

# TP-LINK®

# **User Guide**

# TL-R488T Load Balance Broadband Router



**Rev: 1.1.2** 

# **COPYRIGHT & TRADEMARKS**

Specifications are subject to change without notice. **TP-LINK**  $^{\circledR}$  is a registered trademark of TP-LINK TECHNOLOGIES CO., LTD. Other brands and product names are trademarks or registered trademarks of their respective holders.

No part of the specifications may be reproduced in any form or by any means or used to make any derivative such as translation, transformation, or adaptation without permission from TP-LINK TECHNOLOGIES CO., LTD. Copyright © 2008 TP-LINK TECHNOLOGIES CO., LTD. All rights reserved.

http://www.tp-link.com

## **FCC STATEMENT**



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

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

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

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

# **CE Mark Warning**



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

# **CONTENTS**

Раскаде С	ontents	1	
Chapter 1	Introduction	2	
1.1	Overview of the Router	2	
1.2	Features		
1.3	Conventions	3	
Chapter 2	Hardware installation	4	
2.1	Panel Layout	4	
	2.1.1 The Front Panel	4	
	2.1.2 The Rear Panel	5	
2.2	System Requirements	5	
2.3	Installation Environment Requirements	5	
2.4	Connecting the Router	5	
Chapter 3	Quick Installation Guide	7	
3.1	Configure PC	7	
3.2	Login	11	
Chapter 4	Configuring the Router	15	
4.1	Status	15	
4.2	Quick Setup	17	
4.3	Network	17	
	4.3.1 LAN	17	
	4.3.2 WAN	18	
	4.3.3 Network service detection	29	
	4.3.4 MAC Clone	31	
	4.3.5 Flow Balance	31	
	4.3.6 Balance Policy	33	
	4.3.7 WAN Port Parameter	35	
4.4	DHCP		
	4.4.1 DHCP Settings		
	4.4.2 DHCP Clients List		
	4.4.3 Address Reservation		
4.5	Forwarding		
	4.5.1 Virtual Servers		
	4.5.2 Port Triggering		
	4.5.3 DMZ		
	4.5.4 UPnP		
4.6	Security4.6.1 Firewall		
	4 O I FIIEWAII	40	

	4.6.2	IP Filtering	46
	4.6.3	Domain Filtering	49
	4.6.4	MAC Filtering	50
	4.6.5	Screen	52
4.	7 Static	Routing	55
4.	8 Session	on Limit	57
	4.8.1	Session Limit	57
	4.8.2	Session List	58
4.	9 QoS.		58
	4.9.1	QoS Settings	59
	4.9.2	QoS Rules List	59
4.	10 IP&N	/IAC Binding	60
	4.10.1	Binding Setting	60
	4.10.2	ARP List	62
4.	11 Dynar	nic DNS	63
	4.11.1	Dyndns DDNS	63
	4.11.2	PeanutHull DDNS	64
	4.11.3	Comexe DDNS	65
4.	12 Switch	n Setting	65
	4.12.1	Port Statistics	66
	4.12.2	Port Rate Control	66
	4.12.3	Port Parameter	67
	4.12.4	Port Status	67
4.	13 System	m Tools	68
	4.13.1	Time Setting	68
	4.13.2	Firmware	69
	4.13.3	Factory Defaults	70
	4.13.4	Backup and Restore	70
	4.13.5	Reboot	72
	4.13.6	Password	
	4.13.7	Log	
	4.13.8	Remote Management	
	4.13.9	Statistics	
		WAN Speed Detect	
		1 IP NAT Table	
		2 NAT Source Port Settings	
Appendi	x A: Spe	cifications	79
Appendi	Appendix B: FAQ80		
Appendi	x C: Glos	ssary	85
		<del>-</del>	

# **Package Contents**

The following items should be found in your package:

- > One TL-R488T Load Balance Broadband Router
- > One power cord for TL-R488T Load Balance Broadband Router
- > One Resource CD for TL-R488T Load Balance Broadband Router, including:
  - This Guide
  - Other Helpful Information
- Mounting kits for installing in a standard 19 rack

### P Note:

If any of the listed contents are damaged or missing, please contact the retailer from whom you purchased the product for assistance.

# **Chapter 1 Introduction**

Thank you for choosing the TL-R488T Load Balance Broadband Router!

#### 1.1 Overview of the Router

The TL-R488T Load Balance Broadband Router possesses excellent throughput and driving load capability, which consumedly meets the requirements from Internet cafe and small /medium/sizable enterprise with volumes of users, making a more expedite communication. The superior performance will bring you full-new experience of a non-bottle-neck network.

TL-R488T Load Balance Broadband Router makes plenty of applications become a reality. It can be used for constructing intranet FTP, WEB, and Mail server, etc. Inaccessibly, it features network game ports opened, MSN audio conversation and special application setting, providing much more additional value to your network.

TL-R488T Load Balance Broadband Router provides four WAN ports, with plugging four wan lines, the export bandwidth of it could be multi-time-increased, enjoying various services from different ISPs. The router features fully automatically load balance policy, no need for any manually work, it works with backup and load balancing functions. The connection will furbish when one line is broken down, while the streaming will part automatically.

Featuring firewall and VPN Passthrough, the TL-R488T Load Balance Broadband Router resists most common Internet attacks and ensures secure data connectivity and transmission over the Internet.

TL-R488T Load Balance Broadband Router is easy-to-manage. Quick Setup is supported and friendly help messages are provided for every step. So you can configure it quickly and share Internet access, files and fun comfortably.

#### 1.2 **Features**

- > Intel IXP core, main frequency up to 533Hz
- Complies with IEEE802.3, IEEE802.3u standards
- 1 LAN port, 4 WAN ports, backup connections automatically for each other
- Supports Port Bandwidth Control, Port Mirror, Port-based VLAN for LAN ports
- Built-in NAT and DHCP server supporting static IP address distributing  $\triangleright$
- Supports Virtual Server, Port Triggering, and DMZ host  $\triangleright$
- $\triangleright$ Built-in firewall supporting IP address filtering, Domain Name filtering, and MAC address filtering
- Supports connecting/disconnecting Internet at a specified time of day
- Supports access control, allowing parents and network administrators to establish restricted access policies based on the time of day for children or staff
- Supports TCP/IP, PPPoE, DHCP, ICMP, NAT, SNTP

- Supports UPnP, Dynamic DNS, Static Routing, VPN pass-through  $\triangleright$
- $\triangleright$ **Supports Traffic Statistics**
- Supports ICMP-FLOOD, UDP-FLOOD, TCP-SYN-FLOOD filter
- Ignores Ping packets from WAN or LAN ports
- Supports firmware upgrade
- Supports Remote and Web management

#### **Conventions** 1.3

The Router or TL-R488T mentioned in this User guide stands for TL-R488T Load Balance Broadband Router without any explanations.

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

You can set the parameters according to your demand.

# **Chapter 2 Hardware installation**

## 2.1 Panel Layout

### 2.1.1 The Front Panel

The front panel of the TL-R488T consists of several LED indicators, which is designed to indicate connections. Viewed from left, the next table describes the LEDs on the front panel of the router.

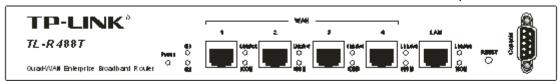


Figure 2-1

### **LED Descriptions:**

Name	Action	Descript	tion
Power	Not lit	The router is power on	
	Lit up	The router is power off	
B 4 4	Not lit	The router works properly	M4 and MO are flashing
M1	Lit up	The router has a hardware error	M1 and M2 are flashing
M2	Not lit	The router has a hardware error	synchronously, that indicate the router is restoring the
	Lit up	The router has a hardware error	factory default settings.
	Flashing	The router works properly	lactory default settings.
\A/A NI/L A NI	Not lit	There is no device linked to the co	orresponding port
(Link/Act)	Lit up	There is a device linked to the corresponding port but no activity	
	Flashing	There is an active device linked to the corresponding port	
100M	Not lit	The linked device is running at 10	Mbps
	Lit up	The linked device is running at 10	0Mbps

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

**Reset:** Use the button to restore the router to the factory defaults.

There are two ways to reset the router:

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

**Method two:** Use the Factory Default Reset button. First, turn off the router's power. Second, press the default reset button, then turn on the router's power, and hold the reset button until the M1 and M2 LED flash simultaneously (about 3 seconds). At last, release the reset button and wait for the router to reboot.

### Note:

Ensure the router is powered on before it restarts completely.

- > WAN: Four RJ45 port for connecting the router to a cable, DSL modem or Ethernet
- LAN: One 10/100Mbps RJ45 port for connecting the router to the local PCs

#### 2.1.2 The Rear Panel

The rear panel of the TL-R488T only features a power receptacle, which is an AC power receptacle. Connect the female of the power cord head here, and the male head to the AC power outlet.

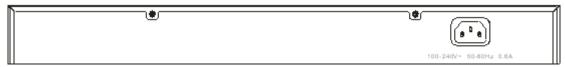


Figure 2-2

#### 2.2 **System Requirements**

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

#### 2.3 **Installation Environment Requirements**

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

### R Note:

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

# **Connecting the Router**

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

TL-R488T

1. Power off your PC(s), Cable/DSL modem, and the router.

- 2. Connect the PC(s) and all Switches/Hubs on your LAN to the LAN Ports on the router, shown in Figure 2-3.
- 3. Connect the DSL/Cable modem to the WAN port on the router, shown in figure 3-1.
- 4. Connect the AC power adapter to the AC power socket on the router, and the other end into an electrical outlet. The router will start to work automatically.
- 5. Power on your PC(s) and Cable/DSL modem.

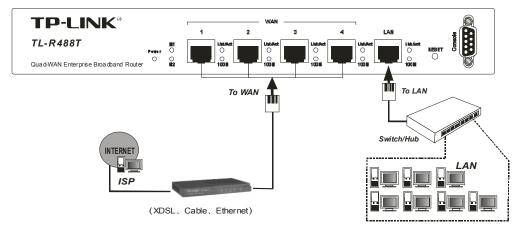


Figure 2-3

# **Chapter 3 Quick Installation Guide**

After connecting the TL-R488T router into your network, you should configure it. This chapter describes how to configure the basic functions of your TL-R488T 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.

### **Configure PC** 3.1

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

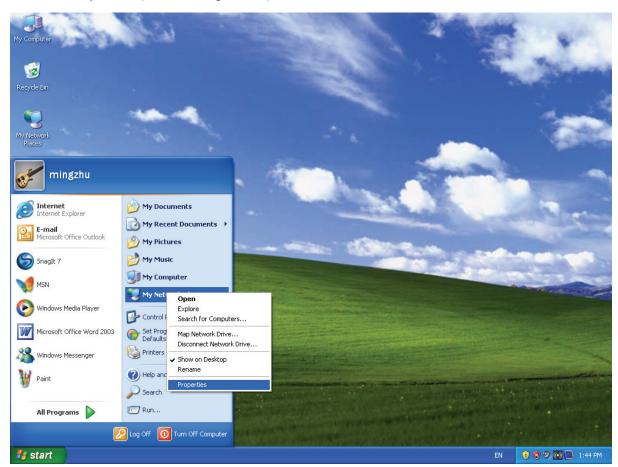


Figure 3-1

Step 2: On the following screen, right click Local Area Connection (LAN), and then select Properties.

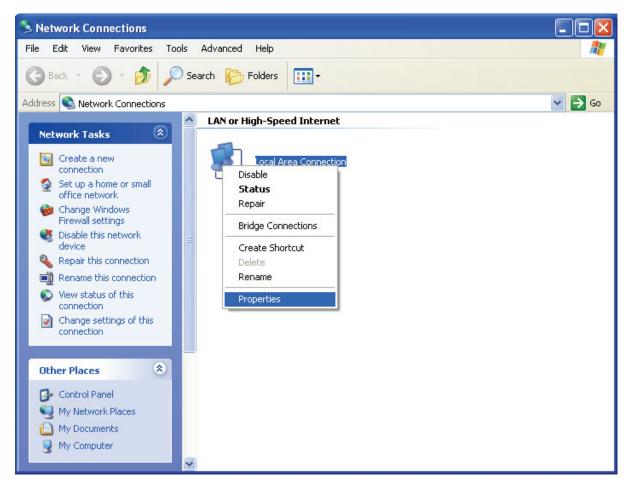


Figure 3-2

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

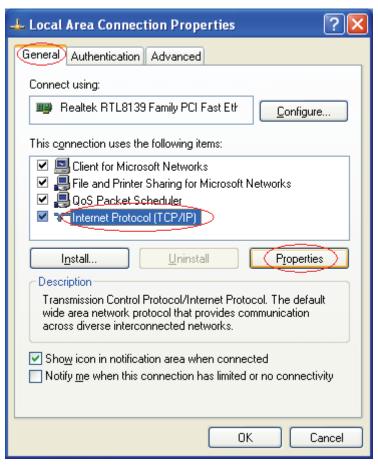


Figure 3-3

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

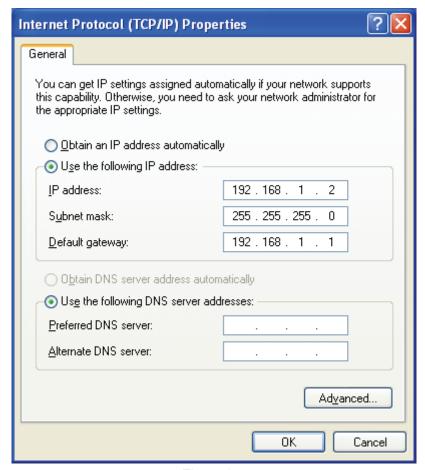


Figure 3-4

### 

You can select "Obtain an IP address automatically" and "Obtain DNS server address automatically" as shown above to get an IP address manually.

Now, you can run the Ping command in the command prompt to verify the network connection. Please click the **Start** menu on your desktop, select **run** tab, type **cmd** in the field, and then type *ping 192.168.1.1* on the next screen, and then press **Enter**.

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

```
Pinging 192.168.1.1 with 32 bytes of data:

Reply from 192.168.1.1: bytes=32 time=1ms TTL=254

Ping statistics for 192.168.1.1:

Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:

Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

Figure 3-5

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

```
C:\Documents and Settings\Administrator>ping 192.168.1.1
Pinging 192.168.1.1 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Ping statistics for 192.168.1.1:
   Packets: Sent = 4, Received = 0, Lost = 4 (100% loss)
```

Figure 3-6

You can check it follow the steps below:

### 

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

#### 3.2 Login

Once your host PC is properly configured, please proceed as follows to use the Web-based Utility: Start your web browser and type the private IP address of the Router in the URL field: 192.168.1.1.



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

Figure 3-7

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

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

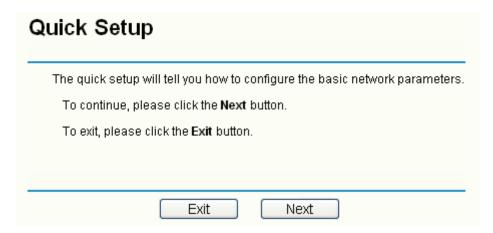


Figure 3-8

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

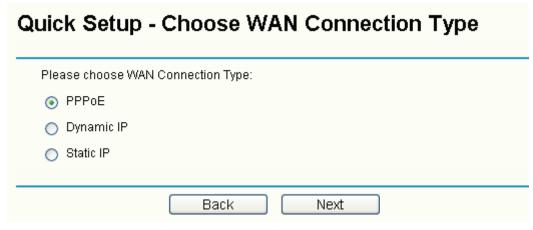


Figure 3-9

The router supports three popular ways to connect to Internet. Please select one compatible with your ISP. If you are given another way not listed here, please refer to **Network**→ **WAN** for detailed list.

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



Figure 3-10

- **Step 4:** If you choose **Dynamic IP** in Figure 3-9, the router will automatically receive the IP parameters from your ISP without needing to enter any parameters.
- **Step 5:** If you Choose **Static IP**, you should enter the detailed IP information in Figure 3-11. Click the **Next** button

Quick Setup - Static IP		
IP Address:	10.20.1.160	
Subnet Mask:	255.255.255.0	
Default Gateway:	0.0.0.0	(Optional)
Primary DNS:	0.0.0.0	(Optional)
Secondary DNS:	0.0.0.0	(Optional)
	Back N	lext

Figure 3-11

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

Quick Setup - Finish		
Congratulations! The router is now connecting you to the Internet.		
Back Finish		

Figure 3-12

# **Chapter 4 Configuring the Router**

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

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

#### 4.1 **Status**

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

#### **Status** Firmware Version: 3.4.1 Build 080509 Rel.57122n Hardware Version: R488Tv2a 000000000 LAN MAC Address: 00-0A-EB-12-34-19 IP Address: 192.168.1.1 Subnet Mask: 255.255.255.0 WAN1 Link Down Status: 00-0A-EB-12-34-1A MAC Address: Dynamic IP IP Address: 0.0.0.0 Subnet Mask: 0.0.0.0 Default Gateway: 0.0.0.0 Renew Obtaining network parameters... DNS Server: 0.0.0.0 , 0.0.0.0 WAN2 Status: Link Down MAC Address: 00-0A-EB-12-34-1B IP Address: 0.0.0.0 Dynamic IP Subnet Mask: 0.0.0.0 Default Gateway: 0.0.0.0 Renew Obtaining network parameters... DNS Server: 0.0.0.0, 0.0.0.0 **WAN3** Link Down Status: MAC Address: 00-0A-EB-12-34-1C IP Address: 0.0.0.0 Dynamic IP 0.0.0.0 Subnet Mask: Default Gateway: 0.0.0.0 Renew Obtaining network parameters... DNS Server: 0.0.0.0, 0.0.0.0 WAN4 Link Down Status: MAC Address: 00-0A-EB-12-34-1D IP Address: 0.0.0.0 Dynamic IP Subnet Mask: 0.0.0.0Default Gateway: 0.0.0.0 Obtaining network parameters... Renew 0.0.0.0 , 0.0.0.0 DNS Server: **Traffic Statistics** Rate Received (Bytes) Sent (Bytes) Received (Packets) Sent (Packets) Total 0 0 0 WAN1 0 n O WAN2 0 0 0 WAN3 0 0 WAN4 0 0 0 day(s) 00:12:34 Refresh System Up Time:

Figure 4-1

- LAN This field displays the current information for the LAN, including the "MAC address", "IP address" and "Subnet Mask".
- > WAN 1~4 This field displays the parameters applied to the WAN ports of the router, including "MAC address", "IP address", "Subnet Mask", "Default Gateway" and so on.

If PPPoE/L2TP/PPTP is chosen as the WAN connection type, the Disconnect button will be shown here while you are accessing the Internet. You can also cut the connection by clicking the button. If you have not connected to the Internet, a Connect button will be shown, and you can click the button to establish the connection.

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

#### 4.2 **Quick Setup**

Please refer to chapter 3"Quick Installation Guide".

#### 4.3 **Network**

Choose menu "Network", the next submenus are as shown below:



Figure 4-2

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

#### 4.3.1 LAN

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

LAN		
	MAC Address:	00-0A-EB-12-34-19
	IP Address:	192.168.1.1
	Subnet Mask:	255.255.255.0
		Save

Figure 4-3

- MAC Address This field displays the physical address of the LAN. The value can't be changed.
- ➤ **IP Address -** Enter the IP address for the LAN of the Router, the formal is in dotted-decimal notation (the factory default value is 192.168.1.1).
- ➤ **Subnet Mask** Enter the subnet mask for the LAN of the Router, this address code determines the size of the network. Normally use 255.255.255.0 as the subnet mask.

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

### 4.3.2 WAN

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

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

### 1. Dynamic IP

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

WAN	
WAN Port:	WAN1 💌
WAN Connection Type:	Dynamic IP
☐ Interior network:	0.0.0.0-0.0.0
IP Address:	0.0.0.0
Subnet Mask:	0.0.0.0
Default Gateway:	0.0.0.0
	Renew Release Obtaining network parameters
MTU Size (in bytes):	(The default is 1500, do not change unless necessary.)
	Use These DNS Servers
Primary DNS:	0.0.0.0
Secondary DNS:	0.0.0.0 (Optional)
	Get IP with Unicast DHCP (It is usually not required.)
Ingress Bandwidth:	100000 Kbps (Optional)
Egress Bandwidth:	100000 Kbps (Optional)
	Save
	0.010

Figure 4-4

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

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

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

### 2. Static IP

If you are given a fixed IP (static IP), please select **Static IP** (shown in Figure 4-5), and then fixed IP parameters specified by your ISP.

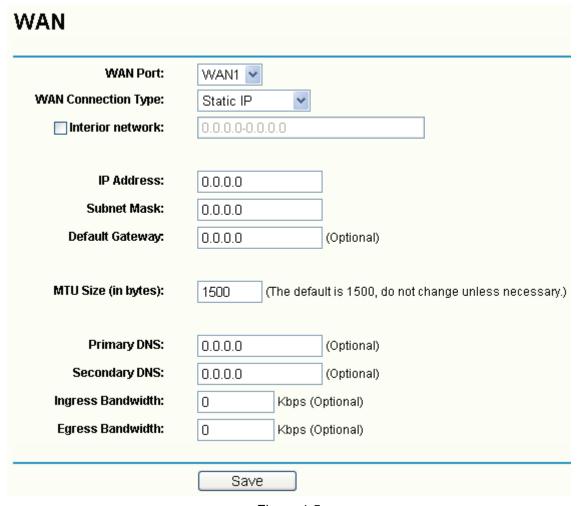


Figure 4-5

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

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

### 3. PPPoE

If you are given a user name and a password, please select **PPPoE** (shown in Figure 4-6). If you are not sure which connection type you use currently, please contact your ISP to obtain the correct information.

WAN	
WAN Port:	WAN1 🕶
WAN Connection Type:	PPPoE 💌
User Name:	23
Password:	•••••
Wan Connection Mode:	Connect on Demand     Max Idle Time: 15 minutes (0 means remain active at all times.)      Connect Automatically
	Time-based Connecting Period of Time:from 0 : 0 (HH:MM) to 23 : 59 (HH:MM)
	Connect Manually  Max Idle Time: 15 minutes (0 means remain active at all times.)  Connect Disconnect
	Save Advanced

Figure 4-6

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

- 1) If you want your Internet connection to remain active at all times, enter 0 in the **Max Idle Time** field. Otherwise, enter the number of minutes you want to have elapsed before your Internet connection terminates.
- 2) Sometimes the connection can not be disconnected although you specify a time to Max Idle Time. This is because there may still be active applications in the background, which may cause fee accounted by your ISP.
- > Connect Automatically Connect automatically after the router is disconnected. To use this option, click the radio button.
- > Time-based Connecting You can configure the router to make it connect or disconnect based on time. Enter the start time in HH:MM for connecting and end time in HH:MM for disconnecting in the **Period of Time** fields.

### Note:

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

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

### Note:

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

Click the **Advanced** button to set up the advanced option as shown in Figure 4-7.

# PPPoE Advanced Settings

MTU Size (in bytes):	(The default is 1492, do not change unless necessary.)
Service Name: AC Name:	
	Use IP address specified by ISP
ISP Specified IP Address:	0.0.0.0
Detect Online Interval:	O Seconds (0 ~ 120 seconds, the default is 0, 0 means not detecting.)
	Use the following DNS Servers
Primary DNS:	0.0.0.0
Secondary DNS:	0.0.0.0 (Optional)
Ingress Bandwidth:	8000 Kbps (Optional)
Egress Bandwidth:	2000 Kbps (Optional)
	Save Back

Figure 4-7

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

### 4. BigPondCable

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

WAN	
WAN Port:	WAN1 🕶
WAN Connection Type:	BigPond Cable 💌
User Name:	
Password:	
Auth Server:	sm-server
Auth Domain:	
Ingress Bandwidth:	100000 Kbps (Optional)
Egress Bandwidth:	100000 Kbps (Optional)
MTU Size (in bytes):	1500 (The default is 1500, do not change unless necessary.)
	O Connect on Demand
	Max Idle Time: 15 minutes (0 means remain active at all times.)
	Connect Automatically
	Connect Manually
	Max Idle Time: 15 minutes (0 means remain active at all times.)
	Connect Disconnected!
	Save

Figure 4-8

- ➤ **User Name/Password** Enter the User Name and Password provided by your ISP. These fields are case-sensitive.
- > **Auth Server** Enter the authenticating server IP address or host name.
- > Auth Domain Type in the domain suffix server name based on your location.
- ➤ MTU Size The normal MTU (Maximum Transmit Unit) value for most Ethernet networks is 1500 bytes. For some ISPs, you may need to modify the MTU. But this is rarely required, and should not be done unless you are sure it is necessary for your ISP connection.
- > Connect on Demand You can configure the router to disconnect your Internet connection

after a specified period of the Internet connectivity (Max Idle Time). If your Internet connec-tion has been terminated due to inactivity, Connect on Demand enables the router to automatically re-establish your connection as soon as you attempt to access the Internet again. If you wish to activate Connect on Demand, click the radio button. If you want your Internet connection to remain active at all times, enter 0 in the Max Idle Time field. Otherwise, enter the number of minutes you want to have elapsed before your Internet connection ter-minates.

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

### Note:

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

### 5. L2TP

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

WAN	
WAN Port:	WAN1 🕶
WAN Connection Type:	L2TP 💌
User Name:	username
Password:	•••••
	Connect Disconnect Disconnected!
	Dynamic IP
Server IP Address/Name:	
IP Address:	0.0.0.0
Subnet Mask:	0.0.0.0
Gateway:	0.0.0.0
DNS:	0.0.0.0 , 0.0.0.0
Internet IP Address:	0.0.0.0
Internet DNS:	0.0.0.0 , 0.0.0.0
MTU Size (in bytes):	1460 (The default is 1460, do not change unless necessary.)
Max Idle Time:	15 minutes (0 means remain active at all times.)
WAN Connection Mode:	Connect on Demand
	Connect Automatically
	Connect Manually
	Save

Figure 4-9

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

enter the number of minutes you want to have elapsed before your Internet connection terminal.

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

### Note:

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

### 6. PPTP

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

WAN	
WAN Port:	WAN1
WAN Connection Type:	PPTP
User Name:	username
Password:	•••••
	Connect Disconnected!
Common ID Address Alexand	Dynamic IP
Server IP Address/Name:	
IP Address:	0.0.0.0
Subnet Mask:	0.0.0.0
Gateway:	0.0.0.0
DNS:	0.0.0.0 , 0.0.0.0
Internet IP Address:	0.0.0.0
Internet DNS:	0.0.0.0 , 0.0.0.0
MTU Size (in bytes):	1420 (The default is 1460, do not change unless necessary.)
Max Idle Time:	15 minutes (0 means remain active at all times.)
WAN Connection Mode:	Connect on Demand
	Connect Automatically
	Connect Manually
	Save

Figure 4-10

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

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

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

#### 4.3.3 **Network service detection**

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

# Network Service Detection WAN1: **Link Down** By Ping **Destination IP Address for Ping:** By DNS Query DNS IP Address: WAN2: Link Down By Ping **Destination IP Address for Ping:** 0.0.0.0 By DNS Query **DNS IP Address:** WAN3: Link Down By Ping **Destination IP Address for Ping:** 0.0.0.0 By DNS Query DNS IP Address: WAN4: **Link Down** By Ping **Destination IP Address for Ping:** 0.0.0.0 By DNS Query **DNS IP Address:** Save

Figure 4-11

- **By Ping** Detect whether Internet connection is online or not by Ping.
- ➤ **Destination IP Address for Ping** Enter the correct IP address that really existed on the WAN network. For example: 202.96.134.188.
- **By DNS Query** Detect whether Internet connection is online or not by sending query packet to DNS Server.
- DNS Server IP Address Enter the correct DNS IP address that really existed on the WAN network. For example: 202.96.134.133.

### 4.3.4 MAC Clone

Choose menu "**Network→MAC Clone**", you can configure the MAC address of the WAN on the screen below (shown in Figure 4-12).

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



Figure 4-12

- ➤ WAN MAC Address (1~4) This field displays the current MAC address of the WAN port, which is used for the WAN port. If your ISP requires that you register the MAC address, please enter the correct MAC address into this field. The format for the MAC address is XX-XX-XX-XX-XX-XX (for example: 00-0A-EB-12-34-1A).
- Your PC's MAC Address This field displays the MAC address of the PC that is managing the router. If the MAC address is required, you can click the Clone MAC Address button and this MAC address will fill in the "WAN MAC Address" field.

### Note:

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

### 4.3.5 Flow Balance

Choose menu "Network → Flow Balance", you can specify priority channels according to source or destination IP addresses, distributing flexibly Internet resource and services from different ISPs. For example, you can specify some packets prior forwarding from WAN port 1, which depend on specified source or destination IP addresses.

#### Flow Balance Enable/Disable WAN Enable Enable Enable Enable Save WAN1 WAN2 WAN3 WAN4 Extra IP Address Dispatch Rules: Disabled Enable Backup: Backup List Files Upload: Upload List Files Browse.. **ID** Appointed Export Address Type Protocol IP Address(Range) Port(Range) Enable Modify Move No. Entry to No. Entry Enable All Disable All Delete All Add New... Previous Next

Figure 4-13

- ➤ Enable/Disable WAN Enable the WAN port you want to use, then click Save to make it effective
- **Extra IP Address Dispatch Rules -** Enable the function, and then make the dispatch rules.
- **Backup -** Click the button to backup the list files.
- ➤ **Upload -** Click the button to upload an existed file. You can click **Browse** to locate the specific file first, and then click the **Upload List Files** to complete the process.
- Rules list This table displays the current dispatch rules.

## To add a dispatch rule:

- **Step 1:** Click **Add New** button in Figure 4-13, Figure 4-14 will appears.
- Step 2: Select the Rules Select, Protocol, Datagram Pass Policy and Transmit Path; enter IP address and Port as shown below.

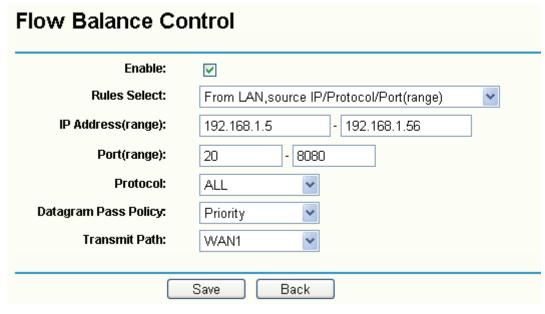


Figure 4-14

## Step 3: Click Save.

To add additional rules, repeat steps 1-3.

# Other configurations for the entries as shown in Figure 4-13:

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

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

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

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

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

## 4.3.6 Balance Policy

Choose menu "**Network→Flow Balance**", you can configure the balance policy in the next screen.

This screen configure the WAN's forward policies which based on three principles: Speed First, Paired IP First, and Application First. We use four tables including Speed Detect Table, Fast Connection Table, Paired IP Table, and Application Table, to register correlative data. Note that, the default time parameters are configured with the corresponding tables, and they have passed relevant tests. If you are not sure, please don't change the settings.

## **Balance Policy** WAN Selected Rules On Fastest-Session: Fastest age for Speed-Detect-Table: 2 seconds (1 ~ 5), default: 2 Age for Speed-Detect-Table: 5 seconds (2 ~ 10), default: 5 Threshold for Fastest-Session: 100 millisecond ( 20 ~ 200 ), default: 100 Age for Fastest-Session-Table: 120 seconds (1 ~ 300), default: 120 Obliged age for Fastest-Session-Table: seconds (10 ~ 1200), default: 600 600 On Existed-IP-Pair: Age for IP-Pairs-Table: 360 seconds(1~1200), default: 360 Obliged age for IP-Pairs-Table seconds(10 ~ 2400), default: 600 600 On Existed-Application Age for Application-Table: 600 seconds (1 ~ 1800), default: 600 Obliged age for Application-Table: 1200 seconds (10 ~ 3600), default: 1200 Save

Figure 4-15

- > On Fastest-Session If you select the option, the data will be transmitted through one of the WAN ports which connect the WAN much quicker than the other.
  - Fastest age for Speed-Detect Table The maximal timeouts for the entries in Speed-Detect-Table. During the time, the entry will be deleted from the table no matter whether the entry has been used.
  - Age for Speed-Detect Table Normal timeouts for the entries in speed-Detect-Table.
     During the time, if an entry has never been used, the entry will be deleted from the table.
  - Threshold for Fastest-Session During the time, if the Router receives a response from Internet, then the connection will be considered as a fast connection. And the connection will be registered in the Faster Connection Table.
  - Age for Fastest-Session-Table Normal timeouts for the entries in Faster-Connection-Table. During the time, if an entry has never been used, the entry will be deleted from the table.
  - Obliged Age for Fastest-Session-Table The maximal timeouts for the entries in Faster-Connection-Table. During the time, the entry will be deleted from the table no matter whether the entry has been used.
- On Existed-IP-Pair If a pair of IP addresses has made a connection via a particular WAN port, then the paired IP address will be registered in the Paired IP Table, and the later

connections between the paired IP will be made through the WAN port also.

- Age for IP-Pairs-Table Normal timeouts for the entries in Paired-IP-first Table. During the time, if an entry has never been used, the entry will be deleted from the Paired IP Table.
- Obliged age for Pairs-IP-Table The maximal timeouts for the entries in Paired-IP-first Table. During the time, the entry will be deleted from the Paired IP Table no matter whether the entry has been used.
- > On Existed-Application If a application has initiated two connections via a particular WAN port, then the connection will be registered in the Application Table, and the later connections related to the application will be made through the WAN port also.
  - Age for Application-Table- Normal timeouts for the entries in Application-first Table. During the time, if an entry has never been used, the entry will be deleted from the Application Table.
  - Obliged age for Application-Table- The maximal timeouts for the entries in Application-first Table. During the time, the entry will be deleted from the Application Table no matter whether the entry has been used.

#### P Note:

The time settings have passed corresponding tests, if you are not sure, please leave it default.

#### **WAN Port Parameter** 4.3.7

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

#### WAN Port Parameter WAN IndexPort Status Flow Control **Negotiation Mode** WAN1 Enabled Enabled Auto Negotiation WAN2 Enabled Enabled Auto Negotiation WAN3 Enabled Enabled Auto Negotiation WAN4 Enabled Enabled Auto Negotiation Port Status Link Speed(Mbps) **Duplex Mode** Flow Control WAN1 Not Connected WAN2 Not Connected WAN3 Not Connected WAN4 Not Connected Ingress Limit Mode Ingress Limit Speed Egress Limit Egress Limit Speed WAN1 No Limit Enable 128Kbps 128Kbps 💌 WAN2 No Limit 128Kbps 💌 Enable 128Kbps WAN3 No Limit 128Kbps 🔽 Enable 128Kbps WAN4 No Limit Enable 128Kbps 💌 128Kbps Refresh Save

Figure 4-16

- > WAN Index This shows the Router's WAN ports.
- **Port Status -** This shows the ports' current status: Enabled (default) or Disabled.
- Flow Control This shows the function of Flow Control is Enabled or Disabled.
- ➤ **Negotiation Mode -** The options are: Auto Negotiation, 10M Half Duplex, 10M Full Duplex, 100M Half Duplex, and 100M Full Duplex.
- Ingress Limit Mode & Ingress Limit Speed Select the limit mode and limit speed for the WAN ports.
- > Egress Limit & Egress Limit speed Enable Egress Limit for WAN ports and select the limit speed for them.

#### 

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

## 4.4 DHCP

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



Figure 4-17

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

#### 4.4.1 **DHCP Settings**

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

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

DHCP Settings		
DHCP Server:	ODisable OEnable	9
Start IP Address:	192.168.1.100	
End IP Address:	192.168.1.199	]
Address Lease Time:	120 minutes (1	~2880 minutes, the default value is 120)
Default Gateway:	192.168.1.1	(optional)
Default Domain:		(optional)
Primary DNS:	0.0.0.0	(optional)
Secondary DNS:	0.0.0.0	(optional)
	Save	

Figure 4-18

- > DHCP Server Enable or disable the DHCP server. If you disable the Server, you must have another DHCP server within your network or else you must manually configure the computer.
- > Start IP Address This field specifies the first address in the IP address pool. The default address is 192.168.1.100.
- > End IP Address This field specifies the end address in the IP address pool. The default address is 192.168.1.199.
- > Address Lease Time This is the amount of time in which a network user will be allowed connection to the router with their current dynamic IP address. Enter the amount of time (in minutes), the range of the time is 1 ~ 2880 minutes. The default value is 120 minutes.

- **Default Gateway –** IP address of the LAN port of the router. Suggest input a value, and the default is 192.168.1.1. (Optional).
- **Default Domain -** Input the domain name of your network. (Optional).
- Primary DNS Input the DNS IP address provided by your ISP. You can consult your ISP for it. (Optional)
- Secondary DNS Input the IP address of another DNS server if your ISP provides two DNS servers. (Optional)

#### Note:

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

#### 4.4.2 **DHCP Clients List**

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

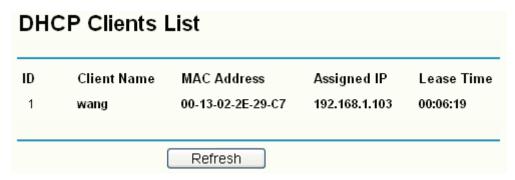


Figure 4-19

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

#### 4.4.3 **Address Reservation**

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

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



Figure 4-20

- MAC Address This field displays the MAC address of the PC for which you want to reserve IP address.
- **Reserved IP Address -** This field displays the IP address of the router reserved.
- > Status This field displays the status of the virtual server entry. Enabled means that the entry will take effect, Disabled means that the entry will not take effect.

## To add/modify a reserved IP address:

- **Step 1:** Click **Add New.../Modify** shown in Figure 4-20, you will see a new screen shown in Figure 4-21.
- **Step 2:** Enter the MAC address, IP address and select Status as shown below.

Add or Modify a Address Reservation Entry		
MAC Address:	00-0A-EB-00-07-8E	
Reserved IP Address:	192.168.1.100	
Status:	Enabled 🕶	
	Save Back	

Figure 4-21

Step 3: Click the Save button when finished.

#### Note:

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

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

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

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

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

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

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

#### **Forwarding** 4.5

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



Figure 4-22

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

#### 4.5.1 Virtual Servers

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

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



Figure 4-23

- Service Port This field displays the numbers of External Ports. It can be a service port or a range of service ports (the format is XXX - YYY, XXX is Start port, YYY is End port).
- **IP Address** This field displays the IP address of the PC running the service application.
- Protocol This field displays the protocol used for this application, either TCP, UDP, or All (all protocols supported by the router).

> Status - This field displays the status of the virtual server entry. Enabled means that the entry will take effect, **Disabled** means that the entry will not take effect.

## To add/modify a virtual server entry:

- Step 1: Click Add New.../Modify shown in Figure 4-20, you will see a new screen shown in Figure 4-24.
- Step 2: Select the service you want from the "Common Service Port", then the port and protocol value will be added to the corresponding field automatically, you only need to configure the IP address for the virtual server; If the "Common Service Port" does not contain the service that you want, please configure the Service Port, IP Address and Protocol manually.

Add or Modify a	Virtual Se	erver Entry
Service Port:	21	(XX-XX or XX)
IP Address:	192.168.1.99	
Protocol:	TCP	~
Status:	Enabled	~
Common Service Port:	FTP	
	Save	Back

Figure 4-24

- **Step 3:** After that, select **Enable** to make the entry take effect.
- **Step 4:** Click **Save** button to save the configuration.

# Note:

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

# Other configurations for the entries as shown in Figure 4-23:

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

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

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

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

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

#### Note:

If you set the virtual server of the service port as 80, you must set the web management port on

**System Tools -> Remote Management** screen to be any value except 80 such as 8080. Or else there will be a conflict to disable the virtual server.

## 4.5.2 Port Triggering

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

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

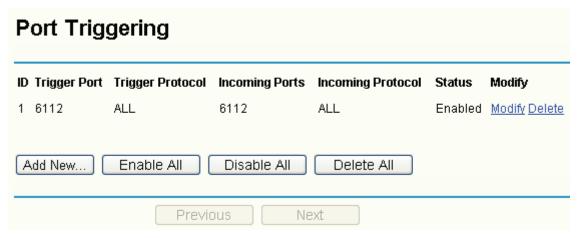


Figure 4-25

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

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

- **Step 1:** A local host makes an outgoing connection using a destination port number defined in the Trigger Port field.
- **Step 2:** The router records this connection, opens the incoming port or ports associated with this entry in the Port Triggering table, and associates them with the local host.

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

## To add/modify a port triggering entry:

- Step 1: Click Add New.../Modify shown in Figure 4-25, you will see a new screen shown in Figure 4-26.
- Step 2: Select the application you want from the "Common Applications", then the Trigger port and Incoming ports will be added to the corresponding field automatically, you only need to configure the Trigger protocol and Incoming Protocol for the entry; If the "Common Applications" does not contain the applications that you want, please configure these options manually.

Add or Modify a	Port Triggering Entry
Trigger Port:	6112
Trigger Protocol:	ALL 💌
Incoming Port:	6112
Incoming Protocol:	ALL 🕶
Status:	Enabled 🕶
Common Applications:	Battle.net
	Save Back

Figure 4-26

- **Step 3:** After that, select **Enabled** to make the entry take effect.
- **Step 4:** Click **Save** button to save the configuration.

#### Note:

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

## Other configurations for the entries as shown in Figure 4-25:

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

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

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

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

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

view the information in the next screen.

#### 4.5.3 DMZ

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

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



Figure 4-27

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

Step 1: Click the Enable radio button

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

Step 3: Click the Save button.

#### Note:

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

#### 4.5.4 UPnP

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

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



Figure 4-28

- ➤ Current UPnP Status If you want to use the Router's UPnP function, please click Enable button. If you don't want use the function, please click Disable button. Allowing the function may cause a risk to security, and this feature is disabled by default.
- App Description This displays the description provided by the application in the UPnP request.
- **External Port -** This displays the external port, which the router opened for the application.
- **Protocol** This displays the protocol for the application.
- > Internal Port This displays the internal port, which the router opened for local host.
- > **IP Address -** The UPnP device that is currently accessing the router.
- Status This displays the status. Enabled means that the port is still active, Disabled means that the port is inactive.

# 4.6 Security

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



Figure 4-29

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

## 4.6.1 Firewall

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

Filtering, MAC Address Filtering and Screen are disabled, and their settings are ineffective in the default settings.

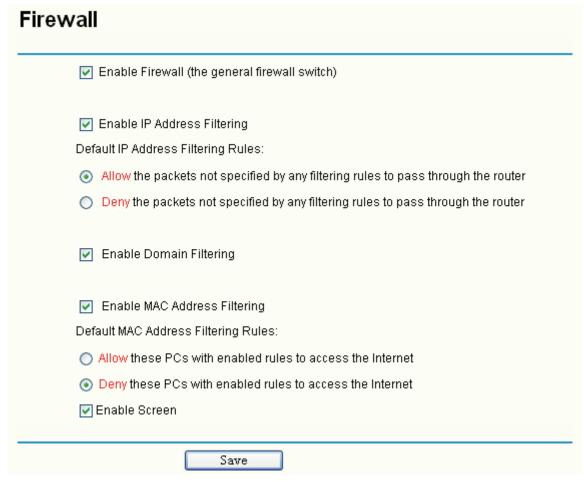


Figure 4-30

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

#### 4.6.2 IP Filtering

Choose menu "Security→IP Filtering", you can configure the IP Address filtering rule in the next screen (shown in Figure 4-31). The IP Address Filtering feature allows you to control Internet Access by specific users on your LAN based on their IP addresses.

#### IP Filtering Firewall Settings (You can change it on Firewall page) Enable Firewall: Enabled Enable IP Filtering: Enabled Default Filtering Rules: Allow the packets not specified by any filtering rules to pass through the router **LAN Port WAN IP** ID Effective time LAN IP WAN Port Protocol Action Status Modify 1 1800-2200 192.168.1.7 ALL Deny Enabled Modify Delete 2 0000-2400 192.168.1.8-192.168.1.12 -202.96.134.12 -ALL Deny Enabled Modify Delete No. Entry to No. Entry Move Add New. Enable All Disable All Delete All Previous Next

Figure 4-31

- Fifective Time This is the time or the range of time for the entry to take effect. For example, 1800 2200, it means that the entry will take effect from 18:00 to 22:00.
- LAN IP This is the LAN IP address or the range of LAN IP addresses in dotted-decimal notation format. For example, 192.168.1.20 192.168.1.30. Keep the field blank, which means all LAN IP addresses are controlled by the rule.
- ➤ LAN Port This is the LAN Port or the range of LAN ports in the field. For example, 1030 2000. Keep the field blank, which means all LAN ports are controlled by the rule.
- ➤ WAN IP This is the WAN IP address or the range of WAN IP addresses in dotted-decimal notation format. For example, 202.96.134.210 202.96.134.230. Keep the field blank, which means all WAN IP addresses are controlled by the rule.
- ➤ WAN Port This is the WAN Port or the range of WAN Ports. For example, 25 110. Keep the field blank, which means all WAN Ports are controlled by the rule.
- Protocol This indicates which protocol is used, TCP, UDP, or All (all protocols supported by the router).
- Action This field displays the action that the Router takes to deal with the traffic. Allow means that the Router allows the traffic through the Router, **Deny** means that the Router rejects the traffic through the router.
- > Status This field displays the status of the rule. Enabled means the rule will take effect,
  Disabled means the rule will not take effect.

## To add/modify an IP Address filtering entry:

**For example:** If you desire to block E-mail received and sent by the IP address 192.168.1.7 on your local network during the time of 1800 to 2200; And wish to make the PCs with IP addresses 192.168.1.8 to 192.168.1.12 unable to visit the website of IP address 202.96.134.12 all the day,

while other PCs have no limit. You can configure the rules as follows.

- Step 1: Enable the "Firewall" and "IP Address Filtering" on the Firewall screen (show in Figure 4-30), and then, you should select the Default IP Address Filtering Rule "Allow the packets not specified by any filtering rules to pass through the router".
- Step 2: Click Add New.../Modify shown in Figure 4-31, you will see a new screen shown in Figure 4-32.
- Step 3: Enter the "Effective time" that the rule will take effect as shown in Figure 4-32.
- Step 4: Enter the "LAN IP Address", "LAN Port", "WAN IP Address" and "WAN Port" in the corresponding field as shown in Figure 4-32.
- **Step 5:** Select the "Protocol", "Action" and "Status" for the rule as shown in the next screen.

Add or Modify an IP Filtering Entry		
Effective time:	1800 - 2200	
LAN IP Address:	192.168.1.7	
LAN Port:	-	
WAN IP Address:	-	
WAN Port:	25 -	
Protocol:	ALL	
Action:	Deny	
Status:	Enabled	
	Save Back	

Figure 4-32

- **Step 6:** Click the **Save** button to save this entry.
- Step 7: Go to Step 2 to complete the other rules continually.

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

ID Effective time	e LAN IP	LAN Por	t WAN IP	WAN Por	t Protoco	l Action	Status	Modify
1 1800-2200	192.168.1.7	-	-	25	ALL	Deny	Enabled	Modify Delete
2 0000-2400	192.168.1.8-192.168.1.12	2 -	202.96.134.1	2 -	ALL	Deny	Enabled	Modify Delete

Figure 4-33

#### Note:

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

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

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

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

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

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

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

#### 4.6.3 **Domain Filtering**

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

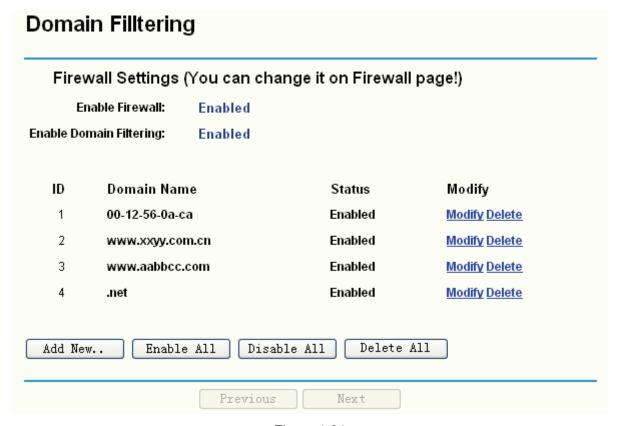


Figure 4-34

- **Effective Time -** This is the time or the range of time for the entry to take effect. For example, 0800 - 2400, it means that the entry will take effect from 08:00 to 20:00.
- > **Domain Name -** This is the domain or key word as desired. Leaving the field blank means all websites on the Internet are prohibited from accessing.
- Status This field displays the status. Enabled means the rule is effective, while Disabled means the rule is ineffective.

## To add or modify a Domain Filtering entry:

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

Step 1: Enable the "Firewall" and "Domain Filtering" on the Firewall screen (show in Figure

TL-R488T

4-30).

- **Step 2:** Click **Add New.../Modify** shown in Figure 4-34, you will see a new screen shown in Figure 4-35.
- **Step 3:** Enter the "Effective time" that the rule will take effect, enter the "Domain Name" as shown in Figure 4-35.
- **Step 4:** Select the "Status" for the rule as shown below.

Add or Modify an Domain Filtering Entry		
Effective time	0000 - 2400	
Domain Name:	www.xxyy.com.cn	
Status:	Enabled 💌	
	Save Back	

Figure 4-35

**Step 5:** Finally, click **Save** to make the rule take effect.

**Step 6:** Go to **Step 2** to complete the other rules continually.

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

ID	Domain Name	Status	Modify
1	www.xxyy.com.cn	Enabled	<u>Modify</u> <u>Delete</u>
2	www.aabbcc.com	Enabled	Modify Delete
3	.net	Enabled	Modify Delete

Figure 4-36

## Note:

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

## Other configurations for the entries as shown in Figure 4-34:

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

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

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

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

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

# 4.6.4 MAC Filtering

Choose menu "Security→MAC Filtering", you can configure the MAC Address filtering rule in the next screen (shown in Figure 4-37). The MAC Address Filtering feature allows you to control

access to the Internet by users on your local network based on their MAC addresses.



Figure 4-37

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

## To add or modify a Domain Filtering entry:

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

- Step 1: Enable the "Firewall" and "MAC Address Filtering" on the Firewall screen (show in Figure 4-30). And then specify the Default MAC Address Filtering Rule "Deny these PCs with enabled rules to access the Internet".
- Step 2: Click Add New.../Modify shown in Figure 4-37, you will see a new screen shown in Figure 4-38.
- Step 3: Enter the appropriate MAC address and descriptions, and then select the status as shown in Figure 4-38.

# Add or Modify a MAC Address Filtering Entry MAC Address: 00-0A-EB-00-07-BE Description: John's computer Status: Enable( > Back

Figure 4-38

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

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

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

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

Figure 4-39

## Note:

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

## Other configurations for the entries as shown in Figure 4-37:

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

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

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

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

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

## 4.6.5 Screen

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

Screen			
Region: WAN			
Scan Attack Defence:			
□ IP Scan	threshold:	5000	microsecond
Port Scan	threshold:	5000	microsecond
☐ IP Deceive			
DoS Attack Defence:			
☐ ICMP Flood	threshold:	1000	PPS
UDP Flood	threshold:	1000	PPS
SYN Flood	threshold:	200	PPS
Land Attack			
WinNuke			
Dubious Packet Defen			
Large ICMP packet(larger than 1024 Bytes)			
TCP packet without Flag			
TCP packet with both SYN and FIN			
TCP packet with FIN but without ACK			
Unknown Protocol			
Packet Defence with IF	option:		
□ IP Timestamp Opt	ion		
☐ IP Security Option			
☐ IP Stream Option			
☐ IP Record Route Option			
□ IP Loose Source Route Option			
☐ IP Strict Source Route Option			
Invalid IP option			
	Save	$\overline{}$	

Figure 4-40

Region - This option used to select the specifically area from which the packets will be monitored by the next settings.

# > Scan Attack Defence

IP Scan: During the specific time, if a computer (identified by a particular source IP address) transmits packets to at least ten different computers (identified by different destination IP addresses), and then the source IP address will be deemed to make IP

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

#### **DoS Attack Defence**

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

#### **Dubious Packet Defence**

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

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

## **Packet Defence with IP option**

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

#### 4.7 Static Routing

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

#### Static Routing ID Destination IP Address Subnet Mask **Default Gateway** Status Modify 1 10.20.1.100 255.255.255.0 10.20.1.1 Enabled Modify Delete Enable All Add New. Disable All Delete All Previous Next

Figure 4-41

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

# To add/modify a static routing entry:

- **Step 1:** Click **Add New.../Modify** shown in Figure 4-41, you will see a new screen shown in Figure 4-42.
- **Step 2:** Enter the appropriate Destination IP Address, Subnet Mask and Default Gateway, and then select the status.

Add or Modify a S	tatic Route Entry
Destination IP Address:	10.20.1.100
Subnet Mask:	255.255.255.0
Default Gateway:	10.20.1.1
Status:	Enabled
	Save Back

Figure 4-42

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

#### Note:

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

## Other configurations for the entries as shown in Figure 4-41:

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

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

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

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

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

## 4.8 Session Limit

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



Figure 4-43

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

## 4.8.1 Session Limit

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

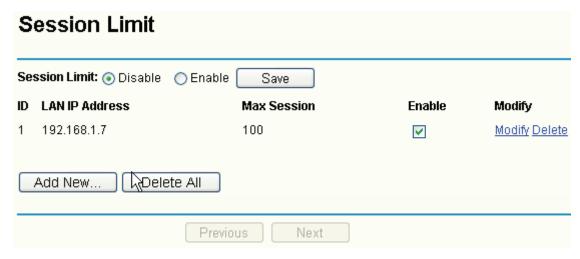


Figure 4-44

- ➤ **Enable**: Enable or disable the session limit. Only after choose "Enable", the configuration will take effect.
- LAN IP address: The controlled computer's IP address. You can input a range of IP address, for example: 192.168.1.20 -192.168.1.30. You can also input an IP address, such as: 192.168.1.40.
- Max Session: The max connections of the computer.

## To add/modify a session limit entry:

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

Figure 4-45.

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

Add or Modify a Session Limit Entry			
Enable:	☑		
LAN IP Address:	192.168.1.7 -		
Max Session:	100		
	Save Back		

Figure 4-45

Step 3: Click the Save button.

## 4.8.2 Session List

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



Figure 4-46

#### ■ Note:

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

# 4.9 QoS

Choose menu "QoS", and you can see the submenus under the main menu.



Figure 4-47

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

# 4.9.1 QoS Settings

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

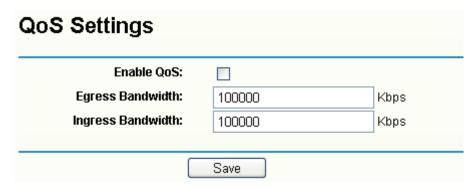


Figure 4-48

## 4.9.2 QoS Rules List

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

#### **QoS Rules List** Egress Bandwidth(Kbps) Ingress Bandwidth(Kbps) ID Description Mode Enable Modify Min Max Max Min 1 | 192.168.1.100 - 192.168.1.110/21 | Share 400 1000 2000 4000 Modify Delete Add New. Delete All. Next Now is the 1 v page

Figure 4-49

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

## To add/modify a QoS rule:

- **Step 1:** Click **Add New.../Modify** shown in Figure 4-49, you will see a new screen shown in Figure 4-50.
- **Step 2:** Enter the information like the screen as shown below.

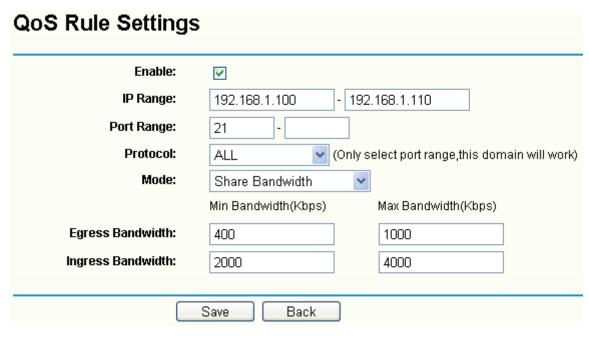


Figure 4-50

Step 3: Click the Save button.

# 4.10 IP & MAC Binding

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



Figure 4-51

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

# 4.10.1 Binding Setting

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



Figure 4-52

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

## To add/modify an IP & MAC binding entry:

- **Step 1:** Click **Add New.../Modify** shown in Figure 4-52, you will see a new screen shown in Figure 4-53.
- **Step 2:** Enter the MAC Address and IP Address in the corresponding field.

IP & MAC Binding Settings		
Bind:	✓	
MAC Address:	00-13-8F-A9-6C-CA	
IP Address:	192.168.1.100	
	Save Back	

Figure 4-53

**Step 3:** Select **Bind** the MAC and IP address, and then click **Save** button to save the configuration.

## To find a specific IP & MAC binding entry:

- Step 1: Click Find shown in Figure 4-52, you will see a new screen shown in Figure 4-54.
- Step 2: Enter the specific MAC Address or IP Address in the corresponding field.

## Find IP & MAC Binding Entry MAC Address: 00-13-8F-A9-6C-CA IP Address: ID MAC Address IP Address Bind Link 00-13-8F-A9-6C-CA 192.168.1.100 1 V to page Find Return

Figure 4-54

- Step 3: Click Find button, then you will see the entry with the specific MAC address or IP address.
- Step 4: Click Return to return the previous screen.

## Note:

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

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

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

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

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

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

#### 4.10.2 **ARP List**

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

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

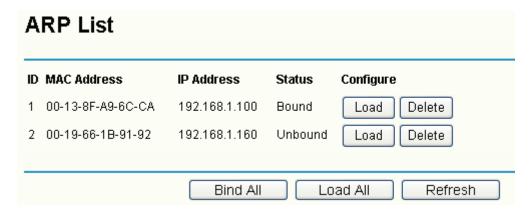


Figure 4-55

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

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

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

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

#### Note:

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

# 4.11 Dynamic DNS

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

The router offers a Dynamic Domain Name System (DDNS) feature. DDNS lets you assign a fixed host and domain name to a dynamic Internet IP address. It is useful when you are hosting your own website, FTP server, or other server behind the router. Before using this feature, you need to sign up for DDNS service providers such as <a href="www.dyndns.org">www.oray.net</a> or <a href="www.comexe.cn">www.comexe.cn</a>. The Dynamic DNS client service provider will give you a password or key.

#### 4.11.1 **Dyndns DDNS**

If your dynamic DNS Service Provider is <a href="https://www.dyndns.org">www.dyndns.org</a>, you can configure in the next screen (shown in Figure 4-56).

DDNS	
Service Provider:	Dyndns ( www.dyndns.org ) 💌 Go to register
WAN Port:	WAN1
User Name: Password:	username
Domain Name:	
Connection Status:	☐ Enable DDNS  DDNS not launching!  Login Logout
	Save

Figure 4-56

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

## To set up for Dyndns DDNS, follow these instructions:

- **Step 1:** Select the WAN port to configure.
- Step 2: Type the "User Name" and "Password" for your DDNS account.
- **Step 3:** Enter the domain name that your dynamic DNS service provider offers.
- **Step 4:** Enable DDNS, and click **Save** to save the current configuration.

Click Login to login the DDNS service.

Click Logout to logout the DDNS service.

#### 4.11.2 PeanutHull DDNS

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

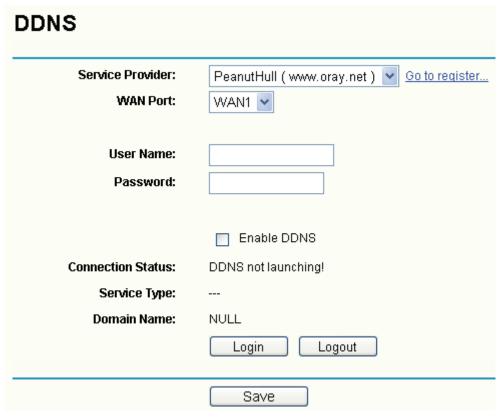


Figure 4-57

## To set up for PeanutHull DDNS, follow these instructions:

- Step 1: Select the WAN port to configure.
- **Step 2:** Type the User Name and Password for your DDNS account.
- **Step 3:** Enter the domain name that your dynamic DNS service provider offers.
- **Step 4:** Enable DDNS, and click **Save** to save the current configuration.

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

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

## 4.11.3 Comexe DDNS

If the dynamic DNS Service Provider is <a href="www.comexe.cn">www.comexe.cn</a>, you can configure in the next screen (shown in Figure 4-58).

DDNS	
Service Provider:	Comexe ( www.comexe.cn ) 💌 Go to register
WAN Port:	WAN1 💌
Domain Name:	
User Name:	
Password:	
	Enable DDNS
Connection Status:	DDNS not launching!
	Login Logout
	Save

Figure 4-58

## To set up for Comexe DDNS, follow these instructions:

- Step 1: Select the WAN port to configure.
- **Step 2:** Enter the domain name your dynamic DNS service provider offer.
- Step 3: Type the "User Name" and "Password" for your DDNS account.
- **Step 4:** Enable DDNS, and click **Save** to save the current configuration.

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

Click Logout to logout the DDNS service.

# 4.12 Switch Setting

Choose menu "Switch Setting", and you can see the submenus under the main menu:

Switch Setting
 Port Statistics
 Port Rate Control
 Port Parameter
 Port Status

Figure 4-59

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

## 4.12.1 Port Statistics

Choose menu "Switch Setting→Port statistics", you can view the statistics information about the LAN port in the next screen (shown in Figure 4-60).

Current Port: Port1		Refresh Clean	
Rx Unicasts:	966	Tx Unicasts:	1114
Rx Broadcasts:	178	Tx Broadcasts:	1
Rx Multicasts:	0	Tx Multicasts:	1330
Rx Bytes:	144663	Tx Bytes:	1206036
Rx Pauses:	0	Tx Pauses:	0
Rx CRC Errors:	0	Rx Collisions:	0
Rx 64 B:	820	Rx 65to127 B:	170
Rx 128to255 B:	6	Rx 256to511 B:	16
Rx 512to1023 B:	132	Rx 1024toMax:	0
Rx Undersizes:	0	Rx Fragments:	0
Rx Oversizes:	0	Rx Jabbers:	0

Figure 4-60

# P Note:

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

## 4.12.2 Port Rate Control

Choose menu "Switch Setting→Port Rate Control", you can control the ingress and egress rate for the LAN port in the next screen (shown in Figure 4-61).



Figure 4-61

## 4.12.3 Port Parameter

Choose menu "Switch Setting→Port Parameter", you can configure the parameters for the LAN port in the next screen (shown in Figure 4-62).



Figure 4-62

## 4.12.4 Port Status

Choose menu "**Switch Setting**→**Port Status**", you can view the status of the LAN port in the next screen (shown in Figure 4-63).

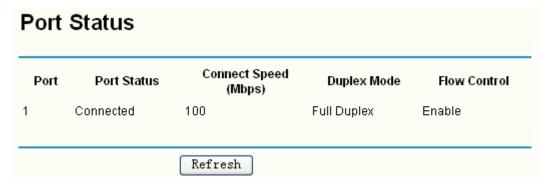


Figure 4-63

# 4.13 System Tools

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



Figure 4-64

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

# 4.13.1 Time Setting

Choose menu "**System Tools→Time**", you can configure the time on the screen (shown in Figure 4-65).

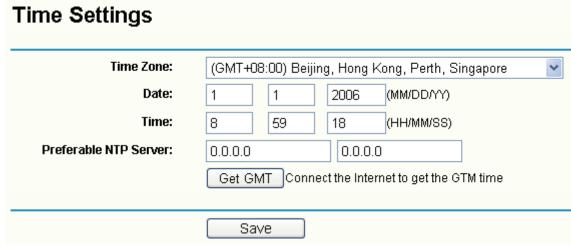


Figure 4-65

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

#### **TL-R488T**

# To configure the system time manually:

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

#### To configure the system automatically:

- **Step 1:** Select your local time zone.
- **Step 2:** Enter the IP address for Preferable NTP Server, then the Router will get the time from the Preferable NTP Server firstly (you can leave it blank also).
- **Step 3:** Click the **Get GMT** button to get system time from Internet if you have connected to the Internet.

#### Note:

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

#### 4.13.2 Firmware

Choose menu "System Tools→Firmware", you can update the latest version of firmware for the Router on the screen (shown in Figure 4-66).

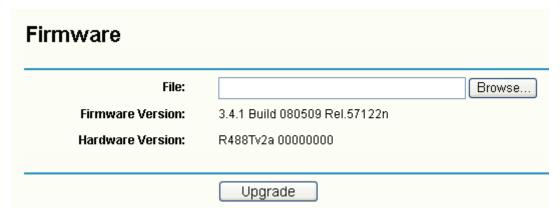


Figure 4-66

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

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

- **Step 1:** Download a more recent firmware upgrade file from the TP-LINK website (www.tp-link.com).
- Step 2: Type the path and file name of the update file into the "File" field. Or click the Browse

button to locate the update file.

# Step 3: Click the Upgrade button.

#### Note:

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

# 4.13.3 Factory Defaults

Choose menu "System Tools→Factory Defaults", you can restore the configurations of the Router to factory defaults on the screen (shown in Figure 4-67).



Figure 4-67

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

# Note:

- 1) The default **User Name** is admin.
- 2) The default **Password** is admin.
- 3) The default **IP Address** is 192.168.1.1.
- 4) The default **Subnet Mask** is 255.255.255.0.

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

# 4.13.4 Backup and Restore

Choose menu "System Tools→Backup and Restore Config", you can save the current configuration of the Router as a backup file and restore the configuration via a backup file (shown in Figure 4-68).



Figure 4-68

# To back up the Router's current settings:

**Step 1:** Click the **Backup** button (shown in Figure 4-68), click **Save** button in the next screen (shown in Figure 4-69) to proceed.



Figure 4-69

**Step 2:** Save the file as the appointed file (shown in Figure 4-70).

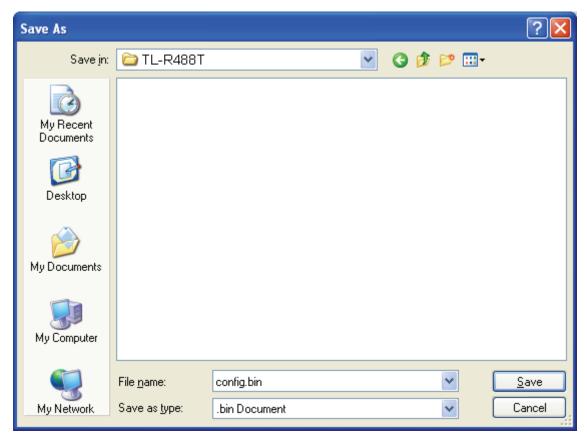


Figure 4-70

# To restore the Router's settings:

- **Step 1:** Click the **Browse** button to locate the update file for the device, or enter the exact path to the Setting file in the text box.
- Step 2: Click the Upgrade button to complete.

### 4.13.5 Reboot

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

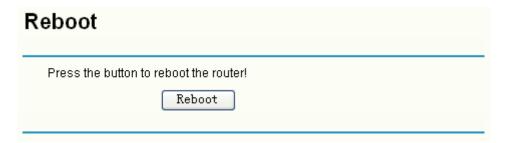


Figure 4-71

# Note:

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

- 1) Change LAN IP Address. (System will reboot automatically)
- 2) MAC Clone (system will reboot automatically)
- 3) DHCP service function.

- TL-R488T
- 4) Static address assignment of DHCP server.
- 5) Web Service Port of the router.
- 6) Upgrade the firmware of the router (system will reboot automatically).
- 7) Restore the router's settings to factory default (system will reboot automatically).

#### 4.13.6 Password

Choose menu "System Tools→Password", you can change the factory default user name and password of the router in the next screen (shown in Figure 4-72). After configuration, click the Save button.



Figure 4-72

# Note:

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

# 4.13.7 Log

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

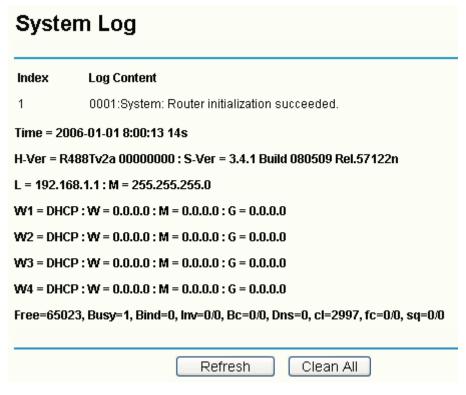


Figure 4-73

The router can keep logs of all traffic. You can query the logs to find what happened to the router. Click the **Refresh** button to refresh the logs.

Click the Clear All button to clear all the logs.

# 4.13.8 Remote Management

Choose menu "System Tools → Remote Management", you can configure the Remote Management function on this screen (shown in Figure 4-74). This feature allows you to manage your Router from a remote location via the Internet.

Remote Management	
Web Management Port: Remote Management IP Address:	0.0.0.0
	Save

Figure 4-74

➤ Web Management Port - Web browser access normally uses the standard HTTP service port 80. This router's default remote management web port number is 80. For greater security, you can change the remote management web interface to a custom port by entering that number in the box provided. Choose a number between 1024 and 65534, but do not use the number of any common service port.

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

#### Note:

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

#### 4.13.9 Statistics

Choose menu "**System Tools→Statistics**", you can view the statistics of the Router. This screen (shown in Figure 4-75) displays the network traffic of each PC on LAN, including total traffic and current traffic of the last "Packets Statistic interval" seconds.

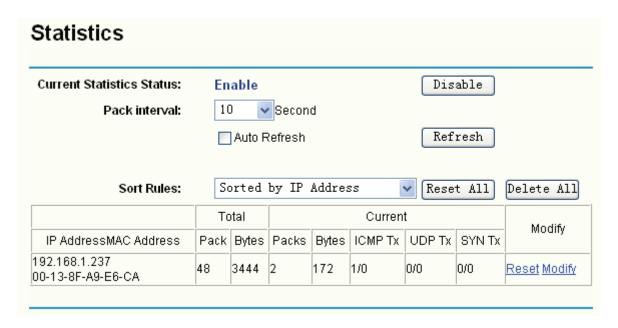


Figure 4-75

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

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

IP Address		The IP address whose statistics information are displayed	
MAC Address		The in dual coe whose stationed information are displayed	
Total	Pack	The total amount of packets received and transmitted by the router	
Total Bytes		The total amount of bytes received and transmitted by the router	
Daala		The total amount of packets received and transmitted in the last "Packets	
	Packs	Statistic interval" seconds	
Durton	The total amount of bytes received and transmitted in the last "Packets		
	Bytes	Statistic interval" seconds	
Current	Command ICMD To	The total amount of the ICMP packets transmitted to WAN in the last	
Current	ICMP Tx	"Packets Statistic interval" seconds	
	LIDD To	The total amount of the UDP packets transmitted to WAN in the last	
db	UDP Tx	"Packets Statistic interval" seconds	
	SYN Tx	The total amount of the TCP SYN packets transmitted to WAN in the last	
	SINIX	"Packets Statistic interval" seconds	

#### Note:

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

Click the Auto-refresh checkbox to refresh automatically.

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

Click the Reset All button to recount again.

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

# 4.13.10 WAN Speed Detect

Choose menu "System Tools→WAN Speed Detect", you can detect the wan speed of the router in the screen below. There are three detecting ways: ICMP DETECT, TCP DETECT, UDP DE-TECT. The detect way is the router sends datagram to destination ip address, and then counts the interval between sending the datagram and receiving the response.

# **WAN Speed Detect**

Detected WAN Port:	WAN1 🕶	
	ICMP DETECT	
	Destination IP:	
	ID:	0
	Detect Result:	
	TCP DETECT	
	Destination IP:	
	Destination Port:	0
	Source Port:	0
	Detect Result:	
	UDP DETECT	
	Destination IP:	
	Destination Port:	0
	Source Port:	0
	UDP Data:	^
	Detect Result:	
	Notice: In the UDP datagram if not, as a whole UDP datag	n, if there is ".", the datagram will be consider as a domain, gram to send away.

Figure 4-76

- **Destination IP** the IP address which datagrams are sent to, such as- 202.96.134.188.
- > **ID** The number of ICMP datagrames to be sent.
- > **Source Port** The port where datagrams are sent to, such as- 5000.
- > **Destination Port** The datagrams' distination port, such as-6000.
- UDP Data The data carried when sent UDP detect datagram, take care if in the UDP data exist character ".", for example, 123.456, www.sohu.com, the datagram would be considered to be a domain name, DNS datagram will be sent, at this time, no matter what the destination port is, the destination port in the sent datagram is always 53. If not, it will be sent as a whole

UDP datagram.

> Detect Result - The interval between sending datagram and recving datagram, uint is ms.

# 4.13.11 IP NAT Table

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

# IP NAT Table

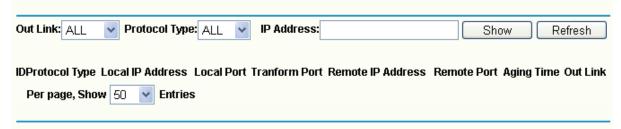


Figure 4-77

- > Out Link The WAN port which links the router.
- > **Protocol Type** The protocol which is used in the link.
- > IP address The local or remote IP address to be examined.
- Show To examine the information which the local or remote IP address equals that you input.
- > Refresh To get the latest status and settings of the router
- Per page To set how many information entries a page show.

# 4.13.12 NAT Source Port Settings

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

NAT Source Port Settings		
NAT Exterior Port:	1040 - 65500	
	Save Restore	

Figure 4-78

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

# Appendix A: Specifications

General		
Standards and Protocols	IEEE 802.3, 802.3u	
	TCP/IP, PPPoE, DHCP, ICMP, NAT, SNTP	
Safety & Emission	FCC、CE	
Ports	Four 10/100M Auto-Negotiation WAN RJ45 port.	
	One 10/100M Auto-Negotiation LAN RJ45 ports (Auto MDI/MDIX)	
	One Console (RS232 DB9 Male)	
	10BASE-T: UTP category 3, 4, 5 cable (maximum 100m)	
Cabling Type	EIA/TIA-568 100Ω STP (maximum 100m)	
Cabling Type	100BASE-TX: UTP category 5, 5e cable (maximum 100m)	
	EIA/TIA-568 100Ω STP (maximum 100m)	
Power Supply	Input: 220VAC 50HZ	
1 ower cuppry	Consumption: 4.1W (Max)	
Physical and Environment		
Working Temperature	0℃~40℃ (32℉~104℉)	
Working Humidity	10% - 90% RH, Non-condensing	

# **Appendix B: FAQ**

- 1. How do I configure the router to access Internet by ADSL users?
- Step 1: First, configure the ADSL modem in RFC1483 bridge model.
- **Step 2:** Connect the Ethernet cable from your ADSL modem to the WAN port on the router. The telephone cord plugs into the Line port of the ADSL modem.
- Step 3: Login to the router, click the menu **Network→WAN** on the left of your browser. On the WAN screen, select "PPPoE" for the type of WAN connection. Then enter the user name and password in the corresponding field, and finish it by clicking **Connect**.

WAN Connection Type:	PPPoE 💌
User Name:	username
Password:	•••••

Figure B-1

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

Wan Connection Mode:	<ul><li>Connect on Demand</li></ul>	
	Max Idle Time: 15 minutes (0 means remain active at all times.)	
	Connect Automatically	
	Time-based Connecting	
	Period of Time:from 0 : 0 (HH:MM) to 23 : 59 (HH:MM)	
	Connect Manually	
	Max Idle Time: 15 minutes (0 means remain active at all times.)	
	Connect Disconnect	
	Save Advanced	

Figure B-2

#### Note:

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

- Step 1: Login to the router, click the menu Network→WAN on the left of your browser, On the WAN screen, select "Dynamic IP" for "WAN Connection Type", and finish it by clicking Save.
- Step 2: Some ISPs require that you register the MAC address of your adapter, which is connected to your cable or DSL modem during installation. If your ISP requires MAC register, login to the router and click the menu Network→MAC Clone. On the MAC Clone screen, if your PC's MAC address is a proper MAC address, click the "Clone MAC Address" button and your PC's MAC address will be filled in the "WAN MAC Address" field; Or else, enter the specific MAC address into the "WAN MAC Address" field manually. Then click the Save button. It will take effect after rebooting.

MAC Clone		
WAN1 MAC Address:	00-0A-EB-12-34-1A	Restore Factory MAC
WAN2 MAC Address:	00-0A-EB-12-34-1B	Restore Factory MAC
WAN3 MAC Address:	00-0A-EB-12-34-1C	Restore Factory MAC
WAN4 MAC Address:	00-0A-EB-12-34-1D	Restore Factory MAC
Your PC's MAC Address:	00-19-66-1B-91-92	Clone MAC Address To WAN1 💌
Save		

Figure B-3

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

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

If you start as a responsor, you need configure Virtual Server or DMZ Host as follows:

#### **Method one: Use Virtual Server**

Login to the router, click the menu **Forwarding→Virtual Servers**. On the Virtual Server screen, add a Virtual Server rule as shown in the next screen: configure 1720 as the "Service Port" and enter your IP address (assuming 192.168.1.102 for an example), then click select the status **Enabled** and click **Save**.

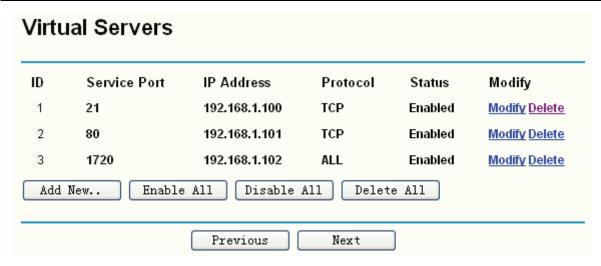


Figure B-4

# Note:

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

#### **Method two: Use DMZ Host**

Login to the router, click the menu **Forwarding→DMZ**. On the DMZ screen, select "Enable", and enter your IP address into the "DMZ Host IP Address" field (using 192.168.1.102 as an example), then to click the **Save** button.



Figure B-5

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

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

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

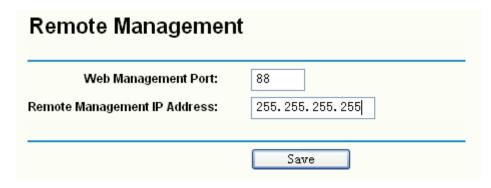


Figure B-6

# Note:

If the above configuration takes effect, you should login the Router by typing in <a href="http://192.168.1.1:88">http://192.168.1.1:88</a> (the router's LAN IP address: Web Management Port) in the address field of the web browser.



Step 2: To add a WEB Server: Login to the router, click the menu Forwarding→Virtual Servers on the left of your browser. On the Virtual Server screen, add a Virtual Server rule as shown below. Configure "80" as the "Service Port", and enter your IP address (assuming 192.168.1.188 for an example), remember to "Enable" and "Save".

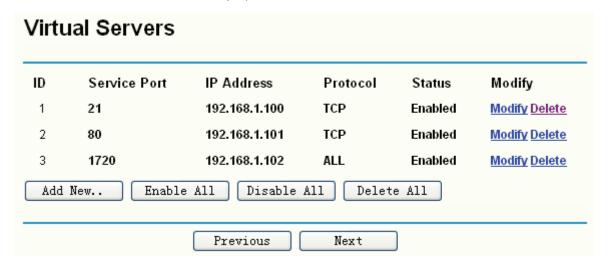


Figure B-7

# **Appendix C: Glossary**

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