

# TP-LINK®

## User Guide

### TL-R600VPN

### SafeStream Gigabit Broadband VPN Router



## COPYRIGHT & TRADEMARKS

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

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 © 2013 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 A digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

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

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

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

## CE Mark Warning



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



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



## Safety Information

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

## 安全諮詢及注意事項

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

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

This product can be used in the following countries:

AT	BG	BY	CA	CZ	DE	DK	EE
ES	FI	FR	GB	GR	HU	IE	IT
LT	LV	MT	NL	NO	PL	PT	RO
RU	SE	SK	TR	UA			

## Package Contents

The following items should be found in your box:

- One TL-R600VPN SafeStream Gigabit Broadband VPN Router
- One Power Cord
- Resource CD

### **Note:**

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

## Conventions

The router or TL-R600VPN mentioned in this guide stands for TL-R600VPN SafeStream Gigabit Broadband VPN Router without any explanation.

# CONTENTS

<b>Chapter 1. Introduction .....</b>	<b>1</b>
1.1 Overview of the Router .....	1
1.2 Features.....	1
1.3 Conventions.....	1
<b>Chapter 2. Hardware Installation .....</b>	<b>2</b>
2.1 Panel Layout.....	2
2.1.1 The Front Panel.....	2
2.1.2 The Rear Panel .....	2
2.2 System Requirements .....	3
2.3 Installation Environment Requirements .....	3
2.4 Connect to Ground .....	3
2.5 Connecting the Router.....	4
<b>Chapter 3. Quick Installation Guide .....</b>	<b>5</b>
3.1 Configure PC .....	5
3.2 Login .....	8
<b>Chapter 4. Configuring the Router .....</b>	<b>12</b>
4.1 Status.....	12
4.2 Quick Setup .....	14
4.3 Network.....	14
4.3.1 WAN .....	14
4.3.2 LAN.....	23
4.3.3 MAC Clone .....	24
4.4 DHCP.....	25
4.4.1 DHCP Settings .....	25
4.4.2 DHCP Clients List.....	26
4.4.3 Address Reservation .....	26
4.5 Forwarding.....	28
4.5.1 Virtual Servers .....	28
4.5.2 Port Triggering.....	30
4.5.3 DMZ.....	31
4.5.4 UPnP .....	32
4.6 Security.....	33
4.6.1 Basic Security.....	33
4.6.2 Advanced Security .....	34
4.6.3 Local Management.....	35
4.7 Access Control.....	36
4.7.1 Rule .....	36
4.7.2 Host .....	38

4.7.3	Target .....	39
4.7.4	Schedule .....	40
4.8	IPsec VPN .....	41
4.8.1	IKE.....	41
4.8.2	IPsec.....	43
4.8.3	SA List .....	46
4.9	PPTP VPN Server .....	47
4.9.1	Server Settings.....	47
4.9.2	Account Settings .....	47
4.9.3	Connection Status.....	48
4.10	Advanced Routing .....	49
4.10.1	Static Routing .....	49
4.10.2	System Routing Table.....	50
4.11	Bandwidth Control .....	51
4.11.1	Control Settings.....	51
4.11.2	Rule List.....	51
4.12	IP & MAC Binding .....	53
4.12.1	Binding Setting .....	53
4.12.2	ARP List.....	55
4.13	Dynamic DNS .....	55
4.13.1	Dyndns DDNS .....	55
4.13.2	PeanutHull DDNS.....	56
4.13.3	Comexe DDNS.....	57
4.13.4	No-IP DDNS .....	57
4.14	System Tools .....	58
4.14.1	Time Settings .....	58
4.14.2	Diagnostic Tools.....	60
4.14.3	Firmware.....	61
4.14.4	Factory Defaults .....	61
4.14.5	Backup and Restore.....	62
4.14.6	Reboot.....	63
4.14.7	Password.....	64
4.14.8	System Log .....	64
4.14.9	Remote Management.....	65
4.14.10	Statistics .....	66
	<b>Appendix A: Specifications .....</b>	<b>68</b>
	<b>Appendix B: Preventing Lightning .....</b>	<b>69</b>
	<b>Appendix C: FAQ.....</b>	<b>70</b>
	<b>Appendix D: Glossary.....</b>	<b>74</b>

# Chapter 1. Introduction

## 1.1 Overview of the Router

The TL-R600VPN SafeStream Gigabit Broadband VPN Router from TP-LINK provides multiple VPN protocols and high VPN performance. Abundant security strategies, such as SPI firewall, protect your network against the attacks and Access Control, provide online behavior management. Anymore, web-based management makes the network setup be an easy work. It's really a cost-effective and reliable VPN solution for chain stores and branch offices.

## 1.2 Features

- Complies with IEEE 802.3, 802.3u , 802.3x standards
- Supports Bandwidth Control
- Built-in NAT and DHCP server supporting static IP address distributing
- Supports Virtual Server, Port Triggering, and DMZ host
- Built-in firewall supporting IP address filtering, Domain Name filtering, and MAC address filtering
- Supports connecting/disconnecting Internet at a specified time of day
- Supports access control, allowing parents and network administrators to establish restricted access policies based on the time of day for children or staff
- Supports TCP/IP, PPPoE, DHCP, ICMP, NAT, SNTP
- Supports UPnP, Dynamic DNS, Static Routing, VPN pass-through
- Supports Traffic Statistics
- Supports IP & MAC Binding
- 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
- Supports IPsec VPN and PPTP Server

## 1.3 Conventions

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

You can set the parameters according to your demand.

## Chapter 2. Hardware Installation

### 2.1 Panel Layout

#### 2.1.1 The Front Panel

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

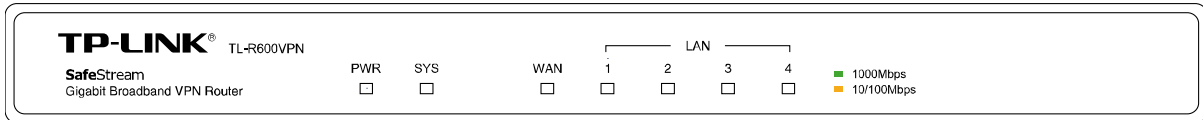


Figure 2-1

#### LED Descriptions:

Name	Status	Indication
PWR	Not lit	The router is powered off.
	Lit up (Green)	The router is powered on.
SYS	Not lit	The router has a hardware error.
	Lit up (Green)	The router has a hardware error.
	Flashing (Green)	The router works properly.
WAN, LAN	Not lit	There is no device linked to the corresponding port.
	Lit up (Green/Yellow)	There is a device linked to the corresponding port but no activity. (Green light indicates the linked device is running at 1000Mbps, and yellow indicates the linked device is running at 10/100Mbps.)
	Flashing (Green/Yellow)	The corresponding port is transmitting or receiving data. (Green light indicates the linked device is running at 1000Mbps, and yellow indicates the linked device is running at 10/100Mbps.)

#### 2.1.2 The Rear Panel

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

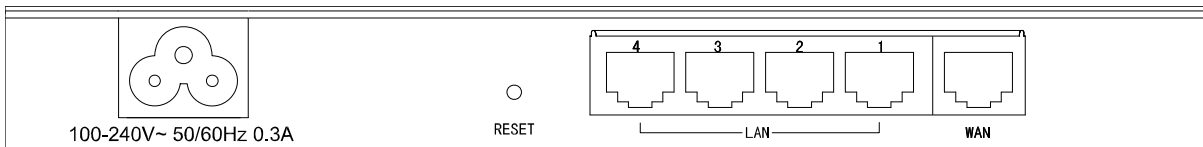


Figure 2-2

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

There are two ways to reset the router:



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

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

 **Note:**

- 1) Please use only the power cord provided with this router.
  - 2) Ensure the router is powered on before it restarts completely.
- **LAN:** Four RJ45 ports for connecting the router to the local PCs.
  - **WAN:** One RJ45 port for connecting the router to a cable DSL modem or Ethernet.

## 2.2 System Requirements

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

## 2.3 Installation Environment Requirements

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

 **Note:**

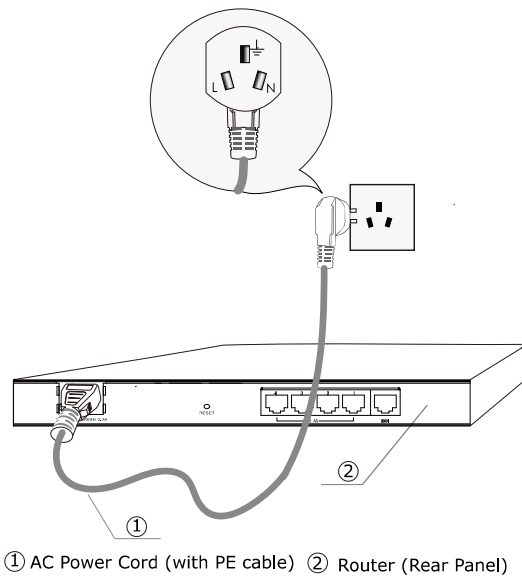
- 1) Do not use this product near water, for example, in a wet basement or near a swimming pool.
- 2) Avoid using this product during an electrical storm. There may be a remote risk of electric shock from lightning.

## 2.4 Connect to Ground

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

### Connecting to the Ground via the power supply

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



### Note:

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

## 2.5 Connecting the Router

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

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

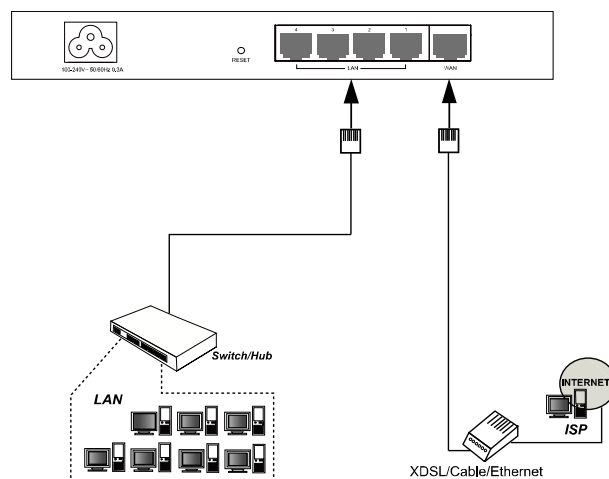


Figure 2-3

## Chapter 3. Quick Installation Guide

This chapter describes how to configure the basic functions of your TL-R600VPN SafeStream Gigabit Broadband VPN Router. These procedures only take you a few minutes. You can access the Internet via the router immediately after it has been successfully configured.

### 3.1 Configure PC

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



Figure 3-1

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

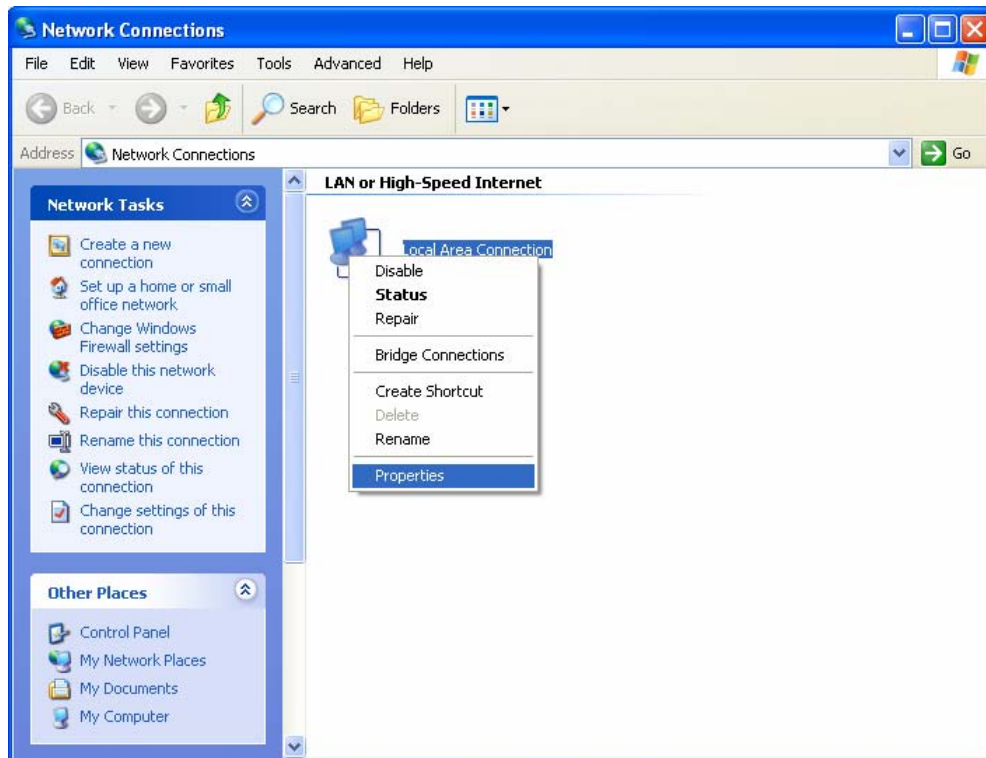


Figure 3-2

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

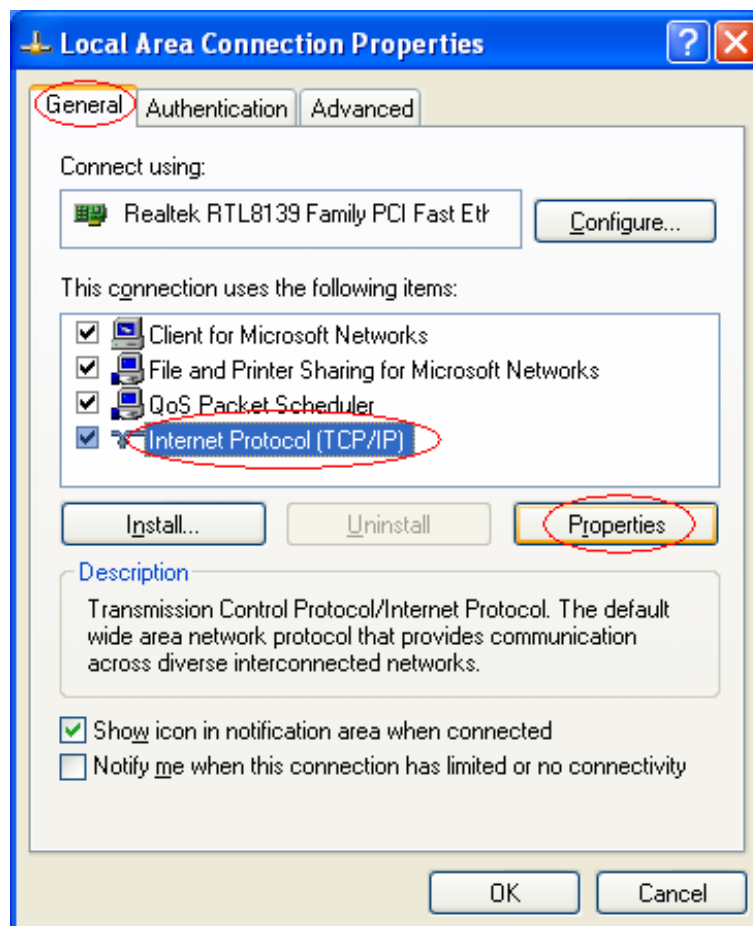


Figure 3-3

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

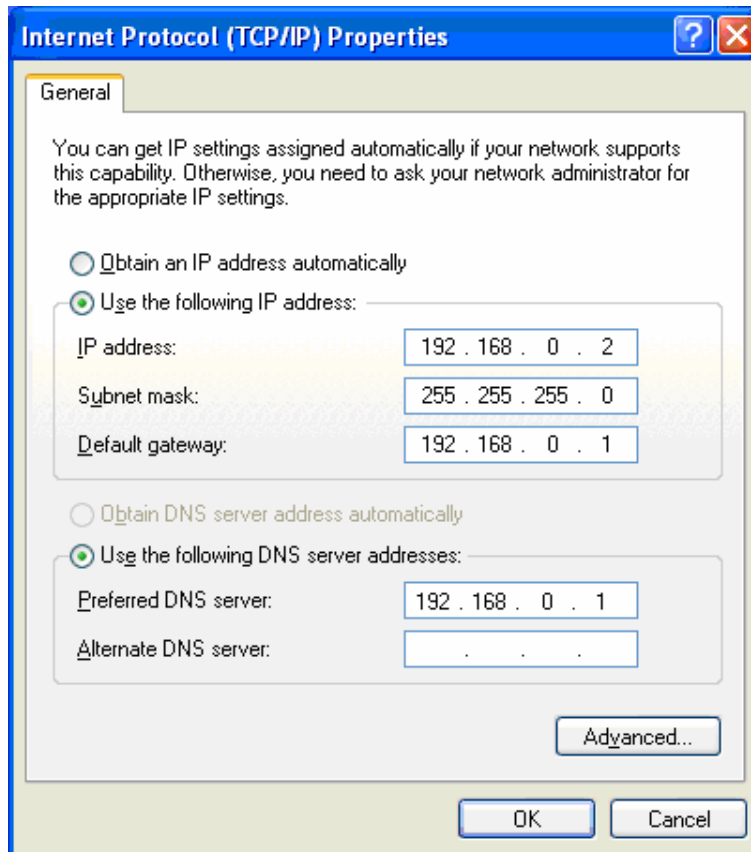


Figure 3-4

**Note:**

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

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

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

```
Pinging 192.168.0.1 with 32 bytes of data:
Reply from 192.168.0.1: bytes=32 time=1ms TTL=254
Reply from 192.168.0.1: bytes=32 time=1ms TTL=254
Reply from 192.168.0.1: bytes=32 time=1ms TTL=254
Reply from 192.168.0.1: bytes=32 time=1ms TTL=254

Ping statistics for 192.168.0.1:
    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 shown below, it means that your PC has not connected to the router.

```
C:\Documents and Settings\Administrator>ping 192.168.0.1

Pinging 192.168.0.1 with 32 bytes of data:

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

Ping statistics for 192.168.0.1:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

Figure 3-6

You can check it follow the steps below:

 **Note:**

**1) Is the connection between your PC and the router correct?**

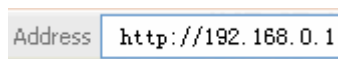
The LEDs of LAN port which you link to the device and the LEDs on your PC's adapter should be lit.

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

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

## 3.2 Login

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



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



Figure 3-7

**Note:**

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

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

## Quick Setup

The quick setup will tell you how to configure the basic network parameters.

To continue, please click the **Next** button.

To exit, please click the **Exit** button.



Figure 3-8

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

## Quick Setup - WAN Connection Type

The Quick Setup is preparing to set up your connection type of WAN port.

The Router will try to detect the Internet connection type your ISP provides if you select the **Auto-Detect** option. Otherwise, you need to specify the connection type manually.

- Auto-Detect** - Let the Router automatically detect the connection type your ISP provides.
- PPPoE** - Usually for ADSL Modem and you will need a PPPoE username and password from your ISP.
- Dynamic IP** - Usually for Cable Modem and the router will automatically obtain an IP address from the DHCP server.
- Static IP** - This type of connection uses a permanent, fixed (static) IP address that your ISP assigned.



Figure 3-9

**Note:**

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

**Step 3:** If **Auto-Detect** is chosen, the router will detect the Internet connection type provided by your ISP automatically.

**Quick Setup - WAN Connection Type**

Detecting the connection type your ISP provides, please wait...

Back

Figure 3-10

**Step 4:** If you choose **PPPoE**, you will see the screen as shown in Figure 3-11. 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.

**Quick Setup - PPPoE**

User Name:   
Password:   
Confirm Password:

Back

Next

Figure 3-11

**Step 5:** 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 6:** If you Choose **Static IP**, you should enter the detailed IP information in Figure 3-12. Click the **Next** button

**Quick Setup - Static IP**

IP Address:   
Subnet Mask:   
Default Gateway:  (Optional)  
Primary DNS:  (Optional)  
Secondary DNS:  (Optional)

Back

Next

Figure 3-12



**Step 7:** 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. For detail settings, please click other menus if necessary.**



Figure 3-13

## Chapter 4. Configuring the Router

It is recommended to use 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 through the Web-based Utility.

After a 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:** 1.2.1 Build 130831 Rel.63039n  
**Hardware Version:** R600VPN v2 00000000

### LAN

**MAC Address:** 00-0A-EB-13-7B-00  
**IP Address:** 192.168.0.1  
**Subnet Mask:** 255.255.255.0

### WAN

**MAC Address:** 00-0A-EB-13-7B-01  
**IP Address:** 192.168.2.4 Dynamic IP  
**Subnet Mask:** 255.255.255.0  
**Default Gateway:** 192.168.2.1   
**DNS Server:** 192.168.2.1 , 0.0.0.0

### Traffic Statistics

	Received	Sent
<b>Bytes:</b>	159689897	39248496
<b>Packets:</b>	164096	131717

**System Up Time:** 3 days 22:20:38

Figure 4-1

- **LAN** - This field displays the current information for the LAN, including the “MAC Address”, “IP Address” and “Subnet Mask”.
- **WAN** - This field displays the parameters applied to the WAN port of the router, including “MAC Address”, “IP Address”, “Subnet Mask”, “Default Gateway” and so on.

 **Note:**

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

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

## 4.2 Quick Setup

Please refer to [chapter 3"Quick Installation Guide"](#).

## 4.3 Network

Choose menu **Network**, the next submenus are shown below.

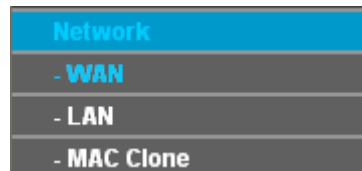


Figure 4-2

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

### 4.3.1 WAN

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

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

#### 1. Dynamic IP

If you aren't given any login parameters and IP information, please select **Dynamic IP** (shown in Figure 4-3), 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

<b>WAN Connection Type:</b>	Dynamic IP	<input type="button" value="Detect"/>
<b>IP Address:</b>	192.168.2.2	
<b>Subnet Mask:</b>	255.255.255.0	
<b>Default Gateway:</b>	192.168.2.1	
	<input type="button" value="Renew"/>	<input type="button" value="Release"/>
<b>MTU Size (in bytes):</b>	1500	(The default is 1500, do not change unless necessary.)
<input type="checkbox"/>	Use These DNS Servers	
<b>Primary DNS:</b>	192.168.2.1	
<b>Secondary DNS:</b>	0.0.0.0	(Optional)
<b>Host Name:</b>	TL-R600VPN	
<input type="checkbox"/>	Get IP with Unicast DHCP (It is usually not required.)	
	<input type="button" value="Save"/>	

Figure 4-3

- **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.
- **Host Name** – This option specifies the host name of the router.

**Note:**

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

- **Get IP with Unicast DHCP:** A few ISPs' DHCP servers do not support the broadcast applications. If you can not get the IP address normally, you can choose this option. (You don't need to select this option generally).

## 2. Static IP

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

The screenshot shows the WAN configuration interface. At the top, there is a blue header with the word "WAN" in white. Below this, the "WAN Connection Type" is set to "Static IP" in a dropdown menu, with a "Detect" button to its right. The "IP Address" field contains "192.168.0.200", the "Subnet Mask" field contains "255.255.255.0", and the "Default Gateway" field contains "192.168.0.1" with "(Optional)" to its right. The "MTU Size (in bytes)" field contains "1500" with the note "(The default is 1500, do not change unless necessary.)" to its right. The "Primary DNS" field contains "0.0.0.0" with "(Optional)" to its right, and the "Secondary DNS" field also contains "0.0.0.0" with "(Optional)" to its right. At the bottom center, there is a "Save" button.

Figure 4-4

- **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).

## 3. PPPoE/Russia PPPoE

If you are given a user name and a password, please select **PPPoE/Russia PPPoE** (shown in Figure 4-5). If you are not sure which connection type you use currently, please contact your ISP to obtain the correct information.

## WAN

**WAN Connection Type:** PPPoE/Russia PPPoE

**PPPoE Connection:**

**User Name:**

**Password:**

**Confirm Password:**

**Secondary Connection:**  Disabled  Dynamic IP  Static IP (For Dual Access/Russia PPPoE)

**Wan Connection Mode:**  Connect on Demand  
 Max Idle Time:  minutes (0 means remain active at all times.)

Connect Automatically

Time-based Connecting  
 Period of Time: from  :  (HH:MM) to  :  (HH:MM)

Connect Manually  
 Max Idle Time:  minutes (0 means remain active at all times.)

**Disconnected!**

---

Figure 4-5

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

 **Note:**

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

**Note:**

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

- **Connect Manually** - You can configure the router to make it connect or disconnect manually. After a specified period of inactivity (**Max Idle Time**), the router will disconnect your Internet connection, and not be able to re-establish your connection automatically even though you attempt to access the Internet again. You need to 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 4-6.

PPPoE Advanced Settings

---

<b>MTU Size (in bytes):</b>	<input type="text" value="1480"/>	<small>(The default is 1480, do not change unless necessary.)</small>
<b>Service Name:</b>	<input type="text"/>	
<b>AC Name:</b>	<input type="text"/>	
	<input type="checkbox"/>	<small>Use IP address specified by ISP</small>
<b>ISP Specified IP Address:</b>	<input type="text" value="0.0.0.0"/>	
<b>Detect Online Interval:</b>	<input type="text" value="0"/>	<small>Seconds (0 ~ 120 seconds, the default is 0, 0 means not detecting.)</small>
	<input type="checkbox"/>	<small>Use the following DNS Servers</small>
<b>Primary DNS:</b>	<input type="text" value="0.0.0.0"/>	
<b>Secondary DNS:</b>	<input type="text" value="0.0.0.0"/>	<small>(Optional)</small>

---

Figure 4-6

- **MTU Size**- The default MTU size is 1480 bytes, which is usually fine. For some ISPs, you need to 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.

#### 4. BigPond Cable

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

WAN

---

**WAN Connection Type:**

**User Name:**

**Password:**

**Auth Server:**

**Auth Domain:**

**MTU Size (in bytes):**  (The default is 1500, do not change unless necessary.)

Connect on Demand  
 Max Idle Time:  minutes (0 means remain active at all times.)

Connect Automatically

Connect Manually  
 Max Idle Time:  minutes (0 means remain active at all times.)

Disconnected!

---

Figure 4-7

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

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

 **Note:**

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

## 5. L2TP/Russia L2TP

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

## WAN

<b>WAN Connection Type:</b>	L2TP/Russia L2TP <input type="button" value="v"/>
<b>User Name:</b>	<input type="text" value="username"/>
<b>Password:</b>	<input type="password" value="••••••••"/>
	<input type="button" value="Connect"/> <input type="button" value="Disconnect"/> <b>Disconnected!</b>
	<input checked="" type="radio"/> Dynamic IP <input type="radio"/> Static IP
<b>Server IP Address/Name:</b>	<input type="text"/>
<b>IP Address:</b>	0.0.0.0
<b>Subnet Mask:</b>	0.0.0.0
<b>Gateway:</b>	0.0.0.0
<b>DNS:</b>	0.0.0.0 , 0.0.0.0
<b>Internet IP Address:</b>	0.0.0.0
<b>Internet DNS:</b>	0.0.0.0 , 0.0.0.0
<b>MTU Size (in bytes):</b>	<input type="text" value="1460"/> (The default is 1460, do not change unless necessary.)
<b>Max Idle Time:</b>	<input type="text" value="15"/> minutes (0 means remain active at all times.)
<b>WAN Connection Mode:</b>	<input checked="" type="radio"/> Connect on Demand <input type="radio"/> Connect Automatically <input type="radio"/> Connect Manually
<input type="button" value="Save"/>	

Figure 4-8

- **User Name/Password** - Enter the User Name and Password provided by your ISP. These fields are case-sensitive.
- **Connect on Demand** - You can configure the router to disconnect your Internet connection after a specified period of the Internet connectivity (**Max Idle Time**). If your Internet connection has been terminated due to inactivity, **Connect on Demand** enables the router to automatically re-establish your connection as soon as you attempt to access the Internet again. If you wish to activate **Connect on Demand**, click the radio button. If you want your Internet connection to remain active at all times, enter **0** in the **Max Idle Time** field. Otherwise, enter the number of minutes you want to have elapsed before your Internet connection terminates.
- **Connect Automatically** - Connect automatically after the router is disconnected. To use this option, click the radio button.
- **Connect Manually** - You can configure the router to make it connect or disconnect manually. After a specified period of inactivity (**Max Idle Time**), the router will disconnect your Internet connection, and not be able to re-establish your connection automatically as soon as you attempt to access the Internet again. To use this option, click the radio button. If you want your Internet connection to remain active at all times, enter **0** in the **Max Idle Time** field.

Otherwise, enter the number in minutes that you wish to have the Internet connecting last unless a new link requested.

 **Note:**

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

## 6. PPTP/Russia PPTP

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

WAN

---

<b>WAN Connection Type:</b>	<input type="text" value="PPTP/Russia PPTP"/>
<b>User Name:</b>	<input type="text" value="username"/>
<b>Password:</b>	<input type="password" value="••••••••"/>
	<input type="button" value="Connect"/> <input type="button" value="Disconnect"/> <span style="color: blue; font-weight: bold;">Disconnected!</span>
	<input checked="" type="radio"/> Dynamic IP <input type="radio"/> Static IP
<b>Server IP Address/Name:</b>	<input type="text" value="1.1.1.1"/>
<b>IP Address:</b>	0.0.0.0
<b>Subnet Mask:</b>	0.0.0.0
<b>Gateway:</b>	0.0.0.0
<b>DNS:</b>	0.0.0.0 , 0.0.0.0
<b>Internet IP Address:</b>	0.0.0.0
<b>Internet DNS:</b>	0.0.0.0 , 0.0.0.0
<b>MTU Size (in bytes):</b>	<input type="text" value="1420"/> (The default is 1420, do not change unless necessary.)
<b>Max Idle Time:</b>	<input type="text" value="15"/> minutes (0 means remain active at all times.)
<b>WAN Connection Mode:</b>	<input checked="" type="radio"/> Connect on Demand <input type="radio"/> Connect Automatically <input type="radio"/> Connect Manually

---

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 terminates.

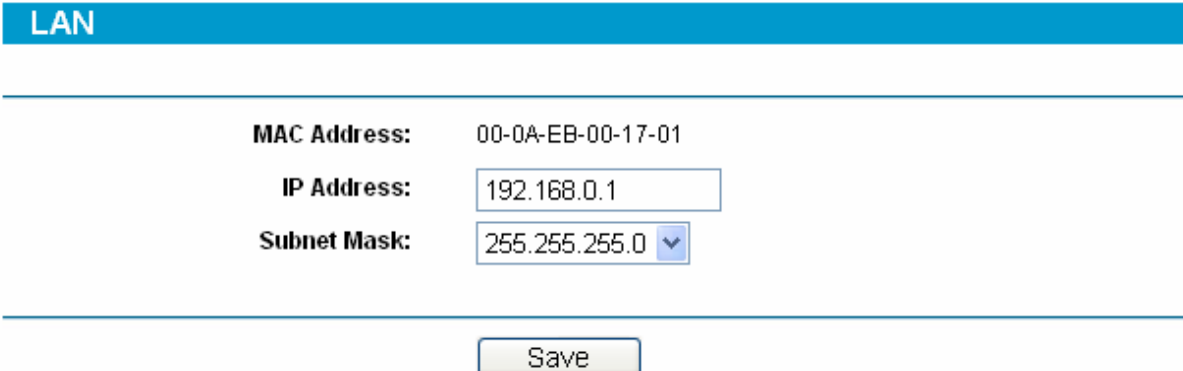
- **Connect Automatically** - Connect automatically after the router is disconnected. To use this option, click the radio button.
- **Connect Manually** - You can configure the router to make it connect or disconnect manually. After a specified period of inactivity (**Max Idle Time**), the router will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

 **Note:**

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

### 4.3.2 LAN

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



<b>MAC Address:</b>	00-0A-EB-00-17-01
<b>IP Address:</b>	<input type="text" value="192.168.0.1"/>
<b>Subnet Mask:</b>	<input type="text" value="255.255.255.0"/>

Figure 4-10

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

 **Note:**

- 1) If you change the IP address of the LAN, you must use the new IP address to login to the router.
- 2) If the new LAN IP Address you set is not in the same subnet, the IP Address pools in the DHCP sever will not take effect, until they are re-configured. Besides this, the Virtual

Server and DMZ Host may change accordingly at the same time; you'd better re-configure it as well.

### 4.3.3 MAC Clone

Choose menu **Network**→**MAC Clone**, you can configure the MAC address of the WAN on the screen below (shown in Figure 4-11).

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.

MAC Clone	
WAN MAC Address:	<input type="text" value="00-0A-EB-13-7B-01"/> <input type="button" value="Restore Factory MAC"/>
Your PC's MAC Address:	<input type="text" value="40-61-86-fc-75-c3"/> <input type="button" value="Clone MAC Address"/>
<input type="button" value="Save"/>	

Figure 4-11

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

 **Note:**

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

## 4.4 DHCP

Choose menu **DHCP**, the next submenus are shown below.

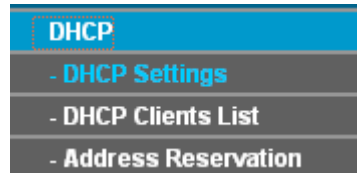


Figure 4-12

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 4-13).

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

---

<b>DHCP Server:</b>	<input type="radio"/> Disable <input checked="" type="radio"/> Enable
<b>Start IP Address:</b>	<input type="text" value="192.168.0.100"/>
<b>End IP Address:</b>	<input type="text" value="192.168.0.199"/>
<b>Address Lease Time:</b>	<input type="text" value="120"/> minutes (1~2880 minutes, the default value is 120)
<b>Default Gateway:</b>	<input type="text" value="192.168.0.1"/> (optional)
<b>Default Domain:</b>	<input type="text"/> (optional)
<b>Primary DNS:</b>	<input type="text" value="0.0.0.0"/> (optional)
<b>Secondary DNS:</b>	<input type="text" value="0.0.0.0"/> (optional)

---

Figure 4-13

- **DHCP Server - Enable or disable** the DHCP server. If you disable the Server, you must have another DHCP server within your network or else you must manually configure the computer.
- **Start IP Address** - This field specifies the first address in the IP address pool. The default address is 192.168.0.100.
- **End IP Address** - This field specifies the end address in the IP address pool. The default address is 192.168.0.199.

- **Address Lease Time** - This is the amount of time in which a network user will be allowed connection to the router with their current dynamic IP address. Enter the amount of time (in minutes), the range of the time is 1 ~ 2880 minutes. The default value is 120 minutes.
- **Default Gateway** - Suggest inputting the IP address of the LAN port of the router, default value is 192.168.0.1. (Optional)
- **Default Domain** - Input the domain name of your network. (Optional)
- **Primary DNS** - Input the DNS IP address provided by your ISP. You can consult your ISP for it. (Optional)
- **Secondary DNS** - Input the IP address of another DNS server if your ISP provides two DNS servers. (Optional)

 **Note:**

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

#### 4.4.2 DHCP Clients List

Choose menu **DHCP→DHCP Clients List**, you can view the information about the clients attached to the router in the next screen (shown in Figure 4-14). Click the **Refresh** button to update the information.

DHCP Clients List				
ID	Client Name	MAC Address	Assigned IP	Lease Time
1	ann	00-19-66-19-40-7F	192.168.0.100	01:59:59

Figure 4-14

- **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 4-15).

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.



## Address Reservation

ID	MAC Address	Reserved IP Address	Status	Modify
1	00-19-66-19-40-7F	192.168.0.100	Enabled	<a href="#">Modify</a> <a href="#">Delete</a>

Figure 4-15

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

### To add/modify a reserved IP address:

**Step 1:** Click **Add New.../Modify** shown in Figure 4-15, you will see a new screen shown in Figure 4-16.

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

## Add or Modify a Address Reservation Entry

**MAC Address:**   
**Reserved IP Address:**   
**Status:**

Figure 4-16

**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 4-15:

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

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

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

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

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

## 4.5 Forwarding

Choose menu “**Forwarding**”, the next submenus are shown below.

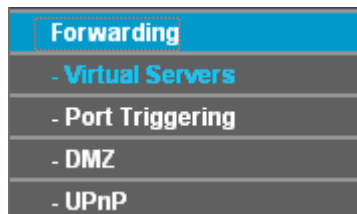


Figure 4-17

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

### 4.5.1 Virtual Servers

Choose menu **Forwarding**→**Virtual Servers**, you can view and add virtual servers in the next screen (shown in Figure 4-18).

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.

Virtual Servers						
ID	Service Port	Internal Port	IP Address	Protocol	Status	Modify
1	21	21	192.168.0.100	TCP	Enabled	<a href="#">Modify</a> <a href="#">Delete</a>
2	20	20	192.168.0.101	TCP	Enabled	<a href="#">Modify</a> <a href="#">Delete</a>

Figure 4-18

- **Service Port** - This field displays the numbers of External Ports. It can be a service port or a range of service ports (the format is XX-YY or XX, XX is Start port, YY is End port).
- **Internal Port** - The Internal Service Port number of the PC running the service application. You can leave it blank if the **Internal Port** is the same as the **Service Port**, or enter a specific port number when **Service Port** is a single one.
- **IP Address** - 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 4-18, you will see a new screen shown in Figure 4-19.

**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 Server Entry

---

Service Port:	<input type="text" value="21"/>	<small>(XX-XX or XX)</small>
Internal Port:	<input type="text" value="21"/>	<small>(XX, Only valid for single Service Port or leave it blank)</small>
IP Address:	<input type="text" value="192.168.0.105"/>	
Protocol:	<input type="text" value="TCP"/>	
Status:	<input type="text" value="Enabled"/>	
Common Service Port: <input type="text" value="FTP"/>		

---

Figure 4-19

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

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

#### **Note:**

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

#### **Other configurations for the entries as shown in Figure 4-18:**

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 4-20).

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.

Port Triggering						
ID	Trigger Port	Trigger Protocol	Incoming Port	Incoming Protocol	Status	Modify
1	6112	ALL	6112	ALL	Enabled	<a href="#">Modify</a> <a href="#">Delete</a>

Figure 4-20

- **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 Port** - 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**, **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 4-20, you will see a new screen shown in Figure 4-21.

**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:	<input type="text" value="6112"/>
Trigger Protocol:	<input type="text" value="ALL"/>
Incoming Port:	<input type="text" value="6112"/>
Incoming Protocol:	<input type="text" value="ALL"/>
Status:	<input type="text" value="Enabled"/>
Common Applications:	<input type="text" value="Battle.net"/>



Figure 4-21

**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 4-20:**

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

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

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

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

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

### 4.5.3 DMZ

Choose menu “**Forwarding**→**DMZ**”, you can view and configure DMZ host in the screen (shown in Figure 4-22).

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.

DMZ

---

Current DMZ Status:  Enabled  Disabled

DMZ Host IP Address:

---

Figure 4-22

**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 4-23). 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.

UPnP

---

Current UPnP Status: **Enabled**

---

**Current UPnP Settings List**

ID	App Description	External Port	Protocol	Internal Port	IP Address	Status
<input type="button" value="Refresh"/>						

Figure 4-23

- **Current UPnP Status** - If you want to use the router's UPnP function, please click **Enable** button. If you don't want use the function, please click **Disable** button. Allowing the function may cause a risk to security; this feature is disabled by default.

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

## 4.6 Security

Choose menu **Security**, the next submenus are shown below.



Figure 4-24

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 Basic Security

Choose menu **Security**→**Basic Security**, you can configure the basic security of the router in the next screen (shown in Figure 4-25).

**Basic Security**

---

**Firewall**

SPI Firewall:  Enable  Disable

---

**VPN**

PPTP Passthrough:  Enable  Disable

L2TP Passthrough:  Enable  Disable

IPSec Passthrough:  Enable  Disable

---

**ALG**

FTP ALG:  Enable  Disable

TFTP ALG:  Enable  Disable

H323 ALG:  Enable  Disable

RTSP ALG:  Enable  Disable

---

Figure 4-25

- **Firewall** - Enable the general firewall or not.
  - **SPI Firewall** - SPI (Stateful Packet Inspection) keeps track of the state of network connections traveling across it. It distinguishes legitimate packets for different types of connections. Only packets matching a known active connection will be allowed by the firewall; others will be rejected. SPI Firewall is enabled by factory default. If you want all the computers on the LAN exposed to the external network, you can disable it.
- **VPN** - VPN Passthrough must be enabled if you want to allow VPN tunnels using VPN protocols to pass through the router.
  - **PPTP Passthrough** - Check the box before **Enable** to allow the PPTP tunnels to pass through the router.
  - **L2TP Passthrough** - Check the box before **Enable** to allow the L2TP tunnels to pass through the router.
  - **IPSec Passthrough** - Check the box before **Enable** to allow the IPSec tunnels to pass through the router.
- **ALG** - You can determine whether to provide ALG (Application Level Gateway) service for FTP, TFTP, H323 and RTSP to keep these special applications from the effect of NAT service.
  - **FTP ALG** - Select **Enable** to allow FTP services to operate properly.
  - **TFTP ALG** - Select **Enable** to allow TFTP services to operate properly.
  - **H323 ALG** - Select **Enable** to allow H323 services to operate properly.
  - **RTSP ALG** - Select **Enable** to allow RTSP services to operate properly.

#### 4.6.2 Advanced Security

Choose menu **Security**→**Advanced Security**, you can protect the router from being attacked by TCP-SYN Flood, UDP Flood and ICMP-Flood in the next screen (shown in Figure 4-26).



## Advanced Security

**Packets Statistics Interval (5 ~ 60):**  Seconds

**DoS Attack Defence:**  Disable  Enable

Enable ICMP-FLOOD Attack Filtering

**ICMP-FLOOD Packets Threshold (5 ~ 3600):**  Packets/s

Enable UDP-FLOOD Filtering

**UDP-FLOOD Packets Threshold (5 ~ 3600):**  Packets/s

Enable TCP-SYN-FLOOD Attack Filtering

**TCP-SYN-FLOOD Packets Threshold (5 ~ 3600):**  Packets/s

Block Ping Packet From WAN Port

Block Ping Packet From LAN Port

Figure 4-26

- **Packets Statistics Interval** - This is the interval for capturing the statistics.
- **DoS Attack Defense** - Enable or disable the DoS Attack Defense.
- **Enable ICMP-FLOOD Attack Filtering** - The attackers flood normal communication by attacking the server with a lot of ICMP packets. Check the box to activate the function to prevent an ICMP Flood attack. The threshold should be within the range of 5-3600 and the default value is 50.
- **Enable UDP-FLOOD Filtering** - Check the box to activate the function to prevent the UDP Flood attack of a fixed source IP. Once the packets rate exceeds threshold value, the packets will be blocked. The threshold should be within the range of 5-3600 .and the default value is 500.
- **Enable TCP-SYN-FLOOD Attack Filtering** - Check the box to activate the function to prevent a TCP-SYN-Flood attack. Once the packets rate exceeds threshold value, the packets will be blocked. The threshold should be within the range of 5-3600 and the default value is 50.

### 4.6.3 Local Management

Choose menu **Security**→**Local Management**, you can configure to prevent the local PCs from accessing the router's web-based utility in the next screen (shown in Figure 4-27).

## Local Management

## Management Rules

- All the PCs on the LAN are allowed to access the Router's Web-Based Utility
- Only the PCs listed can browse the built-in web pages to perform Administrator tasks

MAC 1:

MAC 2:

MAC 3:

MAC 4:

Your PC's MAC Address:

Figure 4-27

- **Management Rules** - Here displays the management rules
- **All the PCs on the LAN are allowed to access the router's Web-Based Utility:** This rule determines that all the PCs connected to the router can visit the router's Web-Based Utility.
  - **Only the PCs listed can browse the built-in web pages to perform Administrator tasks:** This rule determines that only the specified LAN PCs can visit the Web-Based Utility to configure the router.

**To add a PC to the management list:**

**Step 1:** Select the option of **Only the PCs listed can browse the built-in web pages to perform Administrator tasks**.

**Step 2:** Enter the PC's MAC address in the **MAC1/2/3/4** field or click the **Add** button to add your PC's MAC Address to the list.

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

## 4.7 Access Control

Choose menu **Access Control**, the next submenus are shown below.



Figure 4-28

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

### 4.7.1 Rule

Choose menu **Access Control** → **Rule**, you can configure the Internet Access Control to manage Internet activities from LAN hosts in the next screen (shown in Figure 4-29).

## Access Control Rule Management

Enable Internet Access Control

### Default Filter Policy

Allow the packets not specified by any access control policy to pass through the Router

Deny the packets not specified by any access control policy to pass through the Router

Save

ID	Rule Name	Host	Target	Schedule	Action	Status	Modify
1	test	1	Any	Permanent	Deny	Enabled	<a href="#">Edit</a> <a href="#">Delete</a>

Add New...

Enable All

Disable All

Delete All

Move

ID

To ID

Previous

Next

Current No. 1 Page

Figure 4-29

- **Enable Internet Access Control:** Enable or disable the Internet Access Control.
- **Default Filter Policy:** Select a policy to allow or deny the packets matching the rules to pass through the router.
- **Rule Name:** Display the name of the rule and this name is unique.
- **Host:** Displays the hosts to which the rule takes effect.
- **Target:** Displays the corresponding target of the rule.
- **Schedule:** Displays the effective time of the rule.
- **Action:** Display the actions of the router to deal with the packets.
- **Status:** Displays the rule is enabled or disabled.

### To add/modify an Internet Access Control entry:

**Step 1:** Click **Add New.../Edit** shown in Figure 4-29, you will see a new screen shown in Figure 4-30.

**Step 2:** Enter the Rule Name and select the Host, Target, Schedule, Action and Status.

## Add or Modify Internet Access Control Entry

Rule Name:

Host: 1 [Click Here To Add New Host List.](#)

Target: Any Target [Click Here To Add New Target List.](#)

Schedule: Anytime [Click Here To Add New Schedule.](#)

Action: Deny

Status: Enabled

Save

Back

Figure 4-30

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

**Other configurations for the entries as shown in Figure 4-29:**

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.

#### 4.7.2 Host

Choose menu **Access Control** → **Host**, you can configure Host of the Access Control rule in the next screen (shown in Figure 4-31).

ID	Host Description	Information	Modify
1	1	IP: 192.168.0.102 - 192.168.0.110	<a href="#">Edit</a> <a href="#">Delete</a>

Current No.  Page

Figure 4-31

- **Host Description:** Displays the description of the host and the description is unique.
- **Information:** Displays the MAC address or IP address of the PCs to which the rule take effect.

**To add/modify a host for Access Control Rule:**

**Step 1:** Click **Add New.../Edit** shown in Figure 4-31, you will see a new screen shown in Figure 4-32.

**Step 2:** Select the Mode and enter the Host Description and LAN IP Address.

**Mode:**

**Host Description:**

**LAN IP Address:**  -

Figure 4-32

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

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

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.

### 4.7.3 Target

Choose menu **Access Control** → **Target**, you can configure Target of the Access Control rule in the next screen (shown in Figure 4-33).

ID	Target Description	Information	Modify
<input type="button" value="Add New..."/> <input type="button" value="Delete All"/>			
<input type="button" value="Previous"/> <input type="button" value="Next"/> Current No. <input type="text" value="1"/> Page			

Figure 4-33

- **Target Description:** Displays the description of the target and the description is unique.
- **Information:** Displays the IP address, port or domain name that the PCs can access or not.

#### To add/modify a target for Access Control Rule:

**Step 1:** Click **Add New/Modify...** shown in Figure 4-33, you will see a new screen shown in Figure 4-34

**Step 2:** Select the Mode, Protocol, and Common Service Port and enter the Target Description, IP Address and Target port.

**Mode:**

**Target Description:**

**IP Address:**  -

**Target Port:**  -

**Protocol:**

**Common Service Port:**

Figure 4-34

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

#### Other configurations for the entries as shown in Figure 4-33:

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.

#### 4.7.4 Schedule

Choose menu **Access Control** → **Target**, you can configure the effective time of the Access Control rule in the next screen (shown in Figure 4-35).

**Schedule Settings**

---

ID	Schedule Description	Day	Time	Modify
1	1	Every Day	00:00 - 24:00	<a href="#">Edit</a> <a href="#">Delete</a>

---

Current No. 1 Page

Figure 4-35

- **Schedule Description:** Displays the description of the schedule and the description is unique.
- **Day:** Displays the day on which the rule takes effect
- **Time:** Displays the time between which the rule takes effect.

#### To add/modify a target for Access Control Rule:

**Step 1:** Click **Add New.../Edit** shown in Figure 4-35, you will see a new screen shown in Figure 4-36.

**Step 2:** Enter the Schedule Description and select the days, and then specify the Start Time and Stop Time.

**Advance Schedule Settings**

---

Note: The Schedule is based on the time of the Router.

**Schedule Description:**

**Day:**  Everyday  Select Days

Mon  Tue  Wed  Thu  Fri  Sat  Sun

**Time:** all day-24 hours:

**Start Time:**  (HHMM)

**Stop Time:**  (HHMM)

---

Figure 4-36

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

#### Other configurations for the entries as shown in Figure 4-35:

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 IPsec VPN

Choose menu **IPsec VPN**, the next submenus are shown below.



Figure 4-37

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 IKE

Choose menu **IPsec VPN**→**IKE**, you can configure the related parameters for IKE negotiation and view the IKE policy in the next screen (shown in Figure 4-38).

List of IKE Policy							
ID	Policy Name	Exchange Mode	Authentication	Encryption	DH Group	Pre-shared Key	Modify
1	policy1	Main	AUTO	AUTO	DH2	12345678	<a href="#">Modify</a> <a href="#">Delete</a>

---

Current No.  Page

Figure 4-38

- **Policy Name:** The unique name to the IKE policy for identification and management purposes.
- **Exchange Mode:** Displays the IKE Exchange Mode in phase 1, and the remote VPN peer uses the same mode.
  - Main: Main mode provides identity protection and exchanges more information, which applies to the scenarios with higher requirement for identity protection.
  - Aggressive: Aggressive Mode establishes a faster connection but with lower security, which applies to scenarios with lower requirement for identity protection.
- **Authentication:** The authentication algorithm for IKE negotiation. Options include:
  - MD5: MD5 (Message Digest Algorithm) takes a message of arbitrary length and generates a 128-bit message digest.
  - SHA1: SHA1 (Secure Hash Algorithm) takes a message less than  $2^{64}$  (the 64th power of 2) in bits and generates a 160-bit message digest.

- **Encryption:** The encryption algorithm for IKE negotiation. Options include:
  - DES: DES (Data Encryption Standard) encrypts a 64-bit block of plain text with a 56-bit key.
  - 3DES: Triple DES, encrypts a plain text with 168-bit key.
  - AES128: Uses the AES algorithm and 128-bit key for encryption.
  - AES192: Uses the AES algorithm and 192-bit key for encryption.
  - AES256: Uses the AES algorithm and 256-bit key for encryption.
- **DH Group:** The DH (Diffie-Hellman) group to be used in key negotiation phase 1. The DH Group sets the strength of the algorithm in bits. Options include DH1, DH2 and DH5.
  - DH1: 768 bits
  - DH2: 1024 bits
  - DH3: 1536 bits
- **Pre-shared Key:** The Pre-shared Key for IKE authentication, and ensure both the two peers use the same key. The key should consist of visible characters without blank space.

#### To add/modify an IKE entry:

**Step 1:** Click **Add New.../Modify** shown in Figure 4-38, you will see a new screen shown in Figure 4-39.

**Step 2:** Enter the Policy Name, Pre-Shared Key, SA Lifetime and then select the Exchange Mode, Authentication Algorithm, Encryption Algorithm, DH Group. Then enable or disable the DPD.

**IKE Policy Settings**

---

<b>Policy Name:</b>	<input style="width: 60%;" type="text"/>
<b>Exchange Mode:</b>	<input checked="" type="radio"/> Main <input type="radio"/> Aggressive
<b>Authentication Algorithm:</b>	<input type="text" value="AUTO"/> ▾
<b>Encryption Algorithm:</b>	<input type="text" value="AUTO"/> ▾
<b>DH Group:</b>	<input type="text" value="DH2"/> ▾
<b>Pre-shared Key:</b>	<input style="width: 60%;" type="text"/>
<b>SA Lifetime:</b>	<input style="width: 40%;" type="text" value="28800"/> seconds (60-604800)
<b>DPD:</b>	<input type="radio"/> Enable <input checked="" type="radio"/> Disable

---

Figure 4-39

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



### Other configurations for the entries as shown in Figure 4-38:

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.

## 4.8.2 IPsec

Choose menu **IPsec VPN**→**IPsec**, you can configure the related parameters for IPsec negotiation and view the IPsec policy in the next screen (shown in Figure 4-40).

List of IPsec Policy

---

**IPsec:**     Enable     Disable

ID	Policy Name	Local Subnet	Remote Subnet	Exchange Mode	Status	Modify
1	policy1	192.168.2.0/24	192.168.1.0/24	IKE	Enabled	<a href="#">Modify</a> <a href="#">Delete</a>

---

Current No. 1 Page

Figure 4-40

- **IPSec:** Enable or disable IPsec and click save to apply.
- **Policy Name:** The unique name to the IPsec policy for identification and management purposes.
- **Local Subnet:** The IP address range on your local LAN to identify which PCs on your LAN are covered by this policy. It's formed by IP address and subnet mask.
- **Remote Subnet:** The IP address range on your remote network to identify which PCs on the remote network are covered by this policy. It's formed by IP address and subnet mask.
- **Exchange Mode:** The negotiation mode for the policy.

#### **Note:**

When deleting, modifying or adding the IKE/IPsec entries, all the existing VPN tunnels will be disconnected for a few seconds and then reconnected. Operation to the IKE entries not associated with the IPsec will not affect the VPN tunnel.

#### **To add/modify an IPsec entry:**

**Step 1:** Click **Add New.../Modify** shown in Figure 4-40, you will see a new screen shown in Figure 4-41.

**Step 2:** Enter the Policy Name, Local Subnet, Remote Subnet, Remote Gateway, PFS Lifetime and then select the Exchange Mode, Security Protocol, Authentication Algorithm, Encryption Algorithm, IKE Security Policy, PFS Group. Then enable or disable the settings.

## IPsec Policy Settings

<b>Policy Name:</b>	<input type="text"/>
<b>Local Subnet:</b>	<input type="text"/> / <input type="text"/>
<b>Remote Subnet:</b>	<input type="text"/> / <input type="text"/>
<b>Remote Gateway:</b>	<input type="text"/> (IP or domain name)
<b>Exchange Mode:</b>	<input checked="" type="radio"/> IKE <input type="radio"/> Manual
<b>Security Protocol:</b>	<input type="text" value="ESP"/> ▼
<b>Authentication Algorithm:</b>	<input type="text" value="AUTO"/> ▼
<b>Encryption Algorithm:</b>	<input type="text" value="AUTO"/> ▼
<b>IKE Security Policy:</b>	<input type="text" value="policy1"/> ▼ <a href="#">Click here to add IKE list</a>
<b>PFS Group:</b>	<input type="text" value="NONE"/> ▼
<b>PFS Lifetime:</b>	<input type="text" value="28800"/> seconds (60-604800)
<b>Status:</b>	<input type="text" value="Enable"/> ▼

Save

Back

Figure 4-41

- **Policy Name:** Enter the unique name to the IPsec policy for identification and management purposes.
- **Local Subnet:** Enter the IP address range on your local LAN to identify which PCs on your LAN are covered by this policy. It's formed by IP address and subnet mask.
- **Remote Subnet:** Enter the IP address range on your remote network to identify which PCs on the remote network are covered by this policy. It's formed by IP address and subnet mask.
- **Remote Gateway:** Enter the Remote Gateway. It can be IP address or domain name.

**Exchange Mode:** Select the negotiation mode for the policy.

- IKE: The parameters for the VPN tunnel are generated automatically via IKE negotiations.
- Manual: All settings (including the keys) for the VPN tunnel are manually input and no key negotiation is needed.

- **IKE Mode**

**Security Policy:**

It is available when IKE is selected as the negotiation mode. Select the Security Policy for IPsec.

**Authentication Algorithm:**

Select the Authentication Algorithm for IPsec policy. The default value is "Auto".

- Encryption Algorithm:** Select the Encryption Algorithm for IPsec policy. The default value is "Auto".
- IKE Security Policy:** Select the IKE Security Policy for IPsec policy.
- PFS Group:** Select the PFS (Perfect Forward Security) for IKE mode to enhance security. This setting should match the remote peer. With PFS feature, IKE negotiates to create a new key in Phase2. As it is independent of the key created in Phase1, this key can be secure even when the key in Phase1 is de-encrypted. Without PFS, the key in Phase2 is created based on the key in Phase1 and thus once the key in Phase1 is de-encrypted, the key in Phase2 is easy to be de-encrypted, in this case, the communication secrecy is threatened.
- Lifetime:** Specify IPsec SA Lifetime for IKE mode.
- Status:** Enable or disable the entry.
- **Manual Mode**
- Security Protocol:** Select the Security Protocol for IPsec.
- Authentication Algorithm:** Select the Authentication Algorithm for IPsec policy. The default value is "SHA1".
- Encryption Algorithm:** Select the Encryption Algorithm for IPsec policy. The default value is "AES256".
- Incoming SPI:** Specify the Incoming SPI (Security Parameter Index) manually. The Incoming SPI here must match the Outgoing SPI value at the other end of the tunnel, and vice versa.
- In Authentication Key:** Specify the inbound AH Authentication Key manually if AH protocol is used in the corresponding IPsec Proposal. The inbound key here must match the outbound AH authentication key at the other end of the tunnel, and vice versa.

- In Encryption Key:** Specify the Inbound Encryption Key manually if ESP protocol The inbound key here must match the outbound Encryption Key at the other end of the tunnel, and vice versa.
- Outgoing SPI:** Specify the Outgoing SPI (Security Parameter Index) manually. The Outgoing SPI here must match the Incoming SPI value at the other end of the tunnel, and vice versa.
- Out Authentication Key:** Specify the outbound AH Authentication Key manually if AH protocol is used in the corresponding IPsec Proposal. The outbound key here must match the inbound AH authentication key at the other end of the tunnel, and vice versa.
- Out Encryption Key:** Specify the outbound Encryption Key manually The outbound key here must match the inbound Encryption Key at the other end of the tunnel, and vice versa.
- Status:** Enable or Disable the entry.

#### Other configurations for the entries as shown in Figure 4-40:

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.

### 4.8.3 SA List

This page displays the information of the IPsec SA (Security Association). Choose the menu **IPsec VPN**→**SA List** to load the following page.

List of Security Association								
ID	Name	SPI	Tunnel Initiator	Tunnel Receiver	Security Protocol	AH Auth	ESP Auth	ESP Encr
Now the list is empty.								
<input type="button" value="Refresh"/>								

Figure 4-42

This page displays the connection status of the IPsec Policy. As Security Association is unidirectional, an ingoing SA and an outgoing SA are created to protect data flows for each tunnel after

IPsec tunnel is successfully established. The ingoing SPI value and outgoing SPI value are different. However, the Incoming SPI value must match the Outgoing SPI value at the other end of the tunnel, and vice versa. The connection status on the remote endpoint of this tunnel is as the following figure shows. The SPI value is obtained via auto-negotiation.

## 4.9 PPTP VPN Server

Choose menu **PPTP VPN Server**, the next submenus are shown below.

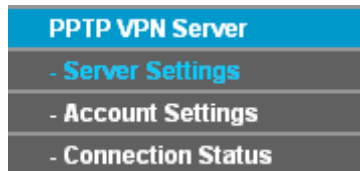


Figure 4-43

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

### 4.9.1 Server Settings

Choose menu **PPTP VPN Server**→**Server Settings**, you can configure the parameters of the PPTP Server in the next screen (shown in Figure 4-44).

 A screenshot of the 'PPTP Server Settings' configuration page. The page has a blue header bar with the title 'PPTP Server Settings'. Below the header, there are four configuration items:
 

- PPTP Server:** Two radio buttons, 'Enable' (unselected) and 'Disable' (selected).
- MPPE Encryption:** Two radio buttons, 'Enable' (unselected) and 'Disable' (selected).
- IP Range Start:** A text input field containing '192.168.0.200'.
- IP Range End:** A text input field containing '192.168.0.215'.

 At the bottom of the form is a 'Save' button.

Figure 4-44

- **PPTP Server** – Enable or disable the PPTP Server.
- **MPPE Encryption** – Enable or disable the MPPE Encryption. If enabled, the PPTP tunnel will be encrypted by MPPE.
- **IP Range Start** - Enter the start IP address to define a range for the server's IP assignment.
- **IP Range End** - Enter the end IP address to define a range for the server's IP assignment.

### 4.9.2 Account Settings

Choose the menu **PPTP VPN Server**→**Account Settings**, you can configure the PPTP account in the next screen (shown in Figure 4-45).

## PPTP Account Settings

ID	Account	Status	Modify
1	123456	Enabled	<a href="#">Modify</a> <a href="#">Delete</a>

Figure 4-45

- **Account** - Displays the PPTP Account.
- **Status** - Displays the status of the PPTP Server.

### To add/modify a PPTP Account rule:

**Step 1:** Click **Add New.../Modify** shown in Figure 4-45, you will see a new screen shown in Figure 4-46.

**Step 2:** Enter the Account, Password and select the status.

### Add or Modify a PPTP Account

**Account:**   
**Password:**   
**Confirm Password:**   
**Status:**

Figure 4-46

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

**Other configurations for the entries as shown in Figure 4-45.**

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.

### 4.9.3 Connection Status

Choose the menu **PPTP VPN Server**→**Connection Status**, you can view the connection status of each user in the next screen (shown in Figure 4-47).

Connection Status				
ID	Account	Remote IP Address	PPTP IP Address	Online Time
<input type="button" value="Refresh"/>				

Figure 4-47

- **Remote IP Address** – Displays the original IP address of the remote client.
- **PPTP IP Address** – Displays the IP address the PPTP Server assigned to the remote client.
- **Online Time** – Displays the online time of the PPTP Server.

## 4.10 Advanced Routing

Choose menu **Advanced Routing**, the next submenus are shown below.

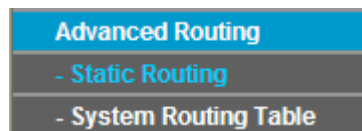


Figure 4-48

### 4.10.1 Static Routing

Choose menu **Advanced Routing**→**Static Routing**, you can configure the static route in the next screen (shown in Figure 4-49). 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	222.88.88.100	255.255.255.0	222.88.88.1	Disabled	<a href="#">Modify</a> <a href="#">Delete</a>

Figure 4-49

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

**To add/modify a static routing entry:**

**Step 1:** Click **Add New.../Modify** shown in Figure 4-49, you will see a new screen shown in Figure 4-50.

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

**Add or Modify a Static Route Entry**

---

<b>Destination IP Address:</b>	<input style="width: 100%;" type="text" value="222.88.88.100"/>
<b>Subnet Mask:</b>	<input style="width: 100%;" type="text" value="255.255.255.0"/>
<b>Default Gateway:</b>	<input style="width: 100%;" type="text" value="222.88.88.1"/>
<b>Status:</b>	<input style="border: 1px solid #ccc;" type="text" value="Enabled"/>

---

Figure 4-50

**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 4-49.**

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.

**4.10.2 System Routing Table**

Choose menu **Advanced Routing**→**System Routing Table**, you can view all of the valid route entries in use. The Destination IP address, Subnet Mask, Gateway, and Interface will be displayed for each entry. Click the **Refresh** button to refresh the data displayed.

**System Routing Table**

---

ID	Destination Network	Subnet Mask	Gateway	Interface
1	192.168.1.0	255.255.255.0	0.0.0.0	LAN

---

Figure 4-51

➤ **Destination Network** - The Destination Network is the address of the network or host to which the static route is assigned



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

## 4.11 Bandwidth Control

Choose menu **Bandwidth Control**, the next submenus are shown below.



Figure 4-52

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

### 4.11.1 Control Settings

Choose menu **Bandwidth Control**→**Control Settings**, you can configure the Egress Bandwidth and Ingress Bandwidth in the next screen (shown in Figure 4-53).

Bandwidth Control Settings

---

<b>Enable Bandwidth Control:</b>	<input type="checkbox"/>		
<b>Line Type:</b>	<input checked="" type="radio"/>	ADSL	<input type="radio"/> Other
<b>Egress Bandwidth:</b>	<input style="width: 150px;" type="text" value="512"/>	Kbps	
<b>Ingress Bandwidth:</b>	<input style="width: 150px;" type="text" value="2048"/>	Kbps	

---

Figure 4-53

- **Enable Bandwidth Control** - Enable or disable the Bandwidth Control.
- **Line Type** - Select the Line Type of the WAN port.
- **Egress/Ingress Bandwidth** – Enter the Egress and Ingress Bandwidth through the WAN port.

### 4.11.2 Rule List

Choose menu **Bandwidth Control**→**Rule List**, you can view the Bandwidth Control rules list.

## Bandwidth Control Rules List

ID	Description	Egress Bandwidth(Kbps)		Ingress Bandwidth(Kbps)		Enable	Modify
		Min	Max	Min	Max		
1	192.168.0.100 - 192.168.0.199	100	1000	100	1000	<input checked="" type="checkbox"/>	<a href="#">Modify</a> <a href="#">Delete</a>

Add New...

Delete All

Previous

Next

Now is the 1 page

Figure 4-54

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

**To add/modify a Bandwidth Control rule:**

**Step 1:** Click **Add New**...**Modify** shown in Figure 4-54, you will see a new screen shown in Figure 4-55

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

## Bandwidth Control Rule Settings

<b>Enable:</b>	<input checked="" type="checkbox"/>	
<b>IP Range:</b>	<input type="text" value="192.168.0.100"/>	- <input type="text" value="192.168.0.199"/>
<b>Port Range:</b>	<input type="text" value="21"/>	- <input type="text"/>
<b>Protocol:</b>	<input type="text" value="ALL"/> ▾	
	Min Bandwidth(Kbps)	Max Bandwidth(Kbps)
<b>Egress Bandwidth:</b>	<input type="text" value="100"/>	<input type="text" value="1000"/>
<b>Ingress Bandwidth:</b>	<input type="text" value="100"/>	<input type="text" value="1000"/>

Figure 4-55

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

**Other configurations for the entries as shown in Figure 4-54:**

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.

## 4.12 IP & MAC Binding

Choose menu **IP & MAC Binding**, the next submenus are shown below.

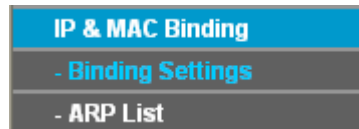


Figure 4-56

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 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 4-57).

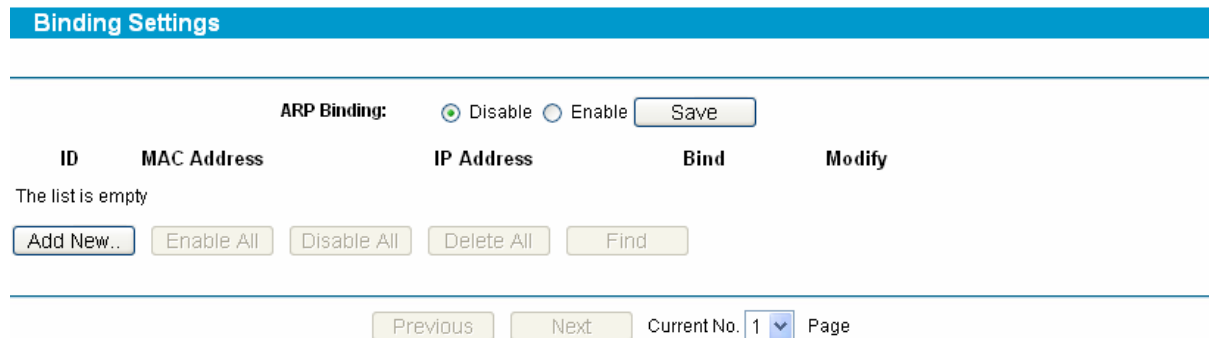


Figure 4-57

- **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**.../Edit shown in Figure 4-57, you will see a new screen shown in Figure 4-58.

**Step 2:** Enter the MAC Address and IP Address in the corresponding field.



Figure 4-58

**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 4-57, you will see a new screen shown in Figure 4-59.

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

Find IP & MAC Binding Entry

---

MAC Address:

IP Address:

ID	MAC Address	IP Address	Bind	Link
Now the current list is empty.				

---

Figure 4-59

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

Find IP & MAC Binding Entry

---

MAC Address:

IP Address:

ID	MAC Address	IP Address	Bind	Link
1	00-E0-4C-00-07-BE	192.168.0.4	<input checked="" type="checkbox"/>	<a href="#">To page</a>

---

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

 **Note:**

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

**Other configurations for the entries as shown in Figure 4-57:**

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.

### 4.12.2 ARP List

Choose menu **IP & MAC Binding**→**ARP List**, you can view the ARP list in the next screen (shown in Figure 4-60). This screen displays the ARP list, it shows all the existing IP & MAC Binding entries.

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

ARP List				
ID	MAC Address	IP Address	Status	Configure
1	00-E0-4C-00-07-BE	192.168.0.4	Bound	<input type="button" value="Load"/> <input type="button" value="Delete"/>
2	00-19-66-19-40-7F	192.168.0.121	Unbound	<input type="button" value="Load"/> <input type="button" value="Delete"/>

Figure 4-60

Click **Load** to load the specific item to the IP & MAC Binding list (shown in Figure 4-57).

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 4-57).

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.

## 4.13 Dynamic DNS

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

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

### 4.13.1 Dyndns DDNS

If your dynamic DNS Service Provider is [www.dyndns.org](http://www.dyndns.org), you can configure in the next screen (shown in Figure 4-61).

## DDNS

---

<b>Service Provider:</b>	Dyndns ( www.dyndns.org )	<a href="#">Go to register...</a>
<b>User Name:</b>	username	
<b>Password:</b>	●●●●●●	
<b>Domain Name:</b>		
	<input type="checkbox"/> Enable DDNS	
<b>Connection Status:</b>	DDNS not launching!	
	<input type="button" value="Login"/>	<input type="button" value="Logout"/>

---

Figure 4-61

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

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

**Step 1:** Type the “User Name” and “Password” for your DDNS account.

**Step 2:** Enter the domain name that your dynamic DNS service provider offers.

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

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

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

#### 4.13.2 PeanutHull DDNS

If your dynamic DNS Service Provider is [www.oray.net](http://www.oray.net), you can configure in the next screen (shown in Figure 4-62).

---

<b>Service Provider:</b>	PeanutHull ( www.oray.com )	<a href="#">Go to register...</a>
<b>User Name:</b>	username	
<b>Password:</b>	●●●●●●	
	<input type="checkbox"/> Enable DDNS	
<b>Connection Status:</b>	DDNS not launching!	
<b>Service Type:</b>	---	
<b>Domain Name:</b>	NULL	
	<input type="button" value="Login"/>	<input type="button" value="Logout"/>

---

Figure 4-62

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

**Step 1:** Type the User Name and Password for your DDNS account.

**Step 2:** Enable DDNS, and click **Save** to save the current configuration.

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

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

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

### 4.13.3 Comexe DDNS

If your dynamic DNS Service Provider is [www.comexe.cn](http://www.comexe.cn), you can configure in the next screen (shown in Figure 4-63).

The screenshot shows a web interface for configuring DDNS. At the top, there is a blue header with the text "DDNS". Below the header, the "Service Provider" is set to "Comexe ( www.comexe.cn )" with a dropdown arrow and a "Go to register..." link. The "User Name" field contains "username" and the "Password" field is masked with dots. There is an unchecked checkbox for "Enable DDNS". The "Connection Status" field displays "DDNS not launching!". The "Domain Name" field is set to "NULL". At the bottom, there are "Login" and "Logout" buttons, and a "Save" button is centered below a horizontal line.

Figure 4-63

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

**Step 1:** Enter the **User Name** for your DDNS account.

**Step 2:** Enter the **Password** for your DDNS account.

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

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

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

**Note:**

If you want to login again with another account after a successful login, please click the **Logout** button, then input your new username and password and click the **Login** button.

### 4.13.4 No-IP DDNS

If your dynamic DNS Service Provider is [www.no-ip.com](http://www.no-ip.com), you can configure in the next screen (shown in Figure 4-64).

## DDNS

---

**Service Provider:** No-IP ( www.no-ip.com )

**User Name:**

**Password:**

**Domain Name:**

Enable DDNS

**Connection Status:** DDNS not launching!

---

Figure 4-64

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

**Step 1** Type the “**User Name**” and “**Password**” for your DDNS account.

**Step 2** Enter the **Domain Name** your dynamic DNS service provider offered.

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

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

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

## 4.14 System Tools

Choose menu “**System Tools**”, and you can see the submenus under the main menu:

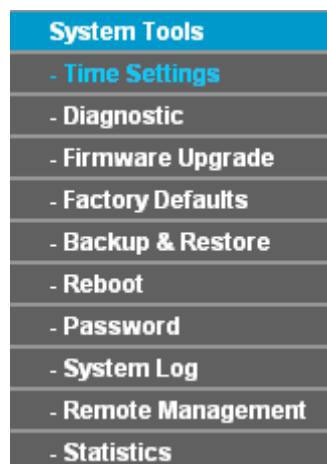


Figure 4-65

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

### 4.14.1 Time Settings

Choose menu **System Tools**→**Time Settings**, you can configure the time on the screen (shown in Figure 4-66).



## Time Settings

Time zone: (GMT+08:00) Beijing, Hong Kong, Perth, Singapore ▼

Date: 1 1 2013 (MM/DD/YY)

Time: 0 2 32 (HH/MM/SS)

NTP Server I: 0.0.0.0 (Optional)

NTP Server II: 0.0.0.0 (Optional)

Enable Daylight Saving

Start: Mar 3rd Sun 2am

End: Nov 2nd Sun 3am

Daylight Saving Status: daylight saving is down.

Note: Click the "GET GMT" to update the time from the internet with the pre-defined servers or entering the customized server (IP Address or Domain Name) in the above frames.

Figure 4-66

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

#### To configure the system time manually:

**Step 1:** Select your local time zone.

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

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

#### To configure the system automatically:

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

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

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

#### To set up daylight saving:

**Step 1:** Select the **Enable Daylight Saving** checkbox to enable daylight saving function.

**Step 2:** Select the correct **Start** time and **End** time of daylight saving range.

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

 **Note:**

- 1). This setting will be used for some time-based functions such as firewall. You must specify your time zone once you login to the router successfully, or else, the time limited on these functions will not take effect.
- 2). The time will be lost if the router is turned off.
- 3). The router will obtain GMT time automatically from Internet if it has already connected to the Internet.
- 4). In daylight saving configuration, start time and end time shall be within one year and start time shall be earlier than end time.
- 5). After you enable daylight saving function, it will take action in one minute.

#### 4.14.2 Diagnostic Tools

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

Diagnostic Tools

---

**Diagnostic Parameters**

**Diagnostic Tool:**  Ping  Traceroute

**IP Address/ Domain Name:**

**Ping Count:**  (1-50)

**Ping Packet Size:**  (4-1472 Bytes)

**Ping Timeout:**  (100-2000 Milliseconds)

**Traceroute Hops:**  (1-30)

**Diagnostic Results**

The Router is ready.

Figure 4-67

- **Diagnostic Tool** - Choose the diagnostic tool. **Ping** and **Tracert** are available.
- **IP address/Domain Name** - Enter destination IP address or Domain name here.
- **Ping Count** -Indicates the number of Echo Request messages sent. The default is 4.
- **Ping Packet Size** - Indicates the data field length of ping packet.
- **Ping Timeout** - Indicates the time before the Ping timeout.
- **Traceroute Hops** – Specify the maximum hops of the Traceroute here.

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

**Note:**

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

### 4.14.3 Firmware

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

**Firmware Upgrade**

**File:**

**Firmware Version:** 1.2.1 Build 130831 Rel.63039n

**Hardware Version:** R600VPN v2.00000000

Figure 4-68

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

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

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

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

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

**Note:**

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

#### 4.14.4 Factory Defaults

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

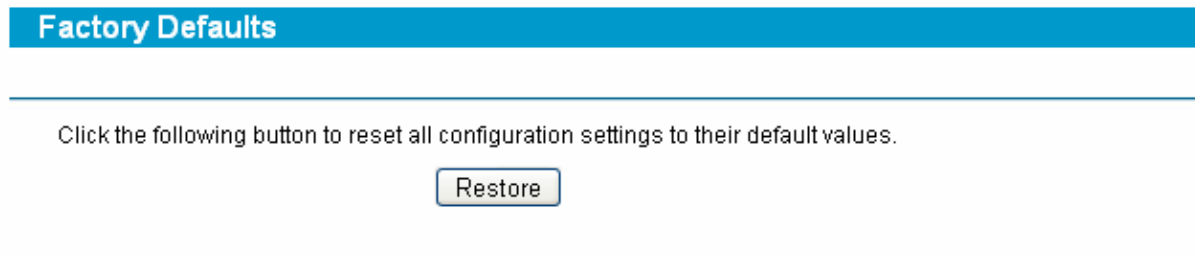


Figure 4-69

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

 **Note:**

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

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

#### 4.14.5 Backup and Restore

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



Figure 4-70

**To back up the router's current settings:**

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

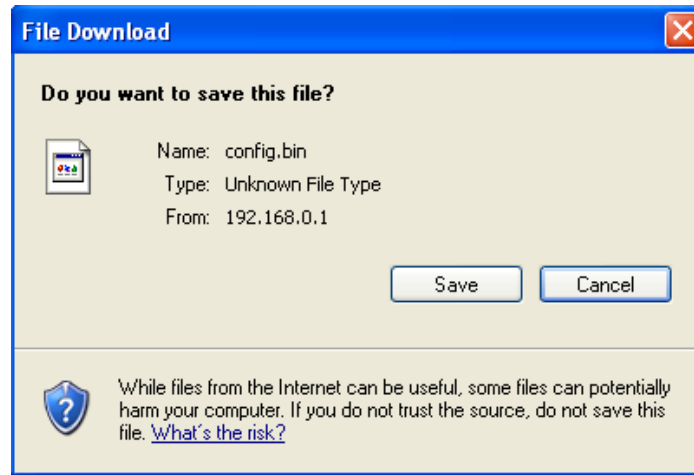


Figure 4-71

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

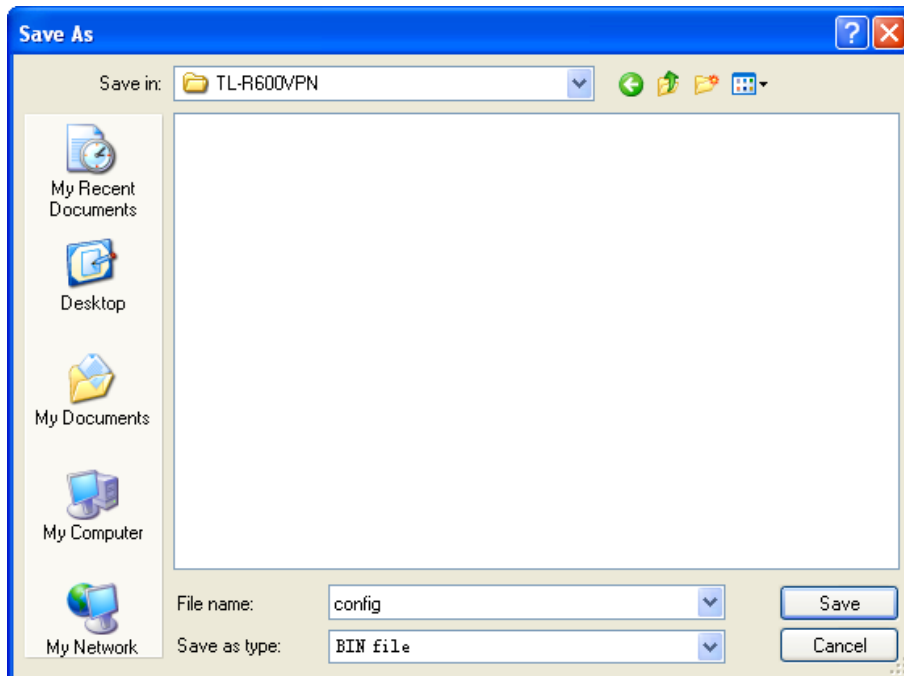


Figure 4-72

**To restore the router's settings:**

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

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

#### 4.14.6 Reboot

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

## Reboot

Click this button to reboot the device.

Reboot

Figure 4-73

### Note:

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

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

### 4.14.7 Password

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

## Password

The username and password must not exceed 14 characters in length and must not include any spaces!

Old User Name:	<input type="text"/>
Old Password:	<input type="text"/>
New User Name:	<input type="text"/>
New Password:	<input type="text"/>
Confirm New Password:	<input type="text"/>

Save

Clear All

Figure 4-74

### Note:

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

- 3) You can click the **Clean All** button to clean all the configurations.

#### 4.14.8 System Log

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

System Log

---

**Auto Mail Feature:** Disabled Mail Settings

**Log Type:** All ▼ **Log Level:** ALL ▼

Index	Time	Type	Level	Log Content
1	Nov 9 10:52:11	OTHER	INFO	User clear system log.

**Time = 2011-11-09 10:52:11 429472s**  
**H-Ver = R600VPN v1 00000000 : S-Ver = 1.0.0 Build 111028 Rel.51449n**  
**L = 192.168.0.1 : M = 255.255.255.0**  
**W1 = DHCP : W = 192.168.2.4 : M = 255.255.255.0 : G = 192.168.2.1**

Refresh
Save Log
Mail Log
Clear Log

---

Previous
Next
Current No. 1 ▼ Page

Figure 4-75

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

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

Click the **Save Log** button to save all the logs in a text file.

Click the **Mail Log** button to send the logs to the specified mailbox.

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

#### 4.14.9 Remote Management

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

Remote Management

---

**Web Management Port:**

**Remote Management IP Address:**  (Enter 255.255.255.255 for all)

Save

Figure 4-76

- **Web Management Port** - Web browser access normally uses the standard HTTP service port 80. This router's default remote management web port number is 80. For greater security, you can change the remote management web interface to a custom port by entering that number in the box provided. Choose a number between 1024 and 65534, but do not use the number of any common service port.
- **Remote Management IP Address** - This is the current address you will use when accessing your router from the Internet. The default IP address is 0.0.0.0. It means this function is disabled. To enable this function, change the default IP address to another IP address as desired.

 **Note:**

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

#### 4.14.10 Statistics

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

Statistics

---

**Current Statistics Status:** Disabled

**Packets Statistics Interval(5~60):**  Seconds

Auto-refresh

**Sorted Rules:**

IP Address/ MAC Address	Total		Current			Modify
	Packets	Bytes	Packets	Bytes	ICMP Tx UDP Tx SYN Tx	
The current list is empty.						

entries per page. Current No.  page

Figure 4-77

- **Current Statistics Status** - Enable or Disable the statistics function. The default status is disabled. Click the **Enable** button to use the function. Click the **Disable** button to disable the function.



- **Packets Statistics Interval** - The default value is 10. Select a value between 5 and 60 seconds in the pull-down list. The Packets Statistic interval value indicates the time section of the packets statistic.
- **Sort Rules** - Select the rule for displaying the traffic information.
- **Statistics Table** - This table displays the statistics information about the traffic.

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

 **Note:**

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

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

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

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

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

## Appendix A: Specifications

<b>General</b>	
Standards and Protocols	IEEE 802.3, IEEE 802.3u, IEEE 802.3ab, TCP/IP, DHCP, ICMP, NAT, PPPoE, SNTP, HTTP, DNS
Safety & Emission	FCC, CE
Ports	One 10/100/1000Mbps Auto-Negotiation WAN RJ45 port Four 10/100/1000Mbps Auto-Negotiation LAN RJ45 ports
Cabling Type	10BASE-T: UTP category 3, 4, 5 cable (maximum 100m) EIA/TIA-568 100Ω STP (maximum 100m) 100BASE-TX: UTP category 5, 5e cable (maximum 100m) EIA/TIA-568 100Ω STP (maximum 100m) 1000BASE-T: UTP/STP of Category 5, 5e, 6 or above (maximum 100m)
<b>Physical and Environment</b>	
Working Temperature	0°C~40°C (32°F~104°F)
Working Humidity	10% - 90% RH, Non-condensing

## Appendix B: Preventing Lightning

To avoid damage during a lightning storm and ensure a stable performance, our router has adopted the professional lightning protection technology to prevent the lightning. However, although these measures have been taken to protect TL-R600VPN from lightning, if the lightning intensity exceeds a certain range, damage to the router may still happen. To protect the router from lightning better, the following should be considered:

- 1) Communication cable should be kept indoors as much as possible to reduce the possibility of equipment damage due to lightning.
- 2) If the Ethernet cable is designed for use indoors, under normal circumstances, the router should not be used outdoors.
- 3) Ensure the ground point of the socket of AC power supply is well grounded.
- 4) To enhance the lightning protection capability of the power supply, a lightning arrester could be installed at the input end of the power supply. Please read the User Manual of the arrester carefully before installing it.
- 5) As for the signal line to which the interface modules of TL-R600VPN are connected, such as LAN's Ethernet cable, ISDN line, telephone line, E1/T1 line, etc, a special lightning arrester should be installed at the input end of the signal line to enhance the lightning protection capability. Please read the User Manual of the arrester carefully before installing it.

 **Note:**

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

## Appendix C: FAQ

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

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

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

**Step 3:** Login to the router, click the menu **Network→WAN** on the left of your browser. On the WAN screen, select **“PPPoE/Russia 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 Connection:**

**User Name:**

**Password:**

**Confirm Password:**

Figure 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:**

Connect on Demand  
Max Idle Time:  minutes (0 means remain active at all times.)

Connect Automatically

Time-based Connecting  
Period of Time: from  :  (HH:MM) to  :  (HH:MM)

Connect Manually  
Max Idle Time:  minutes (0 means remain active at all times.)

---

Figure 2

**Note:**

- 1) Sometimes the connection cannot 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

WAN MAC Address:	<input type="text" value="00-0A-EB-13-7B-01"/>	<input type="button" value="Restore Factory MAC"/>
Your PC's MAC Address:	<input type="text" value="40-61-86-FC-75-C3"/>	<input type="button" value="Clone MAC Address"/>

Figure 3

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

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

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

### Method one: Use Virtual Server

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

Virtual Servers					
ID	Service Port	IP Address	Protocol	Status	Modify
1	21	192.168.0.100	TCP	Enabled	<a href="#">Modify</a> <a href="#">Delete</a>
2	80	192.168.0.101	TCP	Enabled	<a href="#">Modify</a> <a href="#">Delete</a>
3	1720	192.168.0.102	ALL	Enabled	<a href="#">Modify</a> <a href="#">Delete</a>

Figure 4

 **Note:**

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

**Method two: Use DMZ Host**

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

DMZ	
<b>Current DMZ Status:</b>	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled
<b>DMZ Host IP Address:</b>	<input type="text" value="192.168.0.102"/>
<input type="button" value="Save"/>	

Figure 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 **System Tools**→**Remote Management**. On the Remote Management screen, enter a port number except 80 (such as 88) into the "**Web Management Port**" field. Click **Save** and the router will reboot.

## Remote Management

<b>Web Management Port:</b>	<input type="text" value="88"/>
<b>Remote Management IP Address:</b>	<input type="text" value="255.255.255.255"/>

Figure 6

### Note:

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

Address	<input type="text" value="192.168.0.1:88"/>
---------	---------------------------------------------

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

## Virtual Servers

ID	Service Port	IP Address	Protocol	Status	Modify
1	21	192.168.0.100	TCP	Enabled	<a href="#">Modify</a> <a href="#">Delete</a>
2	80	192.168.0.101	TCP	Enabled	<a href="#">Modify</a> <a href="#">Delete</a>
3	1720	192.168.0.102	ALL	Enabled	<a href="#">Modify</a> <a href="#">Delete</a>

Figure 7

## Appendix D: Glossary

- **DDNS (Dynamic Domain Name System)** - The capability of assigning a fixed host and domain name to a dynamic Internet IP address.
- **DHCP (Dynamic Host Configuration Protocol)** - A protocol that automatically configure the TCP/IP parameters for the all the PCs that are connected to a DHCP server.
- **DMZ (Demilitarized Zone)** - A Demilitarized Zone allows one local host to be exposed to the Internet for a special-purpose service such as Internet gaming or videoconferencing.
- **DNS (Domain Name Server)** - An Internet Server that translates the names of websites into IP addresses.
- **Domain Name** - A descriptive name for an address or group of addresses on the Internet.
- **DoS (Denial of Service)** - A hacker attack designed to prevent your computer or network from operating or communicating.
- **DSL (Digital Subscriber Line)** - 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.