start Internal Port** can be different.
- **Port Count:** It specifies the number of service ports provided by the local computer. If the service uses only one port number, enter 1. Change it if the service uses a range of consecutive ports. The maximum value is 20. For example, if the start internal port is 20, the start external port is 2000, and the port count is 2, then the internal port range is from 20 to 21, and the external port range is from 2000 to 2001.
- **Bind to:** It specifies the interface to which this port forwarding entry is bound. The port forwarding entry will use the selected interface’s IP address as its external IP address.

- **Save:** Click to save your changes.
- **Cancel:** Click to revert to the last saved settings.
- **Back:** Click to go back to the **Port Forwarding List**.

7.1.2.3 How to Add Port Forwarding Entries

To add one or more static port forwarding entries, follow these steps:

Step 1 Go to the **Advanced > NAT > Port Forwarding** page, and click the **Add** button to go to the **Port Forwarding Settings** page.

Step 2 Specify the **Name**, and leave the **Enable** check box checked.

Step 3 Specify the **Protocol**, **Internal IP Address** and **Start Internal Port** as required.

Step 4 Specify the **Start External Port** as required. The **Start External Port** and **Start Internal Port** can be different.

Step 5 If the open service uses a range of consecutive ports, you need to specify the **Port Count**.

Step 6 Select an interface from the **Bind to** drop-down list as required. The port forwarding entry will use the selected interface's IP address as its external IP address.

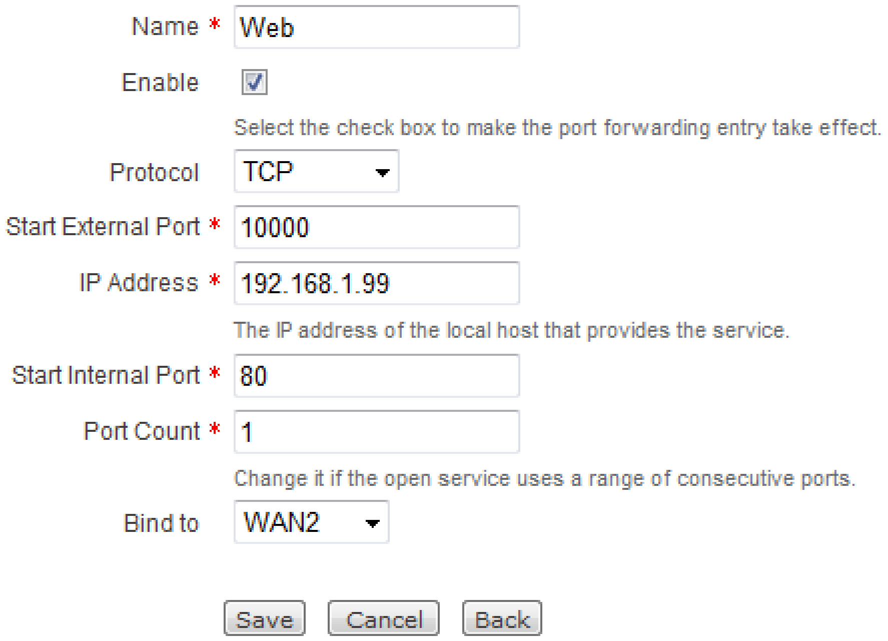
Step 7 Click the **Save** button to save the settings. You can view the port forwarding entry in the **Port Forwarding List**.

Step 8 If you want to add another new port forwarding entry, please repeat the above steps.

7.1.2.4 Configuration Example for Port Forwarding

An organization wants a LAN server (IP Address: 192.168.1.99) to open Web service (Protocol: TCP; Port: 80) to the outside users. And the Wireless Router will use 10000 as the external port and the WAN2 IP address (200.200.200.88 in this example) as the external IP address. Then all the requests to Web service from outside users to 200.200.200.88:10000 will be forwarded to 192.168.1.99:80.

The following figure shows the detailed settings.



Name * Web

Enable ☑

Select the check box to make the port forwarding entry take effect.

Protocol TCP

Start External Port * 10000

IP Address * 192.168.1.99

The IP address of the local host that provides the service.

Start Internal Port * 80

Port Count * 1

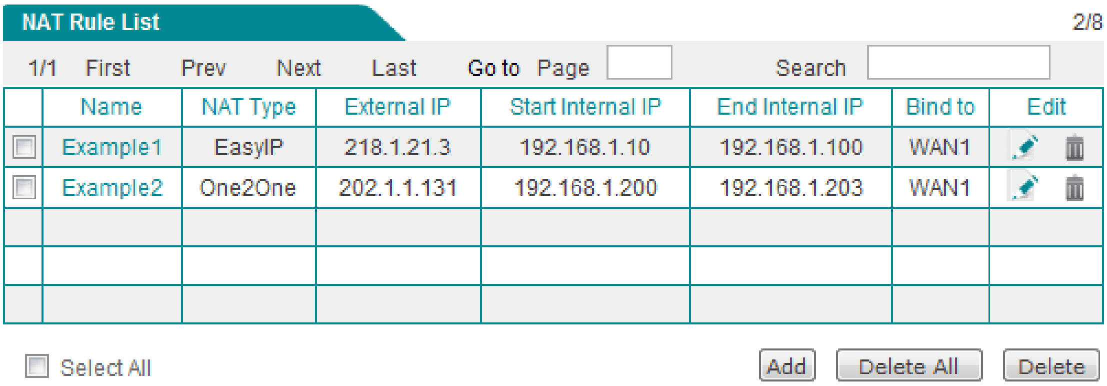
Change it if the open service uses a range of consecutive ports.

Bind to WAN2

Figure 7- 3 Port Forwarding Settings - Example

7.1.3 NAT Rule

7.1.3.1 NAT Rule List



NAT Rule List 2/8

1/1 First Prev Next Last Go to Page Search

	Name	NAT Type	External IP	Start Internal IP	End Internal IP	Bind to	Edit
□	Example1	EasyIP	218.1.21.3	192.168.1.10	192.168.1.100	WAN1	✎ 🗑
□	Example2	One2One	202.1.1.131	192.168.1.200	192.168.1.203	WAN1	✎ 🗑

□ Select All

Figure 7- 4 NAT Rule List

- **Add a NAT Rule:** To add a new NAT rule, first click the **Add** button to go to the **NAT Rule Settings** page, next configure it, lastly click the **Save** button.

- **View NAT Rule(s):** When you have configured one or more NAT rules, you can view them in the **NAT Rule List**.

- **Modify a NAT Rule:** To modify a configured NAT rule, click its **Name** hyperlink or ✎ icon, the related information will be displayed in the setup page. Then modify it, and click the **Save** button.

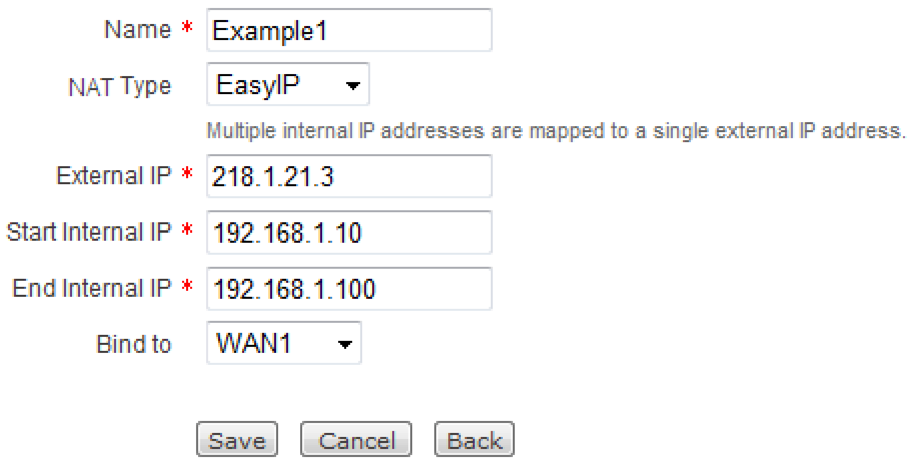
- **Delete NAT Rule(s):** There are three ways to delete NAT rules.

  1. To delete a NAT rule, directly click its 🗑 icon.
  2. To delete more than one NAT rule at a time, select the leftmost check boxes of the NAT rules that you want to delete, and then click the **Delete** button.
  3. To delete all the NAT rules at a time, directly click the **Delete All** button.

7.1.3.2 NAT Rule Settings

The following sections describe the settings of the **EasyIP** NAT rule and **One2One** NAT rule respectively, see Figure 7- 5 and Figure 7- 6.

7.1.3.2.1 NAT Rule Settings - EasyIP

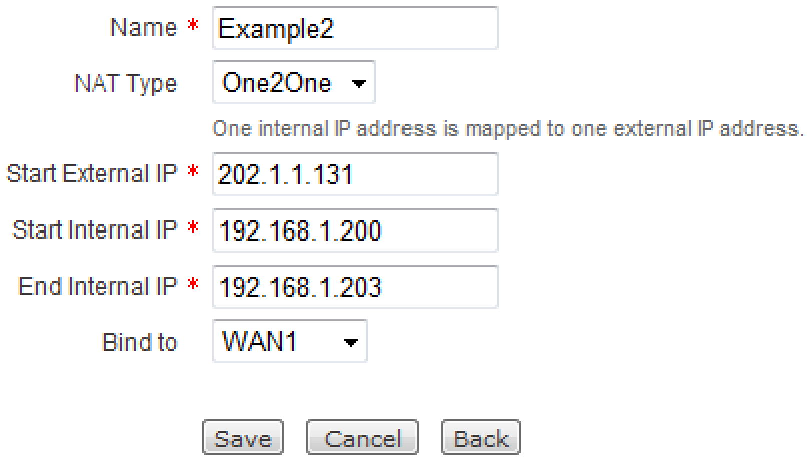


Name *	Example1
NAT Type	EasyIP
	Multiple internal IP addresses are mapped to a single external IP address.
External IP *	218.1.21.3
Start Internal IP *	192.168.1.10
End Internal IP *	192.168.1.100
Bind to	WAN1

Figure 7- 5 NAT Rule Settings - EasyIP

- **Name:** It specifies a unique name of the NAT rule.
- **NAT Type:** It specifies the type of the NAT rule. The available options are **EasyIP** and **One2One**. Here please select **EasyIP**.
- **External IP:** It specifies the external IP address to which the local computers' IP addresses are mapped.
- **Start Internal IP** and **End Internal IP:** They specify a range of internal IP addresses. The local computers within the specified range will preferentially use the NAT rule.
- **Bind to:** It specifies the interface to which the NAT rule is bound.
- **Save:** Click to save your changes.
- **Cancel:** Click to revert to the last saved settings.
- **Back:** Click to go back to the **NAT Rule List**.

7.1.3.2.2 NAT Rule Settings - One2One



Name * Example2

NAT Type One2One

One internal IP address is mapped to one external IP address.

Start External IP * 202.1.1.131

Start Internal IP * 192.168.1.200

End Internal IP * 192.168.1.203

Bind to WAN1

Figure 7- 6 NAT Rule Settings - One2One

- **Name:** It specifies a unique name of the NAT rule.
- **NAT Type:** It specifies the type of the NAT rule. The available options are **EasyIP** and **One2One**. Here please select **One2One**.
- **Start External IP:** It specifies the start external IP address to which the start internal IP address is mapped.
- **Start Internal IP** and **End Internal IP:** They specify the internal IP address range of the NAT rule.
- **Bind to:** It specifies the interface to which the NAT rule is bound.
- **Save:** Click to save your changes.
- **Cancel:** Click to revert to the last saved settings.
- **Back:** Click to go back to the **NAT Rule List**.

✓ **Note**

1. When creating a **One2One** NAT rule, you must set the **Start External IP**. The number of the external IP addresses is the same as the number of internal IP addresses, which is determined by the **Start Internal IP** and **End Internal IP**. For example, if the **Start Internal IP** is 192.168.16.6, **End Internal IP** is 192.168.16.8, and **Start External IP** is 200.200.200.116, then 192.168.16.6, 192.168.16.7, and 192.168.16.8 will be mapped to 200.200.200.116, 200.200.200.117, and 200.200.200.118 respectively.
2. A One2One NAT rule can contain up to 20 external/internal IP addresses.

7.1.3.3 How to Add NAT Rules

To add one or more NAT rules, follow these steps:

Step 1 Please identify the type of the NAT rule that you want to add.

Step 2 Go to the **Advanced > NAT > NAT Rule** page, and click the **Add** button to go to the **NAT Rule Settings** page.

Step 3 Specify the **Name** for the NAT rule, and select a type from the **NAT Type** drop-down list as required.

Step 4 There are two cases:

1) If the NAT rules' type is **EasyIP**, please specify the **External IP**, **Start Internal IP**, and **End Internal IP** as required.

2) If the NAT rules' type is **One2One**, please specify the **Start External IP**, **Start Internal IP**, and **End Internal IP** as required.

Step 5 Select an interface from the **Bind to** drop-down list as required.

Step 6 Click the **Save** button to save the settings. You can view the NAT rule in the **NAT Rule List**.

Step 7 If you want to add another new NAT rule, please repeat the above steps.

✓ **Note**

If you want to delete NAT rule(s), please follow the ways described in **Section 7.1.3.1 NAT Rule List**.

7.1.3.4 Configuration Examples for NAT Rule

7.1.3.4.1 An Example for Configuring an EasyIP NAT Rule

1. Requirements

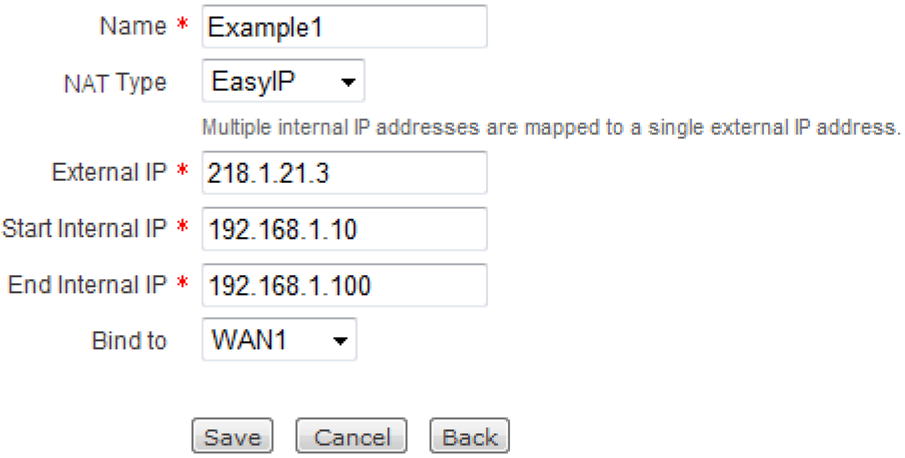
In this example, an Internet café has a single Internet connection, and obtains eight public IP addresses (from 218.1.21.0/29 to 218.1.21.7/29) from the ISP. Therein, 218.1.21.1/29 is used as the Internet connection's gateway IP address, 218.1.21.2/29 is used as the Wireless Router's WAN1 interface IP address. Note that 218.1.21.0/29 and 218.1.21.7/29 cannot be used as they are the subnet number and broadcast address respectively.

The administrator want the local computers in the online game area (its address range is from 192.168.1.10/24 to 192.168.1.100/24) to use 218.1.21.3/29 to access the Internet. To achieve this purpose, he should create an **EasyIP** NAT rule for them. The rule's **External IP** is 218.1.21.3, **Start Internal IP** is 192.168.1.10, **End Internal IP** is 192.168.1.100, and **Bind to** be WAN1.

2. Configuration Steps

The configuration steps are the following:

Step 1 Go to the **Advanced > NAT > NAT Rule** page, and click the **Add** button to go to the **NAT Rule Settings** page, see the following figure.



Name * Example1

NAT Type EasyIP

Multiple internal IP addresses are mapped to a single external IP address.

External IP * 218.1.21.3

Start Internal IP * 192.168.1.10

End Internal IP * 192.168.1.100

Bind to WAN1

Figure 7-7 EasyIP NAT Rule Settings - Example

Step 2 Enter **Example1** in the **Name** text box.

Step 3 Select **EasyIP** from the **NAT Type** drop-down list.

Step 4 Enter **218.1.21.3** in the **External IP** text box; enter **192.168.1.10** and **192.168.1.100** in the **Start Internal IP** and **End Internal IP** text boxes respectively.

Step 5 Select **WAN1** from the **Bind to** drop-down list.

Step 6 Click the **Save** button to save the settings. Till now you have finished configuring the NAT rule, and you can view it in the **NAT Rule List**.

Note

If an **EasyIP** NAT rule's **External IP** is not on the same subnet as the IP address of the interface to which the rule is bound, the Wireless Router's default gateway requires a subnet route for the network to which the **External IP** belongs, or a host route for the **External IP** pointing to the bound interface.

7.1.3.4.2 An Example for Configuring a One2One NAT Rule

1. Requirements

In this example, a business has a single static IP Internet connection, and obtains eight public IP addresses (202.1.1.128/29 - 202.1.1.1.135/29) from the ISP. Therein, 202.1.1.129/29 is used as the Internet connection's gateway IP address, 202.1.1.130/2 is used as the Wireless Router's WAN1 IP address. Note that 202.1.1.128/29 and 202.1.1.1.135/29 cannot be used as they are the subnet number and broadcast address respectively.

The business wants its employees to share a single public IP address of 202.1.1.130/29 to access the Internet; and it wants its four local servers to provide services for the outside users. The LAN subnet is 192.168.1.0/24. The four local servers IP addresses are from 192.168.1.200/24 to 192.168.1.203/24.

2. Analysis

Firstly we need to configure a static IP Internet connection on the WAN1 interface in the **Network > WAN** page or through the **Start > Setup Wizard**. After you have configured the Internet connection, the Wireless Router will automatically create a related system reserved EasyIP NAT rule, and also enable NAT.

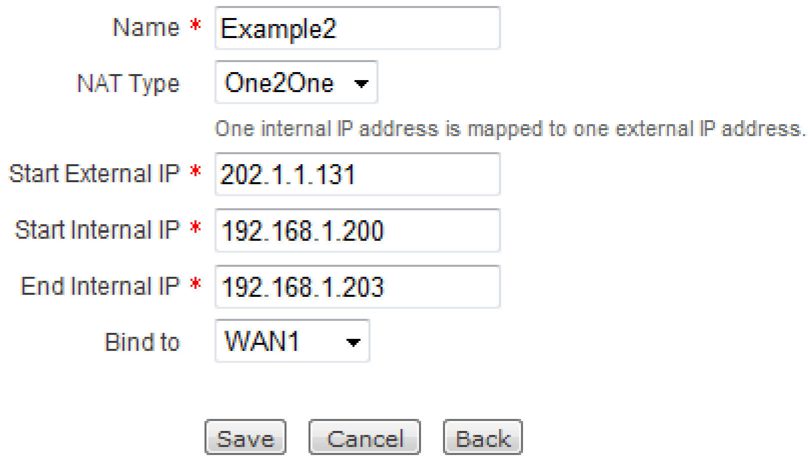
Secondly, we need to create a One2One NAT rule for the four local servers. The IP addresses of the four local servers are mapped to 202.1.1.131/29, 202.1.1.132/29, 202.1.1.133/29, 202.1.1.134/29 respectively. Thus the outside users can use these public addresses to access the local servers through the Wireless Router.

3. Configuration Steps

Here we only describe how to create the **One2One** NAT rule.

Step 1 Go to the **Advanced > NAT > NAT Rule** page, and click the **Add** button to go to the **NAT Rule Settings** page, see the following figure.

Step 2 Enter **Example2** in the **Name** text box.



Name * Example2

NAT Type One2One

One internal IP address is mapped to one external IP address.

Start External IP * 202.1.1.131

Start Internal IP * 192.168.1.200

End Internal IP * 192.168.1.203

Bind to WAN1

Figure 7- 8 One2One NAT Rule Settings - Example

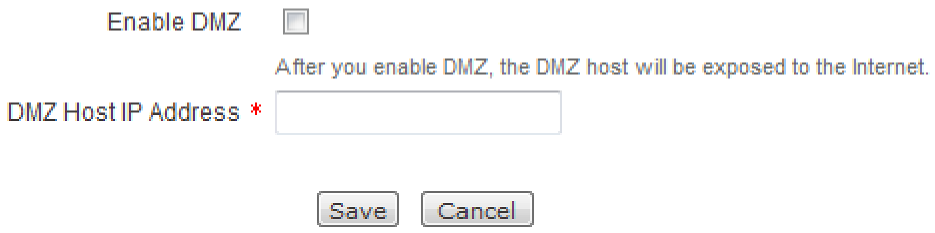
Step 3 Select **One2One** from the **NAT Type** drop-down list.

Step 4 Enter **202.1.1.131** in the **Start External IP** text box; enter **192.168.1.200** and **192.168.1.203** in the **Start Internal IP** and **End Internal IP** text boxes respectively.

Step 5 Select **WAN1** from the **Bind to** drop-down list.

Step 6 Click the **Save** button to save the settings. Till now you have finished configuring the NAT rule, and you can view it in the **NAT Rule List**.

7.1.4 DMZ



Enable DMZ □

After you enable DMZ, the DMZ host will be exposed to the Internet.

DMZ Host IP Address *

Figure 7- 9 DMZ Host Settings

- **Enable DMZ:** It allows you to enable or disable DMZ feature. If you want to enable DMZ feature on the Wireless Router, please select this check box.
- **DMZ Host IP Address:** It specifies the private IP address of the DMZ host.
- **Save:** Click to save your changes.
- **Cancel:** Click to revert to the last saved settings.

✓ **Note**

When a local computer is designated as the DMZ host, it loses firewall protection provided by the Wireless Router. The DMZ host can be accessed through all the WAN interfaces.

7.2 IP/MAC Binding

This section describes the **Security > IP/MAC Binding** page.

7.2.1 Introduction to IP/MAC Binding

7.2.1.1 IP/MAC Binding Overview

To achieve network security management, you should perform user identification before performing user authorization. In this section, we describe how to implement user identification. In **Section 9.1 Firewall > Access Control**, we will describe how to control the Internet behaviors of the LAN users in detail.

The Wireless Router provides IP/MAC binding feature to implement user identification. Using the IP/MAC address pair as a unique user identity, you can protect the Wireless Router and your network against IP spoofing attacks. IP spoofing attack refers to that a computer attempts to use another trusted computer's IP address to connect to or pass through the Wireless Router. The computer's IP address can easily be changed to a trusted address, but MAC address cannot easily be changed as it is added to the Ethernet card at the factory.

7.2.1.2 The Operation Principle of IP/MAC Binding

For the sake of convenience, we firstly introduce several related terms including legal user, illegal user and undefined user.

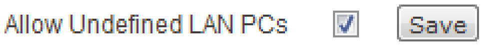
- **Legal User:** A legal user's IP and MAC address pair matches an IP/MAC binding whose **Allow** check box is checked.
- **Illegal User:** An illegal user's IP and MAC address pair matches an IP/MAC binding whose **Allow** check box is cleared; or the IP address or MAC address is the same as that of an IP/MAC binding, but not both.
- **Undefined User:** An undefined user's IP address and MAC address both are different from any IP/MAC binding. The undefined users are all the users except legal and illegal users.

It allows the legal users to access the Wireless Router or access the Internet through the Wireless Router, and denies the illegal users. And the parameter of **Allow Undefined LAN PCs** determines whether it allows the undefined users to access the Wireless Router or access the Internet through the Wireless Router, that is, it will allow them if they **Allow Undefined LAN PCs** check box is checked, else block them.

IP/MAC binding feature can act on the packets initiated from the local computers to the Wireless Router or outside computers. When receiving a packet initiated from LAN, the Wireless Router will firstly determine the sender's identity by comparing the packet with the bindings in the **IP/MAC Binding List**, and then process the packet according to the sender's identity. The details are as follows:

1. If the sender is a legal user, the packet will be allowed to pass, and then be further processed by other function modules.
2. If the sender is an illegal user, the packet will be dropped immediately to prevent IP spoofing.
3. If the sender is an undefined user, there are two cases:
   1) If the **Allow Undefined LAN PCs** check box is checked, the packet will be allowed to pass, and then be further processed by other function modules.
   2) Else, the packet will be dropped immediately.

7.2.2 IP/MAC Binding Global Settings



Allow Undefined LAN PCs ☑ Save

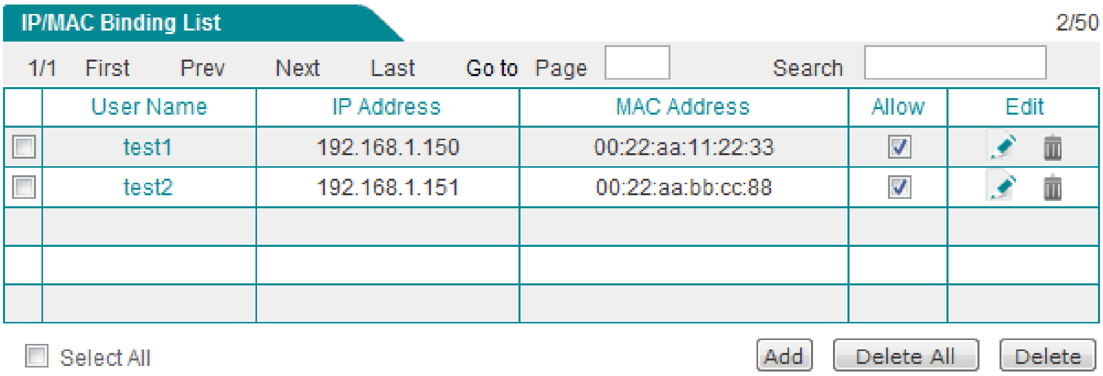
Figure 7- 10 IP/MAC Binding Global Settings

- **Allow Undefined LAN PCs:** It allows or blocks the undefined local computers from accessing the Wireless Router or accessing the Internet through the Wireless Router. If you want to allow the undefined local computers to access the Wireless Router and Internet, please select the check box.
- **Save:** Click to save your changes.

✓ **Note**

If you want to clear the **Allow Undefined LAN PCs** check box to block the undefined local computers, please make sure that you have added the IP/MAC address pair of the computer that you use to administer the Wireless Router into the **IP/MAC Binding List**. Otherwise you cannot access the Wireless Router from that computer.

7.2.3 IP/MAC Binding List



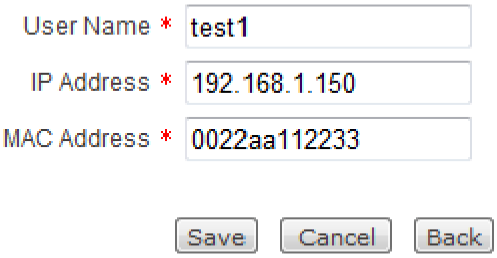
	User Name	IP Address	MAC Address	Allow	Edit
□	test1	192.168.1.150	00:22:aa:11:22:33	☑	✎ 🗑
□	test2	192.168.1.151	00:22:aa:bb:cc:88	☑	✎ 🗑

Figure 7-11 IP/MAC Binding List

- **Add One or More IP/MAC Bindings:** To add one or more IP/MAC bindings, first click the **Add** button to go to the **IP/MAC Binding Settings** page shown in Figure 7-14, next configure them, lastly click the **Save** button.

- **View IP/MAC Binding(s):** When you have configured one or more IP/MAC bindings, you can view them in the **IP/MAC Binding List**.

- **Modify an IP/MAC Binding:** To modify a configured IP/MAC binding, click its **User Name** hyperlink or ✎ icon, the related information will be displayed in the setup page shown in Figure 7-12. Then modify it, and click the **Save** button.



User Name * test1

IP Address * 192.168.1.150

MAC Address * 0022aa112233

Figure 7-12 Modifying an IP/MAC Binding

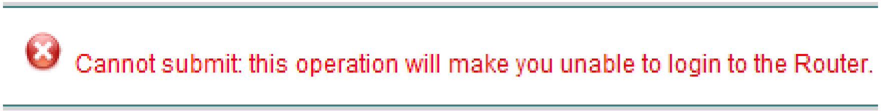
The **Allow** check box is used to allow or block a user matching an IP/MAC binding from accessing the Wireless Router and Internet. To allow the user matching the IP/MAC binding to access, select the IP/MAC binding's **Allow** check box; else clear it.

- **Delete IP/MAC binding(s):** There are three ways to delete IP/MAC bindings.

1. To delete a IP/MAC binding, directly click its 🗑 icon.
2. To delete more than one IP/MAC binding at a time, select the leftmost check boxes of the bindings that you want to delete, and then click the **Delete** button.
3. To delete all the IP/MAC bindings at a time, directly click the **Delete All** button.

Note

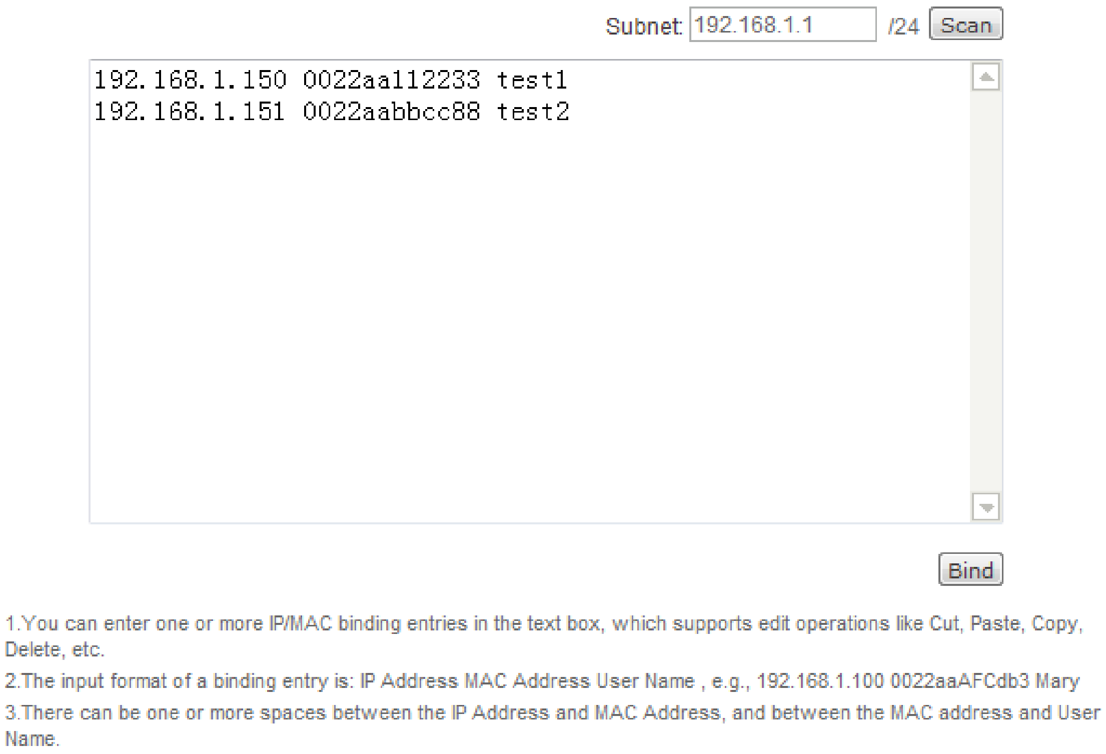
When you add the IP/MAC address pair of the computer that you use to administer the Wireless Router into the **IP/MAC Binding List**, please leave the **Allow** check box checked. Otherwise you cannot access the Wireless Router from that computer. If you attempt to clear the check box, you will be prompted that the operation is not permitted, see the following figure.



Cannot submit: this operation will make you unable to login to the Router.

Figure 7- 13 IP/MAC Binding Error Message

7.2.4 IP/MAC Binding Settings



Subnet: 192.168.1.1 /24 Scan

```
192.168.1.150 0022aa112233 test1
192.168.1.151 0022aabbcc88 test2
```

Bind

1.You can enter one or more IP/MAC binding entries in the text box, which supports edit operations like Cut, Paste, Copy, Delete, etc.

2.The input format of a binding entry is: IP Address MAC Address User Name , e.g., 192.168.1.100 0022aaAFCdb3 Mary

3.There can be one or more spaces between the IP Address and MAC Address, and between the MAC address and User Name.

Figure 7- 14 IP/MAC Binding Settings

- **Subnet:** It specifies the subnet you want to scan. The default is the Wireless Router's LAN IP address and subnet mask.

- **Scan:** If you click the **Scan** button, the Wireless Router will immediately scan the specified subnet to detect active computers connected to the Wireless Router, learn and display dynamic ARP information (that is, IP and MAC address pairs) in the text box. Note that if a computer's IP/MAC address pair has been added in the **IP/MAC Binding List**, this IP/MAC address pair will not be displayed here.

- **Bind:** Click to bind all the valid IP and MAC address pairs in the text box.
- **Add IP/MAC Binding(s) Manually:** To manually add one or more IP/MAC bindings, follow these steps: Enter one or more IP/MAC address pair entries in the text box, and then click the **Bind** button. The input contents are: **IP Address**, **MAC Address** and **User Name**, one address pair entry per line; and the input format for each entry is: **IP Address <Space> MAC Address <Space> User Name <Enter>**.
    - **IP Address:** It specifies the IP address of the local computer.
    - **MAC Address:** It specifies the MAC address of the local computer.
    - **User Name:** It specifies a unique user name of the local computer whose IP/MAC address pair will be bound. It is an optional parameter. If you don't enter it, the system will automatically create a user name for the computer.

✓ **Note**

1. You can use the **ipconfig /all** command at the command prompt to find a Windows-based computer's IP address and MAC address.
2. For an IP/MAC address pair entry entered manually, there can be one or more spaces between the **IP Address** and **MAC Address**, and between the **MAC address** and **User Name**.
3. The **Bind** operation will skip any invalid IP and MAC address pairs in the text box. In other words, it will only bind the valid IP and MAC address pairs.

7.2.5 How to Add IP/MAC Bindings

To add one or more IP/MAC bindings, follow these steps:

Step 1 Go to the **Advanced > IP/MAC Binding** page, and click the **Add** button to go to the **IP/MAC Binding Settings** page.

Step 2 There are two methods to add IP/MAC bindings:

1) **Method One:** Click the **Scan** button to learn current dynamic ARP information (that is, IP and MAC address pairs) of the local computers, next click the **Bind** button to bind the valid IP/MAC address pairs in the text box.

2) **Method Two:** You can manually add one or more IP/MAC address pairs in the text box, next click the **Bind** button to bind these IP/MAC address pairs. Refer to **Section 7.2.4 IP/MAC Binding Settings** for more information.

Step 3 After you have added some IP/MAC bindings, you can view them in the **IP/MAC Binding List**.

Step 4 If you want to block the undefined local computers from accessing the Wireless Router and Internet, please clear the **Allow Undefined LAN PCs** check box; else, the undefined local computers are allowed to access the Wireless Router and Internet.

Step 5 If you want to temporarily block a user matching an IP/MAC binding from accessing the Wireless Router and Internet, please clear the binding's **Allow** check box.

After you have finished configuring IP/MAC binding feature, when receiving a packet initiated from LAN, the Wireless Router will firstly compare the packet with the bindings in the **IP/MAC Binding List**, and then process the packet according to the related configuration. The packet will be allowed to pass or be dropped immediately. If it is allowed to pass, the packet will be further processed by other function modules.

7.2.6 Internet Whitelist and Blacklist

7.2.6.1 Introduction to Internet Whitelist and Blacklist Based on IP/MAC Binding

By utilizing IP/MAC binding feature, you can flexibly configure an Internet whitelist or blacklist for the LAN users.

If you want to allow only a small number of LAN users to access the Internet, you can configure an Internet whitelist for these users. Then all users cannot access the Internet, except those listed in the whitelist.

If you want to block only a small number of LAN users from accessing the Internet, you can configure an Internet blacklist for these users. Then all users can access the Internet, except those listed in the blacklist.

On the Wireless Router, a user listed in the whitelist is a legal user, i.e., the user's IP and MAC address pair matches an IP/MAC binding whose **Allow** check box is checked. A user listed in the blacklist is an illegal user, i.e., the user's IP and MAC address pair matches an IP/MAC binding whose **Allow** check box is cleared; or the IP address or MAC address is the same as that of an IP/MAC binding, but not both.

7.2.6.2 How to Configure an Internet Whitelist

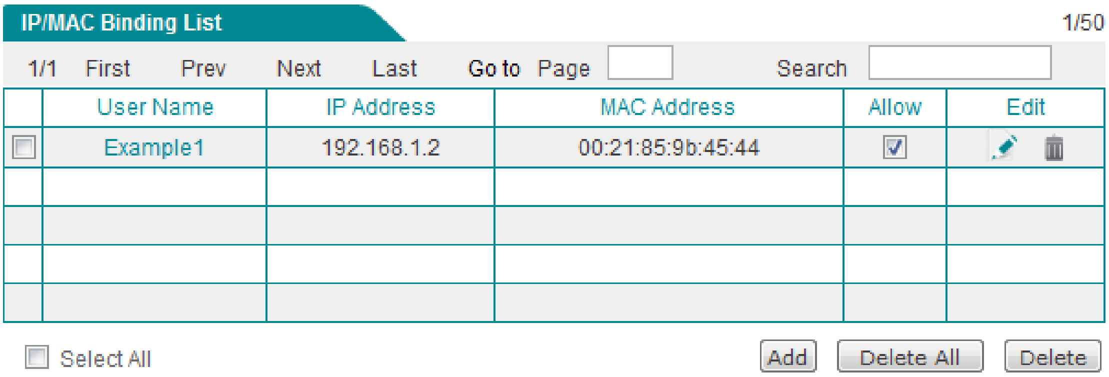
To configure an Internet whitelist, follow these steps:

Step 1 Go to the **Advanced > IP/MAC Binding** page, and click the **Add** button to go to the **IP/MAC Binding Settings** page.

Step 2 Specify the legal users by creating the IP/MAC bindings: Add these users' IP and MAC address pairs into the **IP/MAC Binding List**. By default, an IP/MAC binding's **Allow** check box is checked, which means that the user matching the IP/MAC binding can access the Wireless Router and Internet, so please leave the default value. Refer to **Section 7.2.4 IP/MAC Binding Settings** for detailed information.

Step 3 Clear the **Allow Undefined LAN PCs** check box to block all the undefined users from accessing the Wireless Router and Internet.

For example, if you want to allow a local computer with IP address 192.168.1.2 and MAC address 0021859b4544 to access the Wireless Router and Internet, you can add its IP/MAC address pair into the **IP/MAC Binding List**, see Figure 7-15. The binding's **Allow** check box is checked by default, so please leave the default value.



	User Name	IP Address	MAC Address	Allow	Edit
□	Example1	192.168.1.2	00:21:85:9b:45:44	☑	

Figure 7-15 IP/MAC Binding List - Example 1

7.2.6.3 How to Configure an Internet Blacklist

To configure an Internet blacklist, follow these steps:

Step 1 Go to the **Advanced > IP/MAC Binding** page, and click the **Add** button to go to the **IP/MAC Binding Settings** page.

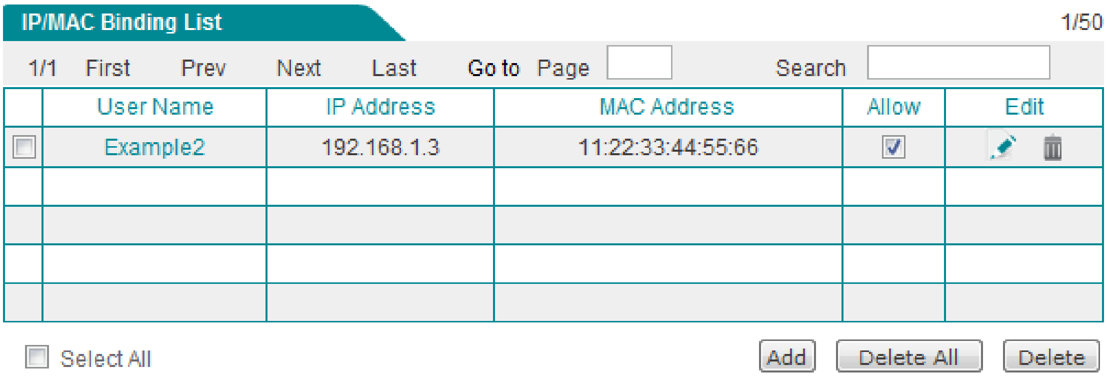
Step 2 Specify the illegal users by creating the IP/MAC bindings. There are two methods (Refer to **Section 7.2.4 IP/MAC Binding Settings** for detailed information.):

1) **Method One:** Bind each illegal user’s IP address to a MAC address which is different from any local computer’s, and add these IP/MAC address pairs into the **IP/MAC Binding List**.

2) **Method Two:** Add these users’ IP and MAC address pairs into the **IP/MAC Binding List**, and clear each IP/MAC binding’s **Allow** check box respectively. Thus the matched users cannot access the Wireless Router and Internet.

Step 3 Select the **Allow Undefined LAN PCs** check box to allow all the undefined users to access the Wireless Router and Internet.

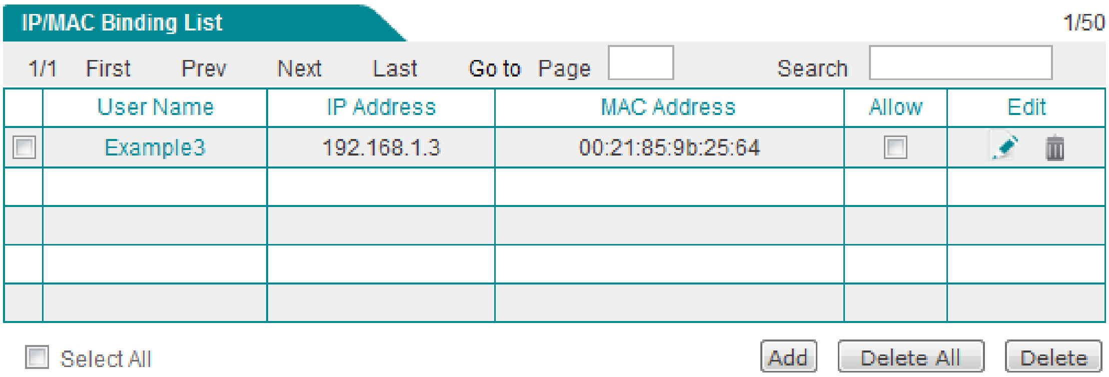
For example, if you want to block a local computer with IP address 192.168.1.3 from accessing the Wireless Router and Internet, you can add an IP/MAC binding into the **IP/MAC Binding List**: the **IP Address** is 192.168.1.3, and the **MAC Address** is different from any local computer’s MAC address (112233445566 here), see Figure 7- 16.



	User Name	IP Address	MAC Address	Allow	Edit
□	Example2	192.168.1.3	11:22:33:44:55:66	☑	✎ 🗑

Figure 7- 16 IP/MAC Binding List - Example 2

Another example is that if you want to block a local computer with IP address 192.168.1.3 and MAC address 0021859b2564 from accessing the Wireless Router and Internet, you can add its IP/MAC address pair into the **IP/MAC Binding List**, next clear the binding’s **Allow** check box, see Figure 7- 17.



	User Name	IP Address	MAC Address	Allow	Edit
□	Example3	192.168.1.3	00:21:85:9b:25:64	□	✎ 🗑

Figure 7- 17 IP/MAC Binding List - Example 3

7.3 Static Route

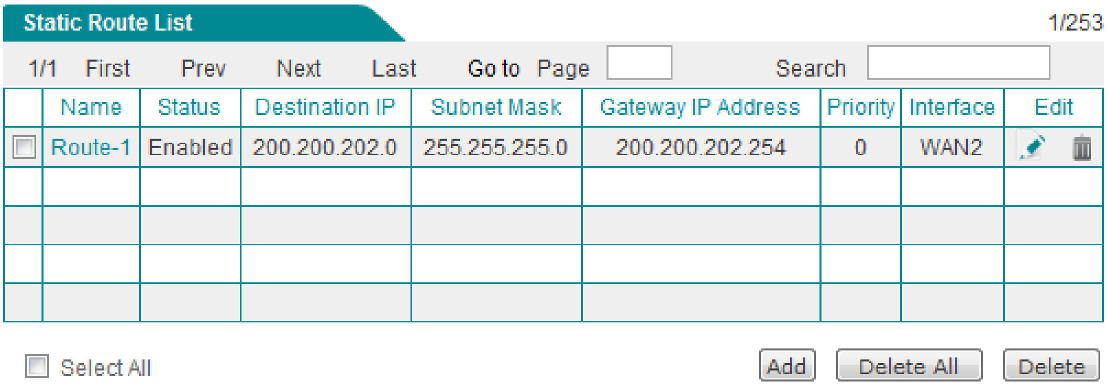
This section describes the **Advanced > Static Route** page, where you can configure and view static routes.

7.3.1 Introduction to Static Route

A static route is manually configured by the network administrator, which is stored in a routing table. By using routing table, the Wireless Router can select an optimal transmission path for each received packet, and forward the packet to the destination site effectively. The proper usage of static routes can not only improve the network performance, but also achieve other benefits, such as traffic control, provide a secure network environment.

The disadvantage of using static routes is that they cannot dynamically adapt to the current operational state of the network. When there is a change in the network or a failure occurs, some static routes will be unreachable. In this case, the network administrator should update the static routes manually.

7.3.2 Static Route List



Static Route List 1/253

1/1 First Prev Next Last Go to Page Search

	Name	Status	Destination IP	Subnet Mask	Gateway IP Address	Priority	Interface	Edit
□	Route-1	Enabled	200.200.202.0	255.255.255.0	200.200.202.254	0	WAN2	✎ 🗑

□ Select All

Figure 7- 18 Static Route List

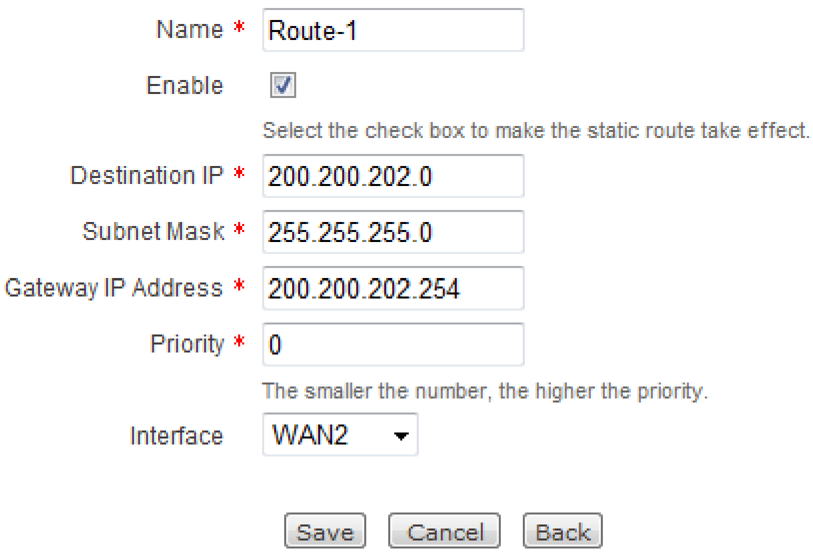
- **Add a Static Route:** To add a new static route, first click the **Add** button to go to the setup page, next configure it, lastly click the **Save** button.
- **View Static Route(s):** When you have configured one or more static routes, you can view them in the **Static Route List**.
- **Modify a Static Route:** To modify a configured static route, click its **Name** hyperlink

or ✎ icon, the related information will be displayed in the setup page. Then modify it, and click the **Save** button.

- **Delete Static Route(s):** There are three ways to delete static route(s).

1. To delete a static route, directly click its 🗑 icon.
2. To delete more than one static route at a time, select the leftmost check boxes of the static routes that you want to delete, and then click the **Delete** button.
3. To delete all the static routes at a time, directly click the **Delete All** button.

7.3.3 Static Route Settings



Name *	Route-1
Enable	☑ Select the check box to make the static route take effect.
Destination IP *	200.200.202.0
Subnet Mask *	255.255.255.0
Gateway IP Address *	200.200.202.254
Priority *	0 The smaller the number, the higher the priority.
Interface	WAN2

Figure 7- 19 Static Route Settings

- **Name:** It specifies a unique name of the static route.
- **Enable:** It allows you to enable or disable the static route. The default value is checked, which means the static route is in effect. If you want to disable the static route temporarily instead of deleting it, please clear the check box.
- **Destination IP:** It specifies the IP address of the destination network or destination host.
- **Subnet Mask:** It specifies the subnet mask associated with the destination network.
- **Gateway IP Address:** It specifies the IP address of the next hop gateway or router to which to forward the packets.
- **Priority:** It specifies the priority of the static route. If there are multiple routes to the same destination with different priorities, the Wireless Router will choose the route with the highest priority to forward the packets. The smaller the number, the higher

the priority.

- **Interface:** It specifies an outbound interface through which the packets are forwarded to the next hop gateway or router. The available options are LAN, WAN1, WAN2, APClient and 3G.

- **Save:** Click to save your changes.
- **Cancel:** Click to revert to the last saved settings.
- **Back:** Click to go back to the **Static Route List**.

7.3.4 How to Add Static Routes

To add one or more static routes, follow these steps:

Step 1 Go to the **Advanced > Static Route** page, and click the **Add** button to go to the setup page.

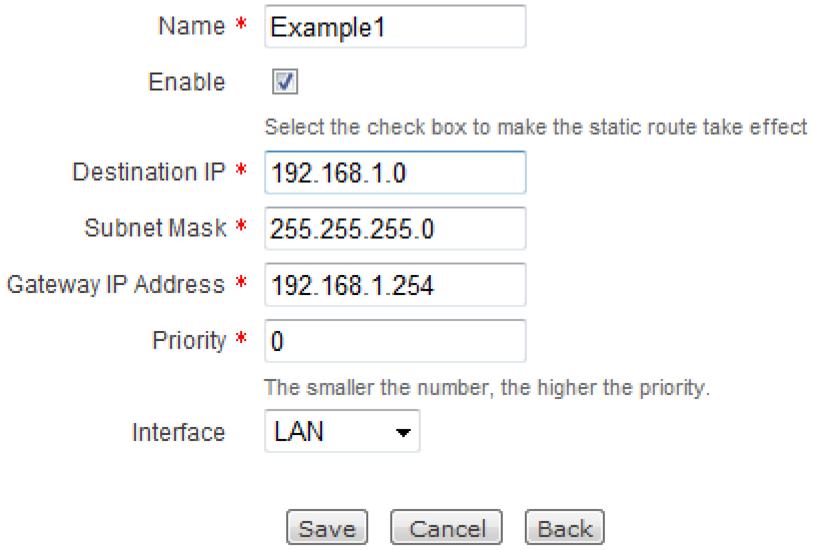
Step 2 Specify the **Name** for the static route, and leave the **Enable** check box checked.

Step 3 Specify the **Destination IP**, **Subnet Mask**, and **Gateway IP Address**.

Step 4 Specify the **Priority** as required.

Step 5 Select an outbound interface from the **Interface** drop-down list as required.

For example, if you want to add a static route for the network 192.168.1.0/24 pointing to 192.168.1.254, please choose **LAN** as the outbound interface. The following figure shows the detailed settings.



Name *	Example1
Enable	☑ Select the check box to make the static route take effect
Destination IP *	192.168.1.0
Subnet Mask *	255.255.255.0
Gateway IP Address *	192.168.1.254
Priority *	0 The smaller the number, the higher the priority.
Interface	LAN

Figure 7- 20 Static Route Settings - Example

Step 6 Click the **Save** button to save the settings. You can view the static route in the **Static Route List**.

Step 7 To add another new static route, please repeat the above steps.

✓ **Note**

If you want to delete static route(s), please follow the ways described in **Section 7.3.2 Static Route List**.

7.4 PPPoE Server

This section describes how to configure PPPoE server global settings and PPPoE account settings, and how to view PPPoE user status.

7.4.1 PPPoE Overview

The PPPoE stands for Point-to-Point Protocol over Ethernet, which uses client/server model. The PPPoE provides the ability to connect the Ethernet hosts to a remote Access Concentrator (AC) over a simple bridging access device. And it provides extensive access control management and accounting benefits to ISPs and network administrators.

The PPPoE is a network protocol for encapsulating PPP frames in Ethernet frames to provide point-to-point connection over an Ethernet network.

7.4.1.1 PPPoE Stages

As specified in RFC 2516, the PPPoE has two distinct stages: a discovery stage and a PPP session stage. The following describes them respectively.

7.4.1.2 PPPoE Discovery Stage

In the PPPoE discovery stage, a PPPoE client will find a proper server, and then build the connection. When a client initiates a PPPoE session, it should perform discovery to indentify the PPPoE server's Ethernet MAC address, and establish a PPPoE session ID.

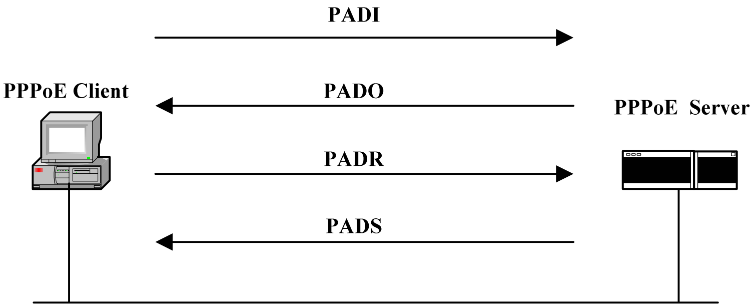


Figure 7- 21 PPPoE Discovery Stage Flows

As shown in Figure 7-21, the discovery stage includes the following four steps:

1. **PADI (PPPoE Active Discovery Initiation):** At the beginning, a PPPoE client

broadcasts a PADI packet to find all the servers that can be connected possibly. Until it receives PADO packets from one or more servers. The PADI packet must contain a service name which indicates the service requested by the client.

2. **PADO (PPPoE Active Discovery Offer):** When a PPPoE server receives a PADI packet in its service range, it will send a PADO response packet. The PADO packet must contain the server's name, and a service name identical to the one in the PADI, and any number of other service names which indicate other services that the PPPoE server can offer. If a PPPoE server receives a PADI packet beyond its service range, it cannot respond with a PADO packet.

3. **PADR (PPPoE Active Discovery Request):** The client may receive more than one PADO packet as the PADI was broadcast. The client chooses one server according to the server's name or the services offered. Then the client sends a PADR packet to the selected server. The PADR packet must contain a service name which indicates the service requested by the client.

4. **PADS (PPPoE Active Discovery Session- confirmation):** When a PPPoE server receives a PADR packet; it prepares to begin a PPP session. It generates a unique PPPoE session ID, and respond to the client with a PADS packet. The PADS packet must contain a service name which indicates the service provided to the client.

When the discovery stage completes successfully, both the server and client know the PPPoE session ID and the peer's Ethernet MAC address, which together define the PPPoE session uniquely.

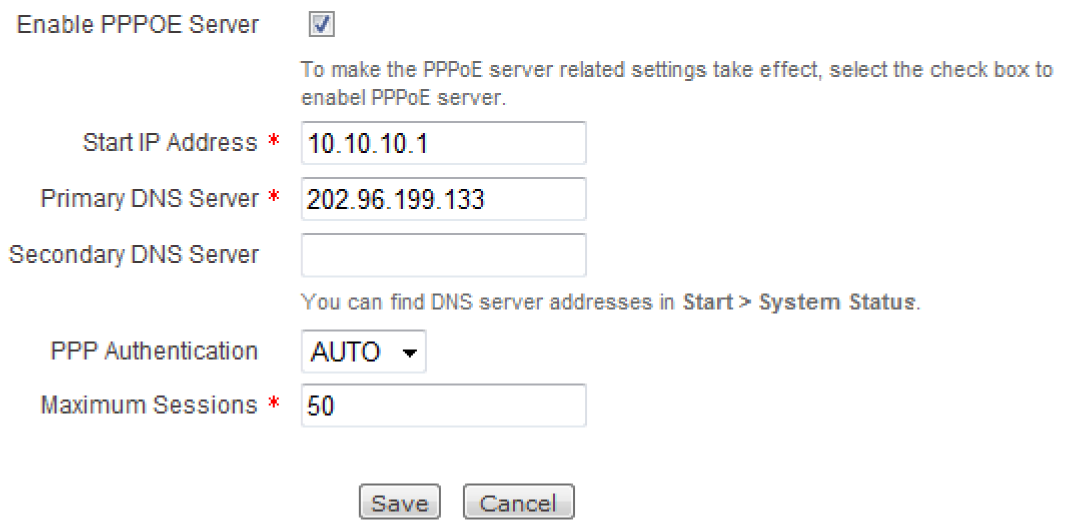
7.4.1.3 PPP Session Stage

In the PPP session stage, the server and client perform standard PPP negotiation to establish a PPP connection. After the PPP connection is established successfully, the original datagram are encapsulated in PPP frames, and PPP frames are encapsulated in PPPoE session frames, which have the Ethernet type 0x8864. Then these Ethernet frames are sent to the peer. In a PPPoE session frame, the session ID must be the value assigned in the Discovery stage, and cannot be changed in this session.

7.4.1.4 PPPoE Session Termination

After a session is established, either the server or client may send a PADT (PPPoE Active Discovery Terminate) packet at anytime to indicate the session has been terminated. The PADT packet's SESSION-ID must be set, to indicate which session is to be terminated. Once received a PADT, no further PPP packets (even normal PPP termination packets) are allowed to be sent using the specified session. A PPP peer should use the PPP protocol itself to terminate a PPPoE session, but can use the PADT packet to terminate the PPPoE session if PPP cannot be used.

7.4.2 PPPoE Server Global Settings



Enable PPPOE Server ☑

To make the PPPoE server related settings take effect, select the check box to enabel PPPoE server.

Start IP Address * 10.10.10.1

Primary DNS Server * 202.96.199.133

Secondary DNS Server

You can find DNS server addresses in **Start > System Status**.

PPP Authentication AUTO

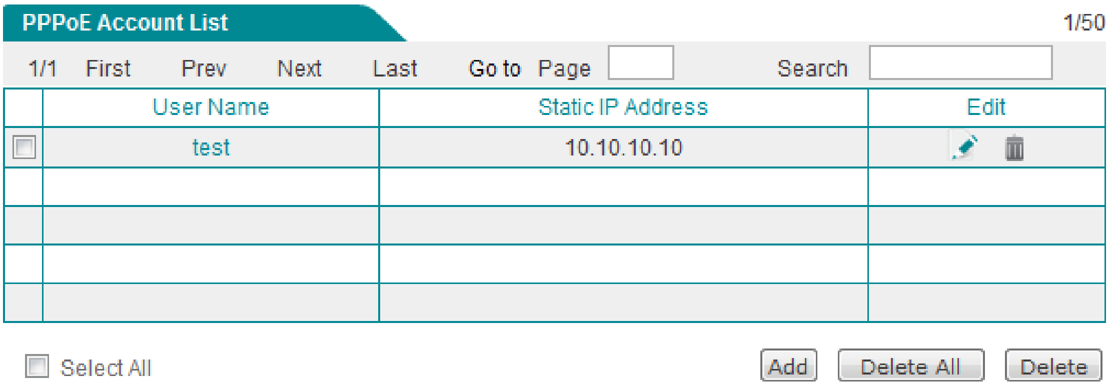
Maximum Sessions * 50

Figure 7- 22 PPPoE Server Global Settings

- **Enable PPPoE Server:** It allows you to enable or disable PPPoE server. If you want to enable PPPoE server on the Wireless Router, please select this check box.
- **Start IP Address:** It specifies the starting IP address that is assigned by the PPPoE server.
- **Primary DNS Server:** It specifies the IP address of the primary DNS server that is available to a PPPoE client.
- **Secondary DNS Server:** It specifies the IP address of the secondary DNS server that is available to a PPPoE client.
- **PPP Authentication:** It specifies the PPP authentication mode by which the PPPoE server authenticates a PPPoE client. The available options are **PAP**, **CHAP** and **AUTO**. In most cases, please leave the default value of **AUTO**, which means that the Wireless Router will automatically choose **PAP** or **CHAP** to authenticate the PPPoE client.
- **Maximum Sessions:** It specifies the maximum number of PPPoE sessions that can be created on the Wireless Router.

- **Save:** Click to save your changes.
- **Cancel:** Click to revert to the last saved settings.

7.4.3 PPPoE Account List



PPPoE Account List 1/50

1/1 First Prev Next Last Go to Page □ Search □

	User Name	Static IP Address	Edit
□	test	10.10.10.10	✎ 🗑

□ Select All

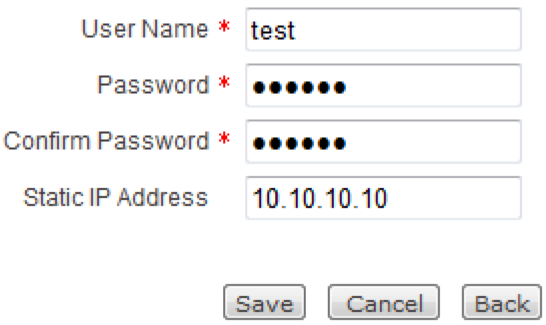
Figure 7-23 PPPoE Account List

- **Add a PPPoE Account:** To add a new PPPoE account, first click the **Add** button to go to the setup page, next configure it, lastly click the **Save** button.
- **View PPPoE Account(s):** When you have configured one or more PPPoE accounts, you can view them in the **PPPoE Account List**.
- **Modify a PPPoE Account:** To modify a configured PPPoE account, click its **User Name** hyperlink or ✎ icon, the related information will be displayed in the setup page. Then modify it, and click the **Save** button.
- **Delete PPPoE Account(s):** There are three ways to delete PPPoE account(s).

1. To delete a PPPoE account, directly click its 🗑 icon.
2. To delete more than one PPPoE account at a time, select the leftmost check boxes of the PPPoE accounts that you want to delete, and then click the **Delete** button.
3. To delete all the PPPoE accounts at a time, directly click the **Delete All** button.

7.4.4 PPPoE Account Settings

Go to the **Advanced > PPPoE Server > PPPoE Account Settings** page, and click the **Add** button to go to the setup page shown in Figure 7-24.



User Name *	test
Password *	●●●●●●
Confirm Password *	●●●●●●
Static IP Address	10.10.10.10

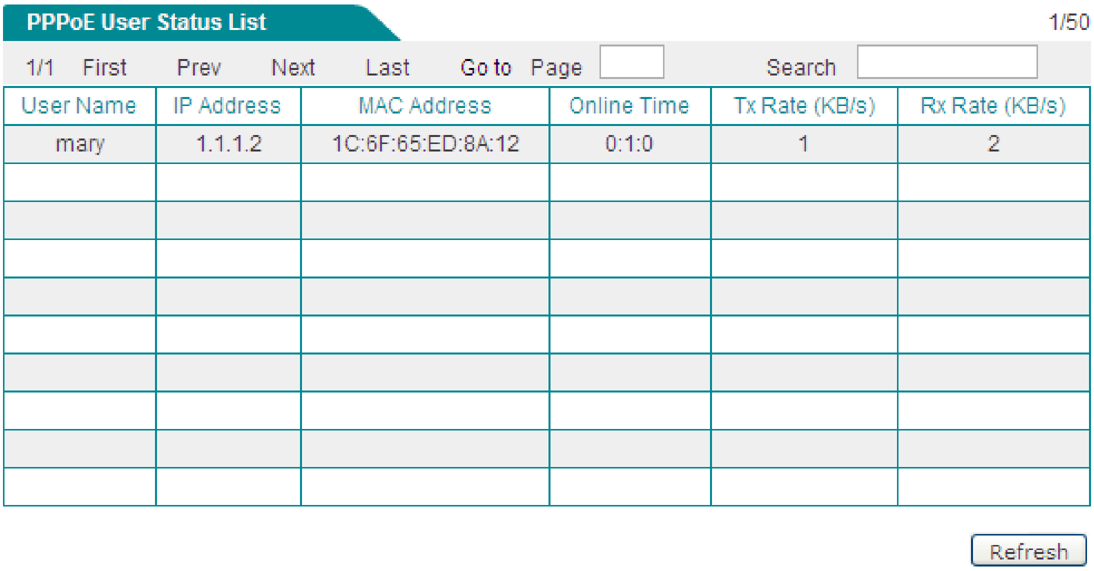
Figure 7- 24 PPPoE Account Settings

- **User Name:** It specifies a unique user name of the PPPoE account. It must be between 1 and 31 characters long. The PPPoE server will use **User Name** and **Password** to identify the PPPoE client.
- **Password**: It specifies the password of the PPPoE account.
- **Confirm Password:** You should re-enter the password.
- **Static IP Address:** It specifies a static IP address that is assigned to the user who uses the current PPPoE account. It must be a valid IP address within the range of IP addresses assigned by the PPPoE server.

- **Save:** Click to save your changes.
- **Cancel:** Click to revert to the last saved settings.
- **Back:** Click to go back to the **PPPoE Account List**.

7.4.5 PPPoE User Status

You can go to the **Advanced > PPPoE Server > PPPoE User Status** page view the status information of online PPPoE dial-in users in the **PPPoE User Status List**, which include the user name, assigned IP address, MAC address, Rx rate and Tx rate, and online time.



User Name	IP Address	MAC Address	Online Time	Tx Rate (KB/s)	Rx Rate (KB/s)
mary	1.1.1.2	1C:6F:65:ED:8A:12	0:1:0	1	2

Figure 7-25 PPPoE User Status List

- **User Name:** It displays the user name of the PPPoE account. The PPPoE dial-in user uses it to dial-up and establish the PPPoE session to the Wireless Router.
- **IP Address:** It displays the PPPoE dial-in user’s IP address assigned by the PPPoE server.
- **MAC Address:** It displays the PPPoE dial-in user’s MAC address.
- **Online Time:** It displays the elapsed time since the PPPoE session was established.
- **Tx Rate:** It displays the real-time upload rate (in kilobytes per second) of the PPPoE dial-in user.
- **Rx Rate:** It displays the real-time download rate (in kilobytes per second) of the PPPoE dial-in user.
- **Refresh:** Click to view the latest information in the list.

Chapter 8 User Management

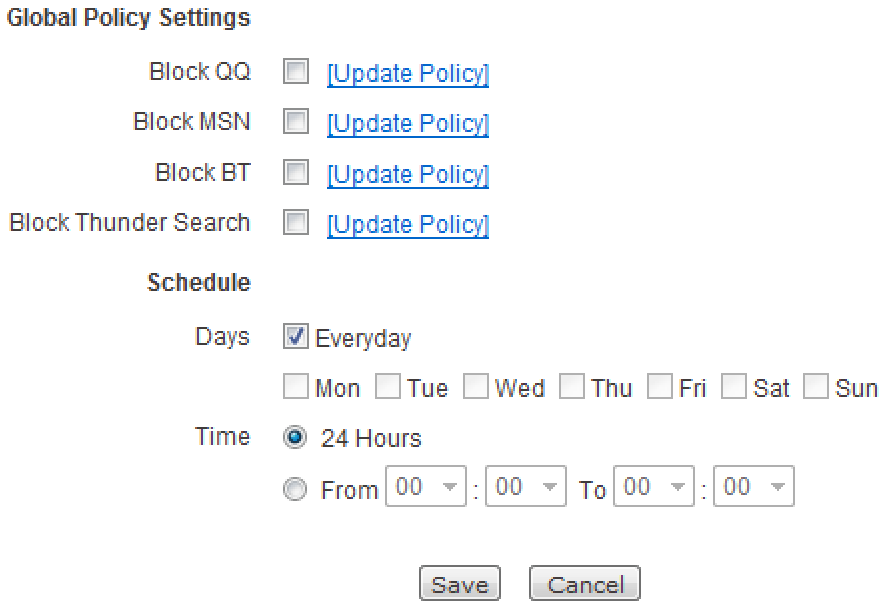
This chapter describes how to control and manage the Internet behaviors of the LAN users, including global management and group management.

8.1 Global Management

This section describes the **User > Global Management** page.

In this page, you can easily control and manage the Internet behaviors of the LAN users based on schedule, which include: allow or block the LAN users from using popular IM (e.g., QQ, MSN) and P2P applications (e.g., Bit Comet, Bit Spirit, Thunder Search) during the specified schedule. Using P2P applications in the LAN will impact the other users accessing the Internet, even cause network congestion and performance deterioration. You can block P2P applications to avoid such situations.

8.1.1 Global Management Policy Settings



Global Policy Settings

Block QQ □ [Update Policy]

Block MSN □ [Update Policy]

Block BT □ [Update Policy]

Block Thunder Search □ [Update Policy]

Schedule

Days ☑ Everyday

□ Mon □ Tue □ Wed □ Thu □ Fri □ Sat □ Sun

Time ● 24 Hours

○ From 00 : 00 To 00 : 00

Figure 8-1 Global Management Policy Settings

- **Block QQ:** It allows or blocks QQ application. If you want to block the LAN users from using QQ to chat with others, please select this check box.

- **Block MSN:** It allows or blocks MSN Messenger. If you want to block the LAN users from using MSN Messenger to chat with others, please select this check box.

- **Block BT:** It allows or blocks BitSpirit and BitComet applications. If you want to block the LAN users from using BitSpirit or BitComet to download files, please select this check box.

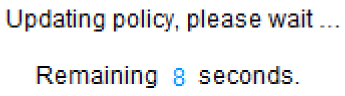
- **Block Thunder Search:** It allows or blocks Thunder search application. If you want to block the LAN users from using Thunder to search resources, please select this check box.

- **Schedule:** It allows you to define a schedule to restrict when the global management policy is in effect. By default, it is always in effect.

  - **Days:** It specifies the day(s) of the week during which the schedule is in effect. By default, the **Everyday** check box is checked, which means all days of the week. You may clear the **Everyday** check box, and then select any single day (Monday, Tuesday, Wednesday, Thursday, Friday, Saturday, or Sunday) or combinations of days as desired.

  - **Time:** It specifies a range of hours and minutes during which the schedule is in effect. By default, the **24 Hours** check box is checked, which means the schedule is in effect all day on the selected day(s). You may clear the **24 Hours** check box, and then choose the daily start time and end time as desired. If the start time is later than the end time, the system will automatically divide it into two time periods. E.g., if you select the **Mon** check box, and choose **23:00** and **06:00** as the daily start time and end time respectively, the schedule will be in effect during 00:00~06:00 and 23:00~23:59 on Monday.

- **Update Policy:** Click to update the corresponding policy. If you click the **Update Policy** hyperlink, the system will jump to the **Update Policy** page (see Figure 8-2), and go back to the **User > Global Management** page after the update is complete.



Updating policy, please wait ...

Remaining 8 seconds.

Figure 8-2 Updating Policy

- **Save:** Click to save your changes.

- **Cancel:** Click to revert to the last saved settings.

Note

The global management policy applies to the LAN users whose IP address is on the same subnet as the Wireless Router's LAN interface, and PPPoE dial-in users. Other users aren't subject to the policy.

8.1.2 An Example for Global Management Policy

A business uses a AC750W Wireless Router to access the Internet. The CEO wants to block the employees from using MSN and BT applications during business hours (Monday to Friday, 9:00 to 17:00).

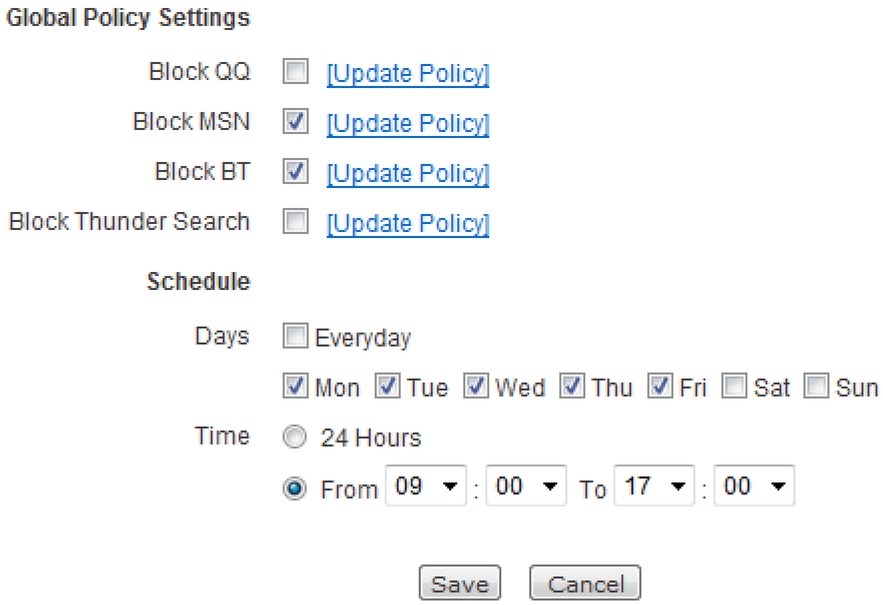
The configuration steps are the following:

Step 1 Go to the **User > Global Management** page.

Step 2 Select the **Block MSN** and **Block BT** check boxes.

Step 3 Define business hours: clear the **Everyday** check box, next select the **Mon**, **Tue**, **Wed**, **Thu**, and **Fri** check boxes; clear the **24 Hours** check box, next choose **09:00** and **17:00** as the daily start time and end time respectively. The above settings are shown in Figure 8-3.

Step 4 Click the **Save** button to save your settings.



Global Policy Settings

Block QQ □ [Update Policy]

Block MSN ☑ [Update Policy]

Block BT ☑ [Update Policy]

Block Thunder Search □ [Update Policy]

Schedule

Days □ Everyday

☑ Mon ☑ Tue ☑ Wed ☑ Thu ☑ Fri □ Sat □ Sun

Time ○ 24 Hours

● From 09 : 00 To 17 : 00

Figure 8-3 Global Management Policy - Example

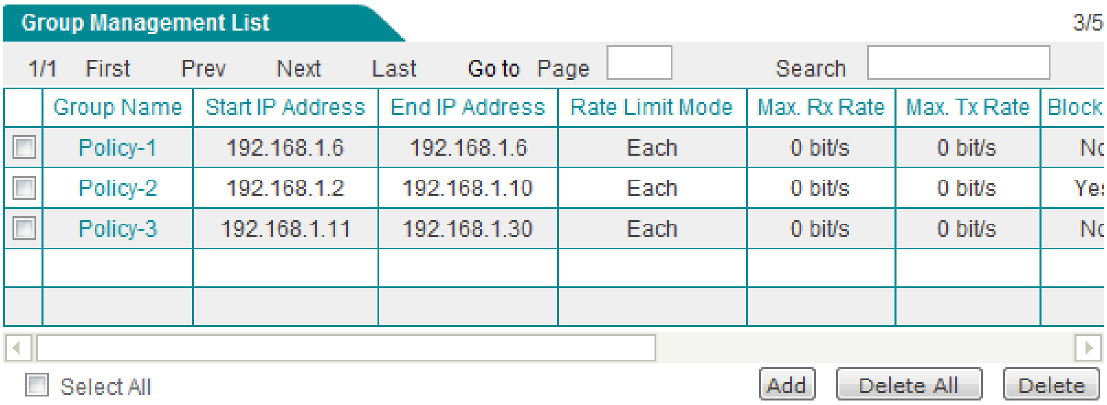
8.2 Group Management

This section describes the **User > Group Management** page.

In this page, you can group the users that have the same Internet access privileges into a user group, and assign a range of contiguous IP addresses to them. After that, you can create group management policies for each group based on schedule. For convenience, a group can also contain a single user.

A group management policy is used to control the Internet behaviors of the users in the group, which include: allow or block these users from using popular IM (e.g., QQ, MSN) and P2P applications (e.g., Bit Comet, Bit Spirit, Thunder Search) during the specified schedule; in addition, it is also used to control the maximum upload and download rate of these users during the specified schedule.

8.2.1 Group Management Policy List



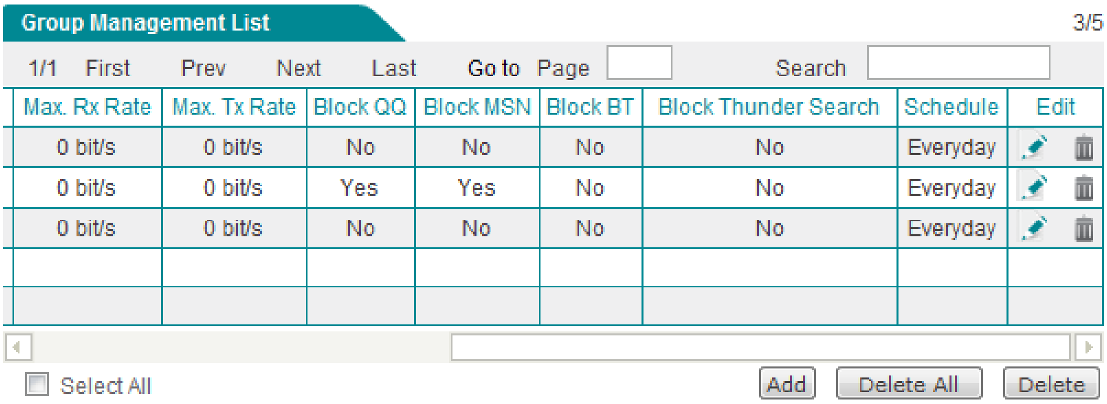
Group Management List 3/5

1/1 First Prev Next Last Go to Page Search

	Group Name	Start IP Address	End IP Address	Rate Limit Mode	Max. Rx Rate	Max. Tx Rate	Block
□	Policy-1	192.168.1.6	192.168.1.6	Each	0 bit/s	0 bit/s	N
□	Policy-2	192.168.1.2	192.168.1.10	Each	0 bit/s	0 bit/s	Ye
□	Policy-3	192.168.1.11	192.168.1.30	Each	0 bit/s	0 bit/s	N

□ Select All Add Delete All Delete

Figure 8- 4 Group Management Policy List



Group Management List 3/5

1/1 First Prev Next Last Go to Page Search

Max. Rx Rate	Max. Tx Rate	Block QQ	Block MSN	Block BT	Block Thunder Search	Schedule	Edit
0 bit/s	0 bit/s	No	No	No	No	Everyday	✎ 🗑
0 bit/s	0 bit/s	Yes	Yes	No	No	Everyday	✎ 🗑
0 bit/s	0 bit/s	No	No	No	No	Everyday	✎ 🗑

□ Select All Add Delete All Delete

Figure 8- 5 Group Management Policy List (Continue)

- **Add a Group Management Policy:** To add a new group management policy, first click the **Add** button to go to the **Group Management Settings** page, next configure it, lastly click the **Save** button.

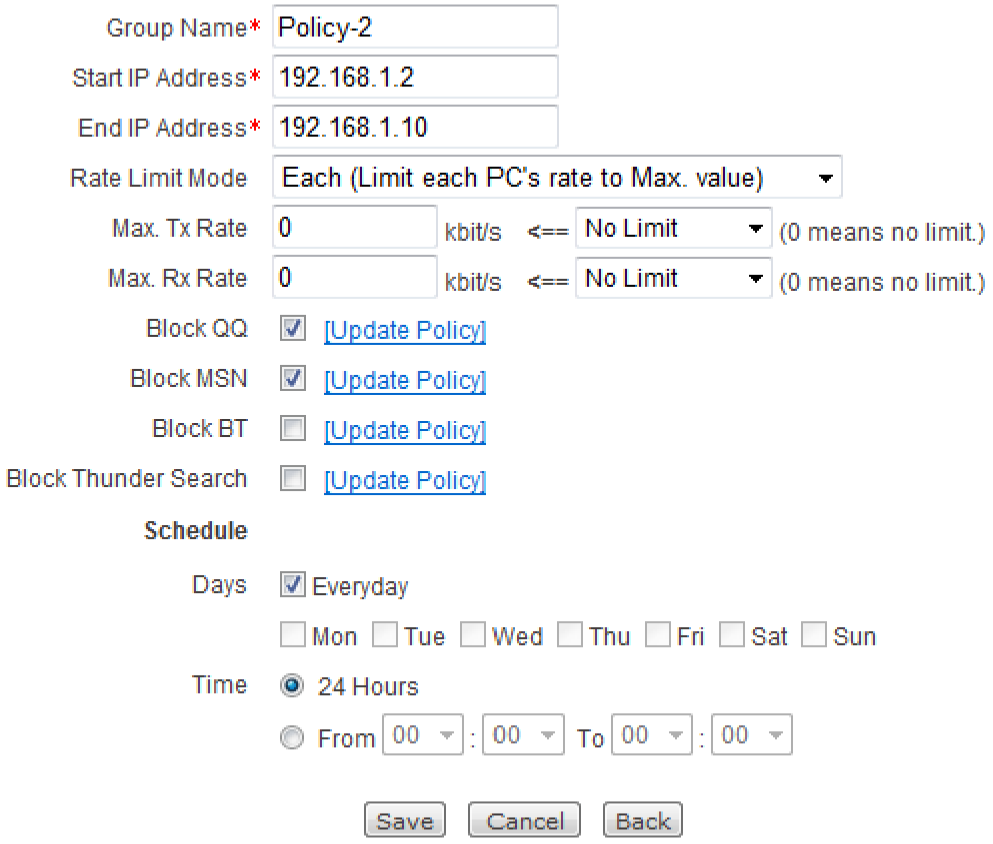
- **View Group Management Policy(s):** When you have configured one or more group management policies, you can view them in the **Group Management List**.

- **Modify a Group Management Policy:** To modify a configured group management policy, click its **Group Name** hyperlink or ✎ icon, the related information will be displayed in the setup page. Then modify it, and click the **Save** button.

- **Delete Group Management Policy(s):** There are three ways to delete group management policy(s).

  1. To delete a group management policy, directly click its 🗑 icon.
  2. To delete more than one group management policy at a time, select the leftmost check boxes of the policies that you want to delete, and then click the **Delete** button.
  3. To delete all the group management policies at a time, directly click the **Delete All** button.

8.2.2 Group Management Policy Settings



Group Name* Policy-2

Start IP Address* 192.168.1.2

End IP Address* 192.168.1.10

Rate Limit Mode Each (Limit each PC's rate to Max. value)

Max. Tx Rate 0 kbit/s <== No Limit (0 means no limit.)

Max. Rx Rate 0 kbit/s <== No Limit (0 means no limit.)

Block QQ ☑ [Update Policy]

Block MSN ☑ [Update Policy]

Block BT □ [Update Policy]

Block Thunder Search □ [Update Policy]

Schedule

Days ☑ Everyday

□ Mon □ Tue □ Wed □ Thu □ Fri □ Sat □ Sun

Time ● 24 Hours

○ From 00 : 00 To 00 : 00

Figure 8-6 Group Management Policy Settings

- **Group Name:** It specifies a unique name of group.
- **Start IP Address** and **End IP Address:** They specify a range of contiguous IP addresses. All the computers within the specified range are members of the group, and are subject to the group management policy.
- **Rate Limit Mode:** It specifies the mode by which the Wireless Router will limit the maximum Tx/Rx rate of the LAN computers belonging to the group.
  - **Each:** If you select this option, the Tx/Rx rate of each computer can reach up to the **Max. Tx Rate/ Max. Rx Rate** you specify.
  - **Share:** If you select this option, the total Tx/Rx rate of all computers in the group can reach up to the **Max. Tx Rate/ Max. Rx Rate** you specify.
- **Max. Tx Rate:** It specifies the maximum upload rate (in Kbit/s) of the LAN computers belonging to the group.
- **Max. Rx Rate:** It specifies the maximum download rate (in Kbit/s) of the LAN computers belonging to the group. There are two ways to set the **Max. Tx Rate** and **Max. Rx Rate**.
  - Enter a value in the associated text box. If you don't want to limit **Max. Tx Rate/ Max. Rx Rate**, please leave the default value of **0**.
  - Select an option from the associated drop-down list. If you don't want to **Max. Tx Rate/ Max. Rx Rate**, please leave the default value of **No Limit**.
- **Block QQ**, **Block MSN**, **Block BT**, **Block Thunder Search**, and **Schedule**: Refer to **Section 8.1.1 Global Management Policy Settings** for detailed information.

- **Update Policy:** Click to update the corresponding policy. Refer to **Section 8.1.1 Global Management Policy Settings** for detailed operation.
- **Save:** Click to save your changes.
- **Cancel:** Click to revert to the last saved settings.
- **Back:** Click to go back to the **Group Management List**.

Note

1. The policy management policies take priority over the global management policy.
2. The Wireless Router supports up to five group management policies.
3. If both **Start IP Address** and **End IP Address** are set to 0.0.0.0, the group will contain all computers on the LAN no matter what IP address they might have. In this case, the Wireless Router will check all the packets initiated from the LAN computers, so the system performance will be degraded to some extent. Therefore, you'd better not set them to 0.0.0.0.

8.2.3 Execution Order of Group Management Policies

If a user's computer belongs to more than one group, in other words, if the user matches more than one group management policy, it will be subject to the first one added. More specifically, after you configure some group management policies, the Wireless Router will search the **Group Management List** to find out if there is a policy matching a user. It will check the user's IP address against each policy in the order in which the policies are listed. The first matching policy will apply to the user. Note that the policies are listed in chronological order of creation (i.e., most recent at the bottom).

8.2.4 Priorities of Global and Group Management Policies and Access Rules

The access rules have higher priority than the group management policies, and the group management policies have higher priority than the global management policy. That is, when receiving a packet initiated from a local computer, the Wireless Router will first check it against the access rules, next the group management policies, lastly the global management policy. The first rule (or policy) that matches the packet is applied. After a match is found, no further rules or policies are checked.

For example, if you have selected the **Block MSN** check box in the **User > Global Management** page, added a group management policy which allows a group of users to use MSN (**Block MSN** check box is cleared) in the **User > Group Management** page, and added an access rule which denies all users access to the Internet in the **Firewall > Access Control** page, then any users are unable to access the Internet because the access rule is matched first. Now if you only delete the access rule, then the users belong to the specified group can use MSN, but other users cannot.

8.2.5 An Example for Group Management Policy

1. Requirements

A business uses a AC750W Wireless Router to access the Internet. The CEO wants to control Internet behaviors of the employees of the Administration Department and Business Department:

1) Block the Administration Department's employees (IP range: 192.168.1.2-192.168.1.10) from using MSN and QQ, and allow them to access all other services.

The exception is that the CEO with IP address 192.168.1.6 can access any services.

2) Allow the Business Department's employees (IP range: 192.168.1.11-192.168.1.30) to access any services.

2. Analysis

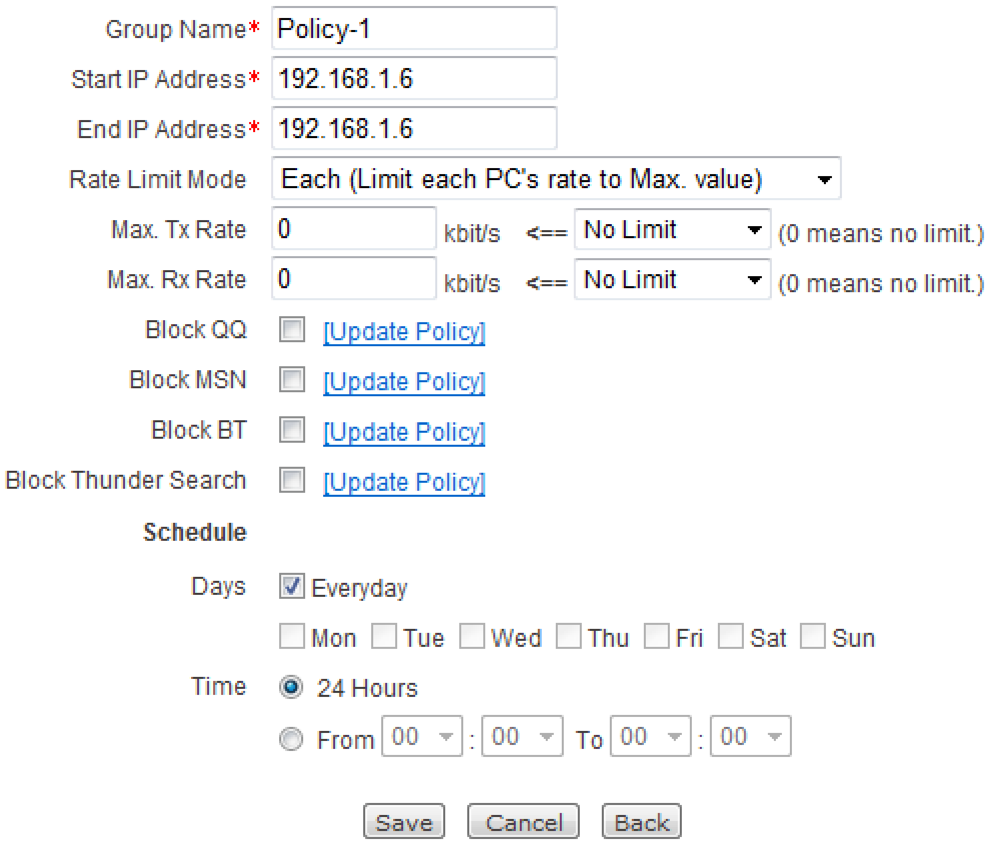
We need to create three group management policies to meet the requirements:

- Group management policy 1: It allows the CEO to access all Internet services.
- Group management policy 2: It blocks the Administration Department's employees from using QQ and MSN.
- Group management policy 3: It allows the Business Department's employees to access all Internet services.

3. Configuration Steps

Step 1 Go to the **User > Group Management** page.

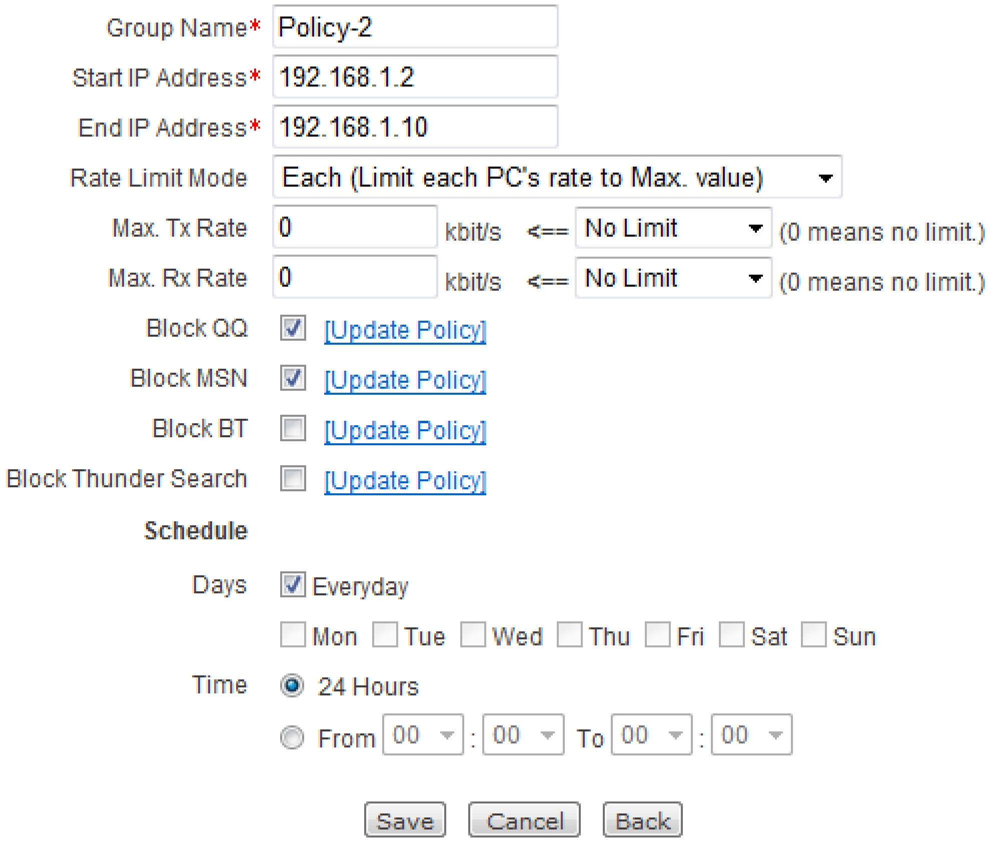
Step 2 Click the **Add** button to go to the **Group Management Settings** page to create the policy 1. The detailed settings are shown in Figure 8-7.



Group Name*	Policy-1
Start IP Address*	192.168.1.6
End IP Address*	192.168.1.6
Rate Limit Mode	Each (Limit each PC's rate to Max. value)
Max. Tx Rate	0 kbit/s <== No Limit (0 means no limit.)
Max. Rx Rate	0 kbit/s <== No Limit (0 means no limit.)
Block QQ	□ [Update Policy]
Block MSN	□ [Update Policy]
Block BT	□ [Update Policy]
Block Thunder Search	□ [Update Policy]
Schedule	
Days	☑ Everyday
	□ Mon □ Tue □ Wed □ Thu □ Fri □ Sat □ Sun
Time	● 24 Hours
	○ From 00 : 00 To 00 : 00

Figure 8-7 Group Management Policy Example - Policy 1

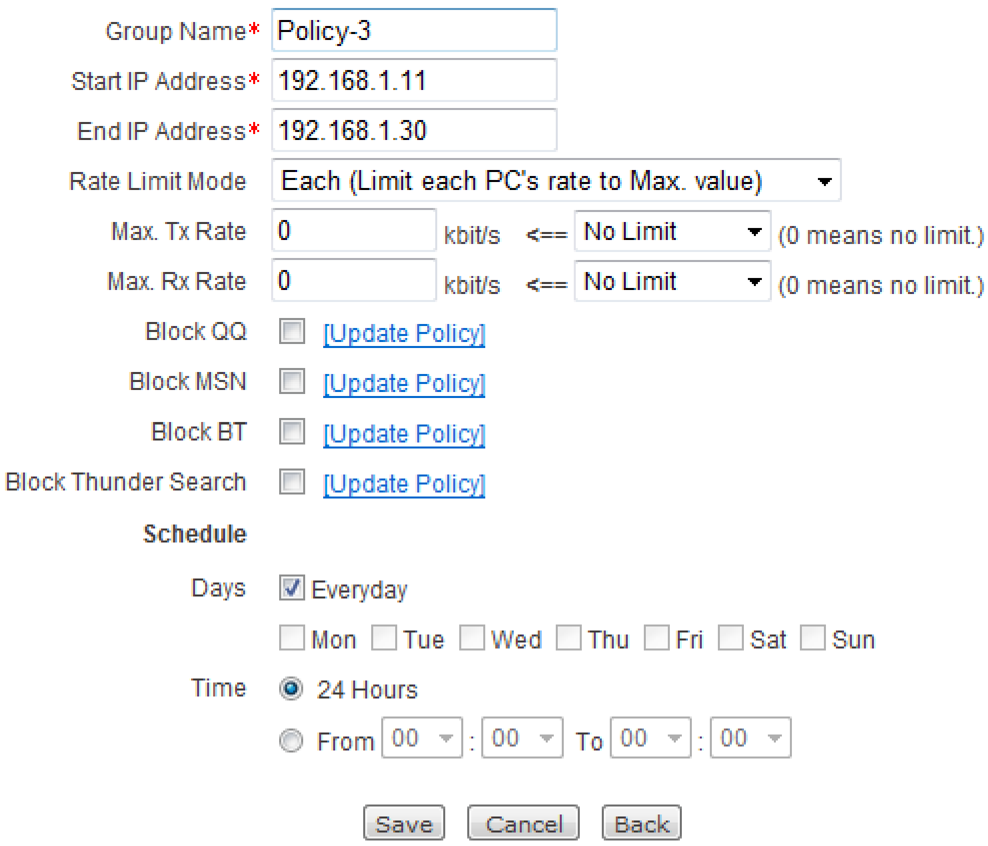
Step 3 Click the **Add** button to go to the **Group Management Settings** page to create the policy 2. The detailed settings are shown in Figure 8-8.



Group Name*	Policy-2
Start IP Address*	192.168.1.2
End IP Address*	192.168.1.10
Rate Limit Mode	Each (Limit each PC's rate to Max. value)
Max. Tx Rate	0 kbit/s <== No Limit (0 means no limit.)
Max. Rx Rate	0 kbit/s <== No Limit (0 means no limit.)
Block QQ	☑ [Update Policy]
Block MSN	☑ [Update Policy]
Block BT	□ [Update Policy]
Block Thunder Search	□ [Update Policy]
Schedule	
Days	☑ Everyday
	□ Mon □ Tue □ Wed □ Thu □ Fri □ Sat □ Sun
Time	● 24 Hours
	○ From 00 : 00 To 00 : 00

Figure 8-8 Group Management Policy Example - Policy 2

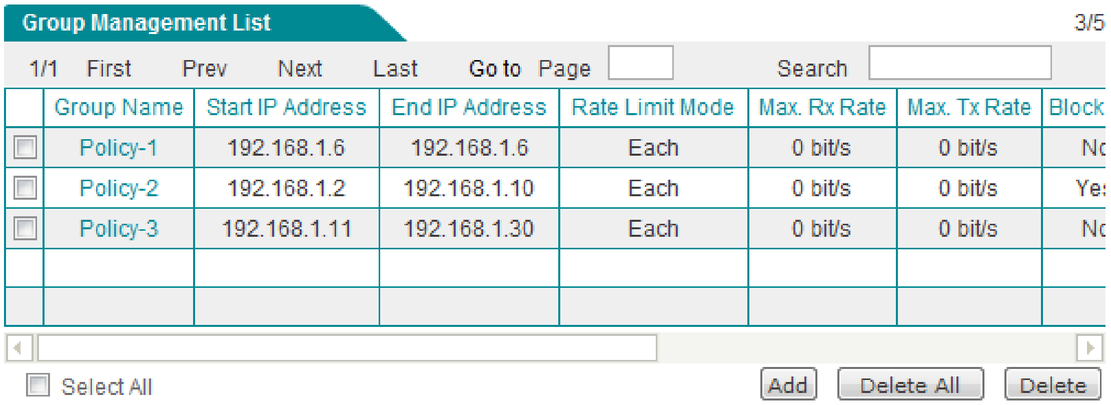
Step 4 Click the **Add** button to go to the **Group Management Settings** page to create the policy 3. The detailed settings are shown in Figure 8-9.



Group Name*	Policy-3
Start IP Address*	192.168.1.11
End IP Address*	192.168.1.30
Rate Limit Mode	Each (Limit each PC's rate to Max. value)
Max. Tx Rate	0 kbit/s <== No Limit (0 means no limit.)
Max. Rx Rate	0 kbit/s <== No Limit (0 means no limit.)
Block QQ	□ [Update Policy]
Block MSN	□ [Update Policy]
Block BT	□ [Update Policy]
Block Thunder Search	□ [Update Policy]
Schedule	
Days	☑ Everyday
	□ Mon □ Tue □ Wed □ Thu □ Fri □ Sat □ Sun
Time	● 24 Hours
	○ From 00 : 00 To 00 : 00

Figure 8- 9 Group Management Policy Example - Policy 3

Step 5 After you have configured the three policies, you can view them in the **Group Management List**, see Figure 8- 10.



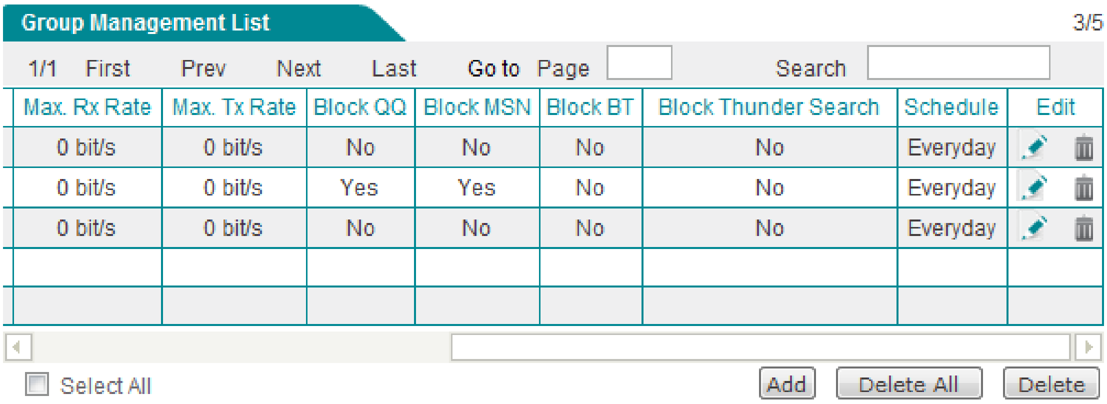
Group Management List 3/5

1/1 First Prev Next Last Go to Page Search

	Group Name	Start IP Address	End IP Address	Rate Limit Mode	Max. Rx Rate	Max. Tx Rate	Block
□	Policy-1	192.168.1.6	192.168.1.6	Each	0 bit/s	0 bit/s	Nc
□	Policy-2	192.168.1.2	192.168.1.10	Each	0 bit/s	0 bit/s	Ye:
□	Policy-3	192.168.1.11	192.168.1.30	Each	0 bit/s	0 bit/s	Nc

□ Select All

Figure 8- 10 Group Management List – Example



Max. Rx Rate	Max. Tx Rate	Block QQ	Block MSN	Block BT	Block Thunder Search	Schedule	Edit
0 bit/s	0 bit/s	No	No	No	No	Everyday	
0 bit/s	0 bit/s	Yes	Yes	No	No	Everyday	
0 bit/s	0 bit/s	No	No	No	No	Everyday	

Figure 8- 11 Group Management List – Example (Continue)

Chapter 9 Firewall

This chapter describes how to configure firewall features, including access control, domain filtering, and attack prevention.

9.1 Access Control

This section describes the **Firewall > Access Control** page, which includes the **Access Rule List** and **Access Rule Settings**.

9.1.1 Introduction to Access Control

9.1.1.1 The Purpose of Access Control Feature

By flexibly utilizing access control, you can not only assign different Internet access privileges to different LAN users, but also assign different Internet access privileges to the same users based on schedules. In practice, you can set appropriate access rules according to the actual requirements of your organization. Such as, for a school, you can block the students from accessing game websites; for a family, you can only allow your children to access the Internet during the specified period of time; for a business, you can block the Financial Department's employees from accessing the Internet.

9.1.1.2 The Operation Principle of Access Control

By default, the Wireless Router will forward all the valid packets received by the LAN interface because no access rule exists. After you have configured some access rules, the Wireless Router will examine each packet received by the LAN interface to determine whether to forward or drop it, based on the criteria you specified in the access rules.

More specifically, when receiving a packet initiated from LAN, the Wireless Router will analyze the packet by extracting its source MAC address, source IP address, destination IP address, protocol type, port number, content, and the date and time at which the packet was received, and then compare them with each rule in decreasing order of priority. The first rule that matches the packet is applied, and the specified **Action** (**Allow** or **Deny**) is taken. After a match is found, no further rules are checked. Note that the rules are listed in decreasing order of priority in the **Access Rule List**: The rule with a higher priority is listed before the one with a lower priority.

9.1.1.3 Filtering Type of Access Rule

The Wireless Router supports three filtering types of access rule, which include IP filtering, URL filtering and keyword filtering. All of them support access control based on schedule.

1. IP Filtering

The IP filtering rules are used to filter IP packets based on the packet header information, such as source IP address, destination IP address, protocol type (TCP, UDP, ICMP, etc.), TCP/UDP source port and destination port.

The filtering criteria that you can specify within an IP filtering rule include: source IP address, destination IP address, protocol, source port, destination port, and schedule.

2. URL Filtering

The URL filtering rules are used to filter URLs based on keyword in the URL. It allows you to filter any web page whose URL contains the specified keyword. For example, if you want to block sex related websites, you can use the URL keyword “sex”. This will block any web page whose URL contains sex, such as www.sexpicture.com. Of course, you can use the full URL (like “www.yahoo.com”) to filter only the specified URL.

The filtering criteria that you can specify within a URL filtering rule include: source IP address, filtering content (i.e., URL keyword), and schedule.

3. Keyword Filtering

The keyword filtering rules are used to block users from submitting information to the web page based on keyword, that is, the information that contains the specified keyword (such as pornography, gambling, etc.) cannot be submitted to any web page. The Wireless Router supports both Chinese and English keyword filtering.

The filtering criteria that you can specify within a keyword filtering rule include: source IP address, filtering content (i.e., keyword in the web page), and schedule.

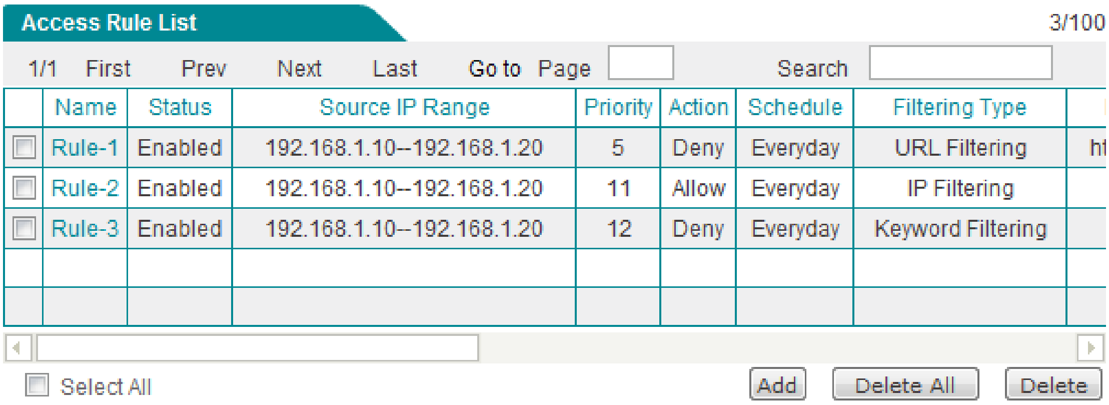
9.1.1.4 Action of Access Rule

The action of an access rule is either **Allow** or **Deny**. As mentioned earlier, the Wireless

Router checks each received packet against the access rules in the **Access Rule List**, and the first access rule that matches a packet determines whether the Wireless Router accepts or drops the packet. If the rule's **Action** is **Allow**, the packet is forwarded. If the rule's **Action** is **Deny**, the packet is dropped.

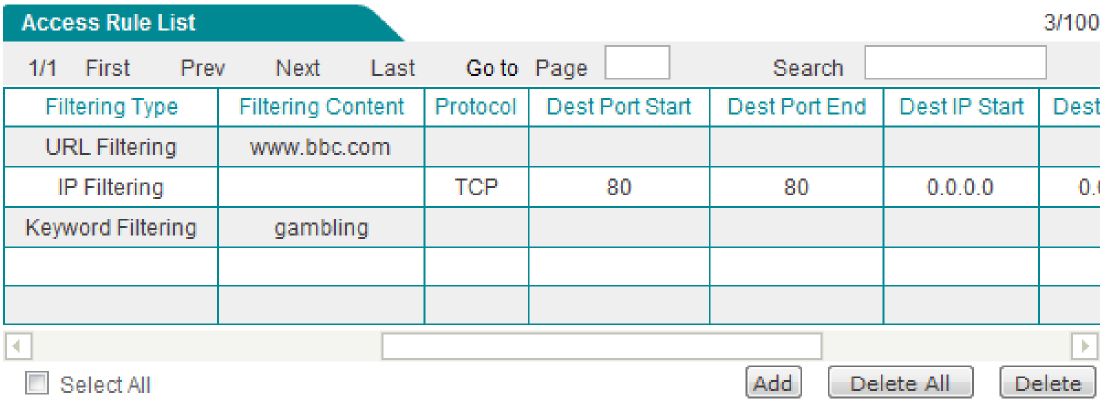
Note that keyword filtering rules only support the **Deny** action.

9.1.2 Access Rule List



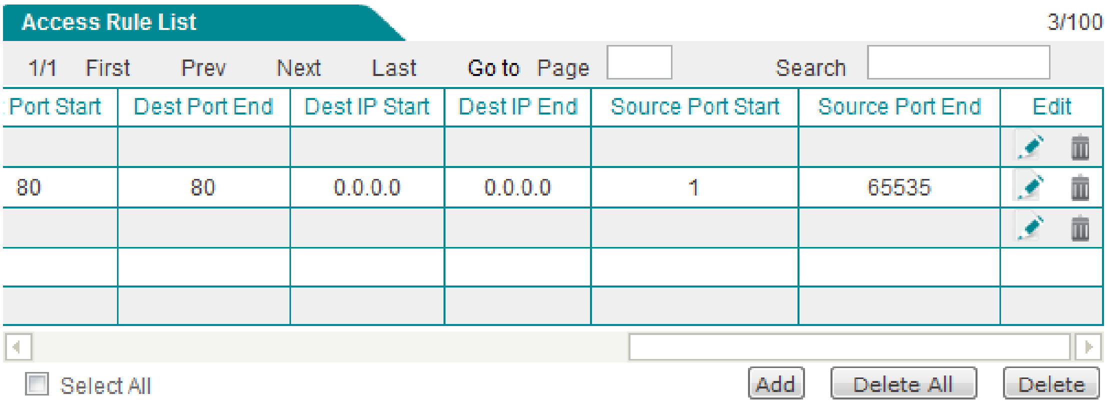
	Name	Status	Source IP Range	Priority	Action	Schedule	Filtering Type	
□	Rule-1	Enabled	192.168.1.10--192.168.1.20	5	Deny	Everyday	URL Filtering	ht
□	Rule-2	Enabled	192.168.1.10--192.168.1.20	11	Allow	Everyday	IP Filtering	
□	Rule-3	Enabled	192.168.1.10--192.168.1.20	12	Deny	Everyday	Keyword Filtering	

Figure 9- 1 Access Rule List



Filtering Type	Filtering Content	Protocol	Dest Port Start	Dest Port End	Dest IP Start	Dest
URL Filtering	www.bbc.com					
IP Filtering		TCP	80	80	0.0.0.0	0.(
Keyword Filtering	gambling					

Figure 9- 2 Access Rule List (Continue)



Port Start	Dest Port End	Dest IP Start	Dest IP End	Source Port Start	Source Port End	Edit
						✎ 🗑
80	80	0.0.0.0	0.0.0.0	1	65535	✎ 🗑
						✎ 🗑

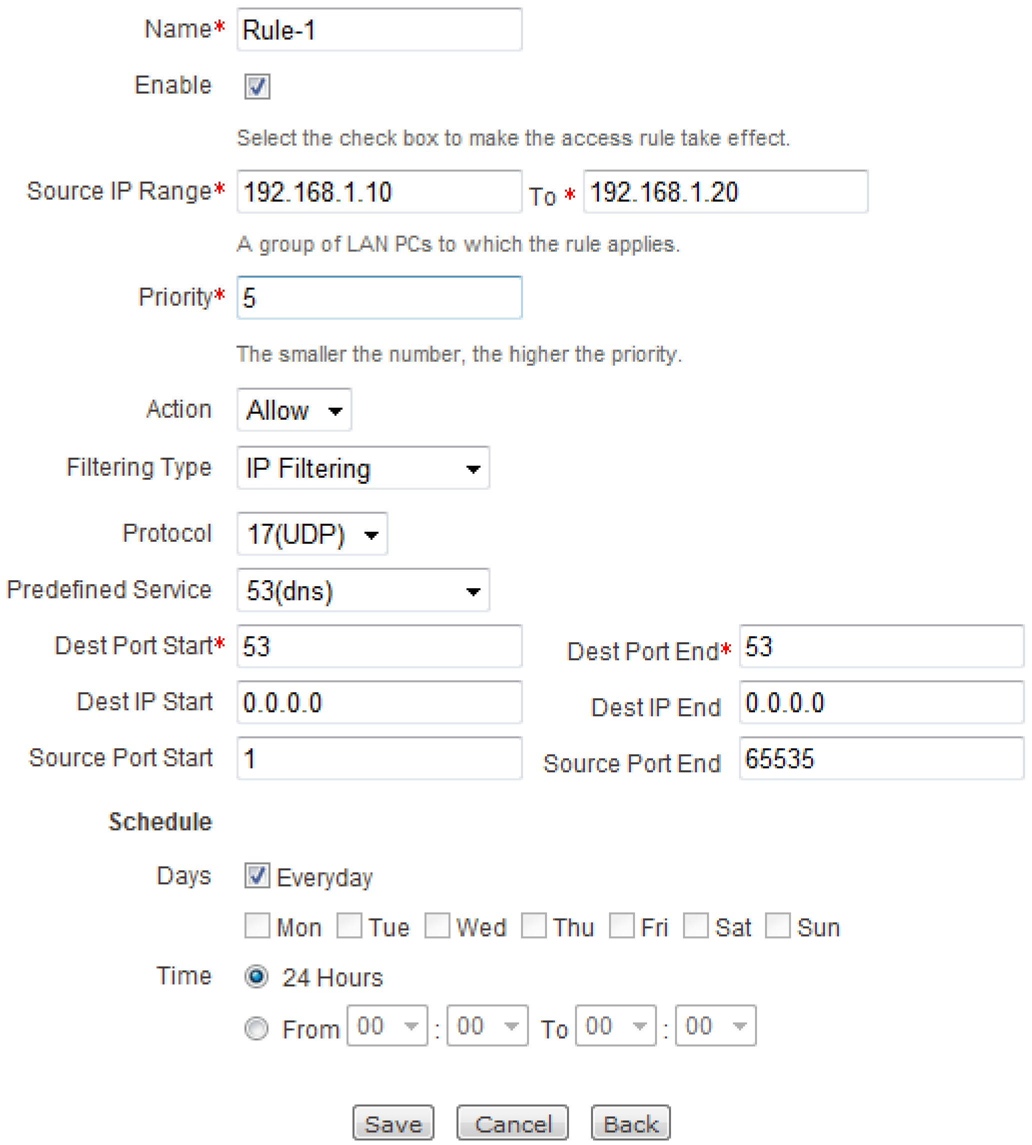
Figure 9- 3 Access Rule List (Continue)

- **Add an Access Rule:** To add a new access rule, first click the **Add** button to go to the **Access Rule Settings** page, next configure it, lastly click the **Save** button.
- **View Access Rule(s):** When you have configured one or more access rules, you can view them in the **Access Rule List**.
- **Modify an Access Rule:** To modify a configured access rule, click its **Name** hyperlink or ✎ icon, the related information will be displayed in the setup page. Then modify it, and click the **Save** button.
- **Delete Access Rule(s):** There are three ways to delete access rule(s).
  1. To delete a access rule, directly click its 🗑 icon.
  2. To delete more than one access rule at a time, select the leftmost check boxes of the access rules that you want to delete, and then click the **Delete** button.
  3. To delete all the access rules at a time, directly click the **Delete All** button.

9.1.3 Access Rule Settings

The following sections describe three types of access rule respectively, which include IP filtering, URL filtering and keyword filtering.

9.1.3.1 Access Rule Settings - IP Filtering



Name* Rule-1

Enable ☑

Select the check box to make the access rule take effect.

Source IP Range* 192.168.1.10 To * 192.168.1.20

A group of LAN PCs to which the rule applies.

Priority* 5

The smaller the number, the higher the priority.

Action Allow

Filtering Type IP Filtering

Protocol 17(UDP)

Predefined Service 53(dns)

Dest Port Start* 53 Dest Port End* 53

Dest IP Start 0.0.0.0 Dest IP End 0.0.0.0

Source Port Start 1 Source Port End 65535

Schedule

Days ☑ Everyday

□ Mon □ Tue □ Wed □ Thu □ Fri □ Sat □ Sun

Time ● 24 Hours

○ From 00 : 00 To 00 : 00

Figure 9- 4 Access Rule Settings - IP Filtering

- **Name:** It specifies a unique name of the access rule.
- **Enable:** It allows you to enable or disable the access rule. The default value is checked, which means the access rule is in effect. If you want to disable the rule temporarily instead of deleting it, please clear the check box.
- **Source IP Range:** It specifies a range of source IP addresses (i.e., a group of local computers) to which the access rule applies. To specify a single local computer, enter its address in both text boxes.
- **Prority:** It specifies the priority of the access rule. The access rules will be checked against the packets in descending order of priority. It must be between 0 and 100. The smaller the number, the higher the priority. And the priority of each access rule cannot

be repeated.

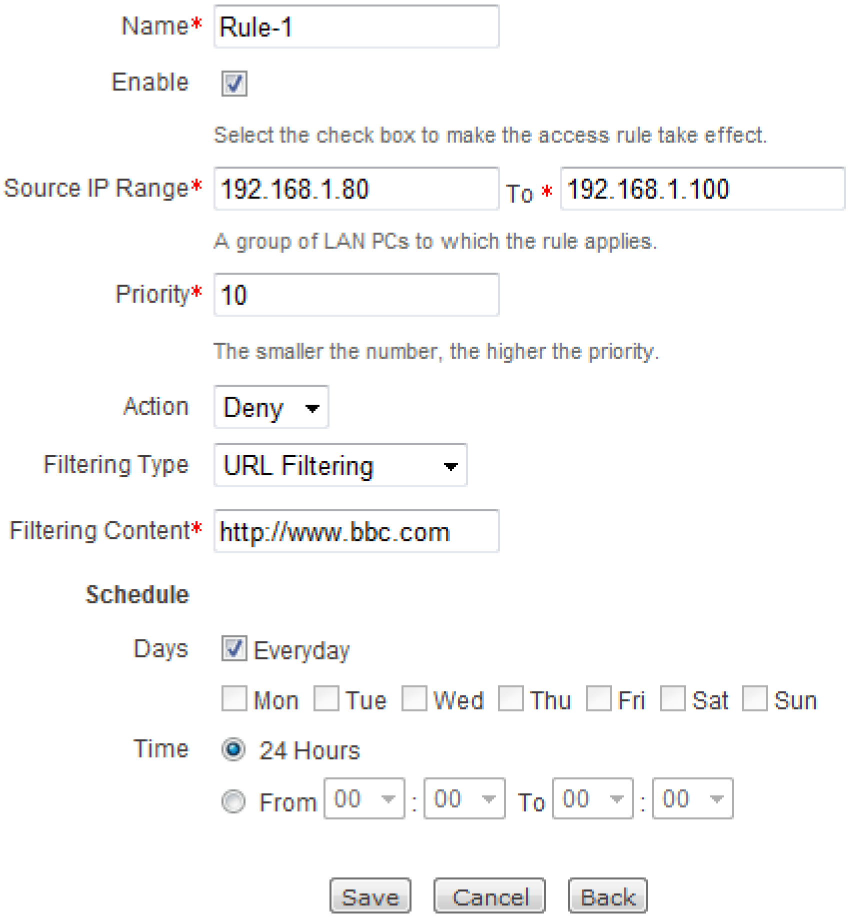
- **Action:** It specifies the action to be taken if a packet matches the access rule. The available options are **Allow** and **Deny**.
  - **Allow:** It indicates that the Wireless Router will allow the packets matching the rule, that is, the Wireless Router will forward these packets.
  - **Deny:** It indicates that the Wireless Router will deny the packets matching the rule, that is, the Wireless Router will drop these packets.
- **Filtering Type:** It specifies the filtering type of the access rule. The options are **IP Filtering**, **URL Filtering**, and **Keyword Filtering**. Here please select **IP Filtering**.
- **Protocol:** It specifies the protocol to which the access rule applies. The options are **1 (ICMP)**, **6 (TCP)**, **17 (UDP)**, **51 (AH)**, and **All**. Select **All** if you want to the rule to apply to all protocols. **Apendix C** provides the list of common IP protocols and their protocol numbers.
- **Predefined Service:** It provides some of the most common services and their associated port numbers. Select **All** if you want to the rule to apply to all ports 1-65535). **Apendix D** provides the list of common services and their port numbers.
- **Dest Port Start** and **Dest Port End:** They specify a range of destination ports to which the access rule applies. To specify a single port, enter the port number in both text boxes. The port number must be between 1 and 65535.
- **Dest IP Start** and **Dest IP End:** They specify a range of destination IP addresses to which the access rule applies. To specify a single IP addres, enter the port number in both text boxes.
- **Source Port Start** and **Source Port End:** They specify a range of source ports to which the access rule applies. To specify a single port, enter the port number in both text boxes. The port number must be between 1 and 65535.
- **Schedule:** It allows you to specify when the access rule is in effect. By default, the access rule is always in effect.

- **Save:** Click to save your changes.
- **Cancel:** Click to revert to the last saved settings.
- **Back:** Click to go back to the **Access Rule List**.

✓ **Note**

By default, the **Source IP Range** is from 0.0.0.0 to 0.0.0.0, which means the access rule applies to all computers on the LAN no matter what IP address they might have. In this case, the Wireless Router will check any packets initiated from the LAN computers, so the system performance will be degraded to some extent. Therefore, you’d better change the default value.

9.1.3.2 Access Rule Settings - URL Filtering



Name* Rule-1

Enable ☑

Select the check box to make the access rule take effect.

Source IP Range* 192.168.1.80 To * 192.168.1.100

A group of LAN PCs to which the rule applies.

Priority* 10

The smaller the number, the higher the priority.

Action Deny

Filtering Type URL Filtering

Filtering Content* http://www.bbc.com

Schedule

Days ☑ Everyday

□ Mon □ Tue □ Wed □ Thu □ Fri □ Sat □ Sun

Time ● 24 Hours

○ From 00 : 00 To 00 : 00

Figure 9- 5 Access Rule Settings - URL Filtering

The parameters **Name**, **Source IP Range**, **Priority** and **Action**, and **Schedule** related parameters are the same as those of the **IP Filtering** access rule, please refer to **Section 9.1.3.1 Access Rule Settings - IP Filtering** for detailed information.

- **Filtering Type:** It specifies the filtering type of the access rule. The options are **IP Filtering**, **URL Filtering**, and **Keyword Filtering**. Here please select **URL Filtering**.

- **Filtering Content:** It specifies the URL keyword that you want to filter. The access rule is used to filter any web pages whose URL contains the specified keyword.

  You can enter part of a URL to match all URLs that contain that string, or you can enter the full URL to match only the specified URL. Here we give two examples.

  Example 1: If you enter **yahoo**, it will match any URL that contains yahoo, such as http://www.yahoo.com, http://news.yahoo.com/, http://cn.yahoo.com/, and so on.

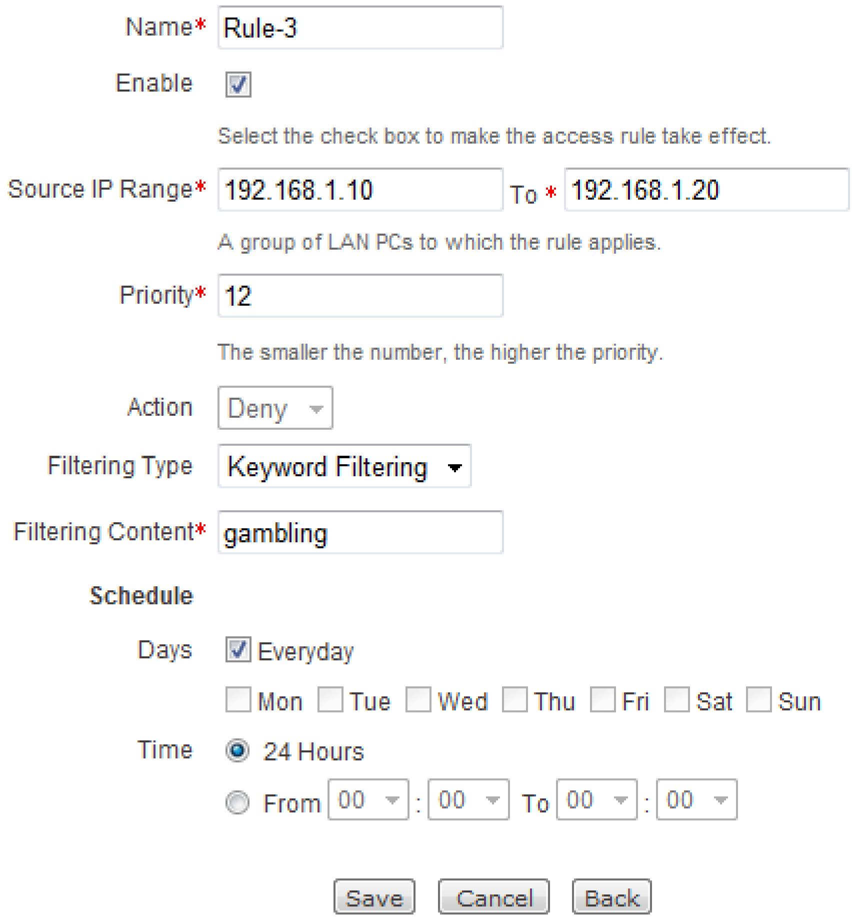
  Example 2: If you enter **news.yahoo.com**, it will match http://news.yahoo.com/ and all URLs that start with news.yahoo.com, such as http://news.yahoo.com/education/. However, it won't match http://www.yahoo.com and http://cn.yahoo.com/.

- **Save:** Click to save your changes.
- **Cancel:** Click to revert to the last saved settings.
- **Back:** Click to go back to the **Access Rule List**.

Note

1. The URL keyword that you enter in the **Filtering Content** text box is case insensitive, and it needn't include http://.
2. The URL filtering rules cannot be used to control users' access to other services through a web browser. For example, to control users' access to ftp://ftp.utt.com.cn, you need to configure an IP filtering rule to allow or deny ftp service.

9.1.3.3 Access Rule Settings - Keyword Filtering



Name* Rule-3

Enable ☑

Select the check box to make the access rule take effect.

Source IP Range* 192.168.1.10 To * 192.168.1.20

A group of LAN PCs to which the rule applies.

Priority* 12

The smaller the number, the higher the priority.

Action Deny

Filtering Type Keyword Filtering

Filtering Content* gambling

Schedule

Days ☑ Everyday

□ Mon □ Tue □ Wed □ Thu □ Fri □ Sat □ Sun

Time ● 24 Hours

○ From 00 : 00 To 00 : 00

Figure 9- 6 Access Rule Settings - Keyword Filtering

The parameters **Name**, **Source IP Range**, **Priority** and **Action**, and **Schedule** related parameters are the same as those of the **IP Filtering** access rule, please refer to **Section**

9.1.3.1 Access Rule Settings - IP Filtering for detailed information.

- **Filtering Type:** It specifies the filtering type of the access rule. The options are **IP Filtering**, **URL Filtering**, and **Keyword Filtering**. Here please select **Keyword Filtering**.

- **Filtering Content:** It specifies the keyword that you want to block. The access rule is used to block users from submitting any information that contains the specified keyword to any web page. The Wireless Router supports both Chinese and English keyword filtering. A keyword must be a single word without white space.

- **Save:** Click to save your changes.

- **Cancel:** Click to revert to the last saved settings.

- **Back:** Click to go back to the **Access Rule List**.

✓ **Note**

1. The keyword filtering rules only support the **Deny** action.
2. The English keyword is case sensitive.

9.1.4 Configuration Examples for Access Rule

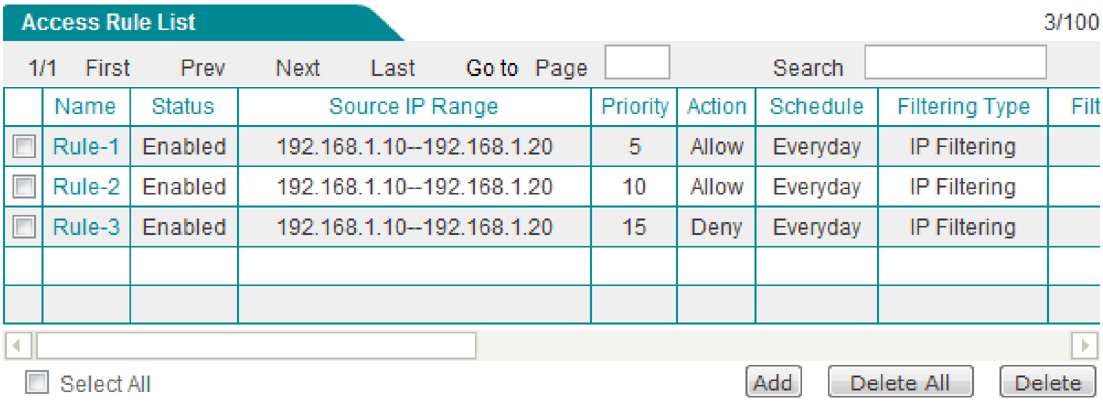
9.1.4.1 Example 1 - Only Allow a Group of Users to Access Certain Services

In this example, we want to allow a group of users (IP address range: 192.168.1.10-192.168.1.20) to access web service, and block them from accessing any other services.

We need to create three access rules to meet the requirements:

- Access rule 1: It allows those users to access DNS service. And it is used to ensure that the domain names can be resolved successfully, thus the users can access web service properly.
- Access rule 2: It allows those users to access Web service.
- Access rule 3: It blocks those users from accessing any Internet services.

Therein, both rule 1 and rule 2 must have a higher priority than rule 3. Otherwise, rule 3 will be matched first. This will make those users unable to access web service.



Access Rule List 3/100

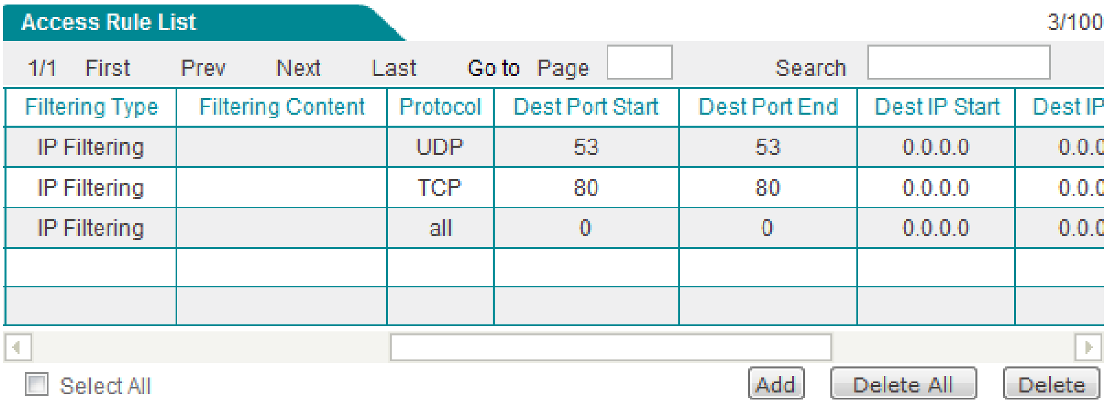
1/1 First Prev Next Last Go to Page □ Search □

	Name	Status	Source IP Range	Priority	Action	Schedule	Filtering Type	Filt
□	Rule-1	Enabled	192.168.1.10--192.168.1.20	5	Allow	Everyday	IP Filtering	
□	Rule-2	Enabled	192.168.1.10--192.168.1.20	10	Allow	Everyday	IP Filtering	
□	Rule-3	Enabled	192.168.1.10--192.168.1.20	15	Deny	Everyday	IP Filtering	

□ Select All

Add Delete All Delete

Figure 9- 7 Access Rule List - Example 1



Access Rule List 3/100

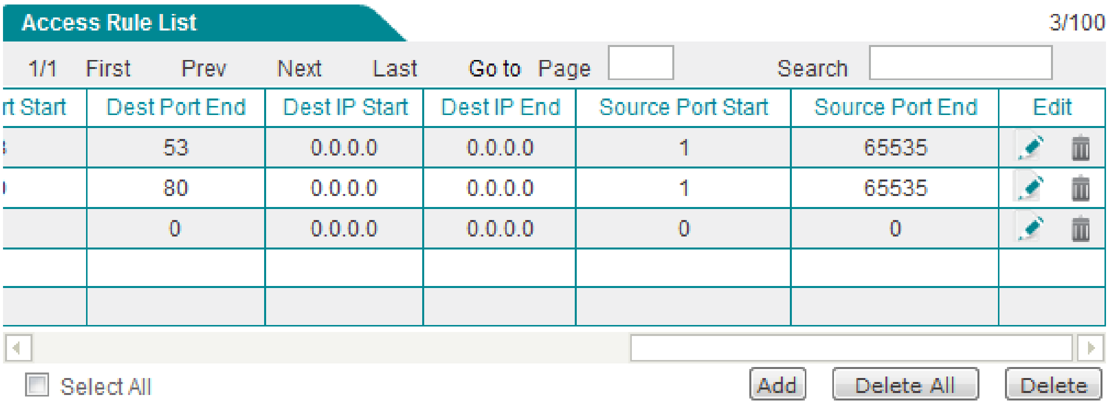
1/1 First Prev Next Last Go to Page □ Search □

Filtering Type	Filtering Content	Protocol	Dest Port Start	Dest Port End	Dest IP Start	Dest IP
IP Filtering		UDP	53	53	0.0.0.0	0.0.0
IP Filtering		TCP	80	80	0.0.0.0	0.0.0
IP Filtering		all	0	0	0.0.0.0	0.0.0

□ Select All

Add Delete All Delete

Figure 9- 8 Access Rule List - Example 1 (Continue)



Access Rule List 3/100

1/1 First Prev Next Last Go to Page □ Search □

rt Start	Dest Port End	Dest IP Start	Dest IP End	Source Port Start	Source Port End	Edit
	53	0.0.0.0	0.0.0.0	1	65535	✎ 🗑
	80	0.0.0.0	0.0.0.0	1	65535	✎ 🗑
	0	0.0.0.0	0.0.0.0	0	0	✎ 🗑

□ Select All

Add Delete All Delete

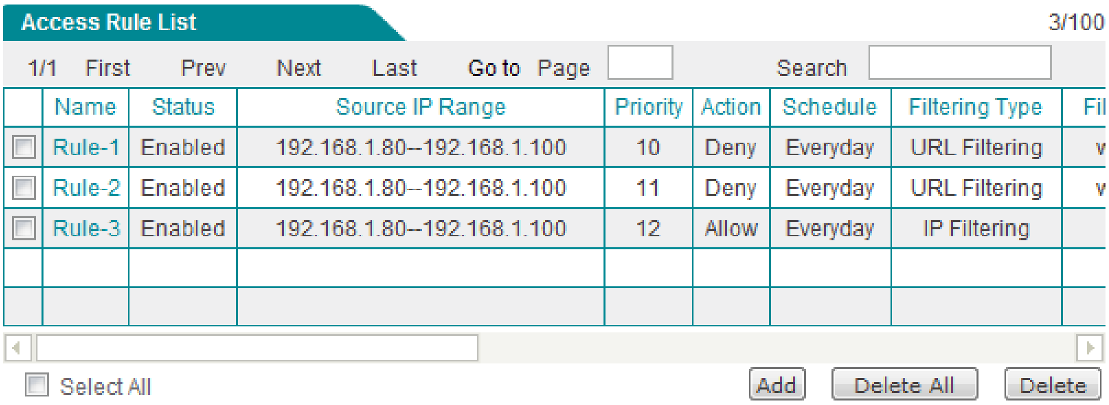
Figure 9- 9 Access Rule List - Example 1 (Continue)

9.1.4.2 Example 2 - Only Block a Group of Users from Accessing Certain Services

In this example, we want to block a group of users (IP address range: 192.168.1.80 -192.168.1.100) from accessing www.bbc.com and www.cnn.com, and allow them to access any other services. We need to create three access rules to meet the requirements:

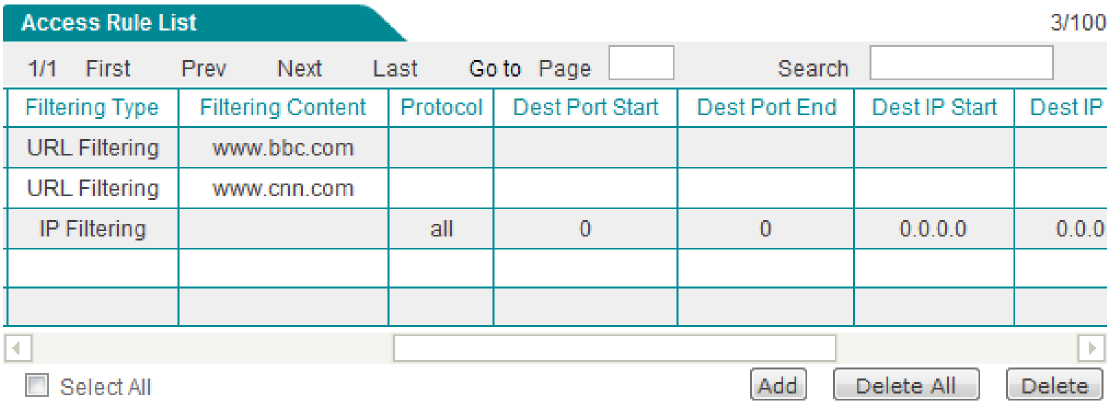
- Access rule 1: It blocks those users from accessing www.bbc.com.
- Access rule 2: It blocks those users from accessing www.cnn.com.
- Access rule 3: It allows those users to access all Internet services.

Therein, both rule 1 and rule 2 must have a higher priority than rule 3. Otherwise, rule 3 will be matched first. This will make those users unable to access www.bbc.com and www.cnn.com.



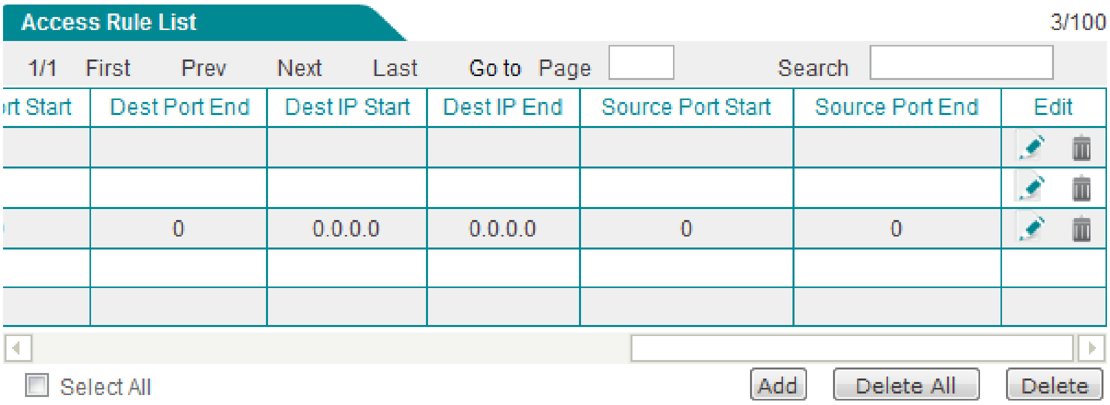
	Name	Status	Source IP Range	Priority	Action	Schedule	Filtering Type	Fil
□	Rule-1	Enabled	192.168.1.80--192.168.1.100	10	Deny	Everyday	URL Filtering	v
□	Rule-2	Enabled	192.168.1.80--192.168.1.100	11	Deny	Everyday	URL Filtering	v
□	Rule-3	Enabled	192.168.1.80--192.168.1.100	12	Allow	Everyday	IP Filtering	

Figure 9-10 Access Rule List - Example 2



Filtering Type	Filtering Content	Protocol	Dest Port Start	Dest Port End	Dest IP Start	Dest IP
URL Filtering	www.bbc.com					
URL Filtering	www.cnn.com					
IP Filtering		all	0	0	0.0.0.0	0.0.0

Figure 9-11 Access Rule List - Example 2 (Continue)



rt Start	Dest Port End	Dest IP Start	Dest IP End	Source Port Start	Source Port End	Edit
						✎ 🗑
						✎ 🗑
	0	0.0.0.0	0.0.0.0	0	0	✎ 🗑

Figure 9- 12 Access Rule List - Example 2 (Continue)

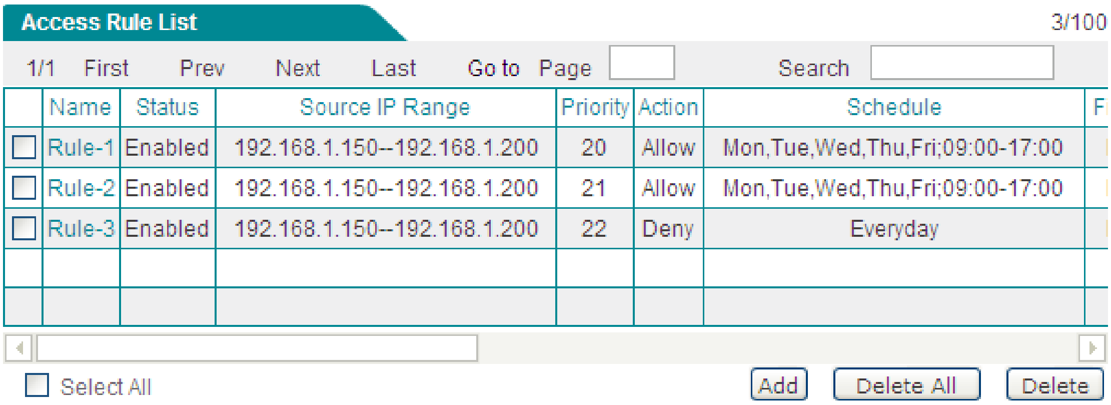
9.1.4.3 Example 3 - Control Internet Behaviors of a Group of Users based on Schedule

In this example, we want to only allow a group of users (IP address range: 192.168.1.150 -192.168.1.200) to access web service during business hours (Monday to Friday, 9:00 to 17:00), and block them from accessing any Internet services during rest periods.

We need to create three access rules to meet the requirements:

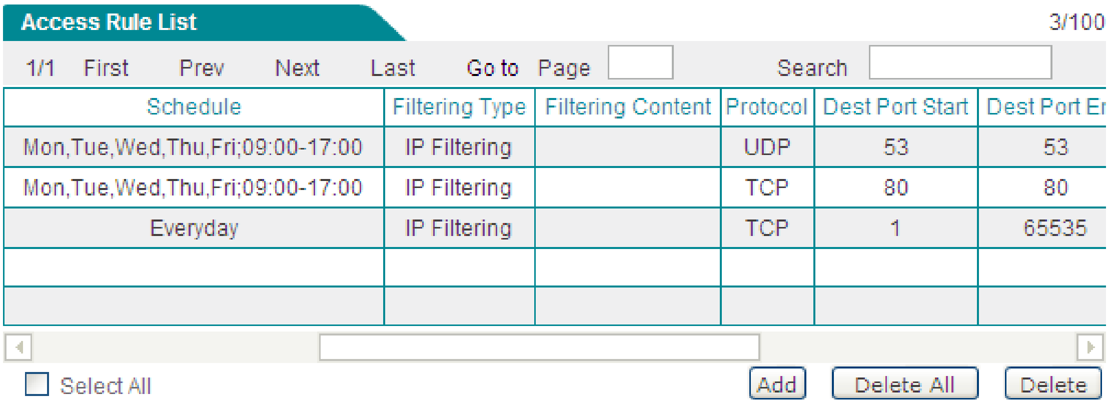
- Access rule 1: It allows those users to access DNS service during business hours. And it is used to ensure that the domain names can be resolved successfully, thus the users can access web service properly.
- Access rule 2: It allows those users to access web service during business hours.
- Access rule 3: It blocks those users from accessing any Internet services.

Therein, both rule 1 and rule 2 must have a higher priority than rule 3. Otherwise, rule 3 will be matched first. This will make those users unable to access web service during business hours.



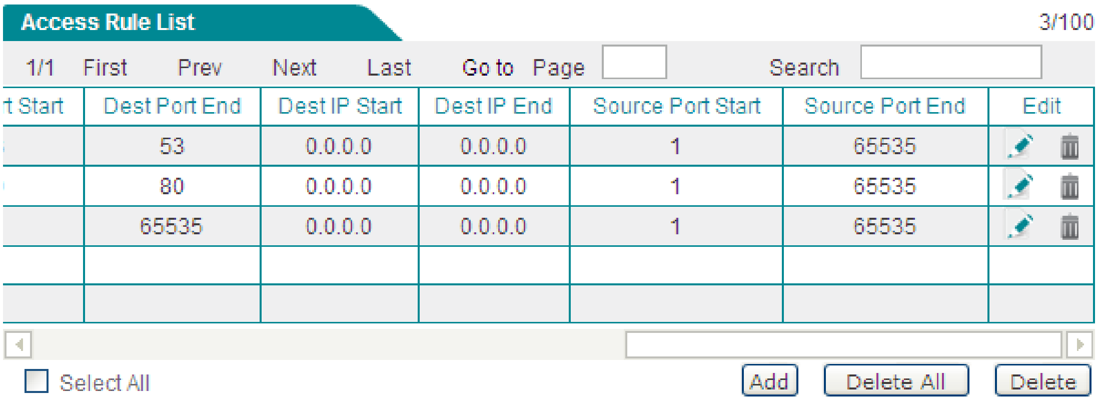
	Name	Status	Source IP Range	Priority	Action	Schedule	F
□	Rule-1	Enabled	192.168.1.150--192.168.1.200	20	Allow	Mon,Tue,Wed,Thu,Fri;09:00-17:00	
□	Rule-2	Enabled	192.168.1.150--192.168.1.200	21	Allow	Mon,Tue,Wed,Thu,Fri;09:00-17:00	
□	Rule-3	Enabled	192.168.1.150--192.168.1.200	22	Deny	Everyday	

Figure 9- 13 Access Rule List - Example 3



Schedule	Filtering Type	Filtering Content	Protocol	Dest Port Start	Dest Port Er
Mon,Tue,Wed,Thu,Fri;09:00-17:00	IP Filtering		UDP	53	53
Mon,Tue,Wed,Thu,Fri;09:00-17:00	IP Filtering		TCP	80	80
Everyday	IP Filtering		TCP	1	65535

Figure 9- 14 Access Rule List - Example 3 (Continue)



Access Rule List 3/100

1/1 First Prev Next Last Go to Page Search

t Start	Dest Port End	Dest IP Start	Dest IP End	Source Port Start	Source Port End	Edit
	53	0.0.0.0	0.0.0.0	1	65535	
	80	0.0.0.0	0.0.0.0	1	65535	
	65535	0.0.0.0	0.0.0.0	1	65535	

Figure 9- 15 Access Rule List - Example 3 (Continue)

9.1.4.4 Example 4 - Control Internet Behaviors of a Single User

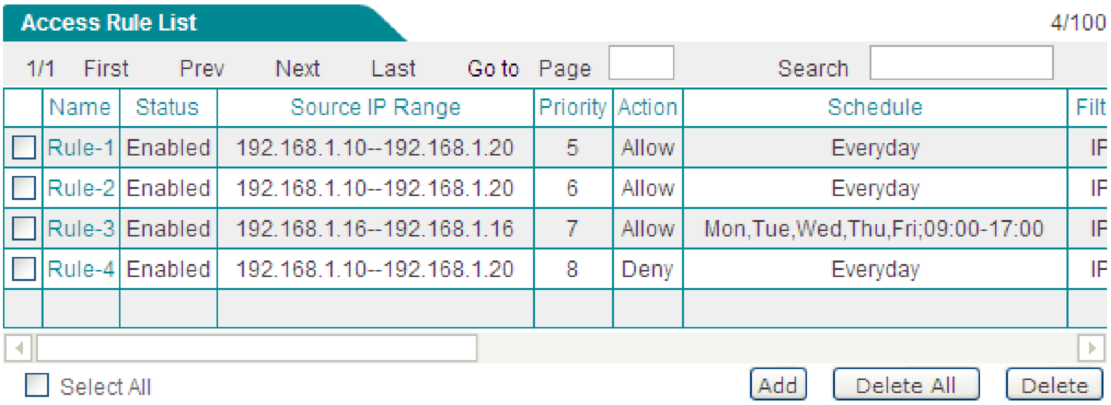
You can assign a range of contiguous IP addresses to the users that have the same Internet access privileges, and then create access rules for the user group. However, if one or several users in the group have special or new Internet needs, you need to individually create access rules for a single user.

In this example, we want to allow a group of users (IP address range: 192.168.1.10-192.168.1.120) to access web service, and block them from accessing all other services. The exception is that the user with IP address 192.168.1.16 is allowed to access all Internet services during business hours (Monday to Friday, 9:00 to 17:00).

We need to create four access rules to meet the requirements:

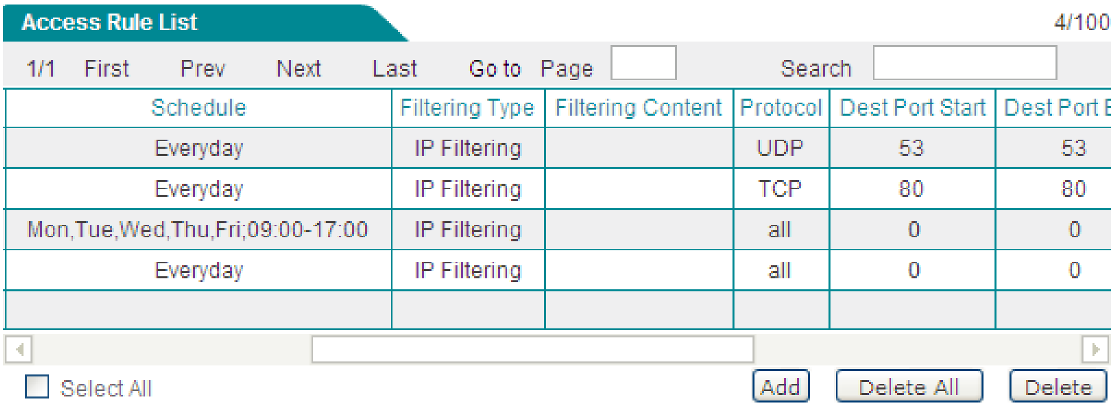
- Access rule 1: It allows the user group to access DNS service.
- Access rule 2: It allows the user group to access web service.
- Access rule 3: It allows the user with IP address 192.168.1.16 to access all Internet services during business hours.
- Access rule 4: It blocks the user group from accessing any Internet services.

Therein, rule 4 must have a lower priority than the other three rules.



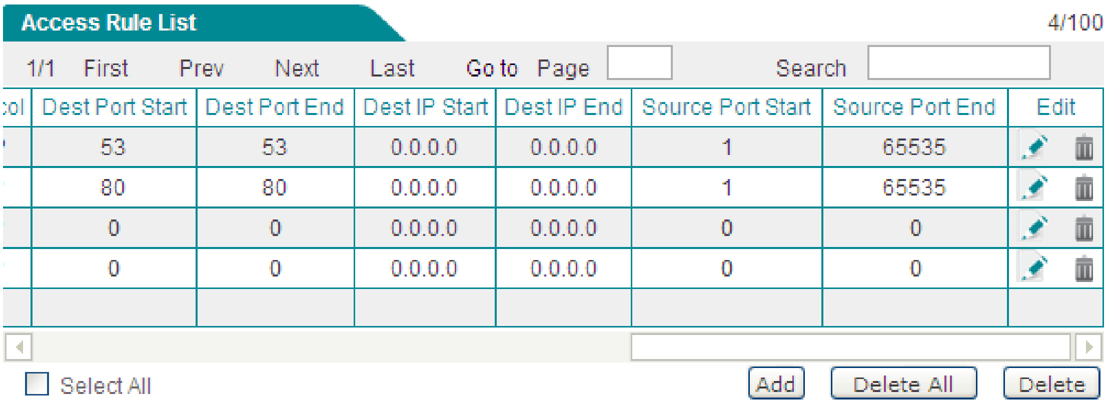
	Name	Status	Source IP Range	Priority	Action	Schedule	Filt
□	Rule-1	Enabled	192.168.1.10--192.168.1.20	5	Allow	Everyday	IF
□	Rule-2	Enabled	192.168.1.10--192.168.1.20	6	Allow	Everyday	IF
□	Rule-3	Enabled	192.168.1.16--192.168.1.16	7	Allow	Mon,Tue,Wed,Thu,Fri;09:00-17:00	IF
□	Rule-4	Enabled	192.168.1.10--192.168.1.20	8	Deny	Everyday	IF

Figure 9-16 Access Rule List - Example 4



Schedule	Filtering Type	Filtering Content	Protocol	Dest Port Start	Dest Port E
Everyday	IP Filtering		UDP	53	53
Everyday	IP Filtering		TCP	80	80
Mon,Tue,Wed,Thu,Fri;09:00-17:00	IP Filtering		all	0	0
Everyday	IP Filtering		all	0	0

Figure 9-17 Access Rule List - Example 4 (Continue)



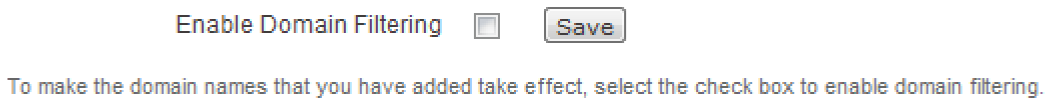
:ol	Dest Port Start	Dest Port End	Dest IP Start	Dest IP End	Source Port Start	Source Port End	Edit
	53	53	0.0.0.0	0.0.0.0	1	65535	✎ 🗑
	80	80	0.0.0.0	0.0.0.0	1	65535	✎ 🗑
	0	0	0.0.0.0	0.0.0.0	0	0	✎ 🗑
	0	0	0.0.0.0	0.0.0.0	0	0	✎ 🗑

Figure 9-18 Access Rule List - Example 4 (Continue)

9.2 Domain Filtering

This section describes the **Firewall > Domain Filtering** page. The domain filtering feature allows you to block access to unwanted websites in your organization.

9.2.1 Domain Filtering Global Settings



Enable Domain Filtering □ Save

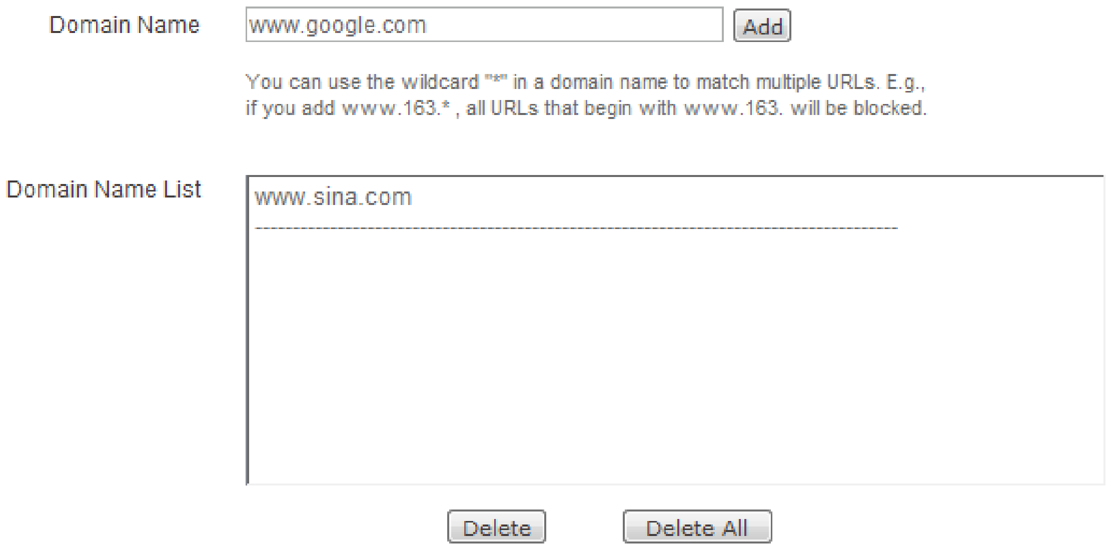
To make the domain names that you have added take effect, select the check box to enable domain filtering.

Figure 9- 19 Domain Filtering Global Settings

- **Enable Domain Filtering:** It allows you to enable or disable domain filtering. If you select the check box to enable domain filtering, the domain names in the **Domain Name List** will take effect. Else, they will be of no effect.

- **Save:** Click to save your changes.

9.2.2 Domain Filtering Settings



Domain Name: www.google.com Add

You can use the wildcard "*" in a domain name to match multiple URLs. E.g., if you add www.163.* , all URLs that begin with www.163. will be blocked.

Domain Name List: www.sina.com

Delete Delete All

Figure 9- 20 Domain Filtering Settings

- **Domain Name:** It specifies the domain name of the website that you want to block.

- **Domain Name List:** It displays the domain names that you have added. The

Wireless Router will block the LAN users from accessing these domain names.

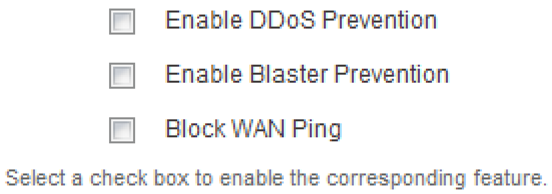
- **Add a Domain Name:** To add a domain name to the **Domain Name List**, enter the domain name of the website that you want to block in the **Domain Name** text box, and then click the **Add** button. You can add up to 100 domain names in the list.
- **Delete:** To delete one or more domain names, select them in the **Domain Name List**, and then click the **Delete** button.
- **Delete All:** To delete all the domain names in the **Domain Name List** at a time, directly click the **Delete All** button.

✓ **Note**

1. The Wireless Router supports up to 100 domain names.
2. The matching rule of domain filtering is whole words matching, that is, only a domain name matches the whole words of the domain name in the **Domain Name List**, the Wireless Router will block access to it.
3. You can use the wildcard "*" in a domain name to filter multiple URLs. For example, if you add www.163.* into the **Domain Name List**, then all the URLs that begin withwww.163. will be blocked.

9.3 Attack Prevention

This section describes the **Firewall > Attack Prevention** page.



□ Enable DDoS Prevention

□ Enable Blaster Prevention

□ Block WAN Ping

Select a check box to enable the corresponding feature.

Figure 9- 21 Attack Prevention Settings

- **Enable DDoS Prevention:** It is used to enable or disable DDoS prevention. If you select the check box to enable this feature, it will effectively protect the Wireless Router against popular DoS/DDoS attacks.
- **Enable Blaster Prevention** It is used to enable or disable blaster virus prevention. If you select the check box to enable this feature, it will effectively protect the Wireless Router against popular virus attacks such as Blaster and Sasser.
- **Block WAN Ping:** It is used to block or allow WAN ping. If you select the check box to block WAN ping, all the WAN interfaces of the Wireless Router will not respond to ping requests from the Internet.
- **Save:** Click to save your changes.

Chapter 10 VPN

The Wireless Router supports PPTP client feature. PPTP is a VPN tunneling protocol which encapsulates PPP frames in IP packets for transmission over a public IP network such as the Internet. PPTP is based on client/server model. The PPTP client initiates a PPTP connection to the server, while the PPTP server accepts the incoming PPTP connection from the client. PPTP is often used to implement remote access VPNs over an IP network (such as a broadband network), to extend the reach of your Intranet.

10.1 Introduction to PPTP Implementation

PPTP is used to encapsulate PPP frames in IP packets for transmission over a public IP network such as the Internet. The PPTP client or server encapsulates the original user packets inside PPP frames before sending them through a PPTP tunnel over the Internet; while the peer performs decapsulation firstly, and then forward the original packets to their intended destinations.

As shown in Figure 10-1, the typical application of PPTP is that some laptop or desktop computers act as the PPTP client devices, that is, some employees in the remote branch offices or mobile users (traveling employees, telecommuters, etc.) use the Windows built-in PPTP client software to initiate PPTP connections; the PPTP server deployed at the head office accepts the PPTP incoming connections from the clients. After a PPTP tunnel has been established between the PPTP client and server, the PPTP server will receive the PPTP packets from the client firstly, and then perform decapsulation, lastly forward the original packets to their intended destinations.

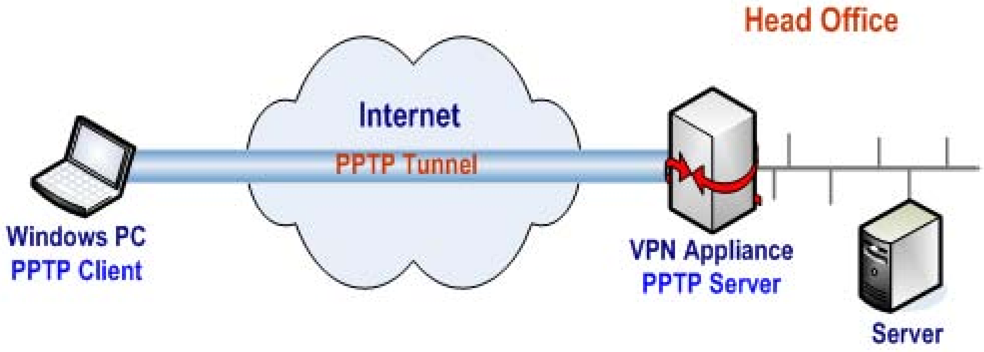


Figure 10-1 Typical Application of PPTP

10.1.1 Protocol Overview

There are two parallel components of PPTP:

1. A PPTP Control Connection

It is a logical connection representing the PPTP tunnel that must be created, maintained, and terminated through a series of PPTP messages. The PPTP control connection traffic uses a dynamically allocated TCP port on the PPTP client and the registered TCP port 1723 on the PPTP server.

2. GRE encapsulation for data

When data is sent through the PPTP tunnel, PPP frames are encapsulated with a Generic Routing Encapsulation (GRE) header, which includes information that identifies the specific PPTP tunnel for the data packet. GRE is described in RFC 1701.

The use of a separate GRE mechanism for PPTP data encapsulation has an interesting side effect for NAT devices. Most NAT devices can translate TCP-based packets for PPTP tunnel maintenance. However, many NAT devices or firewalls cannot handle GRE packets, thus the PPTP data packets with the GRE header cannot pass them. The UTT products support NAT traversal for PPTP tunnels.

In order for the PPTP tunnel to be established and function properly, the following basic conditions are necessary:

1) The PPTP client and server should have IP-route reachability between them.
2) The firewalls between the two endpoints of the tunnel should be configured to open TCP port 1723 and IP protocol 47 (GRE) to allow PPTP traffic.

10.1.2 Packet Flow - PPTP Client

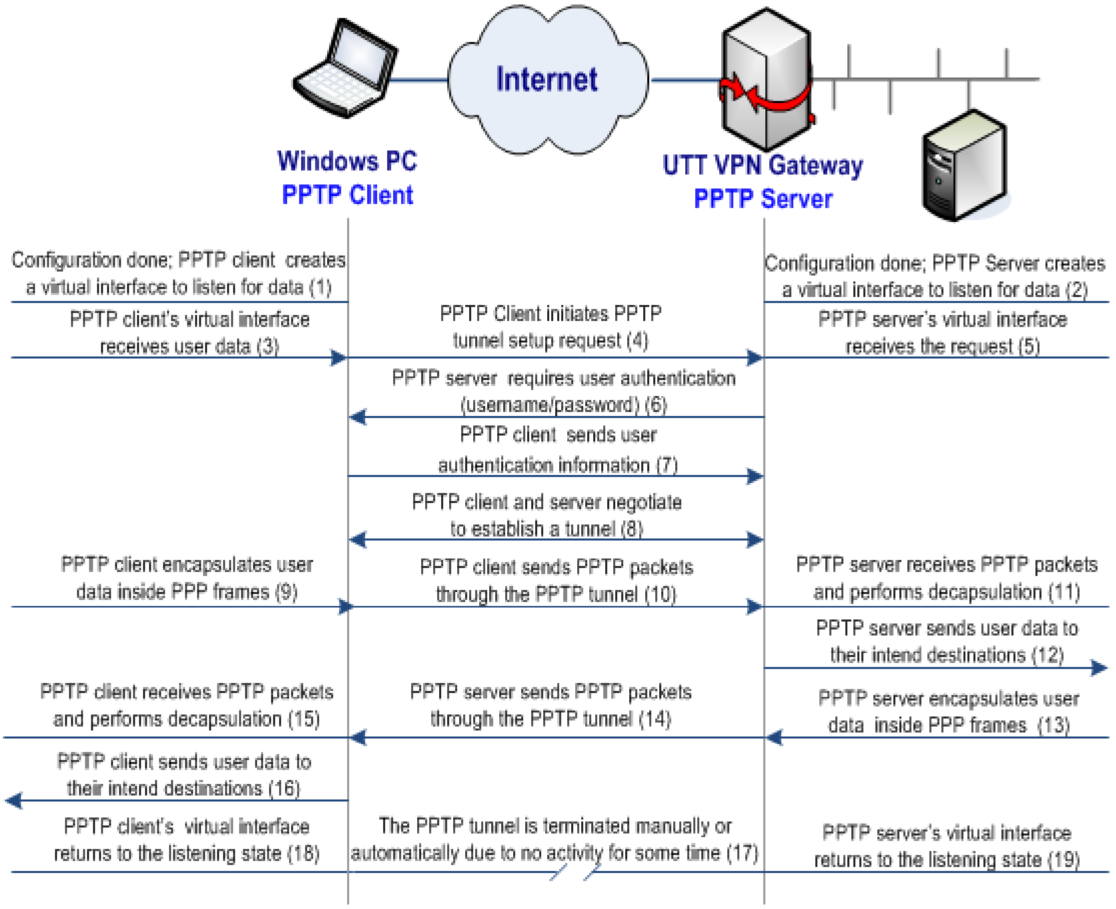

Internet
Windows PC
PPTP Client
UTT VPN Gateway
PPTP Server
Configuration done; PPTP client creates a virtual interface to listen for data (1)
Configuration done; PPTP Server creates a virtual interface to listen for data (2)
PPTP client's virtual interface receives user data (3)
PPTP Client initiates PPTP tunnel setup request (4)
PPTP server's virtual interface receives the request (5)
PPTP server requires user authentication (username/password) (6)
PPTP client sends user authentication information (7)
PPTP client and server negotiate to establish a tunnel (8)
PPTP client encapsulates user data inside PPP frames (9)
PPTP client sends PPTP packets through the PPTP tunnel (10)
PPTP server receives PPTP packets and performs decapsulation (11)
PPTP server sends user data to their intend destinations (12)
PPTP client receives PPTP packets and performs decapsulation (15)
PPTP server sends PPTP packets through the PPTP tunnel (14)
PPTP server encapsulates user data inside PPP frames (13)
PPTP client sends user data to their intend destinations (16)
PPTP client's virtual interface returns to the listening state (18)
The PPTP tunnel is terminated manually or automatically due to no activity for some time (17)
PPTP server's virtual interface returns to the listening state (19)

Figure 10- 2 PPTP Packet Flow

As shown in Figure 10- 2, during the PPTP tunnel establishment and data transmission processes, the packet flow through the PPTP client can be summarized as follows:

- After the PPTP tunnel parameters are configured properly, the PPTP client automatically creates a virtual interface for the new tunnel to listen for user data ((1) in Figure 10- 2).
- The PPTP client's virtual interface listens for the user packets destined for the remote LAN ((3) in Figure 10- 2).
- The PPTP client initiates the PPTP tunnel setup request ((4) in Figure 10- 2).
- The PPTP client receives the user authentication request from the PPTP server, and then responds to the request ((7) in Figure 10- 2).
- The PPTP client negotiates with the PPTP server to establish a PPTP tunnel ((8) in Figure 10- 2).
- The PPTP client receives the user data (i.e., original packets) and encapsulates them in the PPP frames ((9) in Figure 10- 2).

- The PPTP client sends the PPTP packets to the PPTP server through the PPTP tunnel ((10) in Figure 10- 2).
- The PPTP client receives the PPTP packets from the PPTP server, and performs decapsulation ((15) in Figure 10- 2).
- The PPTP client forwards the user data (i.e., original packets) to their intend destinations ((16) in Figure 10- 2).
- The PPTP tunnel is terminated manually by the user or automatically due to no activity for some time ((17) in Figure 10- 2).
- After the PPTP tunnel is terminated, the PPTP client's virtual interface returns to the listening state ((18) in Figure 10- 2).

10.1.3 User Authentication

PPTP provides user authentication to authenticate the user attempting the PPTP connection by PPP-based user authentication modes such as PAP, CHAP, etc. Note that the two endpoints of a PPTP tunnel should use the same authentication mode.

On the Wireless Router, it allows you to choose PAP, CHAP or Either as the user authentication mode for a PPTP client. It also allows you to choose None, which means that no authentication is performed. By default, the authentication mode is Either, which means that the PPTP client will automatically negotiate it with peer.

10.1.4 Data Confidentiality

PPTP doesn't provide any data encryption service by itself; it uses PPP compression and encryption mechanisms (such as CCP, PPE, etc.) to provide data confidentiality.

10.1.5 MTU and Fragmentation

The Wireless Router will fragment an IP packet if it exceeds the MTU of the outbound physical interface. For example, a standard Ethernet-type interface has a MTU of 1500 bytes, thus the Wireless Router will fragment a packet exceeding 1500 bytes in order to transmit it over the Ethernet interface.

With PPTP, the addition of PPTP headers may cause IP fragmentation. When an IP packet is nearly the size of MTU of the outbound physical interface (for example, ERP or FTP packets are often relatively large), and it is further encapsulated with PPTP headers, the encapsulated packet is likely to exceed the MTU of the outbound physical interface. This causes the encapsulated packet to be fragmented before transmission, and the PPTP receiver is responsible for reassembling the fragments back into the original encapsulated packet before decapsulation. More specifically, the receiver cannot perform reassembly until the last fragment is received; and if one fragment is lost, the entire original encapsulated packet must be resent, and it will also be fragmented.

Data fragmentation and reassembly can seriously degrade the system performance, so it is highly necessary to avoid fragmentation and reassembly in the PPTP switching path. To solve this problem, PPTP allows the client and server to negotiate PPP MRU/MTU during PPTP tunnel establishment.

In addition, on the Wireless Router, you can adjust the global PPTP tunnel MTU (i.e., tunnelmtu) to minimize the fragmentation: if an IP packet exceeds the specified MTU, it will be fragmented by the original computer before transmission. The following two examples describe how to calculate PPTP tunnel MTU. Figure 10-3 illustrates the format of the PPTP packet to be sent over a static IP or DHCP Internet connection; and Figure 10-4 illustrates the format of the PPTP packet to be sent over a PPPoE Internet connection. Therein, the sizes of standard Ethernet MTU and each encapsulation header are as follows:

Ethernet MTU	1500 Bytes
IP Header	20 Bytes
GRE Header	8 Bytes
PPTP Header	30 Bytes (at most)
PPPoE Header	8 Bytes

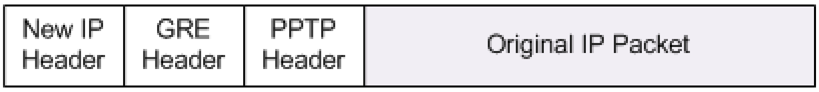


Figure 10-3 PPTP Packet Format - Static IP/DHCP Internet Connection

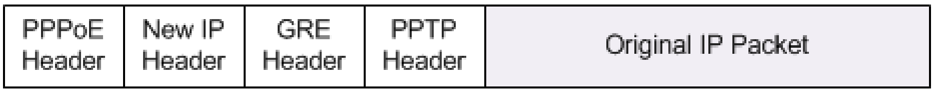


Figure 10-4 PPTP Packet Format - PPPoE Internet Connection

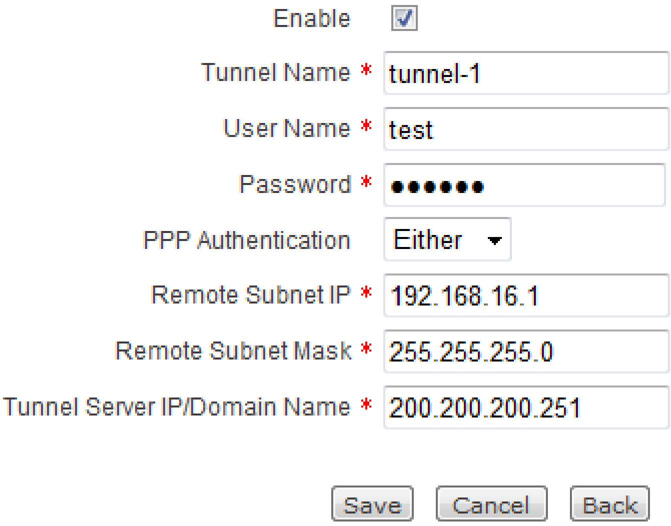
Therefore, to avoid fragmentation and reassembly in the PPTP switching path, the PPTP tunnel MTU should be smaller or equal to 1442 bytes (1500-20-8-30=1442) when the PPTP packets are sent over a static IP or DHCP Internet connection (see Figure 10-3); and it must be smaller or equal to 1434 bytes (1442-8=1434) when the PPTP packets are sent over a PPPoE Internet connection (see Figure 10-4).

On the Wireless Router, the PPTP tunnel MTU is 1400 bytes by default. In most cases, please leave the default value because it can meet most application needs.

10.1.6 PPTP Sessions Limit

The Wireless Router supports two concurrent PPTP sessions (i.e., tunnels) at most. If there are already two active PPTP sessions on the Wireless Router, the system will reject any request for creating a new PPTP session and prompt you.

10.2 PPTP Client Settings



Enable ☑

Tunnel Name * tunnel-1

User Name * test

Password * ●●●●●●

PPP Authentication Either

Remote Subnet IP * 192.168.16.1

Remote Subnet Mask * 255.255.255.0

Tunnel Server IP/Domain Name * 200.200.200.251

Figure 10- 5 PPTP Client Settings

- **Enable:** It allows you to enable or disable the PPTP client entry. The default value is checked, which means the PPTP client entry is in effect. If you want to disable the entry temporarily instead of deleting it, please clear the check box.

- **Tunnel Name:** It specifies a unique name of the PPTP tunnel. It is used to identify multiple tunnels.

- **User Name:** It specifies a unique user name of the PPTP/L2TP client. It must be between 1 and 31 characters long. The remote PPTP/L2TP server will use the **User Name** and **Password** to identify the client.

- **Password:** It specifies a password of the PPTP/L2TP client.

- **PPP Authentication:** It specifies the PPP authentication mode by which the remote PPTP server authenticates the PPTP client. The available options are **None**, **PAP**, **CHAP** and **Either**.

    - **PAP:** Password Authentication Protocol.

    - **CHAP:** Challenge Handshake Authentication Protocol.

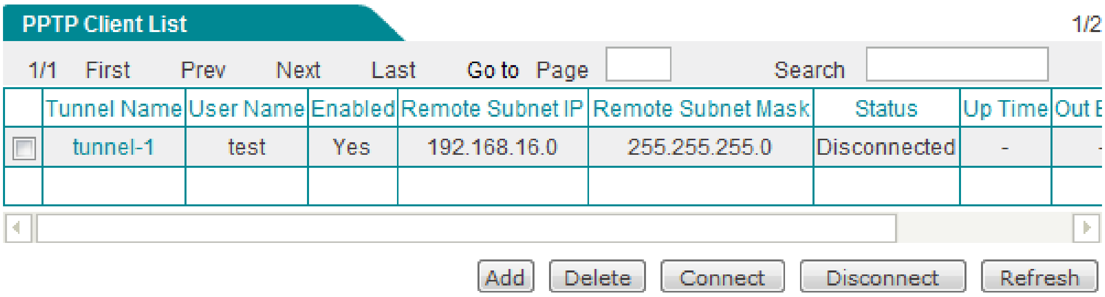
- **None:** It means that no authentication is performed.
- **Either:** It means that the Wireless Router will automatically negotiate it with the remote VPN appliance.

- **Remote Subnet IP:** It specifies the subnet IP address of the remote network. In most cases, you may enter the IP address of the remote VPN appliance's LAN interface.
- **Remote Subnet Mask:** It specifies the subnet mask of the remote network.
- **Tunnel Server IP/Domain Name:** It specifies the IP address or domain name of the remote PPTP/L2TP server. In most cases, you may enter the WAN IP address or domain name of the remote VPN appliance.

- **Save:** Click to save your changes.
- **Cancel:** Click to revert to the last saved settings.
- **Back:** Click to go back to the **PPTP Client List**.

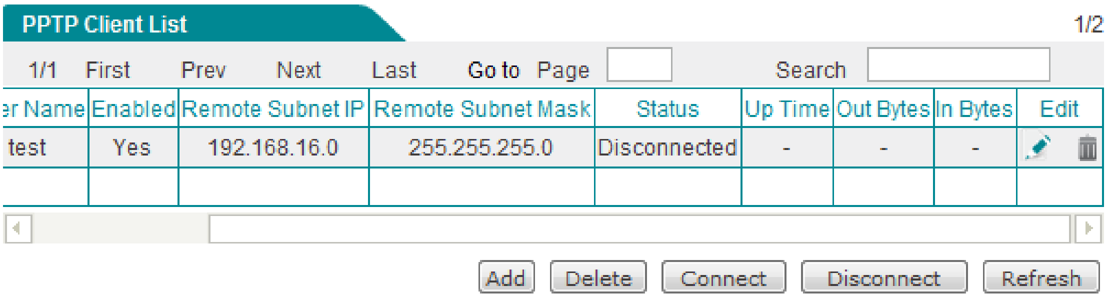
10.3 PPTP Client List

After you have configured a PPTP/L2TP client entry, you can view its configuration and status in the **PPTP Client List**, see Figure 10- 6.



	Tunnel Name	User Name	Enabled	Remote Subnet IP	Remote Subnet Mask	Status	Up Time	Out E
☐	tunnel-1	test	Yes	192.168.16.0	255.255.255.0	Disconnected	-	-

Figure 10- 6 PPTP Client List



er Name	Enabled	Remote Subnet IP	Remote Subnet Mask	Status	Up Time	Out Bytes	In Bytes	Edit
test	Yes	192.168.16.0	255.255.255.0	Disconnected	-	-	-	✎ 🗑

Figure 10- 7 PPTP Client List (Continue)

After the Wireless Router has successfully established a PPTP tunnel with the remote

PPTP server, you will see that the tunnel's **Status** changes from **Disconnected** to **Connected**, the **Up Time** timer starts, and the **Out Bytes** and **In Bytes** will go on increasing as long as there is some network traffic being passed through the PPTP tunnel.

10.4 Configuration Example for PPTP Client

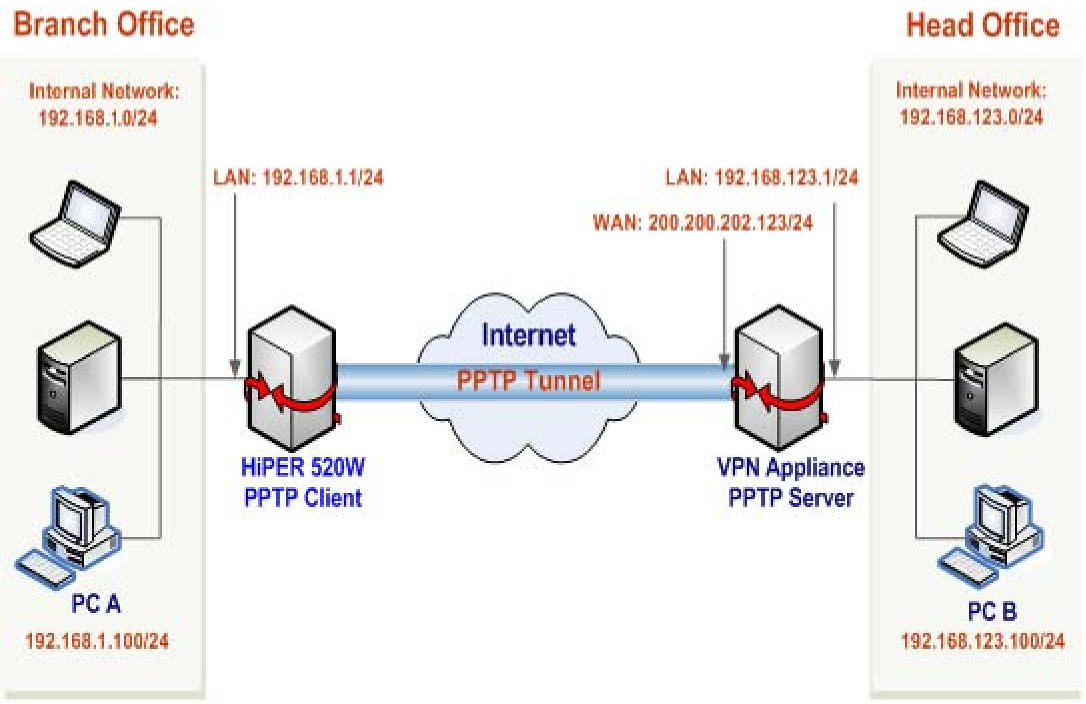


Figure 10- 8 Network Topology - The Wireless Router Acts as a PPTP client

In this example, a company's head office is located in Washington, and its branch office is located in New York. Now the company wants the head office and branch office to securely communicate with each other over the Internet.

As shown in Figure 10- 8, we will use PPTP to establish a VPN tunnel, deploy a AC750W Wireless Router acting as a PPTP client at the branch office, and another VPN appliance (a UTT VPN gateway is recommended) acting as a PPTP server at the head office. The IP addresses are as follows:

The AC750W (PPTP Client) at the branch office:

- LAN Subnet: 192.168.1.0/255.255.255.0
- LAN Interface IP Address: 192.168.1.1/255.255.255.0

The VPN appliance (PPTP Server) at the head office:

- LAN Subnet: 192.168.123.0/255.255.255.0
- LAN Interface IP Address: 192.168.123.1/255.255.255.0

- WAN Interface IP Address: 200.200.202.123/255.255.255.0

To configure the AC750W as a PPTP client, follow these steps:

Step 1 Go to the **VPN > PPTP Client** page, and click the **Add** button to go to the **PPTP Client Settings** page.

Step 2 Make the following settings.

Enable	Select
Tunnel Name	To_HQ
User Name	VPN_test
Password	vpntest
PPP Authentication	Either
Remote Subnet IP	192.168.123.1
Remote Subnet Mask	255.255.255.0
Tunnel Server IP/Domain Name	200.200.202.123

Step 3 Click the **Save** button.

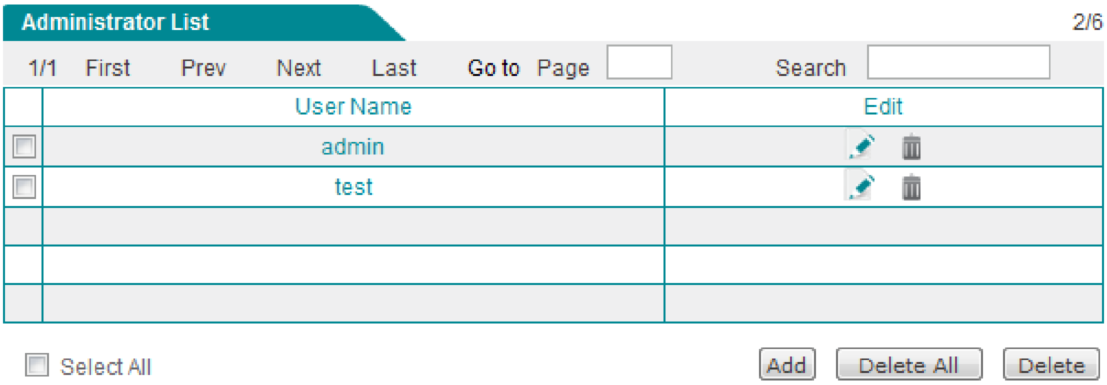
Chapter 11System Administration

This chapter describes how to perform maintenance activities on the Wireless Router, including administrator settings, system time settings, configuration backup and restore, firmware upgrade, remote management, and scheduled task settings.

11.1 Administrator

This section describes the **Administration > Administrator** page, where you can add, view, modify and delete the administrator accounts.

11.1.1 Administrator List



	User Name	Edit
□	admin	✎ 🗑
□	test	✎ 🗑

Figure 11- 1 Administrator List

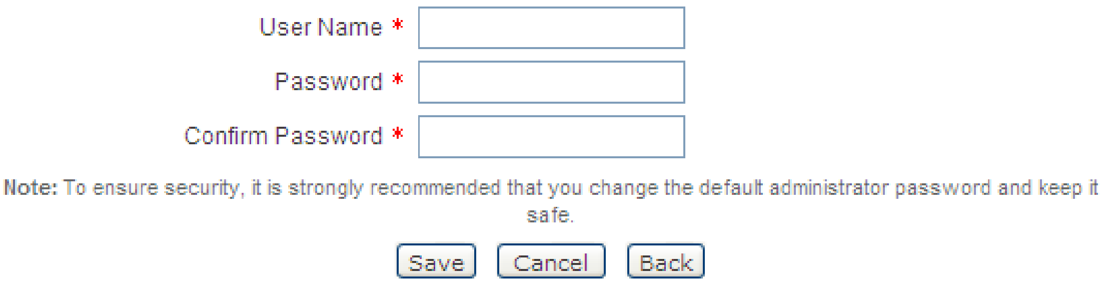
- **Add an Administrator Account:** To add a new administrator account, first click the **Add** button to go to the setup page, next configure it, lastly click the **Save** button.
- **View Administrator Account(s):** When you have configured one or more administrator accounts, you can view them in the **Administrator List**.
- **Modify an Administrator Account:** To modify a configured administrator account, click its **User Name** hyperlink or ✎ icon, the related information will be displayed in the setup page. Then modify it, and click the **Save** button.
- **Delete Administrator Account(s):** There are three ways to delete administrator account(s).

1. To delete an administrator account, directly click its 🗑 icon.
2. To delete more than one administrator account at a time, select the leftmost check boxes of the administrator accounts that you want to delete, and then click the **Delete** button.
3. To delete all the administrator accounts at a time, directly click the **Delete All** button.

✓ **Note**

You can change the default administrator password, but you cannot change its user name or delete it.

11.1.2 Administrator Settings



User Name *

Password *

Confirm Password *

Note: To ensure security, it is strongly recommended that you change the default administrator password and keep it safe.

Figure 11- 2 Administrator Settings

- **User Name:** It specifies a unique login name (case sensitive) of the administrator.
- **Password:** It specifies a login password (case sensitive) of the administrator. This password will be required to login to the Wireless Router in the future.
- **Confirm Password:** You should re-enter the password.
- **Save:** Click to save your changes.
- **Cancel:** Click to revert to the last saved settings.
- **Back:** Click to go back to the **Administrator List**.

✓ **Note**

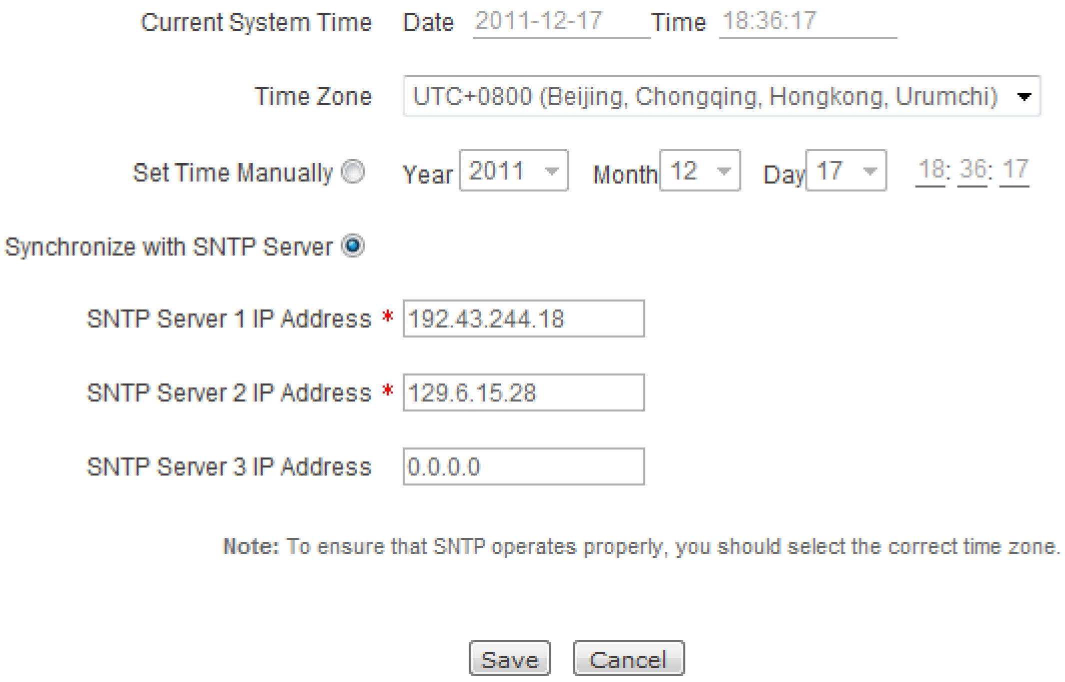
To ensure security, it is strongly recommended that you change the default administrator password, remember your new password and keep it safe. Once changed, you should use the new password to login to the Wireless Router in the future.

11.2 System Time

This section describes the **Administration > Time** page, see Figure 11-3.

To ensure that the time-related features (e.g., DDNS, Schedule, Access Control, etc.) work well, you should synchronize the system clock.

You can manually configure the system time or enable SNTP (Synchronize with SNTP Server) to automatically synchronize the system time from a designated SNTP server on the Internet. It is suggested that you choose SNTP to automatically synchronize time in most cases.



Current System Time Date 2011-12-17 Time 18:36:17

Time Zone UTC+0800 (Beijing, Chongqing, Hongkong, Urumchi)

Set Time Manually ○ Year 2011 Month 12 Day 17 18: 36: 17

Synchronize with SNTP Server ●

SNTP Server 1 IP Address * 192.43.244.18

SNTP Server 2 IP Address * 129.6.15.28

SNTP Server 3 IP Address 0.0.0.0

Note: To ensure that SNTP operates properly, you should select the correct time zone.

Figure 11-3 System Time Settings

- **Current System Time:** It displays the Wireless Router's current date (YYYY-MM-DD) and time (HH:MM:SS).
- **Time Zone:** It specifies the time zone for your local time. To ensure that SNTP operates properly, you must select the correct time zone.
- **Set Time Manually:** If you want to set the date (YYYY-MM-DD) and time (HH:MM:SS) for the Wireless Router manually, select this radio button.
- **Synchronize with SNTP Server:** If you want the Wireless Router to automatically synchronize the system clock from a designated SNTP server on the Internet, select this radio button.

- **SNTP Server 1 IP Address ~ SNTP Server 3 IP Address:** It allows you to configure up to three SNTP servers on the Wireless Router. The Server 1 is the primary server (the default is 192.43.244.18), and the Server 2 is the first backup server (the default is 129.6.15.28), and the Server 3 is the second backup server (the default is 0.0.0.0).
- **Save:** Click to save your changes.
- **Cancel:** Click to revert to the last saved settings.

✓ **Note**

For more information about SNTP, or to find an SNTP server with which you can synchronize the system clock, please refer to http://www.ntp.org.

11.3 Configuration

This section describes the **Administration > Configuration** page, where you can backup the current configuration file to the local PC, restore your previous configuration using the backup configuration file, and reset the Wireless Router to factory default settings.

11.3.1 Backup Configuration

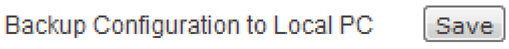


Figure 11-4 Backup Configuration

- **Backup:** Click to export and save the Wireless Router's current configuration to a text file on your local computer.

11.3.2 Restore Configuration

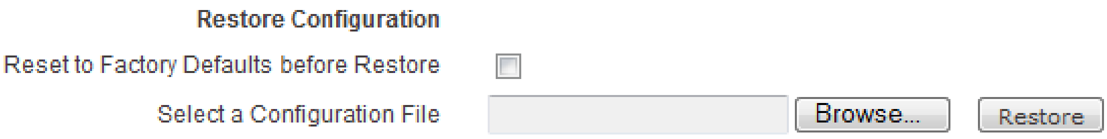

Restore Configuration
Reset to Factory Defaults before Restore
□
Select a Configuration File
Browse...
Restore

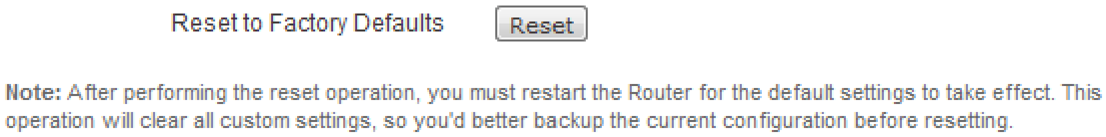
Figure 11-5 Restore Configuration

- **Reset to Factory Defaults before Restore:** If you select this check box, it will reset the Wireless Router to factory default settings before importing the configuration file; else import the file directly.
- **Select a Configuration File:** Click the **Browse** button to choose an appropriate configuration file or enter the file path and name in the text box.
- **Restore:** Click to import the selected configuration file. It will overwrite the current configuration on the Wireless Router with the new configuration.

Note

To avoid any unexpected error, do not power off the Wireless Router during importing the configuration file.

11.3.3 Reset to Factory Defaults



Note: After performing the reset operation, you must restart the Router for the default settings to take effect. This operation will clear all custom settings, so you'd better backup the current configuration before resetting.

Figure 11- 6 Reset to Factory Defaults

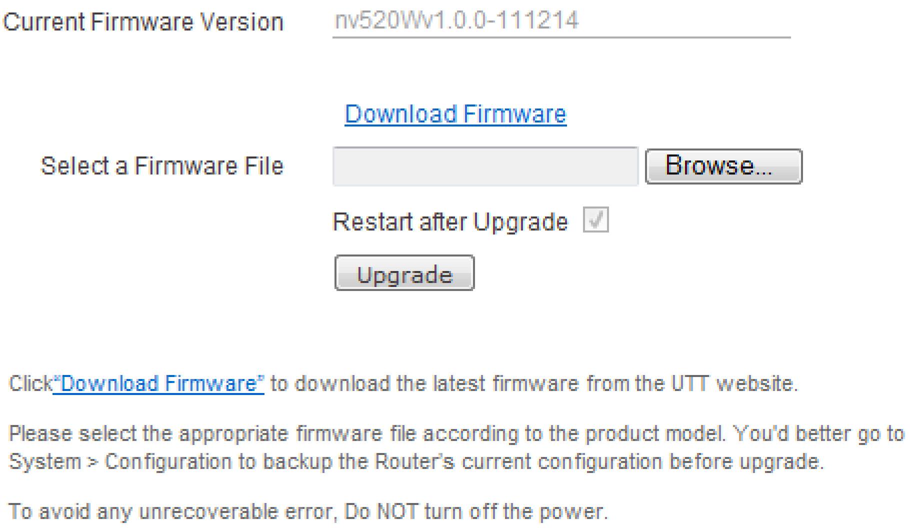
- **Reset:** To reset the Wireless Router to factory default settings, click the **Reset** button, and then restart the Wireless Router.

Note

1. After performing the reset operation, you must manually restart the Wireless Router in order for the default settings to take effect.
2. The reset operation will clear all of the Wireless Router’s custom settings. It is strongly recommended that you backup the current configuration before resetting.
3. The default administrator user name and password both are **admin** (case sensitive). The default LAN IP address is 192.168.1.1 with a subnet mask of 255.255.255.0.

11.4 Firmware Upgrade

This section describes the **Administration > Firmware** page, where you can view the current firmware version information, download the latest firmware from the website of UTT Technologies Co., Ltd., and upgrade the firmware.



Current Firmware Version nv520Wv1.0.0-111214

Select a Firmware File

Restart after Upgrade ☑

Click"Download Firmware" to download the latest firmware from the UTT website.

Please select the appropriate firmware file according to the product model. You'd better go to System > Configuration to backup the Router's current configuration before upgrade.

To avoid any unrecoverable error, Do NOT turn off the power.

Figure 11- 7 Firmware Upgrade

- **Current Firmware Version:** It displays the version of the current firmware installed on the Wireless Router.

To upgrade the Wireless Router's firmware, follow these steps:

Step 1 Downloading the latest firmware

Click the **Download Firmware** hyperlink to download the latest firmware from the website of UTT Technologies Co., Ltd.

Note

1. Please select the appropriate firmware file according to the product model.
2. It is recommended that you go to the **Administration > Configuration** to backup the Wireless Router's current configuration before upgrade.

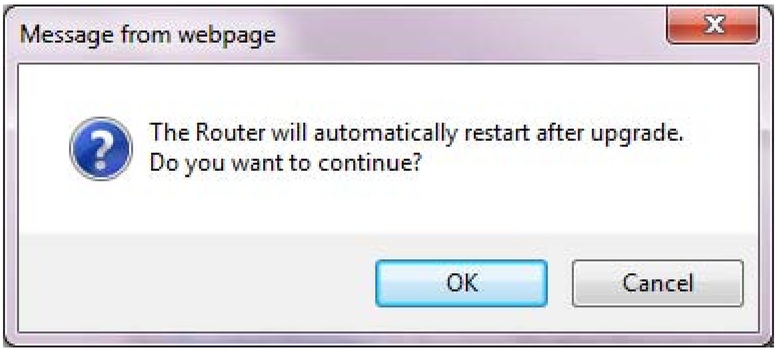
Step 2 Choosing the firmware

Click the **Browse** button to choose the firmware file you want to upgrade or enter the file path and name in the **Select a Firmware File** text box.

- **Restart after Upgrade:** After the upgrade is complete, the Wireless Router will automatically restart in order for the new firmware to take effect.

Step 3 Renewing the firmware

Click the **Upgrade** button to renew the Wireless Router's firmware. If you click the **Upgrade** button, you will be prompted to confirm the upgrade (see Figure 11- 8). Then you can click **OK** to upgrade the firmware and restart the Wireless Router, or click **Cancel** to cancel the operation.


Message from webpage

The Router will automatically restart after upgrade.
Do you want to continue?

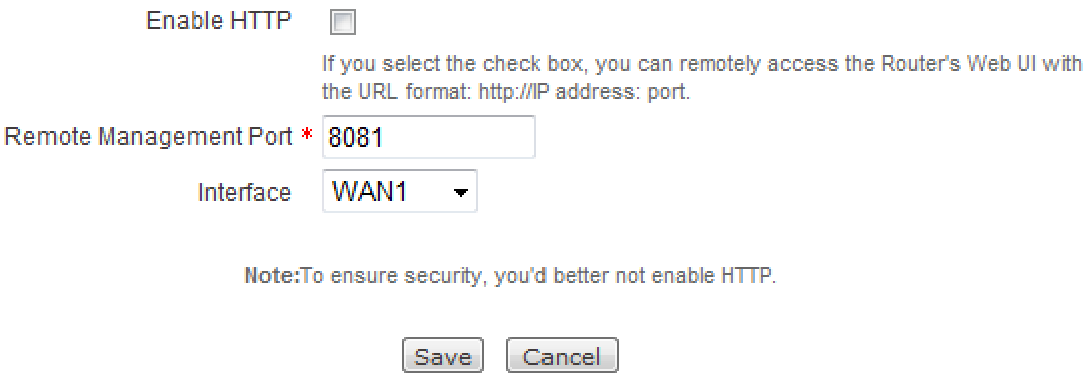
Figure 11- 8 Prompt Dialog Box - Firmware Upgrade

✓ **Note**

1. It is strongly recommended that you upgrade the firmware when the Wireless Router is under light load.
2. If you upgrade firmware timely, the Wireless Router will have more functionality and better performance. The right upgrade will not change the Wireless Router's current settings.
3. To avoid any unexpected error or unrecoverable hardware damage, do not power off the Wireless Router during upgrading.
4. After the upgrade is complete, the Wireless Router will automatically restart in order for the new firmware to take effect, without human intervention.

11.5 Remote Access

This section describes the **Administration > Remote Access** page. In this page, you can enable HTTP remote management, which allows you to access the Wireless Router's Web UI from anywhere over the Internet.



Enable HTTP □

If you select the check box, you can remotely access the Router's Web UI with the URL format: http://IP address: port.

Remote Management Port * 8081

Interface WAN1

Note: To ensure security, you'd better not enable HTTP.

Figure 11- 9 Remote Access Settings

- **Enable HTTP:** It allows you to enable or disable HTTP remote management. Select this check box to enable HTTP remote management. To access the Wireless Router's Web UI over the Internet, you should enter **http://** and the Wireless Router's WAN IP address, followed by a colon and the port number. For example, if the WAN IP address is 218.21.31.3 and port number is 8081, please enter http://218.21.31.3:8081 in your browser's address bar.

- **Remote Management Port:** It specifies the port number that will be open to outside access. The default value is 8081.

- **Interface:** It specifies the interface on which the HTTP remote management is enabled. Here you can select only one interface. To enable HTTP remote management on multiple interfaces at the same time, you need to go to the **Advanced > NAT&DMZ > Port Forwarding** page to create port forwarding entry(s) for the other interface(s).

- **Save:** Click to save your changes.

- **Cancel:** Click to revert to the last saved settings.

Note

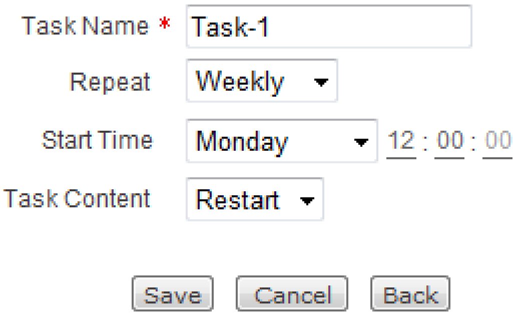
1. To ensure security, it is strongly recommended that you don't enable HTTP remote management unless necessary.

2. After you enable the HTTP remote management, the system will automatically create a port forwarding entry whose name is **admin**. You can go to the **Advanced > NAT&DMZ > Port Forwarding** page to view it in the **Port Forwarding List**.

11.6 Scheduled Task

This section describes the **Administration > Scheduled Task** page, where you can create and view the scheduled tasks. With scheduled tasks, the Wireless Router can periodically start each task at the time you specify.

11.6.1 Scheduled Task Settings



Task Name * Task-1

Repeat Weekly

Start Time Monday 12 : 00 : 00

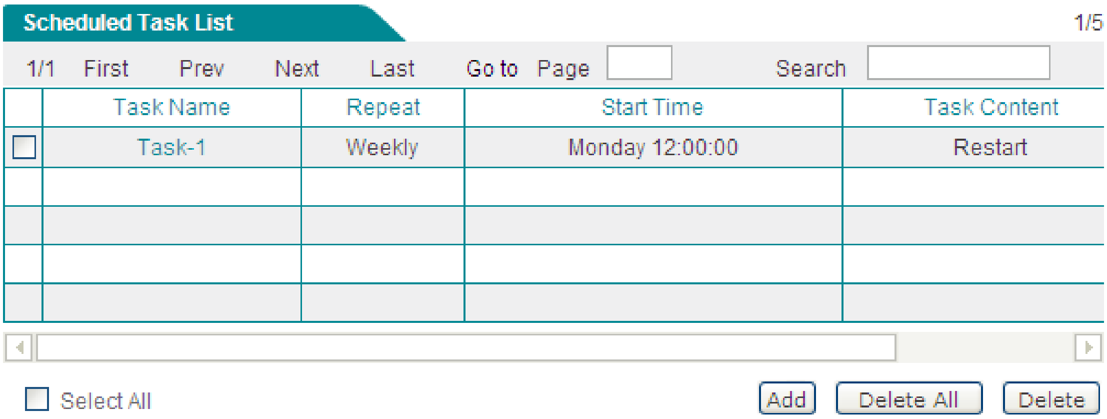
Task Content Restart

Figure 11- 10 Scheduled Task Settings

- **Task Name:** It specifies a unique name of the task.
- **Repeat:** It specifies how often the Wireless Router will perform the task. The available options are **Weekly**, **Daily**, **Hourly**, **Minutely**.
- **Start Time:** It specifies the time at which the Wireless Router will start the task. Its settings depend on the value of **Repeat**.
- **Task Content:** It specifies the content of the task. Now the Wireless Router only provide one option: **Restart**, which means that the Wireless Router will restart itself periodically.

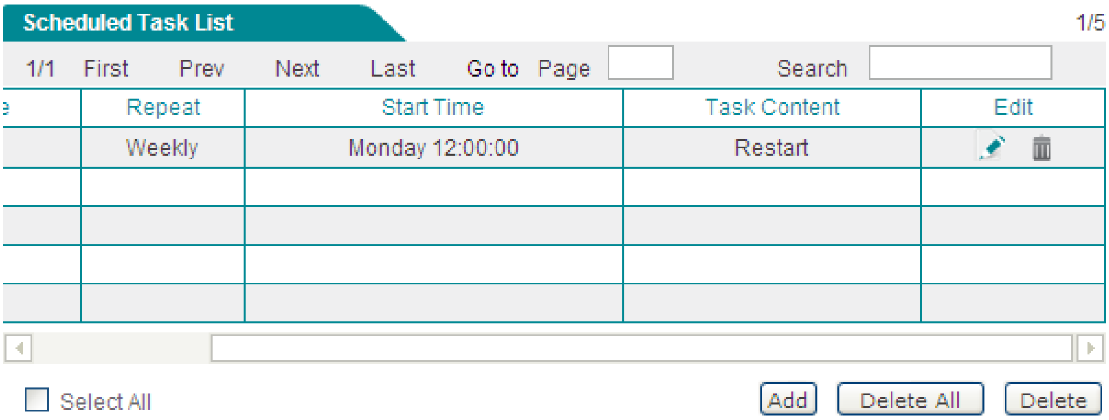
- **Save:** Click to save your changes.
- **Cancel:** Click to revert to the last saved settings.
- **Back:** Click to go back to the **Scheduled Task List.**

11.6.2 Scheduled Task List



□	Task Name	Repeat	Start Time	Task Content
□	Task-1	Weekly	Monday 12:00:00	Restart

Figure 11- 11 Scheduled Task List



e	Repeat	Start Time	Task Content	Edit
	Weekly	Monday 12:00:00	Restart	✎ 🗑

Figure 11- 12 Scheduled Task List (Continue)

- **Add a Scheduled Task:** To add a new scheduled task, first click the **Add** button to go to the **Scheduled Task Settings** page, next configure it, lastly click the **Save** button.

- **View Scheduled Task(s):** When you have configured one or more scheduled tasks, you can view them in the **Scheduled Task List**.

- **Modify a Scheduled Task:** To modify a configured scheduled task, click its **User Name** hyperlink or ✎ icon, the related information will be displayed in the setup page. Then modify it, and click the **Save** button.

- **Delete Scheduled Task(s):** There are three ways to delete scheduled task(s).

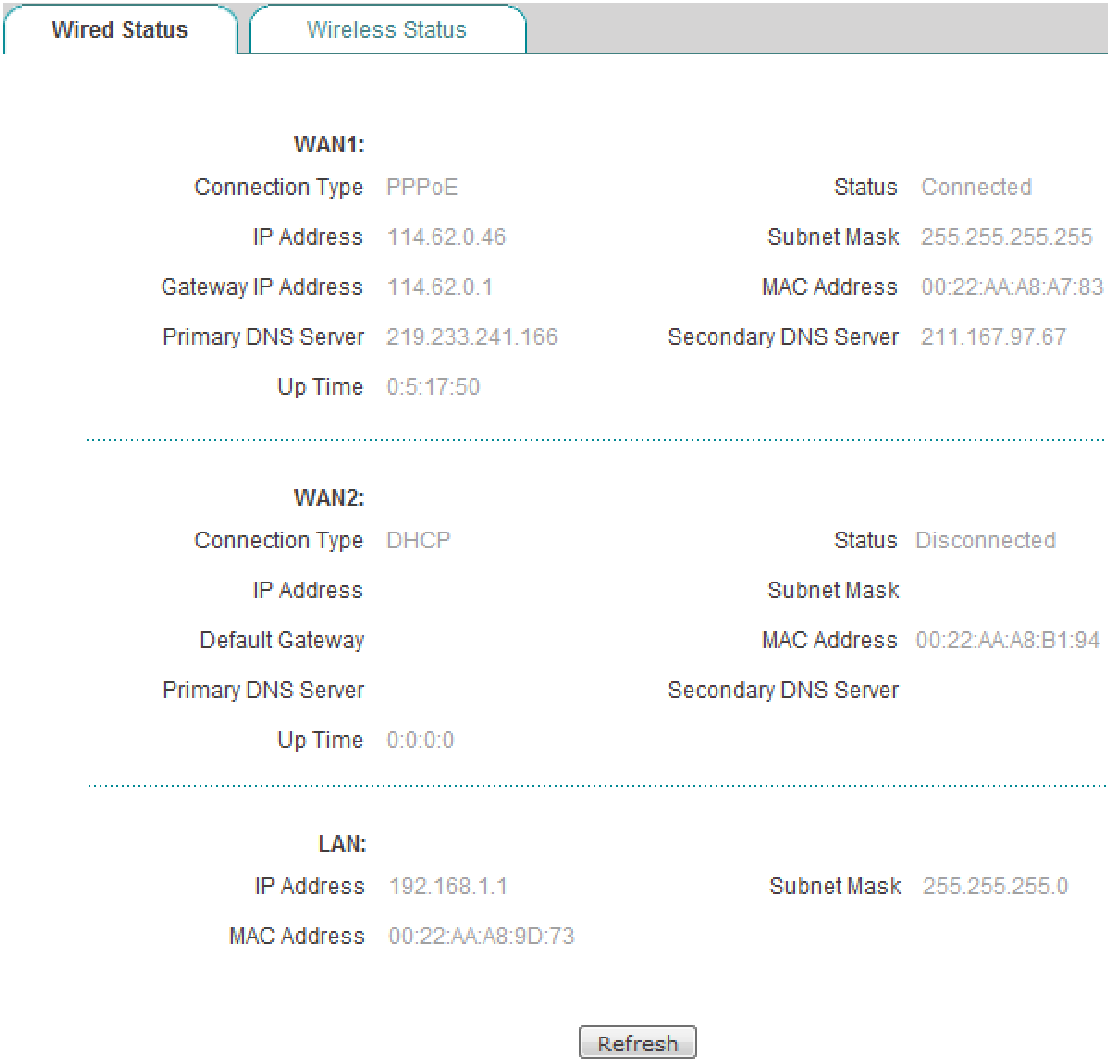
  1. To delete a scheduled task, directly click its 🗑 icon.
  2. To delete more than one scheduled task at a time, select the leftmost check boxes of the tasks that you want to delete, and then click the **Delete** button.
  3. To delete all the scheduled tasks at a time, directly click the **Delete All** button.

Chapter 12 Status

This chapter describes how to view the wired status and wireless status, the traffic statistics for each interface, and system information including the current system time, system up time, system resources usage information, firmware version, and system log.

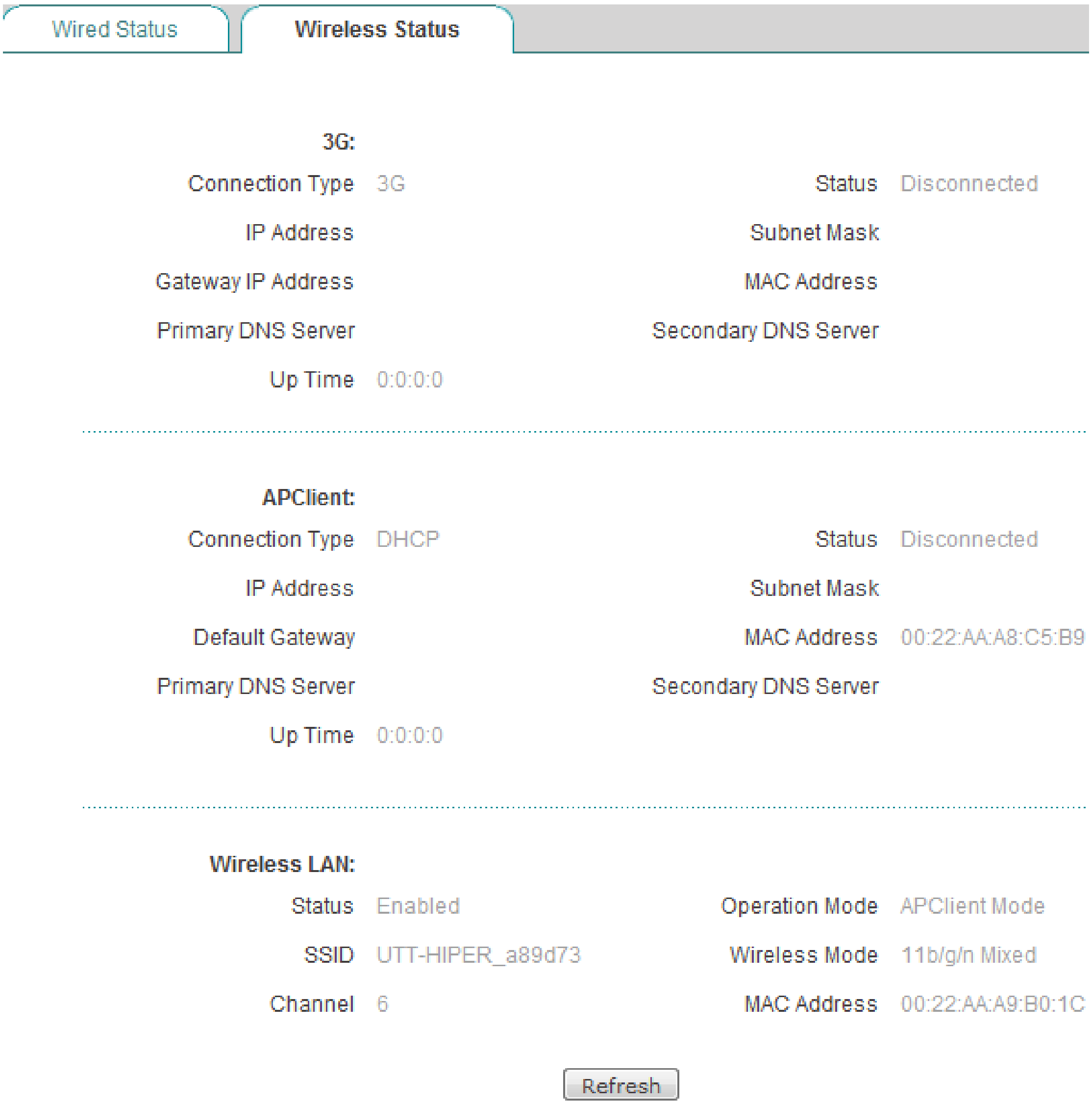
12.1 System Status

This section describes the **Status > System Status** page, which include **Wired Status** and **Wireless Status**.



WAN1:			
Connection Type	PPPoE	Status	Connected
IP Address	114.62.0.46	Subnet Mask	255.255.255.255
Gateway IP Address	114.62.0.1	MAC Address	00:22:AA:A8:A7:83
Primary DNS Server	219.233.241.166	Secondary DNS Server	211.167.97.67
Up Time	0:5:17:50		
WAN2:			
Connection Type	DHCP	Status	Disconnected
IP Address		Subnet Mask	
Default Gateway		MAC Address	00:22:AA:A8:B1:94
Primary DNS Server		Secondary DNS Server	
Up Time	0:0:0:0		
LAN:			
IP Address	192.168.1.1	Subnet Mask	255.255.255.0
MAC Address	00:22:AA:A8:9D:73		

Figure 12- 1 System Status - Wired Status



3G:

Connection Type	3G	Status	Disconnected
IP Address		Subnet Mask	
Gateway IP Address		MAC Address	
Primary DNS Server		Secondary DNS Server	
Up Time	0:0:0:0		

APClient:

Connection Type	DHCP	Status	Disconnected
IP Address		Subnet Mask	
Default Gateway		MAC Address	00:22:AA:A8:C5:B9
Primary DNS Server		Secondary DNS Server	
Up Time	0:0:0:0		

Wireless LAN:

Status	Enabled	Operation Mode	APClient Mode
SSID	UTT-HIPER_a89d73	Wireless Mode	11b/g/n Mixed
Channel	6	MAC Address	00:22:AA:A9:B0:1C

Figure 12- 2 System Status - Wireless Status

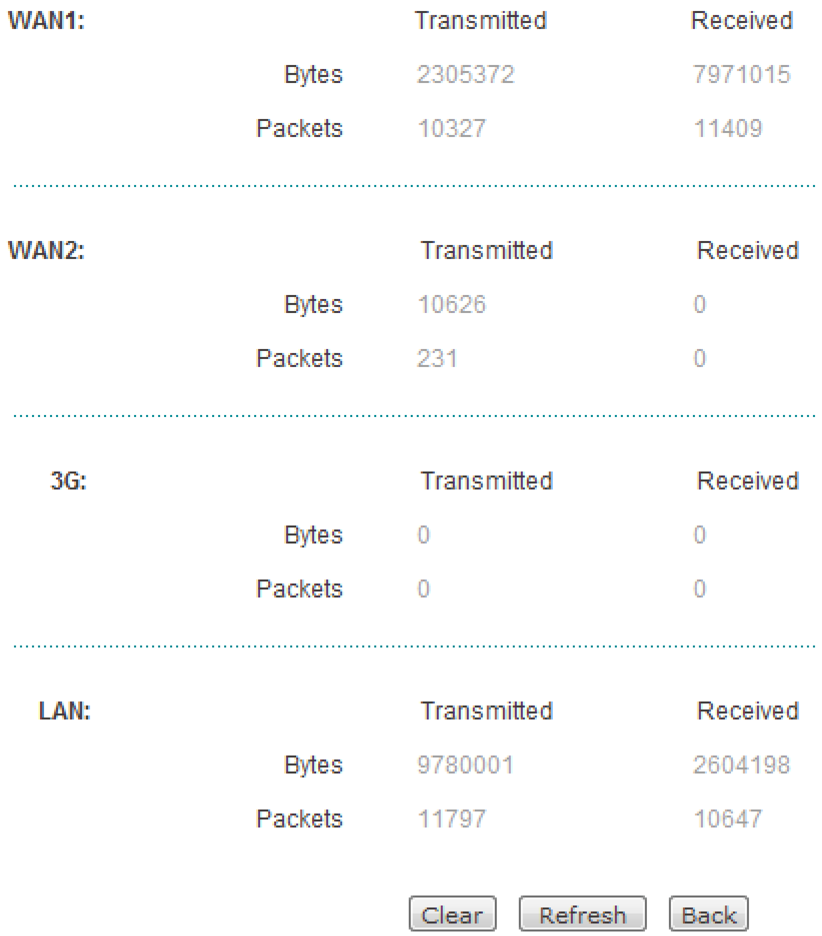
- **Wired Status:** Refer to **Section 4.2.1 Wired Status** for detailed information.
- **Wireless Status:** Refer to **Section 4.2.2 Wireless Status** for detailed information.

Note

The **Wired Status** page and **Wireless Status** page only display the status information of the interfaces that have been configured.

12.2 Traffic Statistics

This section describes the ingress and egress traffic statistics for each interface.



WAN1:	Transmitted	Received
Bytes	2305372	7971015
Packets	10327	11409

WAN2:	Transmitted	Received
Bytes	10626	0
Packets	231	0

3G:	Transmitted	Received
Bytes	0	0
Packets	0	0

LAN:	Transmitted	Received
Bytes	9780001	2604198
Packets	11797	10647

Figure 12-3 Traffic Statistics

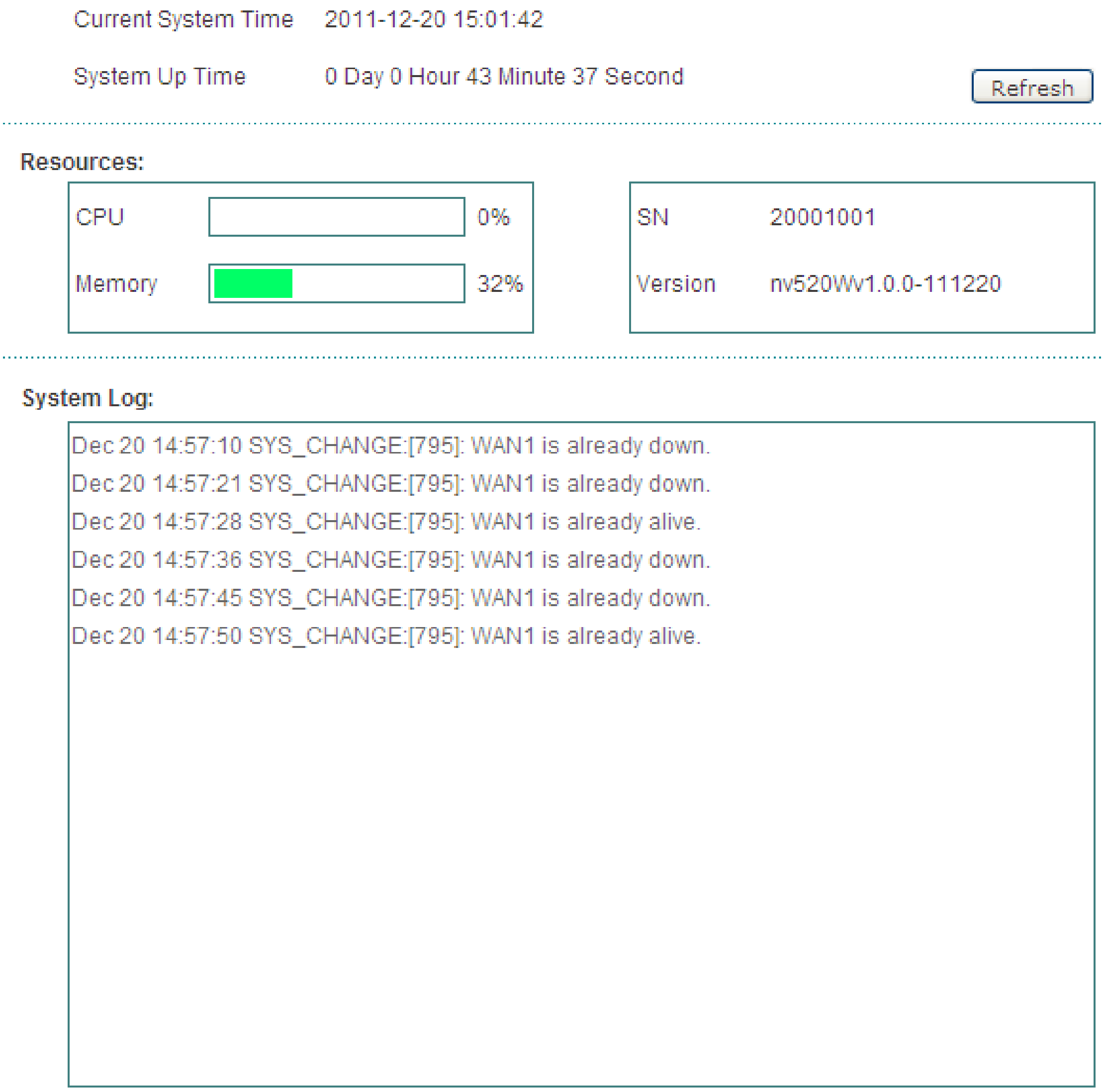
- **WAN1**, **WAN2**, **3G**, **APClient** and **LAN**: You can view the traffic statistics for each interface, including the number of bytes received and transmitted, and the number of packets received and transmitted.
- **Clear:** Click to clear all traffic statistics.
- **Refresh:** Click to view the latest traffic statistics.
- **Back:** Click to go back to the **Start > Interface Traffic** page.

Note

This page only displays the traffic statistics for the interfaces that have been configured.

12.3 System Information

This section describes the **Status > System Info** page, which includes the current system time, system up time, system resources usage information, SN, firmware version, and system log. System information can help you identify and diagnose the source of current system problems, or help you predict potential system problems.



Current System Time 2011-12-20 15:01:42

System Up Time 0 Day 0 Hour 43 Minute 37 Second

Resources:

CPU	0%
Memory	32%

SN	20001001
Version	nv520Wv1.0.0-111220

System Log:

```
Dec 20 14:57:10 SYS_CHANGE:[795]: WAN1 is already down.
Dec 20 14:57:21 SYS_CHANGE:[795]: WAN1 is already down.
Dec 20 14:57:28 SYS_CHANGE:[795]: WAN1 is already alive.
Dec 20 14:57:36 SYS_CHANGE:[795]: WAN1 is already down.
Dec 20 14:57:45 SYS_CHANGE:[795]: WAN1 is already down.
Dec 20 14:57:50 SYS_CHANGE:[795]: WAN1 is already alive.
```

Figure 12- 4 System Information

- **Current System Time:** It displays the Wireless Router’s current date (YYYY-MM-DD) and time (HH:MM:SS).
- **System Up Time:** It displays the elapsed time (in days, hours, minutes and seconds) since the Wireless Router was last started.
- **CPU:** It displays the current CPU usage.
- **Memory:** It displays the current memory usage.

- **SN:** It displays the internal serial number of the Wireless Router, which may be different from the SN found on the label at the bottom of the Wireless Router.
- **Version:** It displays the version of the current firmware installed on the Wireless Router.
- **System Log:** It records the events that occur in the system, such as, system startup, wireless enabled, and so on.

▶ **Refresh:** Click to view the latest system information.

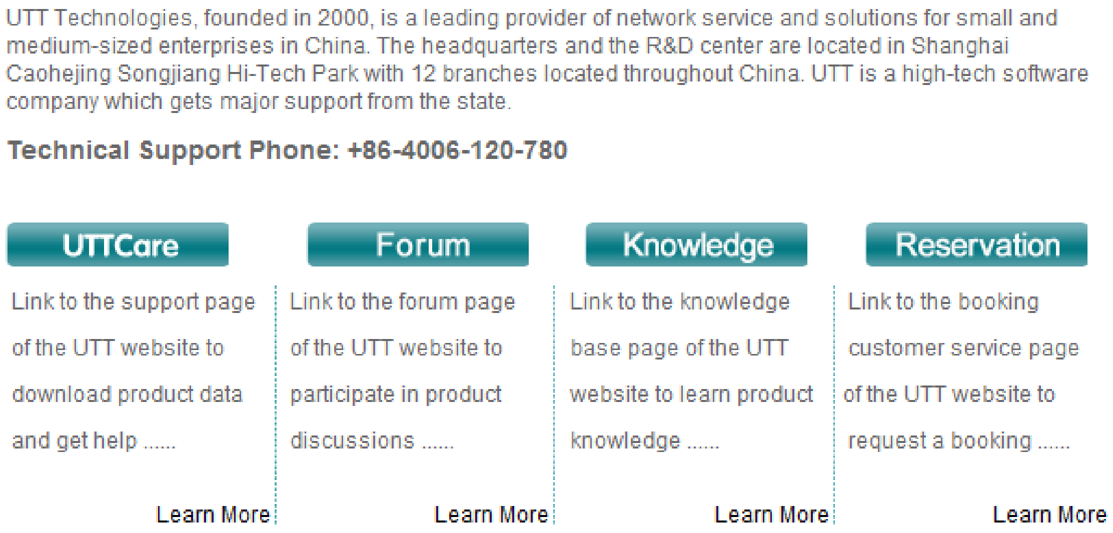
✓ **Note**

The **CPU** and **Memory** are displayed as a status bar and percentage value. The color of the status bar indicates the usage percentage for each resource.

- When the percentage is below 1%, the bar is blank.
- When the percentage is between 1% and 50% (below 50%), the color is green.
- When the percentage is between 50% and 70% (below 70%), the color is orange.
- When the percentage is equal to or above 70%, the color is red.

Chapter 13 Support

The **Support** page provides links to the UTTCare, Forum, Knowledge and Reservation page of the UTT website, which can help you quickly learn the UTT Technologies service system and enjoy the most intimate and professional services.



UTT Technologies, founded in 2000, is a leading provider of network service and solutions for small and medium-sized enterprises in China. The headquarters and the R&D center are located in Shanghai Caohejing Songjiang Hi-Tech Park with 12 branches located throughout China. UTT is a high-tech software company which gets major support from the state.

Technical Support Phone: +86-4006-120-780

UTTCare

Link to the support page of the UTT website to download product data and get help ......

Learn More

Forum

Link to the forum page of the UTT website to participate in product discussions ......

Learn More

Knowledge

Link to the knowledge base page of the UTT website to learn product knowledge ......

Learn More

Reservation

Link to the booking customer service page of the UTT website to request a booking ......

Learn More

Figure 13- 1 Support

As shown in Figure 13- 1, it allows you to click each **Learn More** hyperlink to directly open the corresponding page of the UTT website.

- **UTTCare:** Link to the support page of the UTT website to download product data and get help.
- **Forum:** Link to the forum page of the UTT website to participate in product discussions.
- **Knowledge:** Link to the knowledge base page of the UTT website to learn more about our products and how to use them.
- **Reservation:** Link to the booking customer service page of the UTT website to request a booking.

Appendix A How to Configure Your PC

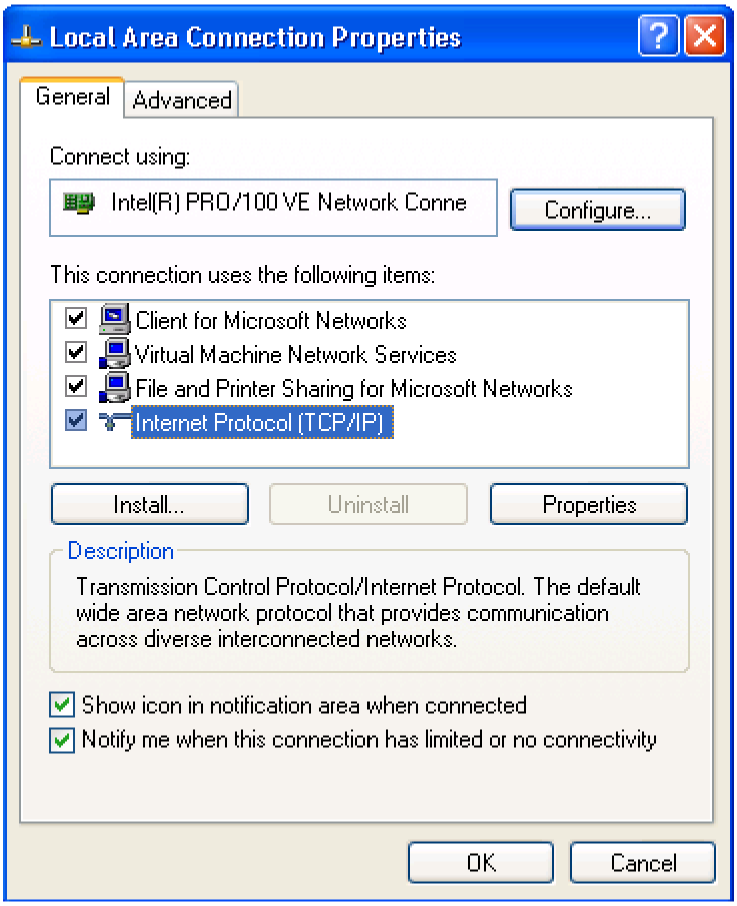
This appendix describes how to configure TCP/IP settings on a Windows XP-based computer.

There are two ways to configure TCP/IP settings: manually configuring TCP/IP settings, and automatically configuring TCP/IP settings with DHCP. The following describes the two ways respectively.

● Method One: Manually Configuring TCP/IP

To configure the TCP/IP protocol manually, follow these steps:

1. On the Windows taskbar, click **Start > Settings > Control Panel**.
2. Double-click the **Network Connections** icon, right-click the **Local Area Connection** icon and select **Properties**. On the **General** tab (see Figure A-0-1), in the **This connection uses the following items** box, click the **Internet Protocol (TCP/IP)** item, and then click the **Properties** button.



Local Area Connection Properties

Connect using:
Intel(R) PRO/100 VE Network Conne

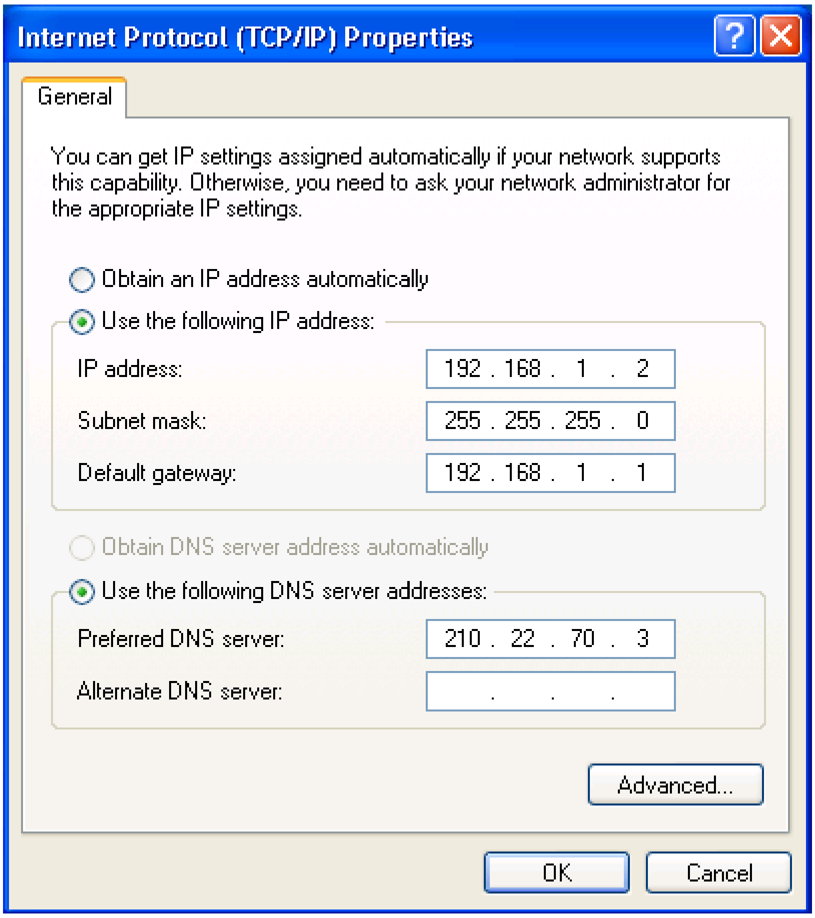
This connection uses the following items:
☑ Client for Microsoft Networks
☑ Virtual Machine Network Services
☑ File and Printer Sharing for Microsoft Networks
☑ Internet Protocol (TCP/IP)

Description
Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.

☑ Show icon in notification area when connected
☑ Notify me when this connection has limited or no connectivity

Figure A- 0- 1 Local Area Connection Properties

3. In the **Internet Protocol (TCP/IP) Properties** dialog box (see Figure A-0-2), select the **Use the following IP address** option，enter 192.168.1.x (x is between 2 and 254, including 2 and 253) in the **IP address** text box, 255.255.255.0 in the **Subnet mask** text box, and 192.168.1.1 in the **Default gateway** text box.



Internet Protocol (TCP/IP) Properties

General

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

○ Obtain an IP address automatically

● Use the following IP address:

IP address:	192 . 168 . 1 . 2
Subnet mask:	255 . 255 . 255 . 0
Default gateway:	192 . 168 . 1 . 1

○ Obtain DNS server address automatically

● Use the following DNS server addresses:

Preferred DNS server:	210 . 22 . 70 . 3
Alternate DNS server:	. . .

Figure A-0- 2 Internet Protocol (TCP/IP) Properties

4. Select the **Use the following DNS server address** option, enter the primary DNS server IP address in the **Preferred DNS server** text box, and enter the secondary DNS server IP address in the **Alternate DNS server** text box (optional). A DNS query is sent to the primary DNS server at first. If the primary DNS server is unable to service the query, the query will be sent to the secondary DNS server.

5. Click the **OK** button. Now you have finished configuring the TCP/IP settings.

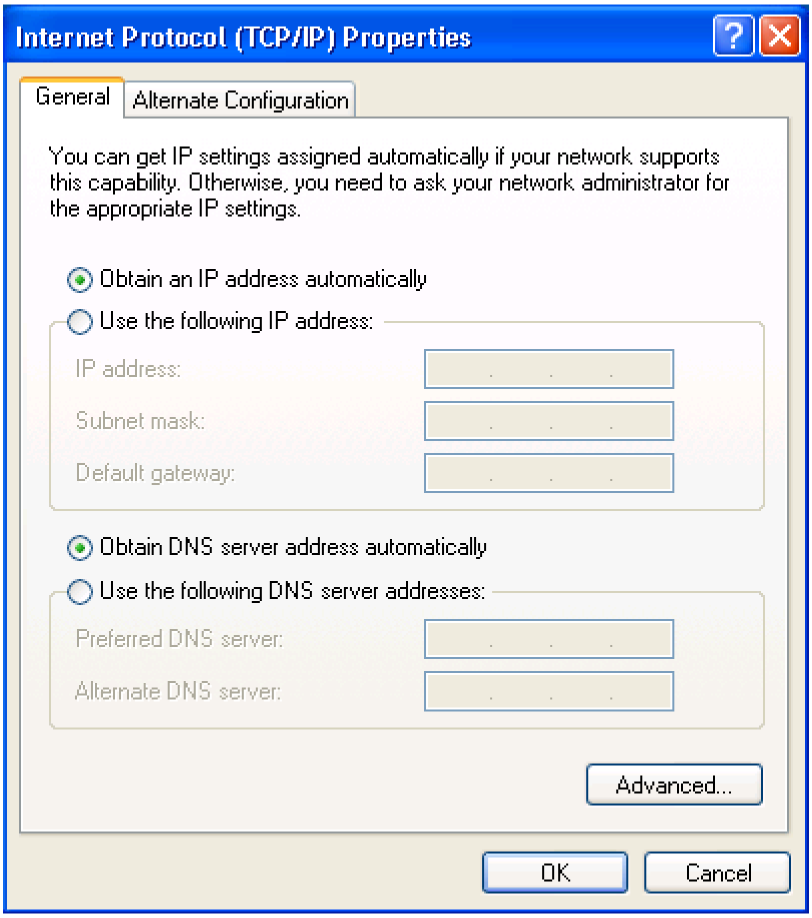
● Method Two: Automatically Configuring TCP/IP with DHCP

1. To ensure that the PC can obtain an IP address and other TCP/IP parameters automatically from the Wireless Router, you should go to the **Network > DHCP Server** page to enable DHCP server on the Wireless Router.

2. On the Windows taskbar, click **Start > Settings > Control Panel**.

3. Double-click the **Network Connections** icon, right-click the **Local Area Connection** icon and select **Properties**. On the **General** tab (see Figure A-0-1), in the **This connection uses the following items** box, click the **Internet Protocol (TCP/IP)** item, and then click the **Properties** button.

4. In the **Internet Protocol (TCP/IP) Properties** dialog box, on the **General** tab (see Figure A-0-3), select the **Obtain an IP address automatically** option and **Obtain DNS server address automatically** option.



You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

● Obtain an IP address automatically

○ Use the following IP address:

IP address: . . .

Subnet mask: . . .

Default gateway: . . .

● Obtain DNS server address automatically

○ Use the following DNS server addresses:

Preferred DNS server: . . .

Alternate DNS server: . . .

Figure A-0- 3 Internet Protocol (TCP/IP) Properties

5. Click the **OK** button. Now you have finished configuring the TCP/IP settings.

Note

In Windows XP, the TCP/IP stack is a core component of the operating system. Therefore, you cannot remove TCP/IP in Windows XP. However, if you have network connectivity problems and think its TCP/IP related, you can reinstall TCP/IP on your Windows XP-based computer. To install TCP/IP on top of itself, follow these steps:

a. On the Windows taskbar, click **Start > Settings > Control Panel**.

a. Double-click **Network Connections**, right-click **Local Area Connection** and select **Properties**.

b. Click **Install**.

c. Click **Protocol**, and then click **Add**.

d. Click **Have Disk**.

e. In the **Copy manufacturer's files from** box, type ***System_Drive_Letter*****:\windows\inf**, and then click **OK**.

f. In the list of available protocols, click **Internet Protocol (TCP/IP)**, and then click **OK**.

g. Restart your computer.

Appendix B FAQ

1. How to connect the Wireless Router to the Internet using PPPoE?

Step 1 Set your ADSL Modem to bridge mode (RFC 1483 bridged mode).

Step 2 Please make sure that your PPPoE Internet connection use standard dial-type. You may use Windows XP built-in PPPoE dial-in client to test.

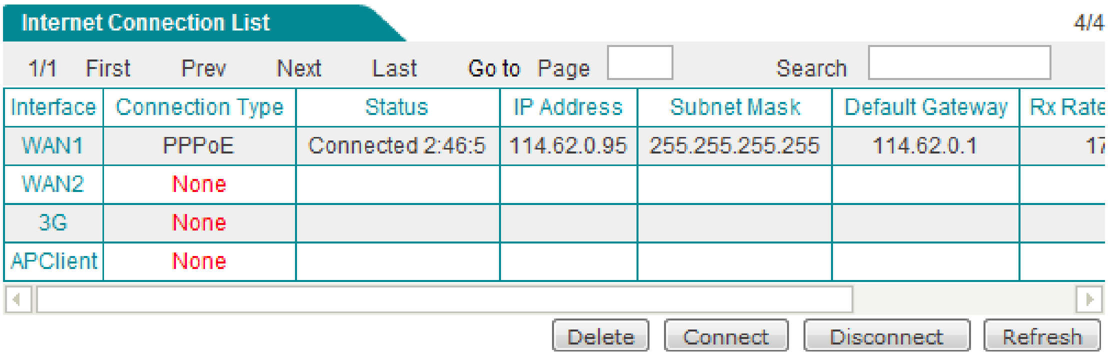
Step 3 Connect a network cable from the ADSL modem to a WAN port of the Wireless Router, and connect your telephone line to the ADSL modem's line port.

Step 4 Configure the PPPoE Internet connection related parameters in the **Start > Setup Wizard** or the **Network > WAN** page.

Step 5 If you pay monthly for the Internet connection, you can choose **Always On** as the **Dial Type**; else, you can choose **On Demand** or **Manual** as the **Dial Type**, and specify the **Idle Timeout** to avoid wasting online time due to that you forget to hang up the connection in time.

Step 6 If you choose **Manual** as the **Dial Type**, you need to dial up manually in the **Internet Connection List** on the **Network > WAN** page. Refer to **Section 5.1.1.3** for more information.

Step 7 After the PPPoE connection is established successfully, you can view its configuration and status information in the **Internet Connection List** on the **Network > WAN** page, such as **Status** (**Connected** means that the connection is established successfully), the connection's **IP address** and **Gateway** assigned by your ISP, **Tx Rate**, **Rx Rate**, and so on, see Figure B-0- 1.

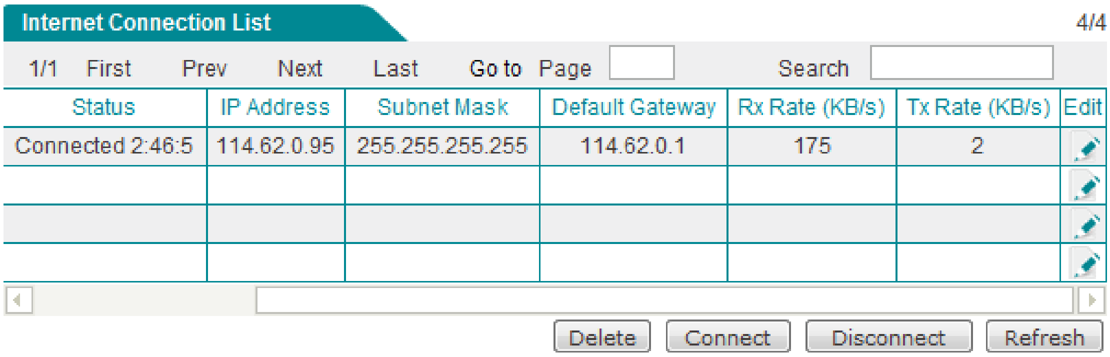


Internet Connection List 4/4

1/1 First Prev Next Last Go to Page Search

Interface	Connection Type	Status	IP Address	Subnet Mask	Default Gateway	Rx Rate
WAN1	PPPoE	Connected 2:46:5	114.62.0.95	255.255.255.255	114.62.0.1	17
WAN2	None					
3G	None					
APClient	None					

Figure B-0- 1 Viewing PPPoE Connection Status in the Internet Connection List



Status	IP Address	Subnet Mask	Default Gateway	Rx Rate (KB/s)	Tx Rate (KB/s)	Edit
Connected 2:46:5	114.62.0.95	255.255.255.255	114.62.0.1	175	2	✎
						✎
						✎
						✎

Figure B-0- 2 Viewing PPPoE Connection Status in the Internet Connection List (Continue)

Step 8 Configure the local computers according to the steps described in **Appendix A How to Configure Your PC**.

2. How to connect the Wireless Router to the Internet using Static IP?

Step 1 Please make sure the Internet connection is normal. You may use your PC to test.

Step 2 Connect a network cable from the network device provided by your ISP to a WAN port of the Wireless Router.

Step 3 Configure the Static IP Internet connection related parameters in the **Start > Setup Wizard** or the **Network > WAN** page.

Step 4 After the Static IP connection is established successfully, you can view its configuration and status information in the **Internet Connection List** on the **Network > WAN** page.

Step 5 Configure the local computers according to the steps described in **Appendix A How to Configure Your PC**.

3. How to connect the Wireless Router to the Internet using DHCP?

Step 1 Please make sure the Internet connection is normal. You may use your PC to test.

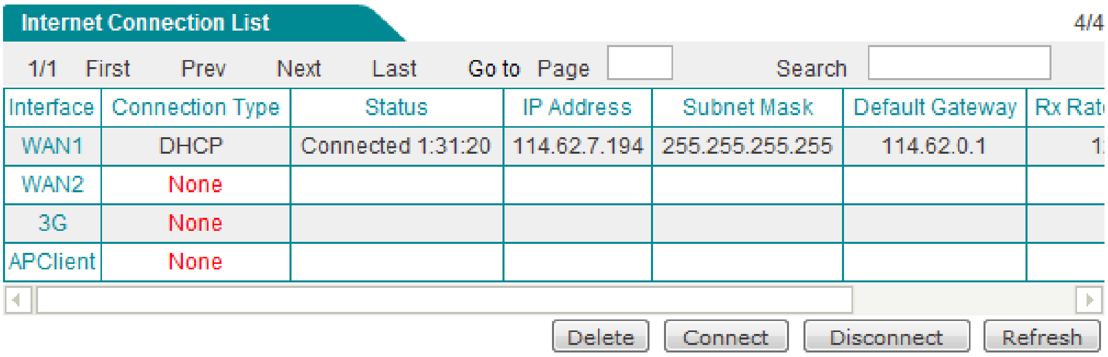
Step 2 Connect a network cable from the network device provided by your ISP to a WAN port of the Wireless Router.

Step 3 Configure the DHCP Internet connection related parameters in the **Start > Setup Wizard** or the **Network > WAN** page.

Note

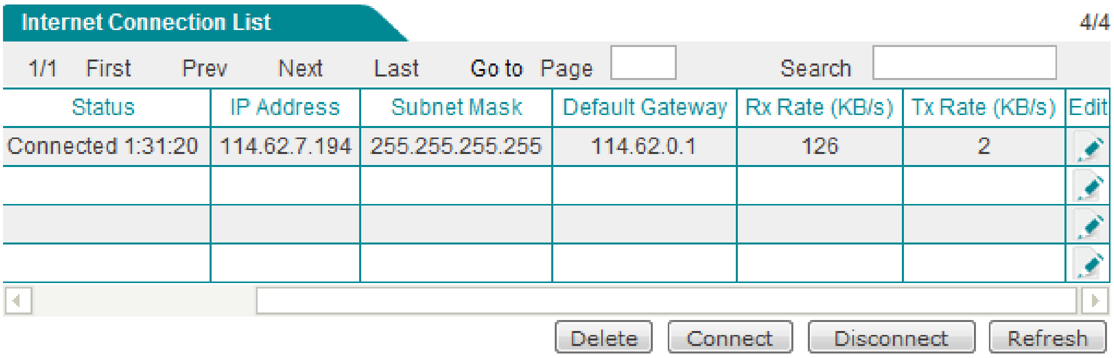
Some ISPs register the MAC address of your network device (usually a computer) when your account is first opened, and they will only accept traffic from that MAC address. In this case, you need to change the new Router’s MAC address to the registered MAC address. The operation is as follows: Go to the **Network > WAN** page, select the **MAC Address Clone** tab, and then change the MAC address of the corresponding interface, lastly click the **Save** button.

Step 4 After the DHCP Internet connection is established successfully, you can go to the view its configuration and status information in the **Internet Connection List** on the **Network > WAN** page, such as **Status** (**Connected** means the connection is established successfully), the connection’s **IP address** and **Gateway** assigned by your ISP, **Tx Rate**, **Rx Rate**, and so on, see Figure B-0-4.



Interface	Connection Type	Status	IP Address	Subnet Mask	Default Gateway	Rx Rat
WAN1	DHCP	Connected 1:31:20	114.62.7.194	255.255.255.255	114.62.0.1	1
WAN2	None					
3G	None					
APClient	None					

Figure B-0-3 Viewing DHCP Connection Status in the Internet Connection List



Status	IP Address	Subnet Mask	Default Gateway	Rx Rate (KB/s)	Tx Rate (KB/s)	Edit
Connected 1:31:20	114.62.7.194	255.255.255.255	114.62.0.1	126	2	✎
						✎
						✎
						✎

Figure B-0-4 Viewing DHCP Connection Status in the Internet Connection List (Continue)

Step 6 Configure the local computers according to the steps described in **Appendix A How to Configure Your PC**.

4. How to reset the Wireless Router to factory default settings?

✓ **Note**

The reset operation will clear all the custom settings on the Wireless Router, so do it with caution.

The following describes how to reset the Wireless Router to factory default settings. There are two cases depending on whether you remember the administrator password or not.

- **Case One: Remember the administrator password**

When you remember the administrator password, you can reset the Wireless Router to factory default settings via the Web UI. The operation is as follows: Go to the **Administration > Configuration** page, and then click the **Reset** button in the **Reset to Factory Defaults** configuration field, lastly manually restart the Wireless Router.

- **Case Two: Forget the administrator password**

If you forget the administrator password, you cannot login to the Wireless Router's Web UI. However, you can reset the Wireless Router to factory default settings via the RESET button, which is located on the rear panel of the Wireless Router. The operation is as follows: While the Wireless Router is powered on, use a pin or paper clip to press and hold the RESET button for more than 5 seconds, and then release the button. After that, the Wireless Router will restart with factory default settings.

Appendix C Common IP Protocols

Protocol Name	Protocol Number	Full Name
IP	0	Internet Protocol
ICMP	1	Internet Protocol Message Protocol
IGMP	2	Internet Group Management
GGP	3	Gateway-Gateway Protocol
IPINIP	4	IP in IP Tunnel Driver
TCP	6	Transmission Control Protocol
EGP	8	Exterior Gateway Protocol
IGP	9	Interior Gateway Protocol
PUP	12	PARC Universal Packet Protocol
UDP	17	User Datagram Protocol
HMP	20	Host Monitoring Protocol
XNS-IDP	22	Xerox NS IDP
RDP	27	Reliable Datagram Protocol
GRE	47	General Routing Encapsulation
ESP	50	Encap Security Payload
AH	51	Authentication Header
RVD	66	MIT Remote Virtual Disk
EIGRP	88	Enhanced Interior Gateway Routing Protocol
OSPF	89	Open Shortest Path First

Appendix D Common Service Ports

Service Name	Port	Protocol	Description
echo	7	tcp	
echo	7	udp	
discard	9	tcp	
discard	9	udp	
systat	11	tcp	Active users
systat	11	udp	Active users
daytime	13	tcp	
daytime	13	udp	
qotd	17	tcp	Quote of the day
qotd	17	udp	Quote of the day
chargen	19	tcp	Character generator
chargen	19	udp	Character generator
ftp-data	20	tcp	FTP, data
ftp	21	tcp	FTP. control
telnet	23	tcp	
smtp	25	tcp	Simple Mail Transfer Protocol
time	37	tcp	timserver
time	37	udp	timserver
rlp	39	udp	Resource Location Protocol
nameserver	42	tcp	Host Name Server
nameserver	42	udp	Host Name Server
nicname	43	tcp	whois
domain	53	tcp	Domain Name Server

domain	53	udp	Domain Name Server
bootps	67	udp	Bootstrap Protocol Server
bootpc	68	udp	Bootstrap Protocol Client
tftp	69	udp	Trivial File Transfer
gopher	70	tcp	
finger	79	tcp	
http	80	tcp	World Wide Web
kerberos	88	tcp	Kerberos
kerberos	88	udp	Kerberos
hostname	101	tcp	NIC Host Name Server
iso-tsap	102	tcp	ISO-TSAP Class 0
rtelnet	107	tcp	Remote Telnet Service
pop2	109	tcp	Post Office Protocol - Version 2
pop3	110	tcp	Post Office Protocol - Version 3
sunrpc	111	tcp	SUN Remote Procedure Call
sunrpc	111	udp	SUN Remote Procedure Call
auth	113	tcp	Identification Protocol
uucp-path	117	tcp	
nntp	119	tcp	Network News Transfer Protocol
ntp	123	udp	Network Time Protocol
epmap	135	tcp	DCE endpoint resolution
epmap	135	udp	DCE endpoint resolution
netbios-ns	137	tcp	NETBIOS Name Service
netbios-ns	137	udp	NETBIOS Name Service
netbios-dgm	138	udp	NETBIOS Datagram Service
netbios-ssn	139	tcp	NETBIOS Session Service
imap	143	tcp	Internet Message Access Protocol
pcmail-srv	158	tcp	PCMail Server

snmp	161	udp	
snmptrap	162	udp	SNMP trap
print-srv	170	tcp	Network PostScript
bgp	179	tcp	Border Gateway Protocol
irc	194	tcp	Internet Relay Chat Protocol
ipx	213	udp	IPX over IP
ldap	389	tcp	Lightweight Directory Access Protocol
https	443	tcp	MCom
https	443	udp	MCom
microsoft-ds	445	tcp	
microsoft-ds	445	udp	
kpasswd	464	tcp	Kerberos (v5)
kpasswd	464	udp	Kerberos (v5)
isakmp	500	udp	Internet Key Exchange
exec	512	tcp	Remote Process Execution
biff	512	udp	
login	513	tcp	Remote Login
who	513	udp	
cmd	514	tcp	
syslog	514	udp	
printer	515	tcp	
talk	517	udp	
ntalk	518	udp	
efs	520	tcp	Extended File Name Server
router	520	udp	route routed
timed	525	udp	
tempo	526	tcp	
courier	530	tcp	

conference	531	tcp	
netnews	532	tcp	
netwall	533	udp	For emergency broadcasts
uucp	540	tcp	
klogin	543	tcp	Kerberos login
kshell	544	tcp	Kerberos remote shell
new-rwho	550	udp	
remotefs	556	tcp	
rmonitor	560	udp	
monitor	561	udp	
ldaps	636	tcp	LDAP over TLS/SSL
doom	666	tcp	Doom Id Software
doom	666	udp	Doom Id Software
kerberos-adm	749	tcp	Kerberos administration
kerberos-adm	749	udp	Kerberos administration
kerberos-iv	750	udp	Kerberos version IV
kpop	1109	tcp	Kerberos POP
phone	1167	udp	Conference calling
ms-sql-s	1433	tcp	Microsoft-SQL-Server
ms-sql-s	1433	udp	Microsoft-SQL-Server
ms-sql-m	1434	tcp	Microsoft-SQL-Monitor
ms-sql-m	1434	udp	Microsoft-SQL-Monitor
wins	1512	tcp	Microsoft Windows Internet Name Service
wins	1512	udp	Microsoft Windows Internet Name Service
ingreslock	1524	tcp	
l2tp	1701	udp	Layer Two Tunneling Protocol
pptp	1723	tcp	Point-to-point tunnelling protocol
radius	1812	udp	RADIUS authentication protocol

radacct	1813	udp	RADIUS accounting protocol
nfsd	2049	udp	NFS server
knetd	2053	tcp	Kerberos de-multiplexor
man	9535	tcp	Remote Man Server

Appendix E Figure Index

Appendix F Table Index

Federal Communication Commission Interference 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 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.

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

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

IMPORTANT NOTE:

FCC Radiation Exposure Statement:

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