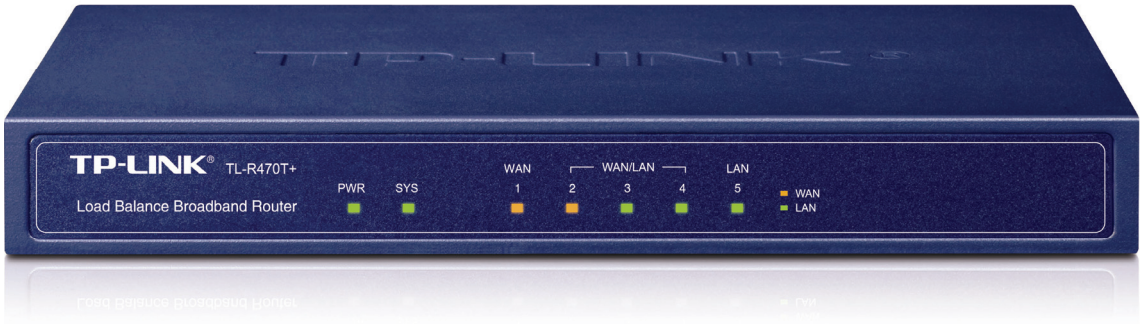
TP-LINK®

User Guide

TL-R470T+

Load Balance Broadband Router



Rev: 1.0.0
1910010409

COPYRIGHT & TRADEMARKS

Specifications are subject to change without notice. TP-LINK® is a registered trademark of TP-LINK TECHNOLOGIES CO., LTD. Other brands and product names are trademarks or registered trademarks of their respective holders.

http://www.tp-link.com

FCC STATEMENT

This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

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

1) This device may not cause harmful interference.
2) This device must accept any interference received, including interference that may cause undesired operation.

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

CE Mark Warning

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

Package Contents

The following items should be found in your box:

- One TL-R470T+ Load Balance Broadband Router
- One power cord for TL-R470T+ Load Balance Broadband Router
- One Resource CD for TL-R470T+ Load Balance Broadband Router, including:
  - This User Guide
  - Other Helpful Information

☞ **Note:**

1) The provided power cord may be different due to local power specifications.
2) Make sure that the package contains the above items. If any of the listed items are damaged or missing, please contact with your distributor.

Conventions

The router or TL-R470T+ mentioned in this guide stands for TL-R470T+ Load Balance Broadband Router without any explanation.

CONTENTS

Chapter 1. Introduction

Thank you for choosing TL-R470T+ Load Balance Broadband Router!

1.1 Overview of the Router

The TL-R470T+ Load Balance Broadband Router possesses excellent throughput and driving load capability, which consumedly meets the requirements from Internet cafe and small office with volumes of users, making a more expedite communication. The superior performance will bring you full-new experience of a non-bottle-neck network.

TL-R470T+ Load Balance Broadband Router provides three adjustable WAN/LAN ports which can work as WAN port or LAN port. By the factory defaults, TL-R470T+ is set to work in the dual WAN ports mode with port 1 and port 2 as WAN ports, while port 3~5 are LAN ports. The Router features fully automatically load balance policy, no need for any manually work, it works with backup and load balancing functions. The connection will furbish when one line is broken down, while the streaming will part automatically.

TL-R470T+ makes plenty of applications become a reality. It can be used for constructing intranet FTP, WEB, and Mail server, etc. Inaccessibly, it features network game ports opened, MSN audio conversation and special application setting, providing much more additional value to your network.

Featuring firewall and VPN Pass-through, the TL-R470T+ Load Balance Broadband Router resists most common Internet attacks and ensures secure data connectivity and transmission over the Internet.

TL-R470T+ Load Balance Broadband Router is easy-to-manage. Quick Setup is supported and friendly help messages are provided for every step. So you can configure it quickly and share Internet access, files and fun comfortably.

1.2 Features

- Complies with IEEE 802.3, 802.3u , 802.3x standards
- 1 fixed WAN port (port 1), 1 fixed LAN port (port 5), and 3 adjustable WAN/LAN ports (By defaults, port 2 is WAN port, port 3~4 are LAN ports), backup connections automatically for each other
- Supports Port Bandwidth Control, Port Mirror for LAN ports
- Supports IP address-based QoS
- Built-in NAT and DHCP server supporting static IP address distributing
- Supports Virtual Server, Port Triggering, and DMZ host
- Built-in firewall supporting IP address filtering, Domain Name filtering, and MAC address filtering
- Supports connecting/disconnecting Internet at a specified time of day
- Supports access control, allowing parents and network administrators to establish restricted access policies based on the time of day for children or staff

- Supports TCP/IP, PPPoE, DHCP, ICMP, NAT, SNTP
- Supports UPnP, Dynamic DNS, Static Routing, VPN pass-through
- Supports Traffic Statistics
- Supports IP & MAC Binding, Switch Setting, and Session Limit
- Supports ICMP-FLOOD, UDP-FLOOD, TCP-SYN-FLOOD filter
- Ignores Ping packets from WAN or LAN ports
- Supports firmware upgrade
- Supports Remote and Web management

1.3 Conventions

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

You can set the parameters according to your demand.

Chapter 2. Hardware installation

2.1 Panel Layout

2.1.1 The Front Panel

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

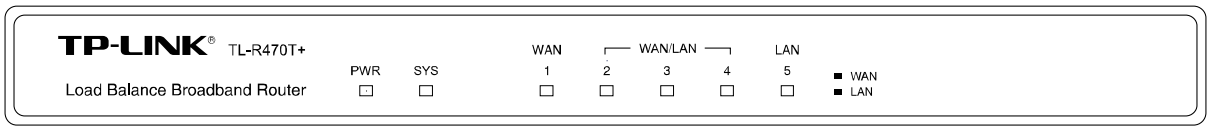


Figure 2-1

LED Descriptions:

Name	Status	Indication
PWR	Not lit	The router is power off.
	Lit up (Green)	The router is power on.
SYS	Not lit	The router has a hardware error.
	Lit up (Green)	The router has a hardware error.
	Flashing (Green)	The router works properly.
WAN/LAN	Not lit	There is no device linked to the corresponding port.
	Lit up (Green/Yellow)	There is a device linked to the corresponding port but no activity. (Green light indicates the corresponding port is working as a LAN port, and yellow indicates WAN port.)
	Flashing (Green/Yellow)	There is an active device linked to the corresponding port. (Green light indicates the corresponding port is working as a LAN port, and yellow indicates WAN port.)

2.1.2 The Rear Panel

The rear panel contains the following features. (Viewed from left to right)

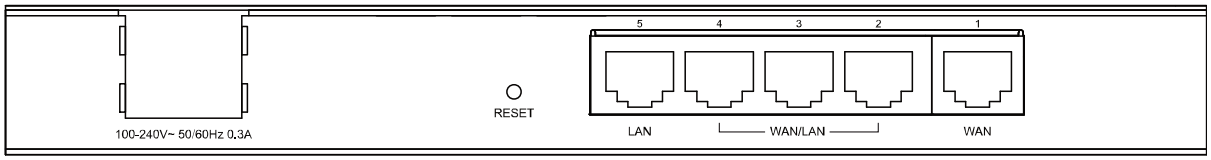


Figure 2-2

- **AC power receptacle:** Connect the female of the power cord head here, and the male head to the AC power outlet.
- **RESET:** Use the button to restore the router to the factory defaults.

There are two ways to reset the router:

Method one: Use the **Factory Defaults** function on **System Tools** -> **Factory Defaults** page in the router's Web-based Utility.

Method two: With the router powered on, use a pin to press and hold the Reset button (about 5 seconds) until the SYS LED lights up and flashes. And then release the button and wait the router to reboot to its factory default settings.

☞ **Note:**

Ensure the router is powered on before it restarts completely.

- **LAN:** A 10/100Mbps RJ45 port for connecting the router to the local PCs. Port 5 is a fixed LAN port.
- **WAN/LAN:** Three RJ45 ports which can be adjusted to be WAN or LAN ports. By defaults, port 2 is WAN port, while port 3 and port 4 are LAN ports.
- **WAN:** A RJ45 port for connecting the router to a cable, DSL modem or Ethernet. Port 1 is a fixed WAN port.

☞ **Note:**

The previous configurations will be cleared if the number of WAN/LAN ports is changed.

2.2 System Requirements

- Broadband Internet Access Service (DSL/Cable/Ethernet)
- One DSL/Cable modem that has an RJ45 connector (It's not necessary if you connect the router to Ethernet)
- Each PC on the LAN needs a working Ethernet Adapter and an Ethernet cable with RJ45 connectors
- Web browser, such as Microsoft Internet Explorer 5.0 or later, Netscape Navigator 6.0 or later

2.3 Installation Environment Requirements

- Not in direct sunlight or near a heater or heating vent
- Not cluttered or crowded. There should be at least 2 inches (5 cm) of clear space on all sides of the router
- Well ventilated (especially if it is in a closet)
- Operating temperature: 0℃~40℃ (32℉~104℉)
- Operating Humidity: 10%~90%RH, Non-condensing

☞ **Note:**

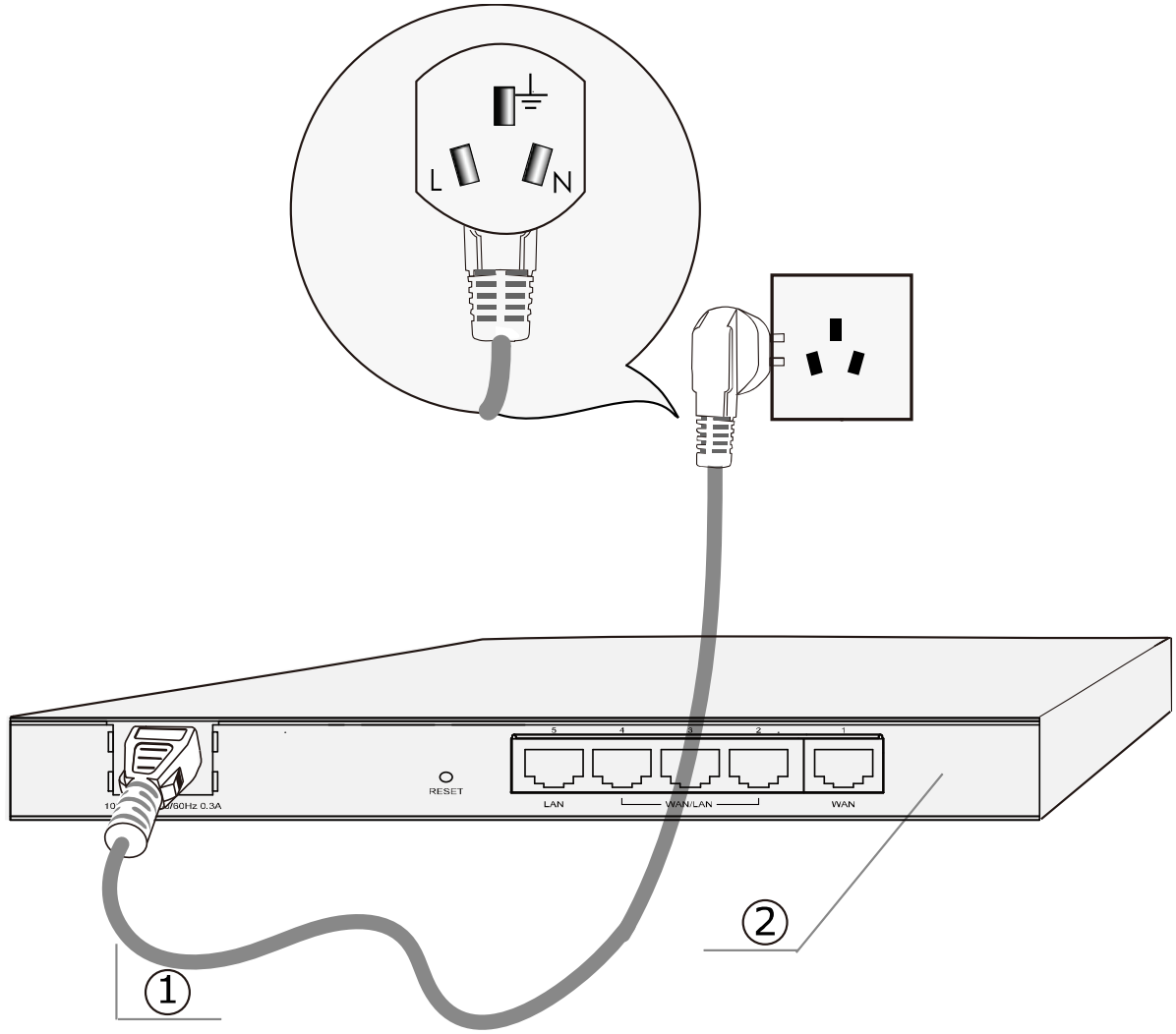
1) Do not use this product near water, for example, in a wet basement or near a swimming pool.
2) Avoid using this product during an electrical storm. There may be a remote risk of electric shock from lightning.

2.4 Connect to Ground

Connecting the router to ground is to quickly release the lightning over-voltage and over-current of the router, which is also a necessary measure to protect the body from electric shock. The following will instruct you to connect the Router to the Ground.

Connecting to the Ground via the power supply

The Router can be grounded via the PE（Protecting Earth）cable of the AC power supply as shown in the following figure.



① AC Power Cord (with PE cable) ② Router (Rear Panel)

Note:

If you intend to connect the Router to the ground via the PE（Protecting Earth）cable of AC power cord, please make sure the PE（Protecting Earth）cable in the electrical outlet is well grounded in advance.

2.5 Connecting the Router

Before you install the router, you should connect your PC to the Internet through your broadband service successfully. If there is any problem, please contact with your ISP for help. After that, please install the router according to the following steps. Don't forget to pull out the power plug and keep your hands dry.

1. Power off your PC(s), Cable/DSL modem, and the router.
2. Connect the PC(s) and all Switches/Hubs on your LAN to the LAN Ports on the router, shown in figure 2-3.

3. Connect the DSL/Cable modem to the WAN port on the router, shown in figure 2-3.
4. Connect the AC power adapter to the AC power socket on the router, and the other end into an electrical outlet. The router will start to work automatically.
5. Power on your PC(s) and Cable/DSL modem.

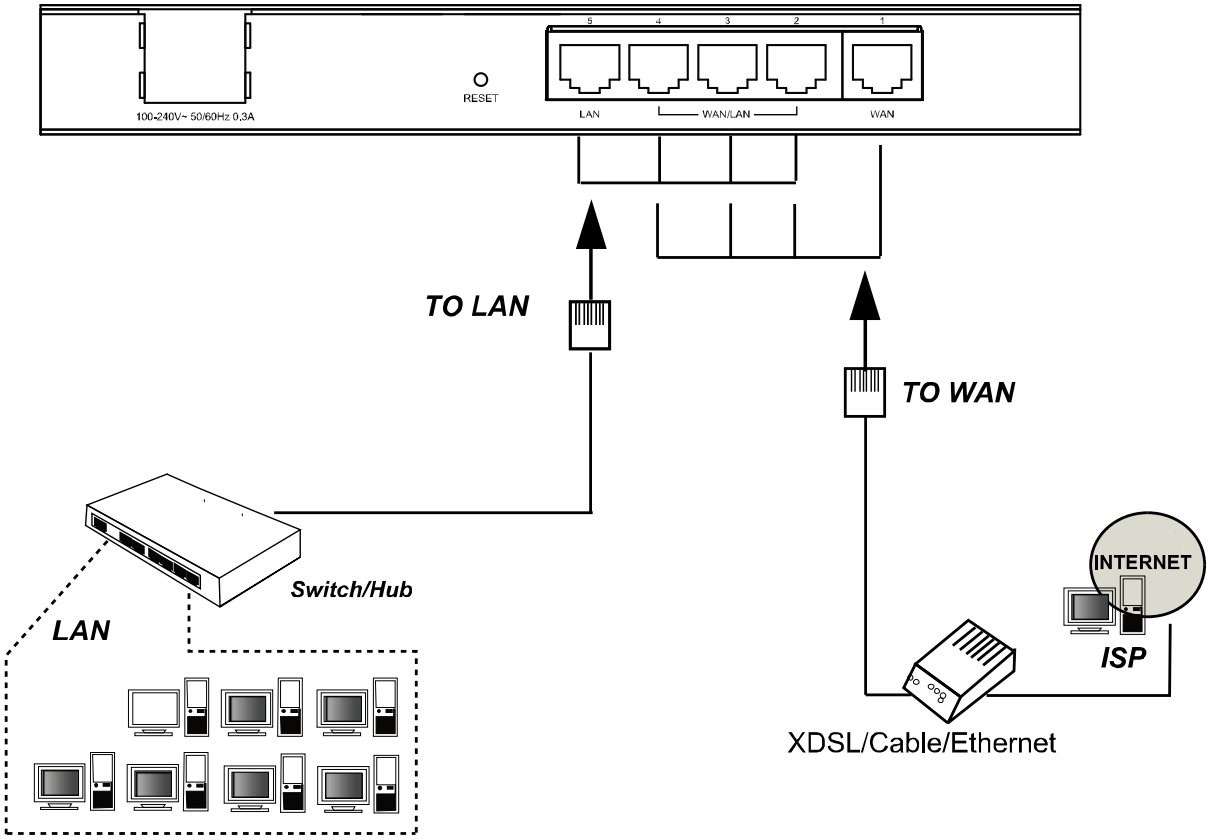


Figure 2-3

Chapter 3. Quick Installation Guide

After connecting the TL-R470T+ router into your network, you should configure it. This chapter describes how to configure the basic functions of your TL-R470T+ Load Balance Broadband Router. These procedures only take you a few minutes. You can access the Internet via the router immediately after it has been successfully configured.

3.1 Configure PC

Step 1: Click the **Start** menu on your desktop, right click **My Network Places**, and then select **Properties** (shown in Figure 3-1).

Figure 3-1

Step 2: In the next screen, right click **Local Area Connection** (LAN), and then select **Properties**.

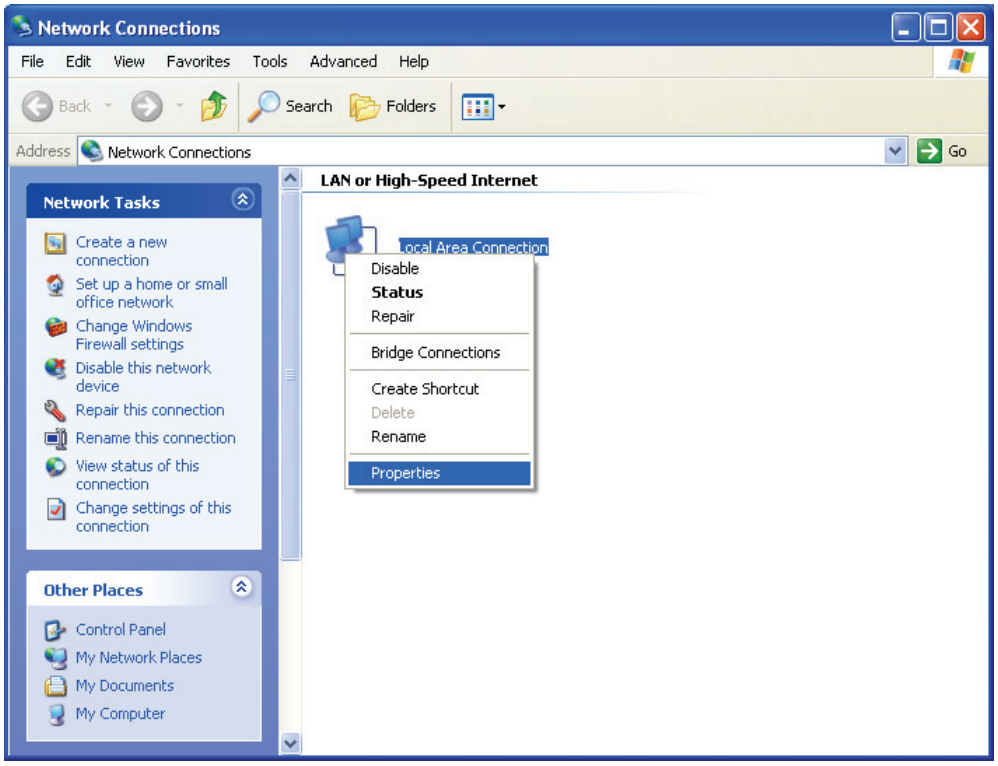


Figure 3-2

Step 3: In the next screen, select **General** tab, highlight Internet Protocol (TCP/IP), and then click the **Properties** button.

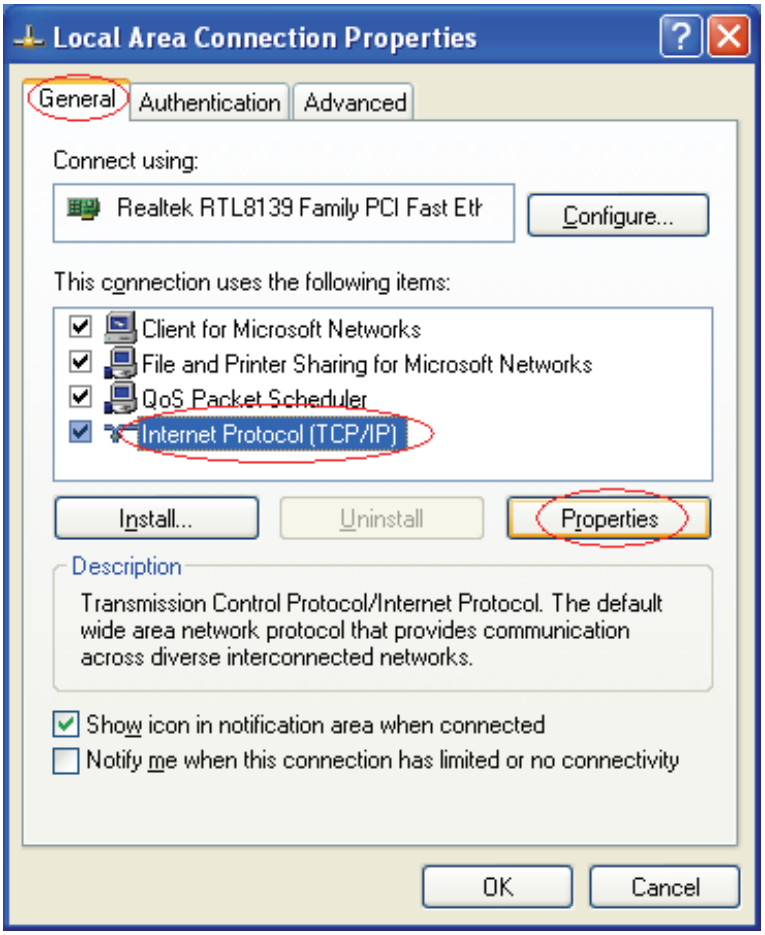


Figure 3-3

Step 4: Configure the IP address as shown in Figure 3-4. After that, click **OK**.

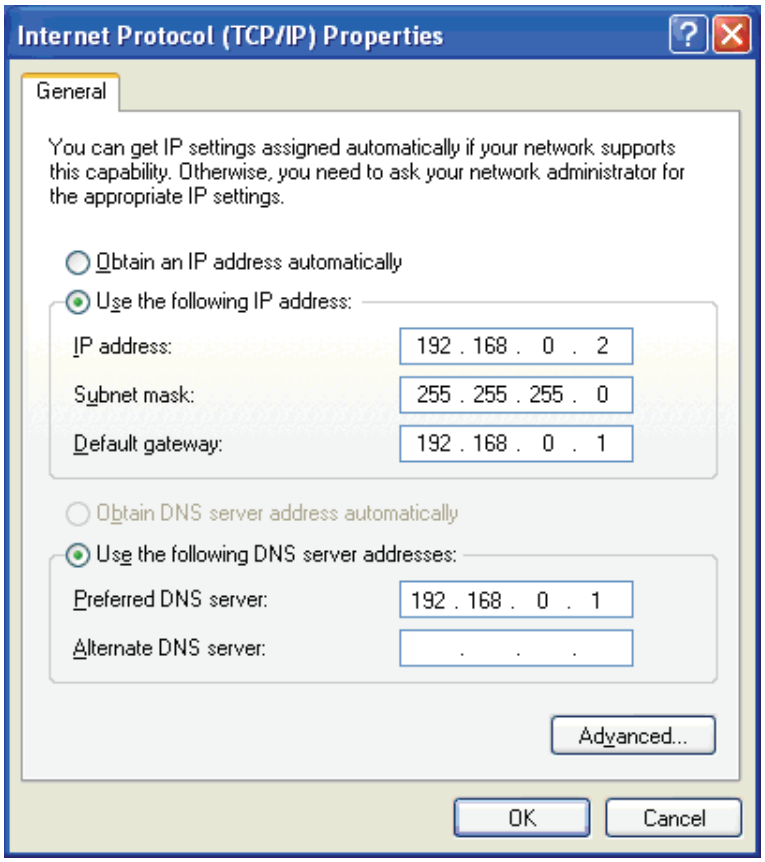


Figure 3-4

☞ **Note:**

You can configure the PC to get an IP address automatically, select "**Obtain an IP address automatically**" and "**Obtain DNS server address automatically**" in the screen above. For Windows 98 OS or earlier, the PC and router may need to be restarted.

Now, you can run the Ping command in the command prompt to verify the network connection. Please click the **Start** menu on your desktop, select **run** tab, type **cmd** in the field, and then type *ping 192.168.0.1* on the next screen, and then press **Enter**.

If the result displayed is similar to the screen below, the connection between your PC and the Router has been established.

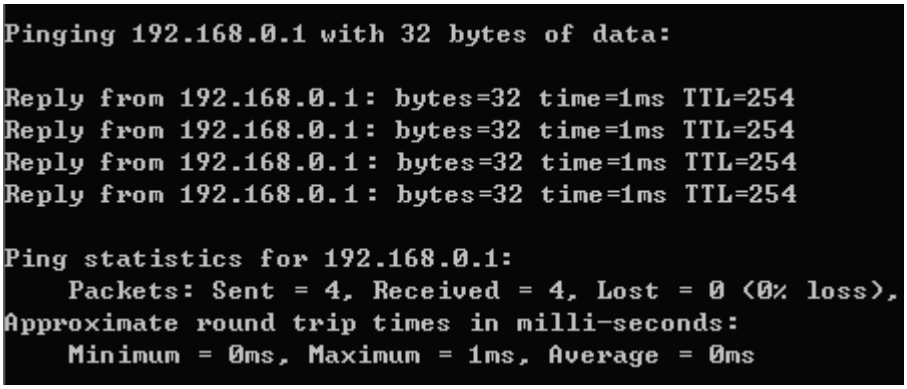


Figure 3-5

If the result displayed is similar to the screen shown below, it means that your PC has not connected to the Router.

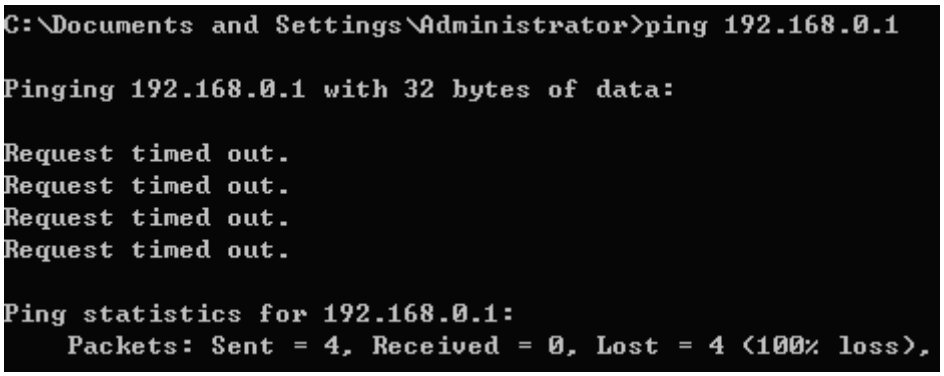


Figure 3-6

You can check it follow the steps below:

☞ **Note:**

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

The LEDs of LAN port which you link to the device and the LEDs on your PC's adapter should be lit.

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

If the Router's IP address is 192.168.0.1, your PC's IP address must be within the range of 192.168.0.2 ~ 192.168.0.254, the gateway must be 192.168.0.1.

3.2 Login

Once your host PC is properly configured, please proceed as follows to use the Web-based Utility: Start your web browser and type the private IP address of the Router in the URL field: **http://192.168.0.1**.

After that, you will see the screen shown below, enter the default User Name **admin** and the default Password **admin**, and then click **OK** to access to the **Quick Setup** screen. You can follow the steps below to complete the Quick Setup.

Figure 3-7

Note:

If the above screen (Figure 3-7) does not prompt, it means that your web-browser may be set to a proxy. Choose **Tools menu→Internet Options→Connections→LAN Settings**, in the screen that appears, cancel the **Using Proxy checkbox**, and click **OK** to finish it.

Step 1: Select the **Quick Setup** tab on the left of the main menu and the "Quick Setup" screen will appear. Click the **Next** button.

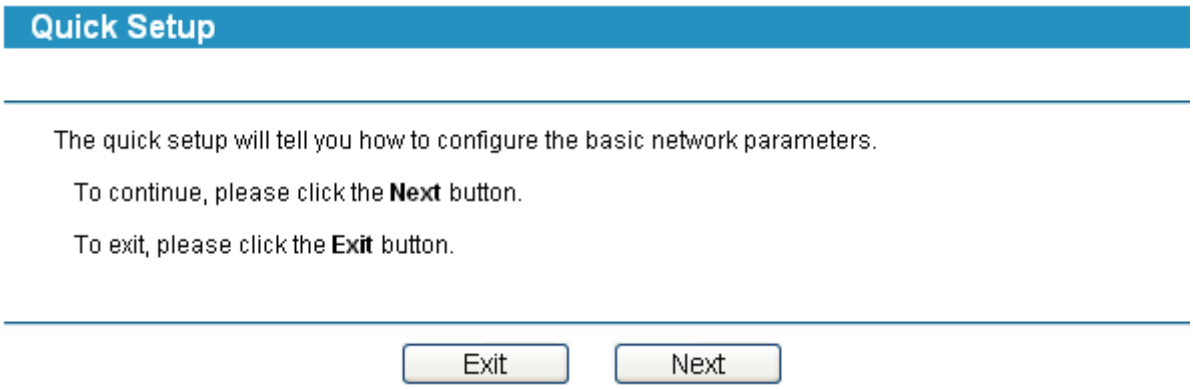


Figure 3-8

Step 2: Select the connection type to connect to the ISP and then click the **Next** button.

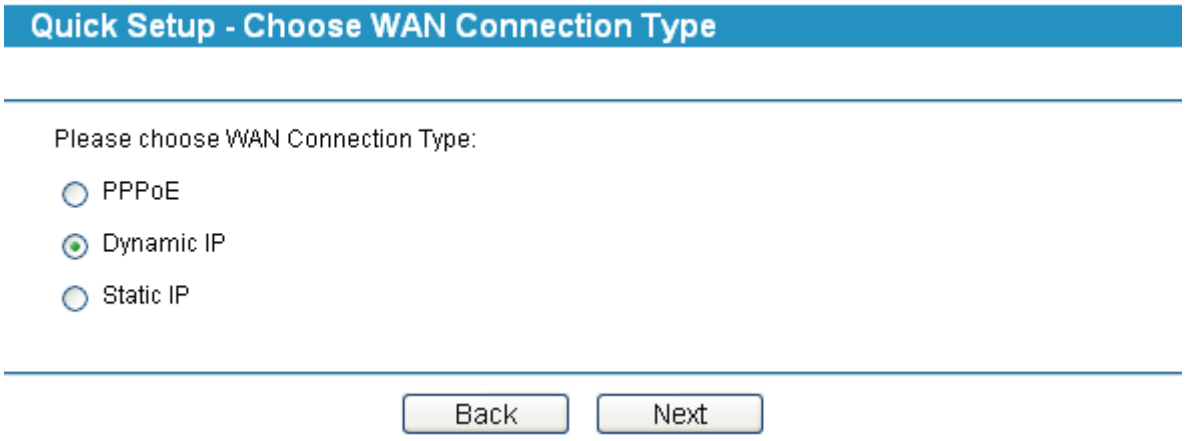


Figure 3-9

Note:

Three popular ways to connect to Internet are provided in Quick Setup. Please select one compatible with your ISP. If you are given another way not listed here, refer to **Network→ WAN** for detailed list.

Step 3: If you choose **PPPoE**, you will see the screen as shown in Figure 3-10. Enter the **Username** and **Password** provided by your ISP. These fields are case sensitive. If you have difficulty with this process, please contact your ISP.

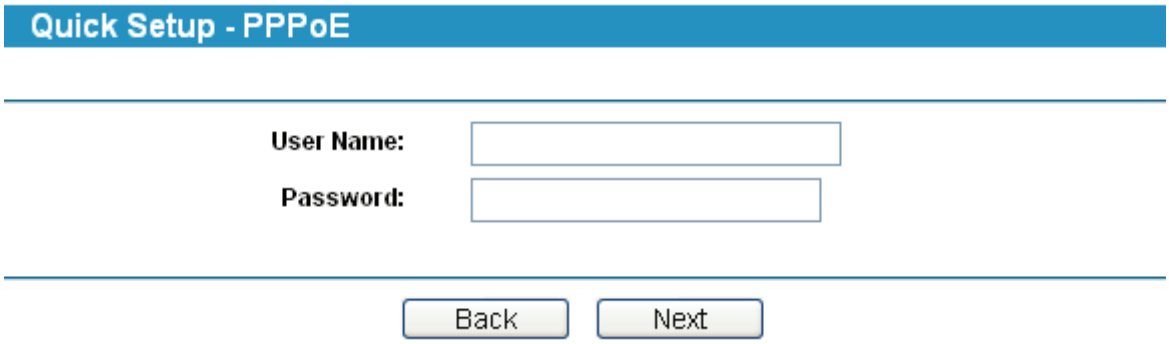


Figure 3-10

Step 4: If you choose **Dynamic IP** in Figure 3-9, the router will automatically receive the IP parameters from your ISP without needing to enter any parameters.

Step 5: If you Choose **Static IP**, you should enter the detailed IP information in Figure 3-11. Click the **Next** button

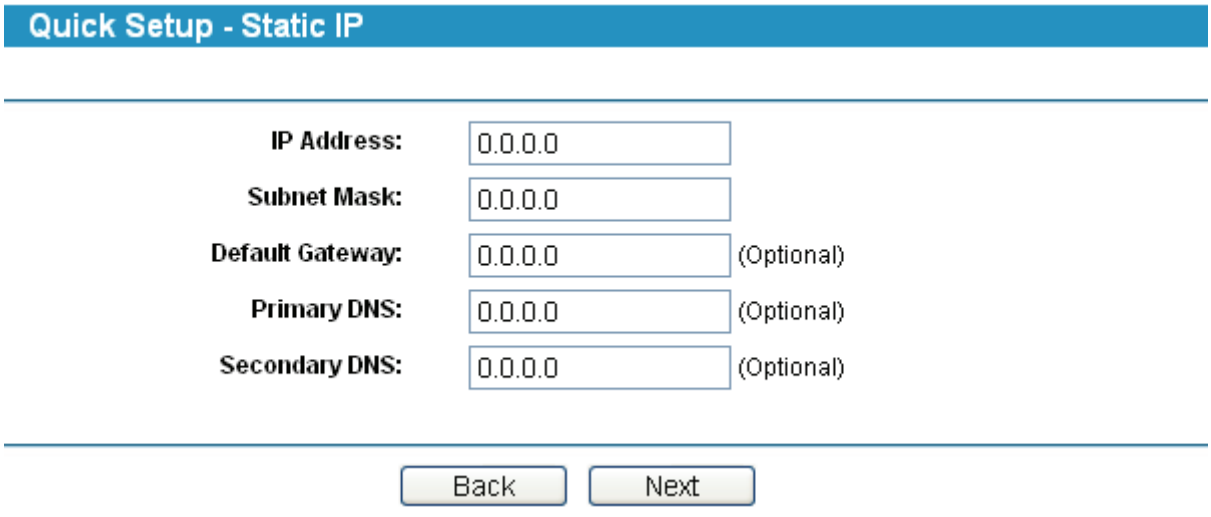


Figure 3-11

Step 6: After that, you will see the next screen. Click **Finish** to complete the quick installation.

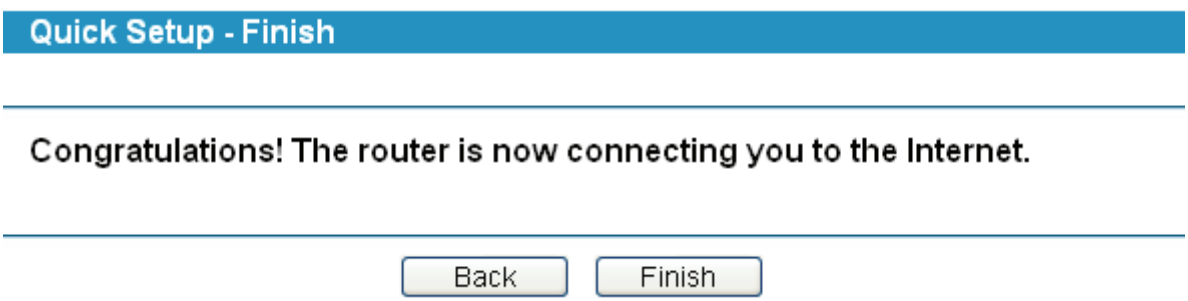


Figure 3-12

Chapter 4. Configuring the Router

This User Guide recommends using the “Quick Installation Guide” for first-time installation. For advanced users, if you want to know more about this device and make use of its functions adequately, you need to read this chapter and configure advanced settings though the Web-based Utility.

After your successful login, you can configure and manage the router. There are main menus on the left of the Web-based Utility. Submenus will be available after you click one of the main menus. On the center of the web-based Utility, you can configure the function. Besides this, you can refer to the help on the right of the Web-based Utility. To apply any settings you have altered on the page, please click the **Save** button.

4.1 Status

Choose “**Status**” menu, you can view the router's current status and configuration as shown in Figure 4-1. All information is read-only.

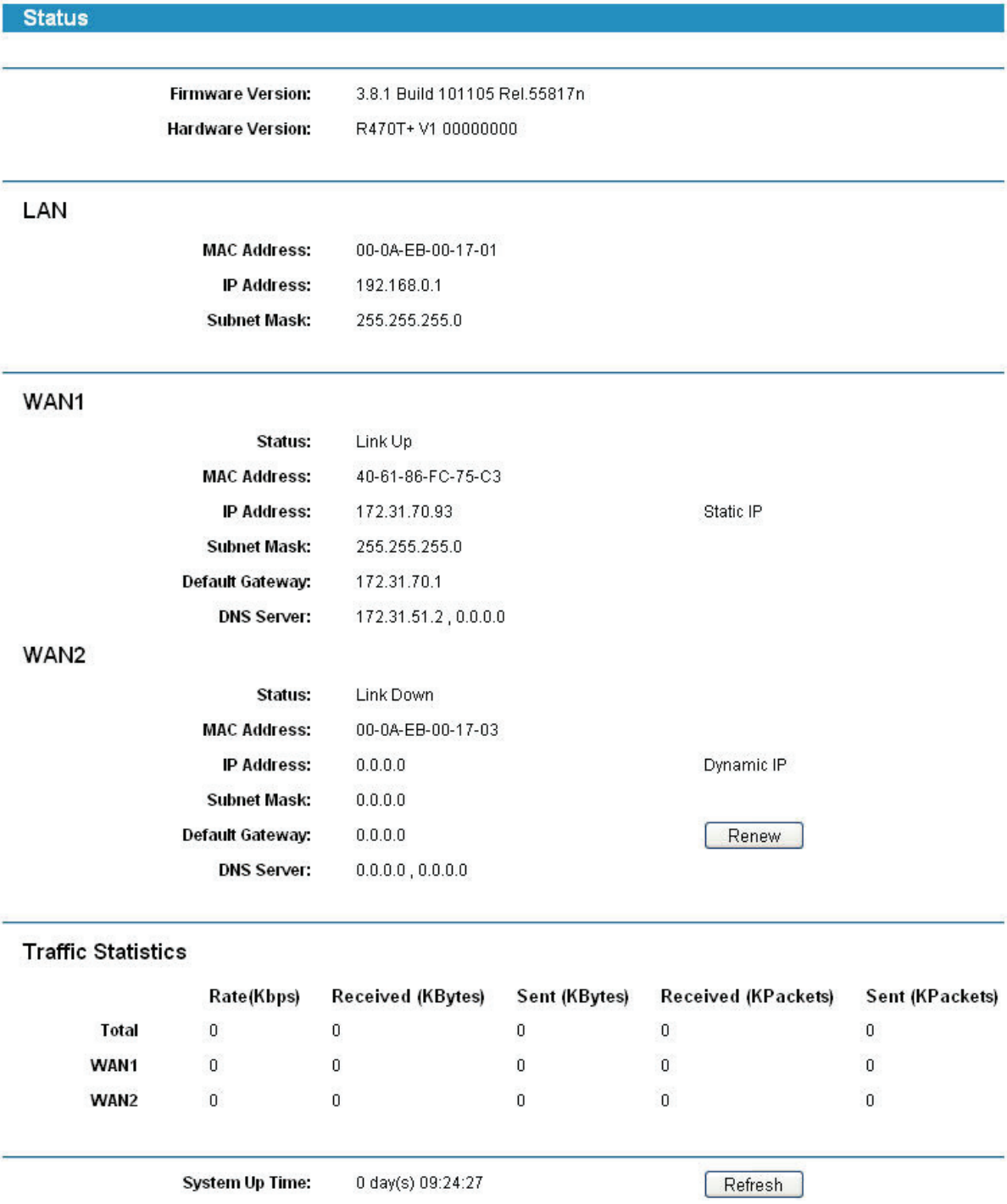


Figure 4-1

- **LAN -** This field displays the current information for the LAN, including the "MAC address", "IP address" and "Subnet Mask".
- **WAN -** This field displays the parameters applied to the WAN ports of the router, including "MAC address", "IP address", "Subnet Mask", "Default Gateway" and so on. The number of WAN ports can be configured on the "**Network→WAN Number**" page. Dual WAN ports mode is set by default.

Note:

If PPPoE/L2TP/PPTP is chosen as the WAN connection type, the **Disconnect** button will be shown here while you are accessing the Internet. You can also cut the connection by clicking the

button. If you have not connected to the Internet, a **Connect** button will be shown, and you can then establish the connection by clicking the button.

- **Traffic Statistics:** This field displays the traffic statistics of WAN ports.
- **System Up Time:** This field displays the time of the router running from the time it is powered on or is reset.

4.2 Quick Setup

Please refer to chapter 3"Quick Installation Guide".

4.3 Network

Choose menu "**Network**", the next submenus are shown below. The submenus "**Network Service Detection**", "**Load Balance**" and "**Balance Policy**" will be hidden when the Router is set to single WAN port mode for these features are only provided in the mode of multiple WAN ports.

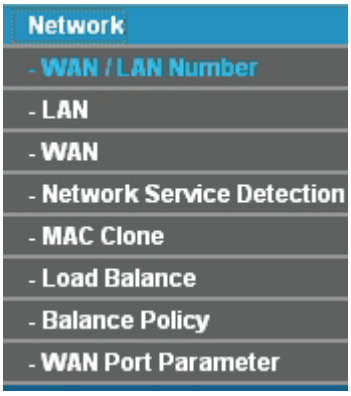


Figure 4-2

Click any of them, and you will be able to configure the corresponding function. The detailed explanations for each submenu are provided below.

4.3.1 WAN/LAN Number

Choose menu "**Network→WAN/LAN Number**", you can set the number of WAN ports on the screen below.

The Router supports multiple WAN ports. The modes of single WAN port, dual WAN ports, ternary WAN ports and quad WAN ports are provided.

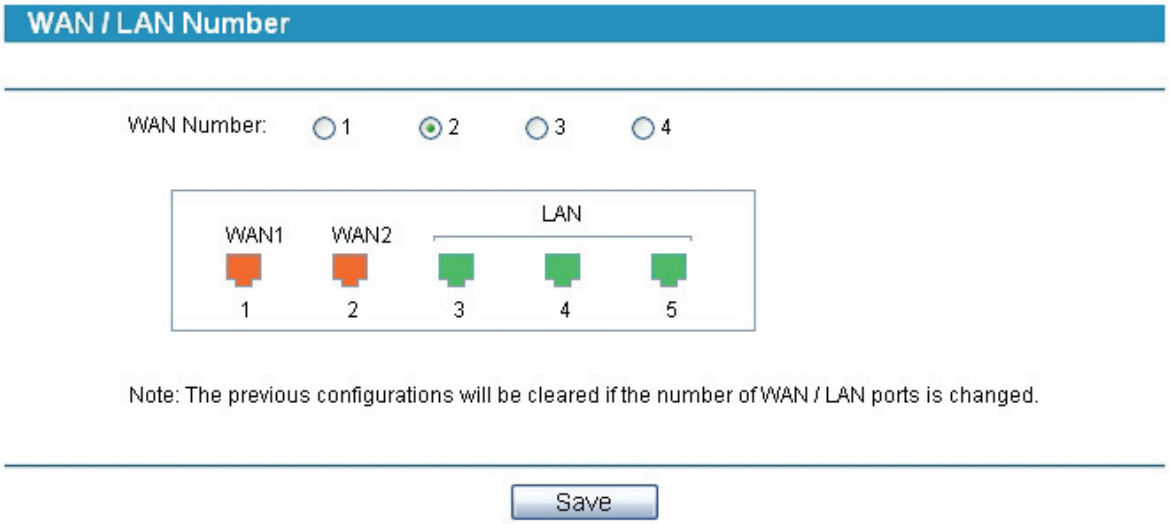


Figure 4-3

- **WAN Number –** Here allows you to select the total number of WAN ports at your need. And the Router will adjust the physical ports accordingly, which can be illustrated on the following port sketch.

Note:

1) By default, TL-R470T+ is set to work at the mode of dual WAN ports.
2) The previous configurations will be cleared if the number of WAN/LAN ports is changed.

4.3.2 LAN

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

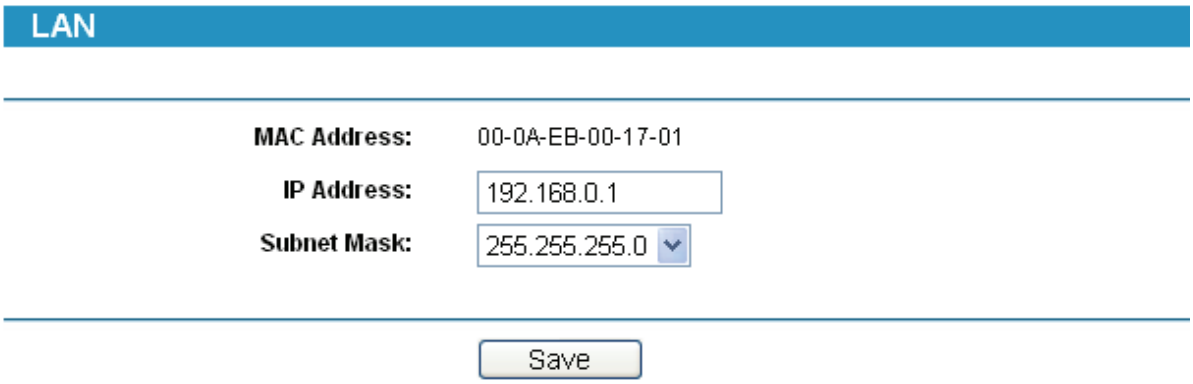


Figure 4-4

- **MAC Address -** This field displays the physical address of the LAN. The value can't be changed.
- **IP Address -** Enter the IP address for the LAN of the Router, the formal is in dotted-decimal notation (the factory default value is 192.168.0.1).
- **Subnet Mask -** Enter the subnet mask for the LAN of the Router, this address code determines the size of the network. Normally use 255.255.255.0 as the subnet mask.

☞ **Note:**

1) If you change the IP address of the LAN, you must use the new IP address to login to the router.
2) If the new LAN IP Address you set is not in the same subnet, the IP Address pools in the DHCP sever will not take effect, until they are re-configured. Besides this, the Virtual Server and DMZ Host may change accordingly at the same time; you'd better re-configure it as well.

4.3.3 WAN

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

The Router provides six connection types for WAN to connect to the Internet, they are "Dynamic IP", "Static IP" , "PPPoE", "BigPondCable" , "L2TP" and "PPTP". For configuring the WAN, you should select the connection type firstly according your needs.

1. Dynamic IP

If you aren't given any login parameters and IP information, please select **Dynamic IP** (shown in Figure 4-5), then the router will automatically get IP parameters from your ISP. Click the **Renew** button to renew the IP parameters from your ISP. Click the **Release** button to release the IP parameters.

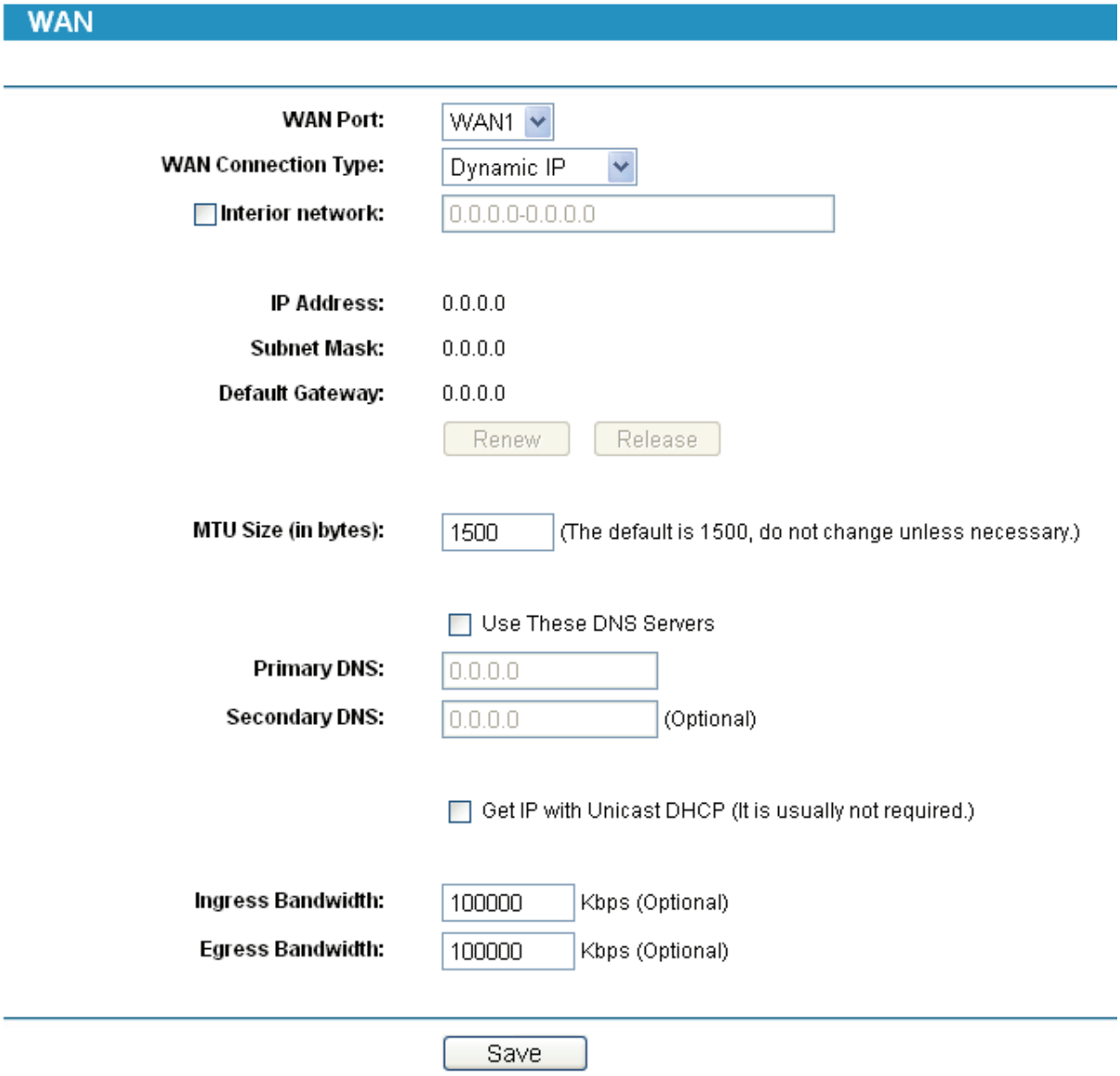


Figure 4-5

- **WAN Port:** Here allows you to select the WAN port to configure.
- **Interior network:** When the WAN is connecting with a LAN, you can select the option, and enter the LAN IP addresses in the field, then the WAN port will only transmit the traffic whose destination IP address are contained in the field.
- **MTU Size -** The normal MTU (Maximum Transmission Unit) value for most Ethernet networks is 1500 Bytes. For some ISPs you need to reduce the MTU. But this is rarely required, and should not be done unless you are sure it is necessary for your ISP connection.
- **Primary DNS & Secondary DNS -** If your ISP gives you one or two DNS addresses, select **Use These DNS Servers** and enter the primary and secondary addresses into the correct fields. Otherwise, the DNS servers will be assigned dynamically from ISP.

Note:

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

- **Get IP with Unicast DHCP:** A few ISPs' DHCP servers do not support the broadcast applications. If you can not get the IP address normally, you can choose this option. (You don't need select this option generally).
- **Ingress Bandwidth:** Enter the bandwidth for ingress traffic.
- **Egress Bandwidth:** Enter the bandwidth for egress traffic.

2. Static IP

If you are given a fixed IP (static IP), please select **Static IP** (shown in Figure 4-6), and then fixed IP parameters specified by your ISP.

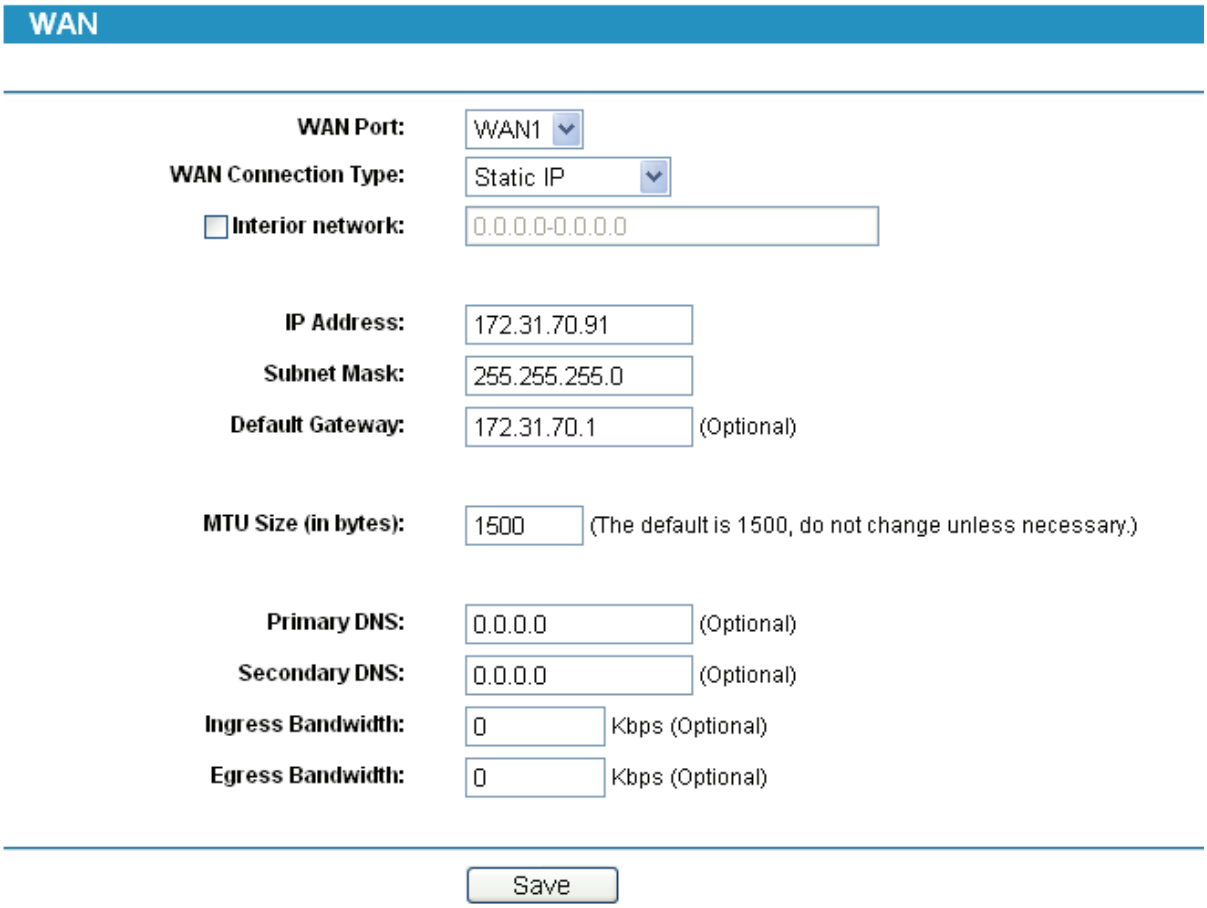


Figure 4-6

- **WAN Port:** Here allows you to select the WAN port to configure.
- **IP Address -** Enter the IP address in dotted-decimal notation provided by your ISP.
- **Subnet Mask -** Enter the subnet Mask in dotted-decimal notation provided by your ISP, usually is 255.255.255.0.
- **Default Gateway -** Enter the gateway IP address in dotted-decimal notation provided by your ISP (Optional).
- **MTU Size -** The normal MTU (Maximum Transmission Unit) value for most Ethernet networks is 1500 Bytes. For some ISPs you may need to modify the MTU. But this is rarely required, and should not be done unless you are sure it is necessary for your ISP connection.

- **Primary DNS -** Type the DNS address in dotted-decimal notation provided by your ISP (Optional).
- **Secondary DNS -** Type another DNS address in dotted-decimal notation provided by your ISP if provided (Optional).
- **Ingress Bandwidth:** Enter the bandwidth for ingress traffic.
- **Egress Bandwidth:** Enter the bandwidth for egress traffic.

3. PPPoE

If you are given a user name and a password, please select **PPPoE** (shown in Figure 4-7). If you are not sure which connection type you use currently, please contact your ISP to obtain the correct information.

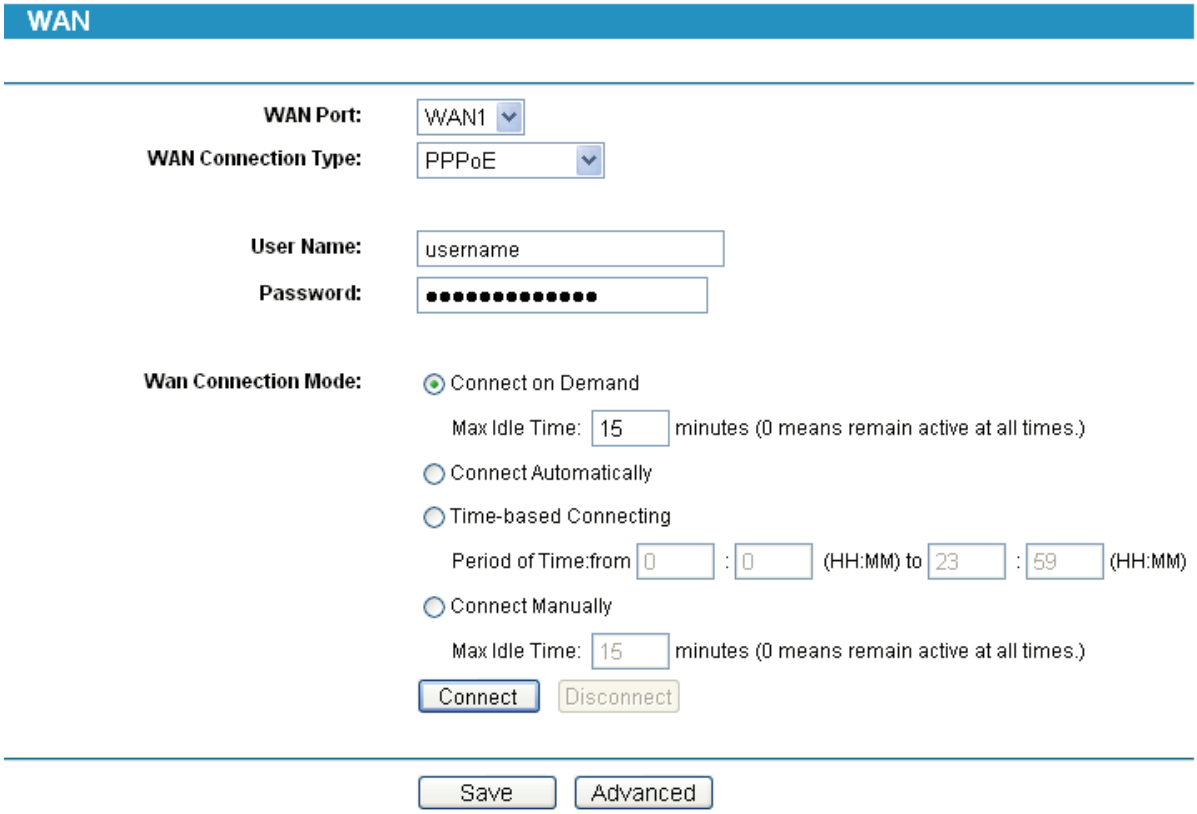


Figure 4-7

- **WAN Port:** Here allows you to select the WAN port to configure.
- **User Name/Password -** Enter the User Name and Password provided by your ISP. These fields are case-sensitive.
- **Connect on Demand -** You can configure the router to disconnect your Internet connection after a specified period of inactivity (**Max Idle Time**). If your Internet connection has been terminated due to inactivity, **Connect on Demand** enables the router to automatically re-establish your connection as soon as you attempt to access the Internet again. If you wish to activate **Connect on Demand**, check the radio button and click **Save** to apply.

☞ **Note:**

1) If you want your Internet connection to remain active at all times, enter 0 in the **Max Idle Time** field. Otherwise, enter the number of minutes you want to have elapsed before your Internet connection terminates.
2) Sometimes the connection can not be disconnected although you specify a time to Max Idle Time. This is because there may still be active applications in the background, which may cause fee accounted by your ISP.

- **Connect Automatically -** Connect automatically after the router is disconnected. To use this option, click the radio button.
- **Time-based Connecting -** You can configure the router to make it connect or disconnect based on time. Enter the start time in HH:MM for connecting and end time in HH:MM for disconnecting in the **Period of Time** fields.

Note:

Only you have set the system time on **System Tools→Time** screen, will the **Time-based Connecting** function take effect.

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

Note:

1) If you want your Internet connection to remain active at all times, enter 0 in the **Max Idle Time** field. Otherwise, enter the number in minutes that you wish to have the Internet connecting last unless a new link is requested.
2) Sometimes the connection cannot be disconnected although you specify a time to Max Idle Time. This is because there may still be active applications in the background, which may cause fee accounted by your ISP.

Click the **Advanced** button to set up the advanced option as shown in Figure 4-8.

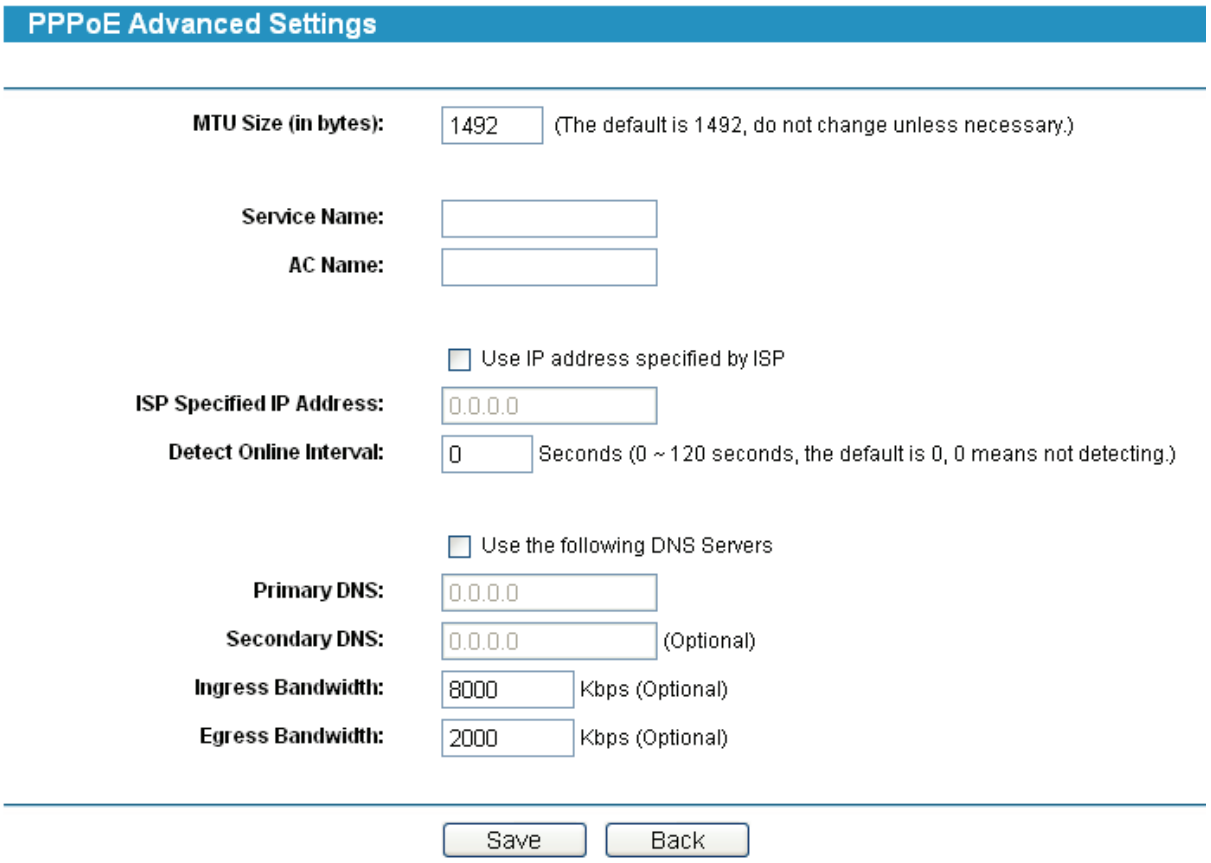


Figure 4-8

- **MTU Size-** The default MTU size is 1492 bytes, which is usually fine. For some ISPs, you need modify the MTU. This should not be done unless you are sure it is necessary for your ISP.
- **Service Name/AC Name -** The service name and AC (Access Concentrator) name should not be configured unless you are sure it is necessary for your ISP.
- **ISP Specified IP Address -** If you know that your ISP does not automatically transmit your IP address to the router during login, select **Use IP Address specified by ISP** and enter the IP address in dotted-decimal notation, which your ISP provided.
- **Detect Online Interval -** The default value is 0, you can input the value between 0 and 120. The router will detect Access Concentrator online at every interval between the times. If the value is 0, it means the Router does not detect.
- **Primary DNS & Secondary DNS -** If you know that your ISP does not automatically transmit DNS addresses to the router during login, select **Use the following DNS servers** and enter the address in dotted-decimal notation of your ISP's primary DNS server. If a secondary DNS server address is available, enter it as well.
- **Ingress Bandwidth:** Enter the bandwidth for download traffic.
- **Egress Bandwidth:** Enter the bandwidth for upload traffic.

4. BigPondCable

If your ISP provides BigPond Cable (or Heart Beat Signal) connection, please select **BigPond Cable** option.

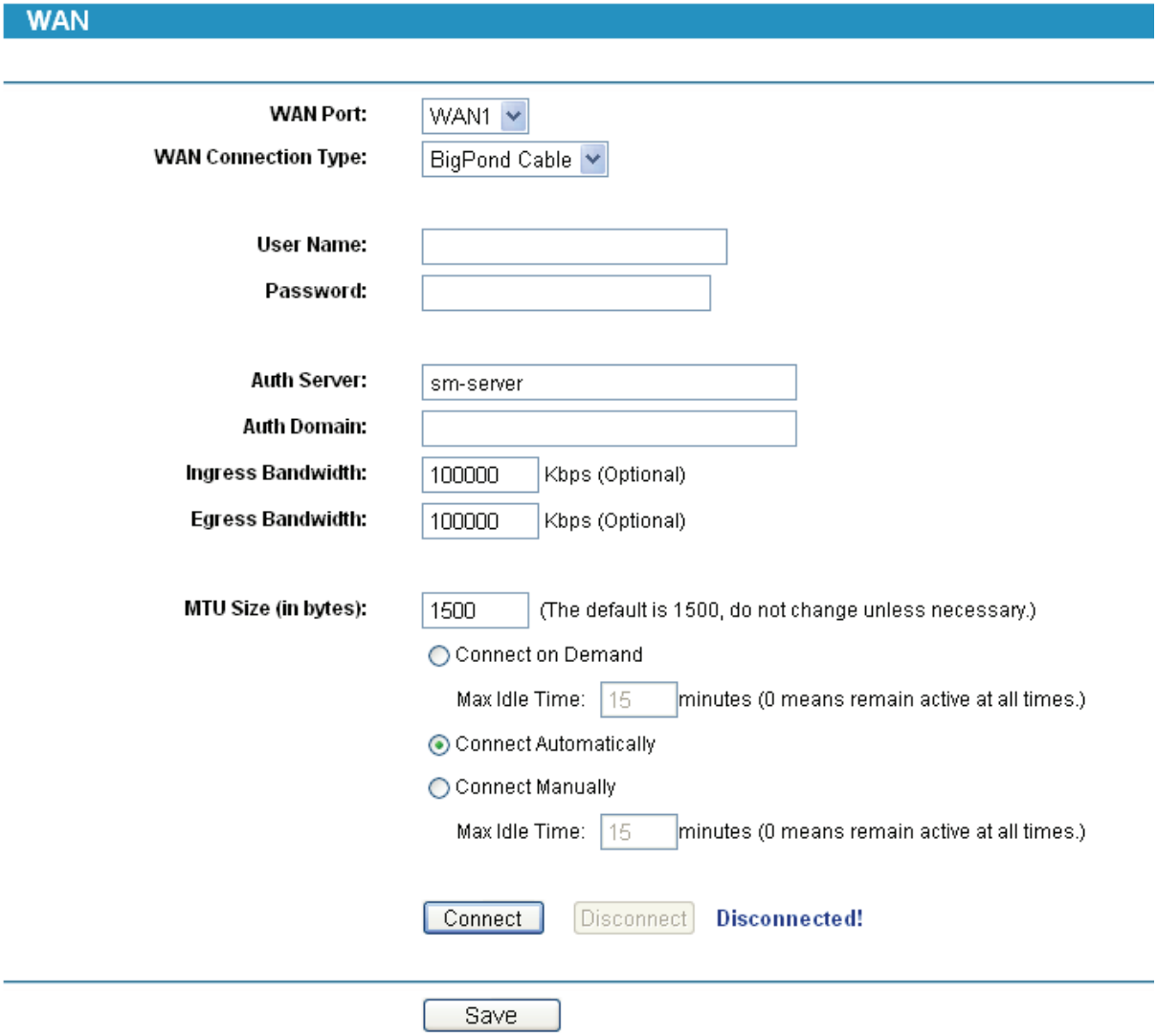


Figure 4-9

- **WAN Port:** Here allows you to select the WAN port to configure.
- **User Name/Password** - Enter the User Name and Password provided by your ISP. These fields are case-sensitive.
- **Auth Server** - Enter the authenticating server IP address or host name.
- **Auth Domain** - Type in the domain suffix server name based on your location.
- **MTU Size** - The normal MTU (Maximum Transmit Unit) value for most Ethernet networks is 1500 bytes. For some ISPs, you may need to modify the MTU. But this is rarely required, and should not be done unless you are sure it is necessary for your ISP connection.
- **Connect on Demand** - You can configure the router to disconnect your Internet connection after a specified period of the Internet connectivity (**Max Idle Time**). If your Internet connection has been terminated due to inactivity, **Connect on Demand** enables the router to automatically re-establish your connection as soon as you attempt to access the Internet again. If you wish to activate **Connect on Demand**, click the radio button. If you want your Internet connection to remain active at all times, enter **0** in the **Max Idle Time** field. Otherwise, enter the number of minutes you want to have elapsed before your Internet connection terminates.

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

☞ **Note:**

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

5. L2TP

If your ISP provides L2TP connection, please select **L2TP** option.

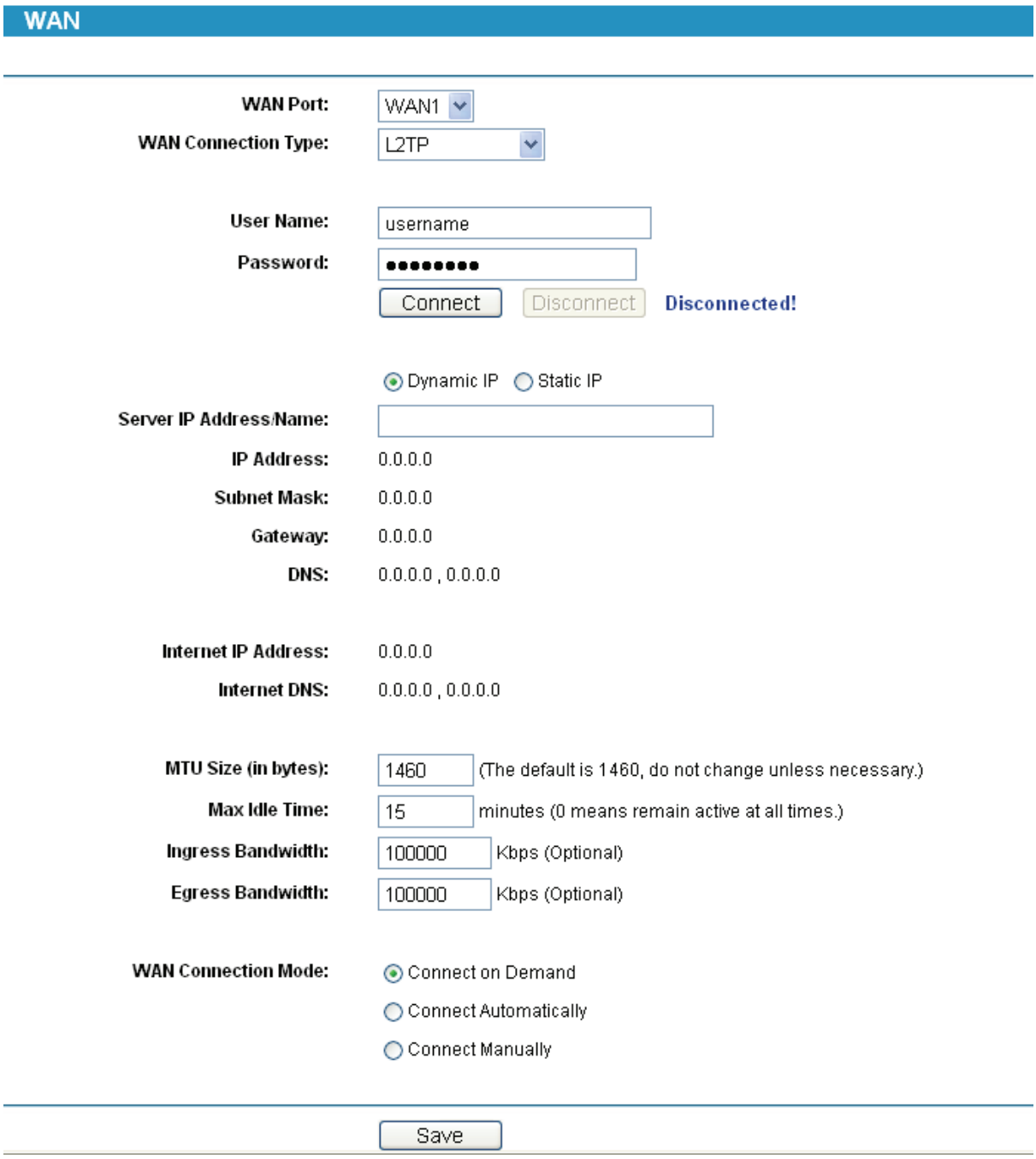


Figure 4-10

- **WAN Port:** Here allows you to select the WAN port to configure.
- **User Name/Password** - Enter the User Name and Password provided by your ISP. These fields are case-sensitive.
- **Connect on Demand** - You can configure the router to disconnect your Internet connection after a specified period of the Internet connectivity (**Max Idle Time**). If your Internet connection has been terminated due to inactivity, **Connect on Demand** enables the router to automatically re-establish your connection as soon as you attempt to access the Internet again. If you wish to activate **Connect on Demand**, click the radio button. If you want your Internet connection to remain active at all times, enter **0** in the **Max Idle Time** field. Otherwise, enter the number of minutes you want to have elapsed before your Internet connection terminates.

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

☞ **Note:**

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

6. PPTP

If your ISP provides PPTP connection, please select **PPTP** option.

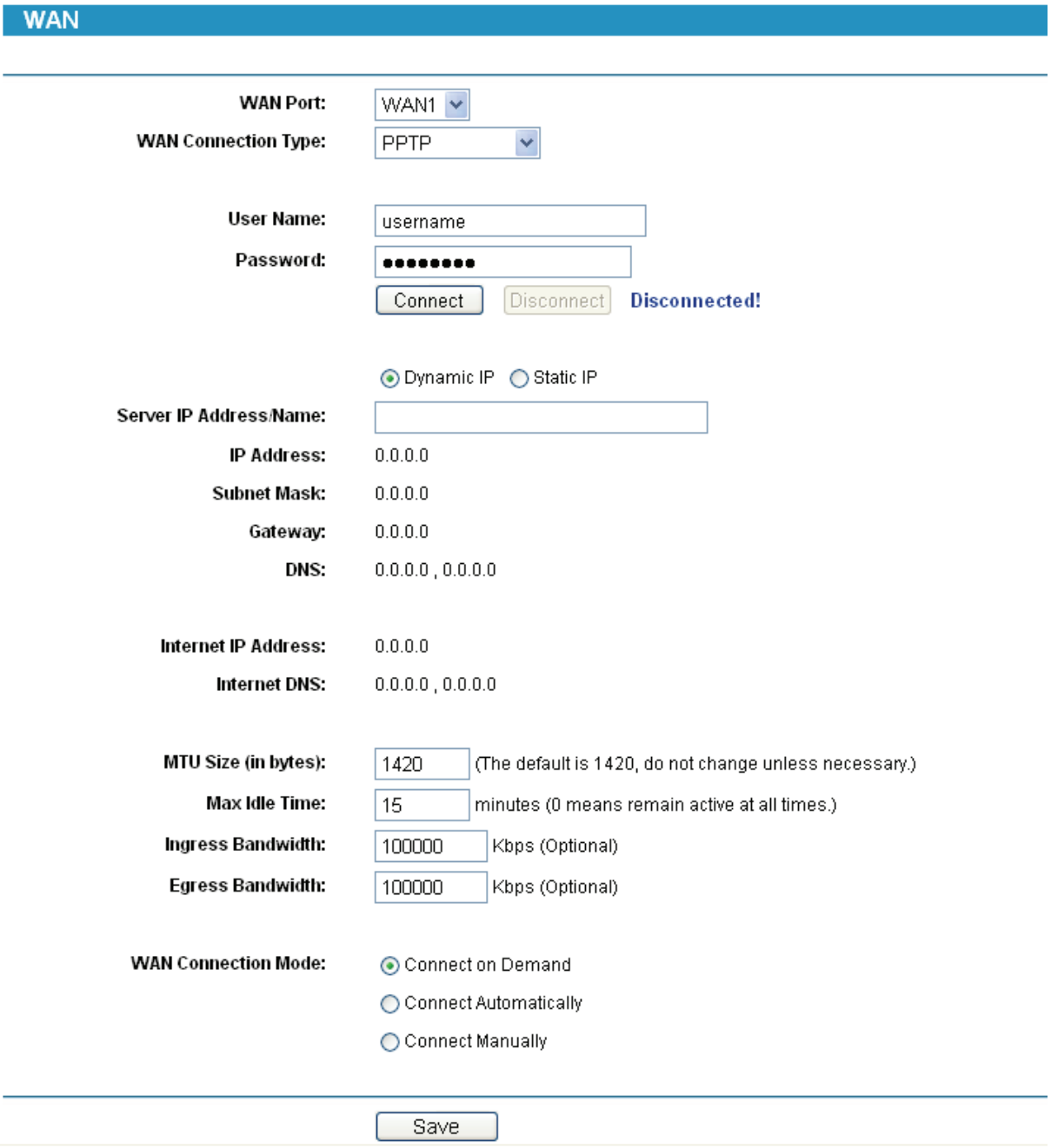


Figure 4-11

- **WAN Port:** Here allows you to select the WAN port to configure.
- **User Name/Password** - Enter the User Name and Password provided by your ISP. These fields are case-sensitive.
- **Connect on Demand** - You can configure the router to disconnect your Internet connection after a specified period of the Internet connectivity (**Max Idle Time**). If your Internet connection has been terminated due to inactivity, **Connect on Demand** enables the router to automatically re-establish your connection as soon as you attempt to access the Internet again. If you wish to activate **Connect on Demand**, click the radio button. If you want your Internet connection to remain active at all times, enter **0** in the **Max Idle Time** field. Otherwise, enter the number of minutes you want to have elapsed before your Internet connection terminates.

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

Note:

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

4.3.4 Network Service Detection

Choose menu "**Network→Network service detection**", you can Use WAN Network Service Detection feature on next screen, this router can detect whether the WAN port is online or not.

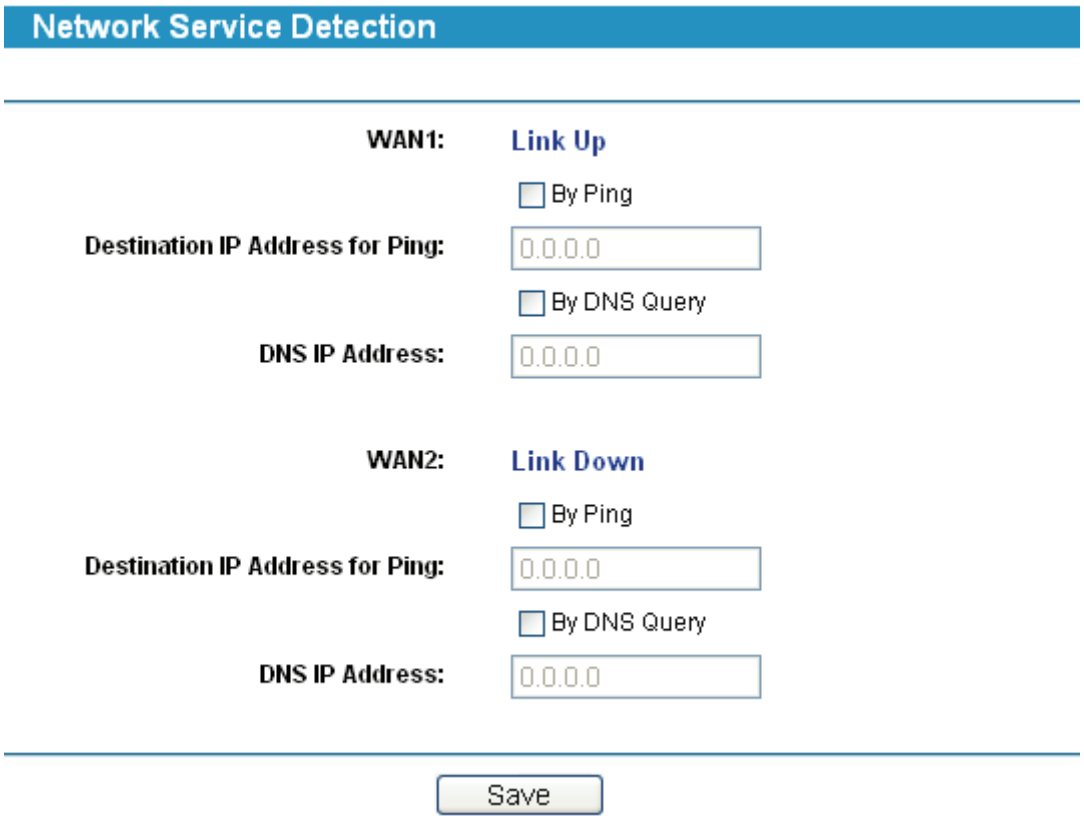


Figure 4-12

- **By Ping -** Detect whether Internet connection is online or not by Ping.
- **Destination IP Address for Ping** - Enter the correct IP address that really existed on the WAN network. For example: 202.96.134.188.
- **By DNS Query** - Detect whether Internet connection is online or not by sending query packet to DNS Server.

- **DNS Server IP Address** - Enter the correct DNS IP address that really existed on the WAN network. For example: 202.96.134.133.

4.3.5 MAC Clone

Choose menu "**Network→MAC Clone**", you can configure the MAC address of the WAN on the screen below (shown in Figure 4-13).

Some ISPs require that you register the MAC address of your adapter, which is connected to your cable, DSL modem or Ethernet during installation. You do not generally need to change anything here.

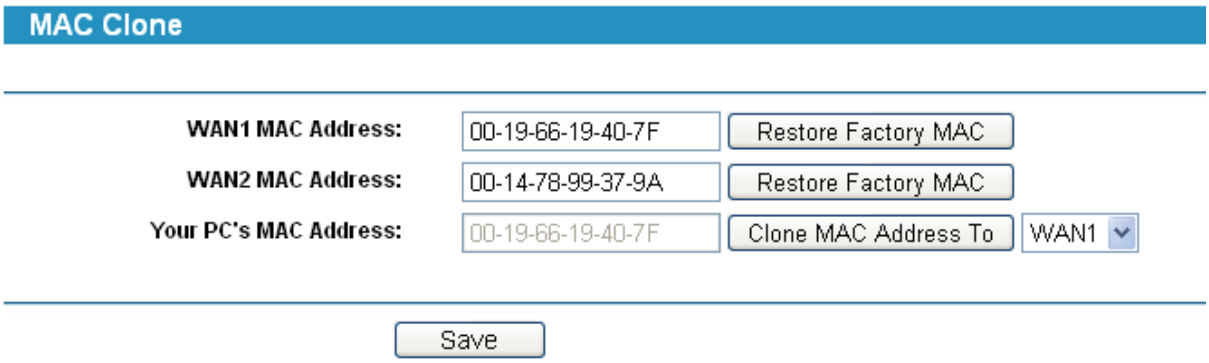


Figure 4-13

- **WAN MAC Address (1~2) -** This field displays the current MAC address of the WAN port, which is used for the WAN port. If your ISP requires that you register the MAC address, please enter the correct MAC address into this field. The format for the MAC address is XX-XX-XX-XX-XX-XX (for example: 00-0A-EB- E6-B9-49).
- **Your PC's MAC Address -** This field displays the MAC address of the PC that is managing the router. If the MAC address is required, you can click the **Clone MAC Address** button and this MAC address will fill in the "WAN MAC Address" field.

Note:

1) Click **Restore Factory MAC** to restore the MAC address of WAN port to the factory default value.
2) Only the PC(s) on your LAN can use the **MAC Address Clone** feature.
3) After you finish the configuration, click the **Save** button, and the router will prompt you to reboot.

4.3.6 Load Balance

Choose menu "**Network→Load Balance**", the following screen will display. In which, you can determine how the traffic load is shared by the WAN ports, and get the information about the router's traffic status of WAN ports on **Current Statistics** and **Overall Statistics** tables.

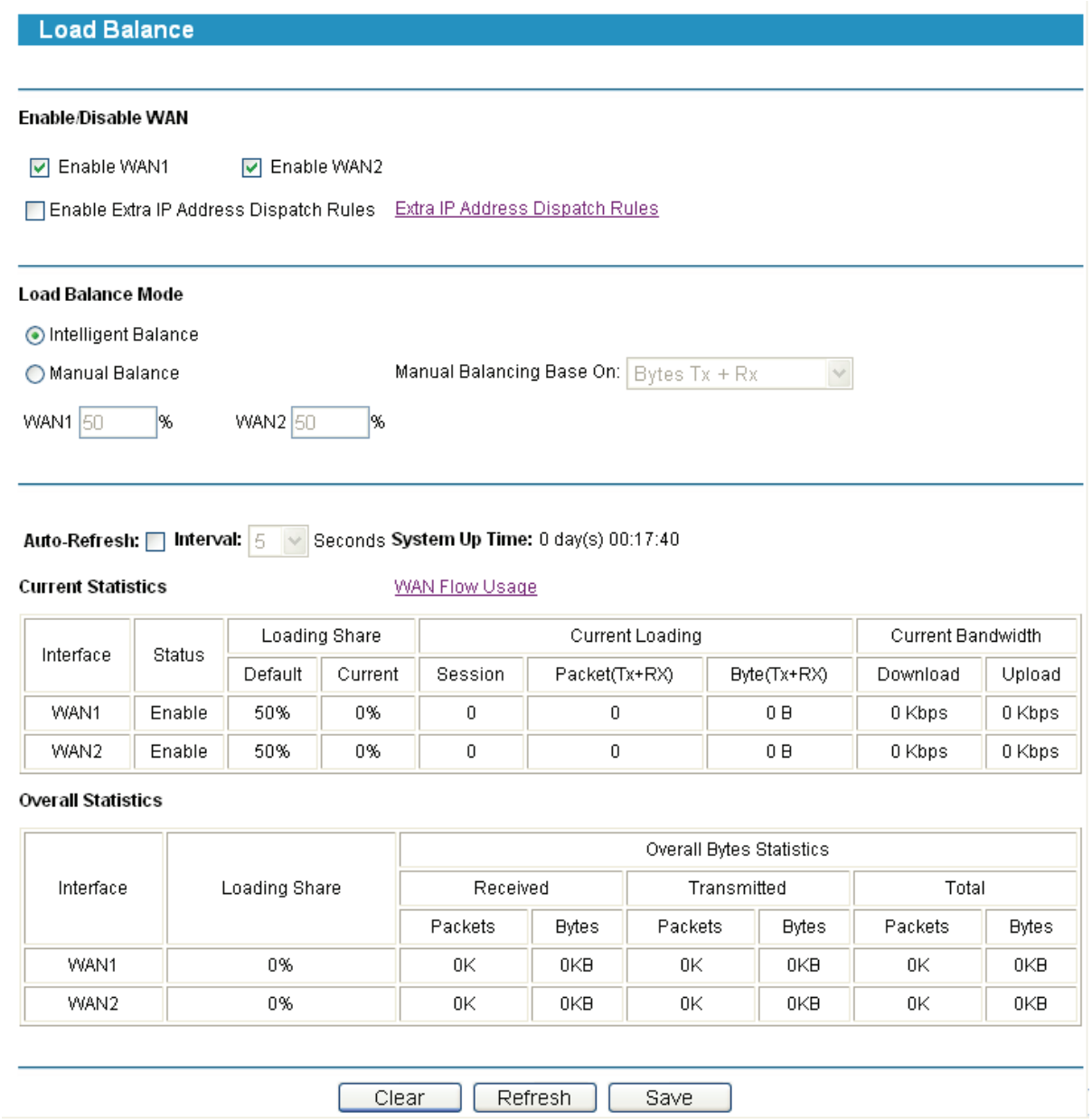


Figure 4-14

- **Enable/Disable WAN** - Click the check box of WAN which you want to enable the Load Balance.
- **Enable Extra IP Address Dispatch Rules** - Click the check box of **Enable Extra IP Address Dispatch Rules** to apply the extra IP address dispatch rules. If you want to add an extra IP address dispatch rule, please click **Extra IP Address Dispatch Rules** (For the detailed instructions, please refer to **How to set an extra IP address dispatch rule?**)

Note:

The Extra IP Address Dispatch Rules are prior to Load Balance. If the datagram comply with the settings in Extra IP Address Dispatch Rules, they will be forwarded by the WAN port specified in the Extra IP Address Dispatch Rules table.

- **Intelligent Balance** - In **Intelligent Balance** mode, the traffic will be transmitted to the WAN port according to idle ingress bandwidth on every WAN.

Note:

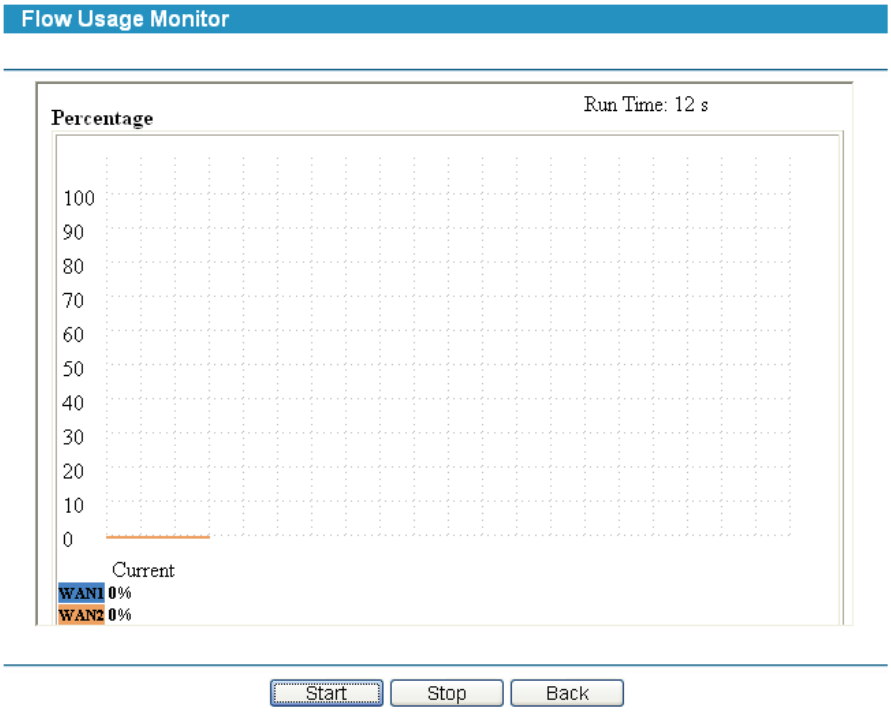
The **Intelligent Balance** mode will only be effective until the **Ingress Bandwidth** of the WAN port has been set in "**Network→WAN**" screen.

- **Manual Balance** - In **Manual Balance** mode, the traffic will be transmitted to the WAN port according to manual Balance type and percentage of traffic load on each WAN port.
- **Manual Balancing Base On** - Here allows you to specify the manual Balance type among the following three.
  - **Bytes Tx + Rx** - Bytes transmitted and received through the WAN port.
  - **Packets Tx + Rx** - Packets transmitted and received through the WAN port.
  - **Sessions Established** - Sessions built on the WAN port.
- **WAN1/WAN2** – Here allows you to specify the percentage of traffic load for each WAN port in Manual Balance mode.

Note:

In **Manual Balance** mode, it is recommended to set the percentage of traffic load for each WAN port according to the WAN port's bandwidth. For example, if the bandwidth of WAN1 is 5M, while the bandwidth of WAN2 is 2M, for best performance, you'd better set the percentage of traffic load for WAN1 higher than that for WAN2.

- **Auto-Refresh** - The default value is 5. Select a value in the range of 5 to 60 seconds in the pull-down list. The interval value indicates the refresh interval of the traffic statistics.
- **System Up Time** - The length of the time since the router was last powered on or reset.
- **WAN Flow Usage** - Click **WAN Flow Usage**, you can enter the page which displays the flow usage info of each WAN port, as the following figure shown. Here, you can click the **Start** button to start flow usage monitor, or click the **Stop** button to stop flow usage monitor.



- **Run Time** - How long this function is running.

- **Current** - Current flow usage of each WAN port.

➢ **Current Statistics/Overall Statistics-** Here displays the information about the router's traffic status of WAN ports.

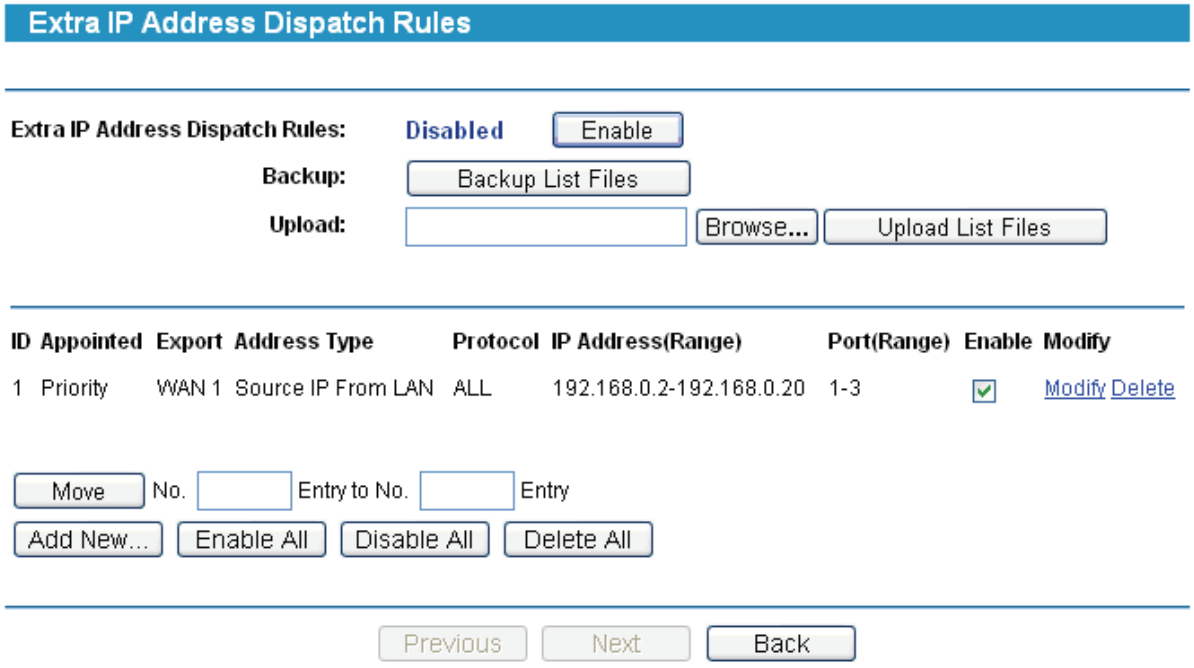
When finished, click the **Save** button to apply your settings.

Click the **Refresh** button to get the latest status of the router.

Click the **Clear** button to clear the **Current Statistics** and **Overall Statistics** of the router.

How to set an extra IP address dispatch rule?

Click **Extra IP Address Dispatch Rules** in Figure 4-14, and you will enter the following screen. On this screen, you can specify priority channels basing on the source or destination IP addresses, distributing flexibly Internet resource and services of different ISPs. For example, you can specify some packets prior forwarding from WAN port 1, which depends on specified source or destination IP addresses.



➢ **Extra IP Address Dispatch Rules** - The status of the extra IP address dispatch rules. "Enabled" means the rules are effective.

➢ **Backup** - Here allows you to backup the existed rule entries to your local computer by clicking **Backup List Files** button.

➢ **Upload** – Here allows you to upload the rule entries from your computer. Click the **Browse** button to locate the files and click the **Upload List Files** button to start the process.

Click the **Move** button to change the sequence of rule entry.

Click the **Add New...** button to add a new scheduler rule.

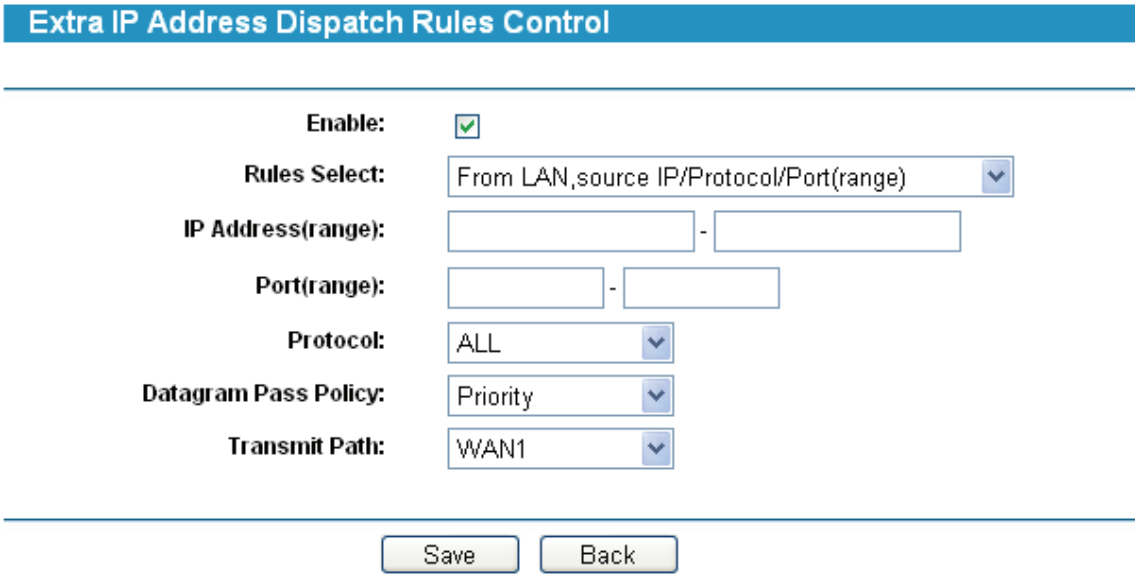
Click the **Enable All** button to enable all scheduler rules.

Click the **Disable All** button to disable all scheduler rules.

Click the **Delete All** button to delete all scheduler rules.

To add a dispatch rule:

Step 1: Click **Add New…** button, you will see the following screen.



- **Enable** - Make the scheduler rule enabled.
- **Rules Select** - The direction rule of the datagram get through the WAN port.
- **IP Address (range)** - The LAN IP or IP range which the extra IP address dispatch rules take effect on. Such as 192.168.0.100 or 192.168.0.115~192.168.0.120.
- **Port (range)** - The port or port range which the extra IP address dispatch rules take effect on. It should be between 1 ~ 65534.
- **Protocol** - The protocol which the extra IP address dispatch rules take effect on, either **TCP, UDP**, or **All** (all protocols supported by the router).
- **Datagram Pass Policy** - To decide how the datagram pass the WAN, **Priority** or **Only**. If **Priority** is selected, the datagram will be preferentially forwarded by the specified WAN port path. If **Only** is selected, the datagram will only be able to pass through the specified WAN port.
- **Transmit Path** - The WAN port name which the transmission uses.

Step 2: Select the **Rules Select, Protocol, Datagram Pass Policy** and **Transmit Path**, and enter the **IP address** and **Port** range.

Step 3: Click **Save** to apply your setting.

4.3.7 Balance Policy

Choose menu "**Network→Balance Policy"**, you can configure the scheduler policy of the WAN. The policy mainly depends on 2 solutions: IP address pair priority and Application priority. So, we create 2 tables for these solutions. They are Existed-IP-Pair-Table and Existed-Application-Table. It is recommended to keep the default settings if you are not sure whether you can set them better.

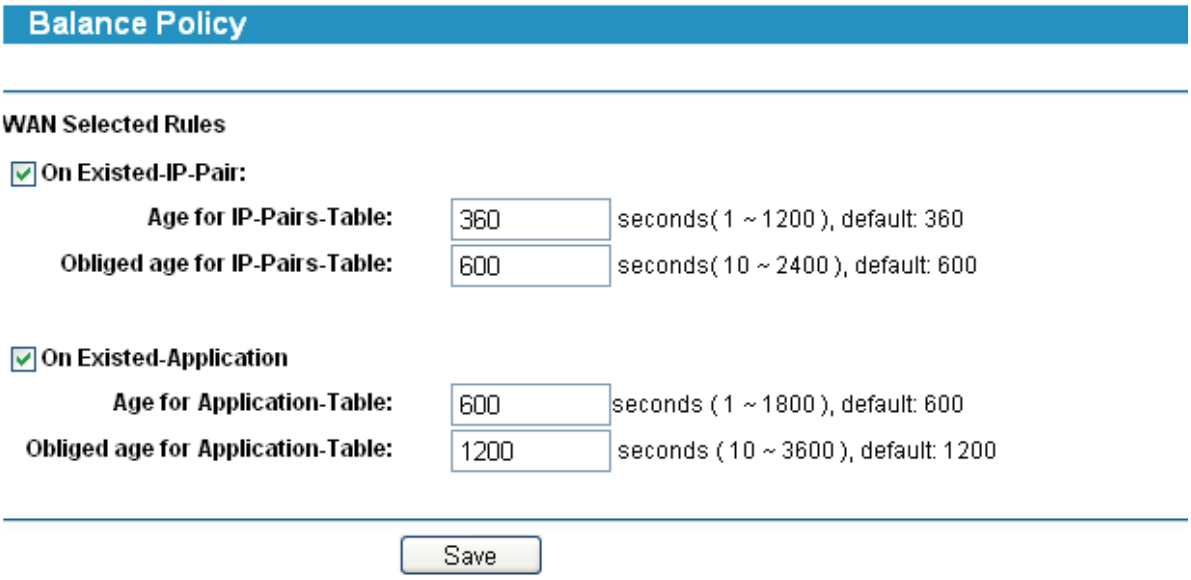


Figure 4-15

- **On Existed-IP-Pair** - If host A in LAN has connected to host B in WAN, then all the packages coming from host A to host B will be forwarded by the same WAN port.
  - **Age for IP-Pairs-Table** - Normal timeouts for the entries in IP-Pairs-Table.
  - **Obliged age for IP-Pairs-Table** - Obliged timeouts for the entries in IP-Pairs-Table.
- **On Existed-Application** - If one application will raise more than 2 connections, then all the packets of this application will forwarded by the same WAN port.
  - **Age for Application-Table** - Normal timeouts for the entries in Application-Table.
  - **Obliged age for Application-Table** - Obliged timeouts for the entries in Application-Table.

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

Note:

The Extra IP Address Dispatch Rules are prior to Balance Policy, while the Balance Policy is prior to Load Balance.

4.3.8 WAN Port Parameter

Choose menu "**Network→WAN Port Parameter**", you can view the information about the WAN ports in the next screen.

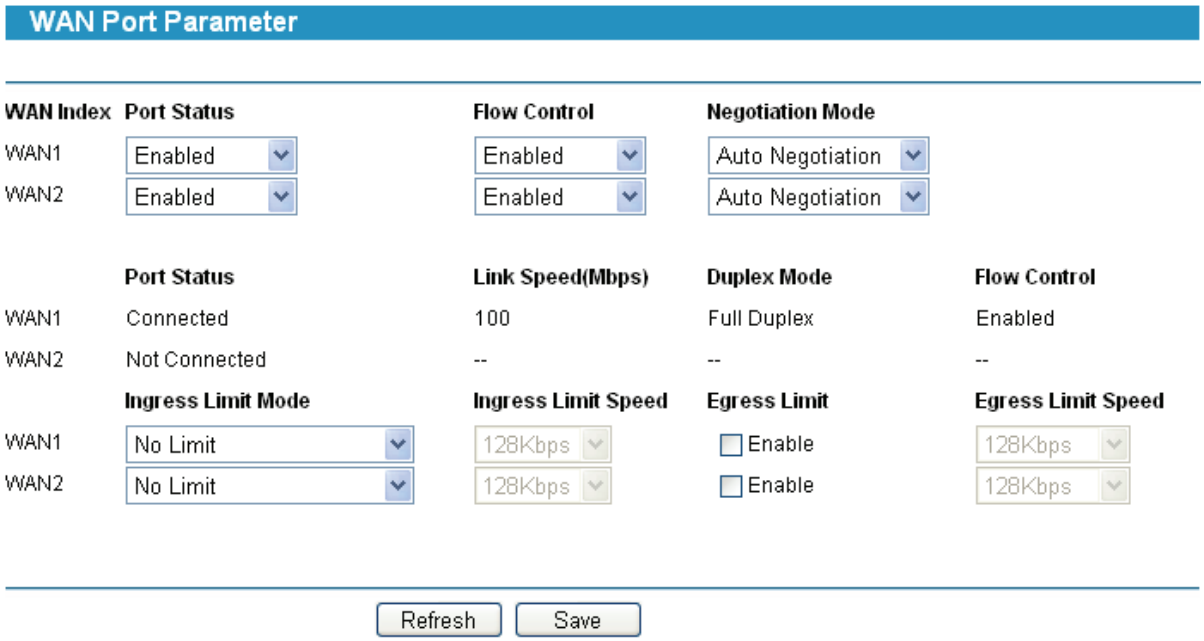


Figure 4-16

- **WAN Index -** This shows the Router's WAN ports.
- **Port Status -** This shows the ports' current status: Enabled or Disabled, the default status is Enabled.
- **Flow Control -** This displays whether the Flow Control is Enabled, "Enabled" means the function is enabled, and “Disabled" means the function isn’t enabled.
- **Negotiation Mode -** The options are: Auto Negotiation, 10M Half Duplex, 10M Full Duplex,100M Half Duplex,100M Full Duplex.
- **Ingress Limit Mode & Ingress Limit Speed** - Select the limit mode and limit speed for the WAN ports.
- **Egress Limit & Egress Limit speed** - Enable Egress Limit for WAN ports and select the limit speed for them.

Note:

Egress speed limit is designed for controlling the broadcasting storm. When the current flux oversteps the setting value, the overstepped datagram will be discarded.

4.4 DHCP

Choose menu “**DHCP**”, you can see the submenus under the main menu: **DHCP Settings**, **DHCP Clients List** and **Address Reservation**.

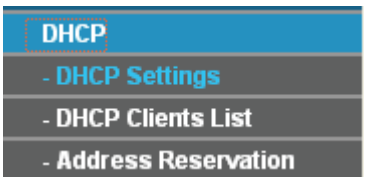


Figure 4-17

Click any of them, and you will be able to configure the corresponding function. The detailed explanations for each submenu are provided below.

4.4.1 DHCP Settings

Choose menu "**DHCP→DHCP Settings**", you can configure the DHCP in the next screen (shown in Figure 4-18).

The router is set up by default as a DHCP (Dynamic Host Configuration Protocol) server, which provides the TCP/IP configuration for all the PCs that are connected to the router on the LAN.

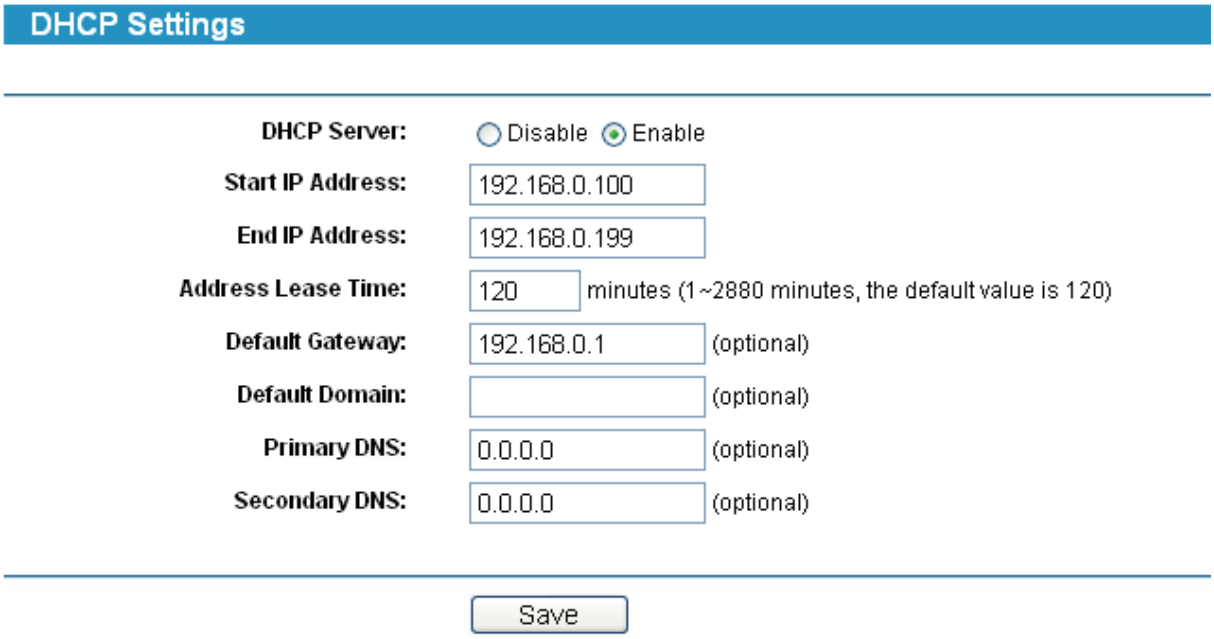


Figure 4-18

- **DHCP Server - Enable** or **disable** the DHCP server. If you disable the Server, you must have another DHCP server within your network or else you must manually configure the computer.
- **Start IP Address -** This field specifies the first address in the IP address pool. The default address is 192.168.0.100.
- **End IP Address -** This field specifies the end address in the IP address pool. The default address is 192.168.0.199.
- **Address Lease Time -** This is the amount of time in which a network user will be allowed connection to the router with their current dynamic IP address. Enter the amount of time (in minutes), the range of the time is 1 ~ 2880 minutes. The default value is 120 minutes.
- **Default Gateway -** Suggest inputting the IP address of the LAN port of the router, default value is 192.168.0.1. (Optional)
- **Default Domain -** Input the domain name of your network. (Optional)
- **Primary DNS -** Input the DNS IP address provided by your ISP. You can consult your ISP for it. (Optional)
- **Secondary DNS -** Input the IP address of another DNS server if your ISP provides two DNS servers. (Optional)

Note:

To use the DHCP server function of the router, you must configure all computers on the LAN as "Obtain an IP Address automatically" mode. This function will take effect until the router reboots.

4.4.2 DHCP Clients List

Choose menu "**DHCP→DHCP Clients List**", you can view the information about the clients attached to the router in the next screen (shown in Figure 4-19). Click the **Refresh** button to update the information.

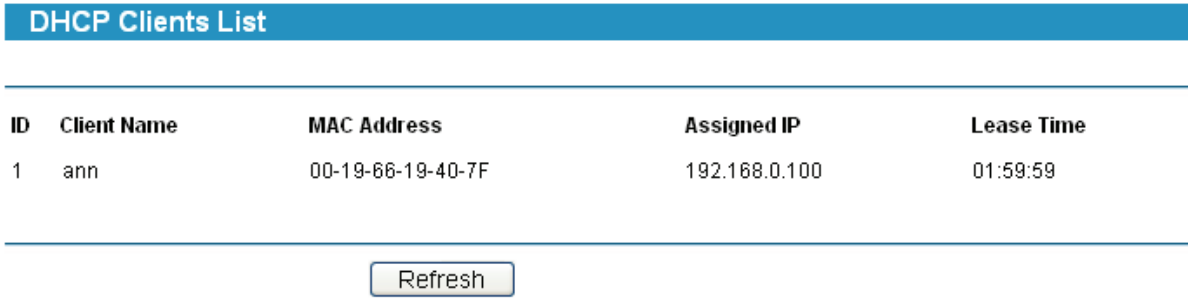


Figure 4-19

- **Client Name -** This field displays the name of the DHCP client
- **MAC Address -** This field displays the MAC address of the DHCP client
- **Assigned IP -** This field displays the IP address that the router has allocated to the DHCP client.
- **Lease Time -** This field displays the time of the DHCP client leased. Before the time is up, DHCP client will request to renew the lease automatically.

4.4.3 Address Reservation

Choose menu "**DHCP→Address Reservation**", you can view and add reserved addresses for clients via the next screen (shown in Figure 4-20).

If you specify a reserved IP address for a PC on the LAN, that PC will always receive the same IP address each time when it accesses the DHCP server. Reserved IP addresses should be assigned to servers that require permanent IP settings.

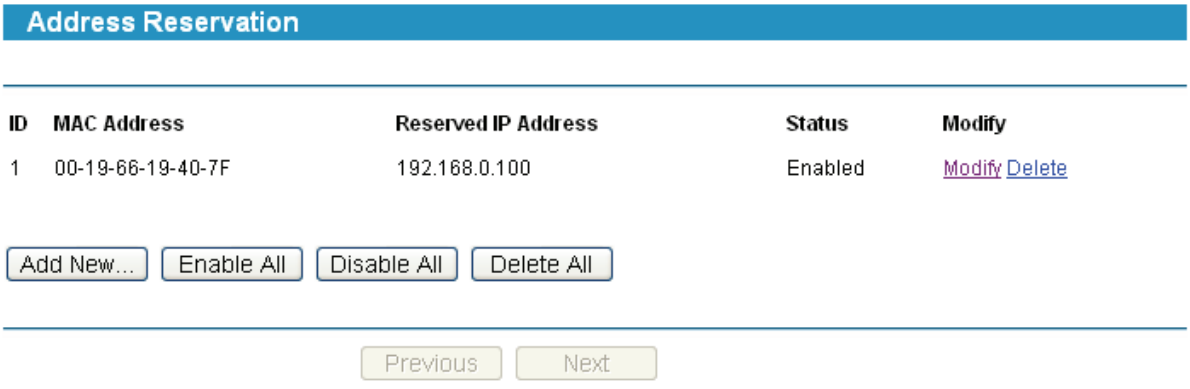


Figure 4-20

- **MAC Address -** This field displays the MAC address of the PC for which you want to reserve IP address.

- **Assigned IP Address -** This field displays the IP address of the router reserved.
- **Status -** This field displays the status of the virtual server entry. **Enabled** means that the entry will take effect, **Disabled** means that the entry will not take effect.

To add/modify a reserved IP address:

Step 1: Click **Add New…/Modify** shown in Figure 4-20, you will see a new screen shown in Figure 4-21.

Step 2: Enter the MAC address, IP address and select Status as shown in the screen below.

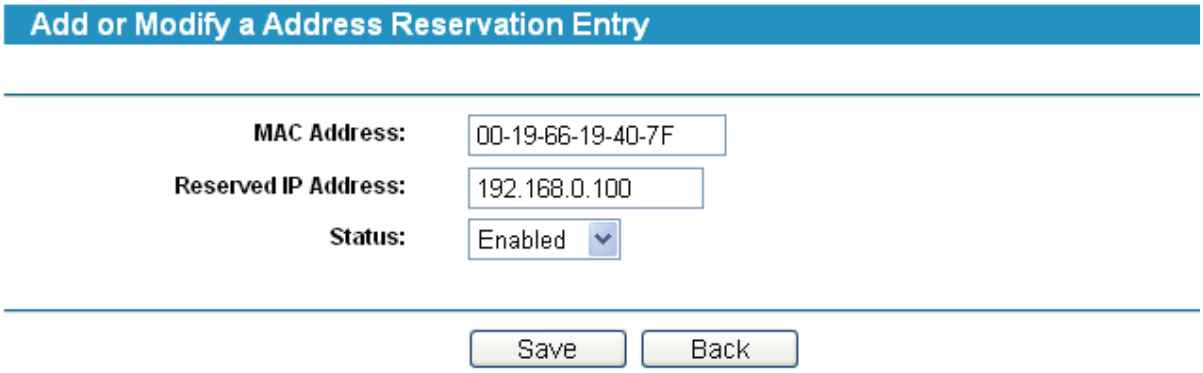


Figure 4-21

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

Note:

1) If you want to add more than one reserved IP, please go to **step 1** to continue.
2) The function won't take effect until the router reboots.

Other configurations for the entries as shown in Figure 4-20:

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

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

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

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

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

4.5 Forwarding

Choose menu "**Forwarding**", you can see the submenus under the main menu: **Virtual Servers**, **Port Triggering**, **DMZ** and **UPnP**.

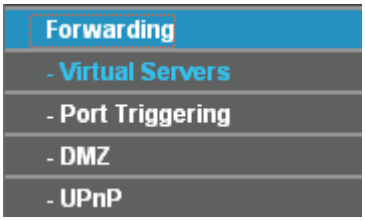


Figure 4-22

Click any of them, and you will be able to configure the corresponding function. The detailed explanations for each submenu are provided below.

4.5.1 Virtual Servers

Choose menu "**Forwarding→Virtual Servers**", you can view and add virtual servers in the next screen (shown in Figure 4-23).

Virtual servers can be used for setting up public services on your LAN, such as DNS, Email and FTP. A virtual server is defined as a service port, and all requests from Internet to this service port will be redirected to the computer specified by the server IP. Any PC that was configured as a virtual server must have a static or a reserved IP address because its IP address may change when using the DHCP function.

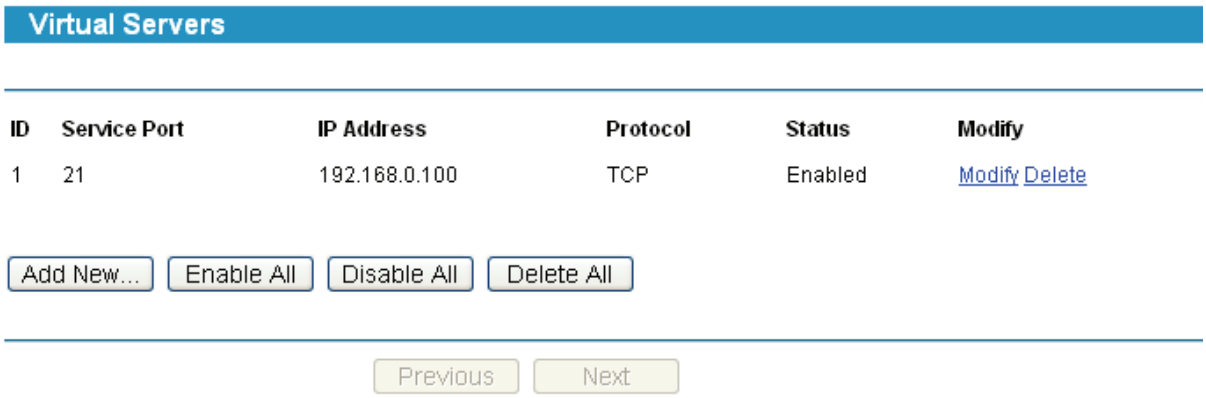


Figure 4-23

- **Service Port -** This field displays the numbers of External Ports. It can be a service port or a range of service ports (the format is XX-YY or XX, XX is Start port, YY is End port).
- **IP Address -** This field displays the IP address of the PC running the service application.
- **Protocol -** This field displays the protocol used for this application, either **TCP**, **UDP**, or **All** (all protocols supported by the router).
- **Status -** This field displays the status of the virtual server entry. **Enabled** means that the entry will take effect, **Disabled** means that the entry will not take effect.

To add/modify a virtual server entry:

Step 1: Click **Add New…/Modify** shown in Figure 4-20, you will see a new screen shown in Figure 4-24.

Step 2: Select the service you want from the "**Common Service Port**", then the port and protocol value will be added to the corresponding field automatically, you only need to configure the IP address for the virtual server; If the "**Common Service Port**" does not contain the service that you want, please configure the Service Port, IP Address and Protocol manually.

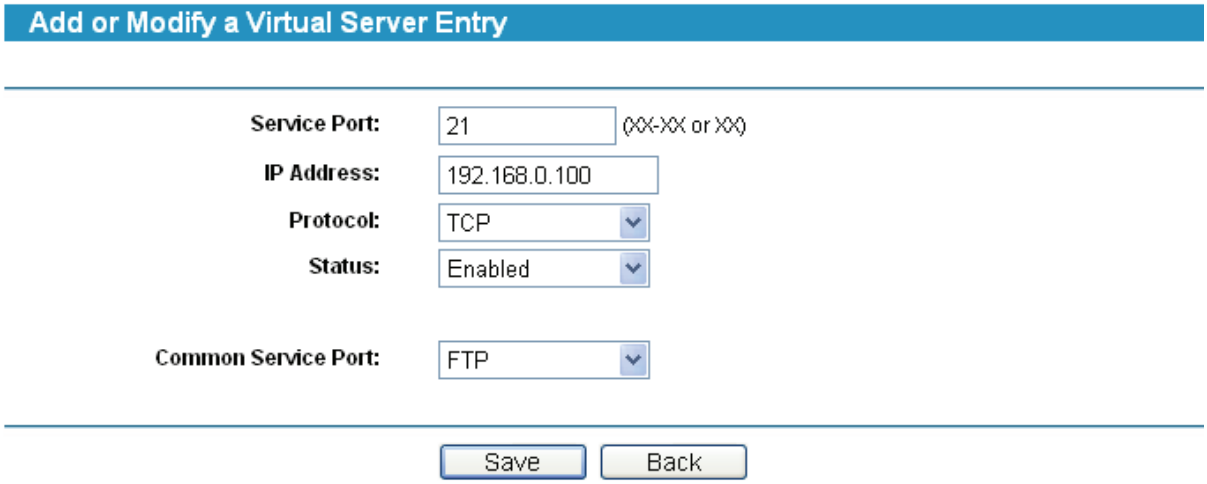


Figure 4-24

Step 3: After that, select **Enable** to make the entry take effect.

Step 4: Click **Save** button to save the configuration.

Note:

1) If you want to add more than one reserved IP, please go to **step 1** to continue.
2) It is possible that you configure more than one type of available service on a computer or server; it means the IP addresses for the virtual servers are same.

Other configurations for the entries as shown in Figure 4-24:

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

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

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

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

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

Note:

If you set the virtual server of the service port as 80, you must set the web management port on **System Tools –> Remote Management** screen to be any value except 80 such as 8080. Or else there will be a conflict to disable the virtual server.

4.5.2 Port Triggering

Choose menu "**Forwarding→Port Triggering**", you can view and add port triggering in the next screen (shown in Figure 4-25).

Some applications require multiple connections, like Internet games, video conferencing, Internet calling and so on. These applications cannot work with a pure NAT router. Port Triggering is used for some of these applications that can work with an NAT router.

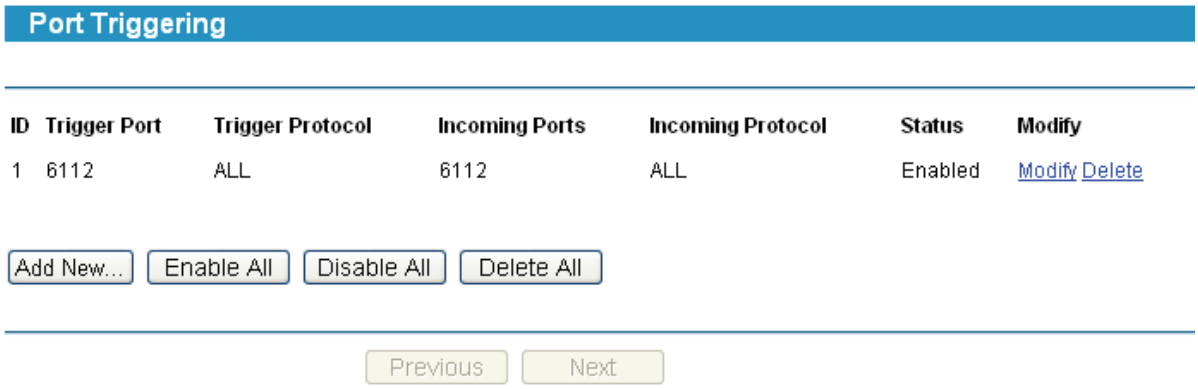


Figure 4-25

- **Trigger Port -** This displays the port for outgoing traffic. An outgoing connection using this port will "Trigger" this rule.
- **Trigger Protocol -** This displays the protocol used for Trigger Ports, either **TCP**, **UDP**, or **All** (all protocols supported by the router).
- **Incoming Ports -** This displays the port or port range used by the remote system, they are used for responding to the outgoing request. A response using one of these ports will be forwarded to the PC that triggered this rule. You can input at most 5 groups of ports (or port section). Every group of ports must be apart with ",". For example, 2000-2038, 2050-2051, 2085, 3010-3030.
- **Incoming Protocol -** This displays the protocol used for Incoming Ports Range, either **TCP** or **UDP**, or **ALL** (all protocols supported by the router).
- **Status -** This displays the status. **Enabled** means that the rule will take effect, **Disabled** means that the rule will not take effect.

Once configured, the operation for Port Triggering will proceed as follows:

Step 1: A local host makes an outgoing connection using a destination port number defined in the Trigger Port field.

Step 2: The router records this connection, opens the incoming port or ports associated with this entry in the Port Triggering table, and associates them with the local host.

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

To add/modify a port triggering entry:

Step 1: Click **Add New…/Modify** shown in Figure 4-25, you will see a new screen shown in Figure 4-26.

Step 2: Select the application you want from the "**Common Applications**", then the Trigger port and Incoming ports will be added to the corresponding field automatically, you only need to configure the Trigger protocol and Incoming Protocol for the entry; If the "**Common Applications**" does not contain the applications that you want, please configure these options manually.

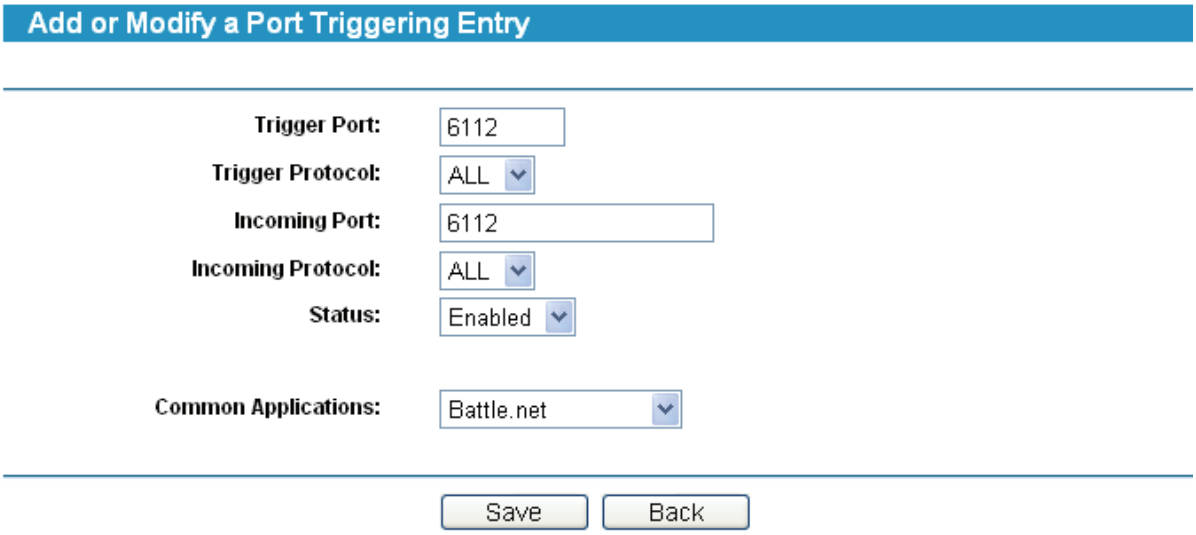


Figure 4-26

Step 3: After that, select **Enabled** to make the entry take effect.

Step 4: Click **Save** button to save the configuration.

Note:

1) If you want to add more than one reserved IP, please go to **step 1** to continue.
2) When the trigger connection is released, the according opening ports will be closed.
3) Each rule allowed to be used only by one host on LAN synchronously. The trigger connection of other hosts on LAN will be refused.
4) Incoming Port Range cannot overlap each other.

Other configurations for the entries as shown in Figure 4-26:

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

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

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

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

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

4.5.3 DMZ

Choose menu "**Forwarding→DMZ**", you can view and configure DMZ host in the screen (shown in Figure 4-27).

The DMZ host feature allows one local host to be exposed to the Internet for a special-purpose service such as Internet gaming or videoconferencing. DMZ host forwards all the ports at the same time. Any PC whose port is being forwarded must have its DHCP client function disabled and should have a new static IP address assigned to it because its IP address may change when using the DHCP function.

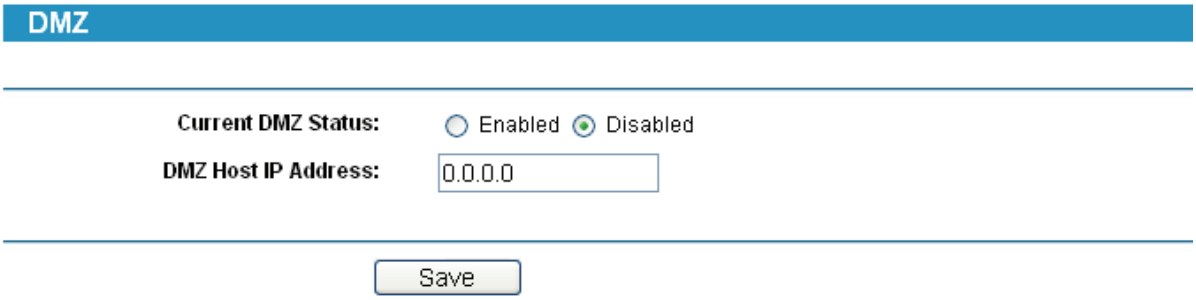


Figure 4-27

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

Step 1: Click the **Enable** radio button

Step 2: Enter the local host IP address in the **DMZ Host IP Address** field

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

Note:

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

4.5.4 UPnP

Choose menu "**Forwarding→UPnP**", you can view the information about UPnP in the screen (shown in Figure 4-28). You can click **Refresh** to update the Current UPnP Settings List before viewing the information.

The Universal Plug and Play (UPnP) feature allows the devices, such as Internet computers, to access the local host resources or devices as needed. UPnP devices can be automatically discovered by the UPnP service application on the LAN.

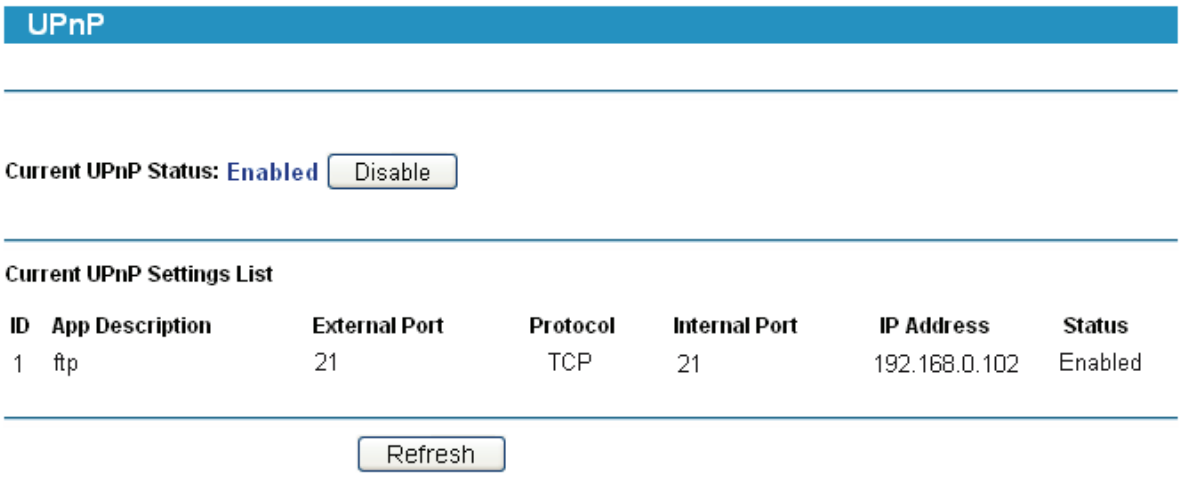


Figure 4-28

- **Current UPnP Status -** If you want to use the Router's UPnP function, please click **Enable** button. If you don't want use the function, please click **Disable** button. Allowing the function may cause a risk to security; this feature is disabled by default.
- **App Description -** This displays the description provided by the application in the UPnP request.
- **External Port -** This displays the external port, which the router opened for the application.

- **Protocol -** This displays the protocol for the application.
- **Internal Port -** This displays the internal port, which the router opened for local host.
- **IP Address -** The UPnP device that is currently accessing the router.
- **Status -** This displays the status. **Enabled** means that the port is still active, **Disabled** means that the port is inactive.

4.6 Security

Choose menu "**Security**", you can see the submenus under the main menu: **Firewall**, **IP Address Filtering**, **Domain Filtering**, **MAC Filtering**, and **Screen**.

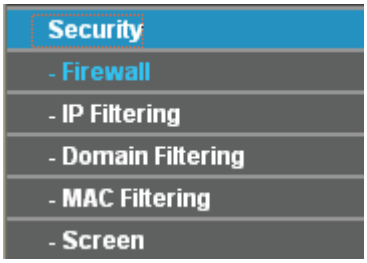


Figure 4-29

Click any of them, and you will be able to configure the corresponding function. The detailed explanations for each submenu are provided below.

4.6.1 Firewall

Choose menu "**Security→Firewall**", you can control the general firewall switch in the next screen (shown in Figure 4-30). The default setting for the switch is off, the IP Address Filtering, Domain Filtering, MAC Address Filtering and Screen are disabled, and their settings are ineffective in the default settings.

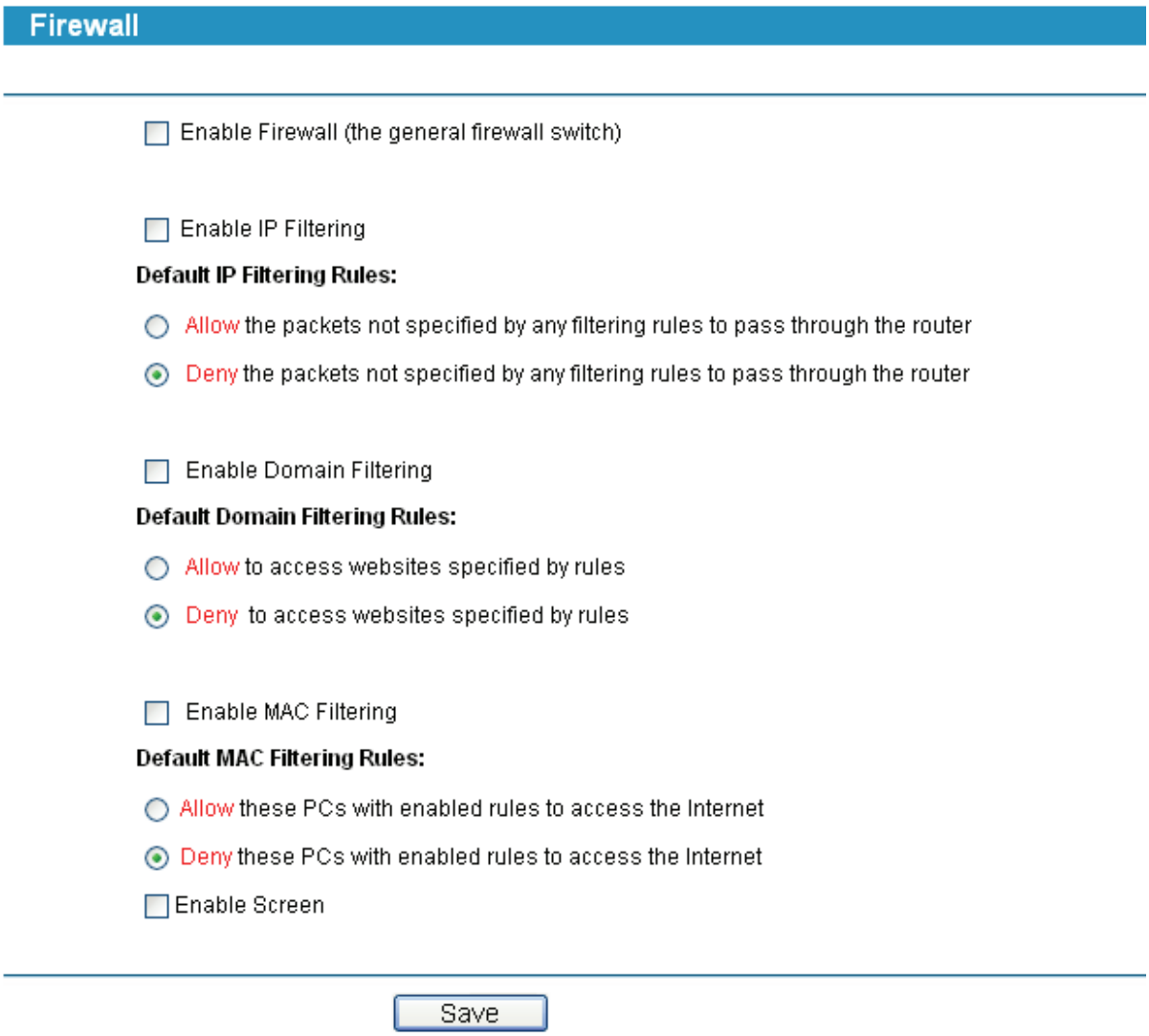


Figure 4-30

- **Enable Firewall -** Enable the general firewall switch or not.
- **Enable IP Address Filtering -** Enable the IP Address Filtering or not. There are two default filtering rules, please select the rule for your need.
- **Enable Domain Filtering -** Enable the Domain Filtering or not. There are two default filtering rules, please select the rule for your need.
- **Enable MAC Address Filtering -** Enable MAC Address Filtering or not. There are two default filtering rules, please select the rule for your need.
- **Enable Screen -** Enable the screen function or not.

4.6.2 IP Filtering

Choose menu "**Security→IP Address Filtering**", you can configure the IP Address filtering rule in the next screen (shown in Figure 4-32). The IP Address Filtering feature allows you to control Internet Access by specific users on your LAN based on their IP addresses.

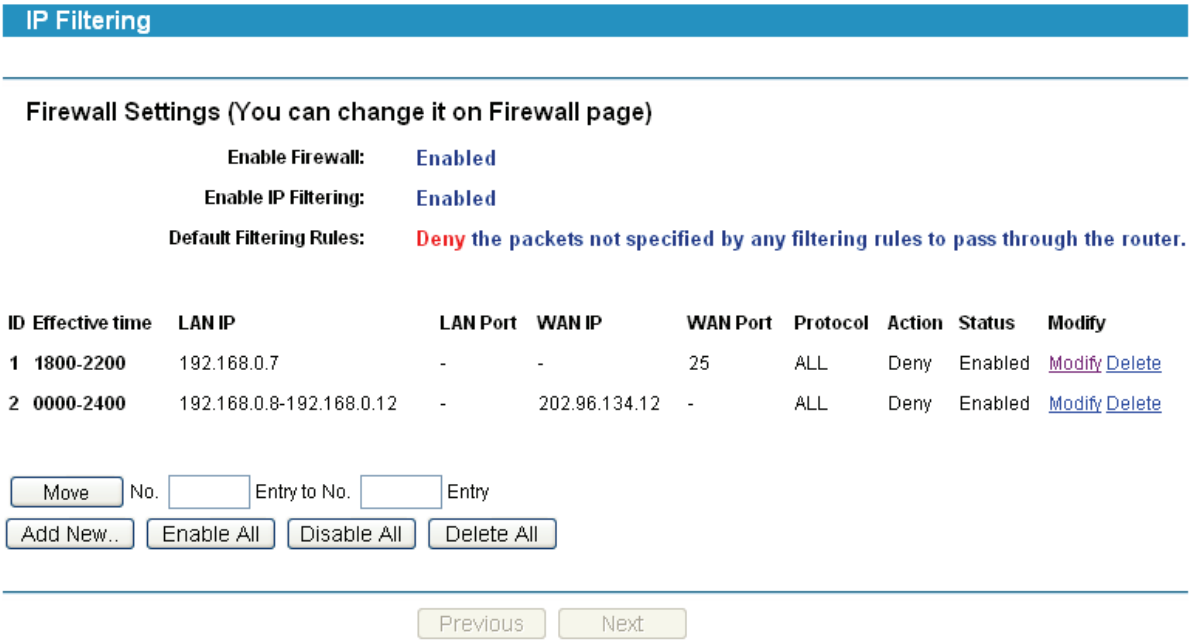


Figure 4-31

- **Effective Time -** This is the time or the range of time for the entry to take effect. For example, 1800 - 2200, it means that the entry will take effect from 18:00 to 22:00.
- **LAN IP -** This is the LAN IP address or the range of LAN IP addresses in dotted-decimal notation format. For example, 192.168.0.20 - 192.168.0.30. Keep the field blank, which means all LAN IP addresses are controlled by the rule.
- **LAN Port -** This is the LAN Port or the range of LAN ports in the field. For example, 1030 - 2000. Keep the field blank, which means all LAN ports are controlled by the rule.
- **WAN IP -** This is the WAN IP address or the range of WAN IP addresses in dotted-decimal notation format. For example, 202.96.134.210 – 202.96.134.230. Keep the field blank, which means all WAN IP addresses are controlled by the rule.
- **WAN Port -** This is the WAN Port or the range of WAN Ports. For example, 25 – 110. Keep the field blank, which means all WAN Ports are controlled by the rule.
- **Protocol -** This indicates which protocol is used, TCP, **UDP**, or **All** (all protocols supported by the router).
- **Action -** This field displays the action that the Router takes to deal with the traffic. **Allow** means that the Router allows the traffic through the Router, **Deny** means that the Router rejects the traffic through the router.
- **Status -** This field displays the status of the rule. **Enabled** means the rule will take effect, **Disabled** means the rule will not take effect.

To add/modify an IP Address filtering entry:

For example: If you desire to block E-mail received and sent by the IP address 192.168.0.7 on your local network during the time of 1800 to 2200; And wish to make the PCs with IP addresses 192.168.0.8 to 192.168.0.12 unable to visit the website of IP address 202.96.134.12 all the day, while other PCs have no limit. You can configure the rules as follows.

Step 1: Enable the "**Firewall**" and "**IP Address Filtering**" on the Firewall screen (show in Figure 4-30), and then, you should select the Default IP Address Filtering Rule "**Allow the packets not specified by any filtering rules to pass through the router**".

Step 2: Click **Add New…/Modify** shown in Figure 4-32, you will see a new screen shown in Figure 4-32.

Step 3: Enter the "**Effective time**" that the rule will take effect as shown in Figure 4-32.

Step 4: Enter the **"192.168.0.7**" as "**LAN IP Address**", and the "**25**" as "**WAN Port**" in the corresponding field as shown in Figure 4-32.

Note:

WAN port 25 is responsible for SMTP (Simple Mail Transfer Protocol), while the WAN port 110 is responsible for POP3 (Post Office Protocol –version 3). To block the reception and transfer of the email, the WAN port 25 and 110 should be denied.

Step 5: Select the "**Protocol**", "**Action**" and "**Status**" for the rule as shown in the next screen.

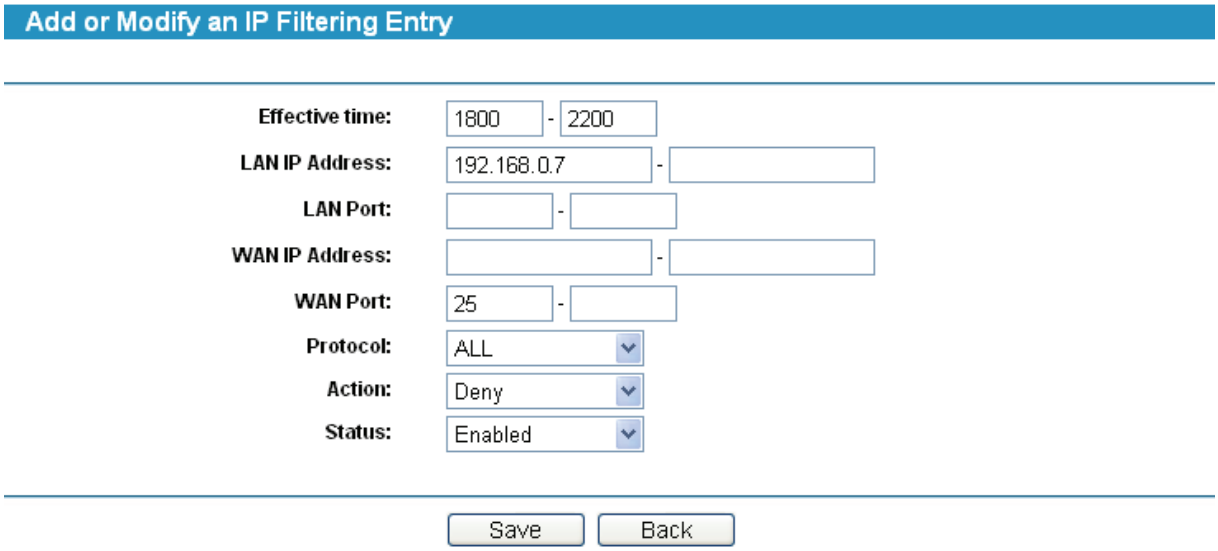


Figure 4-32

Step 6: Click the **Save** button to save this entry.

Step 7: Go to **Step 2** to complete the other rules continually.

After you finish the configurations, you will see the rules in the table below:

ID	Effective time	LAN IP	LAN Port	WAN IP	WAN Port	Protocol	Action	Status	Modify
1	1800-2200	192.168.0.7	-	-	25	ALL	Deny	Enabled	Modify Delete
2	1800-2200	192.168.0.7	-	-	110	ALL	Deny	Enabled	Modify Delete
3	0000-2400	192.168.0.8-192.168.0.12	-	202.96.134.12	-	ALL	Deny	Enabled	Modify Delete

Figure 4-33

Note:

Before adding an IP Address Filtering entry, you should enable the Firewall and the IP Address Filtering function first (shown in Figure 4-30).

Other configurations for the entries as shown in Figure 4-31**:**

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

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

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

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

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

4.6.3 Domain Filtering

Choose menu "**Security→Domain Filtering**", you can configure the Domain filtering rule in the next screen (shown in Figure 4-34). The Domain Filtering feature allows you to control access to certain websites on the Internet by specifying their domains or key words.

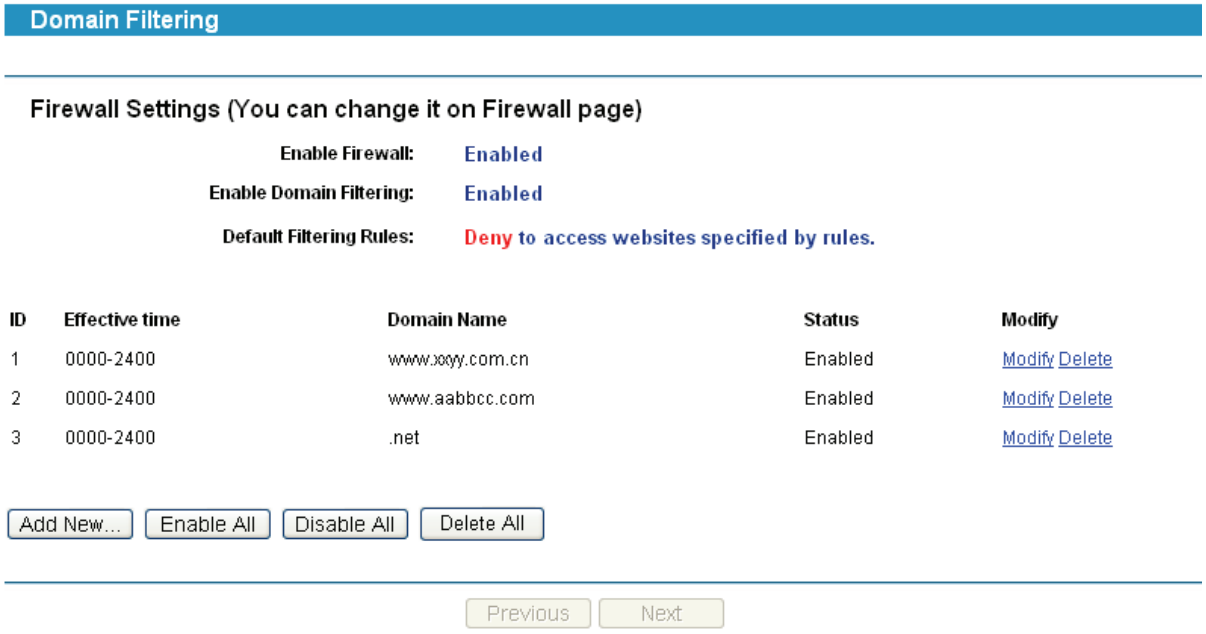


Figure 4-34

- **Default Filtering Rules -** Here displays the default rule of domain filtering, which can be changed on the Firewall page.
  - **Deny to access websites specified by rules:** This rule determines that the websites specified by rules are not permitted to access, but the other websites can be accessed normally.
  - **Allow to access websites specified by rules:** This rule determines that only the websites specified by rules can be accessed, but the other websites are not permitted to access.
- **Effective Time -** This is the time or the range of time for the entry to take effect. For example, 0800 - 2400, it means that the entry will take effect from 08:00 to 20:00.
- **Domain Name -** This is the domain or key word as desired. Leaving the field blank means all websites on the Internet are prohibited from accessing.
- **Status -** This field displays the status, **Enabled** means the rule is effective, **Disabled** means the rule is ineffective.

To add or modify a Domain Filtering entry:

For example: if you want to block the PCs on your LAN from accessing websites www.xxyy.com.cn, www.aabbcc.com and websites with end of .net on the Internet, while no limit for other websites, you can configure as follows.

Step 1: Enable the "**Firewall**" and "**Domain Filtering**" on the Firewall screen (show in Figure 4-30).

Step 2: Select the **Deny to access websites specified by rules** as the **Default Domain Filtering Rules** on the Firewall screen (show in Figure 4-30).

Step 3: Click **Add New…/Modify** shown in Figure 4-34, you will see a new screen shown in Figure 4-35.

Step 4: Enter the "**Effective time**" that the rule will take effect, enter the "**Domain Name**" as shown in Figure 4-35.

Step 5: Select the "**Status**" for the rule as shown in the next screen.

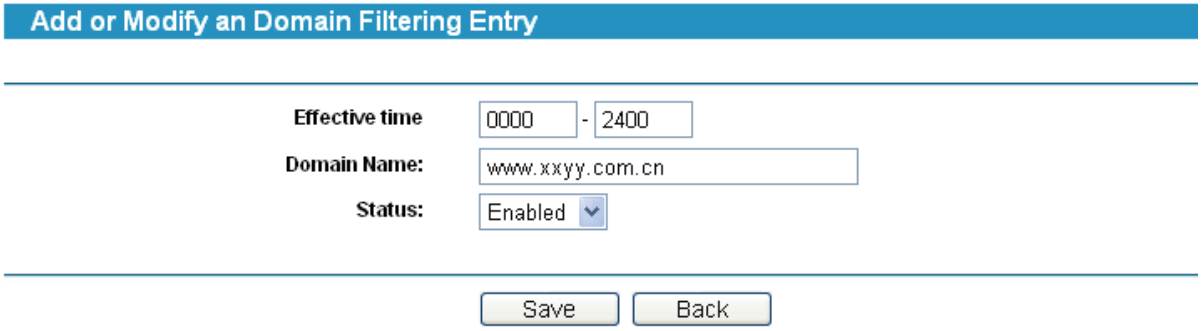


Figure 4-35

Step 6: Finally, click **Save** to make the rule take effect.

Step 7: Go to **Step 2** to complete the other rules continually.

After you finish the configurations, you will see the rules in the table below:

ID	Effective time	Domain Name	Status	Modify
1	0000-2400	www.xxyy.com.cn	Enabled	Modify Delete
2	0000-2400	www.aabbcc.com	Enabled	Modify Delete
3	0000-2400	.net	Enabled	Modify Delete

Figure 4-36

Note:

Before adding an IP Address Filtering entry, you should enable the Firewall and the IP Address Filtering function first (shown in Figure 4-30).

Other configurations for the entries as shown in Figure 4-31**:**

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

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

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

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

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

4.6.4 MAC Filtering

Choose menu "**Security→MAC Filtering**", you can configure the MAC Address filtering rule in the next screen (shown in Figure 4-37). The MAC Address Filtering feature allows you to control access to the Internet by users on your local network based on their MAC addresses.

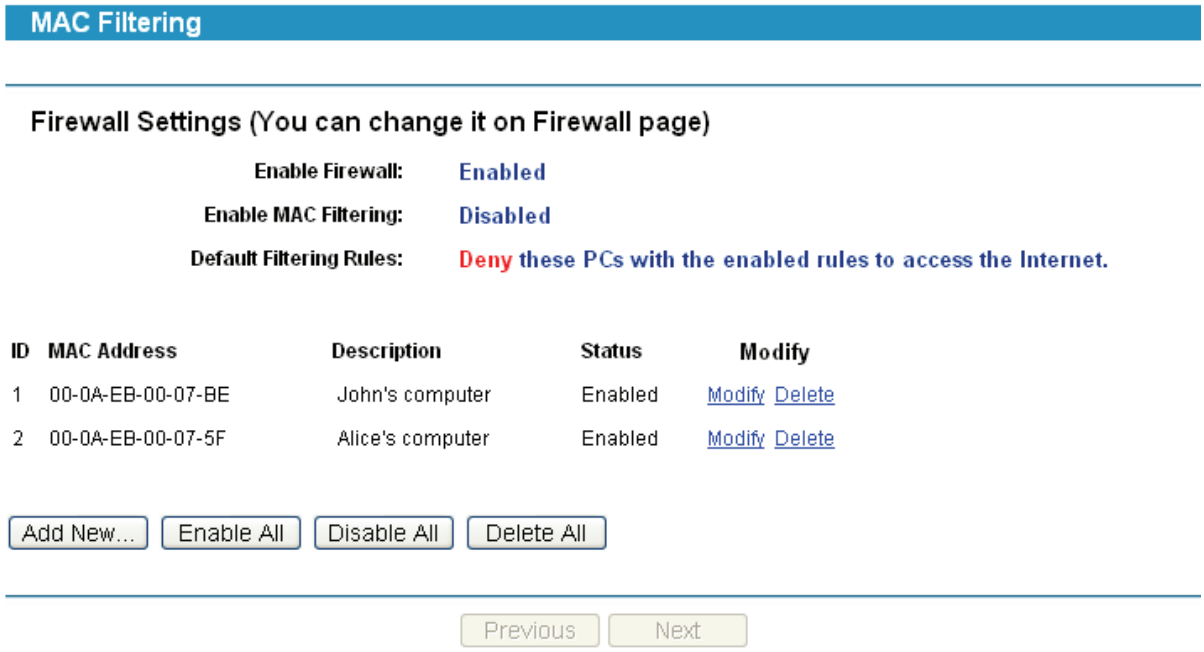


Figure 4-37

- **MAC Address -** .This is the PC'S MAC address which is controlled by the rule, its format of is XX-XX-XX-XX-XX-XX (X is any hexadecimal digit). For example: 00-0E-AE-B0-00-0B.
- **Description -** This is the description about the PC, Fox example: John's PC.
- **Status -** This field displays the status, **Enabled** means the rule is effective, **Disabled** means the rule is ineffective.

To add or modify a MAC Filtering entry:

Fox example: If you want to block the PCs with MAC addresses 00-0A-EB-00-07-BE and 00-0A-EB-00-07-5F to access the Internet, you can configure as follows.

Step 1: Enable the "**Firewall**" and "**MAC Address Filtering**" on the Firewall screen (show in Figure 4-30). And then specify the Default MAC Address Filtering Rule "Deny these PCs with enabled rules to access the Internet".

Step 2: Click **Add New…/Modify** shown in Figure 4-37, you will see a new screen shown in Figure 4-38.

Step 3: Enter the appropriate MAC address and descriptions, then select the status as shown in Figure 4-38.

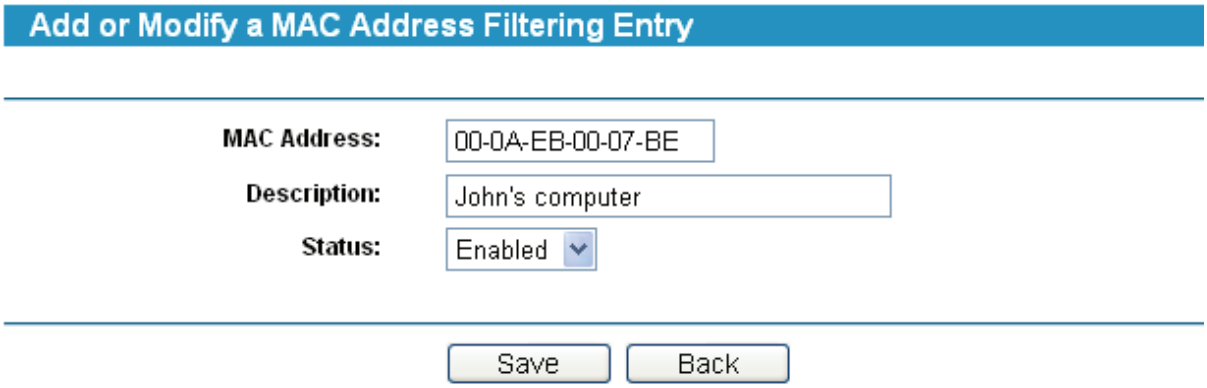


Figure 4-38

Step 4: Finally, click **Save** to make the rule take effect.

Step 5: Go to **Step 2** to complete the other rules continually.

After you finish the configurations, you will see the rules in the table below:

ID	MAC Address	Description	Status	Modify
1	00-0A-EB-00-07-BE	John's computer	Enabled	Modify Delete
2	00-0A-EB-00-07-5F	Alice's computer	Enabled	Modify Delete

Figure 4-39

Note:

Before adding a MAC Address Filtering entry, you should enable the Firewall and the MAC Address Filtering function first (shown in Figure 4-30).

Other configurations for the entries as shown in Figure 4-31**:**

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

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

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

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

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

4.6.5 Screen

Choose menu "**Security→Screen**", you can configure the functions below to protect the router from being attacked in the next two screens.

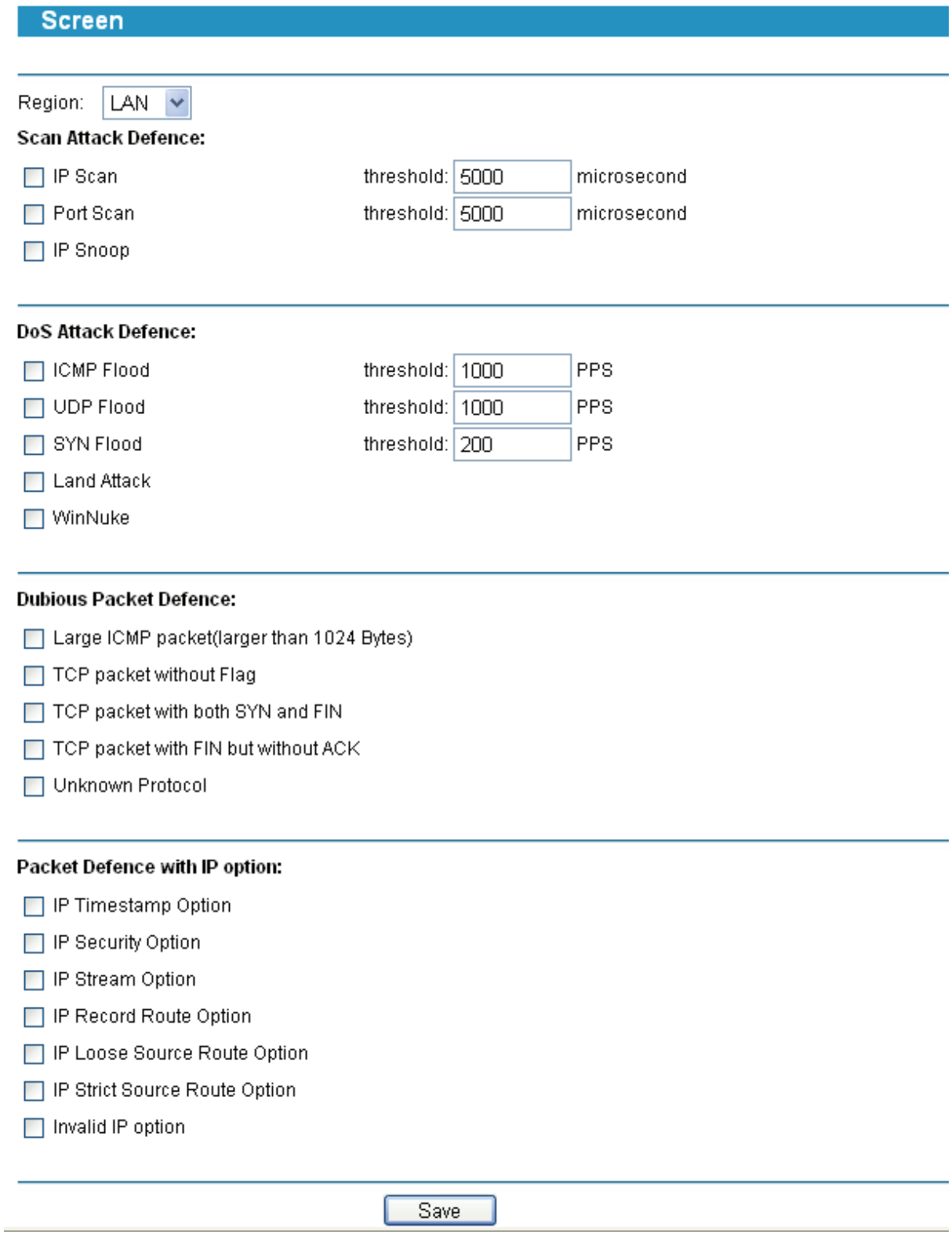


Figure 4-40

- **Region -** This option used to select the specifically area from which the packets will be monitored by the next settings.
- **Scan Attack Defence**
  - **IP Scan:** During the specific time, if a computer (identified by a particular source IP address) transmits packets to at least ten different computers (identified by different

destination IP addresses), then the source IP address will be deemed to make IP Attacks. And the Router will start up the blocking function immediately.

- **Port Scan -** During the specific time, if a computer (identified by a particular source IP address) transmits TCP SYN packets to another computer's (identified by a destination IP address) ten different ports, then the source IP address will be deemed to make Port Attacks. And the Router will start up the blocking function immediately.
- **IP Snoop -** If you select this option, the Router will monitor whether the packets from the particular region is doing IP deceive. In the event, the Router will start up the blocking function immediately. Note: The function takes effect only when the Region is LAN.

➢ **DoS Attack Defence**

- **ICMP Flood** - **-** During a second, if a destination IP addresses receives many packets, and the number of these packets exceeds the prescript value, then the destination IP will be deemed to suffering from ICMP Flood Attack. And the Router will start up the blocking function immediately.
- **UDP Flood -** This means during a second, if a destination IP address receives many packets, and the number of these packets exceeds the prescript value, then the destination IP will be deemed to be suffering from UDP Flood Attack.
- **SYN Flood -** This means during a second, when the Region is LAN, if a source IP address transmits many TCP SYN packets of which the number exceeds the prescript value, then the source IP address will be deemed to make SYN Flood Attack; when the Region is WAN, if a destination IP address receives many TCP SYN packets of which the number exceeds the prescript value, then the destination IP address will be deemed to suffering from SYN Flood Attack.
- **Land Attack -** This is an attack combining Flood attack and IP spoofing. When the attackers send the spoof SYN datagram which including the casualty's IP address and make it the destination and source IP address, the LAND attack happens. And the Router will start up the blocking function immediately.
- **WinNuke -** WinNuke is a Dos attack for any Windows computers running in the internet. The attackers send the TCP fragment (usually sets the emergent field to the Net BIOS'S 139 port) to the connection established computers. So the NetBIOS fragments created and make the Windows computers collapse. And the Router will start up the blocking function immediately.

➢ **Dubious Packet Defence**

- **Large ICMP packet:** The normal ICMP packets are very short, there normal length is shorter than 1024 Bytes. If the ICMP packets' length is larger than 1024 Bytes, then they will be considered as large ICMP packets. And the Router will start up the blocking function immediately.
- **TCP packet without Flag:** The normal TCP packets contain flag in the packet header, or else the packets will be considered as abnormal dubious packets. And the Router will start up the blocking function immediately.

- **TCP packet with both SYN and FIN:** The TCP packets which have both SYN and FIN settings in the packets header will be considered as abnormal TCP packets. And the Router will start up the blocking function immediately.
- **TCP packet with FIN but without ACK:** The TCP packets that contain FIN but without ACK are considered as abnormal. And the Router will start up the blocking function immediately.
- **Unknown Protocol -** In IP head the protocol type field, 135 and the value bigger than 135 is reserved and undefined. Because the protocols are undefined, we can not predict a specifically unknown protocol is well-meaning or baleful. To these nonstandard protocols, the carefully attitude is the best way to prevent them interning into the protected network.

➢ **Packet Defence with IP option**

- **IP Timestamp Option:** If you select this option, the Router will monitor whether the IP packets from the particular region contain the field of Internet Timestamp. In the event, the Router will start up the blocking function immediately.
- **IP Security Option:** If you select this option, the Router will monitor whether the IP packets from the particular region contain the field of Security. In the event, the Router will start up the blocking function immediately.
- **IP Stream Option:** If you select this option, the Router will monitor whether the IP packets from the particular region contain the field of Stream ID. In the event, the Router will start up the blocking function immediately.
- **IP Record Route Option:** If you select this option, the Router will monitor whether the IP packets from the particular region contain the field of Record Route. In the event, the Router will start up the blocking function immediately.
- **IP Loose Source Route Option:** If you select this option, the Router will monitor whether the IP packets from the particular region contain the field of Loose Source Route. In the event, the Router will start up the blocking function immediately.
- **IP Strict Source Route Option:** If you select this option, the Router will monitor whether the IP packets from the particular region contain the field of Strict Source Route. In the event, the Router will start up the blocking function immediately.
- **Invalid IP option:** If you select this option, the Router will monitor whether the IP packets from the particular region is integrated or right. In the event, the Router will start up the blocking function immediately.

4.7 Static Routing

Choose menu “**Static Routing**”, you can configure the static route in the next screen (shown in Figure 4-41). A static route is a pre-determined path that network information must travel to reach a specific host or network.

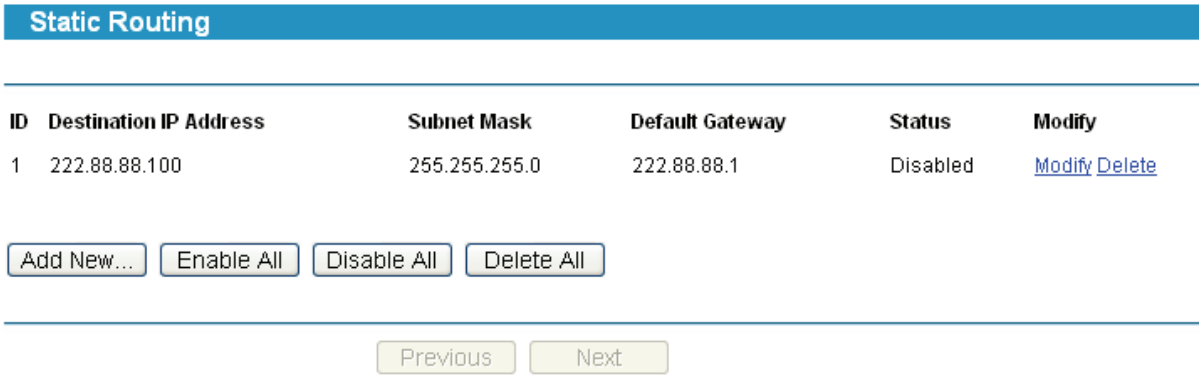


Figure 4-41

- **Destination IP Address -** The "Destination IP Address" is the address of the network or host that you want to assign to a static route.
- **Subnet Mask -** The "Subnet Mask" determines which portion of an IP address is the network portion, and which portion is the host portion.
- **Default Gateway -** This is the IP address of the gateway device that allows for contact between the router and the network or host.
- **Status -** This field displays the status, **Enabled** means the rule is effective, **Disabled** means the rule is ineffective.

To add/modify a static routing entry:

Step 1: Click **Add New…/Modify** shown in Figure 4-41, you will see a new screen shown in Figure 4-42.

Step 2: Enter the appropriate Destination IP Address, Subnet Mask and Default Gateway, and then select the status.

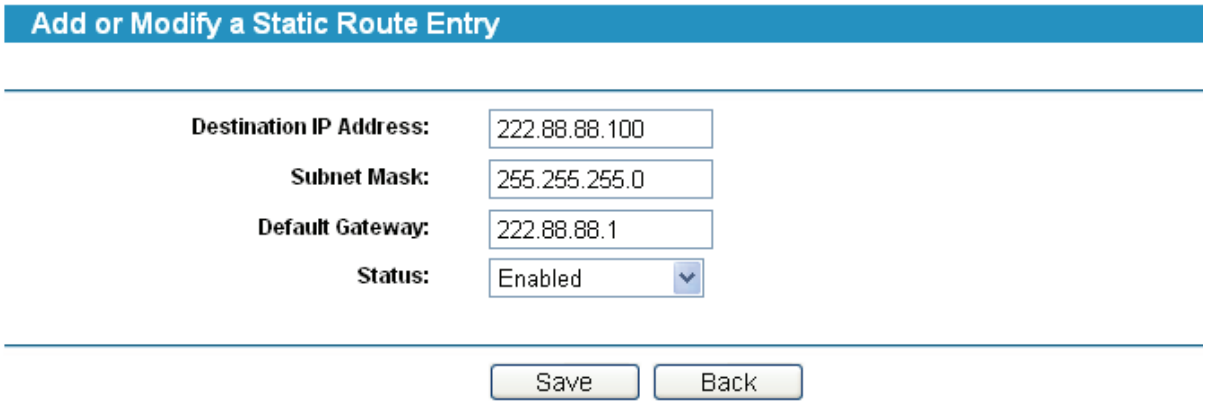


Figure 4-42

Step 3: Click **Save** to make the entry take effect.

Note:

If you want to add more than one static route, please go to **step 1** to continue.

Other configurations for the entries as shown in

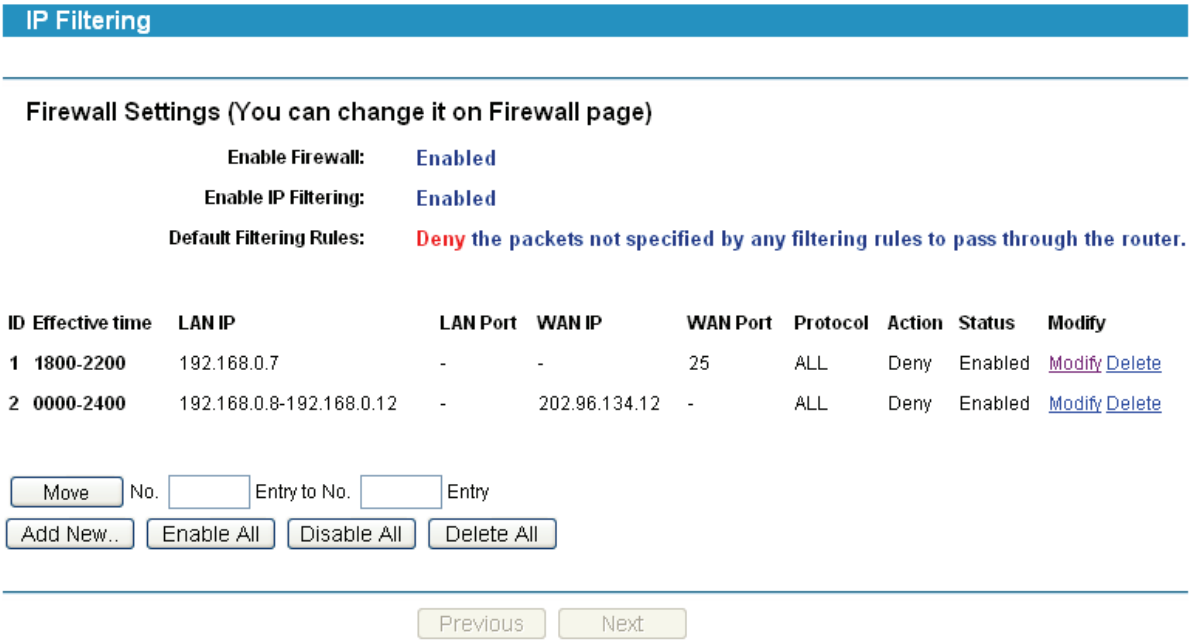


Figure 4-31**:**

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

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

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

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

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

4.8 Session Limit

Choose menu "**Session Limit**", you can see the submenus under the main menu:

Figure 4-43

Click any of them, and you will be able to configure the corresponding function. The detailed explanations for each submenu are provided below.

4.8.1 Session Limit

Choose menu "**Session Limit→Session Limit**", you can view and configure the session limits in the next screen. For conveniently control the connections of the computers in the LAN, you can set the max number of connections for different computers.

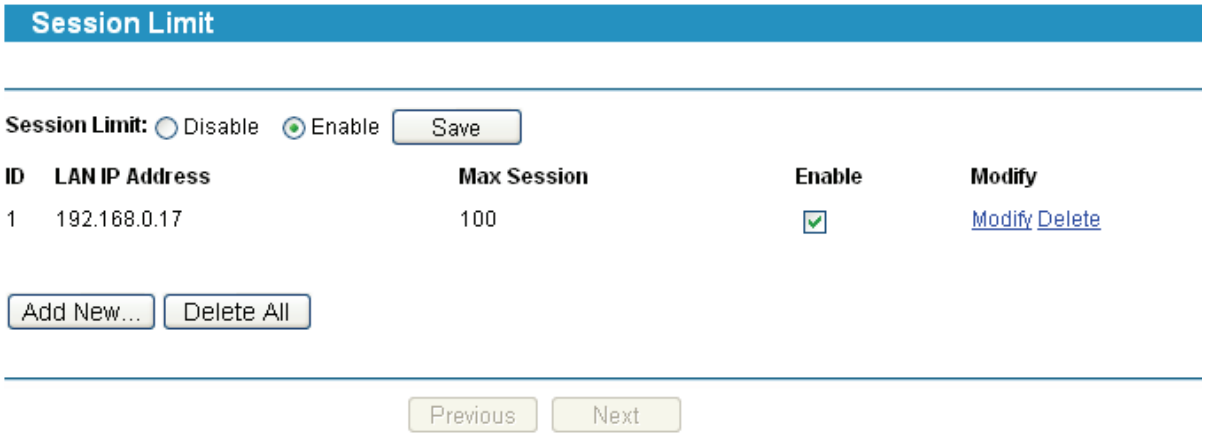


Figure 4-44

- **Enable:** Enable or disable the session limit. Only after choose "Enable", the configuration will take effect.
- **LAN IP address:** The controlled computer's IP address. You can input a range of IP address, for example: 192.168.0.20 -192.168.0.30. You can also input an IP address, such as: 192.168.0.40.
- **Max Session:** The max connections of the computer.

To add/modify a session limit entry:

Step 1: Click **Add New…/Modify** shown in Figure 4-44, you will see a new screen shown in Figure 4-45.

Step 2: Enter the appropriate LAN IP Address, Max Session and then select the status.

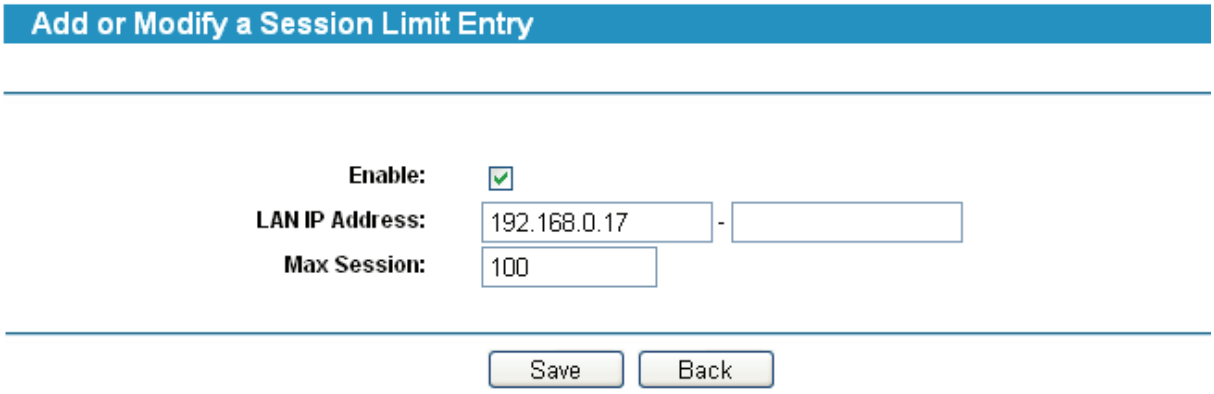


Figure 4-45

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

4.8.2 Session List

Choose menu "**Session Limit→Session List**", you can view the information about the number of connection.

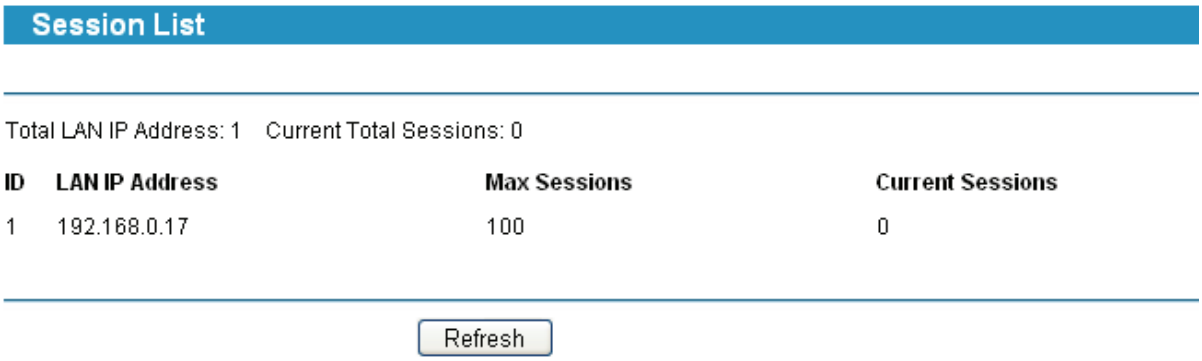


Figure 4-46

Note:

You can click the **Refresh** to update the information.

4.9 QoS

Choose menu "**QoS**", you can see the submenus under the main menu:

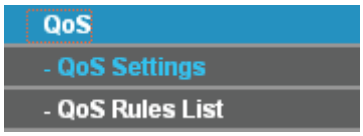


Figure 4-47

Click any of them, and you will be able to configure the corresponding function. The detailed explanations for each submenu are provided below.

4.9.1 QoS Settings

Choose menu "**QoS→QoS Settings**", you can configure the Upload Bandwidth and Download Bandwidth in the next screen, their value you configure should be less than 1000000Kbps.

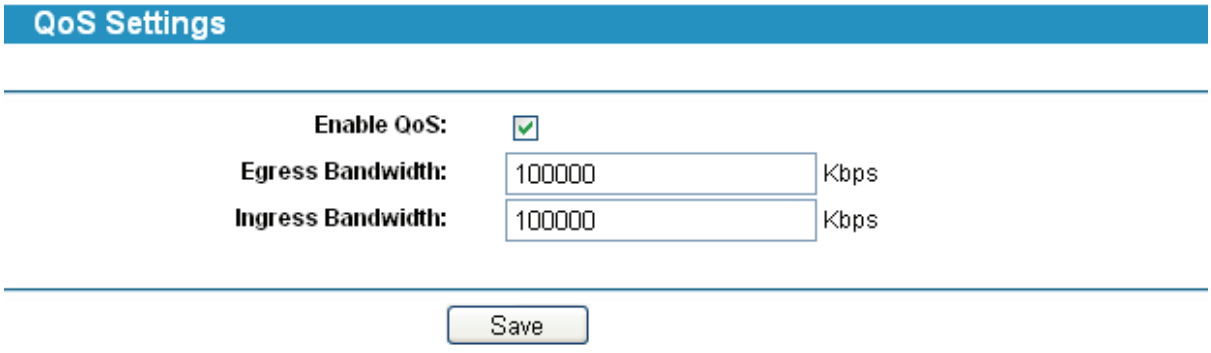


Figure 4-48

4.9.2 QoS Rules List

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

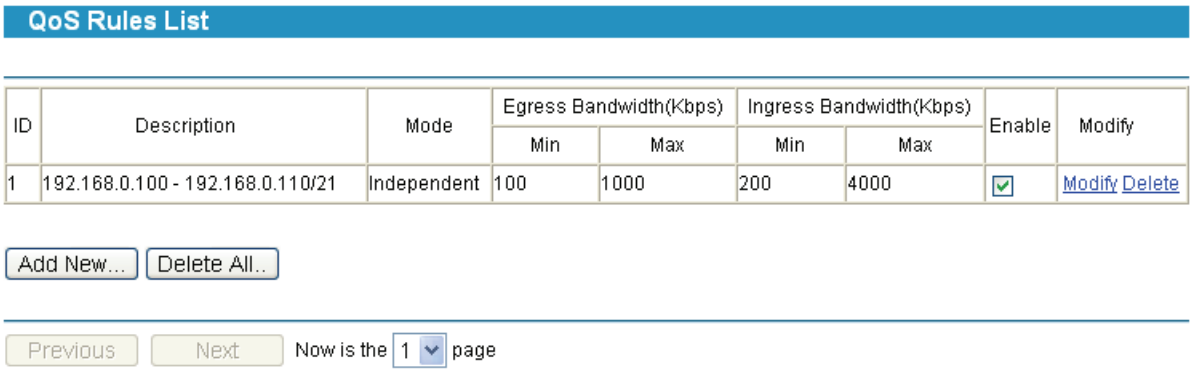
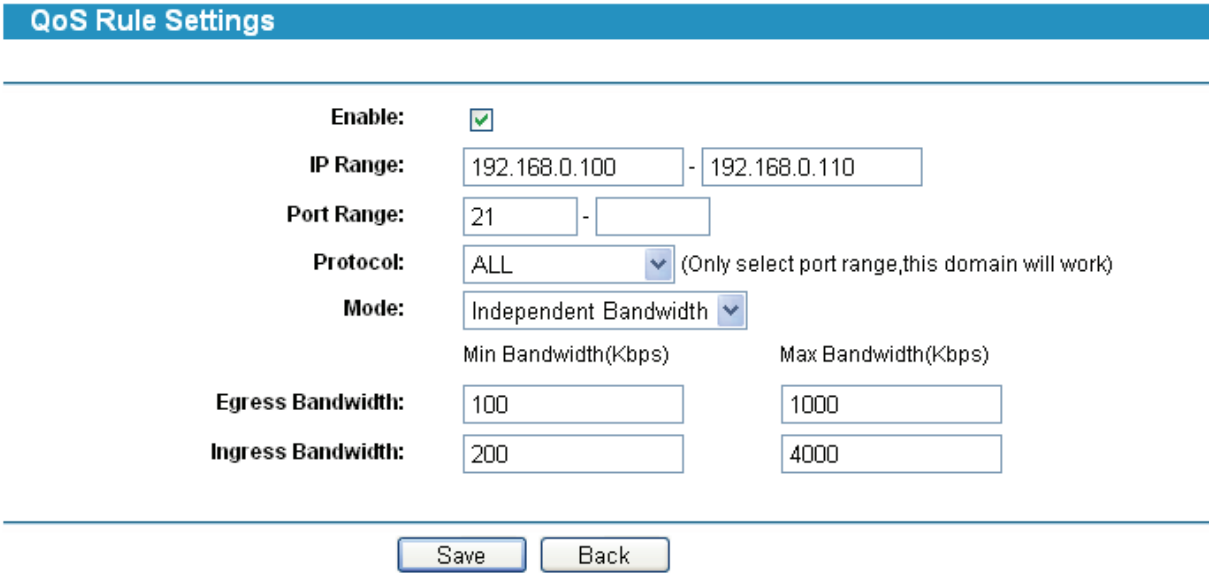


Figure 4-49

- **Description -** This is the information about the rules such as address range.
- **Mode -** Mode can be separated into "independent bandwidth" and "share bandwidth". Independent bandwidth means every port has its own upload and download bandwidth, share bandwidth means address or port share upload and download bandwidth.
- **Egress bandwidth -** This field displays the max and mix upload bandwidth through the WAN port, the default is 0.
- **Ingress bandwidth -** This field displays the max and mix download bandwidth through the WAN port, the default is 0.
- **Enable -** This displays the status of the rule.
- **Modify -** Click "**Modify**" to edit the rule, click "**Delete**" to delete the rule.

To add/modify a QoS rule:

Step 1: Click **Add New…/Modify** shown in Figure 4-49, you will see a new screen shown in



Step 2: Figure 4-50.

Step 3: Enter the information like the screen shown below.

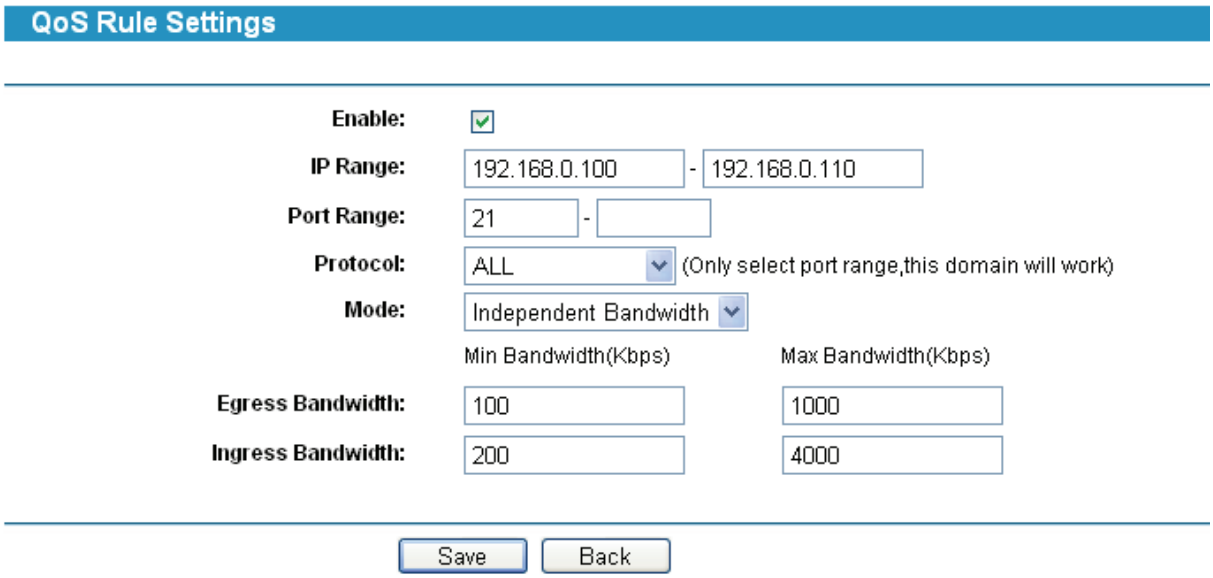


Figure 4-50

Step 4: Click the **Save** button.

4.10 IP & MAC Binding

Choose menu "**IP & MAC Binding**", you can see the submenus under the main menu: **Binding Setting, ARP List**.

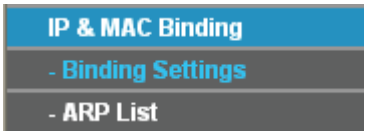


Figure 4-51

Click any of them, and you will be able to configure the corresponding function. The detailed explanations for each submenu are provided below.

4.10.1 Binding Setting

Choose menu "**IP & MAC Binding→Binding Setting**", you can view and add IP & MAC binding entries in the next screen (shown in Figure 4-52).

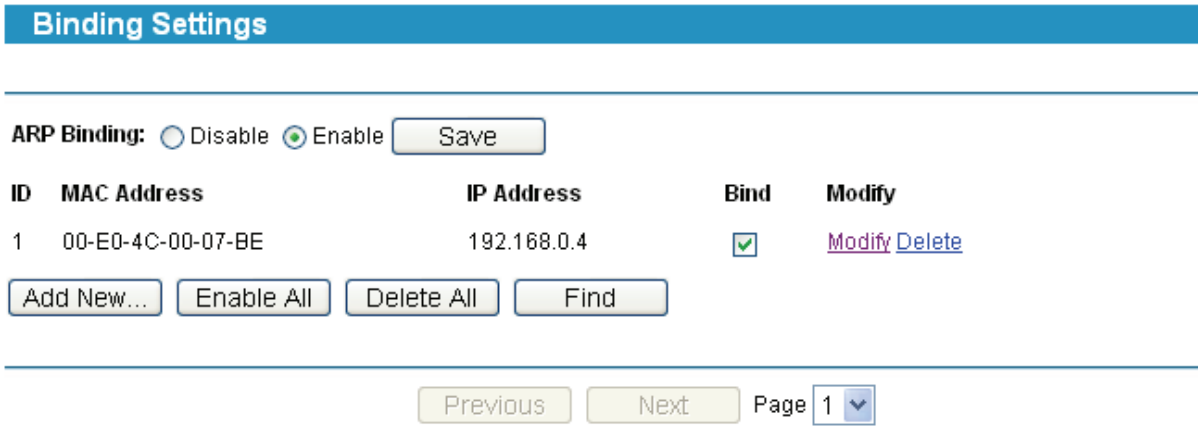
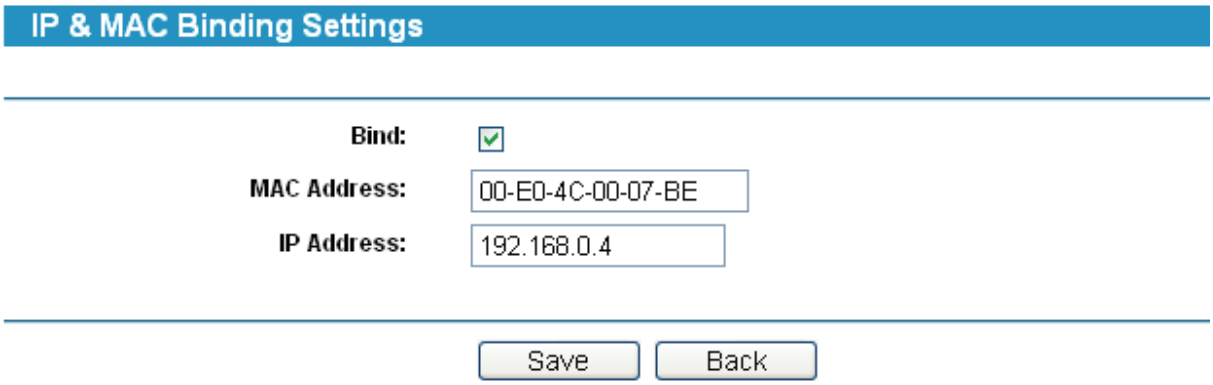


Figure 4-52

- **MAC Address -** This field displays the MAC address of the controlled computer in the LAN.
- **IP Address -** This field displays the assigned IP address of the controlled computer in the LAN.
- **Bind -** Select whether enable the ARP binding or not. Only bind the MAC address and IP address can the function take effect.

To add/modify an IP & MAC binding entry:

Step 1: Click **Add New…/Modify** shown in Figure 4-52, you will see a new screen shown in



Step 2: Figure 4-53.

Step 3: Enter the MAC Address and IP Address in the corresponding field.

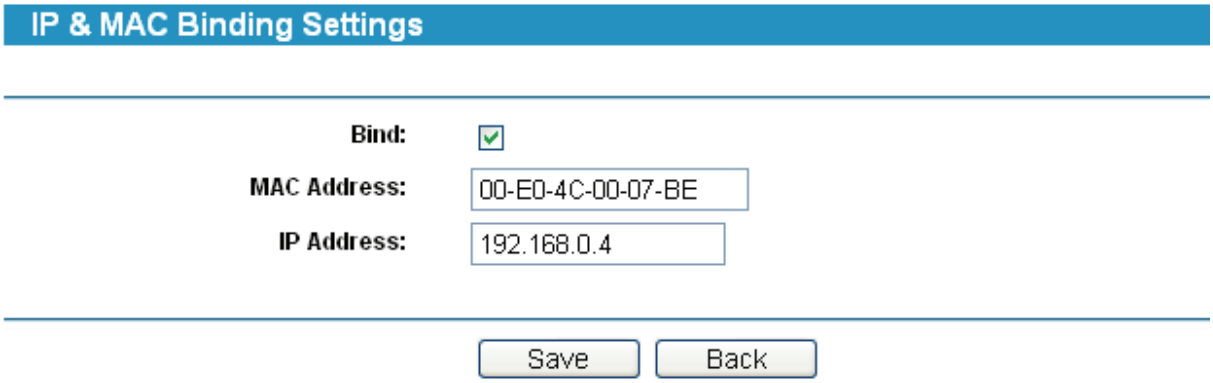


Figure 4-53

Step 4: Select **Bind** the MAC and IP address, and then click **Save** button to save the configuration.

To find a specific IP & MAC binding entry:

Step 1: Click **Find** shown in Figure 4-52, you will see a new screen shown in Figure 4-54.

Step 2: Enter the specific MAC Address or IP Address in the corresponding field.

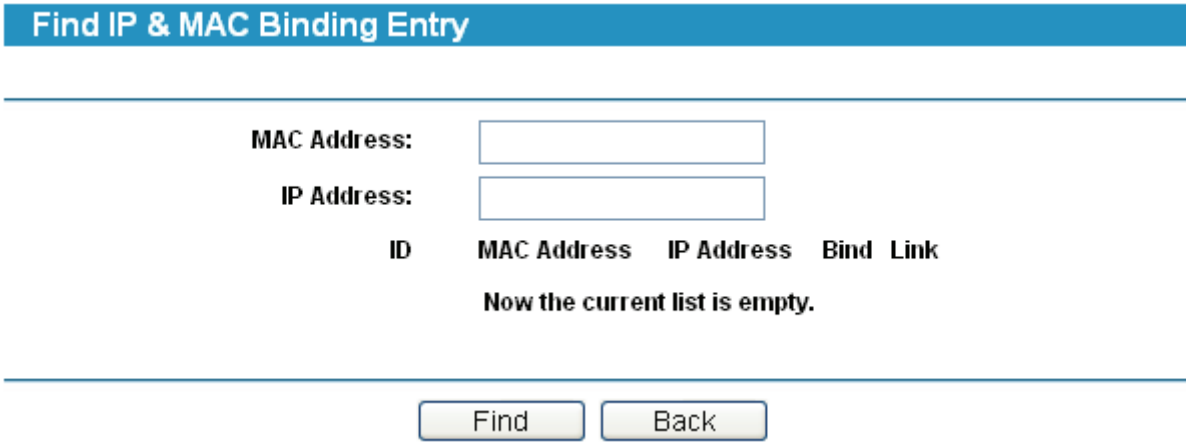
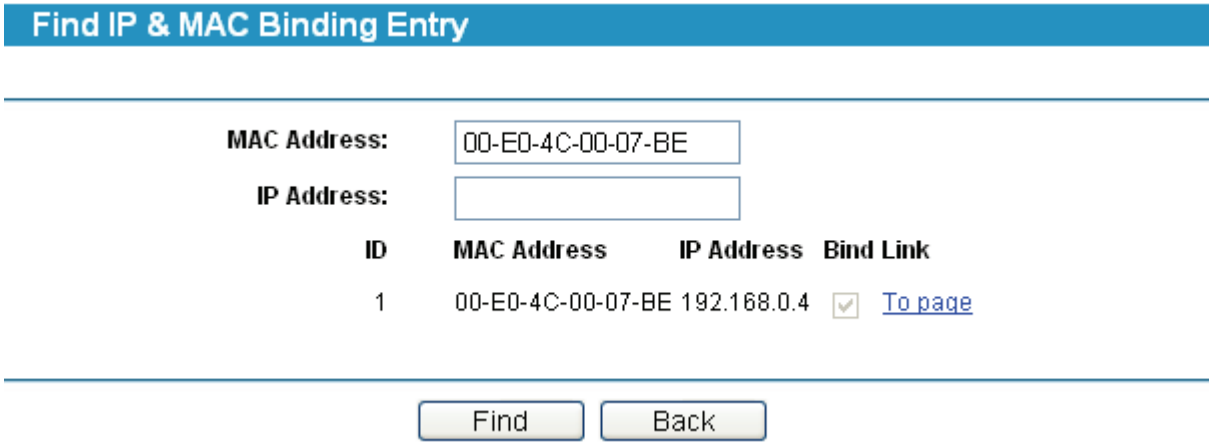


Figure 4-54

Step 3: Click **Find** button, then you will see the entry with the specific MAC address or IP address.



Step 4: Click **Back** to return the previous screen.

Note:

You can click "to page" to edit the entry in the corresponding screen.

Other configurations for the entries as shown in Figure 4-52:

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

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

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

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

4.10.2 ARP List

Choose menu "**IP & MAC Binding→ARP List**", you can view the ARP list in the next screen (shown in Figure 4-55). This screen displays the ARP list, it shows all the existing IP & MAC Binding entries.

To manage the computer, you could observe the computers in the LAN by checking the relationship of MAC address and IP address on the ARP list, and you could configure the items on the ARP list also.

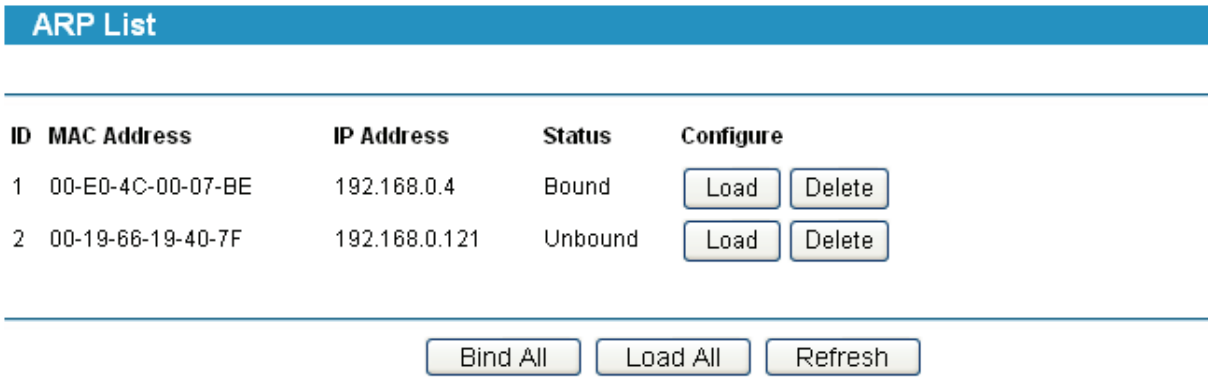


Figure 4-55

Click **Load** to load the specific item to the IP & MAC Binding list (shown in Figure 4-52).

Click **Delete** to load the specific item to the IP & MAC Binding list.

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

Click the **Load All** button to load all items to the IP & MAC Binding list (shown in Figure 4-52).

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

Note:

An item could not be loaded to the IP & MAC Binding list if the IP address of the item has been loaded before.

4.11 Dynamic DNS

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

The router offers a Dynamic Domain Name System (**DDNS**) feature. DDNS lets you assign a fixed host and domain name to a dynamic Internet IP address. It is useful when you are hosting your own website, FTP server, or other server behind the router. Before using this feature, you need to sign up for DDNS service providers such as www.dyndns.org or www.oray.net or www.comexe.cn or www.no-ip.com. The Dynamic DNS client service provider will give you a password or key.

4.11.1 Dyndns DDNS

If your dynamic DNS Service Provider is www.dyndns.org, you can configure in the next screen (shown in Figure 4-56).

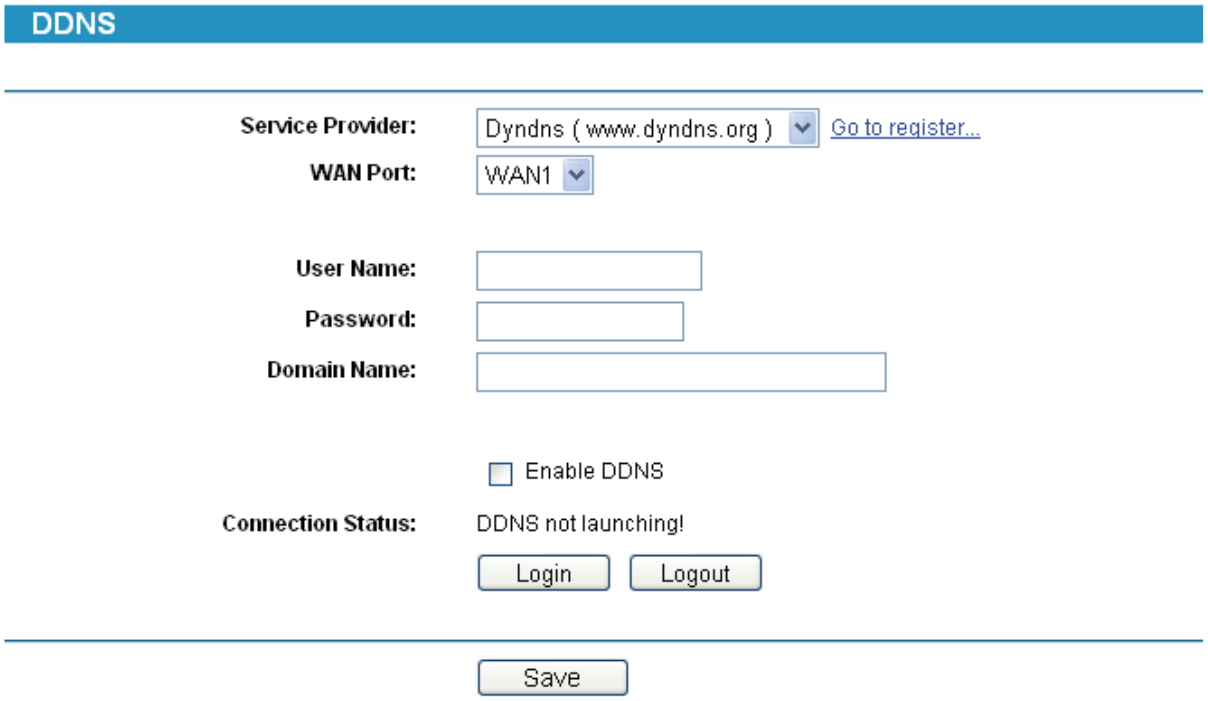


Figure 4-56

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

To set up for Dyndns DDNS, follow these instructions:

Step 1: Select the WAN port to configure.

Step 2: Type the "User Name" and "Password" for your DDNS account.

Step 3: Enter the domain name that your dynamic DNS service provider offers.

Step 4: Enable DDNS, and click **Save** to save the current configuration.

Click **Login** to login the DDNS service.

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

The status of the DDNS service connection is displayed in the **Connection Status** field.

4.11.2 PeanutHull DDNS

If your dynamic DNS Service Provider is www.oray.net, you can configure in the next screen (shown in Figure 4-57).

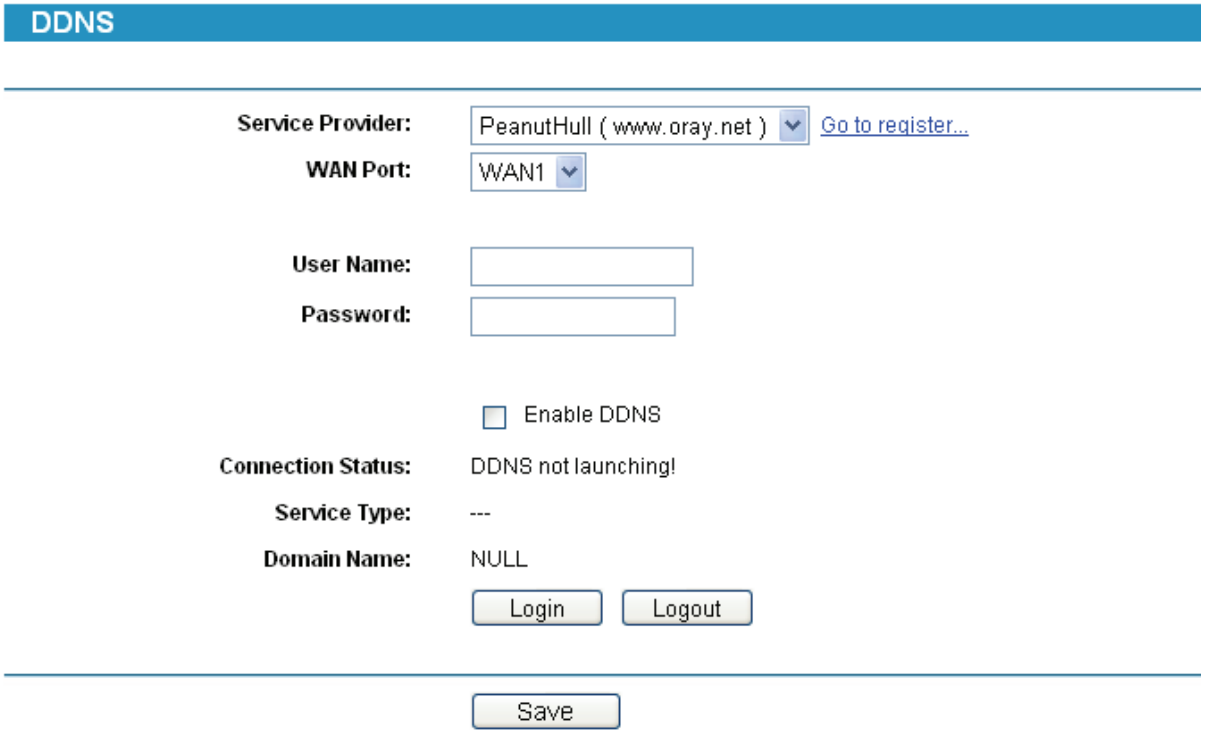


Figure 4-57

To set up for PeanutHull DDNS, follow these instructions:

Step 1: Select the WAN port to configure.

Step 2: Type the User Name and Password for your DDNS account.

Step 3: Enable DDNS, and click **Save** to save the current configuration.

Click the **Login** button to login to the DDNS service.

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

The status of the DDNS service connection is displayed in the **Connection Status** field.

4.11.3 Comexe DDNS

If your dynamic DNS Service Provider is www.comexe.cn, you can configure in the next screen (shown in Figure 4-58).

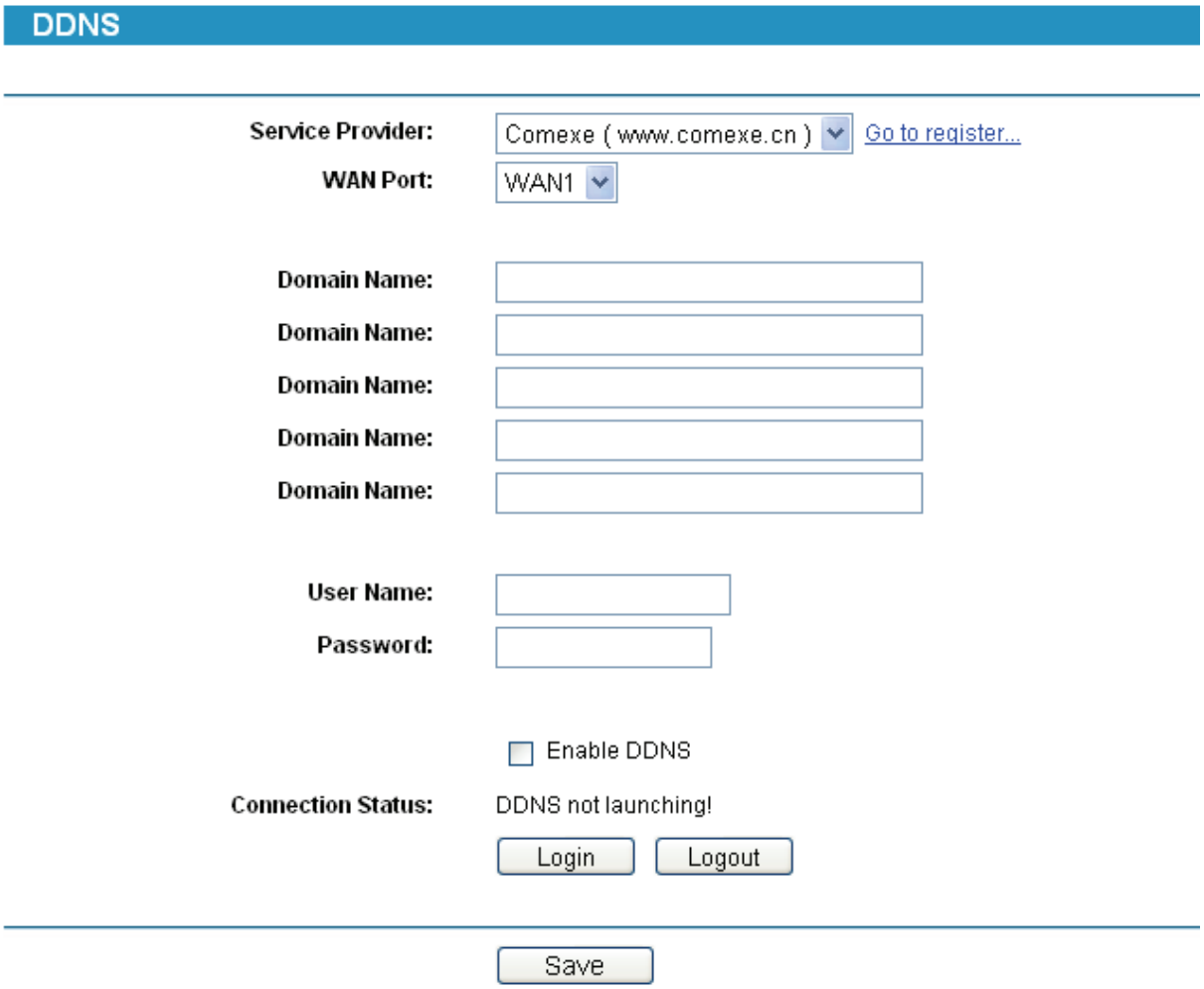


Figure 4-58

To set up for Comexe DDNS, follow these instructions:

Step 1: Select the WAN port to configure.

Step 2: Enter the domain name your dynamic DNS service provider offer.

Step 3: Type the “User Name” and “Password” for your DDNS account.

Step 4: Enable DDNS, and click **Save** to save the current configuration.

Click **Login** to login the DDNS service.

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

The status of the DDNS service connection is displayed in the **Connection Status** field.

4.11.4 No-IP DDNS

If your dynamic DNS Service Provider is www.no-ip.com, you can configure in the next screen (shown in Figure 4-59).

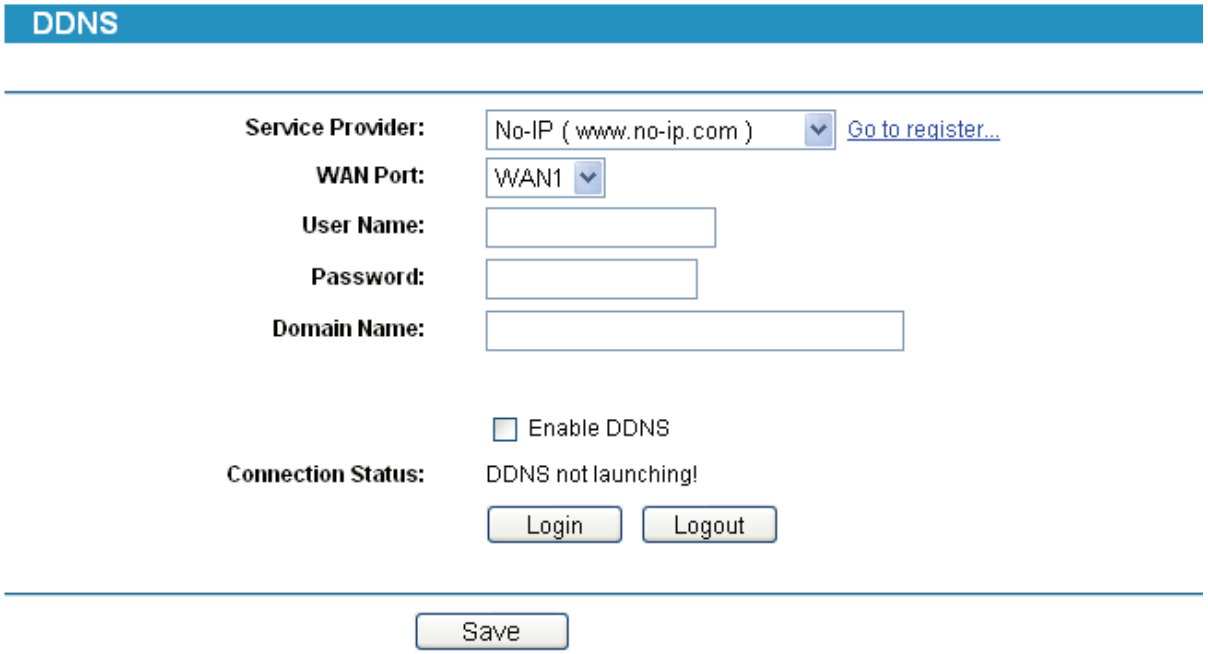


Figure 4-59

To set up for No-IP DDNS, follow these instructions:

Step 1 Select the WAN port to configure.

Step 2 Type the "**User Name**" and "**Password**" for your DDNS account.

Step 3 Enter the **Domain Name** your dynamic DNS service provider offered.

Step 4 Enable DDNS, and click **Save** to save the current configuration.

Click **Login** to login the DDNS service.

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

The status of the DDNS service connection is displayed in the **Connection Status** field.

4.12 Switch Settings

Choose menu "**Switch Settings**", you can see the submenus under the main menu. The submenu "**Port Mirror**" will be hidden when the Router is set to Quad WAN ports mode.

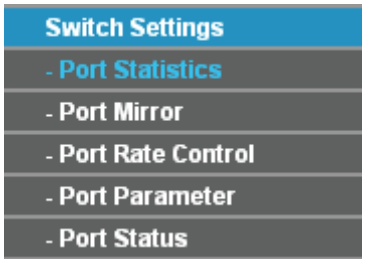


Figure 4-60

Click any of them, and you will be able to configure the corresponding function. The detailed explanations for each submenu are provided below.

4.12.1 Port Statistics

Choose menu "**Switch Setting→Port statistics**", you can view the statistics information about the LAN port in the next screen (shown in Figure 4-61).

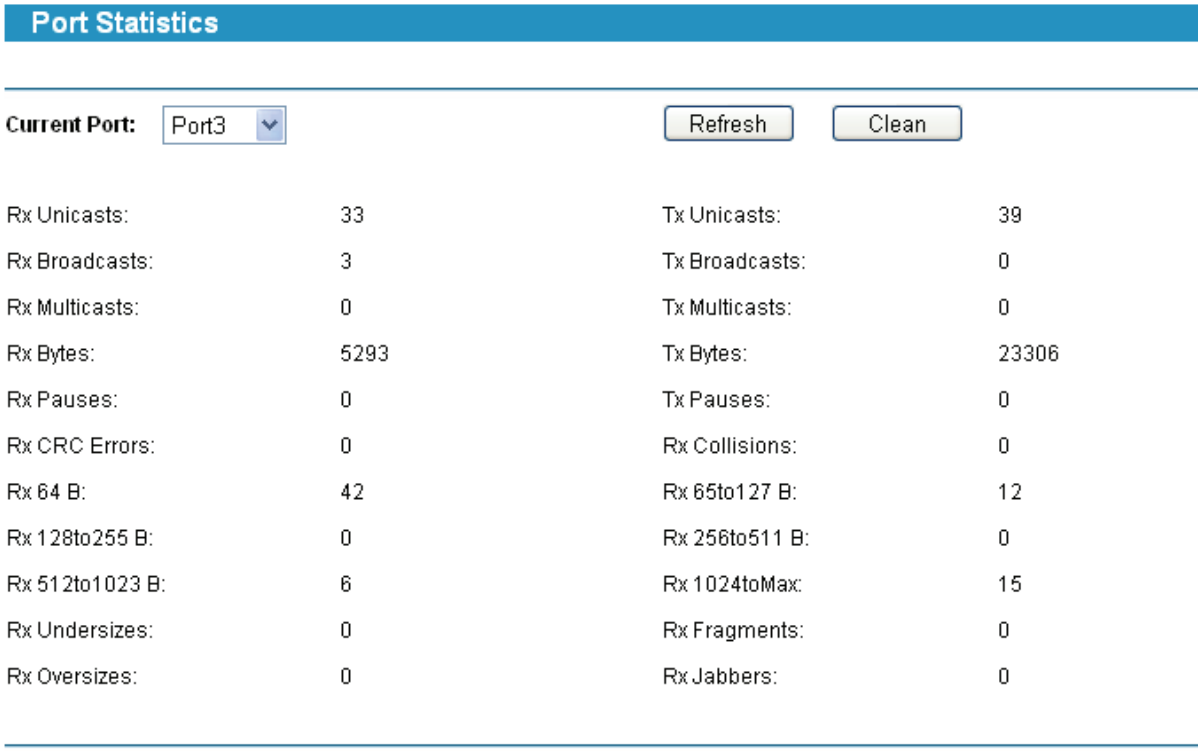


Figure 4-61

Note:

Before you view the information, please click the **Refresh** button to update it.

4.12.2 Port Mirror

Choose menu "**Switch Setting→Port Mirror**", you can configure the Mirror modes, Mirror Port and the Mirrored Ports below.

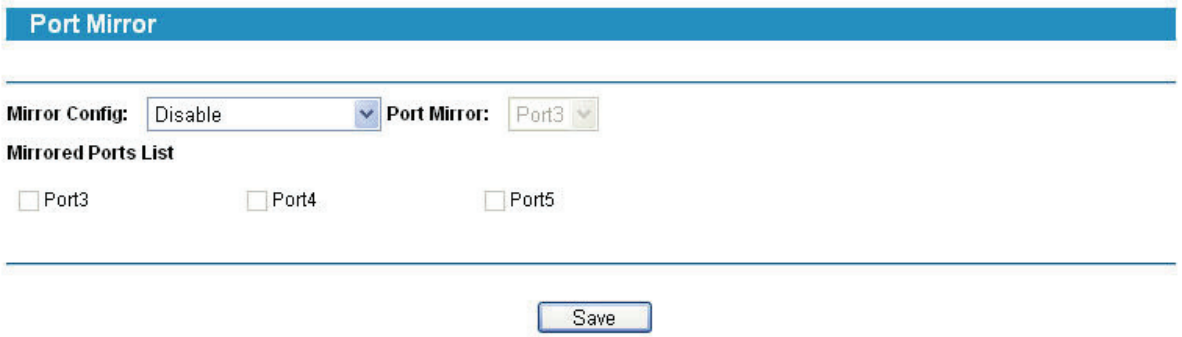


Figure 4-62

- **Mirror Config -** There are three Mirror modes: Disable, Output mirror, Input/Output mirror. The Input/Output mirror option is related to the Router.
- **Port Mirror -** This is the port linked to the mirror computer.
- **Mirrored Ports List -** The option used to select ports to be mirrored.

4.12.3 Port Rate Control

Choose menu "**Switch Setting→Port Rate Control**", you can control the ingress and egress rate for the LAN port in the next screen (shown in Figure 4-63).

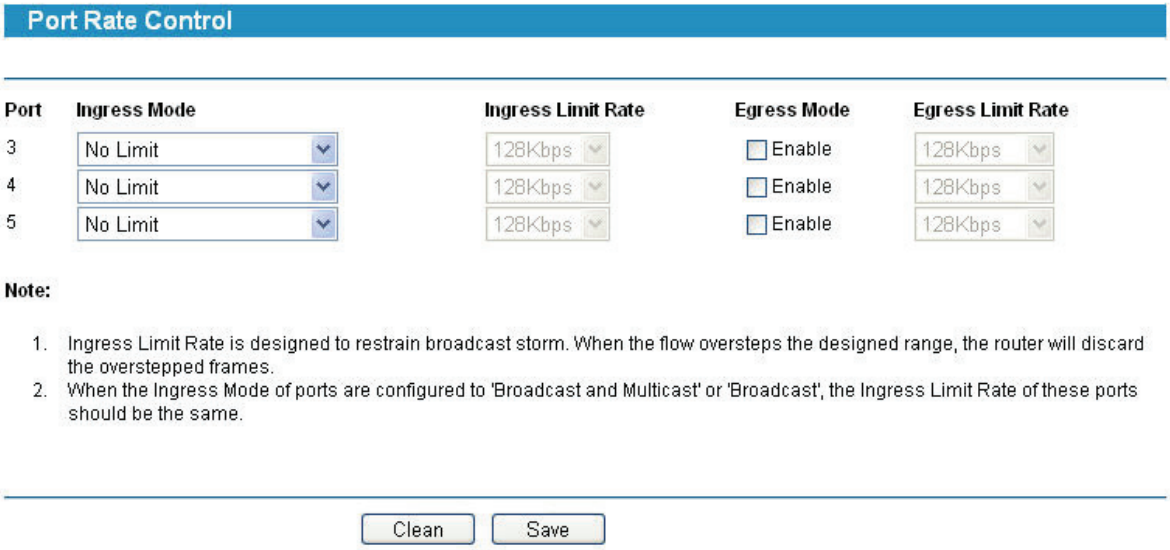


Figure 4-63

- **Port -** Here shows the Router's LAN ports.
- **Ingress Mode -** This option is used to select the limited modes for Ports' import rate.
  - **All Frames -** This means that all import frames will be limited.
  - **Broadcast and Multicast -** This means that broadcast and multicast frames will be limited.
  - **Broadcast -** This means that all broadcast frames will be limited.
  - **No Limit -** This means no limit.
- **Ingress Limit Rate -** This option is used to select the particular import rate.
- **Egress Mode -** This option is used to limit the export rate or not.
- **Egress Limit Rate -** This option is used to select the particular export rate (control all frames).

4.12.4 Port Parameter

Choose menu "**Switch Setting→Port Parameter**", you can configure the parameters for the LAN port in the next screen (shown in Figure 4-64).

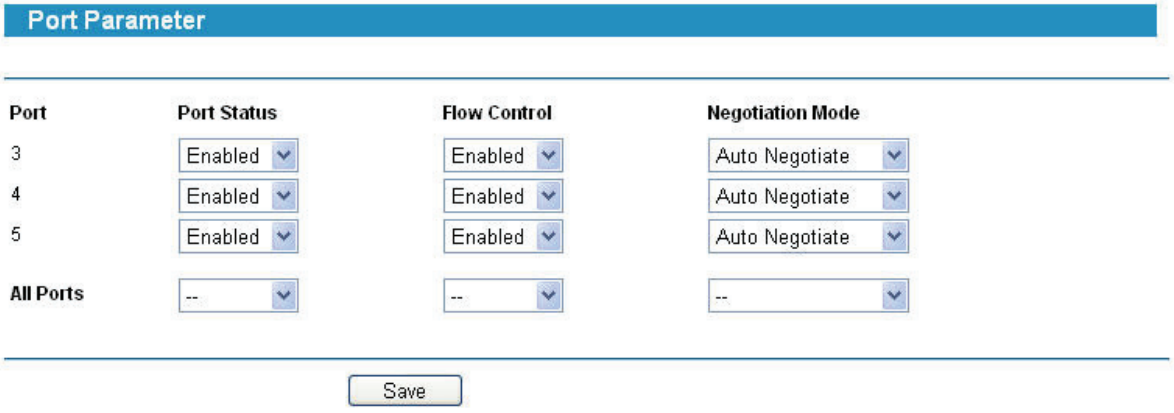


Figure 4-64

- **Port -** Here displays the Router's LAN Ports.
- **Port Status -** There are two statuses- Enabled, Disabled. Enabled (default status) means the ports can be used; Disabled means the ports can't be used.
- **Flow Control -** There are two options- Enabled, Disabled. Enabled means the Flow Control function is adopted; Disabled means the function isn't adopted.
- **Negotiation Mode -** You can select Auto Negotiation, 10M Half Duplex, 10M Full Duplex, 100M Half Duplex, 100M Full Duplex for the negotiation.

4.12.5 Port Status

Choose menu "**Switch Setting→Port Status**", you can view the status of the LAN port in the next screen (shown in Figure 4-65).

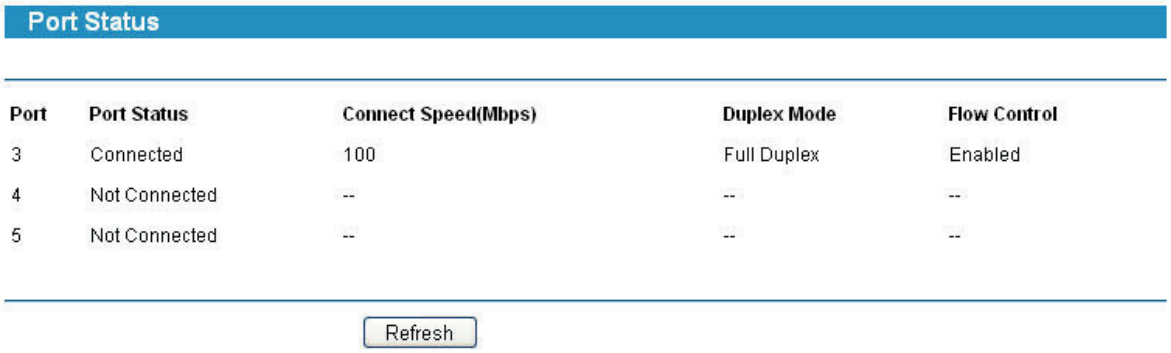


Figure 4-65

- **Port -** This displays the Router's LAN ports.
- **Port Status -** This displays the port's current connection status.
- **Connect Speed (Mbps) -** This displays the port's current connection speed.
- **Duplex Mode -** This displays which duplex mode the ports adopt to communicate, Full Duplex or Half Duplex.
- **Flow Control -** This displays whether the corresponding port adopt Flow Control function. Enable means the function is adopted, Disable means the function is not adopted.

Click the **Refresh** button, the information in the table above will be updated.

4.13 System Tools

Choose menu "**System Tools**", you can see the submenus under the main menu:

Figure 4-66

Click any of them, and you will be able to configure the corresponding function. The detailed explanations for each submenu are provided below.

4.13.1 Time Settings

Choose menu "**System Tools→Time Settings**", you can configure the time on the screen (shown in Figure 4-67).

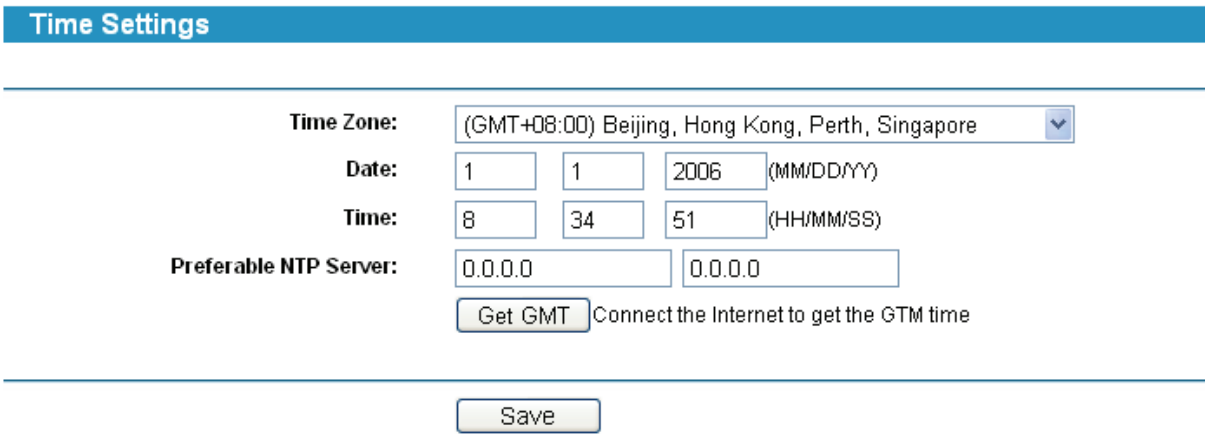


Figure 4-67

- **Time zone -** Select your local time zone from this pull down list.
- **Date -** Enter your local date in MM/DD/YY into the right blanks.
- **Time -** Enter your local time in HH/MM/SS into the right blanks.

To configure the system time manually:

Step 1: Select your local time zone.

Step 2: Enter date and time in the right blanks.

Step 3: Click **Save** to save the configuration.

To configure the system automatically:

Step 1: Enter the address of the preferred NTP server.

Step 2: Click the **Get GMT** button to get system time from Internet if you have connected to the Internet.

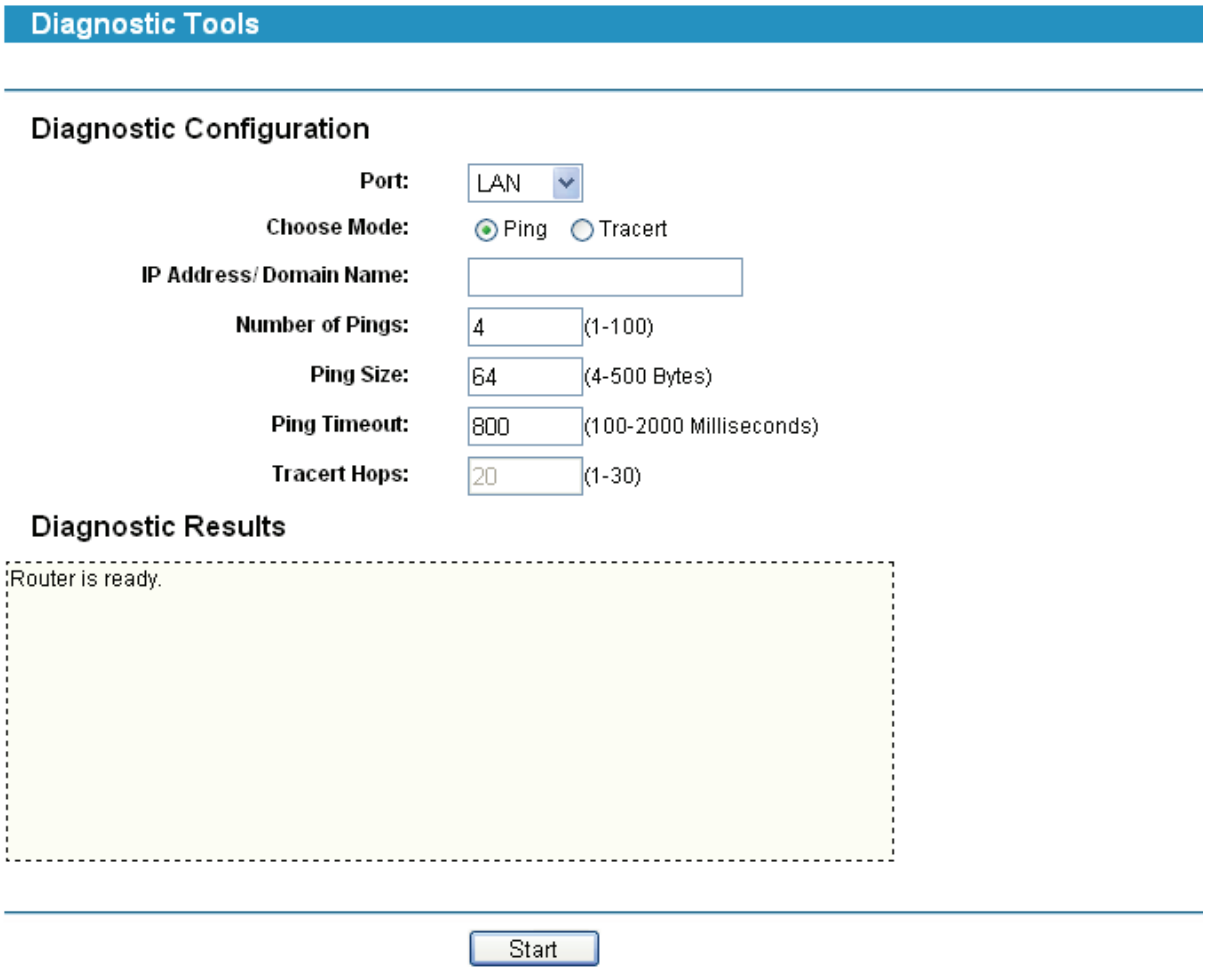
Step 3: Click **Save** to save the configuration.

Note:

1) This setting will be used for some time-based functions such as firewall. You must specify your time zone once you login to the router successfully, or else, the time limited on these functions will not take effect.
2) The time will be lost if the router is turned off.
3) The router will obtain GMT time automatically from Internet if it has already connected to the Internet.

4.13.2 Diagnostic Tools

Choose menu "**System Tools→Diagnostic Tools**", you can test the connectivity between the router and the destination on this page.



- **Port -** Select the **LAN** or **WAN** port to test.
- **Choose Mode -** Choose the test mode. **Ping** and **Tracert** modes are available.
- **IP address/Domain Name -** Enter destination IP address or Domain name here.
- **Number of Pings** - Indicates the ping times in one submission.
- **Ping Size** - Indicates the data field length of ping packet.

- **Ping Timeout -** Indicates the time before the Ping timeout.
- **Tracert Hops –** Specify the maximum hops of the Tracert here.

Click **Start** to start the test and the result will display in the **Diagnostic Result** table.

Note:

1). Only one user can use these tools at one time.
2). These two functions may take several seconds sometimes, please wait.
3). Options "Number of Pings", "Ping size" and "Ping Timeout" are available for **Ping** function.
4). Option "Tracert Hops" is available for **Tracert** function.

4.13.3 Firmware

Choose menu "**System Tools→Firmware**", you can update the latest version of firmware for the Router on the screen (shown in Figure 4-68).

Figure 4-68

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

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

Step 1: Download a more recent firmware upgrade file from the TP-LINK website (http://www.tp-link.com).

Step 2: Type the path and file name of the update file into the "File" field. Or click the **Browse** button to locate the update file.

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

Note:

1) New firmware versions are posted at http://www.tp-link.com and can be downloaded for free. If the router is not experiencing difficulties, there is no need to download a more recent firmware version, unless the version has a new feature that you want to use.
2) When you upgrade the router's firmware, you may lose its current configurations, so please back up the router's current settings before you upgrade its firmware.
3) Do not turn off the router or press the Reset button while the firmware is being upgraded.

4) The router will reboot after the upgrading has been finished.

4.13.4 Factory Defaults

Choose menu "**System Tools→Factory Defaults**", you can restore the configurations of the Router to factory defaults on the screen (shown in Figure 4-69).

Figure 4-69

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

Note:

1) The default **User Name** is admin.
2) The default **Password** is admin.
3) The default **IP Address** is 192.168.0.1.
4) The default **Subnet Mask** is 255.255.255.0.

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

4.13.5 Backup and Restore

Choose menu "**System Tools→Backup and Restore**", you can save the current configuration of the Router as a backup file and restore the configuration via a backup file (shown in Figure 4-70).

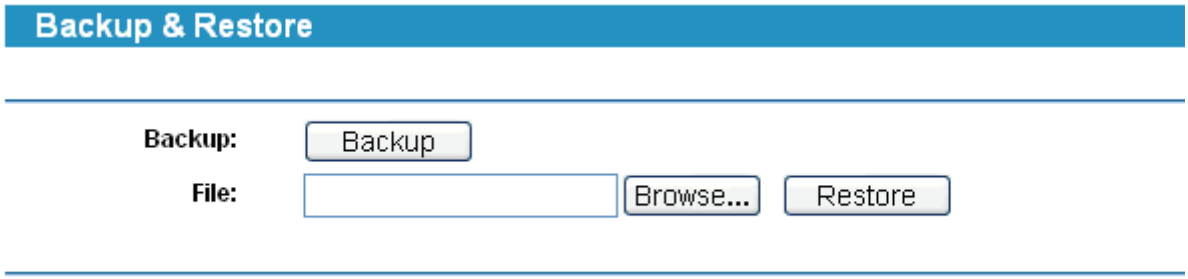


Figure 4-70

To back up the Router's current settings:

Step 1: Click the **Backup** button (shown in Figure 4-70), click **Save** button in the next screen (shown in Figure 4-71) to proceed.

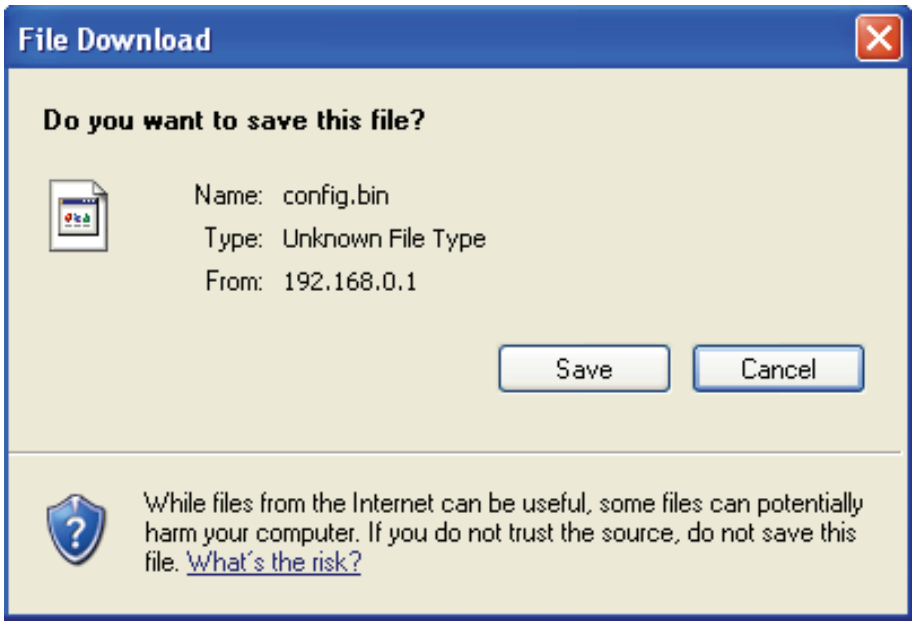


Figure 4-71

Step 2: Save the file as the appointed file (shown in Figure 4-72).

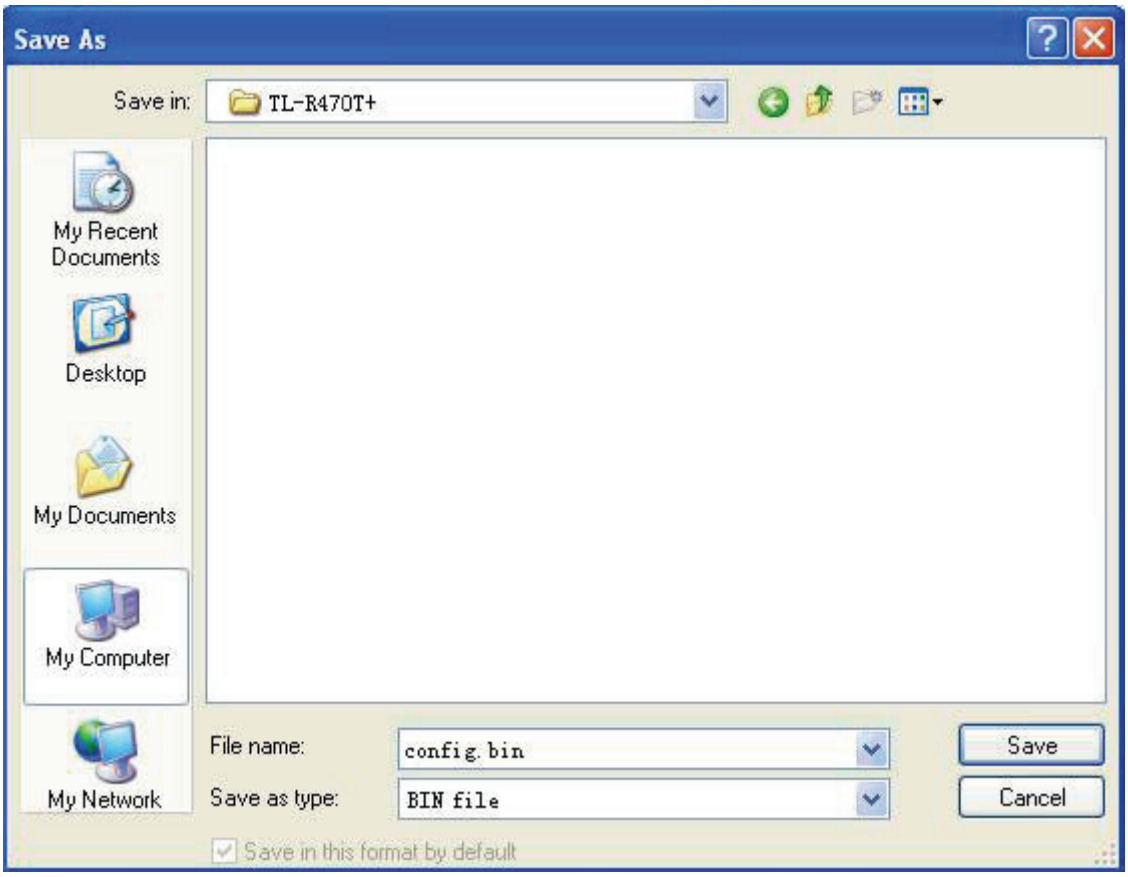


Figure 4-72

To restore the Router's settings:

Step 1: Click the **Browse** button to locate the update file for the device, or enter the exact path to the Setting file in the text box.

Step 2: Click the **Restore** button to complete.

4.13.6 Reboot

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

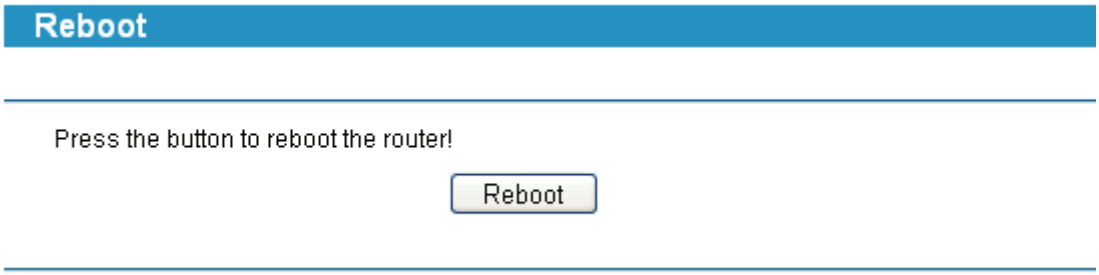


Figure 4-73

Note:

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

1) Change LAN IP Address. (System will reboot automatically)
2) MAC Clone (system will reboot automatically)
3) DHCP service function.
4) Static address assignment of DHCP server.
5) Web Service Port of the router.
6) Upgrade the firmware of the router (system will reboot automatically).
7) Restore the router's settings to factory default (system will reboot automatically).

4.13.7 Password

Choose menu "**System Tools→Password**", you can change the factory default user name and password of the router in the next screen (shown in Figure 4-74). After configuration, click the **Save** button.

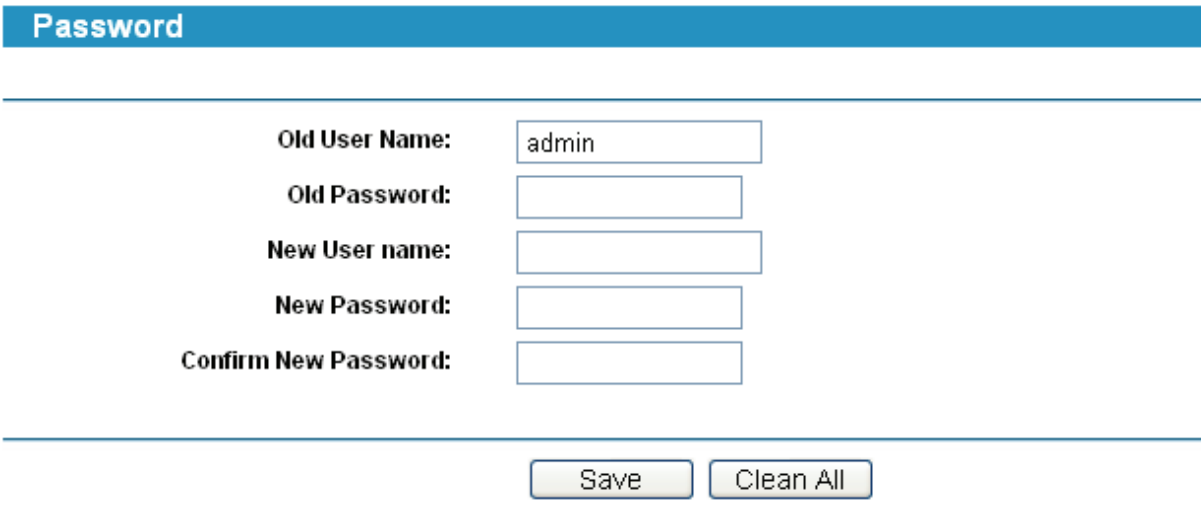


Figure 4-74

Note:

1) It is strongly recommended that you change the factory default user name and password of the router. All users who try to access the router's web-based utility will be prompted for the router's user name and password.
2) The new user name and password must not exceed 14 characters in length and must not include any spaces. Enter the new Password twice to confirm it.
3) You can click the **Clean All** button to clean all the configurations.

4.13.8 System Log

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

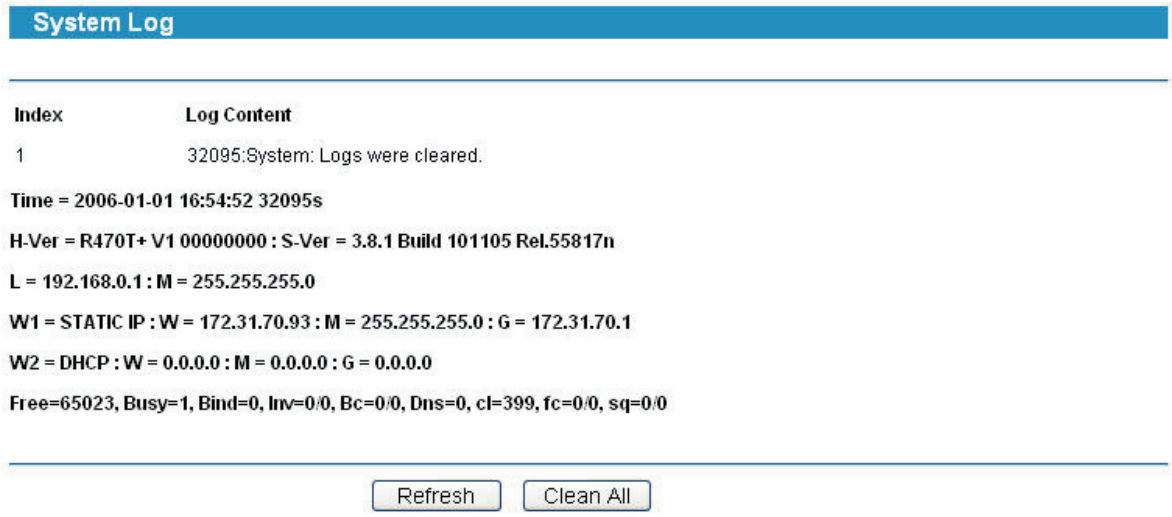


Figure 4-75

The router can keep logs of all traffic. You can query the logs to find what happened to the router.

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

Click the **Clean All** button to clean all the logs.

4.13.9 Remote Management

Choose menu "**Security→Remote Management**", you can configure the Remote Management function on this screen (shown in Figure 4-76). This feature allows you to manage your Router from a remote location via the Internet.

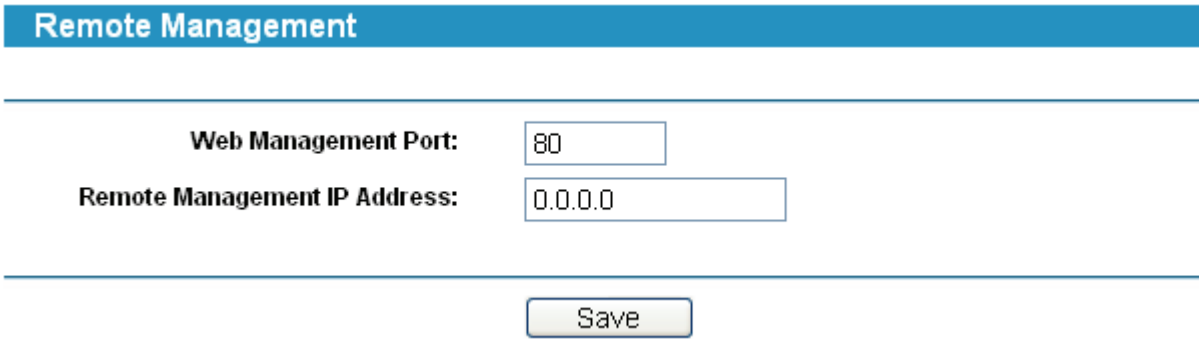


Figure 4-76

- **Web Management Port -** Web browser access normally uses the standard HTTP service port 80. This router's default remote management web port number is 80. For greater

security, you can change the remote management web interface to a custom port by entering that number in the box provided. Choose a number between 1024 and 65534, but do not use the number of any common service port.

- **Remote Management IP Address -** This is the current address you will use when accessing your router from the Internet. The default IP address is 0.0.0.0. It means this function is disabled. To enable this function, change the default IP address to another IP address as desired.

Note:

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

4.13.10 Statistics

Choose menu "**System Tools→Statistics**", you can view the statistics of the Router. This screen (shown in Figure 4-77) displays the network traffic of each PC on LAN, including total traffic and current traffic of the last "Packets Statistic interval" seconds.

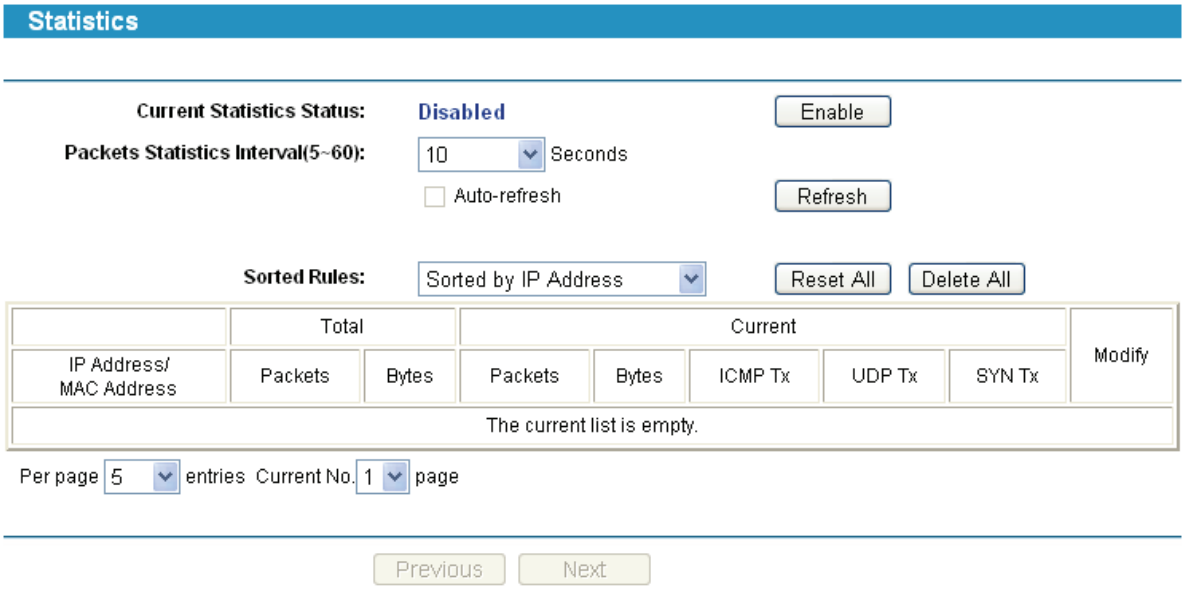


Figure 4-77

- **Current Statistics Status -** Enable or Disable the statistics function. The default status is disabled. Click the **Enable** button to use the function. Click the **Disable** button to disable the function.
- **Packets Statistics Interval -** The default value is 10. Select a value between 5 and 60 seconds in the pull-down list. The Packets Statistic interval value indicates the time section of the packets statistic.
- **Sort Rules -** Select the rule for displaying the traffic information.

➢ **Statistics Table -** This table displays the statistics information about the traffic.

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

☞ **Note:**

1) If the **Current Statistics Status** function is disabled, the DoS protection in **Advanced Security** will be ineffective.
2) Select the **Auto-refresh**, then the traffic information will be refreshed automatically during the Packets Statistics Interval. Click the **Refresh** button to refresh the information in the table immediately.

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

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

Click the **Reset All** button to recount again.

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

4.13.11 IP NAT Table

Choose menu "**System Tools→IP NAT Table**", you will see the IP NAT in the table below:

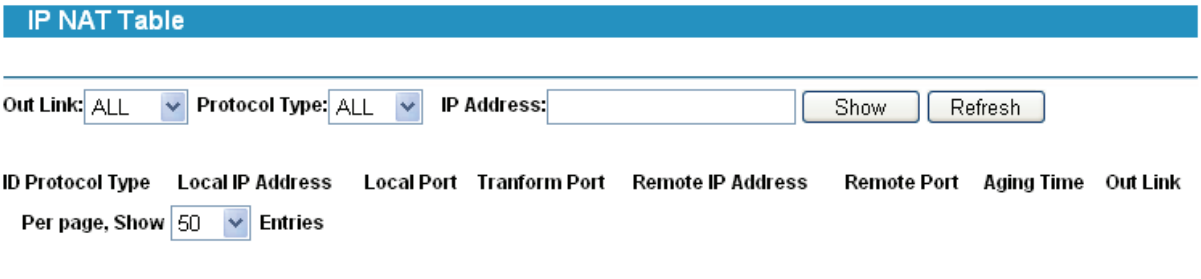


Figure 4-78

➢ **Out Link -** The WAN port which links the router.

➢ **Protocol Type -** The protocol which is used in the link.

- **IP address -** The local or remote IP address to be examined.
- **Show -** To examine the information which the local or remote IP address equals that you input.
- **Refresh -** To get the latest status and settings of the router
- **Per page -** To set how many information entries a page show.

4.13.12 NAT Source Port Settings

Choose menu "**System Tools→NAT Source Port Settings**", you can configure the rang of exterior port for NAT.

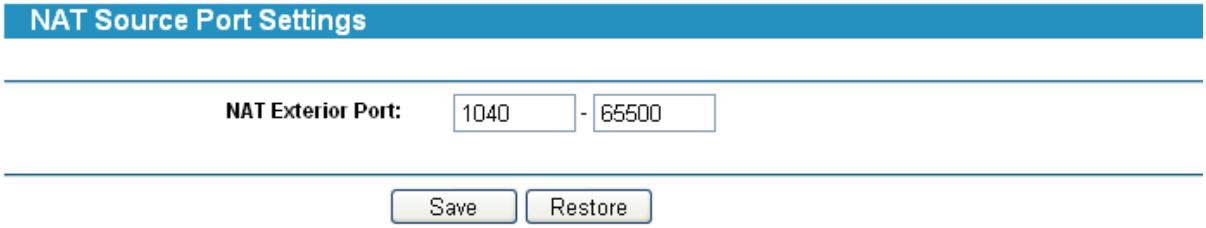


Figure 4-79

Click the **Restore** button to restore the setting to default value- 1040-65500.

Appendix A: Specifications

General	
Standards and Protocols	IEEE 802.3, 802.3u TCP/IP, PPPoE, DHCP, ICMP, NAT, SNTP,HTTP,DNS
Safety & Emission	FCC、CE
Ports	One 10/100M Auto-Negotiation WAN RJ45 port Three adjustable WAN/LAN ports One 10/100M Auto-Negotiation LAN RJ45 port (Auto MDI/MDIX)
Cabling Type	10BASE-T: UTP category 3, 4, 5 cable (maximum 100m) EIA/TIA-568 100Ω STP (maximum 100m) 100BASE-TX: UTP category 5, 5e cable (maximum 100m) EIA/TIA-568 100Ω STP (maximum 100m)
Physical and Environment	
Working Temperature	0℃~40℃ (32℉~104℉)
Working Humidity	10% - 90% RH, Non-condensing

Appendix B: Preventing Lightning

To avoid damage during a lightning storm and ensure a stable performance, our router has adopted the professional lightning protection technology to prevent the lightning. However, although these measures have been taken to protect TL-R470T+ from lightning, if the lightning intensity exceeds a certain range, damage to the router may still happen. To protect the router from lightning better, the following should be considered:

1) Communication cable should be kept indoors as much as possible to reduce the possibility of equipment damage due to lightning.
2) If the Ethernet cable is designed for use indoors, under normal circumstances, should not be used outdoors.
3) Ensure the ground point of the socket of AC power supply is well grounded.
4) To enhance the lightning protection capability of the power supply, a lightning arrester could be installed at the input end of the power supply. Please read the User Manual of the arrester carefully before installing it.
5) As for the signal line to which the interface modules of TL-R470T+ are connected, such as LAN's Ethernet cable, ISDN line, telephone line, E1/T1 line, etc, a special lightning arrester should be installed at the input end of the signal line to enhance the lightning protection capability. Please read the User Manual of the arrester carefully before installing it.

☞ **Note:**

The lightning arrester is not provided with our product. If needed, please self supply the arrester and read the User Manual of the arrester carefully before installing it.

Appendix C: FAQ

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

Step 1: First, configure the ADSL modem in RFC1483 bridge model.

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

Step 3: Login to the router, click the menu **Network→WAN** on the left of your browser. On the WAN screen, select "**PPPoE**" for the type of WAN connection. Then enter the user name and password in the corresponding field, and finish it by clicking **Connect**.

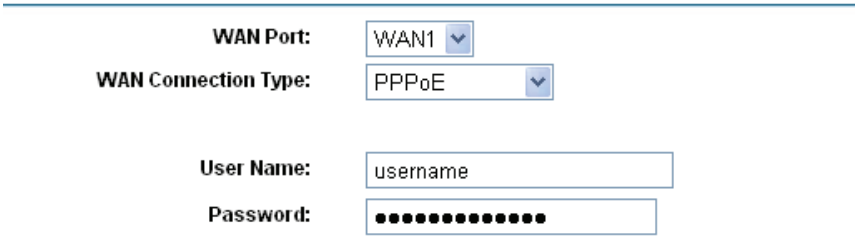


Figure C-1

Step 4: If your ADSL lease is in "**pay-according-time**" mode, select "**Connect on Demand**" or "**Connect Manually**" or "**Time-based Connecting**" for Internet connection mode. Type an appropriate number for "**Max Idle Time**" or "**Period of Time**" to avoid wasting paid time. Otherwise, you can select "**Connect Automatically**" for Internet connection mode.

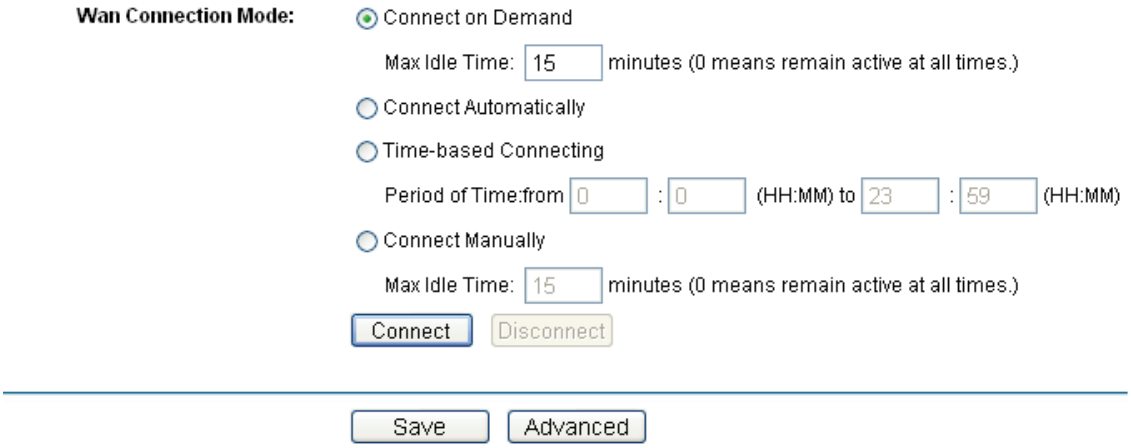


Figure C-2

☞ **Note:**

1) Sometimes the connection can not be disconnected although you specify a time to Max Idle Time, because some applications still visit the Internet continually in the background.
2) If you are a Cable user, please configure the router following the above steps.

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

Step 1: Login to the router, click the menu **Network→WAN** on the left of your browser, On the WAN screen, select "**Dynamic IP**" for "**WAN Connection Type**", and finish it by clicking **Save**.

Step 2: Some ISPs require that you register the MAC address of your adapter, which is connected to your cable or DSL modem during installation. If your ISP requires MAC register, login to the router and click the menu **Network→MAC Clone**. On the MAC Clone screen, if your PC's MAC address is a proper MAC address, click the "**Clone MAC Address**" button and your PC's MAC address will be filled in the "**WAN MAC Address**" field; Or else, enter the specific MAC address into the "**WAN MAC Address**" field manually. Then click the **Save** button. It will take effect after rebooting.

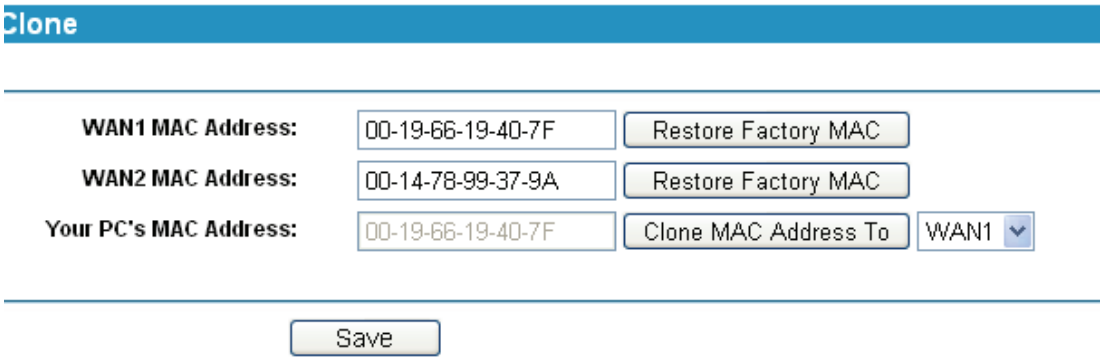


Figure C-3

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

1) If you start a Netmeeting as a host, no configuration is needed but entering the invitee's IP address.

2) If you start a Netmeeting as an invitee, you need to configure Virtual Server or DMZ Host first.

Method one: Use Virtual Server

Login to the router, click the menu **Forwarding→Virtual Servers**. On the Virtual Server screen, add a Virtual Server rule as shown in the next screen: configure 1720 as the "Service Port" and enter your IP address (assuming 192.168.0.102 for an example), then click select the status **Enabled** and click **Save**.

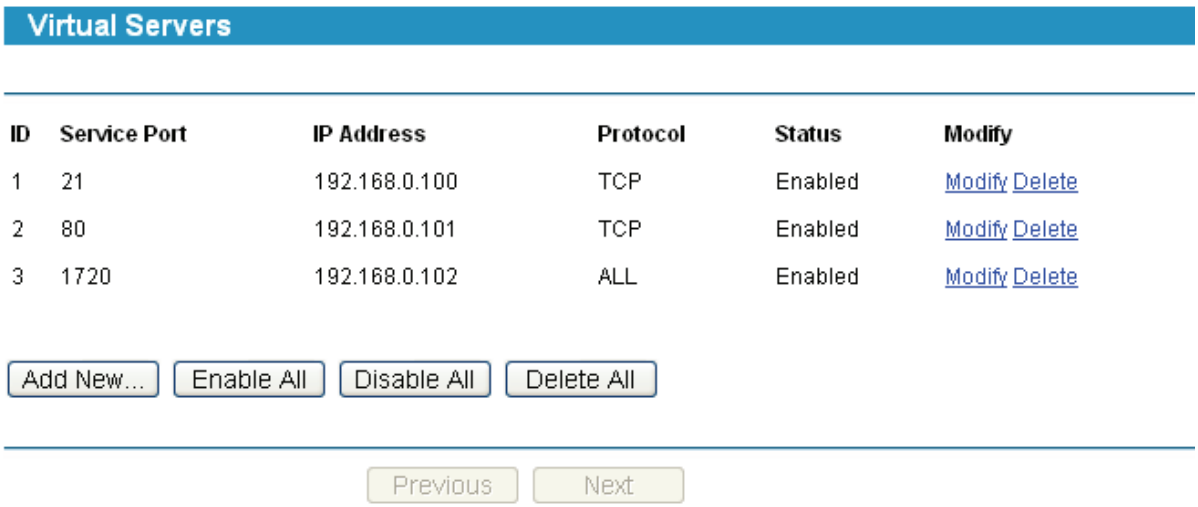


Figure C-4

Note:

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

Method two: Use DMZ Host

Login to the router, click the menu **Forwarding→DMZ**. On the DMZ screen, select “Enable”, and enter your IP address into the “DMZ Host IP Address” field (using 192.168.0.102 as an example), then to click the **Save** button.

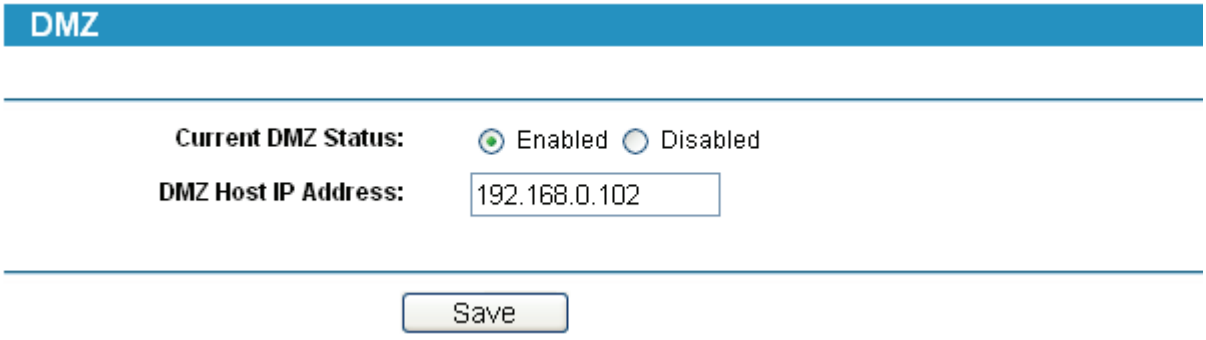


Figure C-5

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

Because the WEB Server port 80 will interfere with the WEB management port 80 on the router, you must change the WEB management port number to avoid interference. And then add a WEB Server on your LAN. You can follow the steps below to proceed.

Step 1: To change the WEB management port number: Login to the router, click the menu **System Tools→Remote Management**. On the Remote Management screen, enter a port number except 80 (such as 88) into the "**Web Management Port**" field. Click **Save** and the router will reboot.

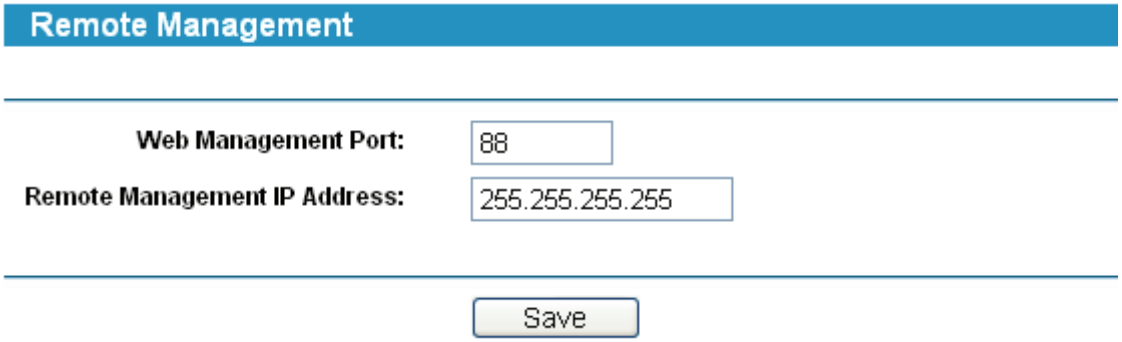
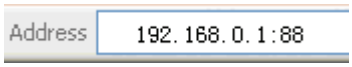


Figure C-6

Note:

If the above configuration takes effect, you should login the Router by entering http://192.168.0.1:88 (the router's LAN IP address: Web Management Port) in the address field of the web browser.



Step 2: To add a WEB Server: Login to the router, click the menu **Forwarding→Virtual Servers** on the left of your browser, On the Virtual Server screen, add a Virtual Server rule as shown in the next screen: configure "80" as the "**Service Port**", and enter your IP address (assuming 192.168.0.188 for an example), remember to "**Enable**" and "**Save**".

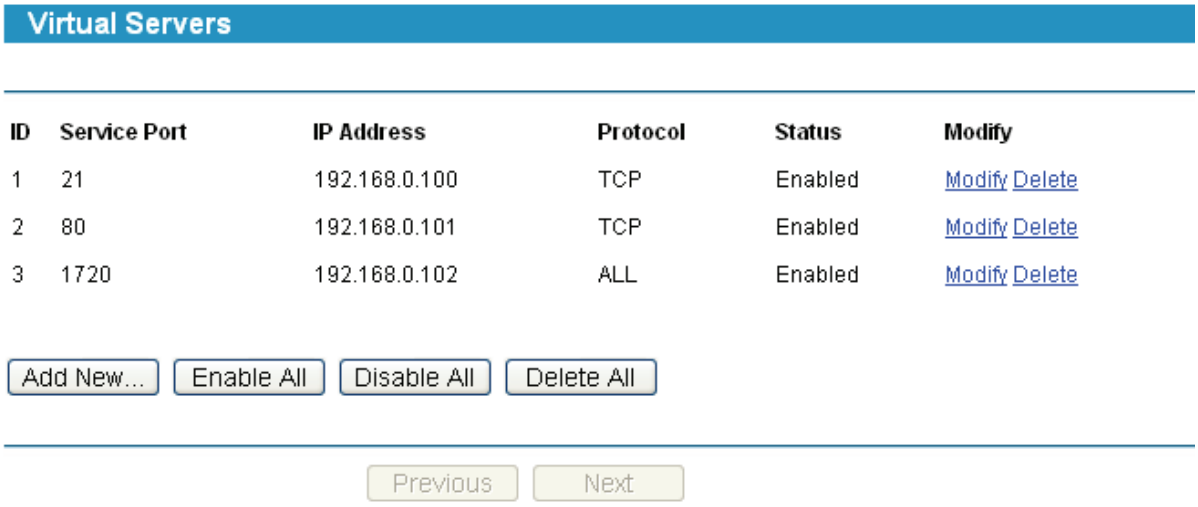


Figure C-7

Appendix D: Glossary

- **DDNS** (**D**ynamic **D**omain **N**ame **S**ystem) **-** The capability of assigning a fixed host and domain name to a dynamic Internet IP address.
- **DHCP** (**D**ynamic **H**ost **C**onfiguration **P**rotocol) **-** A protocol that automatically configure the TCP/IP parameters for the all the PCs that are connected to a DHCP server.
- **DMZ** (**D**emilitarized **Z**one) **-** A Demilitarized Zone allows one local host to be exposed to the Internet for a special-purpose service such as Internet gaming or videoconferencing.
- **DNS** (**D**omain **N**ame **S**erver) **-** An Internet Server that translates the names of websites into IP addresses.
- **Domain Name -** A descriptive name for an address or group of addresses on the Internet.
- **DoS (Denial of Service) -** A hacker attack designed to prevent your computer or network from operating or communicating.
- **DSL** (**D**igital **S**ubscriber **L**ine) **-** A technology that allows data to be sent or received over existing traditional phone lines.
- **ISP** (**I**nternet **S**ervice **P**rovider) **-** A company that provides access to the Internet
- **MTU** (**Maximum Transmission Unit**) **-** The size in bytes of the largest packet that can be transmitted.
- **NAT** (**N**etwork **A**ddress **T**ranslation) **-** NAT technology translates IP addresses of a local area network to a different IP address for the Internet.
- **PPPoE** (**P**oint to **P**oint **P**rotocol **o**ver **E**thernet) **-** PPPoE is a protocol for connecting remote hosts to the Internet over an always-on connection by simulating a dial-up connection.