User Guide

Load Balance Broadband Router

TL-R480T+

REV8.0.0

1910011924

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

CE

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.

Продукт сертифіковано згідно с правилами системи УкрСЕПРО на відповідність вимогам нормативних документів та вимогам, що передбачені чинними законодавчими актами України.

Industry Canada Statement

CAN ICES-3 (A)/NMB-3(A)

Safety Information

- When product has power button, the power button is one of the way to shut off the product; When there is no power button, the only way to completely shut off power is to disconnect the product or the power adapter from the power source.
- Don't disassemble the product, or make repairs yourself. You run the risk of electric shock and voiding the limited warranty. If you need service, please contact us.
- Avoid water and wet locations.

安全諮詢及注意事項

- 請使用原裝電源供應器或只能按照本產品注明的電源類型使用本產品。
- 清潔本產品之前請先拔掉電源線。請勿使用液體、噴霧清潔劑或濕布進行清潔。
- 注意防潮，請勿將水或其他液體潑灑到本產品上。
- 插槽與開口供通風使用，以確保本產品的操作可靠並防止過熱，請勿堵塞或覆蓋開口。
- 請勿將本產品置放於靠近熱源的地方。除非有正常的通風，否則不可放在密閉位置中。
- 請不要私自打開機殼，不要嘗試自行維修本產品，請由授權的專業人士進行此項工作。

此為甲類資訊技術設備，于居住環境中使用時，可能會造成射頻擾動，在此種情況下，使用者會被要求採取某些適當的對策。

Explanation of the symbols on the product label

Symbol	Explanation
	AC voltage
	RECYCLING This product bears the selective sorting symbol for Waste electrical and electronic equipment (WEEE). This means that this product must be handled pursuant to European directive 2012/19/EU in order to be recycled or dismantled to minimize its impact on the environment. User has the choice to give his product to a competent recycling organization or to the retailer when he buys a new electrical or electronic equipment.

CONTENTS

Package Contents **1**

Chapter 1 About this Guide **2**

1.1 Intended Readers 2

1.2 Conventions 2

1.3 Overview of this Guide 2

Chapter 2 Introduction **4**

2.1 Overview of the Router 4

2.2 Appearance 5

2.2.1 Front Panel 5

2.2.2 Rear Panel 6

Chapter 3 Quick Installation Guide **7**

3.1 Configure PC 7

3.2 Login 8

Chapter 4 Configuration **14**

4.1 Status 14

4.2 Quick Setup 15

4.3 Network 15

4.3.1 WAN 15

4.3.2 LAN 32

4.3.3 IPTV 36

4.3.4 MAC Address 37

4.3.5 Switch 38

4.4 User Group 45

4.4.1 Group 45

4.4.2 User 46

4.4.3 View 47

4.5 Advanced 48
4.5.1 NAT 48
4.5.2 Traffic Control 58
4.5.3 Session Limit 62
4.5.4 Load Balance 64
4.5.5 Routing 69
4.6 Firewall 72
4.6.1 Anti ARP Spoofing 72
4.6.2 Attack Defense 76
4.6.3 MAC Filtering 77
4.6.4 Access Control 78
4.6.5 App Control 84
4.7 Services 86
4.7.1 PPPoE Server 86
4.7.2 E-Bulletin 92
4.7.3 Dynamic DNS 94
4.7.4 UPnP 100
4.8 Maintenance 101
4.8.1 Admin Setup 101
4.8.2 Management 105
4.8.3 SNMP 108
4.8.4 Statistics 109
4.8.5 Diagnostics 110
4.8.6 Time 113
4.8.7 Logs 115
4.8.8 NAT Table 117
Appendix A Hardware Specifications 119
Appendix B FAQ 120

Appendix C Glossary 122

Package Contents

The following items should be found in your package:

- One TL-R480T+ Load Balance Broadband Router
- One Power Cord
- One Console Cable
- One Ethernet Cable
- Installation Guide
- Mounting kits for installing in a standard 19-inch rack
- Resource CD

Note:

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

Chapter 1 About this Guide

This User Guide contains information for setup and management of TL-R480T+ Load Balance Broadband Router. Please read this guide carefully before operation.

1.1 Intended Readers

This Guide is intended for Network Engineer and Network Administrator.

1.2 Conventions

In this Guide the following conventions are used:

- The router or TL-R480T+ mentioned in this Guide stands for TL-R480T+ Load Balance Broadband Router without any explanation.
- **Menu Name→Submenu Name→Tab page** indicates the menu structure. **Advanced→NAT →Basic NAT** means the Basic NAT page under the NAT menu option that is located under the Advanced menu.
- **Bold font** indicates a toolbar icon, menu or menu item.
- <Font> indicate a button.

Symbols in this Guide:

Symbol	Description
Note:	Ignoring this type of note might result in a malfunction or damage to the device.
Tips:	This format indicates important information that helps you make better use of your device.

1.3 Overview of this Guide

Chapter 1 About This Guide	Introduces the guide structure and conventions.
Chapter 2 Introduction	Introduces the features and appearance of TL-R480T+ router.
Chapter 3 Quick Installation Guide	Introduces how to log in and set up the router.
Chapter 4 Configuration	Introduces how to configure the router via Web management page.
Appendix A Hardware Specifications	Lists the hardware specifications of this router.

Appendix B FAQ	Provides the possible solutions to the problems that may occur during the installation and operation of the router.
Appendix C Glossary	Lists the glossary used in this guide.

Chapter 2 Introduction

Thanks for choosing the Load Balance Broadband Router TL-R480T+.

2.1 Overview of the Router

The Load Balance Broadband Router TL-R480T+ from TP-LINK possesses excellent data processing capability and multiple powerful functions including Load Balance, Access Control, Bandwidth Control, IGMP Proxy, Session Limit, PPPoE Server and so on, which consumedly meet the needs of small and medium enterprises, hotels and communities with volumes of users demanding an efficient and easy-to-manage network with high security.

- **Powerful Data Processing Capability**

  + Built-in MIPS32 network processor and 64MB DDR high-speed RAM guarantee the stability and reliability for operation.

- **Online Behavior Management**

  + Complete Functions of Access Rules can allow managers to select the network service levels to block or allow applications of FTP downloading, Email, Web browsing and so on.

  + Deploying One-Click restricting of applications to save time & energy.

  + Supporting URL Filtering to prevent potential hazards from visiting the malicious Web sites.

- **Powerful Firewall**

  + Supporting One-Click IP-MAC Binding to avoid ARP spoofing and guarantee a network without stagnation.

  + Featured Attack Defense to protect the network from a variety of flood attacks and packet anomaly attacks.

  + Possessing MAC Filtering function to block the access of illegal hosts.

- **Flexible Traffic Control**

  + Featured Bandwidth Control with flexible bandwidth management to automatically control the bandwidth of the host in bi-direction to avoid bandwidth over occupation, as well as optimize bandwidth usage.

  + Supporting Session Limit to avoid the complaint of a few people to force whole sessions.

- **Multi-WAN Ports**

  + Providing three adjustable WAN/LAN ports for users to configure the amount of WAN ports based on need and connect multiple Internet lines for bandwidth expansion.

  + Supporting multiple Load Balance modes, including Bandwidth Based Balance Routing, Application Optimized Routing, and Policy Routing to optimize bandwidth usage.

+ Featured Link Backup to switch all the new sessions from dropped line automatically to another for keeping an always on-line network.

- **Easy-to-use**

  + Providing easy-to-use GUI with clear configuration steps and detailed help information for the users to configure the router simply.

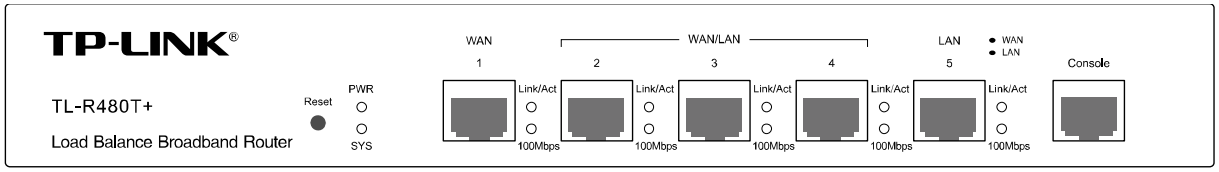
  + Helping administrators to monitor the whole network status and take actions to malfunctions according to the recorded log information.

  + Supporting remote management to manage the router from remote places.

2.2 Appearance

2.2.1 Front Panel

The front panel of TL-R480T+ is shown as the following figure.



- **LEDs**

LED	Status	Indication
PWR	On	The router is powered on.
	Off	The router is powered off or power supply is abnormal.
SYS	Flashing	The router works properly.
	On/Off	The router works improperly.
Link/Act (WAN/LAN)	Off	There is no device linked to the corresponding port.
	On (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.)

LED	Status	Indication
100Mbps (WAN/LAN)	Off	The linked device is running at 10Mbps or no device linked to the corresponding port.
	On (Green/Yellow)	The linked device is running at 100Mbps. (Green light indicates the corresponding port is working as a LAN port, and yellow indicates WAN port.)

- **Interface Description**

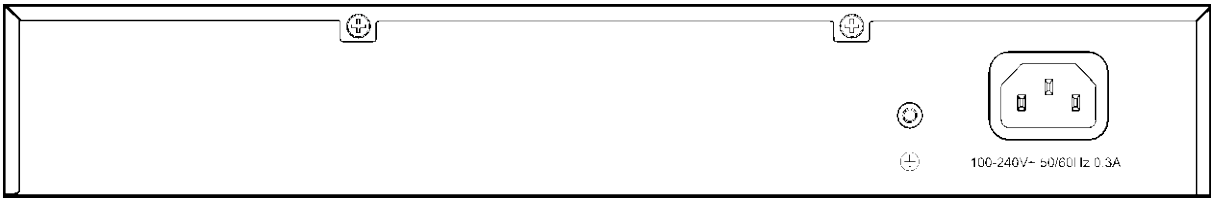
Interface	Port	Description
WAN	1–4	The WAN port is for connecting the router to a DSL/Cable modem or Ethernet by the RJ45 cable.
LAN	2–5	The LAN port is for connecting the router to the local PCs or switches by the RJ45 cable.
Console	/	The Console port is for connecting with the serial port of a computer or terminal to monitor and configure the router.

- **Reset button**

Use the button to restore the router to the factory defaults. With the router powered on, use a pin to press and hold the Reset button (about 5 seconds). If the SYS LED is flashing 5 times in high frequency, release the Reset button. It means the router is restored successfully. The default management address of the router is **http://192.168.0.1**, and the default username and the password are both **admin**.

2.2.2 Rear Panel

The rear panel of TL-R480T+ is shown as the following figure.



- **AC Power Receptacle**

Connect the female connector of the power cord to this power receptacle, and the male connector to the AC power outlet. Please make sure the voltage of the power supply meets the requirement of the input voltage (100-240V~ 50/60Hz).

- **Grounding Terminal**

The router already comes with lightning protection mechanism. You can also ground the router through the PE (Protecting Earth) cable of AC cord or with Ground Cable.

Note:

Please only use the power cord provided with this router.

Chapter 3 Quick Installation Guide

After connecting the TL-R480T+ router into your network, you should configure it. This chapter describes how to configure the basic functions of your TL-R480T+ 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

To log in to the router, the IP address of your PC should be set in the same subnet addresses of the router. The IP address is 192.168.0.x ("x" is any number from 2 to 254), Subnet Mask is 255.255.255.0.

You can also configure the PC to get an IP address automatically from the router.

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 in *ping 192.168.0.1* in the field, 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.

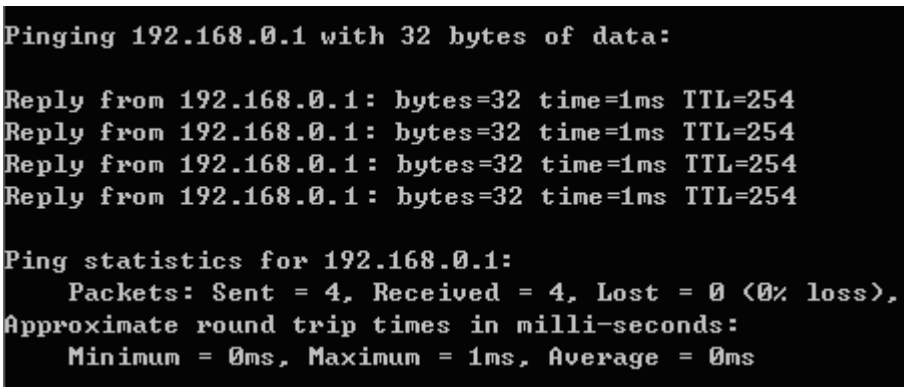


Figure 3-1

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

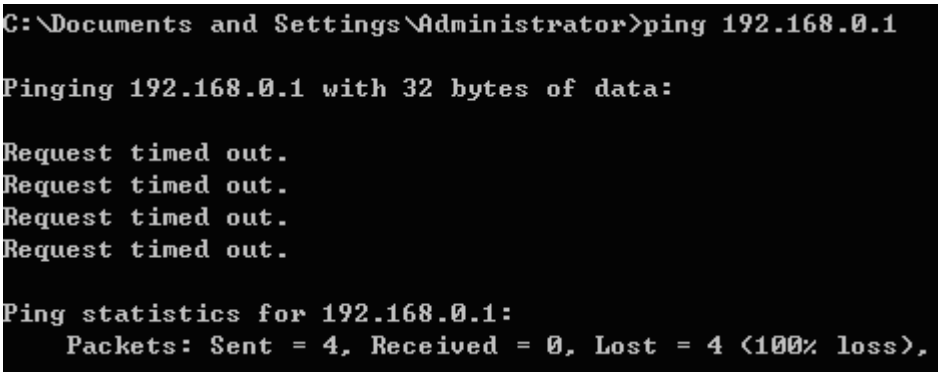


Figure 3-2

You can check it by following the steps below:

Note:

- **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.

- **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 in 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**.

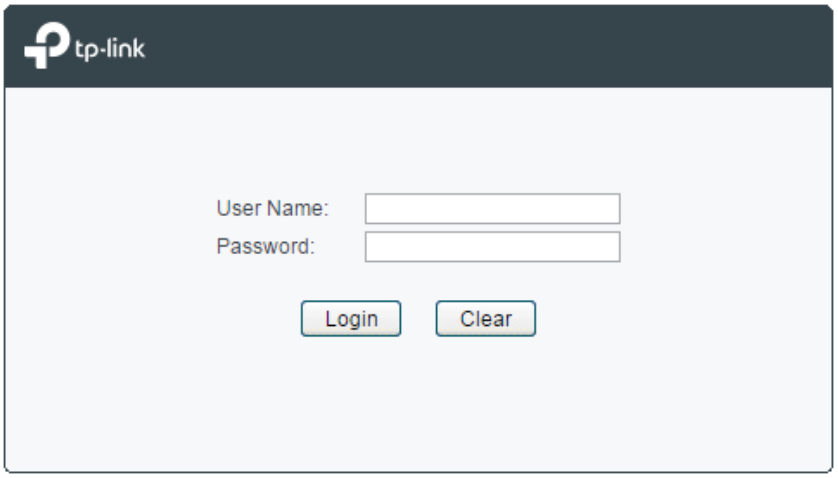


Figure 3-3

After a successful login, the "Quick Setup" screen will pop up as the Figure 3-4 shows. If it does not prompt, you can click the **Quick Setup** on the left of the main menu. Then click <Next>.

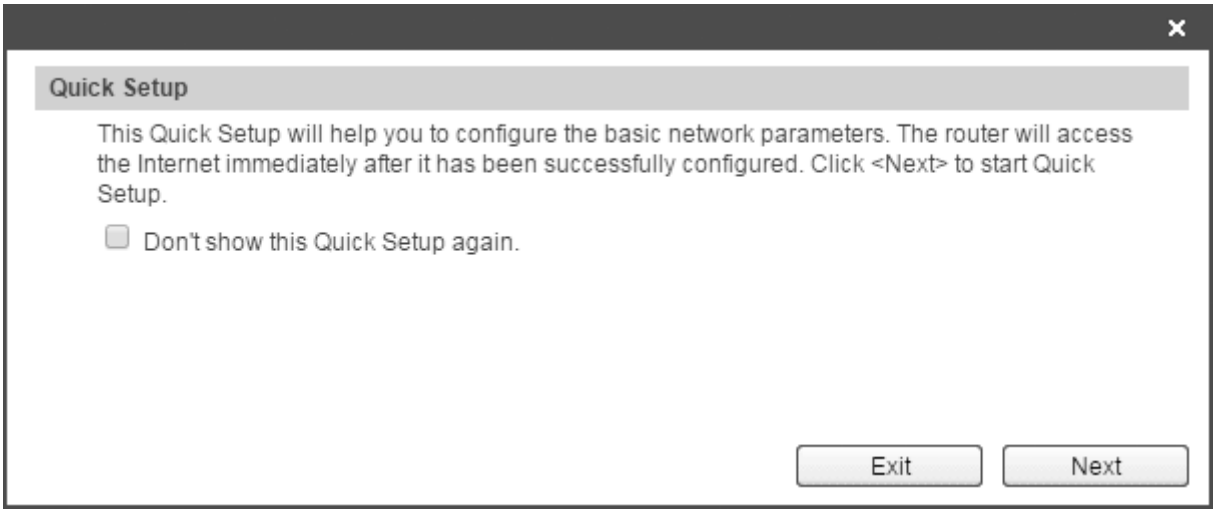


Figure 3-4 Quick Setup

Select the total number of WAN ports you prefer to use as the Figure 3-5 shows. Then click <Next> to load the **WAN Port** screen.

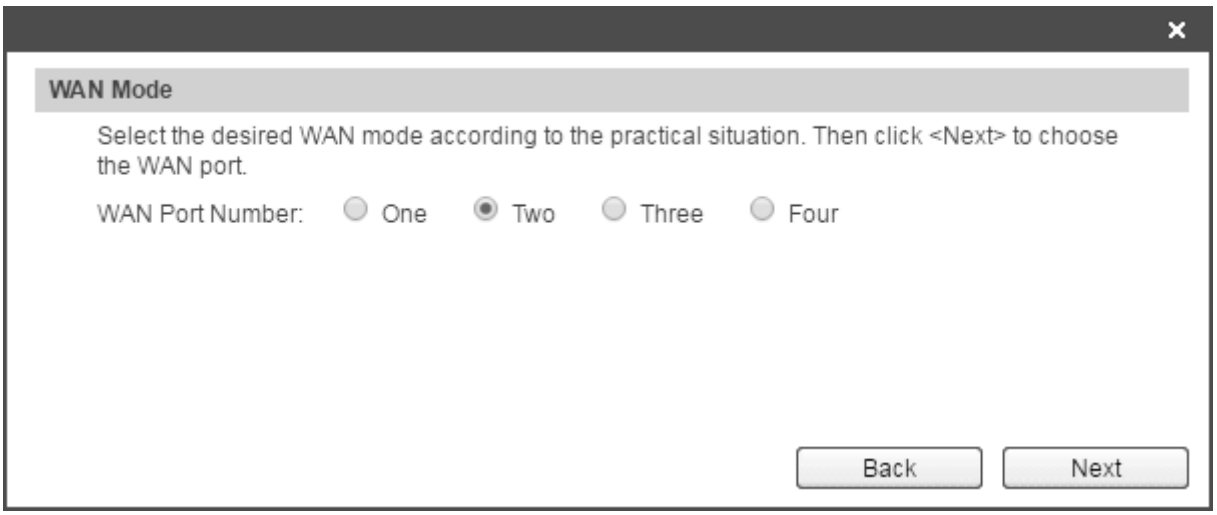


Figure 3-5 WAN Mode

Select the WAN port you want to use as the Figure 3-6 shows, and then click <Next> to load the **WAN Connection Type** screen.

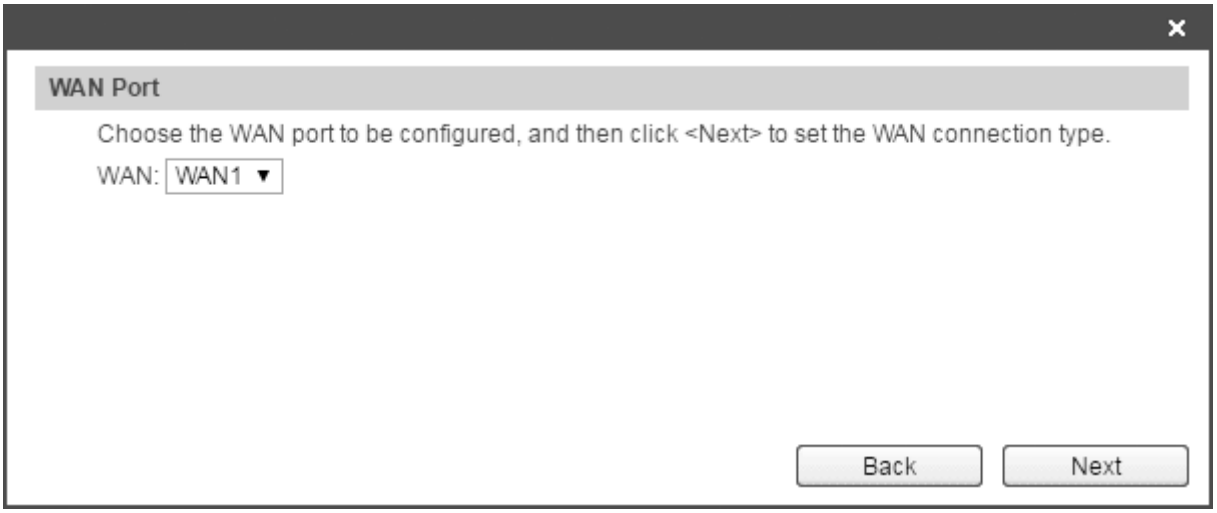


Figure 3-6 WAN Port

Select the connection type provided by your ISP as the Figure 3-7 shows. Three popular types are provided here. For other connection types, please refer to the **4.3.1 WAN**.

Figure 3-7 WAN Connection Type

1) If you choose **PPPoE**, you will see the screen as the Figure 3-8 shows. Enter the **Account Name** and **Password** provided by your ISP (Internet Service Provider).

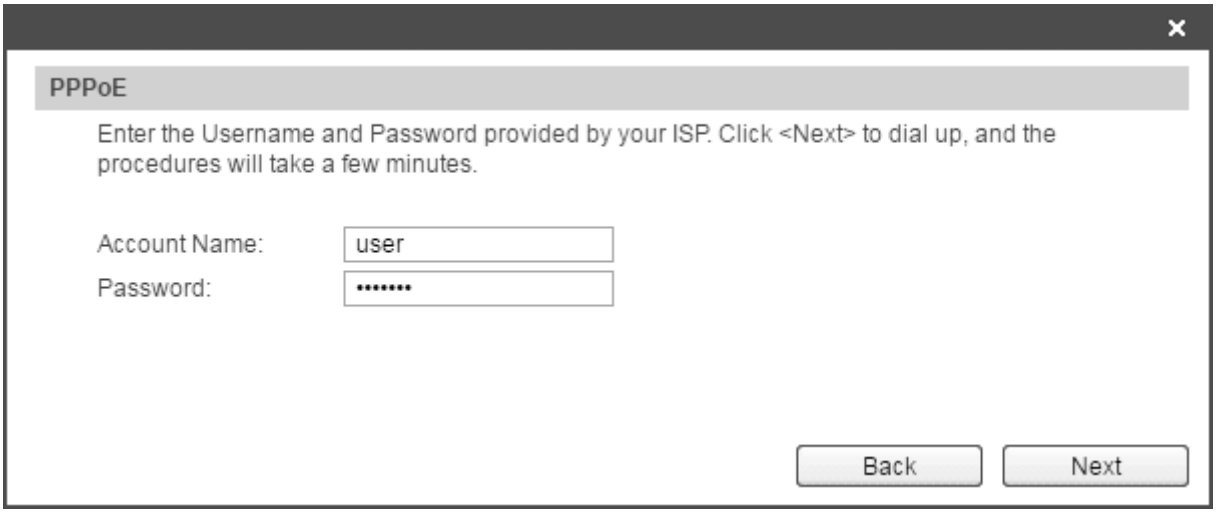


Figure 3-8 WAN Connection Type - PPPoE

Click <Next> to dial up, and the process will take a few minutes. The process of configuring the network parameters is shown as Figure 3-10. If you close the screen during the process, the configuration will still be continued in the background.

These fields are case sensitive. If you have difficulty in this process, please contact your ISP.

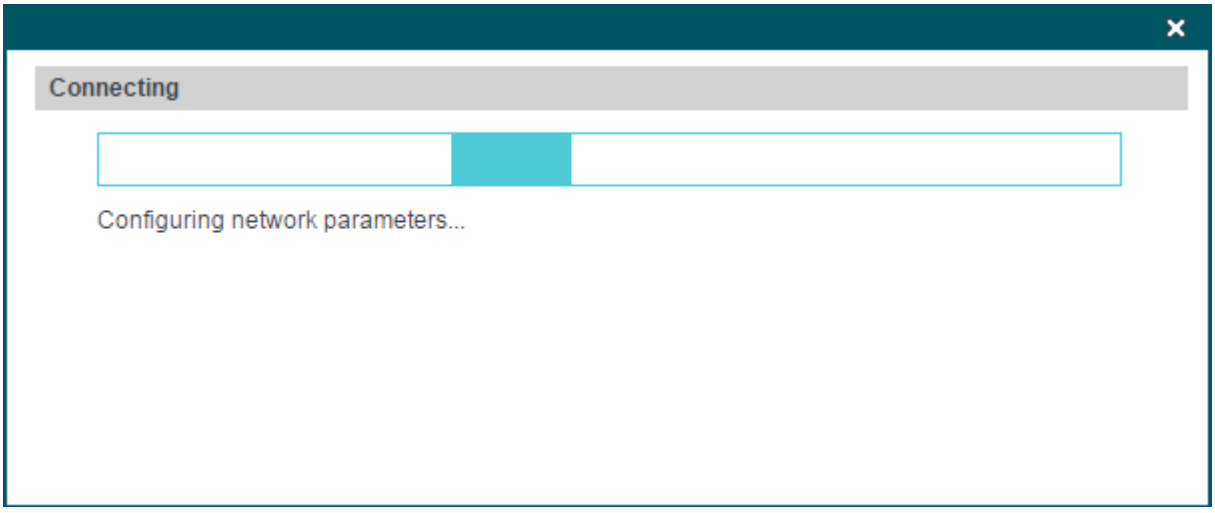


Figure 3-9 WAN Connection Type – PPPoE Connecting

2) If your ISP assigns the IP address automatically, please choose the **Dynamic IP** connection type to obtain the parameters for WAN port automatically. The process for obtain the parameter may take a few minutes as Figure 3-10 shows. If you close the screen during the process, the configuration will still be continued in the background.

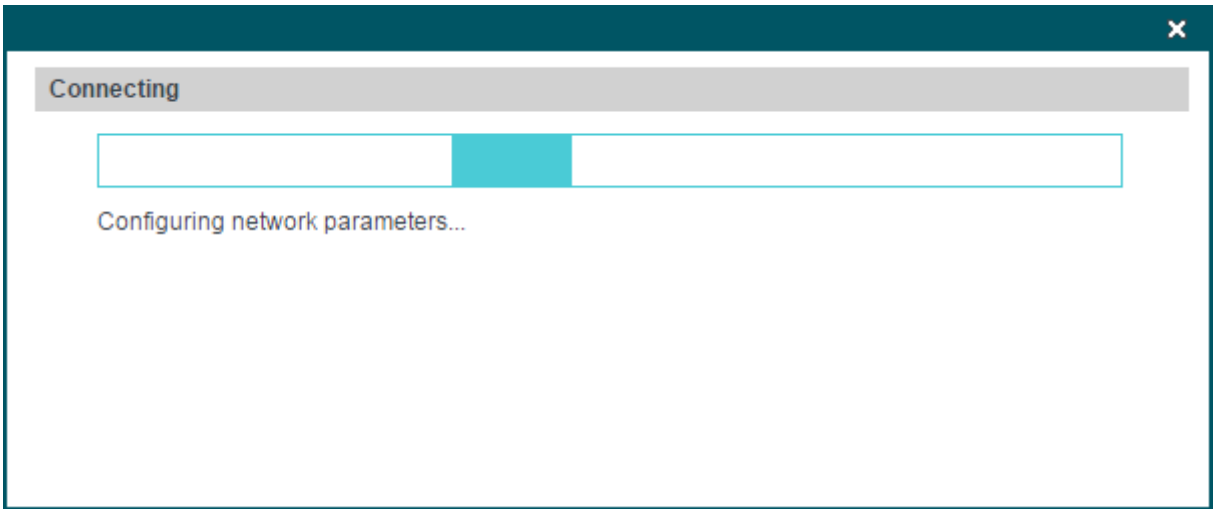


Figure 3-10 WAN Connection Type - Dynamic IP

3) If you choose **Static IP**, you should enter the detailed IP information provided by your ISP in Figure 3-11.

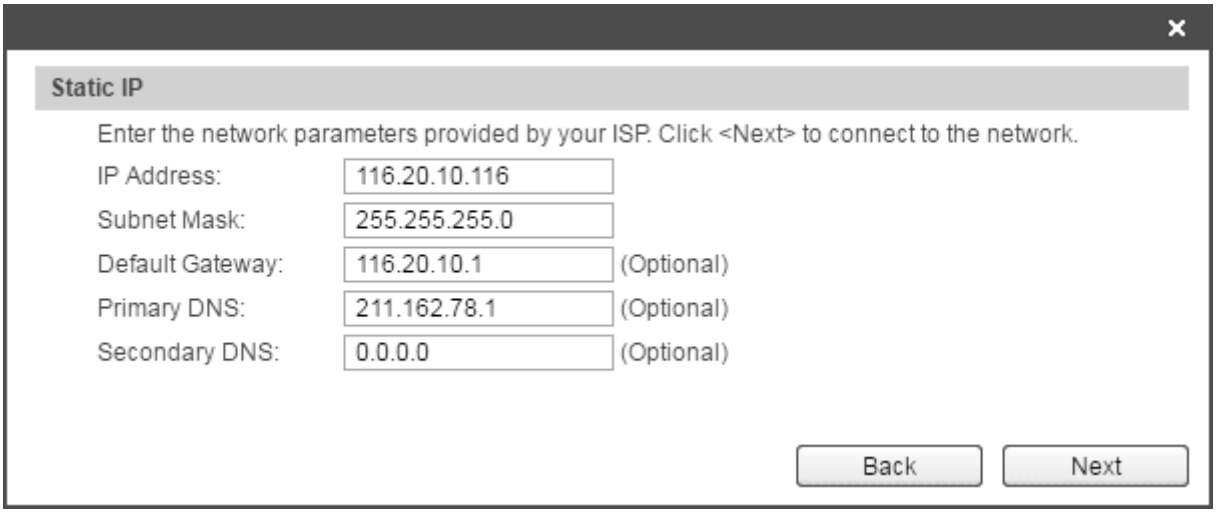


Figure 3-11 WAN Connection Type - Static IP

Then click <Next>. The process for configuring the network parameters is shown as Figure 3-12. If you close the screen during the process, the configuration will still be continued in the background.

If you have difficulty in this process, please contact your ISP.

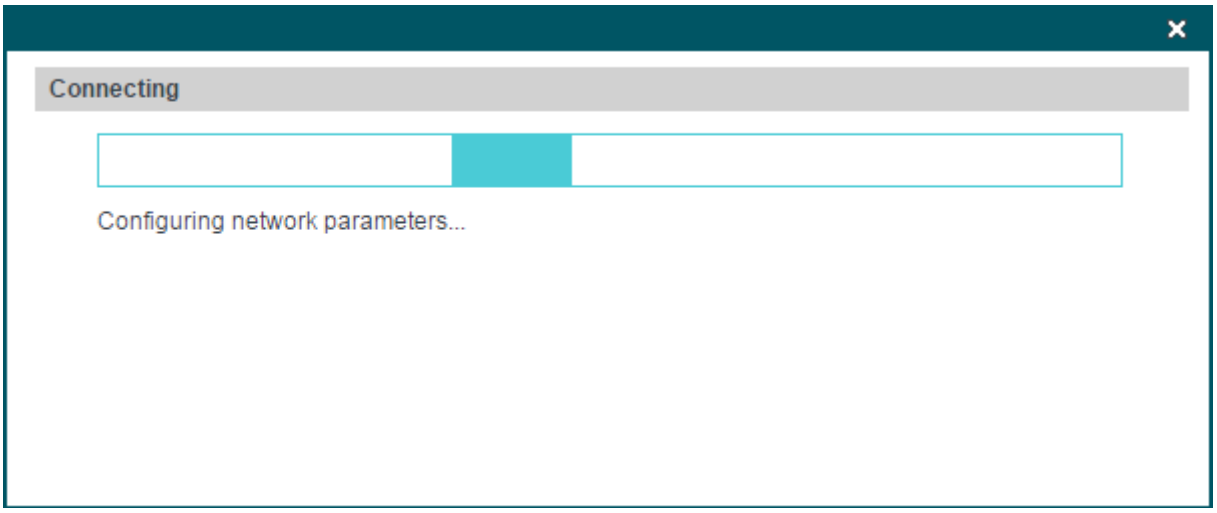


Figure 3-12 WAN Connection Type - Static IP Connecting

After that, you will see the next screen. Click <Finish> to complete the quick installation or click <Continue> to configure other WAN ports.

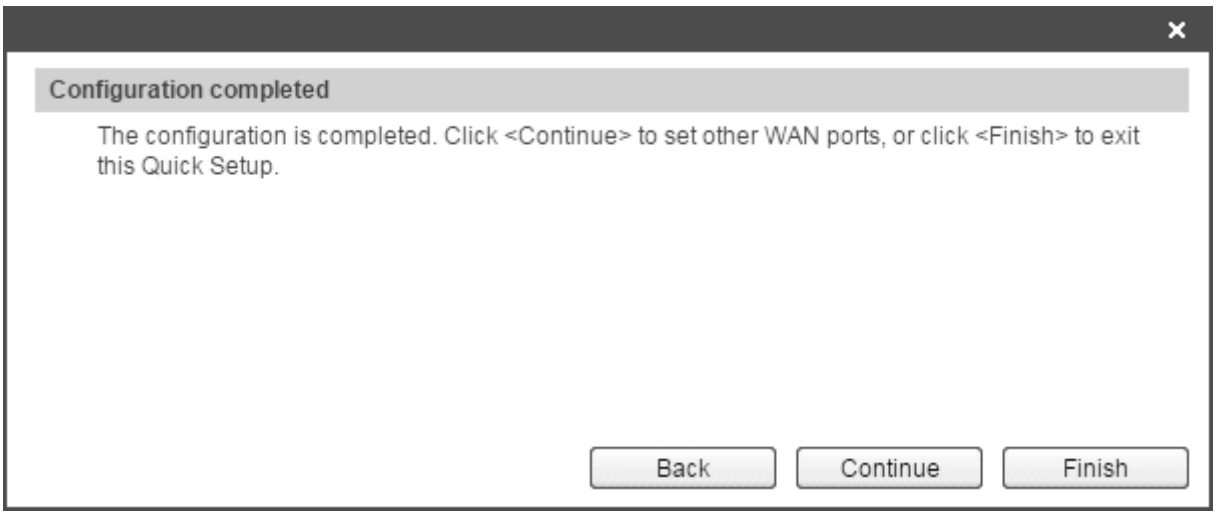


Figure 3-13 Configuration Completed

Chapter 4 Configuration

4.1 Status

The Status page shows the system information, the port connection status and other information related to this router.

Choose the menu **Status** to load the following page.

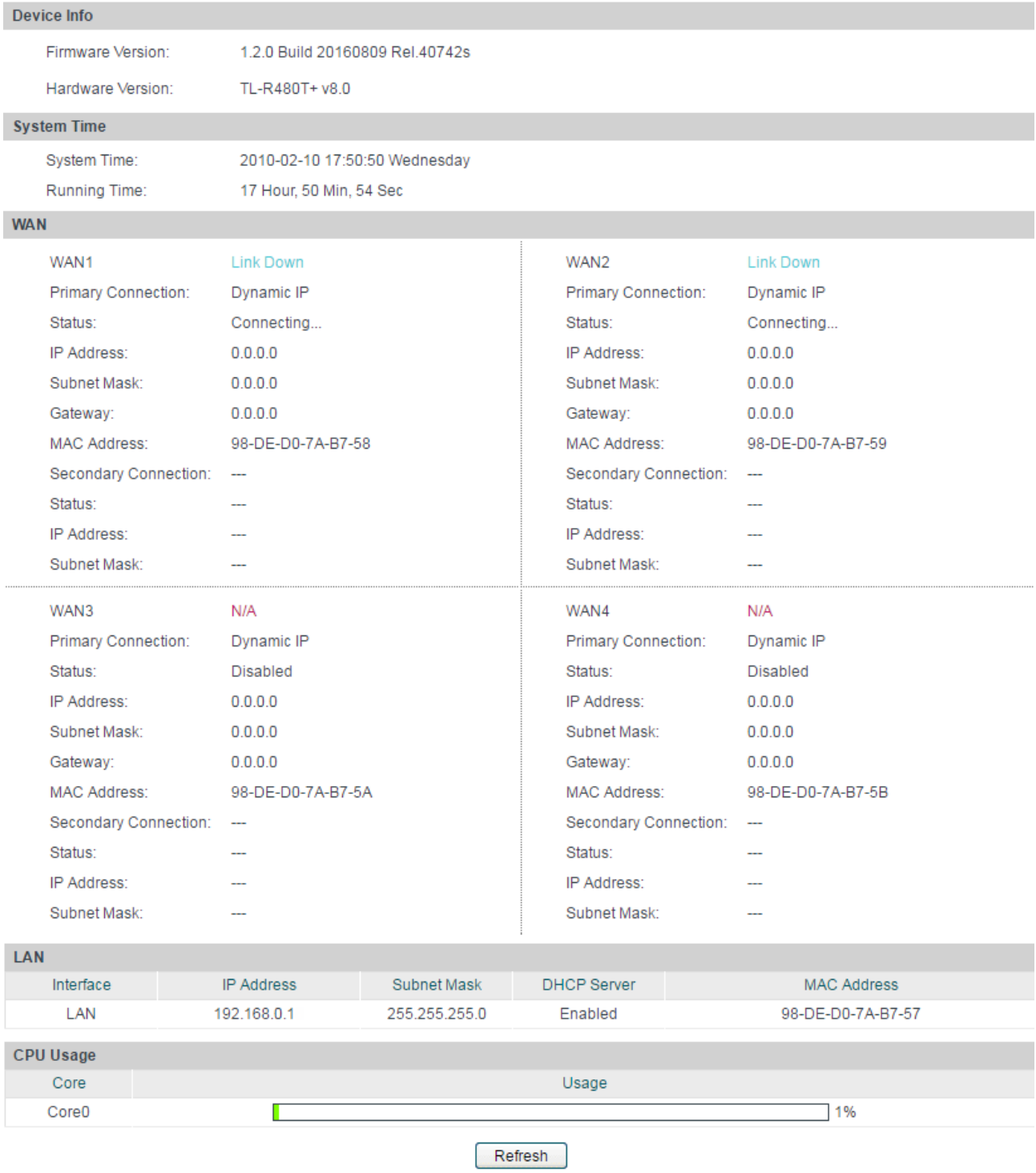


Figure 4-1 Status

4.2 Quick Setup

Please refer to the Chapter 3 Quick Installation Guide.

4.3 Network

4.3.1 WAN

4.3.1.1 WAN Mode

TL-R480T+ provides four available WAN ports. You can set the number of WAN ports on this page.

Choose the menu **Network→WAN→WAN Mode** to load the following page.

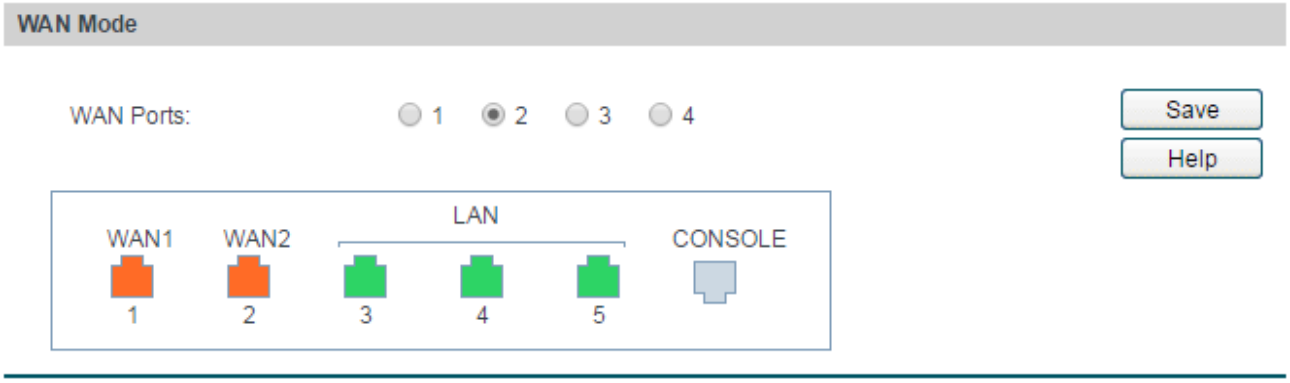


Figure 4-2 WAN Mode

➢ **WAN Mode**

WAN Ports: Select the total number of WAN ports you prefer to use. And the router will adjust the physical ports accordingly, which can be illustrated on the following port sketch.

Note:

- By default, TL-R480T+ is set to work in the mode of dual WAN ports.
- Any change to the number of WAN ports may lead to a loss of current configurations. Please be sure to backup your configurations in advance.

4.3.1.2 WAN1

TL-R480T+ provides the following six Internet connection types: Static IP, Dynamic IP, PPPoE/Russian PPPoE, L2TP/Russian L2TP, PPTP/Russian PPTP and BigPond. To configure the WAN, please first select the type of Internet connection provided by your ISP (Internet Service Provider).

Tips:

- It is allowed to set the IP addresses of multiple WAN ports within the same subnet. However, to guarantee a normal communication, make sure that the WAN ports can access the same network, such as Internet or a local area network.
- The amount of tab pages for WAN port varies with the number of the WAN ports. For the configurations of the other WAN ports, please refer to the instructions of WAN1.

Choose the menu **Network→WAN→WAN1** to load the configuration page.

1) Static IP

If a static IP address has been provided by your ISP, please choose the Static IP connection type to configure the parameters for WAN port manually.

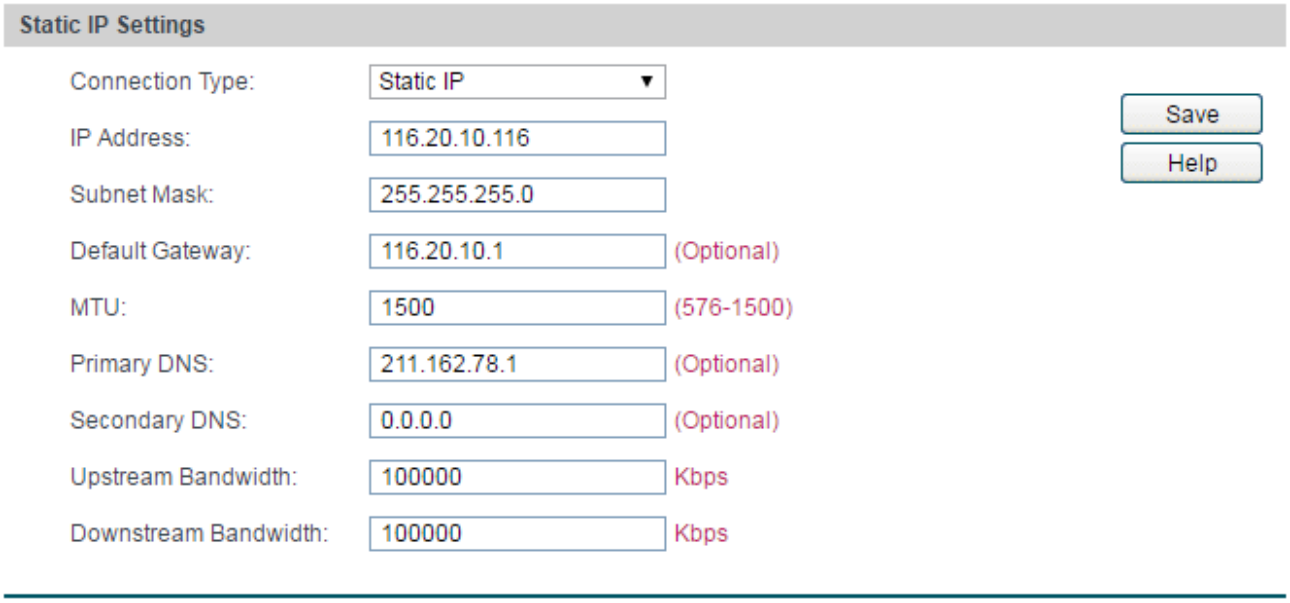


Figure 4-3 WAN – Static IP

The following items are displayed on this screen:

➢ **Static IP**

Connection Type: Select Static IP if your ISP has assigned a static IP address for your computer.

IP Address: Enter the IP address assigned by your ISP. If you are not clear, please consult your ISP.

Subnet Mask: Enter the Subnet Mask assigned by your ISP.

Default Gateway:	Optional. Enter the Gateway assigned by your ISP.
MTU:	MTU (Maximum Transmission Unit) is the maximum data unit transmitted by the physical network. It can be set in the range of 576-1500. The default MTU is 1500. You are recommended to keep the default value if no other MTU value is provided by your ISP.
Primary DNS:	Enter the IP address of your ISP's Primary DNS (Domain Name Server). If you are not clear, please consult your ISP. It is not allowed to access the Internet via domain name if the Primary DNS field is blank.
Secondary DNS:	Optional. If a Secondary DNS Server address is available, enter it.
Upstream Bandwidth:	Specify the bandwidth for transmitting packets on the port.
Downstream Bandwidth:	Specify the bandwidth for receiving packets on the port.

2) Dynamic IP

If your ISP (Internet Service Provider) assigns the IP address automatically, please choose the Dynamic IP connection type to obtain the parameters for WAN port automatically.

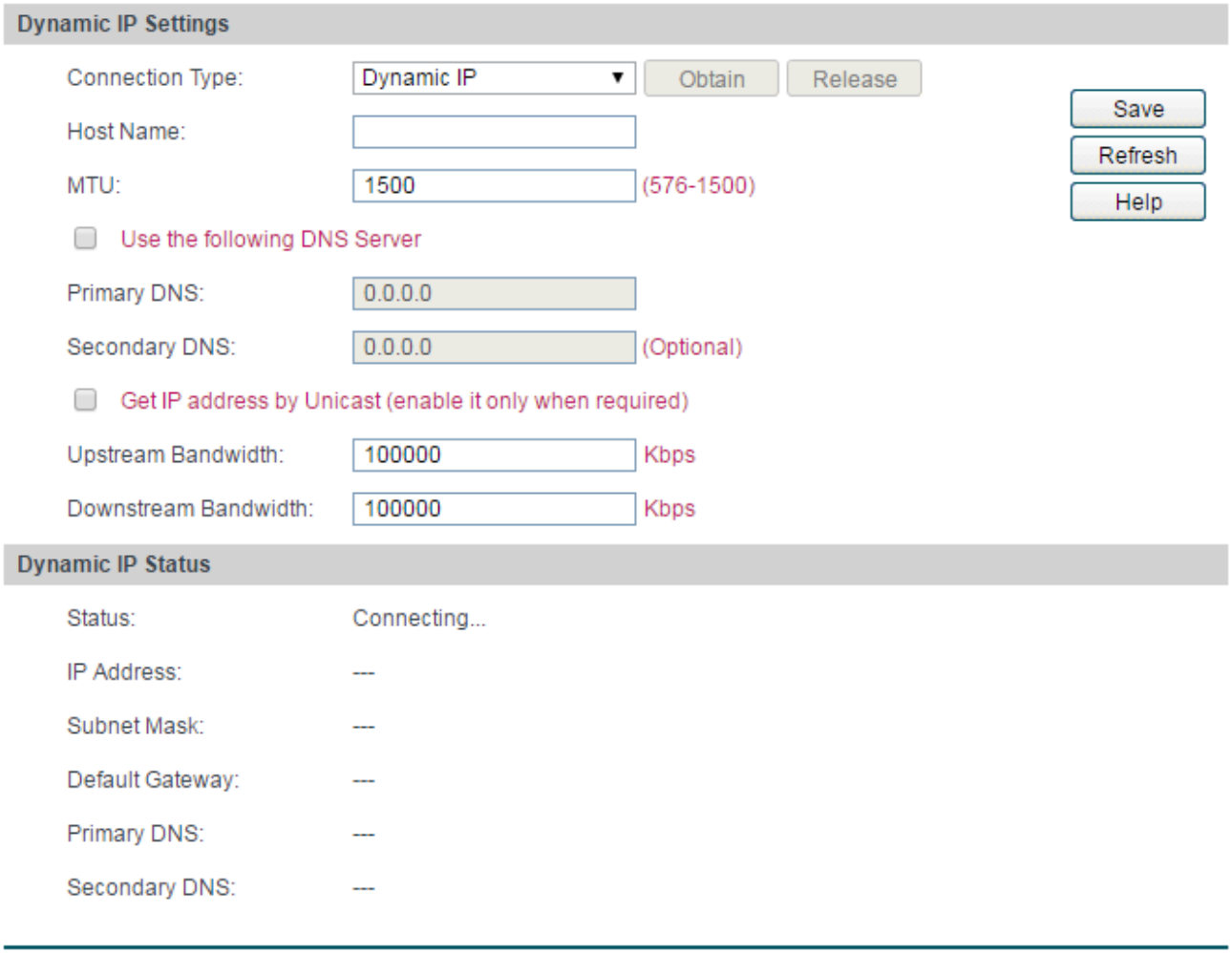


Figure 4-4 WAN – Dynamic IP

The following items are displayed on this screen:

➢ **Dynamic IP**

Connection Type: Select Dynamic IP if your ISP assigns the IP address automatically. Click <Obtain> to get the IP address from your ISP's server. Click <Release> to release the current IP address of WAN port.

Host Name: Optional. This field allows you to give a name for the router. It is blank by default.

MTU: MTU (Maximum Transmission Unit) is the maximum data unit transmitted by the physical network. It can be set in the range of 576-1500. The default MTU is 1500. You are recommended to keep the default value if no other MTU value is provided by your ISP.

Get IP Address by Unicast: The broadcast requirement may not be supported by a few ISPs. Select this option if you can not get the IP address from your ISP even with a normal network connection. This option is not required generally.

Use the following DNS Server: Select this option to enter the DNS (Domain Name Server) address manually.

Primary DNS: Enter the IP address of your ISP's Primary DNS (Domain Name Server). If you are not clear, please consult your ISP.

Secondary DNS: Optional. If a Secondary DNS Server address is available, enter it.

Upstream Bandwidth: Specify the bandwidth for transmitting packets on the port.

Downstream Bandwidth: Specify the bandwidth for receiving packets on the port.

➢ **Dynamic IP Status**

Status: Displays the status of obtaining an IP address from your ISP.

- "Disabled" indicates that the Dynamic IP connection type is not applied.
- "Connecting" indicates that the router is obtaining the IP parameters from your ISP.
- "Connected" indicates that the router has successfully obtained the IP parameters from your ISP.
- "Disconnected" indicates that the IP address has been manually released or the router gets no response from your ISP. Please check your network connection and consult your ISP if this problem remains.

IP Address: Displays the IP address assigned by your ISP.

Subnet Mask: Displays the Subnet Mask assigned by your ISP.

Gateway Address: Displays the Gateway Address assigned by your ISP.

Primary DNS: Displays the IP address of your ISP's Primary DNS.

Secondary DNS: Displays the IP address of your ISP's Secondary DNS.

3) PPPoE

If your ISP (Internet Service Provider) has provided the account information for the PPPoE connection, please choose the PPPoE/Russian PPPoE connection type (Used mainly for DSL Internet service).

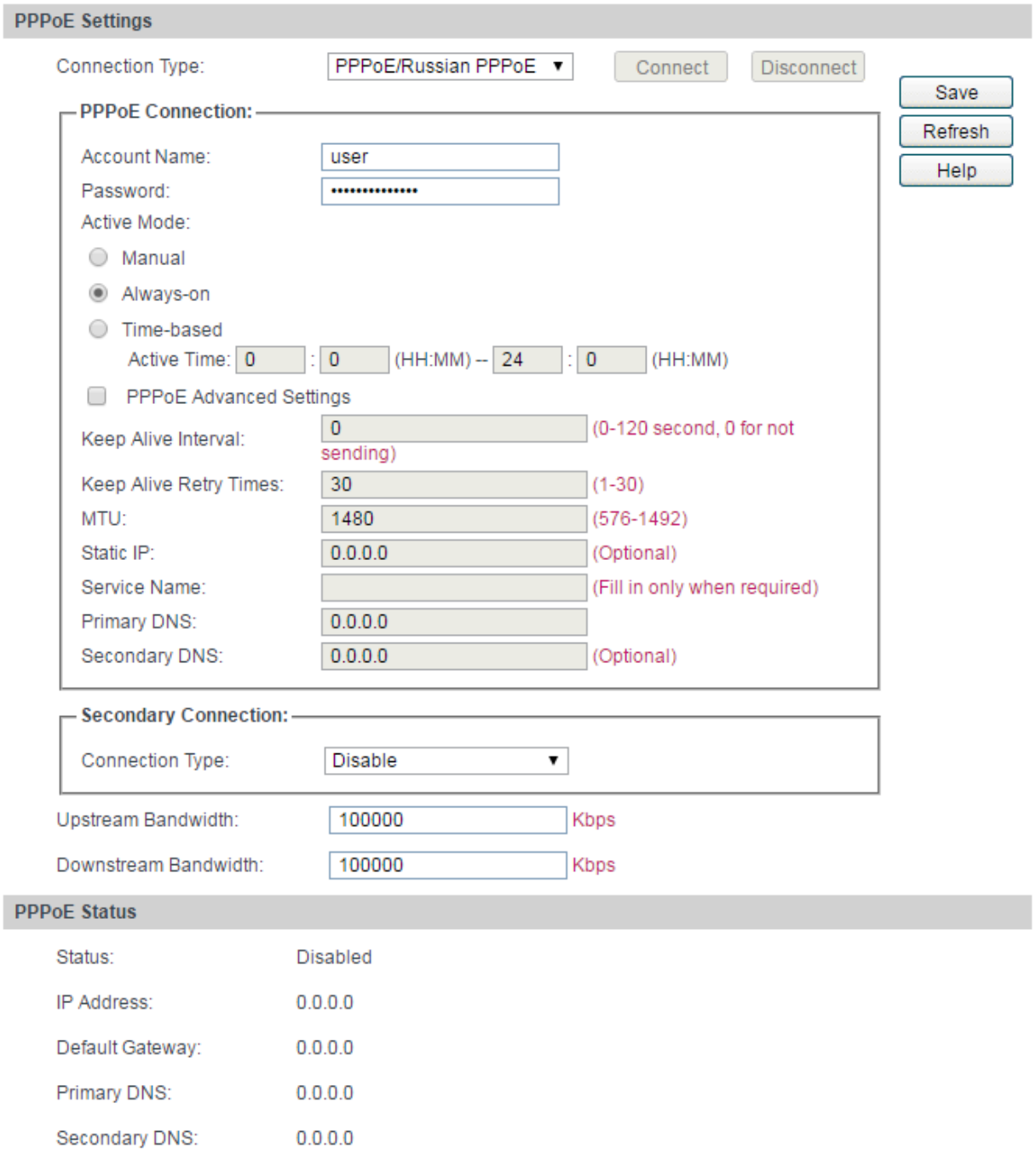


Figure 4-5 WAN - PPPoE

The following items are displayed on this screen:

➢ **PPPoE Settings**

Connection Type: Select PPPoE/Russian PPPoE if your ISP provides xDSL Virtual Dial-up connection. Click <Connect> to dial-up to the Internet and obtain the IP address. Click <Disconnect> to disconnect the Internet and release the current IP address.

Account Name: Enter the Account Name provided by your ISP. If you are not clear, please consult your ISP.

Password: Enter the Password provided by your ISP.

Active Mode: You can select the proper Active mode according to your need.

- Manual: Select this option to manually activate or terminate the Internet connection by the <Connect> or <Disconnect> button. It is optimum for the dial-up connection charged on time.
- Always-on: Select this option to keep the connection always on. The connection can be re-established automatically when it is down.
- Time-based: Select this option to keep the connection on during the Active time you set.

PPPoE Advanced Settings: Check here to enable PPPoE advanced settings.

Keep Alive: Once PPPoE is connected, the router will send keep-alive packets every "Keep Alive Interval" sec and "Keep Alive Retry Times" to make sure the connection is still alive. If the router does not get the response from ISP after sending keep-alive packets, the router will terminate the connection.

MTU: MTU (Maximum Transmission Unit) is the maximum data unit transmitted by the physical network. It can be set in the range of 576-1492. The default MTU is 1480. You are recommended to keep the default value if no other MTU value is provided by your ISP.

ISP Address:	Optional. Enter the ISP address provided by your ISP. It is null by default.
Service Name:	Optional. Enter the Service Name provided by your ISP. It is null by default.
Primary DNS:	Enter the IP address of your ISP's Primary DNS.
Secondary DNS:	Optional. Enter the IP address of your ISP's Secondary DNS.
Secondary Connection:	Here allows you to configure the secondary connection. Dynamic IP and Static IP connection types are provided.
Connection Type:	Select the secondary connection type. Options include Disable, Dynamic IP and Static IP.
IP Address:	If Static IP is selected, configure the IP address of WAN port. If Dynamic IP is selected, the obtained IP address of WAN port is displayed.
Subnet Address:	If Static IP is selected, configure the subnet address of WAN port. If Dynamic IP is selected, the obtained subnet address of WAN port is displayed.
Status:	Displays the status of secondary connection.
Upstream Bandwidth:	Specify the bandwidth for transmitting packets on the port.
Downstream Bandwidth:	Specify the bandwidth for receiving packets on the port.

➢ **PPPoE Status**

Status: Displays the status of PPPoE connection.

- "Disabled" indicates that the PPPoE connection type is not applied.
- "Connecting" indicates that the router is obtaining the IP parameters from your ISP.
- "Connected" indicates that the router has successfully obtained the IP parameters from your ISP.
- "Disconnected" indicates that the connection has been manually terminated or the router gets no response from your ISP. Please ensure that your settings are correct and your network is connected well. Consult your ISP if this problem remains.

IP Address: Displays the IP address assigned by your ISP.

Gateway Address: Displays the Gateway Address assigned by your ISP.

Primary DNS: Displays the IP address of your ISP's Primary DNS.

Secondary DNS: Displays the IP address of your ISP's Secondary DNS.

4) L2TP

If your ISP (Internet Service Provider) has provided the account information for the L2TP connection, please choose the L2TP/Russian L2TP connection type.

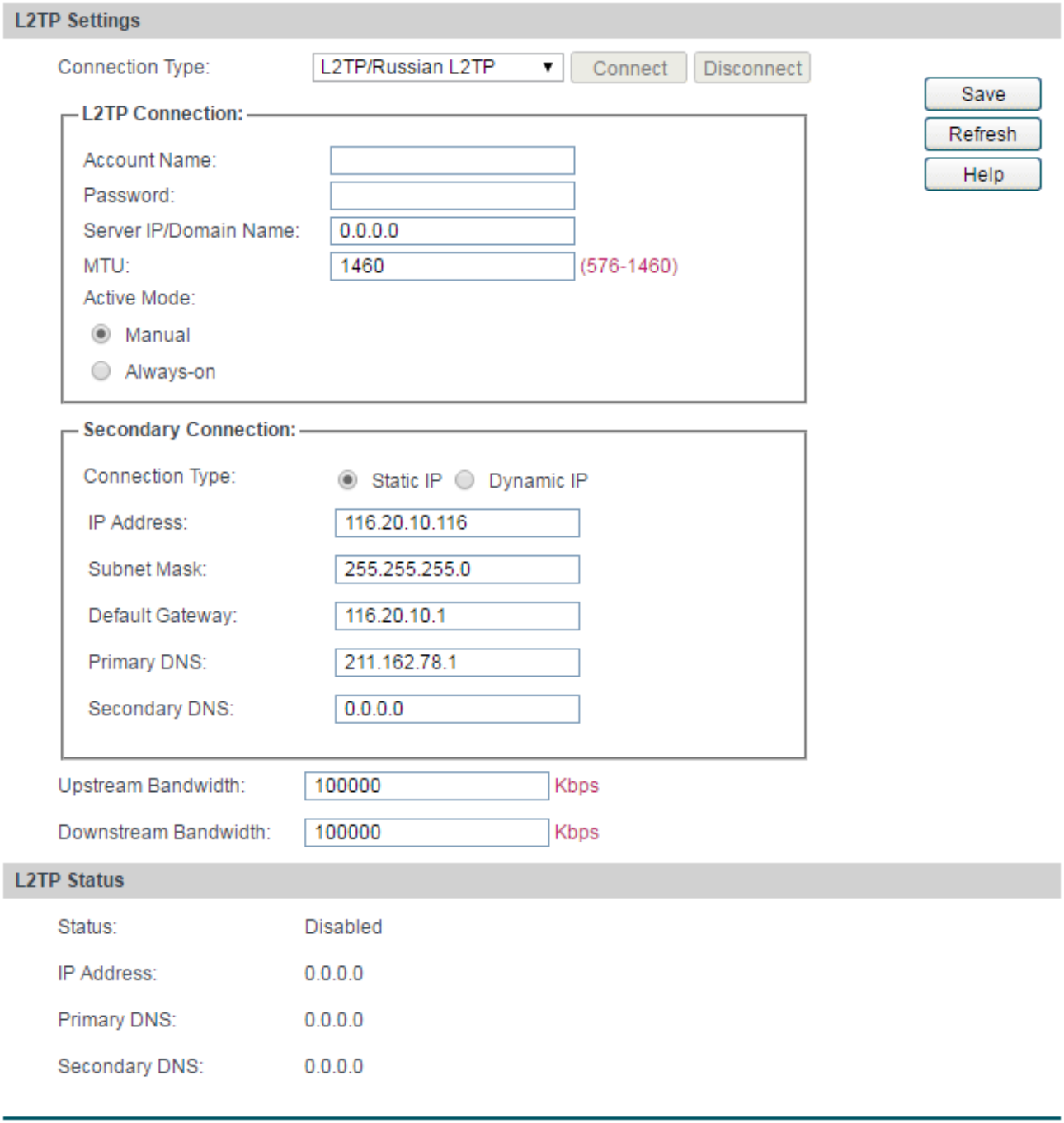


Figure 4-6 WAN - L2TP

The following items are displayed on this screen:

➢ **L2TP Settings**

Connection Type: Select L2TP/Russian L2TP if your ISP provides an L2TP connection. Click <Connect> to dial-up to the Internet and obtain the IP address. Click <Disconnect> to disconnect the Internet and release the current IP address.

Account Name: Enter the Account Name provided by your ISP. If you are not clear, please consult your ISP.

Password: Enter the Password provided by your ISP.

Server IP: Enter the Server IP provided by your ISP.

MTU: MTU (Maximum Transmission Unit) is the maximum data unit transmitted by the physical network. It can be set in the range of 576-1460. The default MTU is 1460. You are recommended to keep the default value if no other MTU value is provided by your ISP.

Active Mode: You can select the proper Active Mode according to your need.

- Manual: Select this option to manually activate or terminate the Internet connection by the <Connect> or <Disconnect> button. It is optimum for the dial-up connection charged on time.
- Always-on: Select this option to keep the connection always on. The connection can be re-established automatically when it is down.

Secondary Connection: Here allows you to configure the secondary connection. Dynamic IP and Static IP connection types are provided.

Connection Type: Select the secondary connection type. Options include Disable, Dynamic IP and Static IP.

IP Address: If Static IP is selected, configure the IP address of WAN port. If Dynamic IP is selected, the IP address of WAN port obtained is displayed.

Subnet Mask: If Static IP is selected, configure the subnet mask of WAN port. If Dynamic IP is select, the subnet mask of WAN port obtained is displayed.

Default Gateway: If Static IP is selected, configure the default gateway. If Dynamic IP is selected, the obtained default gateway is displayed.

Primary DNS/Secondary DNS: If Static IP is selected, configure the DNS. If Dynamic IP is selected, the obtained DNS is displayed.

Upstream Bandwidth: Specify the bandwidth for transmitting packets on the port.

Downstream Bandwidth: Specify the bandwidth for receiving packets on the port.

➢ **L2TP Status**

Status: Displays the status of L2TP connection.

- "Disabled" indicates that the L2TP connection type is not applied.
- "Connecting" indicates that the router is obtaining the IP parameters from your ISP.
- "Connected" indicates that the router has successfully obtained the IP parameters from your ISP.
- "Disconnected" indicates that the connection has been manually terminated or the router gets no response from your ISP. Please ensure that your settings are correct and your network is connected well. Consult your ISP if this problem remains.

IP Address: Displays the IP address assigned by your ISP.

Primary DNS: Displays the IP address of your ISP's Primary DNS.

Secondary DNS: Displays the IP address of your ISP's Secondary DNS.

5) PPTP

If your ISP (Internet Service Provider) has provided the account information for the PPTP connection, please choose the PPTP/Russian PPTP connection type.

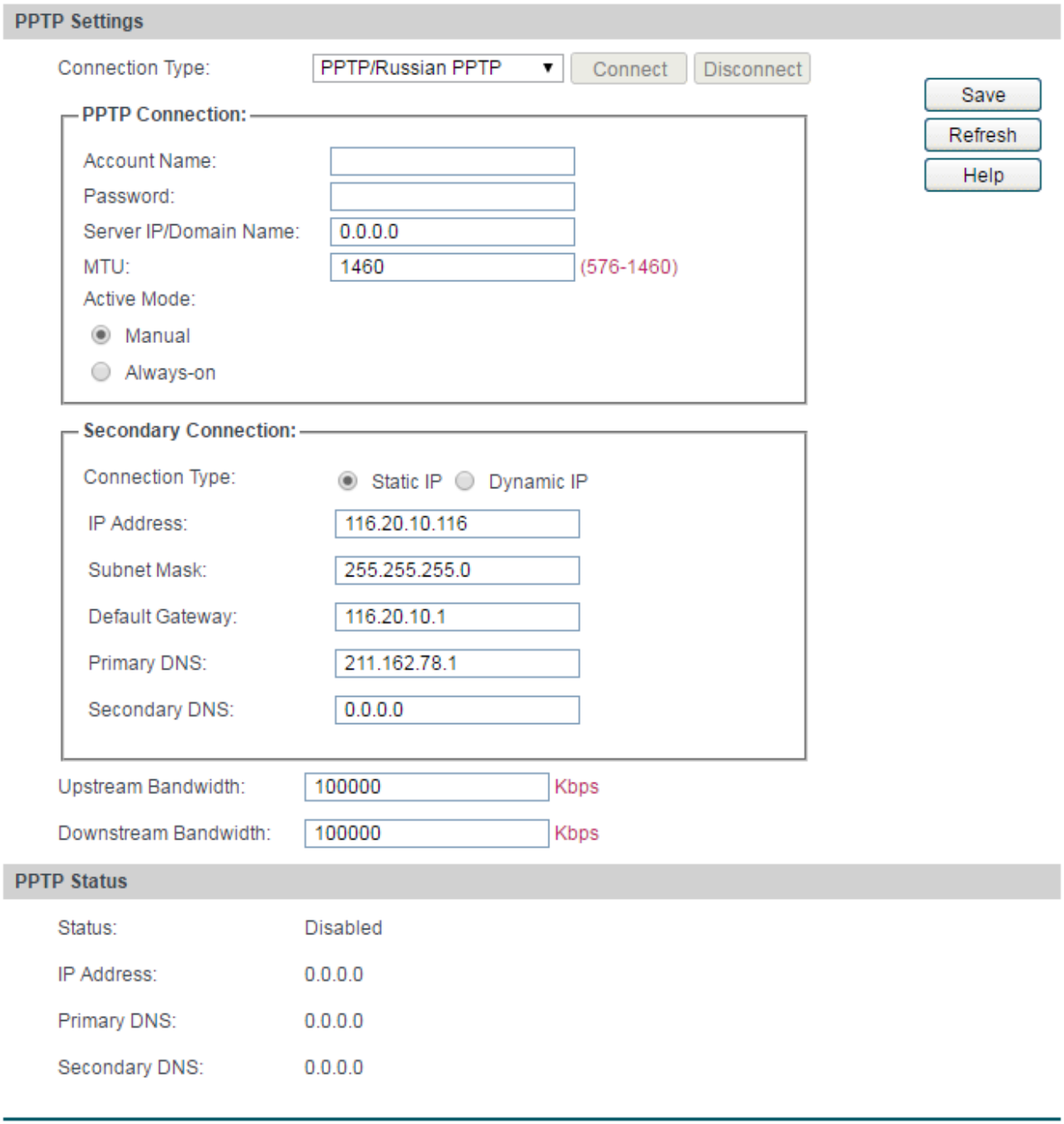


Figure 4-7 WAN - PPTP

The following items are displayed on this screen:

➢ **PPTP Settings**

Connection Type: Select PPTP/Russian PPTP if your ISP provides a PPTP connection. Click <Connect> to dial-up to the Internet and obtain the IP address. Click <Disconnect> to disconnect the Internet and release the current IP address.

Account Name: Enter the Account Name provided by your ISP. If you are not clear, please consult your ISP.

Password: Enter the Password provided by your ISP.

Server IP: Enter the Server IP provided by your ISP.

MTU: MTU (Maximum Transmission Unit) is the maximum data unit transmitted by the physical network. It can be set in the range of 576-1460. The default MTU is 1460. You are recommended to keep the default value if no other MTU value is provided by your ISP.

Active Mode: You can select the proper Active mode according to your need.

- Manual: Select this option to manually activate or terminate the Internet connection by the <Connect> or <Disconnect> button. It is optimum for the dial-up connection charged on time.
- Always-on: Select this option to keep the connection always on. The connection can be re-established automatically when it is down.

Secondary Connections: Here allows you to configure the secondary connection. Dynamic IP and Static IP connection types are provided.

Connection Type: Select the secondary connection type. Options include Disable, Dynamic IP and Static IP.

IP Address: If Static IP is selected, configure the IP address of WAN port. If Dynamic IP is selected, the IP address of WAN port obtained is displayed.

Subnet Mask: If Static IP is selected, configure the subnet mask of WAN port. If Dynamic IP is select, the subnet mask of WAN port obtained is displayed.

Default Gateway: If Static IP is selected, configure the default gateway. If Dynamic IP is selected, the obtained default gateway is displayed.

Primary DNS/Secondary DNS: If Static IP is selected, configure the DNS. If Dynamic IP is selected, the obtained DNS is displayed.

Upstream Bandwidth: Specify the bandwidth for transmitting packets on the port.

Downstream Bandwidth: Specify the bandwidth for receiving packets on the port.

➢ **PPTP Status**

Status: Displays the status of PPTP connection.

- "Disabled" indicates that the PPTP connection type is not applied.
- "Connecting" indicates that the router is obtaining the IP parameters from your ISP.
- "Connected" indicates that the router has successfully obtained the IP parameters from your ISP.
- "Disconnected" indicates that the connection has been manually terminated or the router gets no response from your ISP. Please ensure that your settings are correct and your network is connected well. Consult your ISP if this problem remains.

IP Address: Displays the IP address assigned by your ISP.

Primary DNS: Displays the IP address of your ISP's Primary DNS.

Secondary DNS: Displays the IP address of your ISP's Secondary DNS.

6) BigPond

If your ISP (Internet Service Provider) has provided the account information for the BigPond connection, please choose the BigPond connection type.

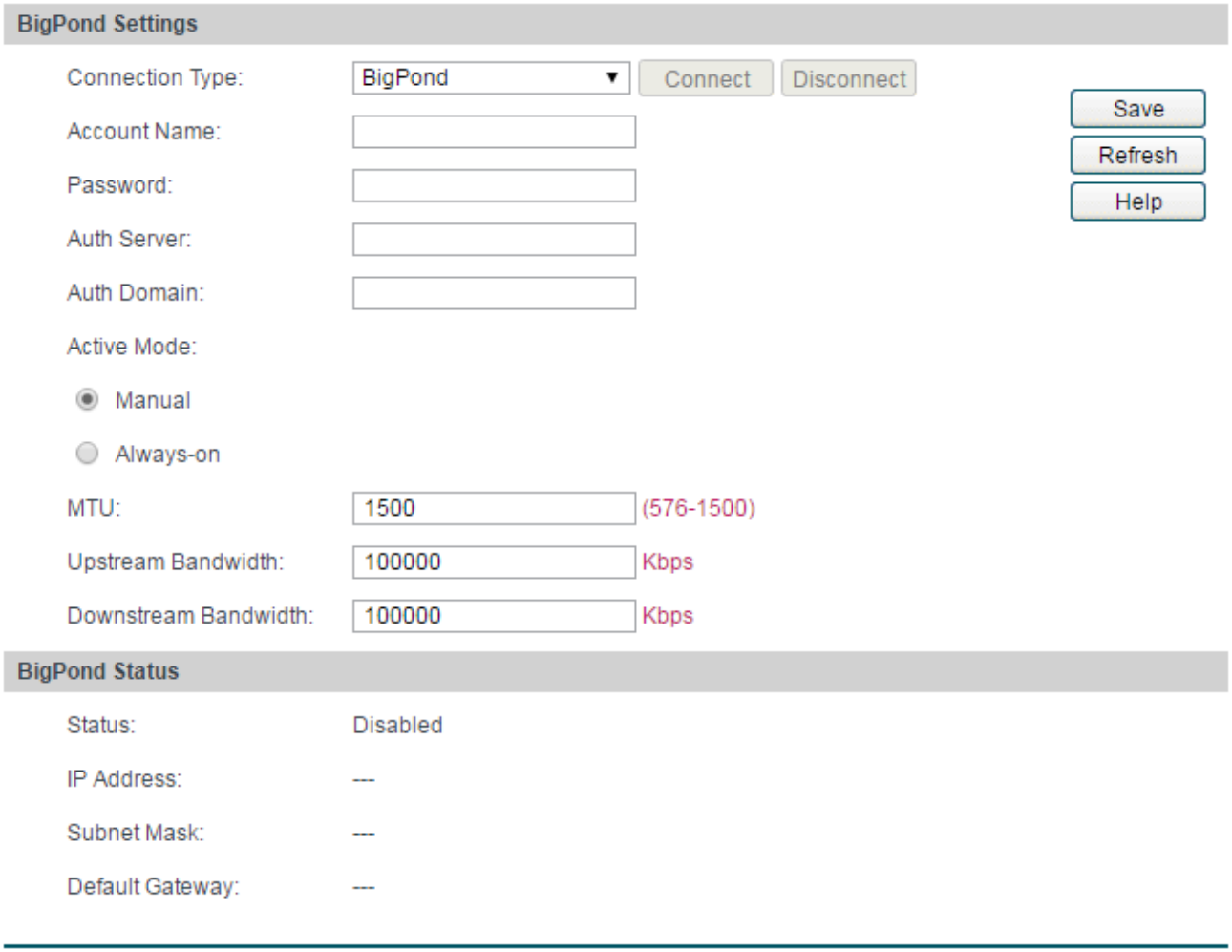


Figure 4-8 WAN – Bigpond

The following items are displayed on this screen:

➢ **BigPond Settings**

Connection Type: Select BigPond if your ISP provides a BigPond connection. Click <Connect> to dial-up to the Internet and obtain the IP address. Click <Disconnect> to disconnect the Internet and release the current IP address.

Account Name: Enter the Account Name provided by your ISP. If you are not clear, please consult your ISP.

Password: Enter the Password provided by your ISP. If you are not clear, please consult your ISP.

Auth Server: Enter the address of authentication server. It can be IP address or server name.

Auth Domain: Enter the domain name of authentication server. It is only required when the address of Auth Server is a server name.

Auth Mode: You can select the proper Active mode according to your need.

- Manual: Select this option to manually activate or terminate the Internet connection by the <Connect> or <Disconnect> button. It is optimum for the dial-up connection charged on time.
- Always-on: Select this option to keep the connection always on. The connection can be re-established automatically when it is down.

MTU: MTU (Maximum Transmission Unit) is the maximum data unit transmitted by the physical network. It can be set in the range of 576-1500. The default MTU is 1500.

Upstream/Downstream Bandwidth: Specify the Upstream/Downstream Bandwidth for the port. To make "Load Balance" and "Bandwidth Control" take effect, please set these parameters correctly.

➢ **BigPond Status**

Status: Displays the status of BigPond connection.

- "Disabled" indicates that the BigPond connection type is not applied.
- "Connecting" indicates that the router is obtaining the IP parameters from your ISP.
- "Connected" indicates that the router has successfully obtained the IP parameters from your ISP.
- "Disconnected" indicates that the connection has been manually terminated or the router gets no response from your ISP. Please ensure that your settings are correct and your network is connected well. Consult your ISP if this problem remains.

IP Address: Displays the IP address assigned by your ISP.

Subnet Mask: Displays the Subnet Mask assigned by your ISP.

Default Gateway: Displays the IP address of the default gateway assigned by your ISP.

Note:

To ensure the BigPond connection re-established normally, please restart the connection at least 5 seconds after the connection is off.

4.3.2 LAN

4.3.2.1 LAN

On this page, you can configure the parameters for LAN port of this router.

Choose the menu **Network→LAN→LAN** to load the following page.

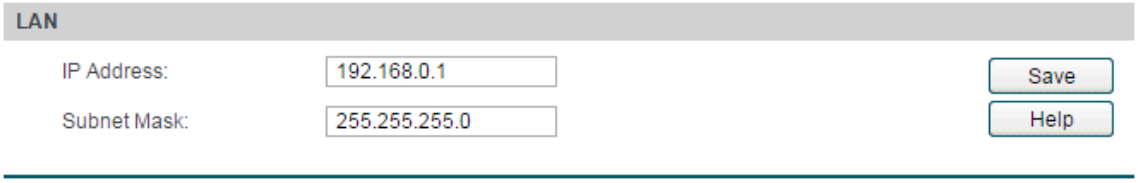


Figure 4-9 LAN

The following items are displayed on this screen:

➢ **LAN**

IP Address: Enter the LAN IP address of the router. 192.168.0.1 is the default IP address. The Hosts in LAN can access the router via this IP address. It can be changed according to your network.

Subnet Mask: Enter the Subnet Mask. The default subnet mask is 255.255.255.0.

Note:

If the LAN IP address is changed, you must use the new IP address to login to the router. To guarantee a normal communication, please be sure that the Gateway address and the Subnet Mask of the Hosts are consistent with that of the router accordingly.

4.3.2.2 DHCP

The router with its DHCP (Dynamic Host Configuration Protocol) server enabled can automatically assign an IP address to the computers in the LAN.

Choose the menu **Network→LAN→DHCP** to load the following page.

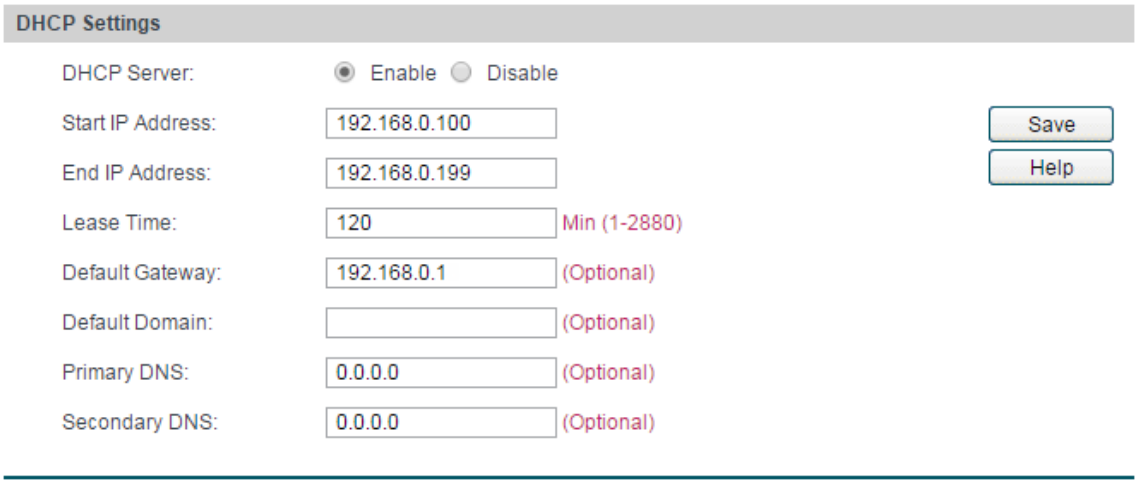


Figure 4-10 DHCP Settings

The following items are displayed on this screen:

➢ **DHCP Settings**

DHCP Server: Enable or disable the DHCP server on your router. Select Enable to make the router automatically assign TCP/IP parameters to the computers in the LAN.

Start IP Address: Enter the Start IP address to define a range for the DHCP server to assign dynamic IP addresses. This address should be in the same IP address subnet with the router's LAN IP address. The default address is 192.168.0.2.

End IP Address: Enter the End IP address to define a range for the DHCP server to assign dynamic IP addresses. This address should be in the same IP address subnet with the router's LAN IP address. The default address is 192.168.0.254.

Lease Time: Specify the length of time the DHCP server will reserve the IP address for each computer. After the IP address expired, the client will be automatically assigned a new one.

Default Gateway: Optional. Enter the Gateway address to be assigned. It is recommended to enter the IP address of the LAN port of the router.

Default Domain: Optional. Enter the domain name of your network.

Primary DNS: Optional. Enter the Primary DNS server address provided by your ISP. It is recommended to enter the IP address of the LAN port of the router.

Secondary DNS: Optional. If a Secondary DNS Server address is available, enter it.

4.3.2.3 DHCP Client

On this page, you can view the information about all the DHCP clients connected to the router.

Choose the menu **Network→LAN→DHCP Client** to load the following page.

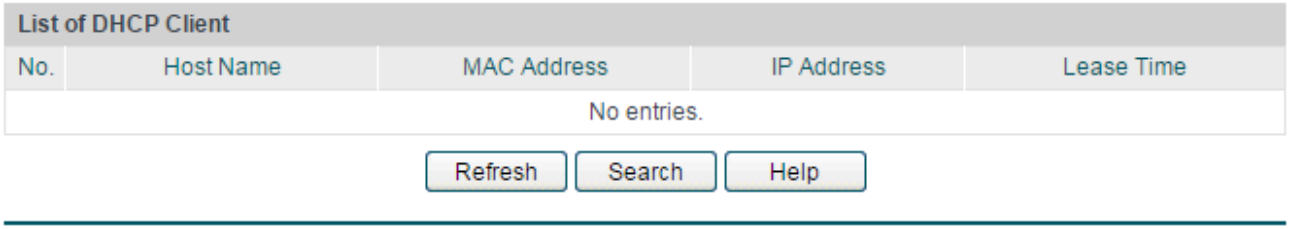


Figure 4-11 DHCP Client

You can view the information of the DHCP clients in this table. Click the **Refresh** button for the updated information.

4.3.2.4 DHCP Reservation

DHCP Reservation feature allows you to reserve an IP address for the specified MAC address. The client with this MAC address will always get the same IP address each time when it accesses the DHCP server.

Choose the menu **Network→LAN→DHCP Reservation** to load the following page.

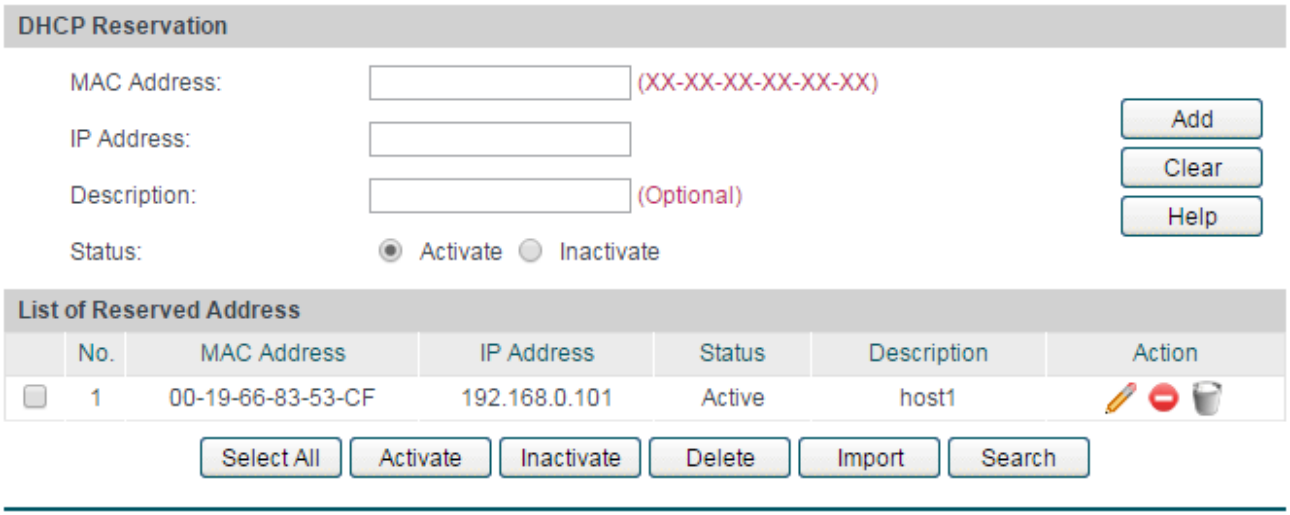


Figure 4-12 DHCP Reservation

The following items are displayed on this screen:

➢ **DHCP Reservation**

MAC Address: Enter the MAC address of the computer for which you want to reserve the IP address.

IP Address: Enter the reserved IP address.

Description: Optional. Enter a description for the entry. Up to 28 characters can be entered.

Status: Activate or Inactivate the corresponding entry.

➢ **List of Reserved Address**

In this table, you can view the information of the entries and edit them by the Action buttons. Up to 512 DHCP static address entries can be supported for LAN by this router.

The first entry in Figure 4-12 indicates: The IP address 192.168.0.101 is reserved for the computer with the MAC address 00-19-66-83-53-CF, and this entry is activated.

Note:

It is recommended that users first bind the IP address and the MAC address in 4.6.1.1 IP-MAC Binding, then import the entries from the IP-MAC binding table to the List of Reserved Address in buck by clicking <Import> button in Figure 4-12 DHCP Reservation.

4.3.3 IPTV

On this page, you can configure the IPTV function. The router will work with IGMP Proxy technology, allowing watching IPTV via wired connection.

Choose the menu **Network→IPTV→IPTV** to load the page.

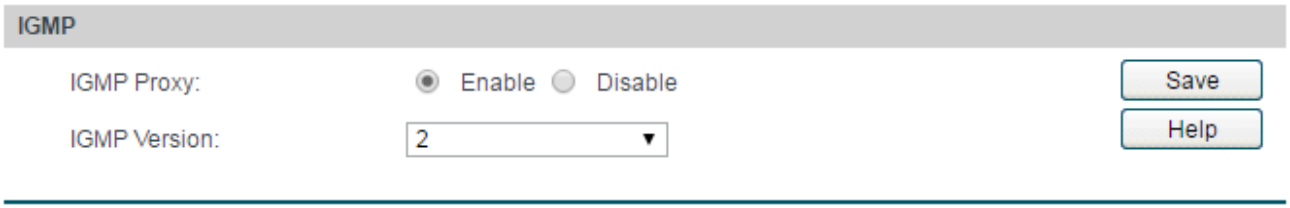


Figure 4-13 IPTV

The following items are displayed on this screen:

➢ **IGMP**

IGMP Proxy: IGMP Proxy is to act as a multicast proxy for hosts on the LAN side.

IGMP Version: You can choose the highest IGMP version that the system supports: IGMPv2 or IGMPv3.

Tips:

- Among the WAN ports, only WAN1(Port1) can be used for IPTV service.
- When IGMP Proxy option is Enabled, you need to ensure the Block IP options under the **Firewall→Attack Defense→Attack Defense** is not selected.
- If the data traffic is heavy when you use IPTV function, it is recommended to increase the parameters of Stationary source UDP Flood and Multi-connections UDP Flood on the page of **Firewall→Attack Defense→Attack Defense**, or deselect the options.

4.3.4 MAC Address

The MAC (Media Access Control) address, as the unique identifier of the router in network, does not need to be changed commonly.

Set the MAC Address for LAN port:

In a complex network topology with all the ARP bound devices, if you want to use TL-R480T+ instead of the current router in a network node, you can just set the MAC address of TL-R480T+'s LAN port the same to the MAC address of the previous router, which can avoid all the devices under this network node to update their ARP binding tables.

Set the MAC Address for WAN port:

In the condition that your ISP has bound the account and the MAC address of the dial-up device, if you want to change the dial-up device to be TL-R480T+, you can just set the MAC address of TL-R480T+'s WAN port the same to the MAC address of the previous dial-up device for a normal Internet connection.

Choose the menu **Network→MAC Address→MAC Address** to load the following page.

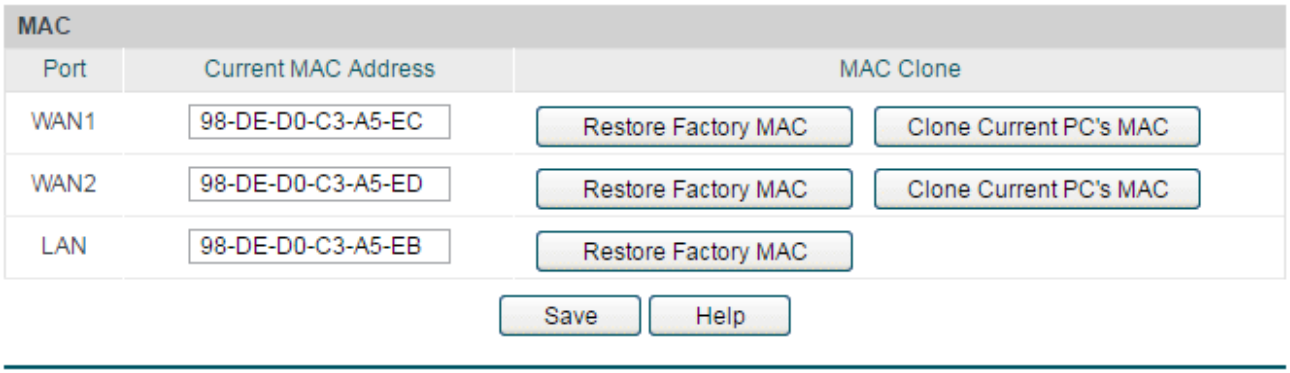


Figure 4-14 MAC Address

The following items are displayed on this screen:

- **MAC Address**

Port: Displays the port type of the router.

Current MAC Address: Displays the current MAC address of the port.

MAC Clone: It is only available for WAN port. Click the <Restore Factory MAC> button to restore the MAC address to the factory default value or click the <Clone Current PC's MAC> button to clone the MAC address of the PC you are currently using to configure the router. Then click <Save> to apply.

Note:

To avoid a conflict of MAC address on the LAN, it is not allowed to set the MAC address of the router's LAN port to the MAC address of the current management PC.

4.3.5 Switch

Some basic switch port management functions are provided by TL-R480T+, which facilitates you to monitor the traffic and manage the network effectively.

4.3.5.1 Statistics

Statistics screen displays the detailed traffic information of each port, which allows you to monitor the traffic and locate faults promptly.

Choose the menu **Network→Switch→Statistics** to load the following page.

Statistics

	Packets	Port 1	Port 2	Port 3	Port 4	Port 5
Received	Unicast	0	0	0	0	14377
	Broadcast	0	0	0	0	812039
	Pause	0	0	0	0	0
	Multicast	0	0	0	0	57009
	Undersize	0	0	0	0	0
	Normal	0	0	0	0	883425
	Oversize	0	0	0	0	0
	Total (Bytes)	0	0	0	0	273958567
Transmitted	Unicast	0	0	0	0	22778
	Broadcast	0	0	0	0	267
	Pause	0	0	0	0	0
	Multicast	0	0	0	0	6493
	Total (Bytes)	0	0	0	0	27560966

Refresh Clear All Help

Figure 4-15 Statistics

The following items are displayed on this screen:

➢ **Statistics**

Unicast: Displays the number of normal unicast packets received or transmitted on the port.

Broadcast: Displays the number of normal broadcast packets received or transmitted on the port.

Pause: Displays the number of flow control frames received or transmitted on the port.

Multicast: Displays the number of normal multicast packets received or transmitted on the port.

Undersize: Displays the number of the received frames (including error frames) that are less than 64 bytes.

Normal: Displays the number of the received packets (including error frames) that are between 64 bytes and the maximum frame length. The maximum untagged frame this router can support is 1518 bytes long and the maximum tagged frame is 1522 bytes long.

Oversize: Displays the number of the received packets (including error frames) that are longer than the maximum frame.

Total (Bytes): Displays the total number of the received or transmitted packets (including error frames).

Check the box and click the <Clear> button to clear the traffic statistics of the corresponding port.

Click the <Clear All> button to clear all the traffic statistics.

4.3.5.2 Port Mirror

Port Mirror, the packets obtaining technology, functions to forward copies of packets from one/multiple ports (mirrored port) to a specific port (mirroring port). Usually, the mirroring port is connected to a data diagnose device, which is used to analyze the mirrored packets for monitoring and troubleshooting the network.

Choose the menu **Network→Switch→Port Mirror** to load the following page.

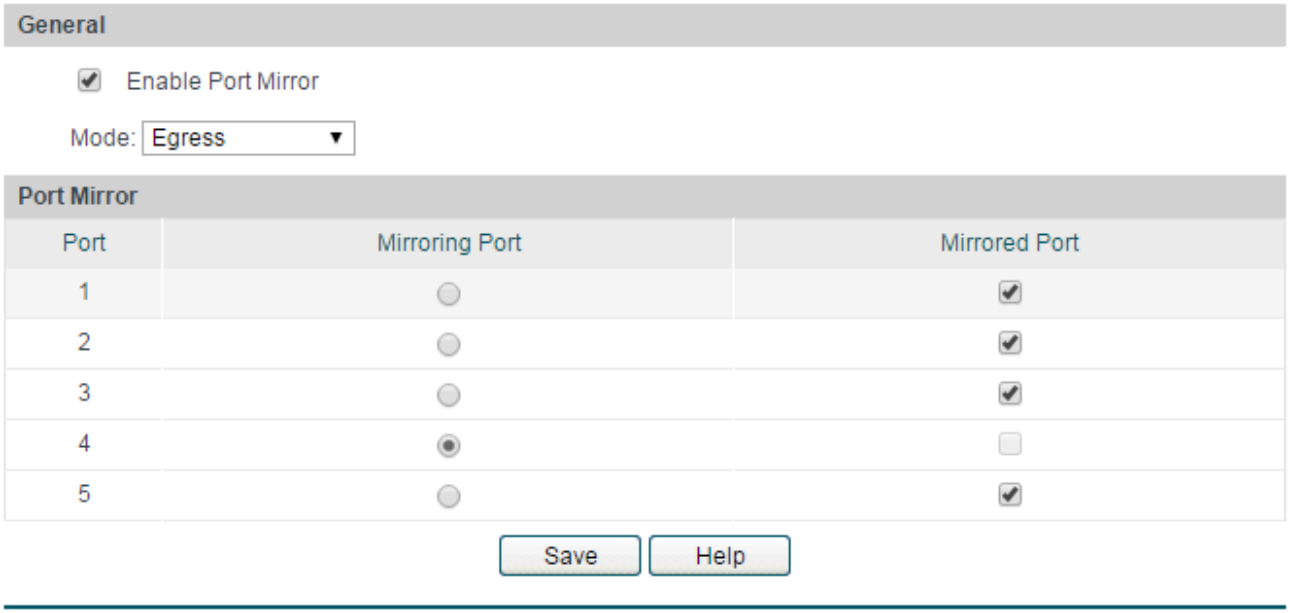


Figure 4-16 Port Mirror

The following items are displayed on this screen:

➢ **General**

Enable Port Mirror: Check the box to enable the Port Mirror function. If unchecked, it will be disabled.

Mode: Select the mode for the port mirror function. Options include:

- **Ingress:** When this mode is selected, only the incoming packets sent by the mirrored port will be copied to the mirroring port.
- **Egress:** When this mode is selected, only the outgoing packets sent by the mirrored port will be copied to the mirroring port.
- **Ingress&Egress:** When this mode is selected, both the incoming and outgoing packets through the mirrored port will be copied to the mirroring port.

➢ **Port Mirror**

Mirroring Port: Select the Mirroring Port to which the traffic is copied. Only one port can be selected as the mirroring port.

Mirrored Port: Select the Mirrored Port from which the traffic is mirrored. One or multiple ports can be selected as the mirrored ports.

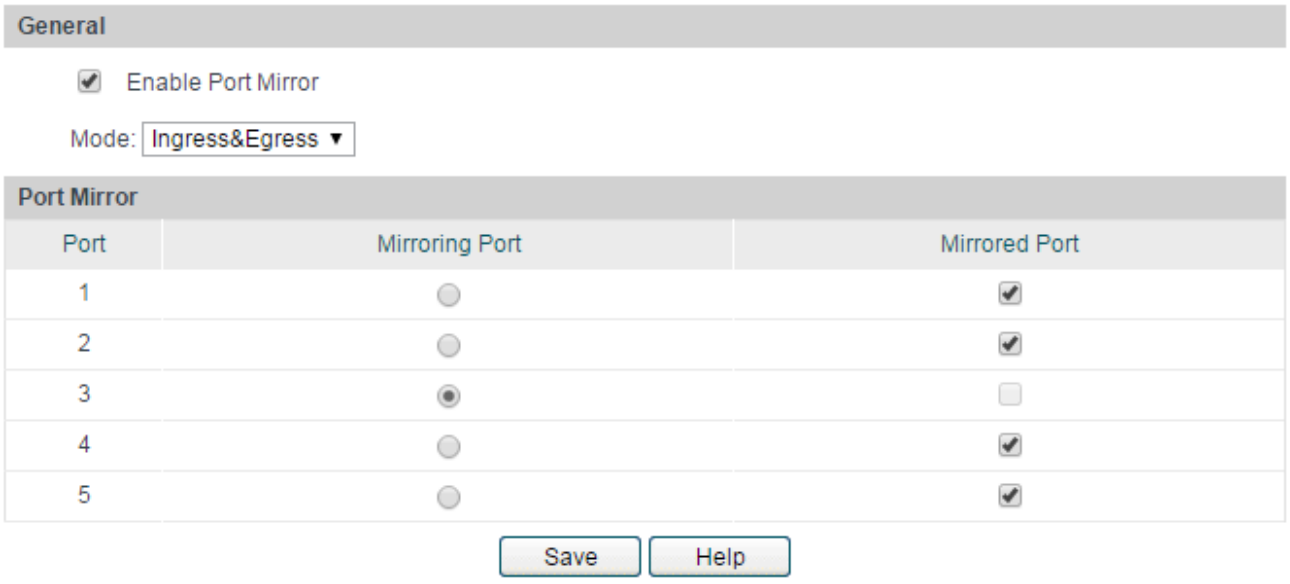
The entry in Figure 4-16 indicates: The outgoing packets sent by port 1, port 2, port 3 and port 5 (mirrored ports) will be copied to port 4 (mirroring port).

Tips:

If both the mirrored port and the mirroring port are the LAN ports, these two LAN ports should be in the same Port VLAN. For example, if port 3 (the mirroring port) and port 4 (the mirrored port) are the LAN ports, the Port Mirror function can take effect only when port 3 and port 4 are in the same Port VLAN.

Application Example

To monitor all the traffic and analyze the network abnormity for an enterprise's network, please set the Port Mirror function as below:



1) Check the box before **Enable Port Mirror** to enable the Port Mirror function and select the **Ingress & Egress** mode.

2) Select Port 3 to be the Mirroring Port to monitor all the packets of the other ports.

3) Select all the other ports to be the Mirrored Ports.

4) Click the <Save> button to apply.

4.3.5.3 Rate Control

On this page, you can control the traffic rate for the specific packets on each port so as to manage your network flow.

Choose the menu **Network→Switch→Rate Control** to load the following page.

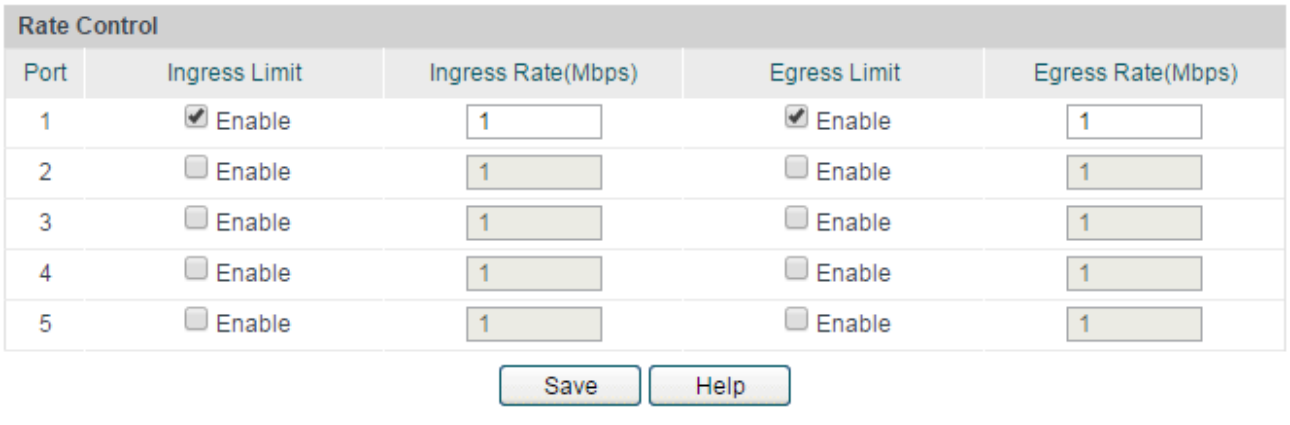


Figure 4-17 Rate Control

The following items are displayed on this screen:

➢ **Rate Control**

Port: Displays the port number.

Ingress Limit: Specify whether to enable the Ingress Limit feature.

Ingress Rate: Specify the limit rate for the ingress packets.

Egress Limit: Specify whether to enable Egress Limit feature.

Egress Rate: Specify the limit rate for the egress packets.

The first entry in Figure 4-17 indicates: The Ingress and Egress Limits are enabled for port 1. The Ingress and Egress Rates are 1Mbps. That is, the receiving rate for all the ingress packets will not exceed 1Mbps, and the transmitting rate for all the egress packets will not exceed 1Mbps.

4.3.5.4 Port Config

On this page, you can configure the basic parameters for the ports.

Choose the menu **Network→Switch→Port Config** to load the following page.

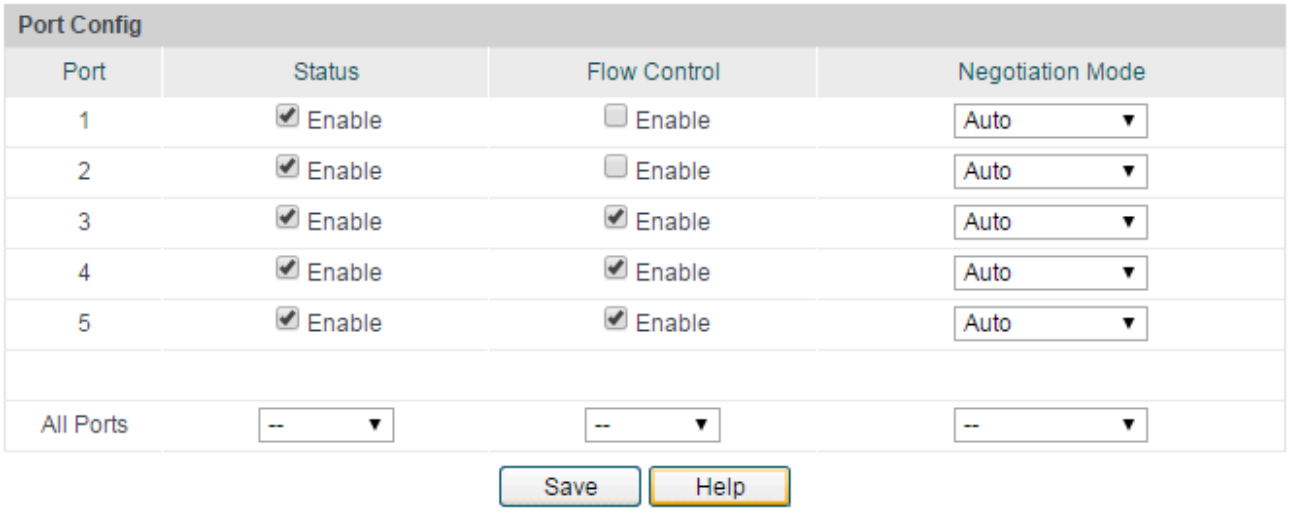


Figure 4-18 Port Config

The following items are displayed on this screen:

➢ **Port Config**

Status: Specify whether to enable the port. The packets can be transported via this port after being enabled.

Flow Control: Allows you to enable/disable the Flow Control function.

Negotiation Mode: Select the Negotiation Mode for the port.

All Ports: Allows you to configure the parameters for all the ports at one time.

4.3.5.5 Port Status

On this page, you can view the current status of each port.

Choose the menu **Network→Switch→Port Status** to load the following page.

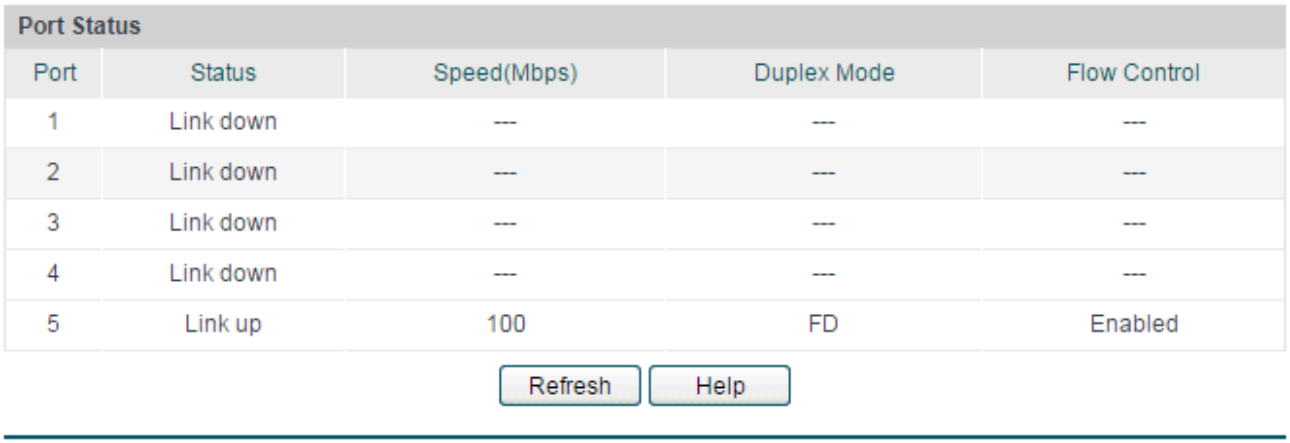


Figure 4-19 Port Status

4.3.5.6 Port VLAN

A VLAN (Virtual Local Area Network) is a network topology configured according to a logical scheme rather than the physical layout, which allows you to divide the physical LAN into multiple logical LANs so as to control the communication among the ports.

The VLAN function can prevent the broadcast storm in LANs and enhance the network security. By creating VLANs in a physical LAN, you can divide the LAN into multiple logical LANs, each of which has a broadcast domain of its own. Hosts in the same VLAN communicate with one another as if they are in a LAN. However, hosts in different VLANs cannot communicate with one another directly. Therefore, broadcast packets are limited in a VLAN.

TL-R480T+ provides the Port VLAN function, which allows you to create multiple logical VLANs for the LAN ports based on their port numbers.

Choose the menu **Network→Switch→Port VLAN** to load the following page.

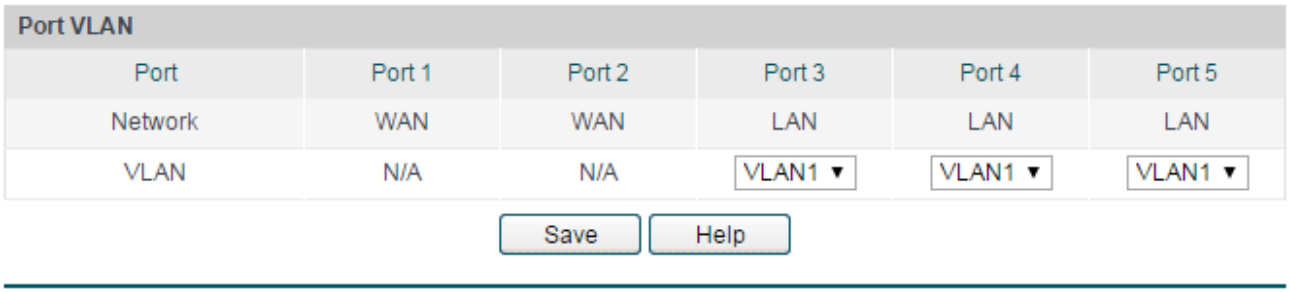


Figure 4-20 Port VLAN

The following items are displayed on this screen:

➢ **Port VLAN**

Network: Displays the current logical network of the physical port.

VLAN: Select the desired VLAN for the port.

Tips:

The Port VLAN can only be created among the LAN ports.

4.4 User Group

The User Group function is used to group different users for unified management, so that you can perform other applications such as Bandwidth Control, Session Limit, and Access Control etc. on per group.

4.4.1 Group

On this page you can define the group for management.

Choose the menu **User Group→Group** to load the following page.

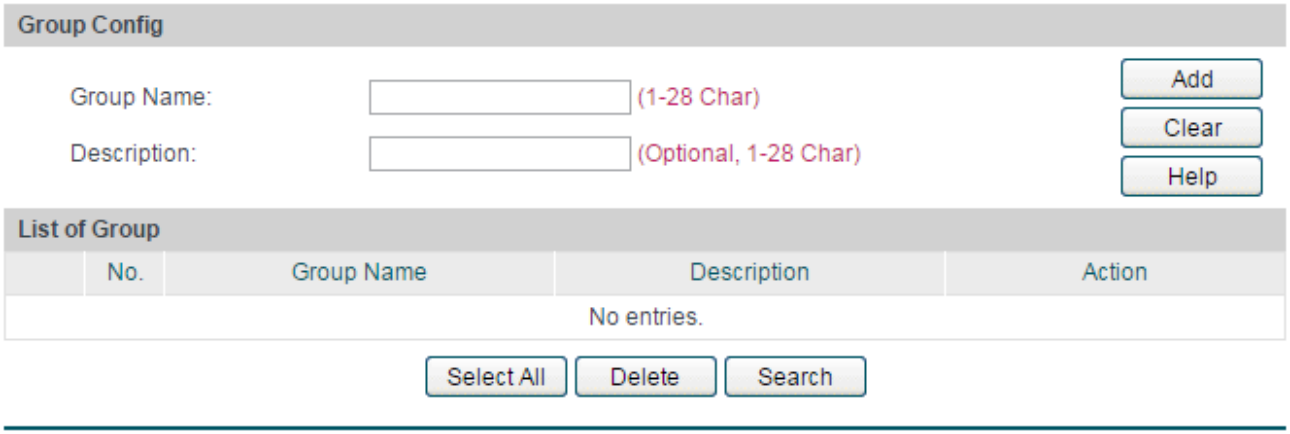


Figure 4-21 Group Configuration

The following items are displayed on this screen:

➢ **Group Config**

Group Name: Specify a unique name for the group.

Description: Give a description for the group. It is optional.

➢ **List of Group**

In this table, you can view the information of the Groups and edit them by the Action buttons.

4.4.2 User

On this page, you can configure the User for the group.

Choose the menu **User Group→User** to load the following page.

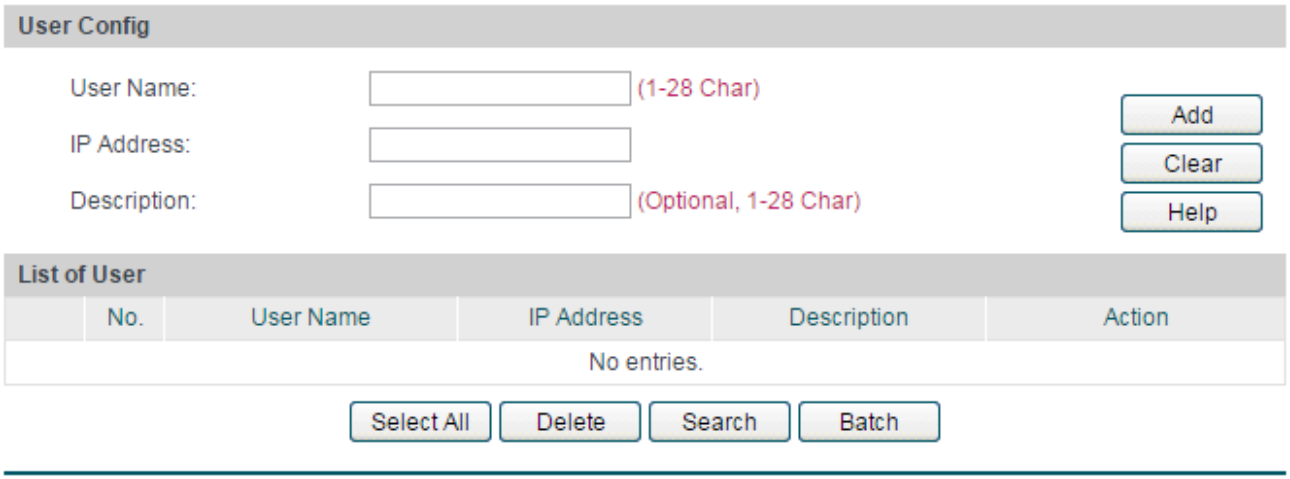


Figure 4-22 User Configuration

The following items are displayed on this screen:

- **User Config**

  User Name: Specify a unique name for the user.

  IP Address: Enter the IP Address of the user. It cannot be the network address or broadcast address of the port.

  Description: Give a description to the user for identification. It is optional.

- **List of User**

  In this table, you can view the information of the Users and edit them by the Action buttons.

4.4.3 View

On this page, you can configure the User View or Group View.

Choose the menu **User Group→View** to load the following page.

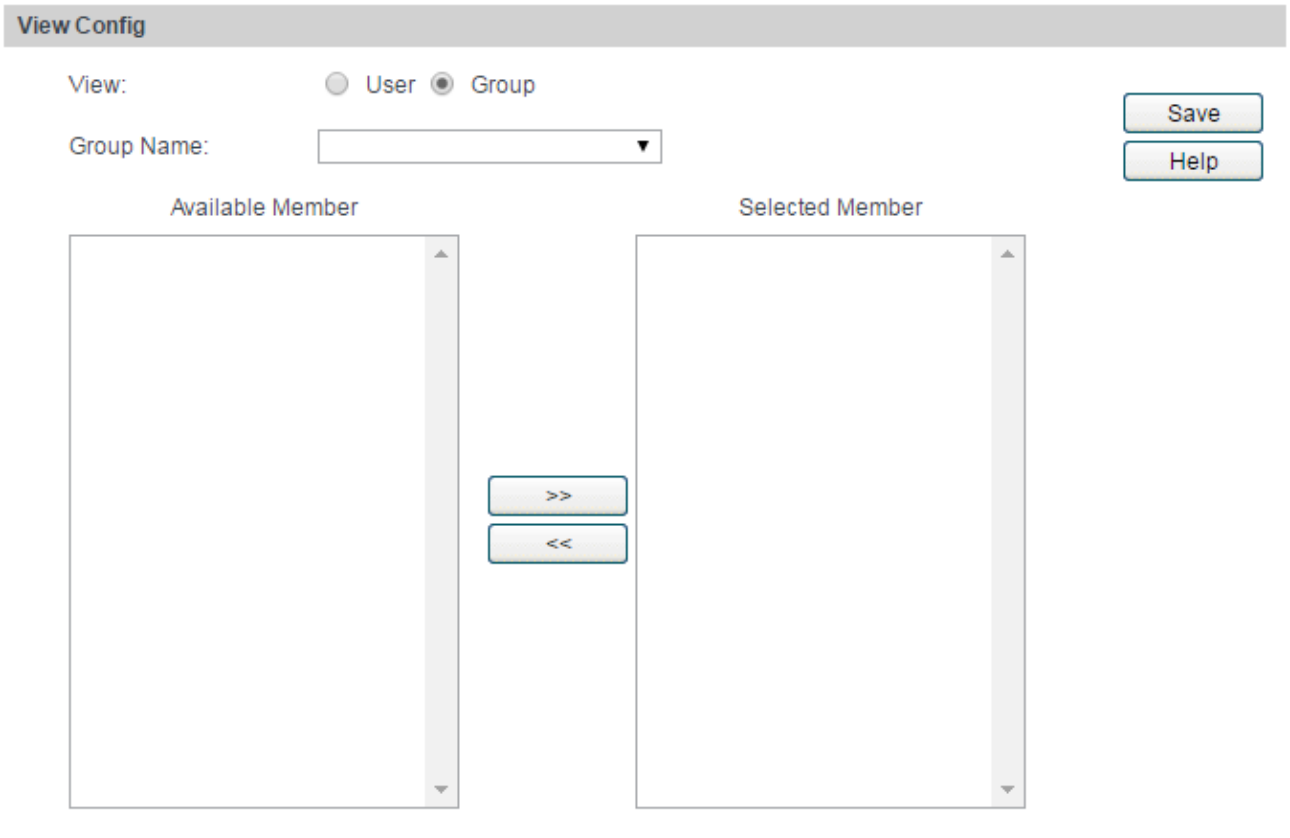


Figure 4-23 View Configuration

The following items are displayed on this screen:

- **View Config**

View:	Select the desired view for configuration.
User Name:	Select the name of the desired User.
Available Group:	Displays the Groups that the User can join.
Selected Group:	Displays the Groups to which this User belongs.
Group Name:	Select the name of the desired Group.
Group Structure:	Click this button to view the tree structure of this group. All the members of this group will be displayed, including Users and sub-Groups. The Group Names are displayed in bold.
Available Member:	Displays the Users and the Groups which can be added into this group.
Selected Member:	Displays the members of this group, including Users and Groups.

4.5 Advanced

4.5.1 NAT

NAT (Network Address Translation) is the translation between private IP and public IP, which allows private network users to visit the public network using private IP addresses.

With the explosion of the Internet, the number of available IP addresses is not enough. NAT provides a way to allow multiple private hosts to access the public network with one public IP at the same time, which alleviates the shortage of IP addresses. Furthermore, NAT strengthens the LAN (Local Area Network) security of the network since the address of LAN host never appears on the Internet.

4.5.1.1 NAT Setup

On this page, you can set up the NAT function.

Choose the menu **Advanced→NAT→NAT Setup** to load the following page.

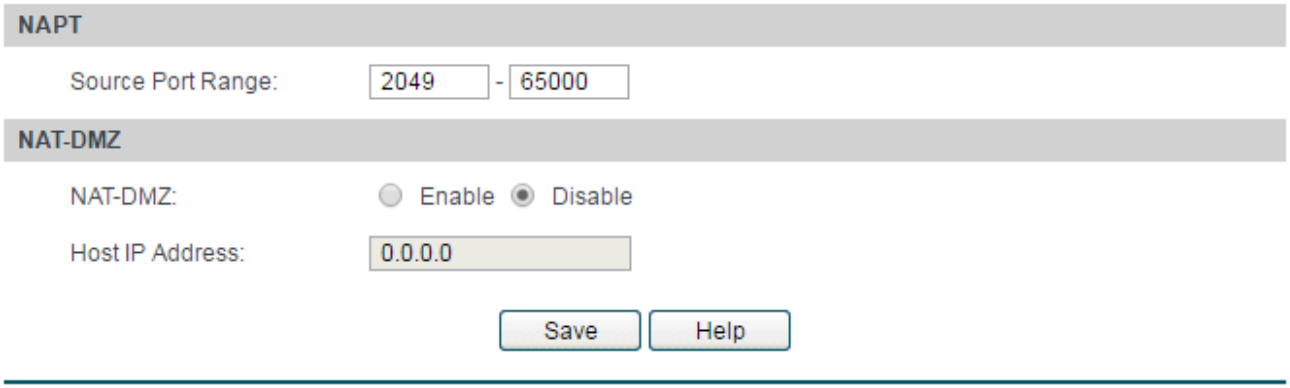


Figure 4-24 NAT Setup

The following items are displayed on this screen:

- **NAPT**

  Source Port Range: Enter the source port range between 2049 and 65000, the span of which must be not less than 100.

- **NAT-DMZ**

  NAT-DMZ: Enable or disable NAT-DMZ. NAT DMZ is a special service of NAT application, which can be considered as a default forwarding rule. When NAT DMZ (Pseudo DMZ) is enabled, all the data initiated by external network falling short of the current connections or forwarding rules will be forwarded to the pReset NAT DMZ host.

  Host IP Address: Enter the IP address of the host specified as NAT DMZ server.

4.5.1.2 One-to-One NAT

On this page, you can configure the One-to-One NAT.

Choose the menu **Advanced→NAT→One-to-One NAT** to load the following page.

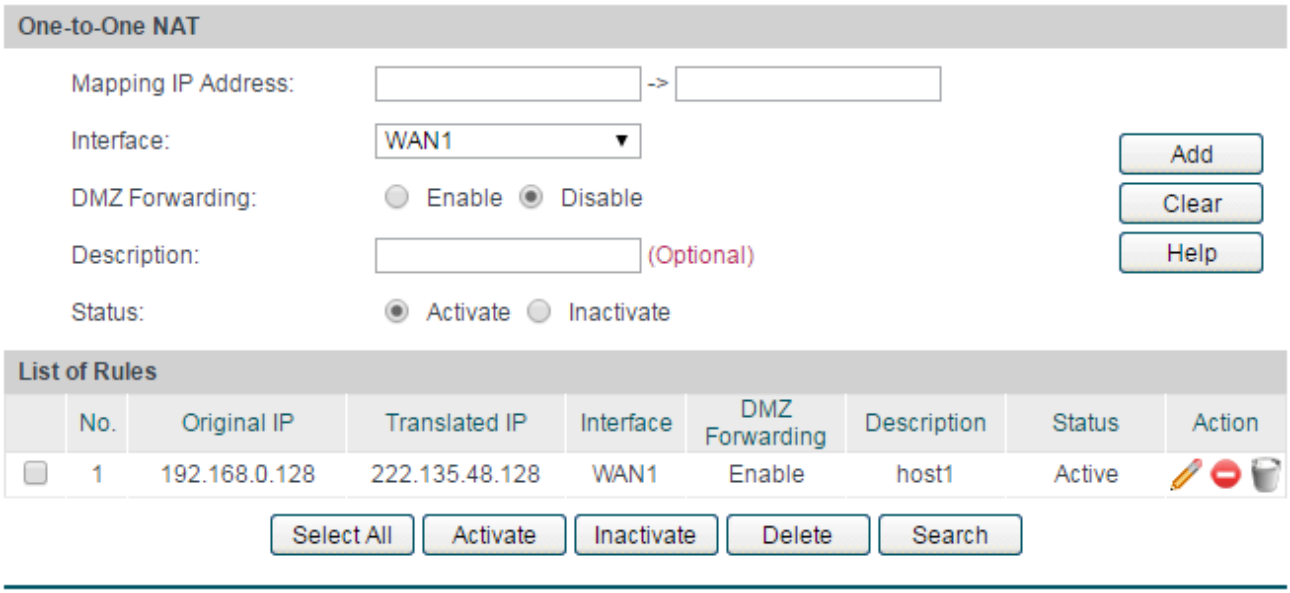


Figure 4-25 NAT Setup

The following items are displayed on this screen:

➢ **One-to-One NAT**

Mapping IP Address: Enter the Original IP Address in the first checkbox and Translated IP Address in the second checkbox. TL-R480T+ allows mapping from LAN port to WAN port.

Interface: Select an interface for forwarding data packets.

DMZ Forwarding: Enable or disable DMZ Forwarding. The packets transmitted to the Translated IP Address will be forwarded to the host of Original IP if DMZ Forwarding is enabled.

Description: Give a description for the entry.

Status: Activate or inactivate the entry.

➢ **List of Rules**

In this table, you can view the information of the entries and edit them by the Action buttons.

The first entry in Figure 4-25 indicates: The IP address of host1 in local network is 192.168.0.128 and the WAN IP address after NAT mapping is specified to be 222.135.48.128. The data packets are transmitted from WAN1 port. DMZ Forwarding and this entry are both activated.

Note:

One-to-One NAT entries take effect only when the Connection Type of WAN is Static IP. Changing the Connection type from Static IP to other ones will make the entries attached to the interface disabled.

4.5.1.3 Multi-Nets NAT

Multi-Nets NAT functions to allow the IP under LAN within multiple subnets to access the Internet via NAT.

Choose the menu **Advanced→NAT→Multi-Nets NAT** to load the following page.

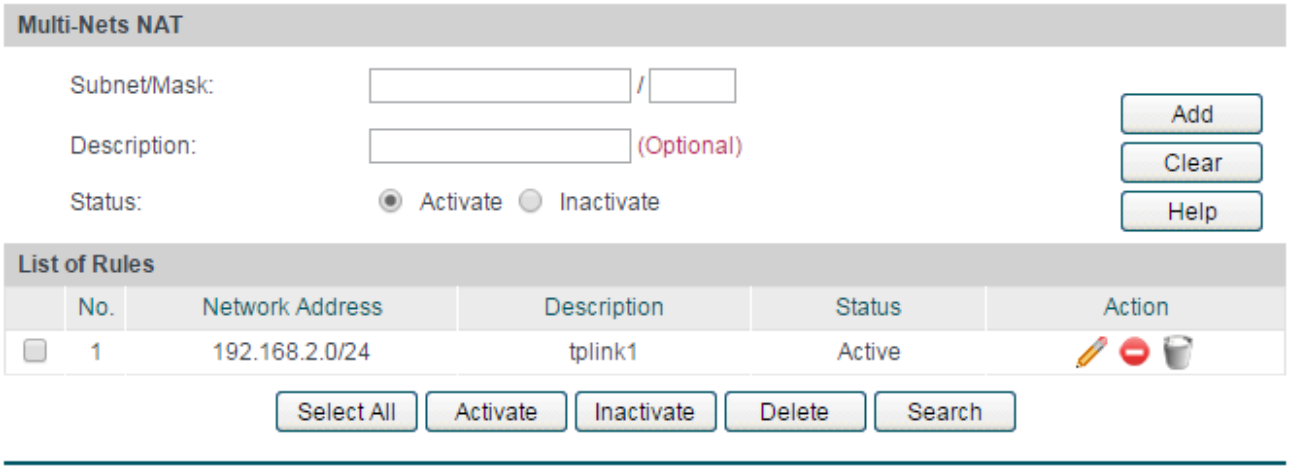


Figure 4-26 Multi-Nets NAT

The following items are displayed on this screen:

➢ **Multi-Nets NAT**

Subnet/Mask: Enter the subnet/mask to make the address range for the entry.

Description: Give a description for the entry.

Status: Activate or inactivate the entry.

➢ **list of Rules**

You can view the information of the entries and edit them by the Action buttons.

The first entry in Figure 4-26 indicates that: This is a Multi-Nets NAT entry named tplink1. The subnet under the LAN port of the router is 192.168.2.0/24 and this entry is activated. After the corresponding Static Route entry is set, the hosts within this subnet can access the Internet through the router via NAT.

Note:

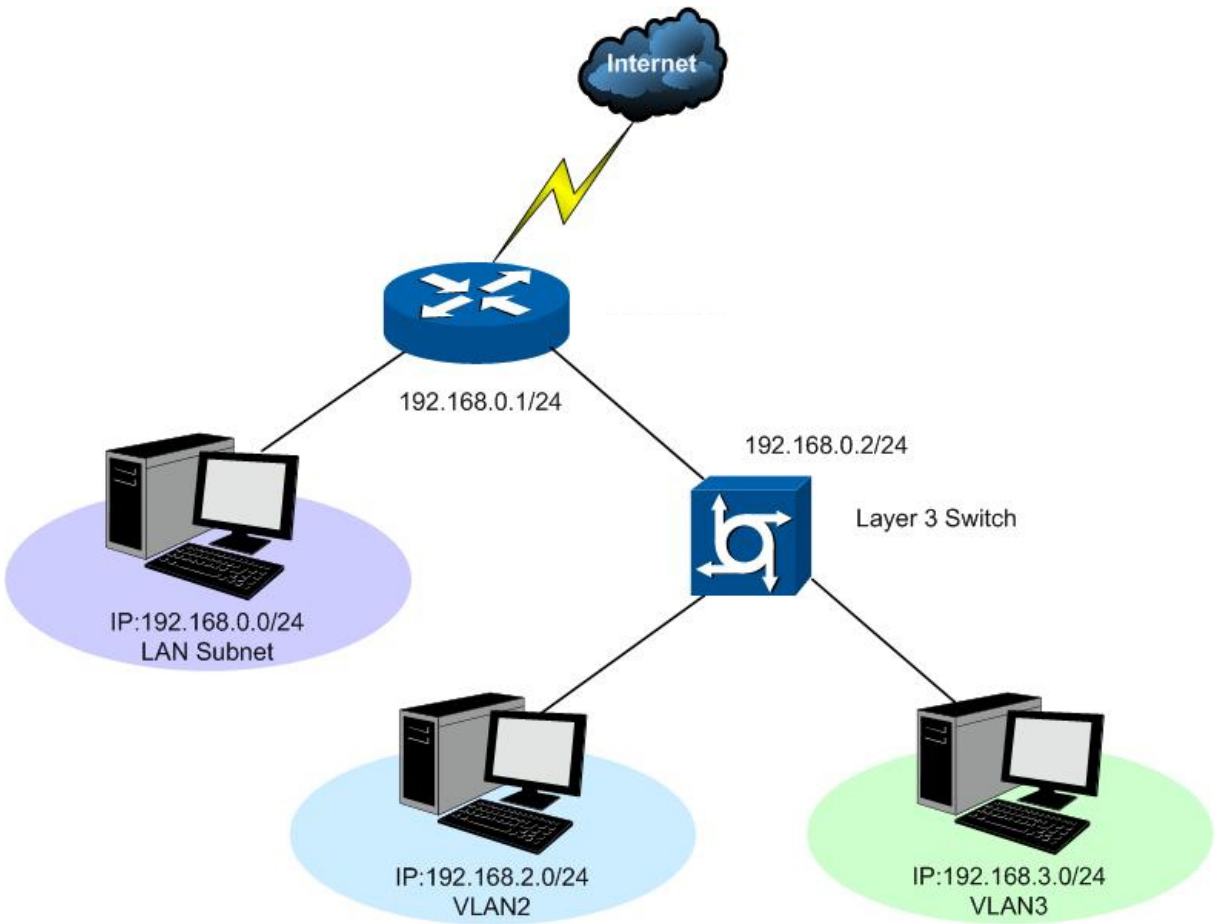
- Multi-Nets NAT entry takes effect only when cooperating with the corresponding Static Route entries.
- For detailed setting of subnet mask, please refer to the **Appendix B FAQ.**

Application Example

➢ **Network Requirements**

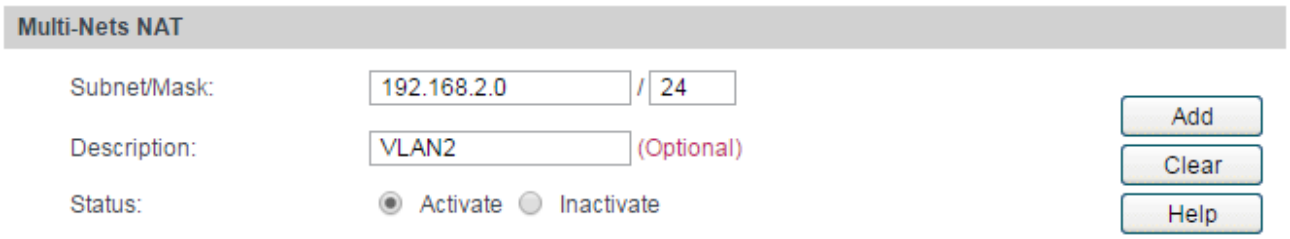
The LAN subnet of TL-R480T+ is 192.168.0.0 /24, the subnet of VLAN2 under a three layer switch is 192.168.2.0 /24, while the subnet of VLAN3 is 192.168.3.0 /24. The IP of VLAN for cascading the switch to the router is 192.168.0.2. Now the hosts within VLAN2 and VLAN3 desire to access the Internet.

The network topology is shown as the following:

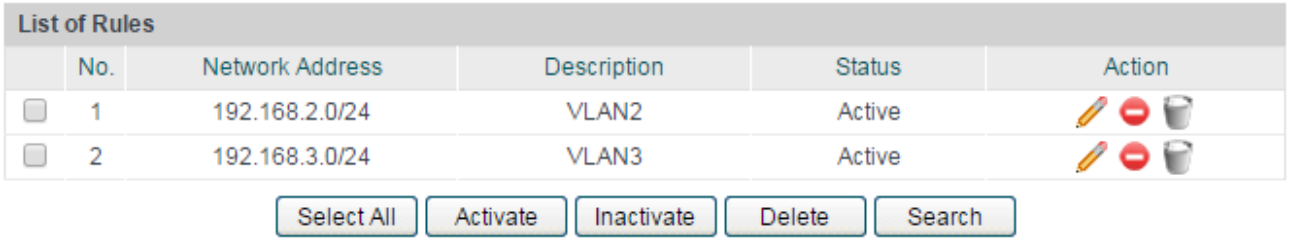


➢ **Configuration procedure**

1. Establish the Multi-Nets NAT entries with Subnet/Mask of VLAN2 and VLAN3.

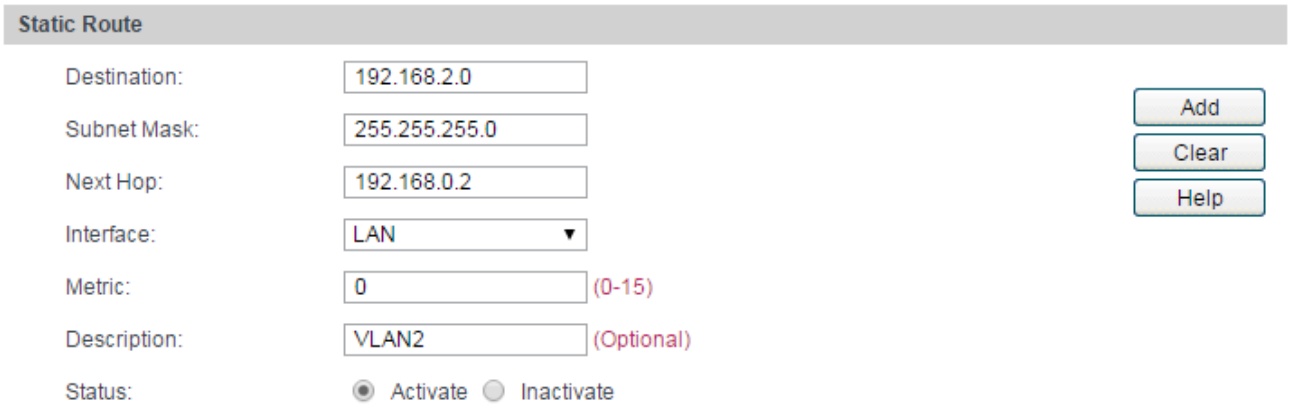


The configured entries are as follows:

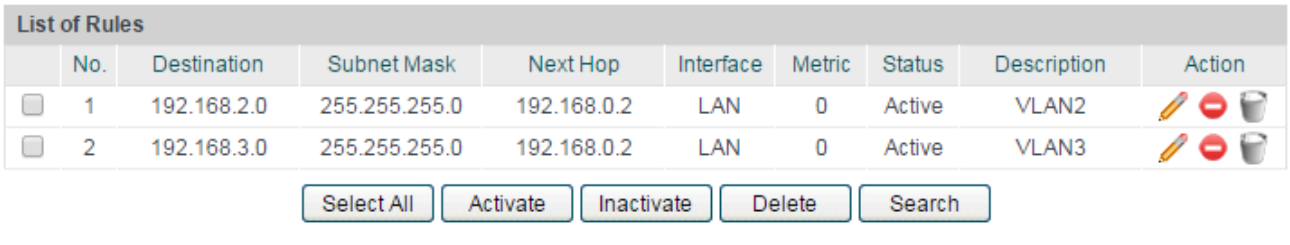


2. Then set the corresponding Static Route entry, enter the IP address of the interface connecting the router and the three layer switch into the Next Hop field.

Choose the menu **Advanced→Routing→Static Route** to load the following page.



The set Static Route entry is as follows:



4.5.1.4 Virtual Server

Virtual server can be used for setting up public services in your private network, such as DNS, Email and FTP. Virtual server can define a service port. All the service requests to this port will be transmitted to the LAN server appointed by the router via IP address.

Choose the menu **Advanced→NAT→Virtual Server** to load the following page.

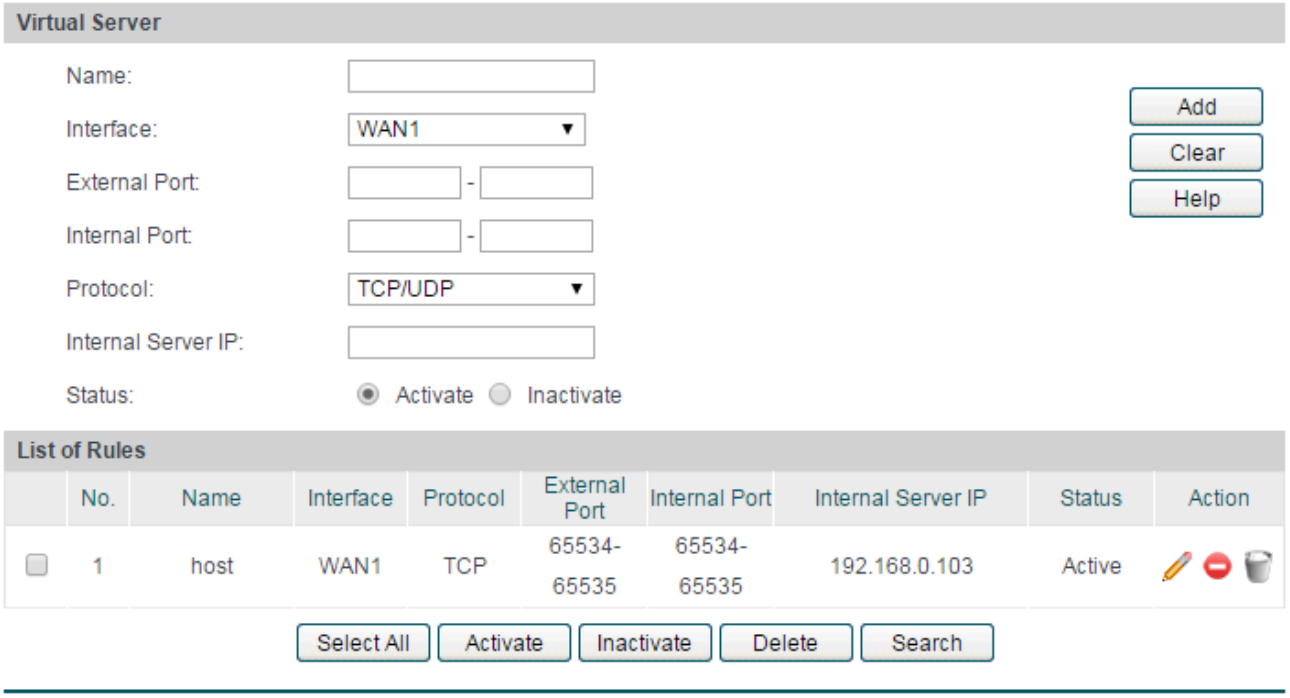


Figure 4-27 Virtual Server

The following items are displayed on this screen:

➢ **Virtual Server**

Name: Enter a name for Virtual Server entry. Up to 28 characters can be entered.

Interface: Select an interface for forwarding data packets.

External Port: Enter the service port or port range provided by router for accessing external network. All requests from Internet to the service port(s) will be redirected to the specified server in local network.

Internal Port: Specify the service port of the LAN host as virtual server.

Protocol: Specify the protocol used for the entry.

Internal Server IP: Enter the IP address of the specified internal server for the entry. All the requests from the Internet to the specified LAN port will be redirected to this host.

Status: Activate or inactivate the entry.

Note:

- The External port and Internal Port should be set in the range of 1-65535.
- The external ports of different entries should be different, whereas the internal ports can be the same.

➢ **List of Rules**

In this table, you can view the information of the entries and edit them by the Action buttons.

The first entry in Figure 4-27 indicates: This is a Virtual Server entry named host, all the TCP data packets from the Internet to port 65534-65535 of the router will be redirected to the port 65534-65535 of the LAN host with IP address of 192.168.0.103, and the data packets are transmitted from WAN1 port. This entry is activated.

4.5.1.5 Port Triggering

Some applications require multiple connections, like Internet games, video conferencing, Internet calling, P2P download and so on. Port Triggering is used for those applications requiring multiple connections.

When an application initiates a connection to the trigger port, all the ports corresponding to the incoming port will open for follow-up connections.

Choose the menu **Advanced→NAT→Port Triggering** to load the following page.

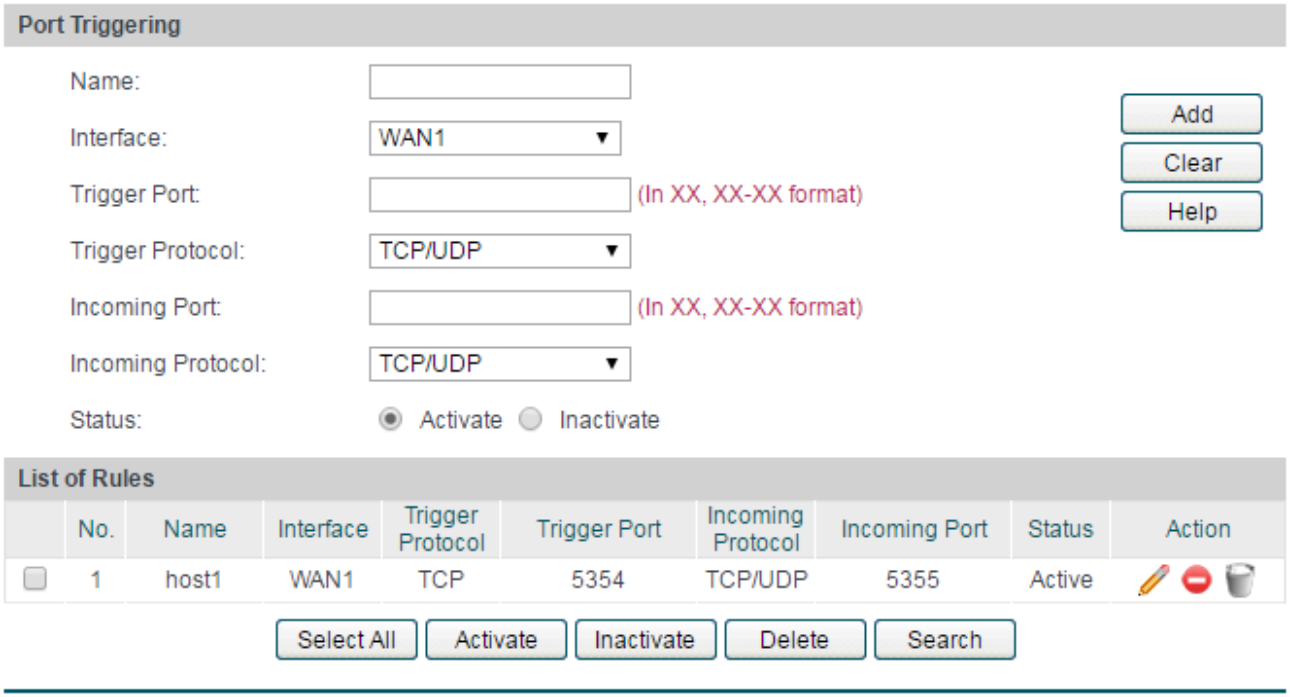


Figure 4-28 Port Triggering

The following items are displayed on this screen:

➢ **Port Triggering**

Name: Enter a name for Port Triggering entries. Up to 28 characters can be entered.

Interface: Select an interface for forwarding data packets.

Trigger Port: Enter the trigger port number or range of port numbers. Only when the trigger port initiates connection will all the corresponding incoming ports open and provide service for the applications, otherwise the incoming ports will not open.

Trigger Protocol: Select the protocol used for trigger port.

Incoming Port: Enter the incoming port number or range of port numbers. The incoming port will open for follow-up connection after the trigger port initiates connection.

Incoming Protocol: Select the protocol used for incoming port.

Status: Activate or inactivate the entry.

Note:

- The Trigger Port and Incoming Port should be set in the range of 1-65535. The Incoming Port can be set in a continuous range such as 8690-8696.
- The router supports up to 16 Port Triggering entries. Each entry supports at most 5 groups of trigger ports and overlapping between the ports is not allowed.
- Each entry supports at most 5 groups of incoming ports and the sum of incoming ports you set for each entry should not be more than 100.

➢ **List of Rules**

In this table, you can view the information of the entries and edit them by the Action buttons.

The first entry in Figure 4-28 indicates that: This is a Port Triggering entry named host1, when the LAN host initiates a TCP request via port of 5354, the incoming port 5355 will open for TCP and UDP protocol, and the data packets are transmitted from WAN1 port. This entry is activated.

4.5.1.6 ALG

Some special protocols such as FTP, H.323, SIP, IPsec and PPTP will work properly only when ALG (Application Layer Gateway) service is enabled.

Choose the menu **Advanced→NAT→ALG** to load the following page.

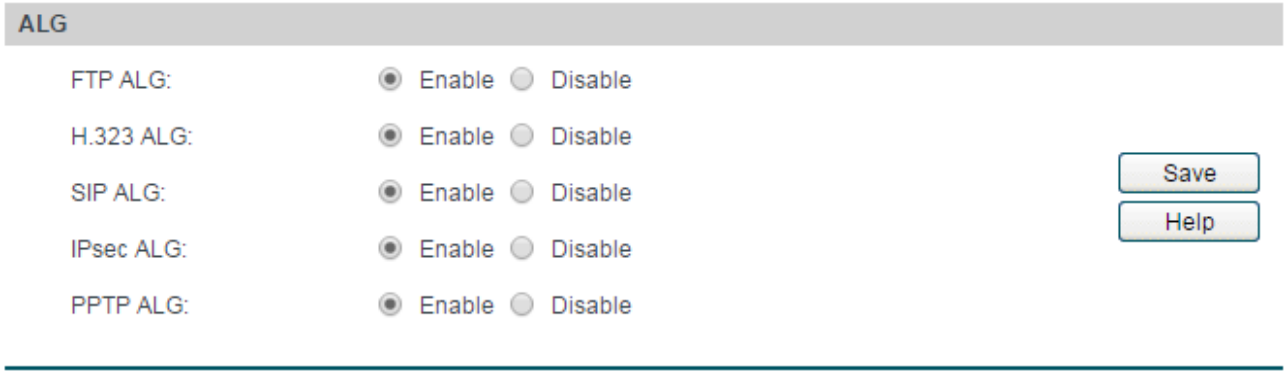


Figure 4-29 ALG

The following items are displayed on this screen:

- **ALG**

FTP ALG: Enable or disable FTP ALG. The default setting is enabled. It is recommended to keep the default setting if no special requirement.

H.323 ALG: Enable or disable H.323 ALG. The default setting is enabled. H.323 is used for various applications such as NetMeeting and VoIP.

SIP ALG: Enable or disable SIP ALG. The default setting is enabled. It is recommended to keep the default setting if no special requirement.

IPsec ALG: Enable or disable IPsec ALG. The default setting is enabled. It is recommended to keep default if no special requirement.

PPTP ALG: Enable or disable PPTP ALG. The default setting is enabled. It is recommended to keep default if no special requirement.

4.5.2 Traffic Control

Traffic Control functions to control the bandwidth by configuring rules for limiting various data flows. In this way, the network bandwidth can be reasonably distributed and utilized.

4.5.2.1 Setup

Choose the menu **Advanced→Traffic Control→Setup** to load the following page.

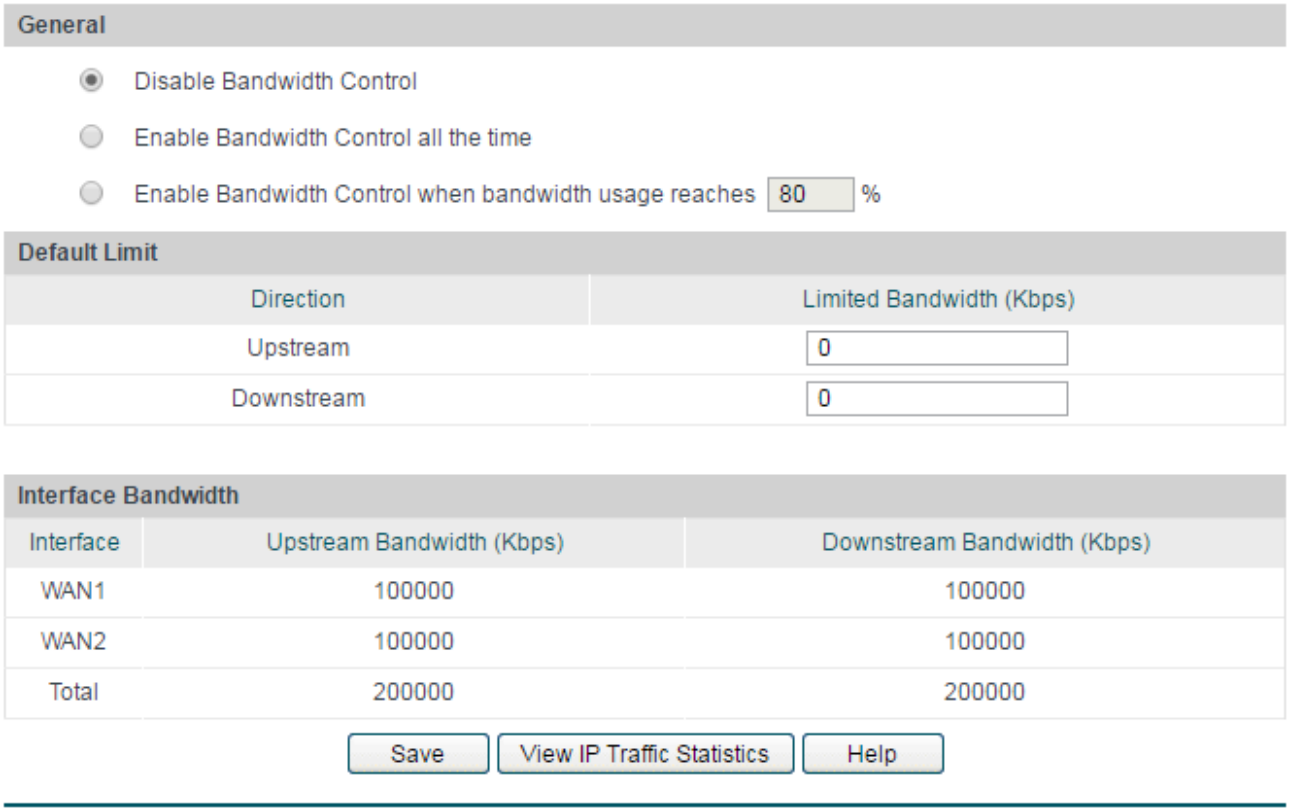


Figure 4-30 Configuration

The following items are displayed on this screen:

➢ **General**

Disable Bandwidth Control: Select this option to disable Bandwidth Control.

Enable Bandwidth Control all the time: Select this option to enable Bandwidth Control all the time.

Enable Bandwidth Control When: With this option selected, the Bandwidth Control will take effect when the bandwidth usage reaches the specified value.

➢ **Default Limit**

Limited Bandwidth: Default Limit applies only for users that are not constrained by Bandwidth Control Rules. These users share certain bandwidth with upper limit configured here. Value 0 means all the remained bandwidth is available to use.

➢ **Interface Bandwidth**

Interface: Displays the current enabled WAN port(s). The Total bandwidth is equal to the sum of bandwidth of the enabled WAN ports.

Upstream Bandwidth: Displays the bandwidth of each WAN port for transmitting data. The Upstream Bandwidth of WAN port can be configured on **WAN** page.

Downstream Bandwidth: Displays the bandwidth of each WAN port for receiving data. The Downstream Bandwidth of WAN port can be configured on **WAN** page.

Note:

- The Upstream/Downstream Bandwidth of WAN port you set must not be more than the bandwidth provided by ISP. Otherwise the Traffic Control will be invalid.
- If there are data flowing into the router from interface A and out from interface B while the downstream bandwidth of A is different from the upstream bandwidth of B, then the smaller one should be considered as the effective bandwidth, and vise versa.
- Click the <View IP Traffic Statistics> button to jump to IP Traffic Statistics page.

4.5.2.2 Bandwidth Control

On this page, you can configure the Bandwidth Control function.

Choose the menu **Advanced→Traffic Control→Bandwidth Control** to load the following page.

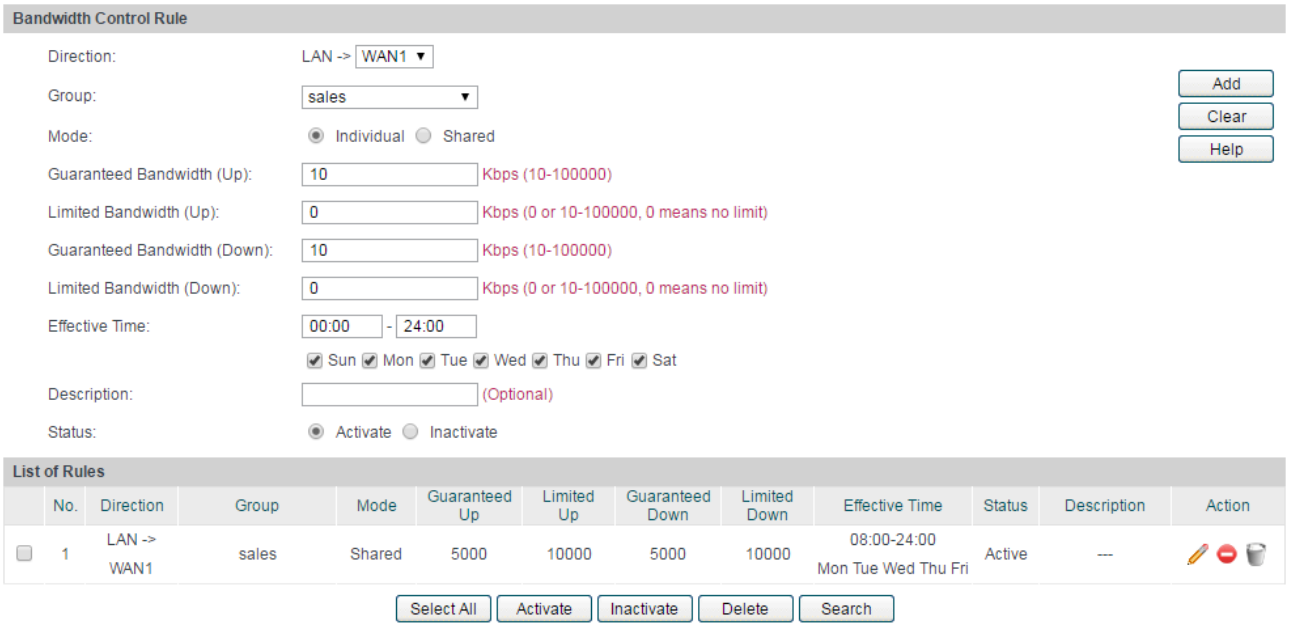


Figure 4-31 Bandwidth Control

The following items are displayed on this screen:

➢ **Bandwidth Control Rule**

Direction: Select the data stream direction for the entry. The direction of arrowhead indicates the data stream direction WAN-ALL means all WAN ports through which the data flow might pass. Individual WAN port cannot be selected after WAN-ALL rules are added.

Group: Select the group to define the controlled users.

Mode: Individual: The bandwidth of each user equals to the current bandwidth of this entry.

Shared: The total bandwidth of all controlled IP addresses equals to the current bandwidth of this entry.

Guaranteed Bandwidth (Up): Specify the Guaranteed Upstream Bandwidth for this entry.

Limited Bandwidth (Up): Specify the Limited Upstream Bandwidth for this entry.

Guaranteed Bandwidth (Down): Specify the Guaranteed Downstream Bandwidth for this entry.

Limited Bandwidth (Down):	Specify the Limited Downstream Bandwidth for this entry.
Effective Time:	Specify the time for the entry to take effect.
Description:	Give a description for the entry.
Status:	Activate or inactivate the entry.

➢ **List of Rules**

You can view the information of the entries and edit them by the Action buttons.

The first entry in Figure 4-31 indicates: The users within group "sales" share the bandwidth and the Downstream/Upstream Guaranteed Bandwidth is 5000kbps, while the Downstream/Upstream Limited bandwidth is 10000kbps. This entry takes effect at 8 a.m. to 10 p.m. from Monday to Friday.

Note:

- The premise for single rule taking effect is that the bandwidth of the interface for this rule is sufficient and not used up.
- It is impossible to satisfy all the guaranteed bandwidth if the total guaranteed bandwidth specified by all Bandwidth Control rules for certain interface exceeds the physical bandwidth of this interface.

4.5.3 Session Limit

The amount of TCP and UDP sessions supported by the router is finite. If there are some local hosts transmitting too many TCP and UDP sessions to the public network, the communication quality of the other local hosts will be affected, thus it is necessary to limit the sessions of those hosts.

4.5.3.1 Session Limit

On this page, you can configure the session limit to specified PCs.

Choose the menu **Advanced→Session Limit→Session Limit** to load the following page.

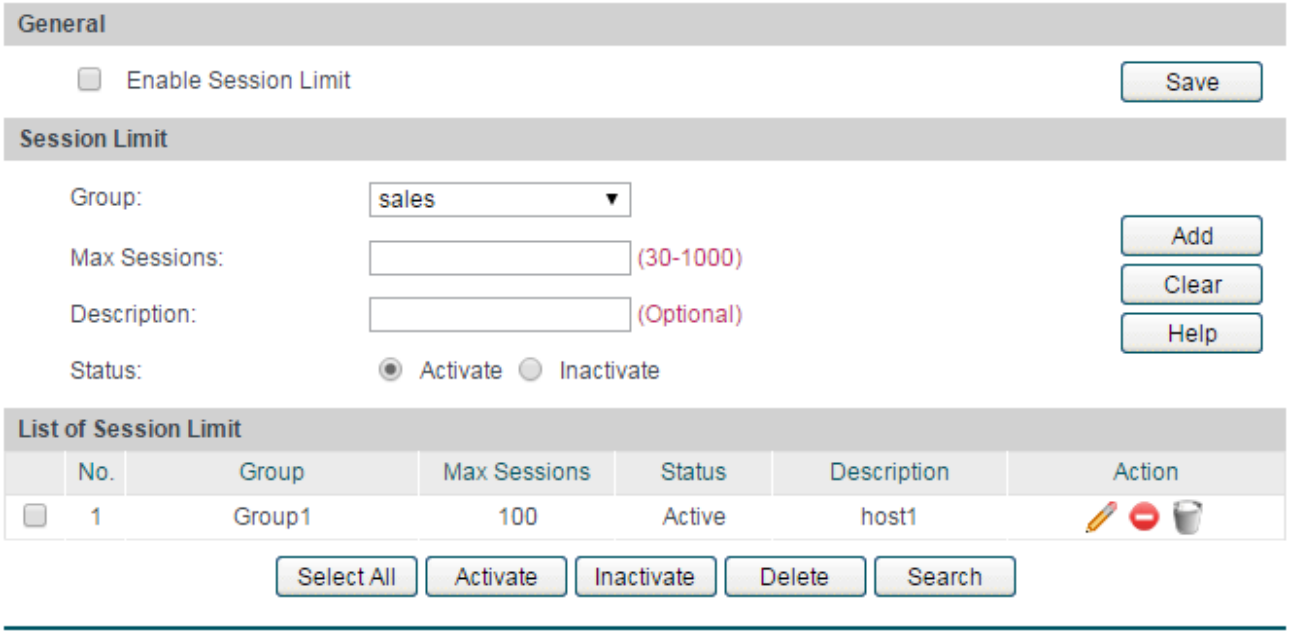


Figure 4-32 Session Limit

The following items are displayed on this screen:

➢ **General**

Enable Session Limit: Check here to enable Session Limit, otherwise all the Session Limit entries will be disabled.

➢ **Session Limit**

Group: Select a group to define the controlled user.

Max. Sessions: Enter the max. Sessions for the users.

Description: Give a description for the entry.

Status: Activate or inactivate the entry.

➢ **List of Session Limit**

You can view the information of the entries and edit them by the Action buttons.

The first entry in Figure 4-32 indicates: The amount of maximum sessions for the hosts within group1 is 100 and this entry is enabled.

4.5.3.2 Session List

On this page, you can view the Session Limit information of hosts configured with Session Limit.

Choose the menu **Advanced→Session Limit→Session List** to load the following page.

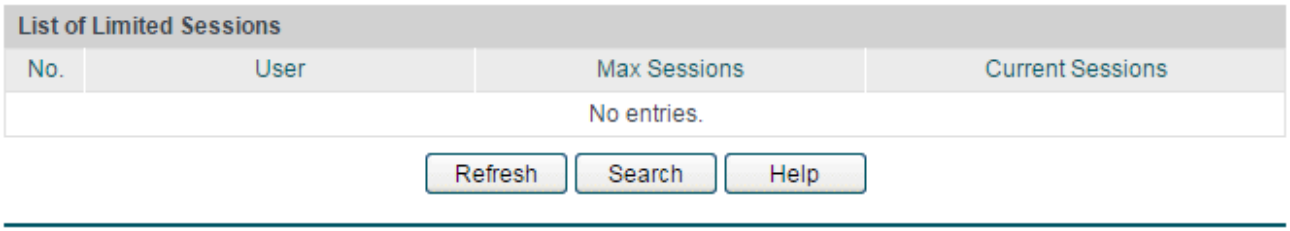


Figure 4-33 Session List

In this table, you can view the session limit information of users configured with Session Limit. Click the <Refresh> button to get the latest information.

4.5.4 Load Balance

On this part, you can configure how the traffic load is shared by the WAN ports to optimize the resource utilization.

4.5.4.1 Configuration

Choose the menu **Advanced→Load Balance→Configuration** to load the following page.

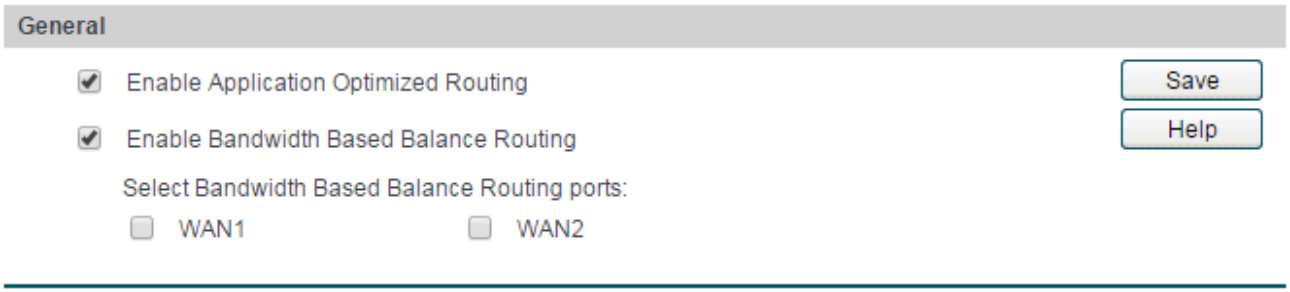


Figure 4-34 Configuration

With the box before **Enable Application Optimized Routing** checked, the router will consider the source IP address and destination IP address of the packets as a whole and record the WAN port they pass through. And then the packets with the same source IP address and destination IP address or destination port will be forwarded to the recorded WAN port. This feature is to ensure the multi-connected applications to work properly.

Check the box before **Enable Bandwidth Based Balance Routing** and select the WAN port below, Load Balance of the specified WAN port will be enabled automatically if no routing rules are set.

Then click the <Save> button to apply the settings.

Note:

The WAN ports not connecting to the Internet will not apply Intelligent Balance, please do not select them.

4.5.4.2 Policy Routing

Policy Routing provides a more accurate way to control the routing based on the policy defined by the network administrator.

Choose the menu **Advanced→Load Balance→Policy Routing** to load the following page.

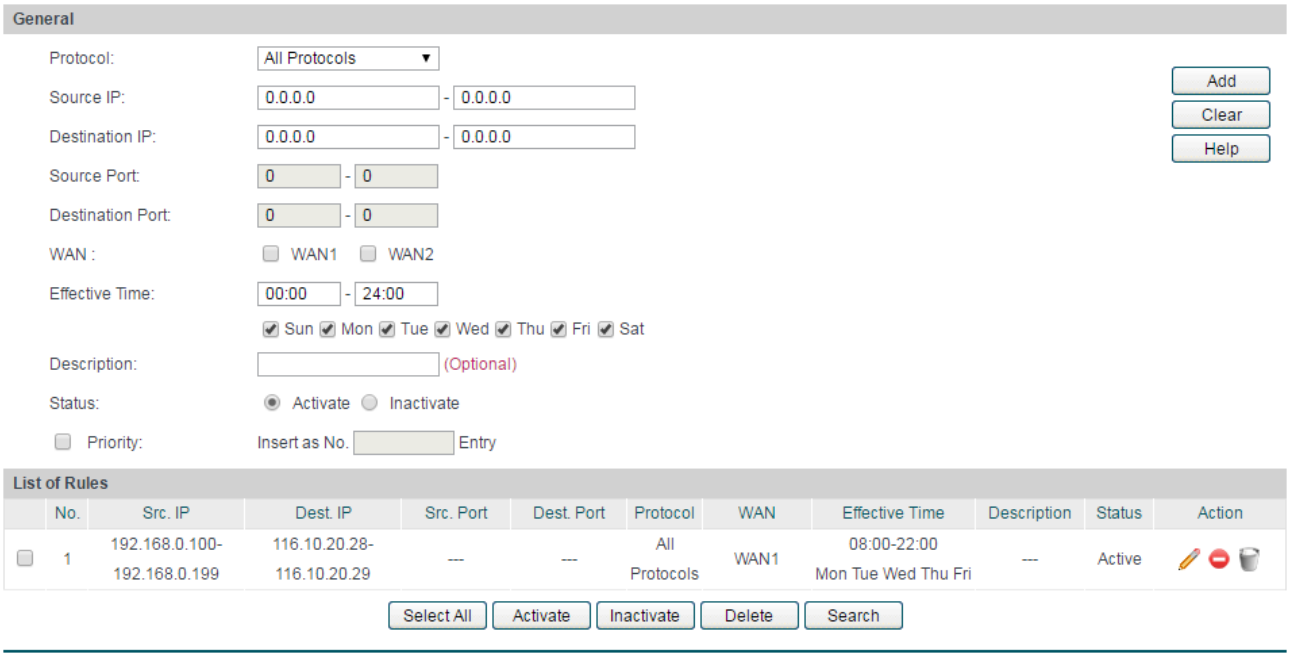


Figure 4-35 Policy Routing

The following items are displayed on this screen:

➢ **General**

Protocol: Select the protocol for the entry in the drop-down list. If the protocol you want to set is not in the list, you can add it to the list on **4.5.4.4 Protocol** page.

Source IP: Enter the source IP range for the entry. 0.0.0.0 - 0.0.0.0 means any IP is acceptable.

Destination IP: Enter the destination IP range for the entry. 0.0.0.0 - 0.0.0.0 means any IP is acceptable.

Source Port: Enter the source Port range for the entry, which is effective only when the protocol is TCP, UDP or TCP/UDP. The default value is 1 – 65535, which means any port is acceptable.

Destination Port: Enter the destination port range for the entry, which is effective only when the protocol is TCP, UDP or TCP/UDP. The default value is 1 – 65535, which means any port is acceptable.

WAN: Select the WAN port for transmitting packets.

Effective Time: Specify the time for the entry to take effect.

Status: Activate or inactivate the entry.

Priority: Select this option to specify the priority for the added entries. The latest enabled entry will be displayed at the end of the list by default.

- **List of Rules**

  You can view the information of the entries and edit them by the Action buttons.

  The first entry in Figure 4-35 indicates: All the packets with Source IP between 192.168.0.100 and 192.168.0.199 and Destination IP between 116.10.20.28 and 116.10.20.29 will be forwarded from WAN1 port, regardless of the port and protocol. This entry is activated d and will take effect at 8 am to 10 pm from Monday to Friday.

4.5.4.3 Link Backup

With Link Backup function, the router will switch all the new sessions from dropped line automatically to another to keep an always on-line network.

On this page, you can configure the Link Backup function based on actual need to reduce the traffic burden of WAN port and improve the network efficiency.

Choose the menu **Advanced→Load Balance→Link Backup** to load the following page.

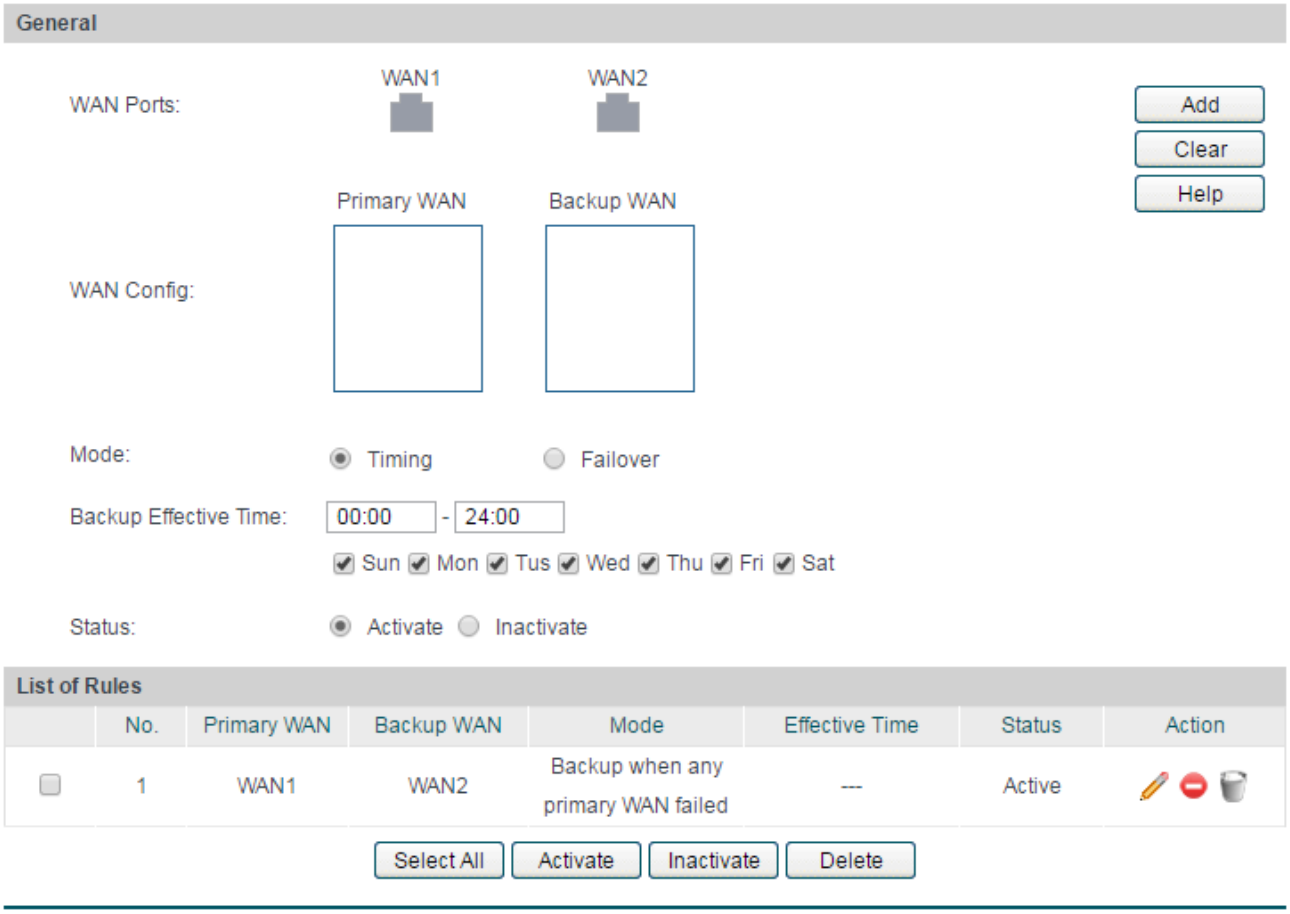


Figure 4-36 Link Backup

The following items are displayed on this screen:

➢ **General**

WAN Ports: Displays all the WAN ports in use. You can drag the light-blue WAN button to primary and backup WAN list. The color of WAN button changing to gray indicates that the WAN port is already in the primary and backup WAN list.

WAN Config: The WAN port in the secondary WAN list will share the traffic for the WAN in the primary WAN list under the specified condition. The primary WAN list can contain one or more WAN ports, while the backup WAN list contains only one WAN port.

Mode: You can select Timing or Failover.

Timing: Link Backup will be enabled if the specified effective time is reached. All the traffic on the primary WAN will switch to the backup WAN at the beginning of the effective time; the traffic on the backup WAN will switch to the

primary WAN at the ending of the effective time.

Failover: Specify the premise for Failover Mode. The backup WAN port will be enabled only when the premise is met.

Backup Effective Time: Specify the backup effective time if Timing Mode has been selected. Then the backup WAN port will be enabled, while the primary WAN port is disabled in the specified time period. When the start time you enter is not earlier than the end time, the default effective time is from the start time of the day to the end time of the next day.

Status: Activate or inactivate the entry.

➢ **List of Rules**

You can view the information of the entries and edit them by the Action buttons.

The first entry in Figure 4-36 indicates: WAN1 is the primary port and WAN2 is the backup port. WAN2 will be enabled while WAN1 is failed. This entry is enabled.

Note:

The same WAN port cannot be added to the primary and secondary WAN lists at the same time, and one WAN port should be added to only one list.

4.5.4.4 Protocol

On this page, you can specify the protocol for routing rules conveniently. A protocol constitutes of the name and number. The router predefines four commonly used protocols such as TCP, UDP, TCP/UDP and ICMP. Moreover, you can also add new protocols as your wish.

Choose the menu **Advanced→Load Balance→Protocol** to load the following page.

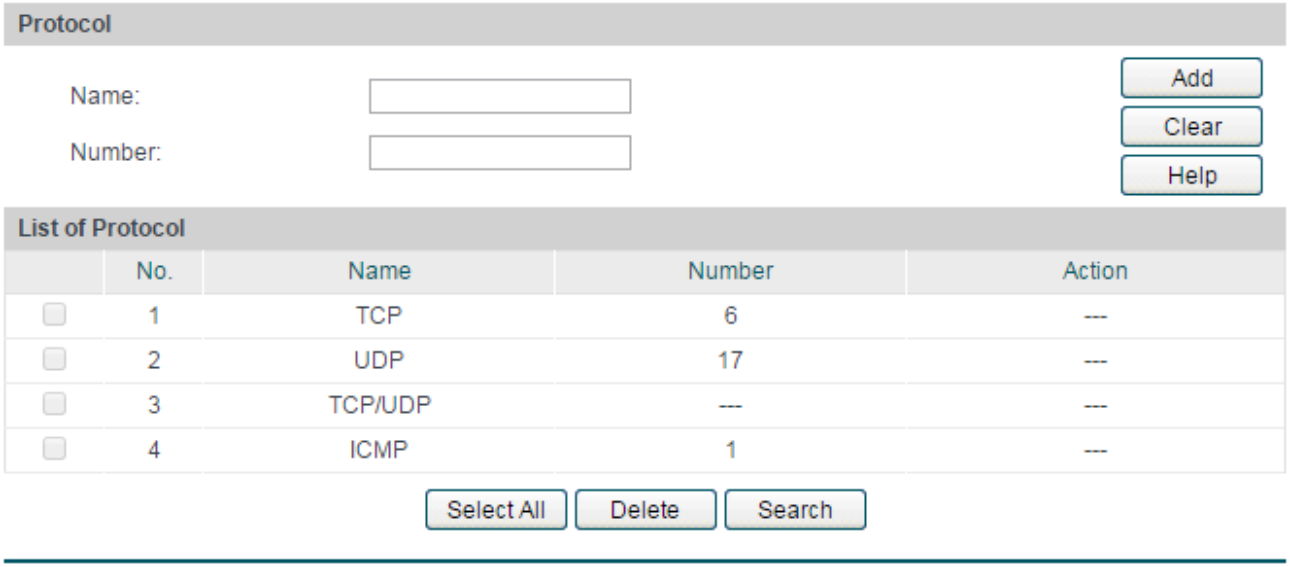


Figure 4-37 Protocol

The following items are displayed on this screen:

➢ **Protocol**

Name: Enter a name to indicate a protocol. The name will display in the drop-down list of Protocol on Access Rule page.

Number: Enter the Number of the protocol in the range of 0-255.

➢ **List of Protocol**

You can view the information of the entries and edit them by the Action buttons.

Note:

The system predefined protocols cannot be configured.

4.5.5 Routing

4.5.5.1 Static Route

Routing is the process of selecting optimized paths in a network along which to send network traffic. Static Route is a kind of special routing configured by the administrator, which is simple, efficient, and reliable.

Commonly used in small-sized network with fixed topology, Static Route does not change along with the network topology automatically. The administrator should modify the static route information manually as long as the network topology or link status is changed.

Choose the menu **Advanced→Routing→Static Route** to load the following page.

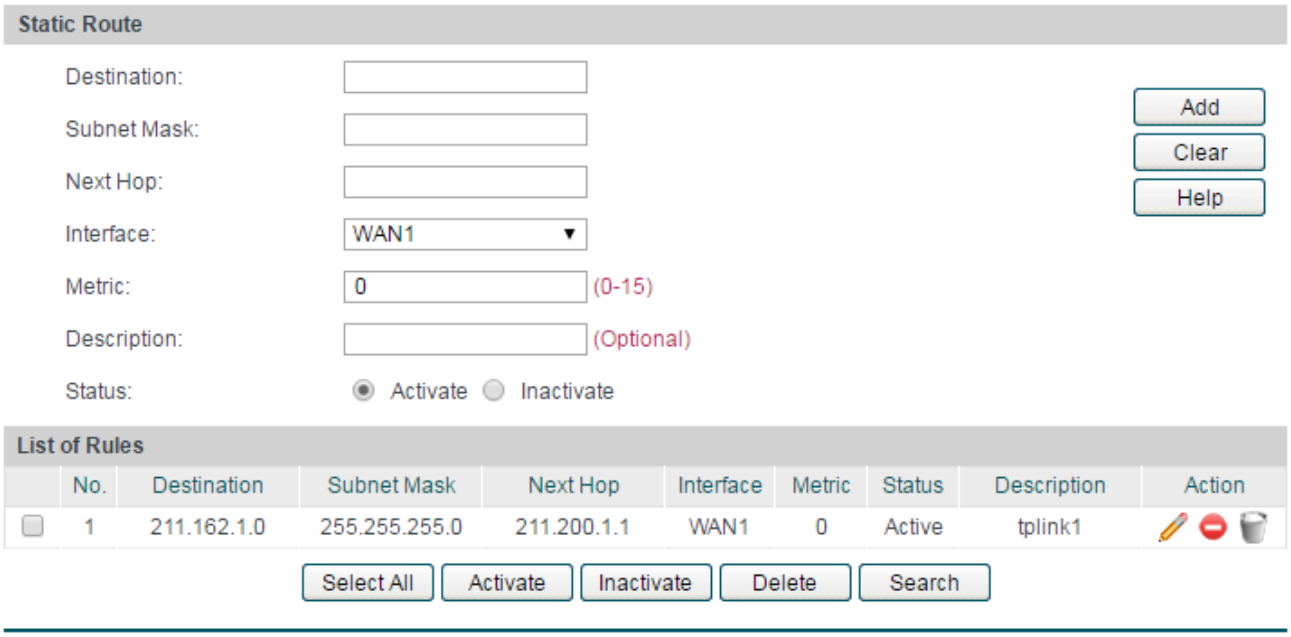


Figure 4-38 Static Route

The following items are displayed on this screen:

➢ **Static Route**

Destination: Enter the destination host the route leads to.

Subnet Mask: Enter the Subnet Mask of the destination network.

Next Hop: Enter the gateway IP address to which the packet should be sent next.

Interface: Select the physical network interface, through which this route is accessible.

Metric: Defines the priority of the route. The smaller the value is, the higher the priority is. The default value is 0. Keep the default value if unnecessary.

Description: Give a description for the entry.

Status: Activate or inactivate the entry.

➢ **List of Rules**

You can view the information of the entries and edit them by the Action buttons.

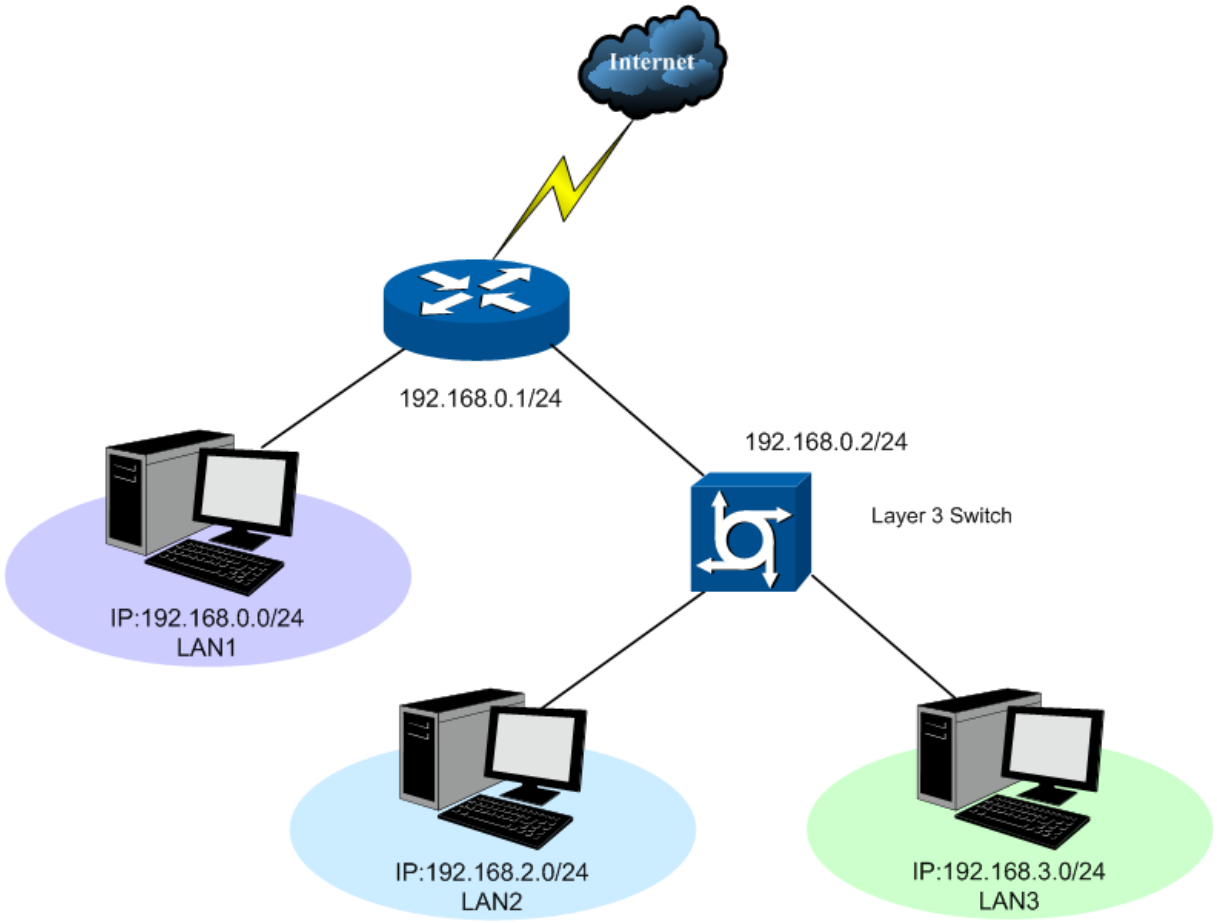
The first entry in Figure 4-38 indicates: If there are packets being sent to a device with IP address of 211.162.1.0 and subnet mask of 255.255.255.0, the router will forward the packets from WAN1 port to the next hop of 211.200.1.1.

Application Example

➢ **Network Requirements**

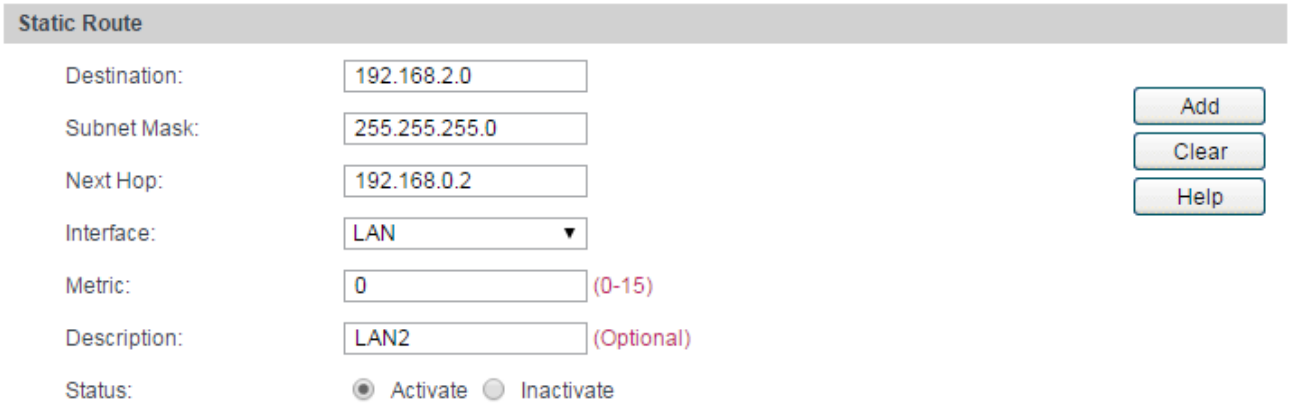
LAN1 is under the router and it uses network segment 192.168.0.0 /24. LAN2 and LAN3 are under a layer 3 switch and they use network segments 192.168.2.0 /24 and 192.168.3.0 /24 respectively. The IP address of the cascading LAN port between the layer 3 switch and the router is 192.168.0.2. Now the hosts within LAN1 desire to access the hosts within LAN2 and LAN3.

The network topology is shown as the following:



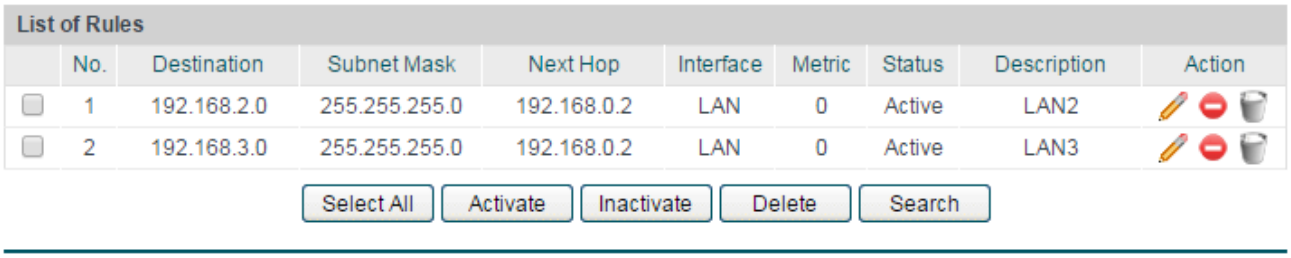
➢ **Configuration procedure**

1. On the **Static Route** page, add a static routing rule for LAN2 with destination address 192.168.2.0 (LAN2's IP address) and next hop address 192.168.0.2 (IP address of the cascading LAN port) as shown in the following figure. Then click the <Add> button.



2. Add a static routing rule for LAN3 by referring to step 2.

   The static routing rules are shown in the following figure.



4.6 Firewall

4.6.1 Anti ARP Spoofing

ARP (Address Resolution Protocol) is used to analyze and map IP addresses to the corresponding MAC addresses so that packets can be delivered to their destinations correctly.

ARP functions to translate the IP address into the corresponding MAC address and maintain an ARP Table, where the latest used IP address-to-MAC address mapping entries are stored. ARP protocol can facilitate the Hosts in the same network segment to communicate with one another or access to external network via Gateway. However, since ARP protocol is implemented with the premise that all the Hosts and Gateways are trusted, there are high security risks during ARP Implementation Procedure in the actual complex network.

The attacker may send the ARP spoofing packets with false IP address-to-MAC address mapping entries, and then the device will automatically update the ARP table after receiving wrong ARP packets, which results in a breakdown of the normal communication. Thus, ARP defense technology is generated to prevent the network from this kind of attack.

4.6.1.1 IP-MAC Binding

IP-MAC Binding functions to bind the IP address, MAC address of the host together and only allows the Hosts matching the bound entries to access the network.

Choose the menu **Firewall→Anti ARP Spoofing→IP-MAC Binding** to load the following page.

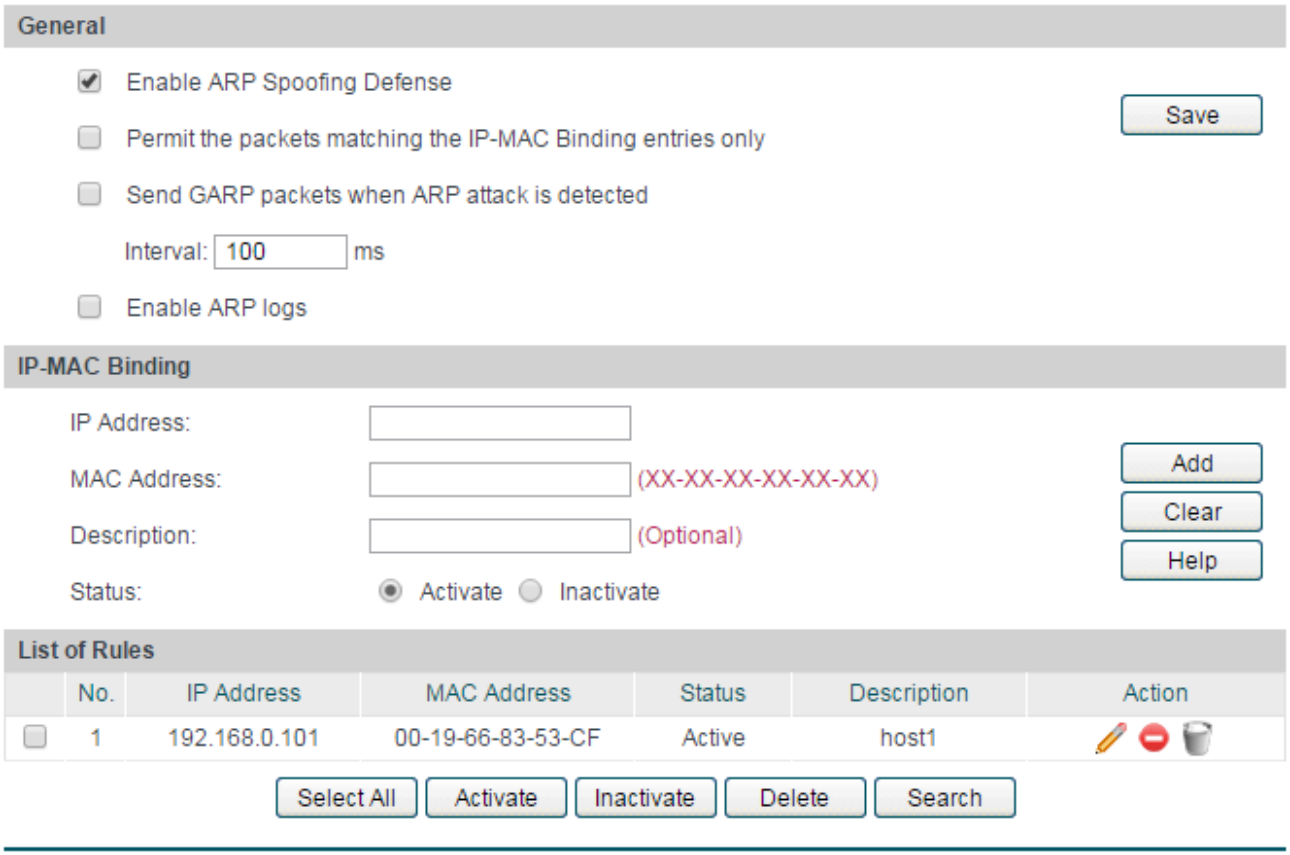


Figure 4-39 IP-MAC Binding

The following items are displayed on this screen:

➢ **General**

It is recommended to check all the options. You should import the IP and MAC address of the host to List of IP-MAC Binding and enable the corresponding entry before enabling "Permit the packets matching the IP-MAC Binding entries only".

When suffered ARP attack, the correct ARP information will be sent to the device suffering attack initiatively by GARP (Gratuitous ARP) packets, thus the error ARP information of the device will be replaced. You can set the packets sending rate in the Interval field.

Check the box before **Enable ARP Logs**, and the router will send ARP logs to the specified server. The IP address of server is the Server IP set on **4.8.7 Logs**.

➢ **IP-MAC Binding**

IP Address: Enter the IP Address to be bound.

MAC Address: Enter the MAC Address corresponding to the IP Address.

Description: Give a description for the entry.

Status: Activate or inactivate the entry.

➢ **List of Rules**

You can view the information of the entries and edit them by the Action buttons.

The first entry in Figure 4-39 indicates: The IP address of 192.168.1.101 and MAC address of 00-19-66-83-53-CF have been bound and this entry is activated.

Note:

If all the entries in the binding list are disabled and "Permit the packets of IP-MAC Binding entries only" option is selected and saved, the WEB management page of the router cannot be login. At the moment, you should restore the router to factory default and login again.

4.6.1.2 ARP Scanning

ARP Scanning feature enables the router to scan the IP address and corresponding MAC address and display them on the List of Scanning Result.

Choose the menu **Firewall→Anti ARP Spoofing→ARP Scanning** to load the following page.

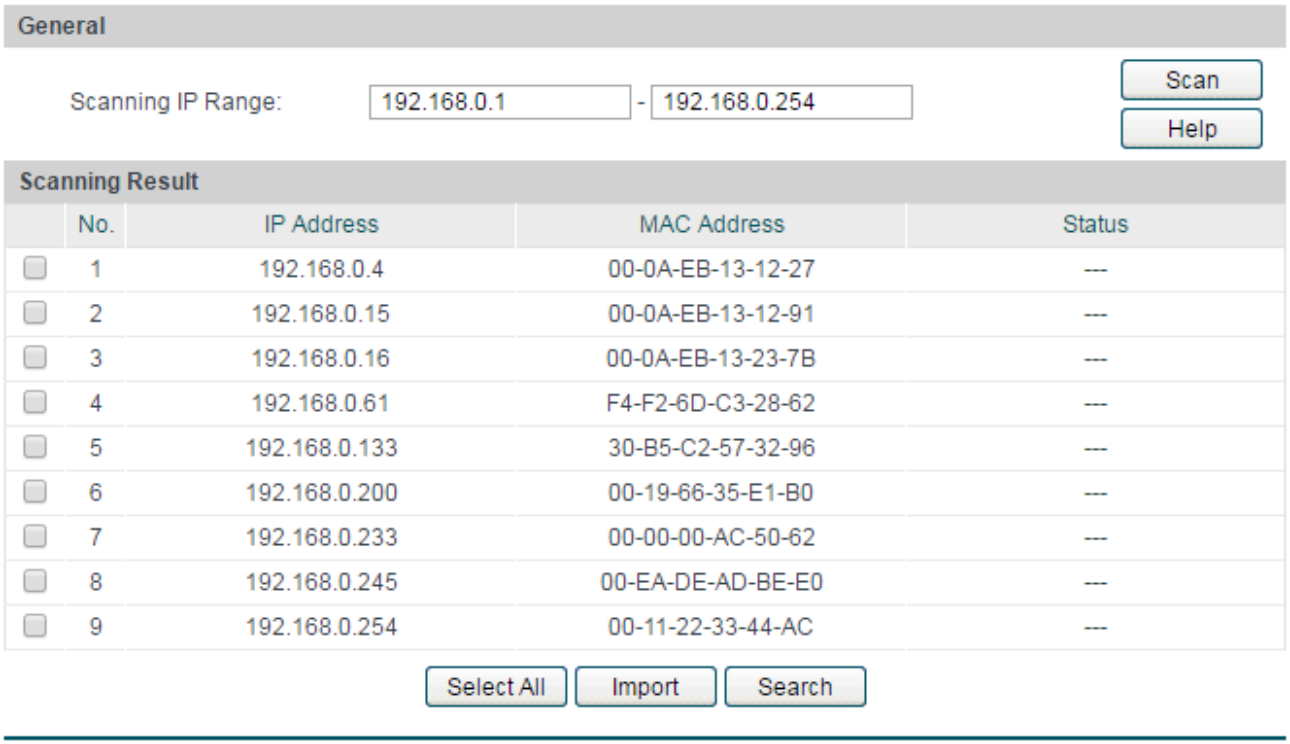


Figure 4-40 ARP Scanning

Enter the start and the end IP addresses in the Scanning IP Range field. Then click the <Scan> button, the router will scan all the active hosts within the scanning range and display the result in the list.

The entries displayed on the List of Scanning Result do not mean the IP and MAC addresses are already bound. The current status for the entry will display in the "Status" field.

---	Indicates that the IP and MAC address of this entry is not bound and may be replaced by error ARP information.
	Indicates that this entry is imported to the list on IP-MAC Binding page, but not effective yet.
	Indicates that the IP and MAC address of this entry is already bound.

To bind the entries in the list, check these entries and click the <Import> button, then the settings will take effect if the entries do not conflict with the existed entries.

Note:

If the local hosts suffered from ARP attack, you cannot add IP-MAC Binding entries on this page. Please add entries manually on **4.6.1.1 IP-MAC Binding**.

4.6.1.3 ARP List

On this page, the IP-MAC information of the hosts which communicated with the router recently will be saved in the ARP list.

Choose the menu **Firewall→Anti ARP Spoofing→ARP List** to load the following page.

ARP List

	No.	IP Address	MAC Address	Status
☐	1	192.168.0.4	00-0A-EB-13-12-27	---
☐	2	192.168.0.15	00-0A-EB-13-12-91	---
☐	3	192.168.0.16	00-0A-EB-13-23-7B	---
☐	4	192.168.0.61	F4-F2-6D-C3-28-62	---
☐	5	192.168.0.101	00-19-66-83-53-CF	
☐	6	192.168.0.133	30-B5-C2-57-32-96	---
☐	7	192.168.0.200	00-19-66-35-E1-B0	---
☐	8	192.168.0.233	00-00-00-AC-50-62	---
☐	9	192.168.0.245	00-EA-DE-AD-BE-E0	---
☐	10	192.168.0.254	00-11-22-33-44-AC	---

Select All | Import | Refresh | Search | Help

Figure 4-41 ARP List

The configurations for the entries is the same as the configuration of List of Scanning Result on **4.6.1.2 ARP Scanning** page.

The unbound IP-MAC information will be replaced by new IP-MAC information or be automatically removed from the list if it has not been communicated with others for a long time. This period is regarded as the aging time of the ARP information.

4.6.2 Attack Defense

With Attack Defense function enabled, the router can distinguish the malicious packets and prevent the port scanning from external network, so as to guarantee the network security.

Choose the menu **Firewall→Attack Defense→Attack Defense** to load the following page.

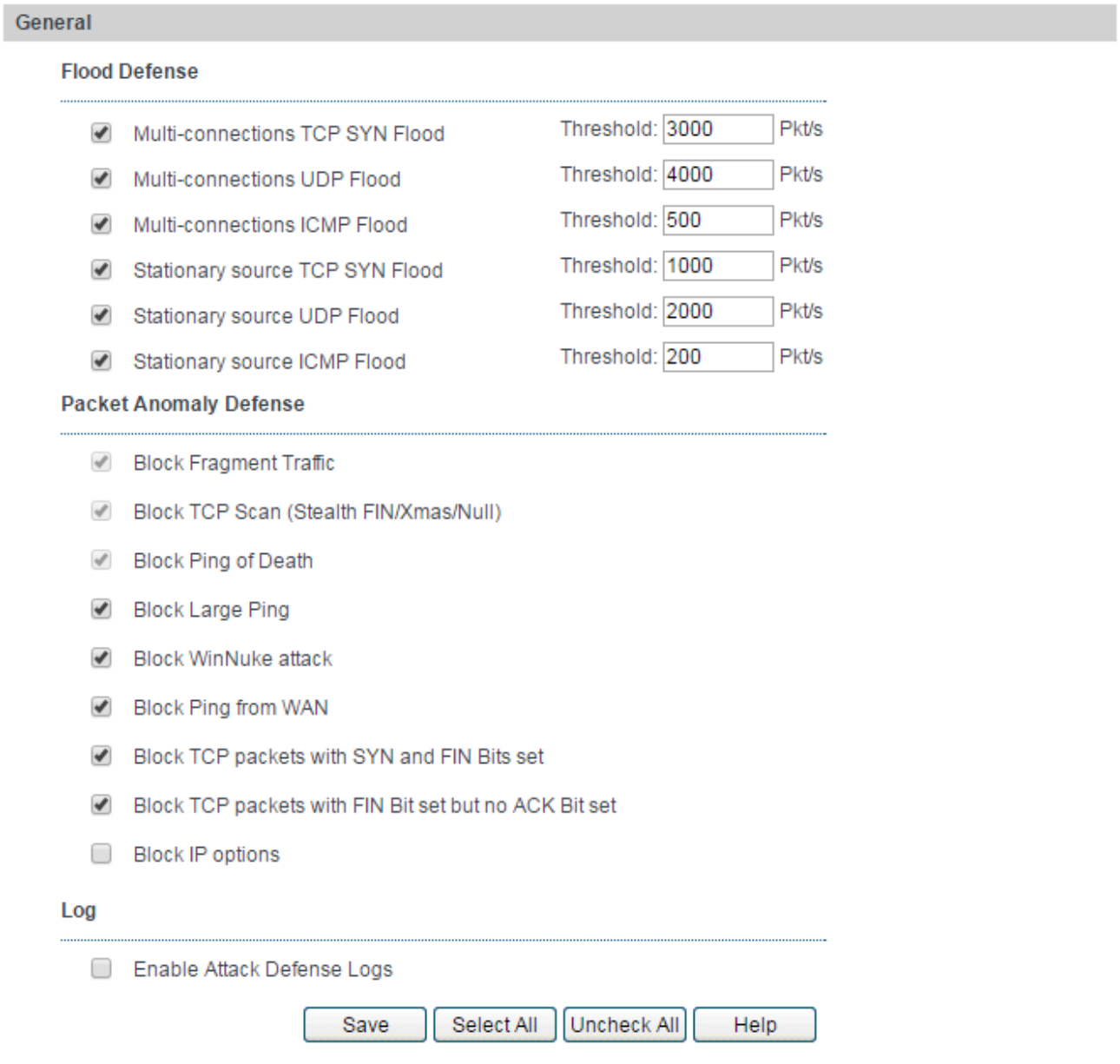


Figure 4-42 Attack Defense

The following items are displayed on this screen:

➢ **General**

Flood Defense:	Flood attack is a kind of commonly used DoS (Denial of Service), which including TCP SYN, UDP, ICMP and so on. It is recommended to check all the Flood Defense options and specify the corresponding thresholds. Keep the default settings if you are not sure.
Packet Anomaly Defense:	Packet Anomaly refers to the abnormal packets. It is recommended to select all the Packet Anomaly Defense options.
Enable Attack Defense Logs:	With this box checked, the router will record the defense logs.

Tips:

When IPTV works in Automatic mode, ensure that the Block IP options is not selected.

4.6.3 MAC Filtering

On this page, you can control the access to the Internet of local host by specifying their MAC addresses.

Choose the menu **Firewall→MAC Filtering→MAC Filtering** to load the following page.

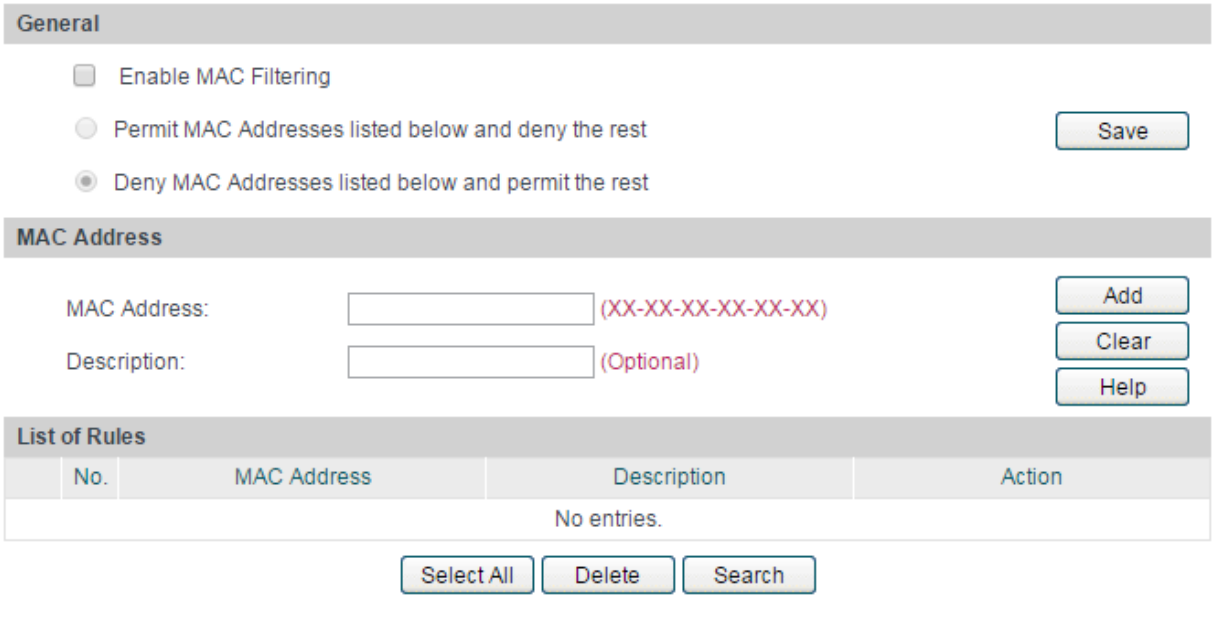


Figure 4-43 MAC Filtering

The following items are displayed on this screen:

- **General**

  To control the access to Internet for hosts in you private network, it is recommended to check the box before **Enable MAC Filtering** and select a filtering mode according to actual situation.

- **MAC Filtering**

  MAC Address: Enter the MAC Address to be filtered.

  Description: Give a description for the entry.

- **List of Rules**

  You can view the information of the entries and edit them by the Action buttons.

4.6.4 Access Control

4.6.4.1 URL Filtering

URL (Uniform Resource Locator) specifies where an identified resource is available and the mechanism for retrieving it. URL Filter functions to filter the Internet URL address, so as to provide a convenient way for controlling the access to Internet from LAN hosts.

Choose the menu **Firewall→Access Control→URL Filtering** to load the following page.

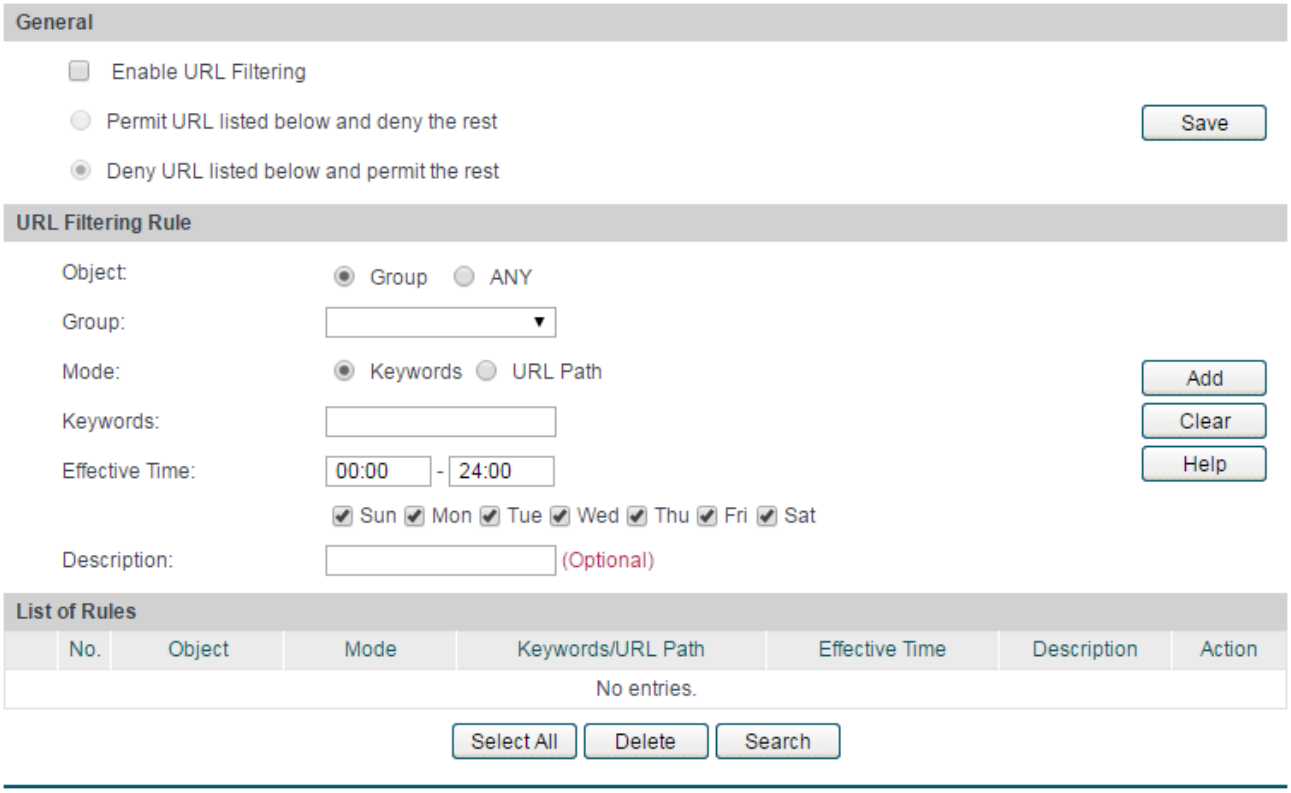


Figure 4-44 URL Filtering

The following items are displayed on this screen:

➢ **General**

To control the access to Internet for hosts in your private network, you are recommended to check the box before **Enable URL Filtering** and select a filtering rule based on the actual situation.

➢ **URL Filtering Rule**

Object: Select the range in which the URL Filtering takes effect:

- Group: URL Filtering will take effect to all the users in group.
- ANY: URL Filtering will take effect to all the users.

Mode: Select the mode for URL Filtering. "Keywords" indicates that all the URL addresses including the specified keywords will be filtered. "URL Path" indicates that the URL address will be filtered only when it exactly matches the specified URL.

Effective Time: Specify the time for the entry to take effect.

Description: Give a description for the entry.

➢ **List of Rules**

You can view the information of the entries and edit them by the Action buttons.

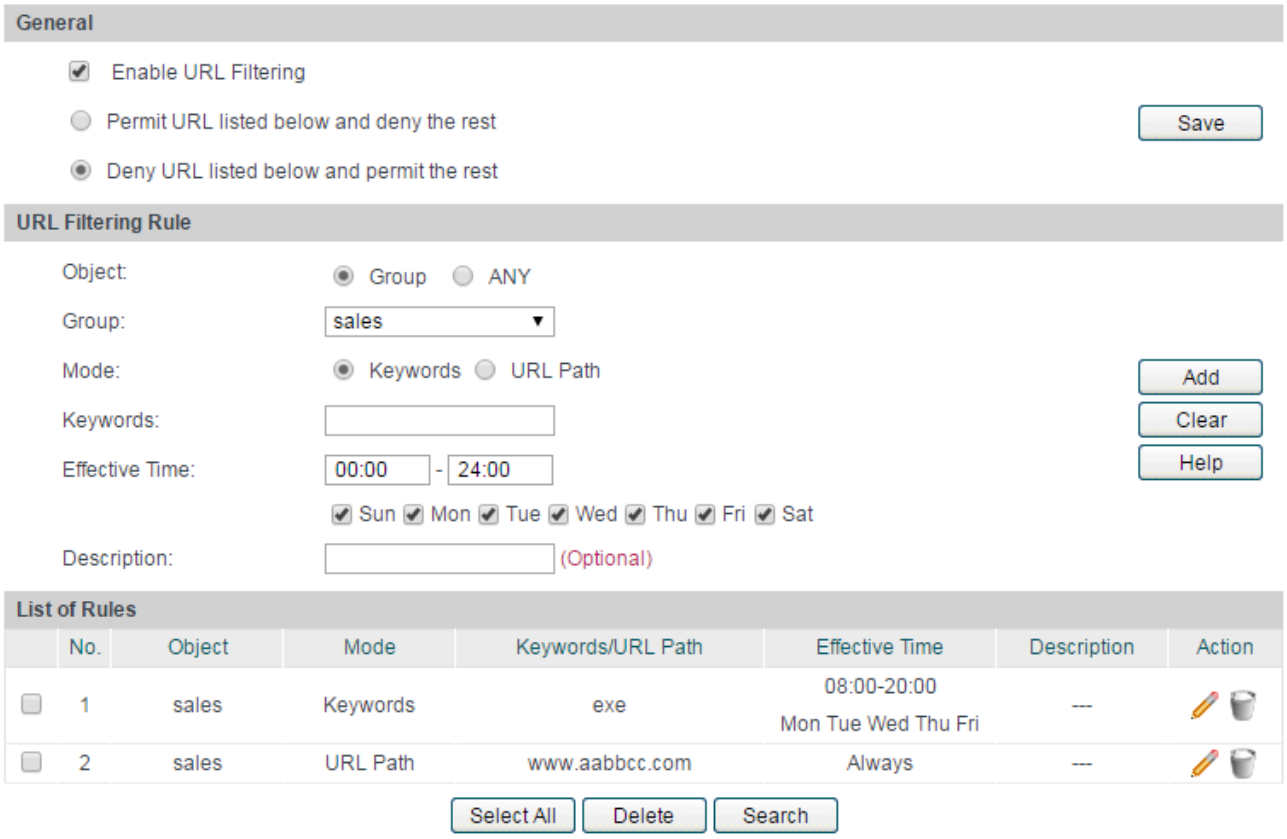
Application Example

➢ **Network Requirements**

Prevent the local hosts from accessing Internet website www.aabbcc.com anytime and downloading the files with suffix of "exe" at 8:00-20:00 from Monday to Friday.

➢ **Configuration Procedure**

Select Keywords mode and type in "exe" in the field, select URL mode and type in "www.aabbcc.com" as the following figure shows, then specify the effective time and click the <Add> button to make the setting take effect.



4.6.4.2 Web Filtering

On this page, you can filter the desired web components.

Choose the menu **Firewall→Access Control→Web Filtering** to load the following page.

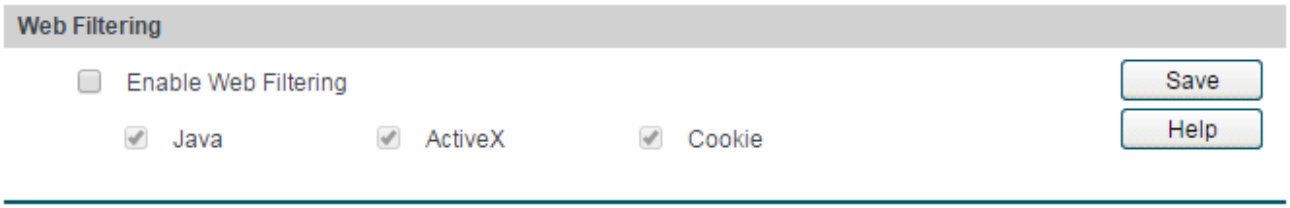


Figure 4-45 Web Filtering

Check the box before **Enable Web Filtering** and select the web components to be filtered.

4.6.4.3 Access Rules

Choose the menu **Firewall→Access Control→Access Rules** to load the following page.

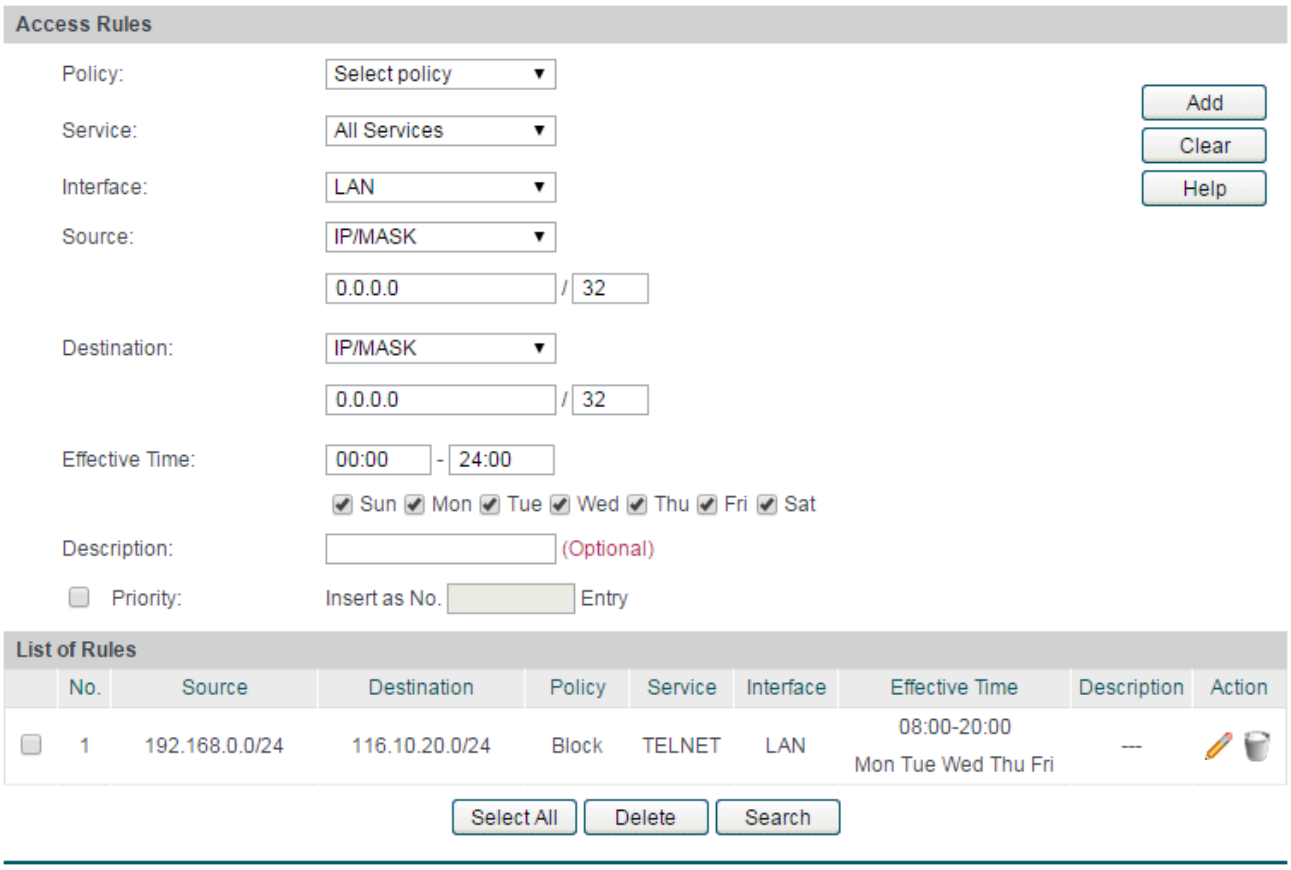


Figure 4-46 Access Rule

The following items are displayed on this screen:

➢ **Access Rules**

Policy: Select a policy for the entry:

- Block: When this option is selected, the packets obeyed the rule will not be allowed to pass through the router.
- Allow: When this option is selected, the packets obeyed the rule will be allowed to pass through the router.

Service: Select the service for the entry. Only the service belonging to the specified service type is limited by the entry. For example, if you select "Block" for Policy and only FTP for Service, the packets of other service types can still pass through the router. You can add new service types on **4.6.4.4 Service**.

Interface: Select interface for the entry. The entry will take effect when the interface to which the data is flowing is selected. WAN or LAN refers to all the WAN or LAN interfaces.

Source: Select the Source IP Range for the entries, including the following three ways:

- IP/MASK: Enter an IP address or subnet mask. ("0.0.0.0/32" means any IP).
- Group: Select a predefined group of users. You can set the group on4.4.1 Group.
- ANY: Means for any users.

Destination: Select the Destination IP Range for the entries, including the following two ways:

- IP/MASK: Enter an IP address or subnet mask. ("0.0.0.0/32" means any IP is acceptable).
- ANY: Means for any users.

Effective Time: Specify the time for the entry to take effect.

Description: Give a description for the entry.

Priority: Select this option to specify the priority for the added entries. The latest enabled entry will be displayed at the end of the list by default.

➢ **List of Rules**

You can view the information of the entries and edit them by the Action buttons. The smaller the value is, the higher the priority is.

The first entry in Figure 4-46 indicates: The TELNET packets transmitted from the hosts within the network of 192.168.0.0/24 will be not allowed to pass through the router at 8:00-20:00 from Tuesday to Saturday.

Note:

- For the users in the private network and not being set access rule, the default Policy is Allow.
- To specify all IP addresses, type in "0.0.0.0 / 32" in the Policy field.
- For detailed setting of subnet mask, please refer to **Appendix B FAQ**.

4.6.4.4 Service

The Service function allows you to specify the protocol and port number to be filtered for Firewall function conveniently. Protocol name and port range constitute a service type. The router predefines three commonly used services such as HTTP, FTP and TELNET and you can also add customized services if needed.

Choose the menu **Firewall→Access Control→Service** to load the following page.

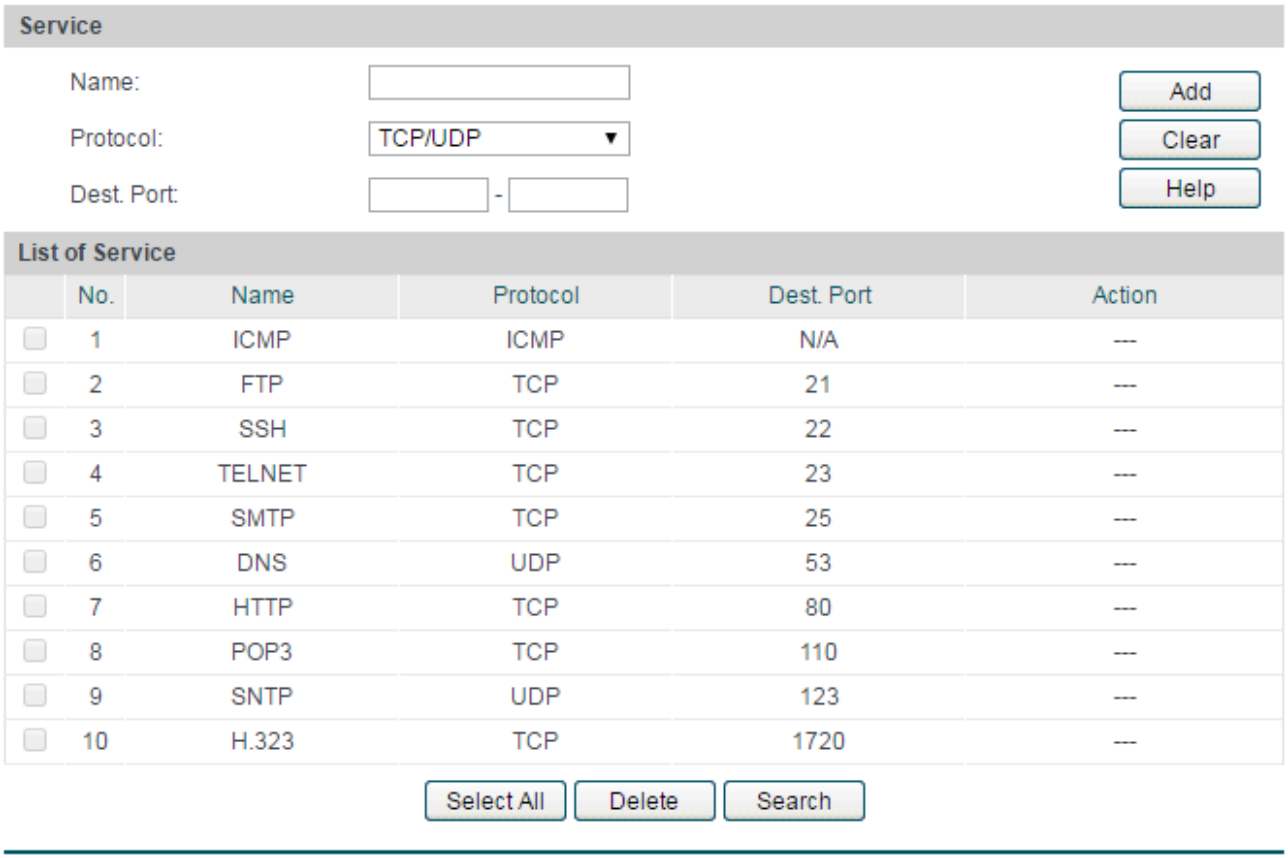


Figure 4-47 Service

The following items are displayed on this screen:

➢ **Service**

Name: Enter a name for the service. The name should not be more than 28 characters. The name will display in the drop-down list of Protocol

on Access Rule page.

Protocol: Select the protocol for the service. The system predefined protocols include TCP, UDP and TCP/UDP.

Dest. Port: Enter the start and end ports to make a destination port range for the service. The start port number cannot be greater than the end port number.

➢ **List of Service**

You can view the information of the entries and edit them by the Action buttons.

Note:

The service types predefined by the system cannot be modified.

4.6.5 App Control

4.6.5.1 Control Rules

On this page, you can enable the Application Rules function.

Choose the menu **Firewall→App Control→Control Rules** to load the following page.

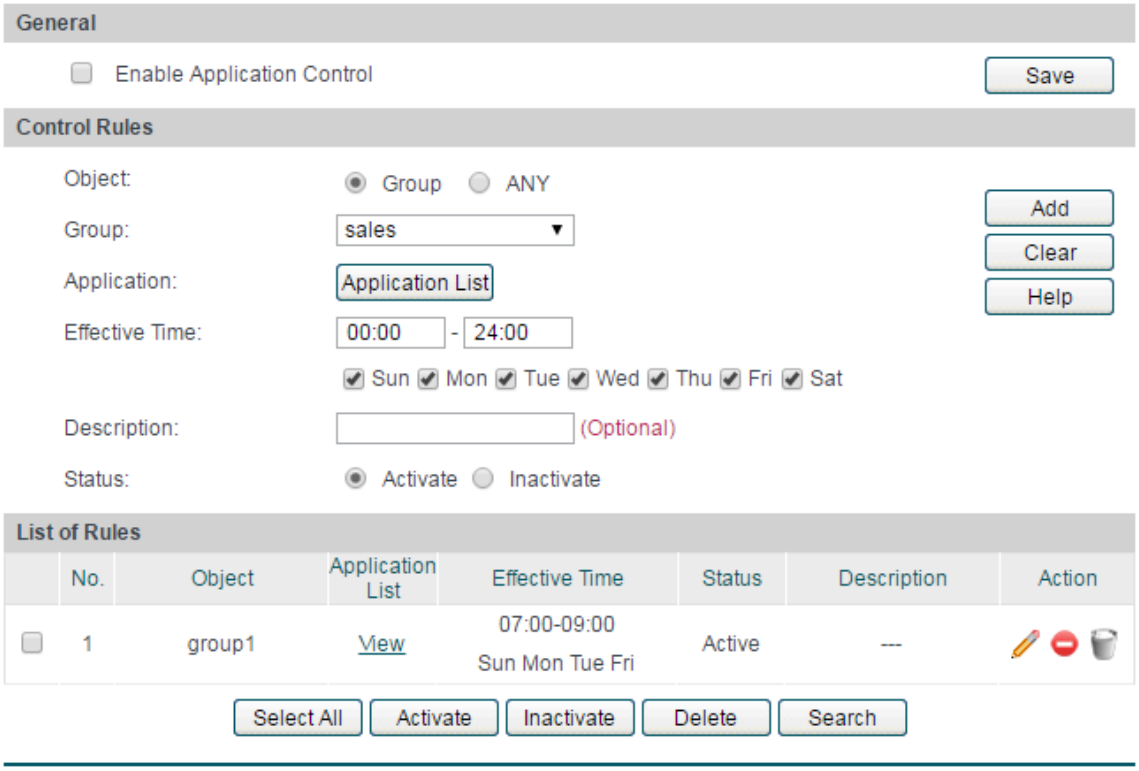


Figure 4-48 Application Rules

The following items are displayed on this screen:

- **General**

  Check the box before **Enable Application Control** to make the Application Control function take effect. The specified application used by the specified local users will be not allowed to access the Internet if the Application Control entry is enabled.

- **Control Rules**

  Object: Specify the object for the entry. You can select "Group" to limit the predefined group, or select "ANY" to limit all the users.

  Group: If select "Group" as object, you can select the group in the drop-down list. To establish new group, please refer to **4.4.1 Group**.

  Application: Click the <Application List> button to select applications from the popup checkbox. The applications include IM, Web IM, SNS, P2P, Media, Basic and Proxy. The default setting is to limit all the applications in the application list except for Basic and Proxy.

  Effective Time: Specify the time for the entry to take effect.

  Description: Give a description for the entry.

  Status: Activate or inactivate the entry.

- **List of Rules**

  You can view the information of the entries and edit them by the Action buttons.

  The first entry in Figure 4-48 indicates: The group1 is applied with Application Rules. You can click <View> to view the limited applications in the popup checkbox. The effective time of this entry is 7:00-9:00 on Monday, Tuesday, Friday, Saturday and Sunday. This entry is enabled.

Note:

To set the group and group members, please refer to **4.4.1 Group**.

4.6.5.2 Database

On this page, you can upgrade the application database.

Choose the menu **Firewall→App Control→Database** to load the following page.

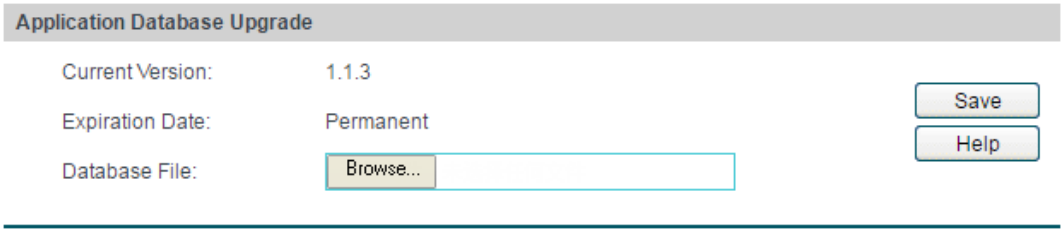


Figure 4-49 Database

The database refers to all the applications in the application list on the Application Rules page. You can download the latest database from http://www.tp-link.com. Click the <Browse> button and select the file, and then click the <Upgrade> button to upgrade the database.

4.7 Services

4.7.1 PPPoE Server

The router can be configured as a PPPoE server to specify account and IP address to users in LAN and thus you can control the dial-up of users for a high efficiency in network management.

The PPPoE configuration can be implemented on **General**, **IP Address Pool**, **Account**, **Exceptional IP** and **List of Account** pages.

4.7.1.1 General

On this page, you can configure PPPoE function globally.

Choose the menu **Services→PPPoE Server→General** to load the following page.

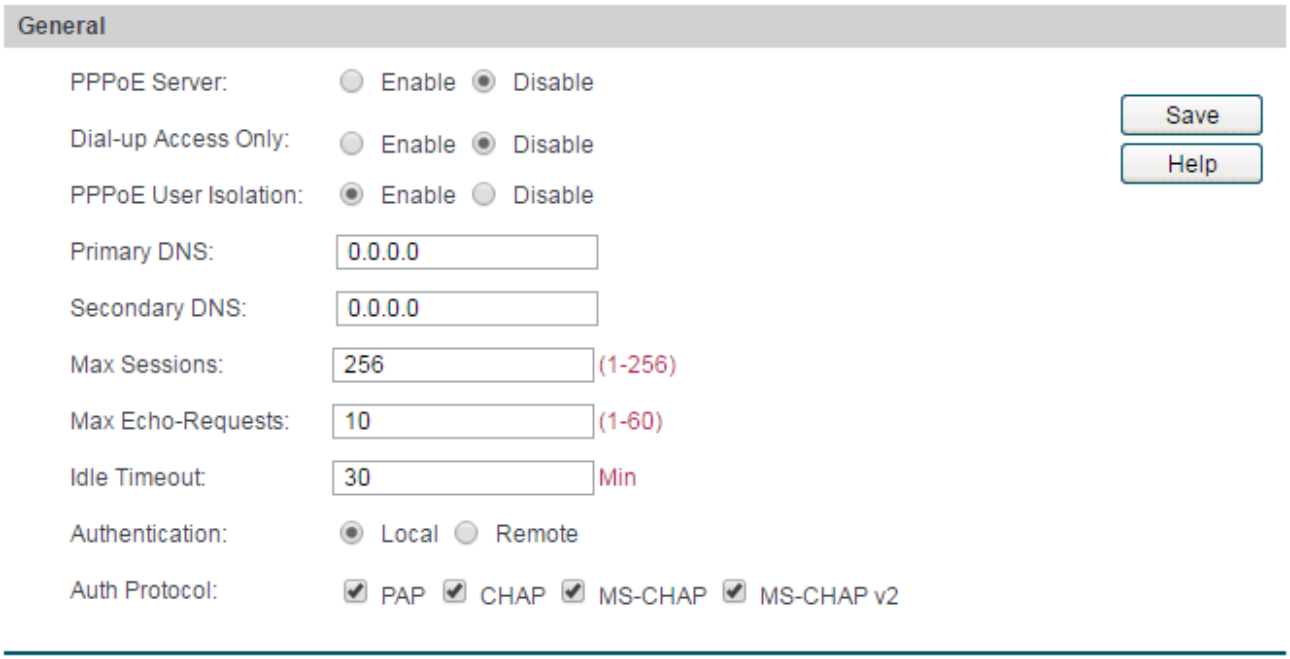


Figure 4-50 General

The following items are displayed on this screen:

- **General**

PPPoE Server: Specify whether to enable the PPPoE Server function.

Dial-up Access Only: Specify whether to enable the Dial-up Access Only function. If enabled, only the Dial-in Users and the user with Exceptional IP can access the Internet.

PPPoE User Isolation: Specify whether to allow the Dial-in Users to communicate with one another.

Primary/Secondary DNS: Enter the Primary/Secondary DNS server address. The default is 0.0.0.0.

Max Sessions: Specify the maximum number of the sessions for PPPoE server. The default is 256.

Max Echo-Requests: Specify the maximum number of Echo-Requests sent by the server to wait for response. The default is 10. The link will be dropped when the number of the unacknowledged LCP echo requests reaches your specified Max Echo-Requests.

Idle Timeout: Enter the maximum idle time. The session will be terminated after it has been inactive for this specified period. It can be 0-10080 minutes. If you want your Internet connection to remain on at all times, enter 0 in the Idle Timeout field. The default value is 30.

Authentication: Select the Authentication type. It can be Local authentication and Remote authentication. Select Local authentication for authentication in PPPoE server and select Remote authentication for authentication in the remote server.

Auth Protocol: Select at least one authentication protocol for Local Authentication.

- PAP, transferring username and password in plain text in the network, is used in a less secured network.
- CHAP is more secured for it adopts three handshakes and does not transfer password in plain text.
- MS-CHAP, put forward by Microsoft, adopts a different encryption algorithm of CHAP.
- MS-CHAP v2 with a higher security is an improved version of MS-CHAP.

Radius Server: It is available when Remote Authentication is selected. RADIUS (Remote Authentication Dial In User Service) provides an authentication for dial-up users. Enter the Radius Server address for Remote authentication.

Shared Key: Enter the Shared Key for Remote authentication. It should be the same to the shared key of the Radius Server.

4.7.1.2 IP Address Pool

On this page, you can define or edit the IP Address Pool.

Choose the menu **Services→PPPoE Server→IP Address Pool** to load the following page.

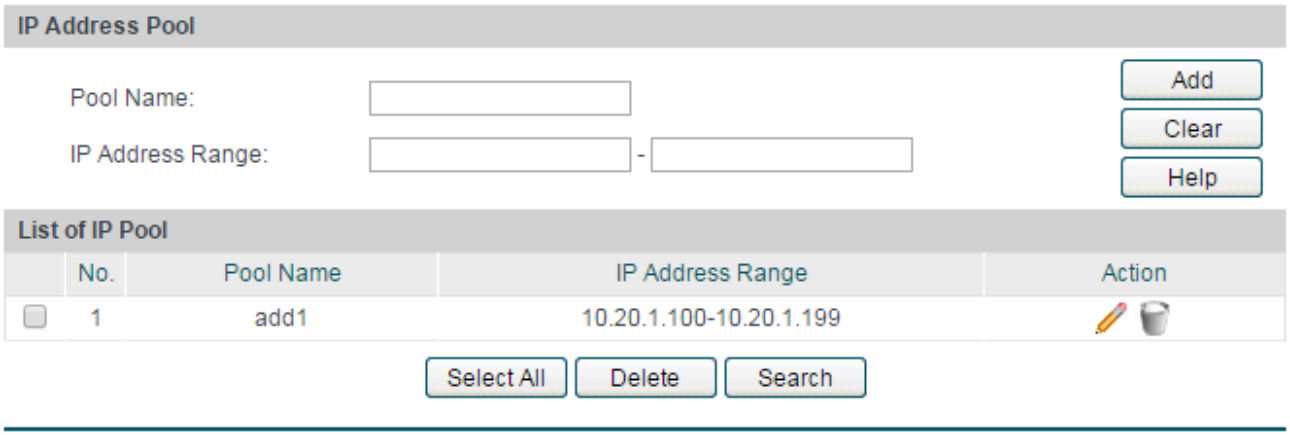


Figure 4-51 IP Address Pool

The following items are displayed on this screen:

➢ **IP Address Pool**

Pool Name: Specify a unique name to the IP Address Pool for identification and management purposes.

IP Address Range: Specify the start and the end IP address for IP Pool. The start IP address should not exceed the end address and the IP address ranges must not overlap.

➢ **List of IP Pool**

In this table, you can view the information of IP Address Pools and edit them by the Action buttons.

4.7.1.3 Account

On this page, you can configure the PPPoE account.

Choose the menu **Services→PPPoE Server→Account** to load the following page.

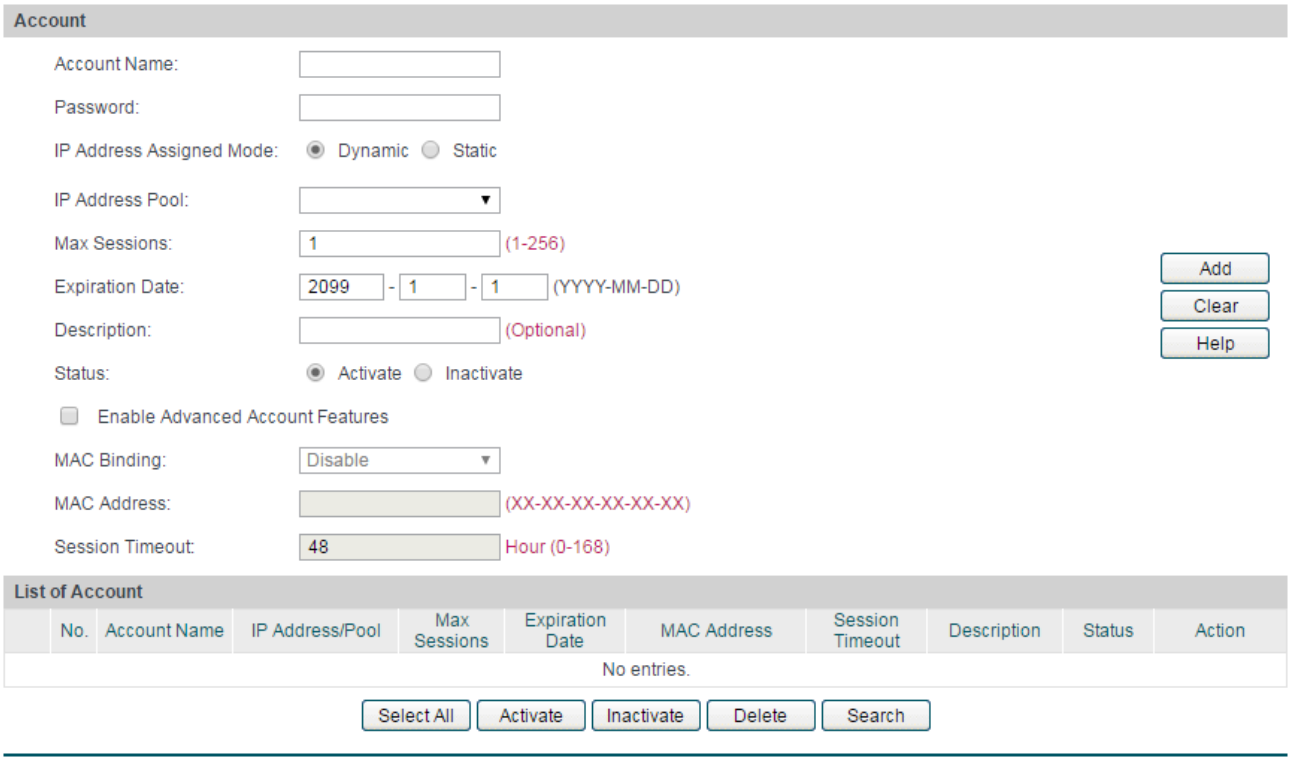


Figure 4-52 Account

The following items are displayed on this screen:

➢ **Account**

Account Name: Enter the account name. This name should not be the same with the one in L2TP/PPTP connection settings.

Password: Enter the password.

IP Address Assigned Mode: Select the IP Address Assigned Mode for IP assignment.

- Static: Select this option to assign a static IP address to the client.
- Dynamic: Select this option to assign available IP addresses to the client automatically.

Static IP Address: It is available on Static mode. Enter a static IP address for the client.

IP Address Pool: It is available on Dynamic mode. Select an IP Address Pool to make a range to assign dynamic IPs.

Max Sessions: Specify the maximum number of sessions for the client. The default value is 1.

Expiration Date: Specify the Expiration Date of the account. The default is 2099-1-1.

Description: Enter the description for management and search purposes. Up to 28 characters can be entered.

Status: Activate or inactivate the entry.

MAC Binding: Select a MAC Binding type from the pull-down list. Options include:

- Disable: Select this option to disable the MAC Binding function.
- Manual: Select this option to bind the account to a MAC address manually. Only from the Host with this MAC address can the account log on to the server.
- Automatical: Select this option to bind the account to the MAC address of its first login automatically. Only from the Host with this MAC address can the account log on to the server.

MAC Address: It is available when Manually is selected. Enter the MAC address of the Host to bind with the account.

Session Timeout: Enter a time after which the connection will be dropped. To keep the connection always on, enter 0 in the Session Timeout field. The default is 48. If **Enable Advanced Account Features** is not selected, the Session Timeout value is 0 by default.

➢ **List of Account**

In this table, you can view the information of accounts and edit them by the Action buttons.

4.7.1.4 Exceptional IP

When the Dial-up Access Only function is enabled, only the Dial-in Users and the user with Exceptional IP can access the Internet. On this page, you can specify the Exceptional IP.

Choose the menu **Services→PPPoE Server→Exceptional IP** to load the following page.

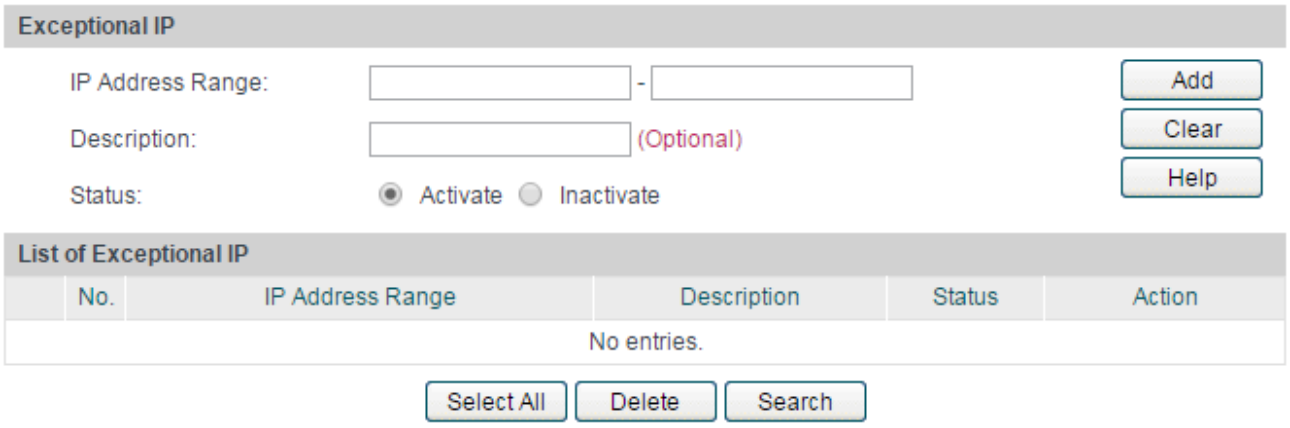


Figure 4-53 Exceptional IP

The following items are displayed on this screen:

➢ **Exceptional IP**

IP Address Range: Specify the start and the end IP address to make an exceptional IP address range. This range should be in the same IP range with LAN port of the router. The start IP address should not exceed the end address and the IP address ranges must not overlap.

Description: Give a description to the exceptional IP address range for identification.

Status: Activate or inactivate the entry.

➢ **List of Exceptional IP**

In this table, you can view the information of Exceptional IPs and edit them by the Action buttons.

4.7.1.5 List of Account

On this page, you can view the detailed information of all accounts you have established.

Choose the menu **Services→PPPoE Server→List of Account** to load the following page.

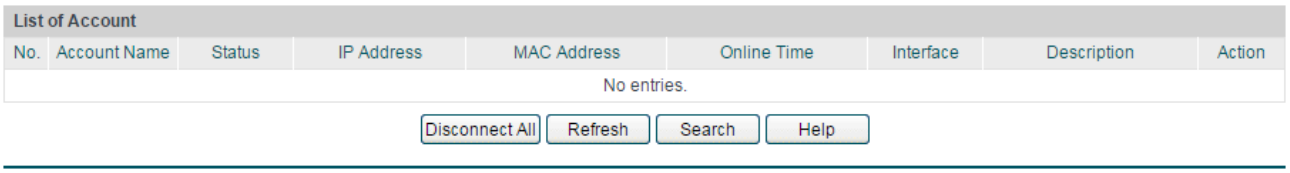


Figure 4-54 List of Account

Figure 4-54 displays the connection information of PPPoE users. Click ⛔ to disconnect the account. Click the <Disconnect All> button to disconnect all accounts.

4.7.2 E-Bulletin

With E-Bulletin function, bulletin information can be released to the specified users. On this page you can edit the bulletin content and specify the receiving user group.

Choose the menu **Services→E-Bulletin** to load the following page.

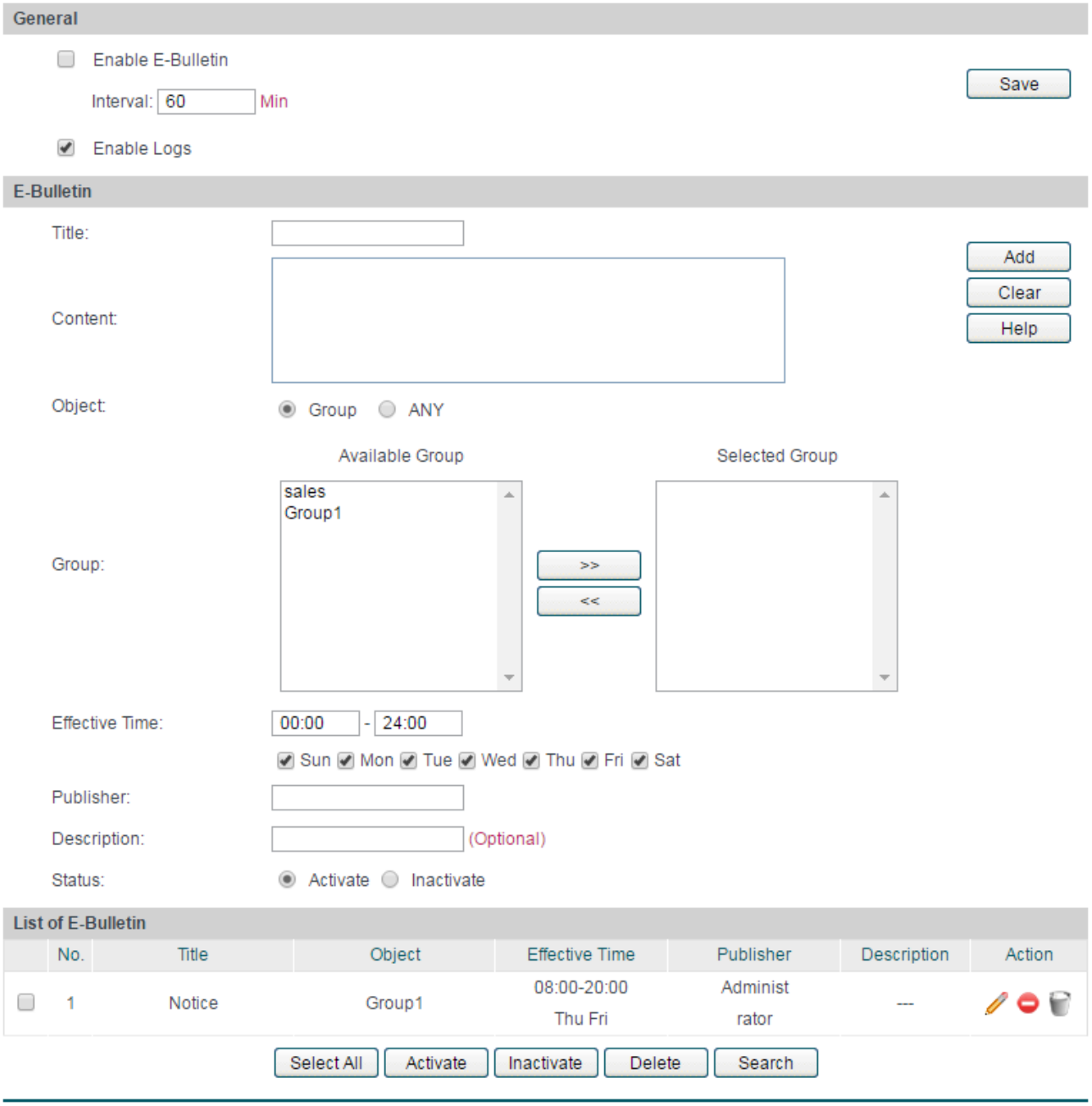


Figure 4-55 E-Bulletin

The following items are displayed on this screen:

➢ **General**

Enable E-Bulletin: Specify whether to enable electronic bulletin function.

Interval: Specify the interval to release the bulletin.

Enable Logs: Specify whether to log the E-Bulletin.

➢ **E-Bulletin**

Title: Enter a title for the bulletin.

Content: Enter the content of the bulletin.

Object: Select the object of this bulletin. Options include:

- ANY: The bulletin will be released to all the users and the PCs on the LAN.
- Group: The bulletin will be released to the users in the selected group. You can click <>> button to add a group to the selected group and click <<< to remove a group from the selected group. Group is created on **User Group→Group** page.

Effective Time: Specify the effective time for the bulletin. Only one bulletin can be set for the object at the same time.

Publisher: Enter the name of the bulletin's publisher.

Description: Enter the description for the bulletin.

Status: Activate or inactivate the entry.

➢ **List of E-Bulletin**

In this table, you can view the existing bulletins and edit them by the Action button.

The No.1 entry in Figure 4-55 indicates: This bulletin is released by the administrator, and it is released to the Group1 from 8am to 20pm on Thursday and Friday every a bulletin interval. (the interval in the figure is 30 min). This entry is enabled.

Tips:

For the configuration for groups and users, please refer to the **User Group** section.

4.7.3 Dynamic DNS

DDNS (Dynamic DNS) service allows you to assign a fixed domain name to a dynamic WAN IP address, which enables the Internet hosts to access the router or the hosts in LAN using the domain names.

As many ISPs use DHCP to assign public IP addresses in WAN, the public IP address assigned to the client is unfixed. In this way, it is very difficult for other clients to get the latest IP address of this client for access.

DDNS (Dynamic DNS) server provides a fixed domain name for DDNS client and maps its latest IP address to this domain name. When DDNS server works, DDNS client informs the DDNS server of the latest IP address, the server will update the mappings between the domain name and IP address in DNS database. Therefore, the users can use the same domain name to access the DDNS client even if the IP address of the DDNS client has changed. DDNS is usually used for the Internet users to access the private website and FTP server, both of which are established based on Web server.

The router, as a DDNS client, cannot provide DDNS service. Prior to using this function, be sure you have registered on the official websites of DDNS service providers for username, password and domain name. TL-R480T+ router offers PeanutHull DDNS client, Dyndns DDNS client, NO-IP DDNS client and Comexe DDNS client.

The **Dynamic DNS** can be implemented on **DynDNS DDNS**, **No-IP DDNS**, **Peanuthull DDNS** and **Comexe DDNS** pages.

4.7.3.1 DynDNS

On this page, you can configure DynDNS client.

Choose the menu **Services→Dynamic DNS→DynDNS** to load the following page.

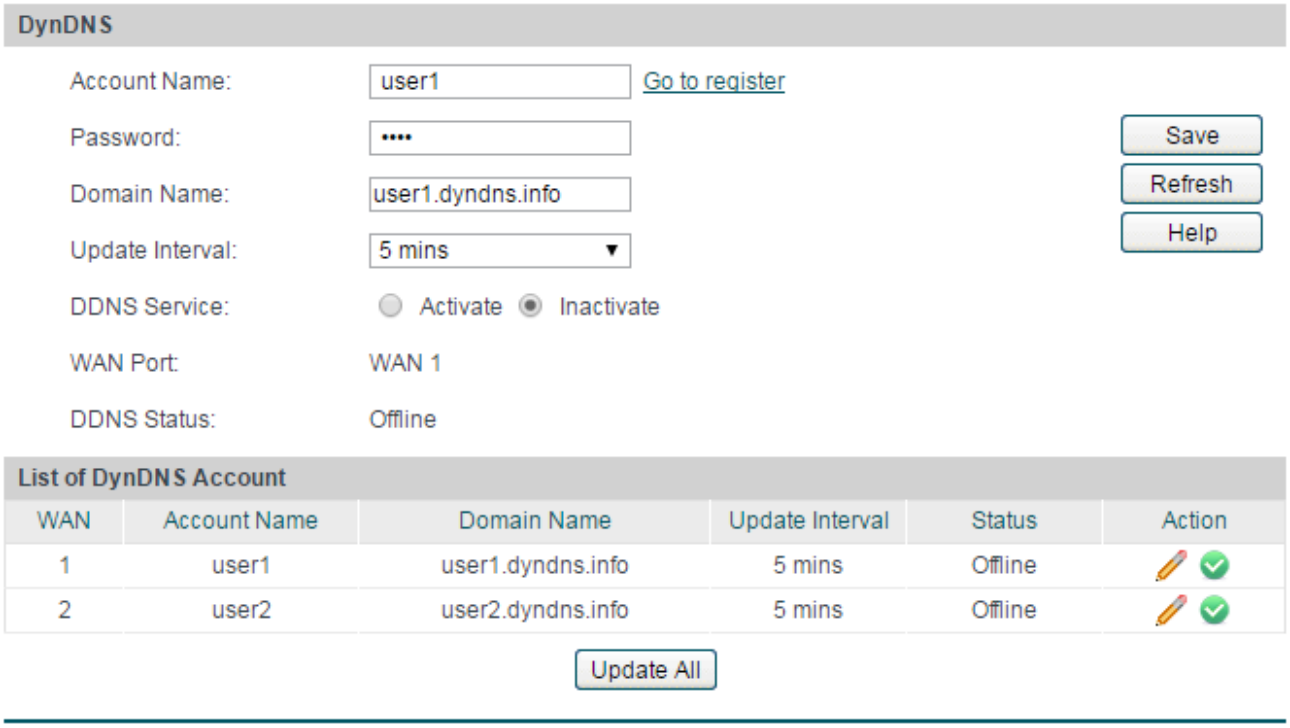


Figure 4-56 DynDNS DDNS

The following items are displayed on this screen:

➢ **Dyndns DDNS**

Account Name: Enter the Account Name of your DDNS account. If you have not registered, click <Go to register> to go to the website of Dyndns for register.

Password: Enter the password of your DDNS account.

Domain Name: Enter the Domain Name that you registered with your DDNS service provider.

Update Interval: Select the interval to update DDNS service.

DDNS Service: Activate or inactivate DDNS service here.

WAN Port: Displays the WAN port for which Dyndns DDNS is selected.

DDNS Status: Displays the current status of DDNS service.

- Offline: DDNS service is disabled.
- Connecting: Client is connecting to the server.
- Online: DDNS works normally.
- Authorization fails: The Account Name or Password is incorrect. Please check and enter it again.
- Block: This account is blocked.

➢ **List of DynDNS Account**

In this table, you can view the existing DDNS entries or edit them by the Action button.

Click the <Update All> button to update the DDNS service manually.

4.7.3.2 No-IP

On this page you can configure NO-IP DDNS client.

Choose the menu **Services→Dynamic DNS→No-IP** to load the following page.

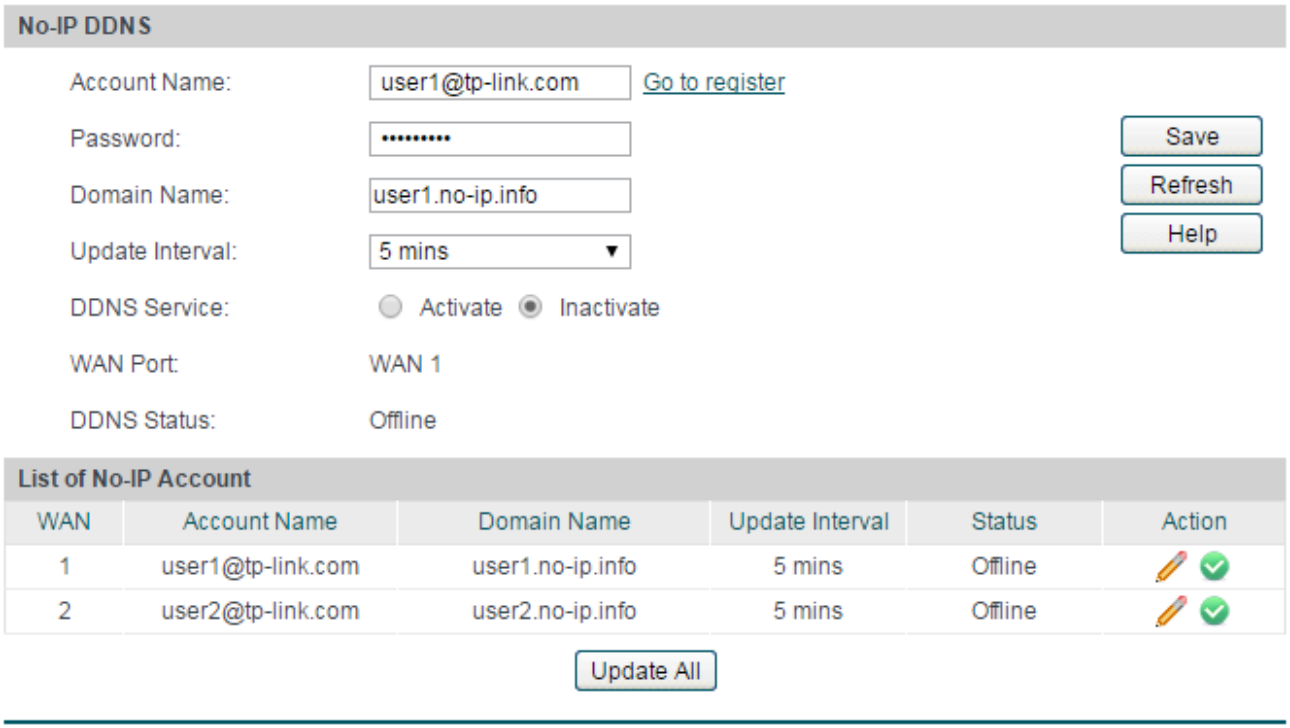


Figure 4-57 NO-IP DDNS

The following items are displayed on this screen:

➢ **No-IP DDNS**

Account Name: Enter the Account Name of your DDNS account. If you have not registered, click <Go to register> to go to the website of No-IP for register.

Password: Enter the password of your DDNS account.

Domain Name: Enter the Domain Name that you registered with your DDNS service provider.

Update Interval: Select the interval to update DDNS service.

DDNS Service: Activate or inactivate DDNS service here.

WAN Port: Displays the WAN port for which No-IP DDNS is selected.

DDNS Status: Displays the current status of DDNS service.

- Offline: DDNS service is disabled.
- Connecting: Client is connecting to the server.
- Online: DDNS works normally.
- Authorization fails: The Account Name or Password is incorrect. Please check and enter it again.
- Invalid Domain name: The Domain Name is incorrect or unregistered. Please check and enter it again.

➢ **List of No-IP Account**

In this table, you can view the existing DDNS entries or edit them by the Action button.

Click the <Update All> button to update the DDNS service manually.

4.7.3.3 PeanutHull

On this page you can configure PeanutHull DDNS client.

Choose the menu **Services→Dynamic DNS→PeanutHull** to load the following page.

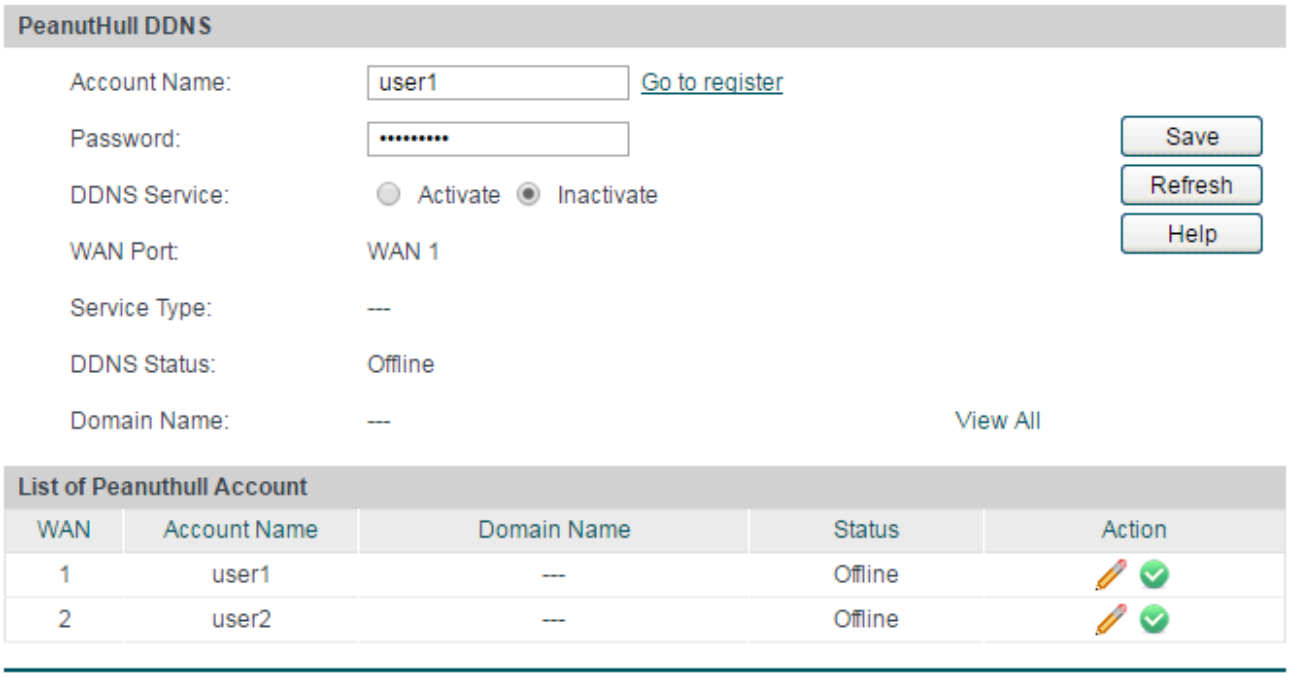


Figure 4-58 PeanutHull DDNS

The following items are displayed on this screen:

➢ **PeanutHull DDNS**

Account Name: Enter the Account Name of your DDNS account. If you have not registered, click <Go to register> to go to the website of PeanutHull for register.

Password: Enter the password of your DDNS account.

DDNS Service: Activate or inactivate DDNS service here.

WAN Port: Displays the WAN port for which PeanutHull DDNS is selected.

Service Type: Displays the DDNS service type, including Professional service and Standard service.

DDNS Status: Displays the current status of DDNS service.

- Offline: DDNS service is disabled.
- Connecting: Client is connecting to the server.
- Online: DDNS works normally.
- Authorization fails: The Account Name or Password is incorrect. Please check and enter it again.

Domain Name: Displays the domain names obtained from the DDNS server. Up to 16 domain names can be displayed here.

➢ **List of PeanutHull Account**

In this table, you can view the existing DDNS entries or edit them by the Action button.

4.7.3.4 Comexe

On this page you can configure Comexe DDNS client.

Choose the menu **Services→Dynamic DNS→Comexe** to load the following page.

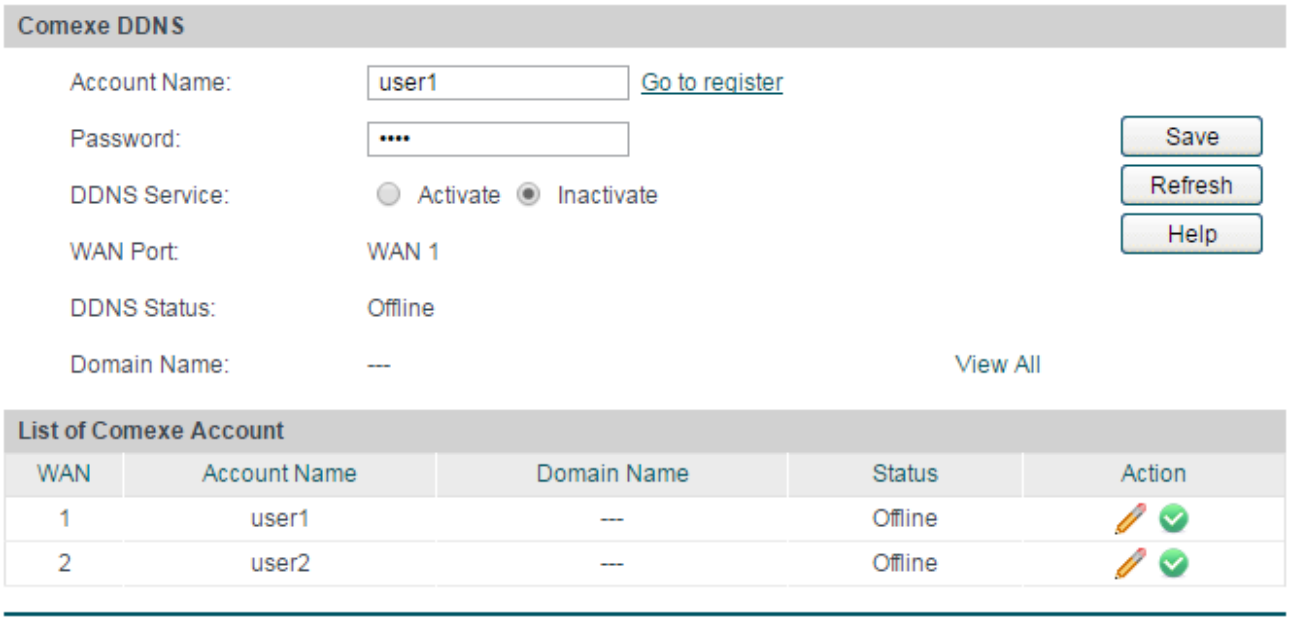


Figure 4-59 Comexe DDNS

The following items are displayed on this screen:

➢ **Comexe DDNS**

Account Name: Enter the Account Name of your DDNS account. If you have not registered, click <Go to register> to go to the website of Comexe for register.

Password: Enter the password of your DDNS account.

DDNS Service: Activate or inactivate DDNS service here.

WAN Port: Displays the WAN port for which Comexe DDNS is selected.

DDNS Status: Displays the current status of DDNS service.

- Offline: DDNS service is disabled.
- Connecting: Client is connecting to the server.
- Online: DDNS works normally.
- Authorization fails: The Account Name or Password is incorrect. Please check and enter it again.

Domain Name: Displays the domain names obtained from the DDNS server. Up to 5 domain names can be displayed here.

➢ **List of Comexe Account**

In this table, you can view the existing DDNS entries or edit them by the Action button.

4.7.4 UPnP

Devices based on UPnP (Universal Plug and Play) protocol from different manufacturer can automatically discover and communicate with one another.

If UPnP groupware are installed in the host in LAN and UPnP function is enabled for the router, the host in LAN can automatically open the corresponding port to allow the UPnP application in WAN to access the resource of the host in LAN via this port, so that the functions limited to NAT can work normally. For example, MSN Messenger installed in Windows XP and Windows ME system is using UPnP protocol when audio and video communications are processing.

On this page you can configure UPnP service.

Choose the menu **Services→UPnP** to load the following page.

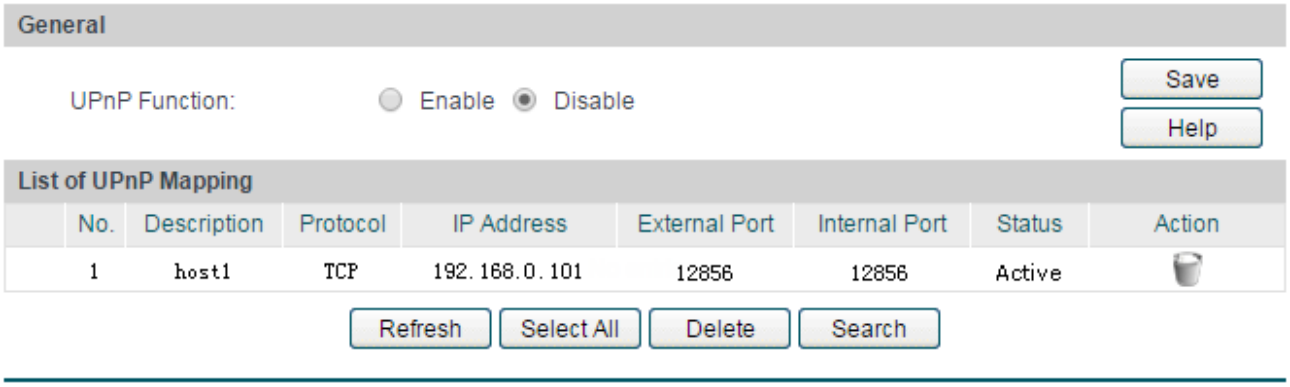


Figure 4-60 UPnP

The following items are displayed on this screen:

➢ **General**

UPnP Function: Enable or disable the UPnP function globally.

➢ **List of UPnP Mapping**

After UPnP is enabled, all UPnP connection rules will be displayed in the list of UPnP Mapping.

The NO.1 entry in Figure 4-60 indicates: TCP data received on port 12856 of the WAN port in the router will be forwarded to port 12856 in 192.168.0.101 server in LAN.

Note:

- When using UPnP function, make sure the UPnP is enabled for the router, and the operating system and applications in the host support UPnP service.
- As some Trojan and viruses can open the specific port using UPnP service resulting in hacker attack on the host, be careful of using UPnP service.

4.8 Maintenance

4.8.1 Admin Setup

4.8.1.1 Administrator

On this page, you can modify the factory default user name and password of the router.

Choose the menu **Maintenance→Admin Setup→Administrator** to load the following page.

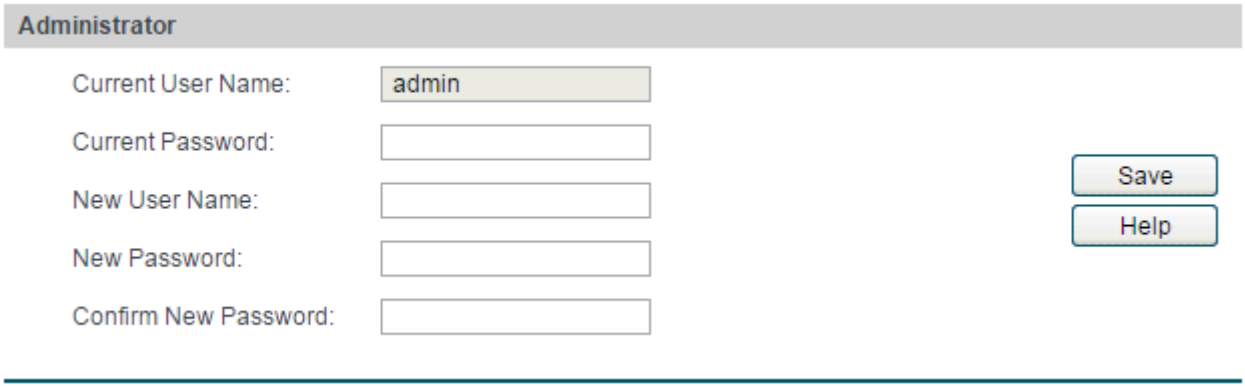


Figure 4-61 Administrator

The following items are displayed on this screen:

➢ **Administrator**

Current User Name: Enter the current user name of the router.

Current Password: Enter the current password of the router.

New User Name: Enter a new user name for the router.

New Password: Enter a new password for the router.

Confirm New Password: Re-enter the new password for confirmation.

Note:

- The factory default password and user name are both admin.
- You should enter the new user name and password when next login if the current username and password has been changed.
- The new user name and password must not exceed 31 characters in length and must consist of numbers or letters. All the fields are case-sensitive.

4.8.1.2 Login Parameter

On this page, you can configure and modify the Web and Telnet port.

Choose the menu **Maintenance→Admin Setup→Login Parameter** to load the following page.

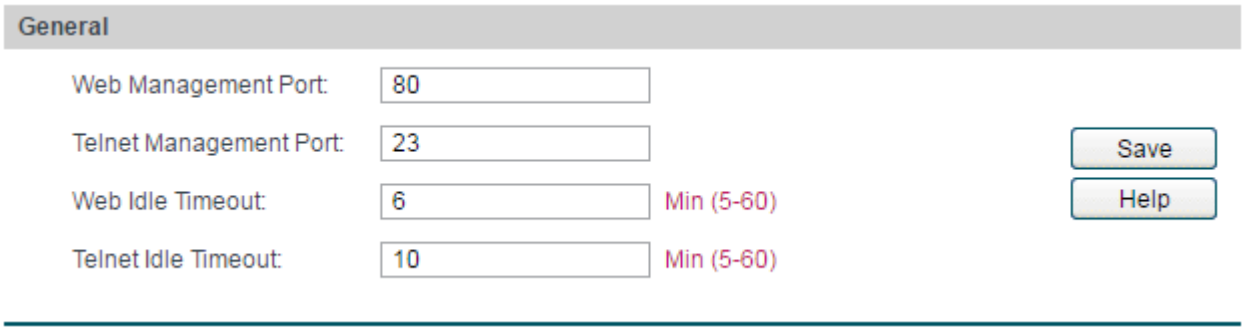


Figure 4-62 Login Parameter

The following items are displayed on this screen:

➢ **General**

Web Management Port: Enter the Web Management Port for the router.

Telnet Management Port: Enter the Telnet Management Port for the router.

Web Idle Timeout: Enter a timeout period that the router will log you out of the Web-based Utility after a specified period (Web Idle Timeout) of inactivity.

Telnet Idle Timeout: Enter a timeout period that the router will log the remote PCs out of the Web-based Utility after a specified period (Telnet Idle Timeout) of inactivity.

Note:

- The default Web Management Port is 80. If the port is changed, you should type in "http://IP address: port" to login the router. For example, if the Web Management Port is changed to 88, type in http://192.168.0.1:88 in the address filed to login the router.
- The new timeout period will take effect when next login.

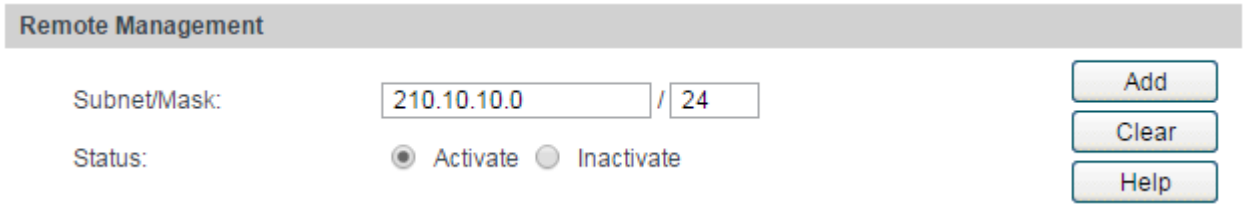
Application Example

➢ **Network Requirements**

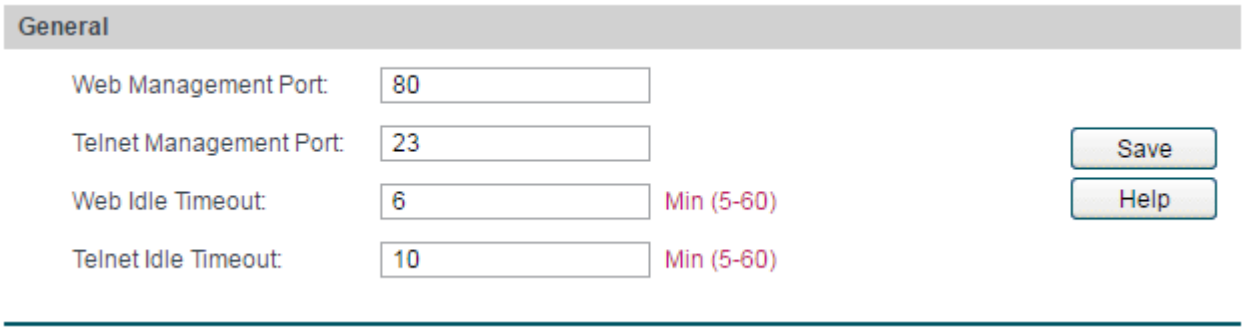
Allow the IP address within 210.10.10.0/24 segment to manage the router with IP address of 210.10.10.50 remotely.

➢ **Configuration Procedure**

Type in 210.10.10.0/24 in the Subnet/Mask field on Remote Management page and enable the entry as the following figure shows.



Then type in the corresponding port number in Web Management Port and Telnet Management Port fields as the following figure shows.



Finally, start the web browser and type in 210.10.10.50 in the URL field to log in the Web management page of the router.

4.8.1.3 Remote Management

On this page you can configure the Remote Management function. This feature allows managing your router from a remote location via the Internet.

Choose the menu **Maintenance→Setup→Remote Management** to load the following page.

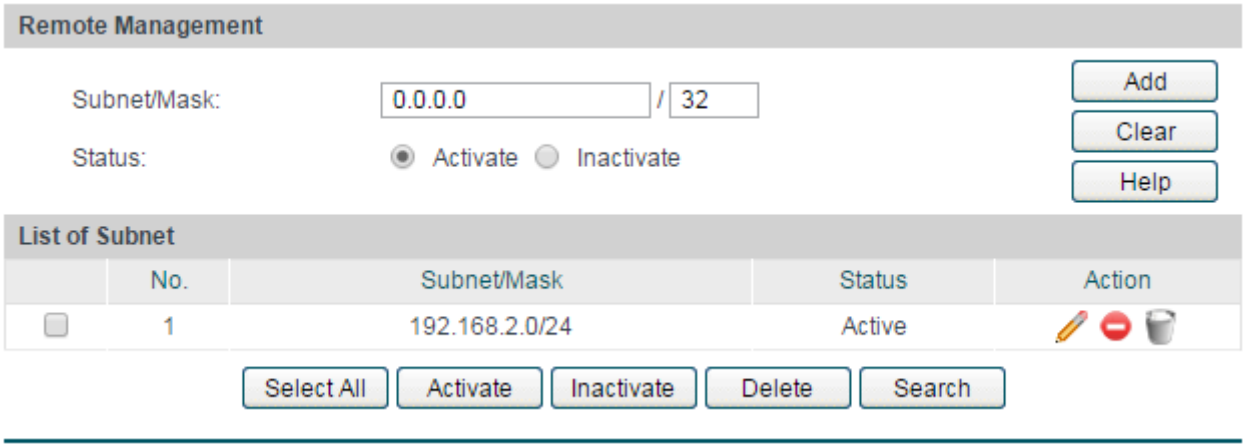


Figure 4-63 Remote Management

The following items are displayed on this screen:

- **Remote Management**

  Subnet/Mask: Specify a single IP address or network address for the hosts desired to access the router from external network.

  Status: Activate or inactivate the entry.

- **List of Subnet**

  In this list, you can view the Remote Management entries and edit them by the Action buttons.

  The first entry in Figure 4-63 indicates that: The hosts with IP address in subnet of 192.168.2.0/24 are allowed to access the router and this entry is activated.

4.8.2 Management

4.8.2.1 Factory Defaults

Choose the menu **Maintenance→Management→Factory Defaults** to load the following page.

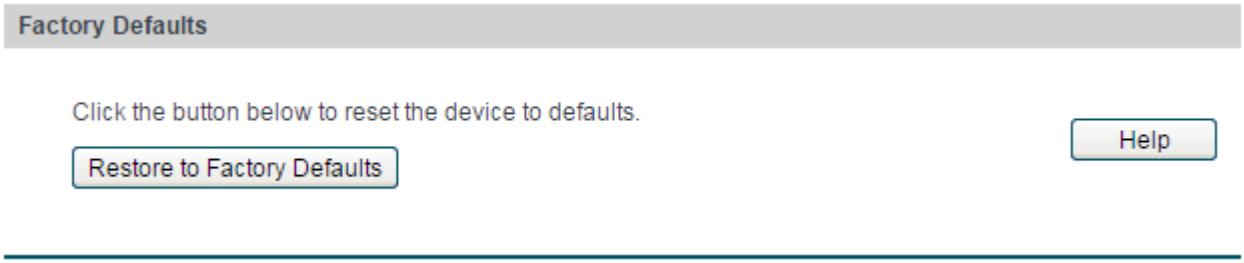


Figure 4-64 Factory Defaults

Click the <Restore to Factory Defaults> button to Reset all configuration settings to their default values.

The default IP address is 192.168.0.1; the default login user name and password are both admin.

4.8.2.2 Export and Import

Choose the menu **Maintenance→Management→Export and Import** to load the following page.

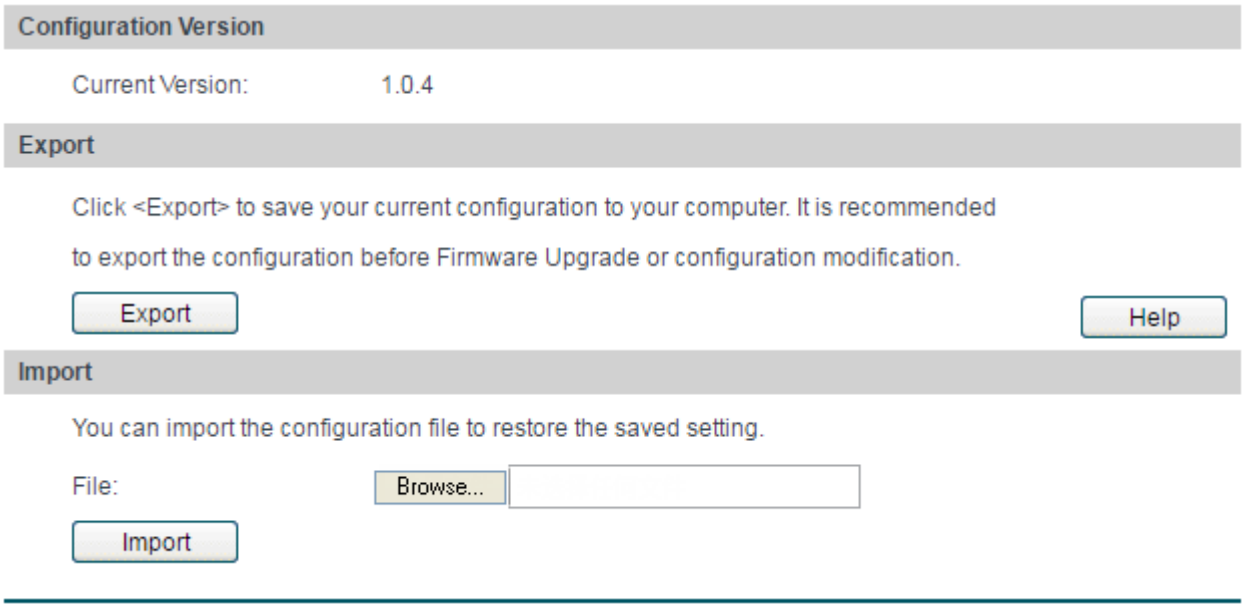


Figure 4-65 Export and Import

The following items are displayed on this screen:

- **Configuration Version**

  Displays the current configuration version of the router.

- **Export**

  Click the <Export> button to save the current configuration as a file to your computer. You are suggested to take this measure before upgrading or modifying the configuration.

- **Import**

  Click the <Browse> button to locate the update file for the device, or enter the exact path to the saved file in the text box. Then click the <Import> button to restore the saved setting.

Note:

- To avoid any damage, please do not power down the router while being restored.
- Configurations may be lost if the configuration file you imported varies greatly from current configurations.

4.8.2.3 Reboot

Choose the menu **Maintenance→Management→Reboot** to load the following page.

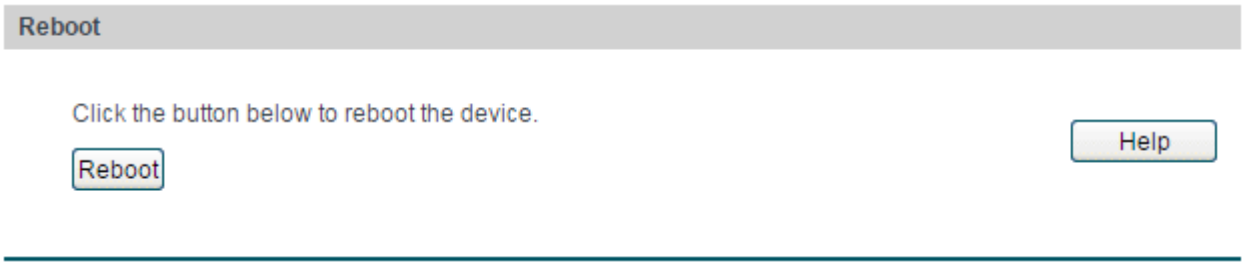


Figure 4-66 Reboot

Click the <Reboot> button to reboot the router.

The configuration will not be lost after rebooting. The Internet connection will be temporarily interrupted while rebooting.

Note:

To avoid damage, please do not turn off the device while rebooting.

4.8.2.4 Firmware Upgrade

Choose the menu **Maintenance→Management →Firmware Upgrade** to load the following page.

Figure 4-67 Firmware Upgrade

Upgrade the router to get more functions and better performance. Go to http://www.tp-link.com to download the updated firmware.

Type in the path and file name of the update file into the "File" field. Or click the <Browse> button to locate the update file. Then click the <Upgrade> button to complete.

Note:

- After upgrading, the device will reboot automatically.
- To avoid damage, please do not turn off the device while upgrading.
- You are suggested to backup the configuration before upgrading.

4.8.3 SNMP

SNMP (Simple Network Management Protocol) provides a management frame to monitor and maintain the network devices. It is used for automatically managing various network devices regardless of their physical differences. Currently, the most network management systems are based on SNMP.

Choose the menu **Maintenance→SNMP→SNMP** to load the following page.

Figure 4-68 SNMP

The following items are displayed on this screen:

➢ **General**

SNMP: Enable or disable the SNMP function.

Device Name: Enter the name of the router.

Location: Enter the location of the router.

Contact: Enter the name of the network administrator for the router, as well as a contact number or an e-mail address.

Get Community: Enter the password that allows read-only access to the router's SNMP information. The default password is public.

Set Community: Enter the password that allows read/write access to the router's SNMP information. The default password is private.

SNMP Trusted Host: You can restrict access to the router's SNMP information by IP address. Enter the IP address of the SNMP Trusted Host, which is

allowed to access the router's SNMP information. If this field is left blank, then access from any IP address is permitted.

4.8.4 Statistics

4.8.4.1 Interface Traffic Statistics

Interface Traffic Statistics screen displays the detailed traffic information of each port and extra information of WAN ports.

Choose the menu **Maintenance→Statistics→Interface Traffic Statistics** to load the following page.

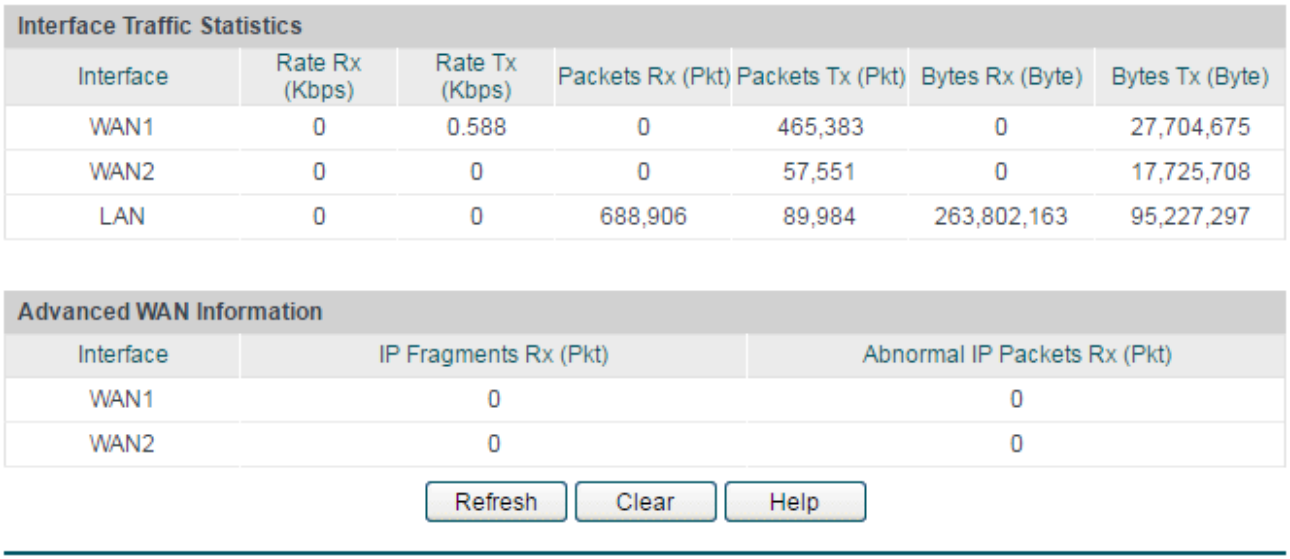


Figure 4-69 Interface Traffic Statistics

The following items are displayed on this screen:

- **Interface Traffic Statistics**

  Interface: Displays the interface.

  Rate Rx: Displays the rate for receiving data frames.

  Rate Tx: Displays the rate for transmitting data frames.

  Packets Rx: Displays the number of packets received on the interface.

  Packets Tx: Displays the number of packets transmitted on the interface.

  Bytes Rx: Displays the bytes of packets received on the interface.

  Bytes Tx: Displays the bytes of packets transmitted on the interface.

- **Advanced WAN Information**

  Interface: Displays the interface.

IP Fragment Rx: Displays the amount of IP Fragments received by WAN port.

Abnormal IP Packets Rx: Displays the rate for transmitting data frames.

4.8.4.2 IP Traffic Statistics

IP Traffic Statistics screen displays the detailed traffic information of each PC on LAN.

Choose the menu **Maintenance→Statistics→IP Traffic Statistics** to load the following page.

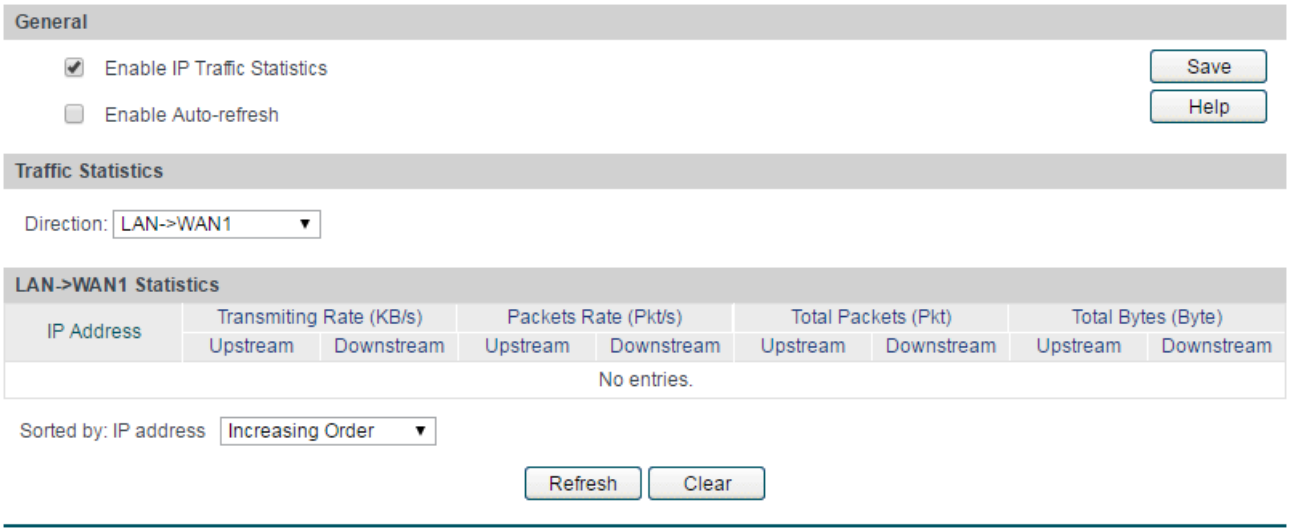


Figure 4-70 IP Traffic Statistics

The following items are displayed on this screen:

➢ **General**

Enable IP Traffic Statistics: Allows you to enable or disable IP Traffic Statistics.

Enable Auto-refresh: Allows you to enable/disable refreshing the IP Traffic Statistics automatically. The default refresh interval is 5 seconds.

➢ **Traffic Statistics**

Direction: Select the direction in the drop-down list to get the Flow Statistics of the specified direction.

➢ **IP Traffic Statistics**

This table displays the detailed traffic information of corresponding PCs.

Sorted by: Select the rule for displaying the traffic information.

4.8.5 Diagnostics

4.8.5.1 Diagnostics

This router provides Ping test and Tracert test functions for network diagnose.

Choose the menu **Maintenance→Diagnostics→Diagnostics** to load the following page.

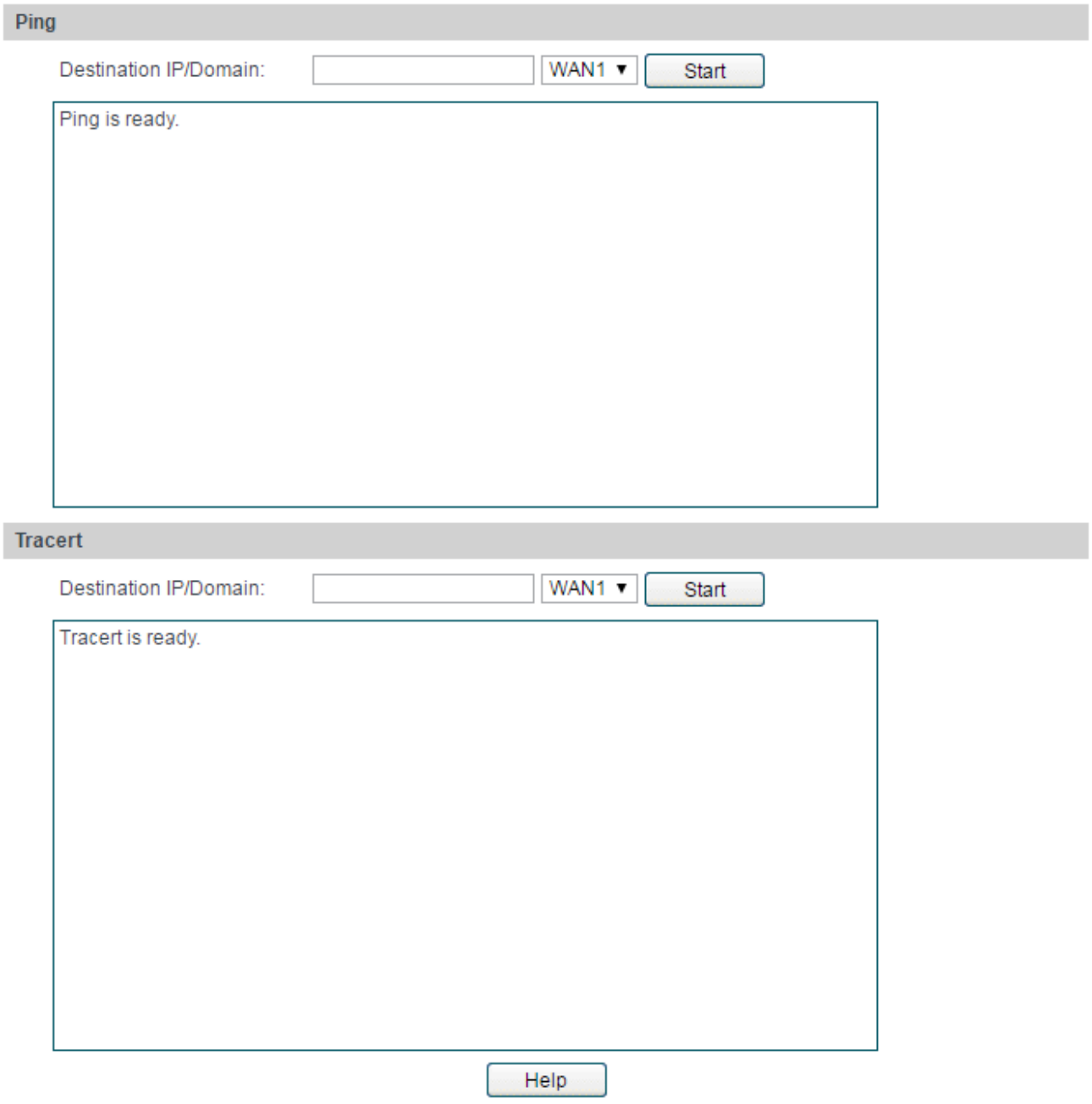


Figure 4-71 Diagnostics

The following items are displayed on this screen:

➢ **Ping**

Destination IP/Domain: Enter destination IP address or Domain name here. Then select a port for testing, if you select "Auto", the router will select the interface of destination automatically. After clicking <Start> button, the router will send Ping packets to test the network connectivity and reachability of the host and the results will be displayed in the box below.

➢ **Tracert**

Destination IP/Domain: Enter destination IP address or Domain name here. Then select a port for testing, if Auto is selected, the router will select the interface of destination automatically. After clicking the <Start> button, the router will send Tracert packets to test the connectivity of the gateways during the journey from the source to destination of the test data and the results will be displayed in the box below.

4.8.5.2 Online Detection

On this page, you can detect the WAN port is online or not.

Choose the menu **Maintenance→Diagnostics→Online Detection** to load the following page.

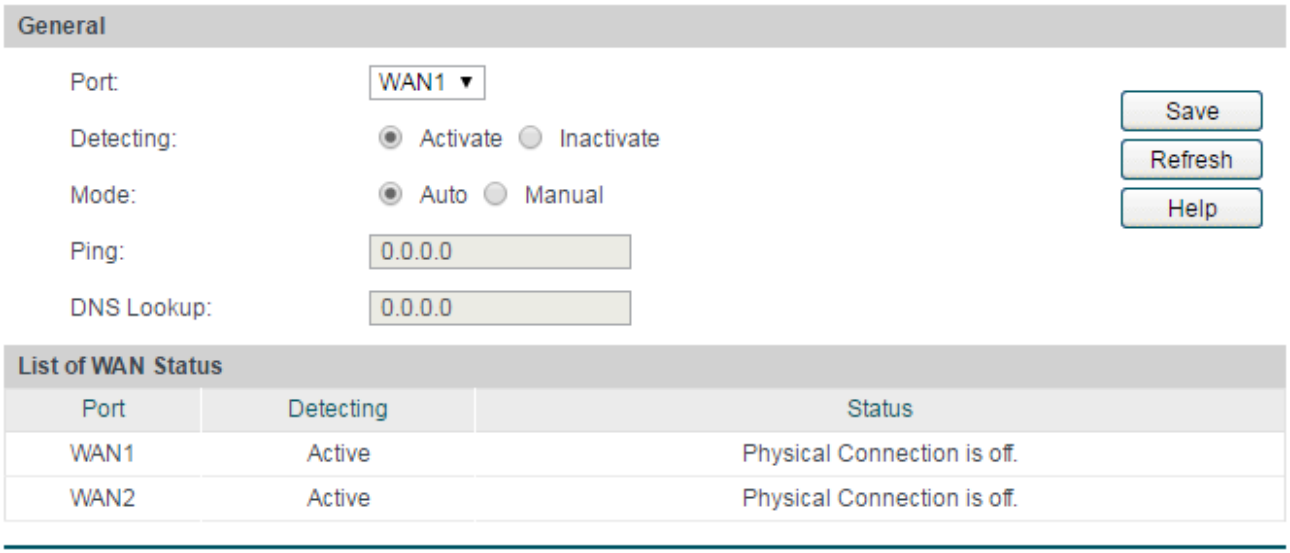


Figure 4-72 Online Detection

The following items are displayed on this screen:

➢ **General**

Port: Select the port to be detected.

Detecting: Activate or inactivate Online Detection function. When Online Detection is active, WAN status will depend on the result of both PING and DNS Lookup. When Online Detection is inactive, WAN status will be detected according to physical connection status and dial-up status.

Mode: Detect automatically or Manually. In Auto mode, gateway will be selected as destination for PING detection, DNS server of WAN port will be selected as destination for DNS Lookup. In Manual Mode, you can configure the destination for PING and DNS Lookup manually.

Ping: Enter the destination IP for Ping in Manual mode. 0.0.0.0 means PING detection is disabled.

DNS Lookup: Enter the IP address of DNS server in Manual mode. 0.0.0.0 means DNS Lookup is disabled.

➢ **List of WAN status**

Port: Displays the detected WAN port.

Detection: Displays whether the Online Detection is enabled.

WAN Status: Display the detecting results.

4.8.6 Time

4.8.6.1 Time

System Time is the time displayed while the router is running. On this page you can configure the system time and the settings here will be used for other time-based functions like Access Rule, PPPoE and Logs.

Choose the menu **Maintenance→Time→Time** to load the following page.

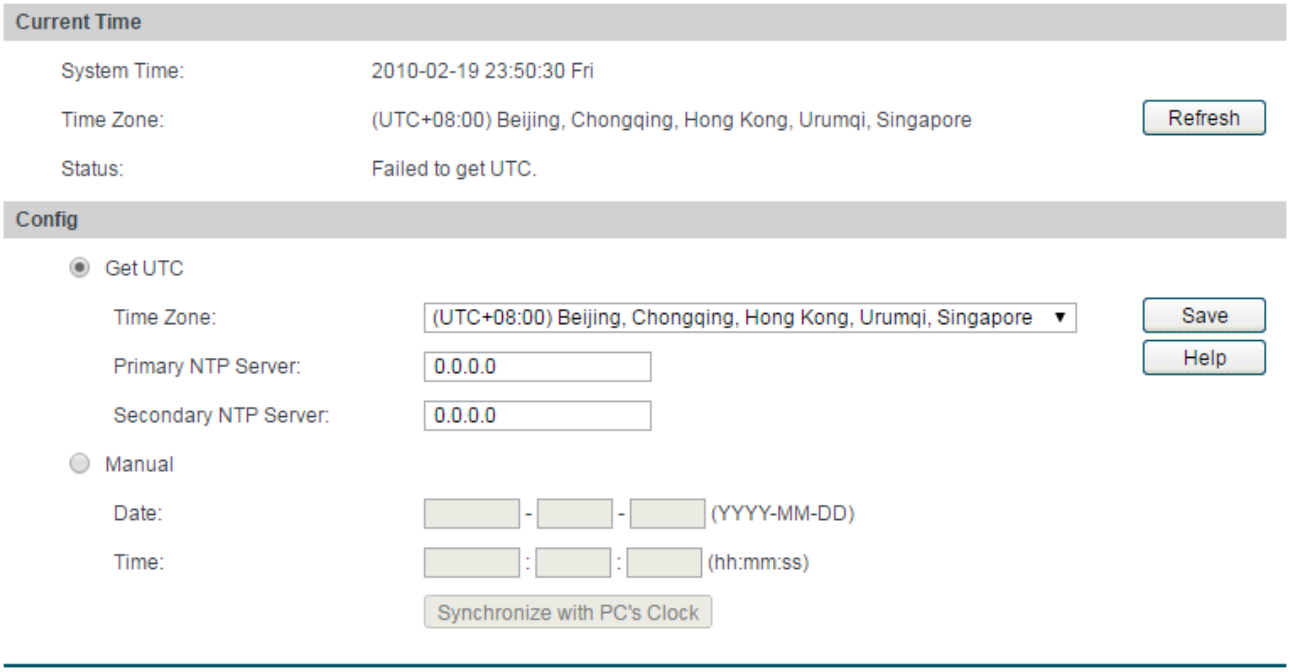


Figure 4-73 Time

The following items are displayed on this screen:

➢ **Current Time**

System Time: Displays the current date and time of the router.

Time Zone: Displays the current time zone of the router.

Status: Displays the status of time capturing.

➢ **Config**

Get UTC: When this option is selected, you can configure the time zone and the IP address for the NTP server. The router will get UTC automatically if it has connected to an NTP server.

- Time Zone: Select the time zone for the router.
- Primary/Secondary NTP Server: Enter the IP address or domain name of the NTP server.

Manual: With this option selected, you can set the date and time manually.

Synchronize with PC'S Clock: With this option selected, the administrator PC's clock is utilized.

Note:

- If Get UTC function cannot be used properly, please add an entry with UDP port of 123 to the firewall software of the PC.
- The time will be lost when the router is restarted. The router will obtain UTC time automatically from Internet.

4.8.6.2 Daylight Saving Time

On this page you can configure the Daylight Saving Time of the router.

Choose the menu **Maintenance→Time→Daylight Saving Time** to load the following page.

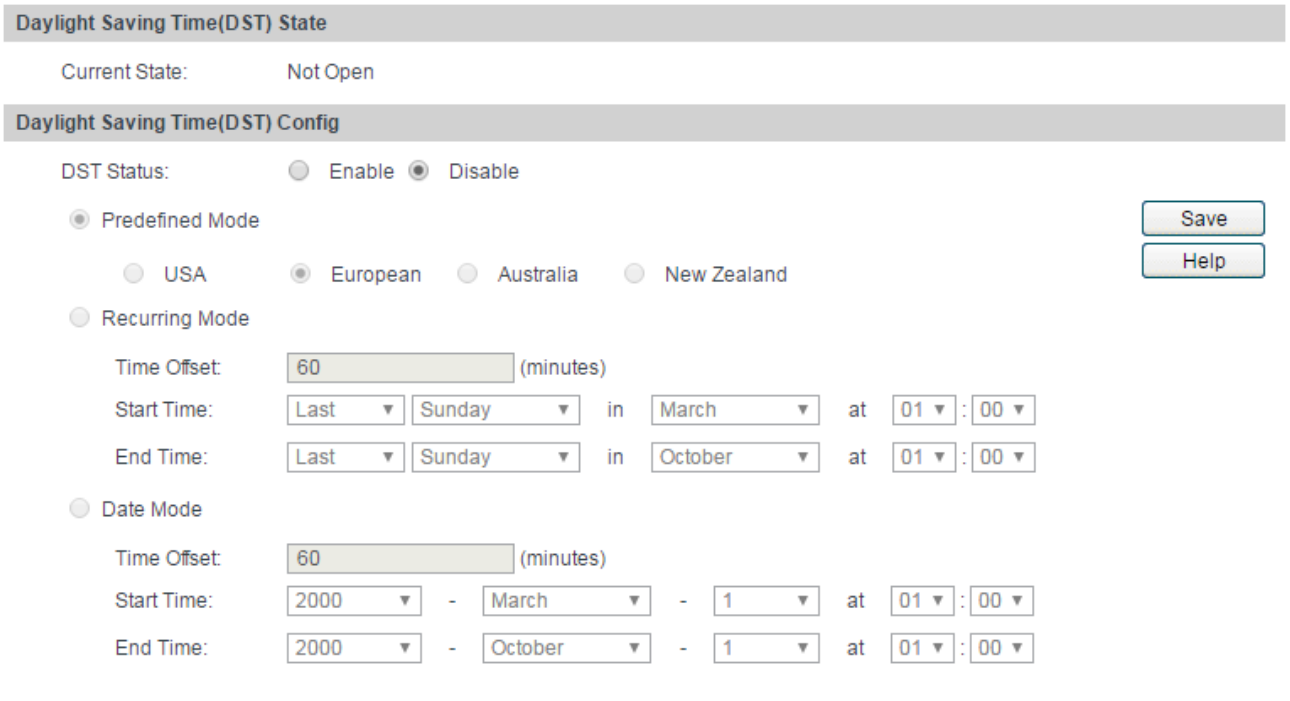


Figure 4-74 Daylight Saving Time

The following items are displayed on this screen:

- **Daylight Saving Time(DST) State**

  Show the work state of DST.

- **Daylight Saving Time(DST) Config**

  DST Status: Enable or disable the DST.

  Predefined Mode: Select a predefined DST configuration.

  - USA: Second Sunday in March, 02:00 – First Sunday in November, 02:00.
  - European: Last Sunday in March, 01:00 – Last Sunday in October, 01:00.
  - Australia: First Sunday in October, 02:00 – First Sunday in April, 03:00.
  - New Zealand: Last Sunday in September, 02:00 – First Sunday in April, 03:00.

  Recurring Mode: Specify the DST configuration in recurring mode. This configuration is recurring in use.

  - Time Offset: Specify the time adding in minutes when Daylight Saving Time comes.
  - Start/End Time: Select the start time and end time of Daylight Saving Time. The start time is standard time, and the end time is Daylight Saving Time.

  Date Mode: Specify the DST configuration in Date mode. This configuration is one-off in use.

  - Time Offset: Specify the time adding in minutes when Daylight Saving Time comes.
  - Start/End Time: Select the start time and end time of Daylight Saving Time. The start time is standard time, and the end time is Daylight Saving Time.

Note:

- When the DST is disabled, the predefined mode, recurring mode and date mode cannot be configured.
- When the DST is enabled, the default daylight saving time is of European in predefined mode.

4.8.7 Logs

The Log system of router can record, classify and manage the system information effectively.

Choose the menu **Maintenance→Logs→Logs** to load the following page.

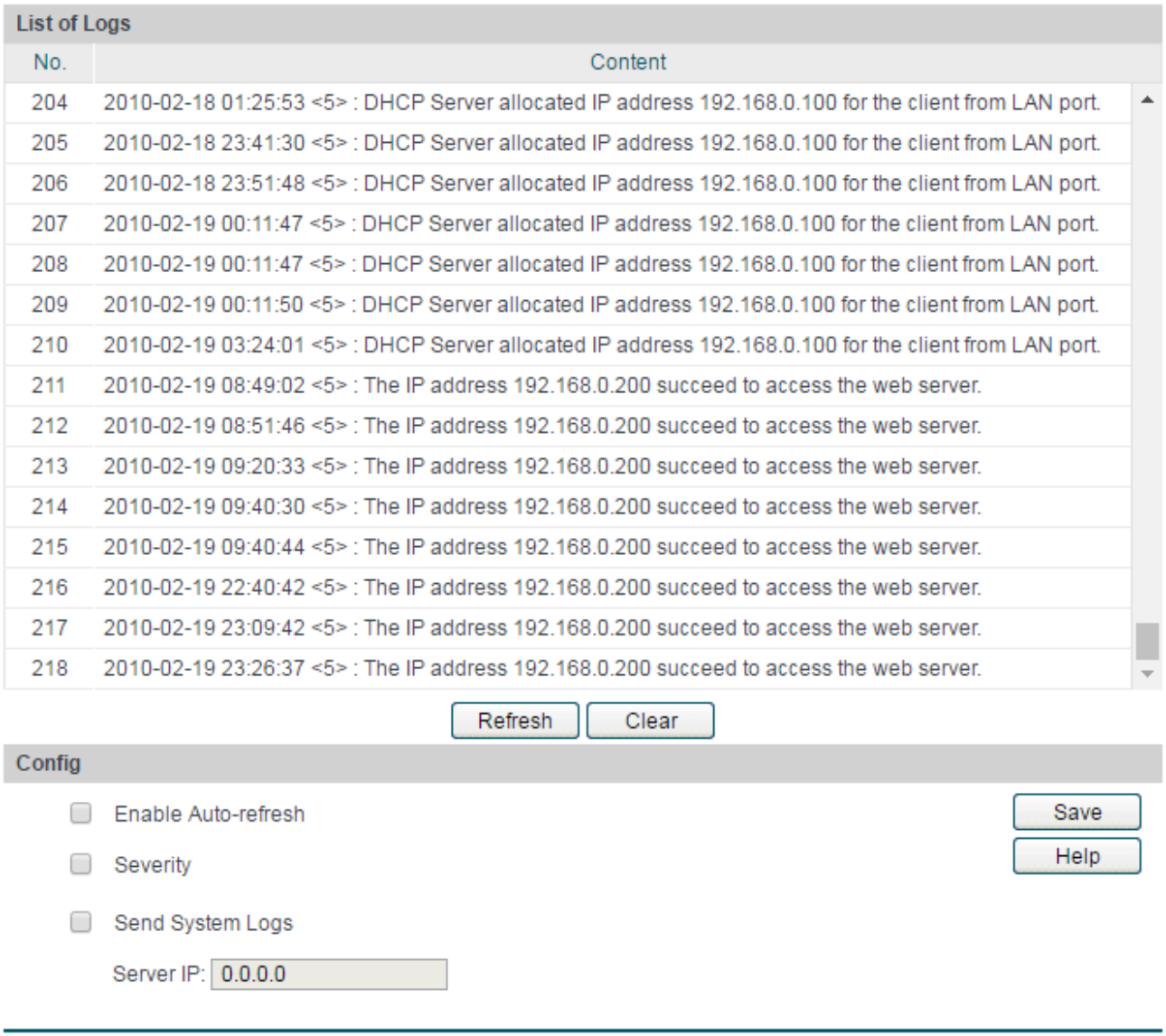


Figure 4-75 Logs

- **List of Logs**

  List of Logs displays the system log information in log buffer.

- **Config**

  Enable Auto-refresh: With this option selected, the page will refresh automatically every 5 seconds.

  Severity: Displays the severity level of the log information. You can select a severity level to display the log information with the same level.

  Send System Logs: Select Send System Logs and specify the server IP, then the new added logs will be sent to the specified server.

The Logs of switch are classified into the following eight levels.

Severity	Level	Description
emergencies	0	The system is unusable.
alerts	1	Action must be taken immediately.
critical	2	Critical conditions
errors	3	Error conditions
warnings	4	Warnings conditions
notifications	5	Normal but significant conditions
informational	6	Informational messages
debugging	7	Debug-level messages

4.8.8 NAT Table

NAT Table corresponds to a mapping relation, which displays the connection sessions in network to help user check forwarding status and troubleshoot network.

Choose the menu **Maintenance→NAT Table→NAT Table** to load the following page.

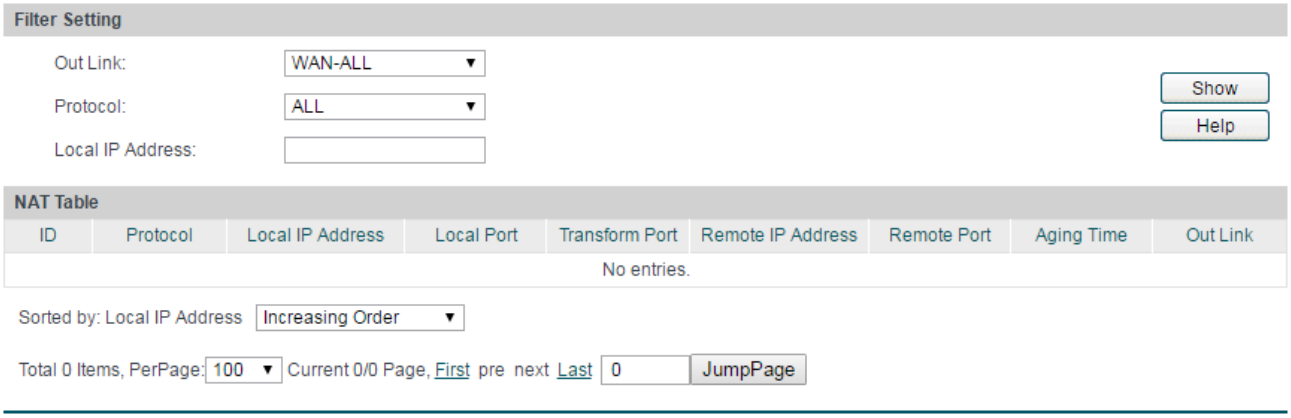


Figure 4-76 NAT Table

The following items are displayed on this screen:

➢ **Filter Setting**

Out Link: Select an interface for forwarding data packets.

Protocol: Select the protocol which is used in the link.

Local IP Address: Optional. Enter the local IP address to be filtered.

Configure the options above, then click <Show> to apply.

➢ **NAT Table**

Protocol:	Displays the protocol used in the current network link.
Local IP Address:	Displays the IP address of the device in LAN.
Local Port:	Displays the used port of the device in LAN.
Transform Port:	Displays the WAN port through which the data is sent after transformed by NAT.
Remote IP Address:	Displays the IP address of the device in WAN.
Remote Port:	Displays the used port of the device in WAN.
Aging Time:	Displays the time which the link lasts (Unit: second).
Out Link:	Displays the WAN port which is used in the link.
Sorted by:	Select the rule for displaying the NAT Table. You can click table headers to sort items.

Appendix A Hardware Specifications

Standards and Protocols	IEEE 802.3, 802.3u TCP/IP, PPPoE, DHCP, ICMP, NAT, SNTP,HTTP,DNS
Ports	One 10/100 Auto-Negotiation WAN RJ45 port (Auto MDI/MDIX)
	Three adjustable 10/100M Auto-Negotiation WAN/LAN RJ45 ports (Auto MDI/MDIX)
	One 10/100M Auto-Negotiation LAN RJ45 port (Auto MDI/MDIX)
	One Console Port
Transmission Medium	10Base-T: UTP/STP of Cat. 3 or above (≤100m)
	100Base-TX: UTP/STP of Cat. 5 or above (≤100m)
LEDs	PWR, SYS, Link/Act, 100Mps
Power	100-240V~ 50/60Hz 0.3A
Operating Environment	Operating Temperature: 0ºC to 40ºC
	Storage Temperature: -40ºC to 70ºC
	Operating Humidity: 10% to 90%RH Non-condensing
	Storage Humidity: 5% to 90%RH Non-condensing

Appendix B FAQ

Q1. What can I do if I cannot access the web-based configuration page?

1. For the first login, please try the following steps:

    1) Make sure the cable is well connected to the LAN port of the router. The corresponding LED should flash or be solid light.

    2) Make sure the IP address of your PC is set in the same subnet addresses of the router. It is recommended to set your PC to get the IP address automatically. Then the router with DHCP enabled can automatically assign the IP address to your PC. If you want to configure your PC manually, please set 192.168.0.x ("x" is any number between 2 to 254) for the IP address and 255.255.255.0 for the Subnet Mask.

    3) Test the connection between your PC and TL-R480T+ via Ping command.

    4) If you still cannot access the configuration page, please restore your router to its factory default settings and try to log in again.

2. If your management port has been changed, please log into the router with the new address, such as http://192.168.0.1:XX ("XX" is the new management port number).

3. If you had successfully logged into the router before, but now you cannot access the router. It is quite possible that the configuration of your router has been changed by others, especially when the Remote Web Management function is enabled. You are recommended to restore your router and reconfigure the management port number and the username as well as the password for your network security.

4. If you cannot access the router even after restoring the router to its defaults, or your login is dropped down just after a while, it is quite possible that your router is attacked by ARP cheating. It is recommended to locate and quarantine the source of ARP cheating so as to prevent your network from the attacks.

5. Check to see if you have configured the proxy server for IE browser. If so, please disable the IE proxy server first.

Q2: What can I do if I forgot the username and the password of the router? How to restore the router to its factory default settings?

You can restore the router to its factory default settings by the **Reset** button. It must be noted that once the router is Reset, all the current configuration settings will be lost.

With the router powered on, use a pin to press and hold the **Reset** button (about 5 seconds). If the SYS LED is flashing 5 times in high frequency, release the **Reset** button. It means the router is restored successfully. The default management address of the router is **http://192.168.0.1**, and the default username and the password are both **admin**.

Q3: What can I do if the router with the remote management function enabled cannot be accessed by the remote computer?

1. Make sure that the IP address of the remote computer is in the subnet allowed to remotely access the router.
2. If the router's management port has been modified, please log into the router with the new address, such as http://192.168.0.1:XX ("XX" is the new management port number).
3. Check to see if the management port has been mapped to the service port of the LAN host in the Virtual Server function. If so, you should make a change in the router's management port or virtual server's service port.
4. Make sure that the NAT DMZ service is disabled.

Q4: Some function of the router need to define the IP address subnet with Subnet Mask. What are the common values of the Subnet Mask?

Subnet Mask is a 32-bit binary address used to distinguish the network address and the host address. When dividing the network, the different Subnet Mask defines different subnet, and each subnet owns different number of hosts.

After conversed from 32-bit binary address to decimal address, the common Subnet Mask values can be 8 (which represents the default Subnet Mask value of class A: 255.0.0.0), 16 (which represents the default Subnet Mask value of class B: 255.255.0.0), 24 (which represents the default Subnet Mask value of class C: 255.255.255.0) or 32 (which represents the default Subnet Mask value of class D: 255.255.255.255).

Appendix C Glossary

	Glossary	Description
A	ALG (Application Layer Gateway)	Application Level Gateway (ALG) is application specific translation agent that allows an application on a host in one address realm to connect to its counterpart running on a host in different realm transparently.
	ARP (Address Resolution Protocol)	Internet protocol used to map an IP address to a MAC address.
	AH (Authentication Header)	A security protocol that provides data authentication and optional anti-replay services. AH is embedded in the data to be protected (a full IP datagram).
D	DDNS (Dynamic Domain Name Server)	The capability of assigning a fixed host and domain name to a dynamic Internet IP address.
	DHCP (Dynamic Host Configuration Protocol)	A protocol that automatically configure the TCP/IP parameters for the all the PCs that are connected to a DHCP server.
	DMZ (Demilitarized Zone)	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 (Domain Name Server)	An Internet Server that translates the names of websites into IP addresses.
	DSL (Digital Subscriber Line)	A technology that allows data to be sent or received over existing traditional phone lines.
E	ESP (Encapsulating Security Payload)	Security protocol that provides data privacy services, optional data authentication, and anti-replay services. ESP encapsulates the data to be protected.
F	FTP (File Transfer Protocol)	Application protocol, part of the TCP/IP protocol stack, used for transferring files between network nodes.

	Glossary	Description
H	H.323	H.323 allows dissimilar communication devices to communicate with each other by using a standardized communication protocol. H.323 defines a common set of CODECs, call setup and negotiating procedures, and basic data transport methods.
	HTTP (Hypertext Transfer Protocol)	The protocol used by Web browsers and Web servers to transfer files, such as text and graphic files.
I	ICMP (Internet Control Messages Protocol)	Network layer Internet protocol that reports errors and provides other information relevant to IP packet processing.
	Internet	Largest global Internetwork, connecting tens of thousands of networks worldwide and having a "culture" that focuses on research and standardization based on real-life use.
	IP (Internet Protocol)	Network layer protocol in the TCP/IP stack offering a connectionless Internetwork service. IP provides features for addressing, type-of-service specification, fragmentation and reassembly, and security.
	ISP (Internet Service Provider)	Company that provides Internet access to other companies and individuals.
	IKE (Internet Key Exchange)	IKE establishes a shared security policy and authenticates keys for services (such as IPSec) that require keys. Before any IPSec traffic can be passed, each router/firewall/host must verify the identity of its peer.
	IPsec (IP Security)	A framework of open standards that provides data confidentiality, data integrity, and data authentication between participating peers.
L	LAN (Local Area Network)	High-speed, low-error data network covering a relatively small geographic area (up to a few thousand meters). LANs connect workstations, peripherals, terminals, and other devices in a single building or other geographically limited area.

	Glossary	Description
M	MAC address (Media Access Control address)	Standardized data link layer address that is required for every port or device that connects to a LAN. Other devices in the network use these addresses to locate specific ports in the network and to create and update routing tables and data structures. MAC addresses are 6 bytes long and are controlled by the IEEE.
	MTU (Maximum Transmission Unit)	The size in bytes of the largest packet that can be transmitted.
N	NAT (Network Address Translator)	Mechanism for reducing the need for globally unique IP addresses. NAT allows an organization with addresses that are not globally unique to connect to the Internet by translating those addresses into globally routable address space.
	NTP Server	NTP Server is used for synchronising the time across computer networks.
P	POP3 (Post Office Protocol 3)	POP3 is intended to permit a workstation to dynamically access a maildrop on a server host in a useful fashion.
	PPPoE (Point-to-Point Protocol over Ethernet)	PPPoE is a network protocol for encapsulating Point-to-Point Protocol (PPP) frames inside Ethernet frames.
S	SMTP (Simple Mail Transfer Protocol)	SMTP is an Internet standard for electronic mail (e-mail) transmission
	SSH (Secure Shell Protocol)	SSH is a network protocol that allows data to be exchanged using a secure channel between two networked devices.
	SA (Security Association)	SA is the establishment of shared security attributes between two network entities to support secure communication.

	Glossary	Description
T	TCP (Transfer Control Protocol)	Connection-oriented transport layer protocol that provides reliable full-duplex data transmission.
	TCP/IP (Transmission Control Protocol/ Internet Protocol)	Common name for the suite of protocols to support the construction of worldwide Internetworks. TCP and IP are the two best-known protocols in the suite.
	Telnet (Telecommunication Network protocol)	Telnet is used for remote terminal connection, enabling users to log in to remote systems and use resources as if they were connected to a local system.
U	UDP (User Datagram Protocol)	UDP is a simple protocol that exchanges datagrams without acknowledgments or guaranteed delivery, requiring that error processing and retransmission be handled by other protocols.
	UPnP (Universal Plug and Play)	UPnP is a set of networking protocols for primarily residential networks without enterprise class devices that permits networked devices.
	URL (Uniform Resource Locator)	URL describes the access method and the location of an information resource object on the Internet
V	VLAN (Virtual Local Area Network)	Group of devices on one or more LANs that are configured (using management software) so that they can communicate as if they were attached to the same wire, when in fact they are located on a number of different LAN segments. Because VLANs are based on logical instead of physical connections, they are extremely flexible.
W	WAN (Wide Area Network)	Data communications network that serves users across a broad geographic area and often uses transmission devices provided by common carriers.