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 © 2011 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.
Package Contents

The following items should be found in your box:

- One TL-R600VPN SafeStream™ Gigabit Broadband VPN Router
- One power cord for TL-R600VPN SafeStream™ Gigabit Broadband VPN Router
- One Resource CD for TL-R600VPN SafeStream™ Gigabit Broadband VPN Router, including:
  - This User Guide
  - Other Helpful Information

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

Chapter 1. Introduction ........................................................................................................ 1
  1.1 Overview of the Router .................................................................................................. 1
  1.2 Features ....................................................................................................................... 1
  1.3 Conventions ................................................................................................................. 1

Chapter 2. Hardware installation ...................................................................................... 2
  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

Chapter 3. Quick Installation Guide .................................................................................. 6
  3.1 Configure PC ............................................................................................................... 6
  3.2 Login .......................................................................................................................... 9

Chapter 4. Configuring the Router .................................................................................... 13
  4.1 Status ......................................................................................................................... 13
  4.2 Quick Setup ............................................................................................................... 15
  4.3 Network ...................................................................................................................... 15
    4.3.1 WAN ...................................................................................................................... 15
    4.3.2 LAN ...................................................................................................................... 24
    4.3.3 MAC Clone ........................................................................................................... 25
  4.4 DHCP ......................................................................................................................... 26
    4.4.1 DHCP Settings ...................................................................................................... 26
    4.4.2 DHCP Clients List ................................................................................................. 27
    4.4.3 Address Reservation ............................................................................................ 27
  4.5 Forwarding .................................................................................................................. 29
    4.5.1 Virtual Servers ..................................................................................................... 29
    4.5.2 Port Triggering ...................................................................................................... 31
    4.5.3 DMZ ..................................................................................................................... 33
    4.5.4 UPnP .................................................................................................................... 33
  4.6 Security ...................................................................................................................... 34
    4.6.1 Basic Security ...................................................................................................... 34
    4.6.2 Advanced Security ............................................................................................... 36
    4.6.3 Local Management .............................................................................................. 37
  4.7 Access Control .......................................................................................................... 37
    4.7.1 Rule ....................................................................................................................... 38
    4.7.2 Host ....................................................................................................................... 39
4.7.3 Target .............................................................................................................................40
4.7.4 Schedule ........................................................................................................................41
4.8 IPsec VPN ........................................................................................................................42
  4.8.1 IKE ..................................................................................................................................42
  4.8.2 IPsec ...............................................................................................................................44
  4.8.3 SA List ............................................................................................................................48
4.9 PPTP VPN Server ....................................................................................................... 49
  4.9.1 Server Settings ...........................................................................................................49
  4.9.2 Account Settings ............................................................................................................50
  4.9.3 Connection Status .........................................................................................................51
4.10 Static Routing .............................................................................................................. 51
4.11 Bandwidth Control ...................................................................................................52
  4.11.1 Control Settings ...........................................................................................................52
  4.11.2 Rule List .......................................................................................................................53
4.12 IP & MAC Binding ........................................................................................................54
  4.12.1 Binding Setting ...........................................................................................................54
  4.12.2 ARP List .......................................................................................................................56
4.13 Dynamic DNS ...............................................................................................................57
  4.13.1 Dyndns DDNS ...........................................................................................................57
  4.13.2 PeanutHull DDNS ......................................................................................................58
  4.13.3 Comexe DDNS ...........................................................................................................58
  4.13.4 No-IP DDNS ...............................................................................................................59
4.14 System Tools ...............................................................................................................60
  4.14.1 Time Settings .............................................................................................................61
  4.14.2 Diagnostic Tools ........................................................................................................62
  4.14.3 Firmware ......................................................................................................................62
  4.14.4 Factory Defaults .........................................................................................................63
  4.14.5 Backup and Restore ....................................................................................................64
  4.14.6 Reboot ........................................................................................................................65
  4.14.7 Password ....................................................................................................................66
  4.14.8 System Log ................................................................................................................66
  4.14.9 Remote Management .................................................................................................67
  4.14.10 Statistics ..................................................................................................................68

Appendix A: Specifications ................................................................................... 70
Appendix B: Preventing Lightning ....................................................................... 71
Appendix C: FAQ .................................................................................................... 72
Appendix D: Glossary ............................................................................................. 76
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).

LED Descriptions:

<table>
<thead>
<tr>
<th>Name</th>
<th>Status</th>
<th>Indication</th>
</tr>
</thead>
<tbody>
<tr>
<td>PWR</td>
<td>Not lit</td>
<td>The router is powered off.</td>
</tr>
<tr>
<td></td>
<td>Lit up (Green)</td>
<td>The router is powered on.</td>
</tr>
<tr>
<td>SYS</td>
<td>Not lit</td>
<td>The router has a hardware error.</td>
</tr>
<tr>
<td></td>
<td>Lit up (Green)</td>
<td>The router has a hardware error.</td>
</tr>
<tr>
<td></td>
<td>Flashing (Green)</td>
<td>The router works properly.</td>
</tr>
<tr>
<td></td>
<td>Flashing (Green/Yellow)</td>
<td>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.)</td>
</tr>
<tr>
<td>WAN, LAN</td>
<td>Lit up (Green/Yellow)</td>
<td>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.)</td>
</tr>
</tbody>
</table>

2.1.2 The Rear Panel

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

- **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.
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.

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. 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).

Step 2: In the next screen, right click Local Area Connection (LAN), and then select Properties.
Step 3: In the next screen, select **General** tab, highlight Internet Protocol (TCP/IP), and then click the **Properties** button.
Step 4: Configure the IP address as shown in Figure 3-4. After that, click OK.

![Internet Protocol (TCP/IP) Properties](image)

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.

![Ping output](image)

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.

```
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.
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](image)

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

![Quick Setup - WAN Connection Type](image)
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...

![Figure 3-10](image)

**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: 

![Figure 3-11](image)

**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: 0.0.0.0
Subnet Mask: 0.0.0.0
Default Gateway: 0.0.0.0 (Optional)
Primary DNS: 0.0.0.0 (Optional)
Secondary DNS: 0.0.0.0 (Optional)

![Figure 3-12](image)
Step 7: After that, you will see the next screen. Click Finish to complete the quick installation.

Congratulations! The Router is now connecting you to the Internet. For detail settings, please click other menus if necessary.
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 though 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.
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.

![Network Menu](image)

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.
### 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 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.

<table>
<thead>
<tr>
<th><strong>WAN Connection Type:</strong></th>
<th>Static IP</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>IP Address:</strong></td>
<td>192.168.0.200</td>
</tr>
<tr>
<td><strong>Subnet Mask:</strong></td>
<td>255.255.255.0</td>
</tr>
<tr>
<td><strong>Default Gateway:</strong></td>
<td>192.160.0.1 (Optional)</td>
</tr>
<tr>
<td><strong>MTU Size (in bytes):</strong></td>
<td>1500 (The default is 1500, do not change unless necessary)</td>
</tr>
<tr>
<td><strong>Primary DNS:</strong></td>
<td>0.0.0.0 (Optional)</td>
</tr>
<tr>
<td><strong>Secondary DNS:</strong></td>
<td>0.0.0.0 (Optional)</td>
</tr>
</tbody>
</table>

**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.
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 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**

- **MTU Size (in bytes):** 1480 (The default is 1480, do not change unless necessary)
- **Service Name:**
- **AC Name:**
- **ISP Specified IP Address:** 0.0.0.0
- **Detect Online Interval:** 0 Seconds (0 ~ 120 seconds, the default is 0, 0 means not detecting)
- **Primary DNS:** 0.0.0.0
- **Secondary DNS:** 0.0.0.0 (Optional)

- **Use IP address specified by ISP**
- **Use the following DNS Servers**

**Figure 4-6**

- **MTU Size** - The default MTU size is 1480 bytes, which is usually fine. For some ISPs, you need modify the MTU. This should not be done unless you are sure it is necessary for your ISP.
- **Service Name/AC Name** - The service name and AC (Access Concentrator) name should not be configured unless you are sure it is necessary for your ISP.
ISP Specified IP Address - If you know that your ISP does not automatically transmit your IP address to the router during login, select Use IP Address specified by ISP and enter the IP address in dotted-decimal notation, which your ISP provided.

Detect Online Interval - The default value is 0, you can input the value between 0 and 120. The router will detect Access Concentrator online at every interval between the times. If the value is 0, it means the Router does not detect.

Primary DNS & Secondary DNS - If you know that your ISP does not automatically transmit DNS addresses to the router during login, select Use the following DNS servers and enter the address in dotted-decimal notation of your ISP’s primary DNS server. If a secondary DNS server address is available, enter it as well.

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

![Figure 4-7](image)

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 Connection Type:

| WAN Connection Type:  | L2TP/Radius L2TP |

#### User Name/Password

- **User Name:** Enter the User Name and Password provided by your ISP. These fields are case-sensitive.

#### Connect on Demand

- **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** - Connect automatically after the router is disconnected. To use this option, click the radio button.

#### Connect Manually

- **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.

---

**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.

![User Interface](image)

**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.

![LAN Configuration](image)

- **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**

<table>
<thead>
<tr>
<th>WAN MAC Address:</th>
<th>00-0A-EB-13-7B-01</th>
<th>Restore Factory MAC</th>
</tr>
</thead>
<tbody>
<tr>
<td>Your PC’s MAC Address:</td>
<td>4D-51-86-c0:75-c3</td>
<td>Clone MAC Address</td>
</tr>
</tbody>
</table>

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.

![DHCP menu]

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

- **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**: 192.168.0.100
- **End IP Address**: 192.168.0.199
- **Address Lease Time**: 120 minutes (1~2680 minutes, the default value is 120)
- **Default Gateway**: 192.168.0.1 (optional)
- **Default Domain**: (optional)
- **Primary DNS**: 0.0.0.0 (optional)
- **Secondary DNS**: 0.0.0.0 (optional)

![DHCP settings]

Click **Save**
- **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**

<table>
<thead>
<tr>
<th>ID</th>
<th>Client Name</th>
<th>MAC Address</th>
<th>Assigned IP</th>
<th>Lease Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>ann</td>
<td>0C-19-56-13-43-7F</td>
<td>192.168.0.100</td>
<td>01:59:59</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>ID</th>
<th>MAC Address</th>
<th>Reserved IP Address</th>
<th>Status</th>
<th>Modify</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>00-19-56-19-40-7F</td>
<td>192.168.0.100</td>
<td>Enabled</td>
<td>Modify Delete</td>
</tr>
</tbody>
</table>

- **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:** 00-19-56-19-40-7F
- **Reserved IP Address:** 192.168.0.100
- **Status:** Enabled

**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.

![Forwarding menu](image)

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](image)

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

**Step 1:** Click **Add New…/**Modify shown in Figure 4-18, 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**

<table>
<thead>
<tr>
<th>Service Port: 21</th>
<th>8080 or more</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP Address: 192.168.0.100</td>
<td></td>
</tr>
<tr>
<td>Protocol: TCP</td>
<td></td>
</tr>
<tr>
<td>Status: Enabled</td>
<td></td>
</tr>
<tr>
<td>Common Service Port: FTP</td>
<td></td>
</tr>
</tbody>
</table>

![Figure 4-19](image)

**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.

<table>
<thead>
<tr>
<th>ID</th>
<th>Trigger Port</th>
<th>Trigger Protocol</th>
<th>Incoming Port</th>
<th>Incoming Protocol</th>
<th>Status</th>
<th>Modify</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>6112</td>
<td>ALL</td>
<td>6112</td>
<td>ALL</td>
<td>Enabled</td>
<td>Modify</td>
</tr>
</tbody>
</table>

Add New...  Enable All  Disable All  Delete All

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

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Trigger Port:</td>
<td>6112</td>
</tr>
<tr>
<td>Trigger Protocol:</td>
<td>ALL</td>
</tr>
<tr>
<td>Incoming Port:</td>
<td>6112</td>
</tr>
<tr>
<td>Incoming Protocol:</td>
<td>ALL</td>
</tr>
<tr>
<td>Status:</td>
<td>Enabled</td>
</tr>
<tr>
<td>Common Applications:</td>
<td>Bottle not</td>
</tr>
</tbody>
</table>

**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.

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.
Current UPnP Status: Enabled

Current UPnP Settings List

<table>
<thead>
<tr>
<th>ID</th>
<th>App Description</th>
<th>External Port</th>
<th>Protocol</th>
<th>Internal Port</th>
<th>IP Address</th>
<th>Status</th>
</tr>
</thead>
</table>

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.

#### 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 or Disable

VPN

PPTP Passthrough: Enable or Disable
L2TP Passthrough: Enable or Disable
IPSec Passthrough: Enable or Disable

ALG

FTP ALG: Enable or Disable
TFTP ALG: Enable or Disable
H323 ALG: Enable or Disable
RTSP ALG: Enable or 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):**
  - **DoS Attack Defense:**
    - Disable
    - Enable

- **Enable ICMP-FLOOD Attack Filtering**
  - **ICMP-FLOOD Packets Threshold (5 - 3600):** 50 Packets/s

- **Enable UDP-FLOOD Filtering**
  - **UDP-FLOOD Packets Threshold (5 - 3600):** 500 Packets/s

- **Enable TCP-SYN-FLOOD Attack Filtering**
  - **TCP-SYN-FLOOD Packets Threshold (5 - 3600):** 50 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).

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

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.

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**

<table>
<thead>
<tr>
<th>ID</th>
<th>Rule Name</th>
<th>Host</th>
<th>Target</th>
<th>Schedule</th>
<th>Action</th>
<th>Status</th>
<th>Modify</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>test</td>
<td>1</td>
<td>Any</td>
<td>Permanent</td>
<td>Deny</td>
<td>Enabled</td>
<td>Edit</td>
</tr>
</tbody>
</table>

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.
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).

<table>
<thead>
<tr>
<th>ID</th>
<th>Host Description</th>
<th>Information</th>
<th>Modify</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td></td>
<td>IP: 192.168.0.102 - 192.168.0.110</td>
<td>Edit Delete</td>
</tr>
</tbody>
</table>

- **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.

**Add or Modify a Host Entry**

<table>
<thead>
<tr>
<th>Mode:</th>
<th>IP Address:</th>
<th>Host Description:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**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).

**Target Settings**

<table>
<thead>
<tr>
<th>ID</th>
<th>Target Description</th>
<th>Information</th>
<th>Modify</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**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.
Add or Modify an Access Target Entry

<table>
<thead>
<tr>
<th>Mode</th>
<th>IP Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>Target Description</td>
<td></td>
</tr>
<tr>
<td>IP Address</td>
<td></td>
</tr>
<tr>
<td>Target Port</td>
<td></td>
</tr>
<tr>
<td>Protocol</td>
<td>ALL</td>
</tr>
<tr>
<td>Common Service Port</td>
<td>--please select--</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>ID</th>
<th>Schedule Description</th>
<th>Day</th>
<th>Time</th>
<th>Modify</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1</td>
<td>Every Day</td>
<td>00:00 - 24:00</td>
<td>Edit Delete</td>
</tr>
</tbody>
</table>

- **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

- **Schedule Description:**
- **Days:** Everyday □ Select Days
  - Mon □ Tue □ Wed □ Thu □ Fri □ Sat □ Sun
- **Time:** all day 24 hours □
- **Start Time:** (HH:MM)
- **Stop Time:** (HH:MM)

![Figure 4-36](image)

**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.

- **IPsec VPN**
  - IKE
  - IPsec
  - SA List

![Figure 4-37](image)

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).
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

<table>
<thead>
<tr>
<th>Policy Name:</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Exchange Mode:</td>
<td><img src="on" alt="Main" /> <img src="off" alt="Aggressive" /></td>
</tr>
<tr>
<td>Authentication Algorithm:</td>
<td>AUTO</td>
</tr>
<tr>
<td>Encryption Algorithm:</td>
<td>AUTO</td>
</tr>
<tr>
<td>DH Groups:</td>
<td>DH2</td>
</tr>
<tr>
<td>Pre-shared Key:</td>
<td></td>
</tr>
<tr>
<td>SA Lifetime:</td>
<td>26800 seconds (60-604800)</td>
</tr>
<tr>
<td>DPD:</td>
<td><img src="on" alt="Enable" /> <img src="off" alt="Disable" /></td>
</tr>
</tbody>
</table>

![Figure 4-39](image)

**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

<table>
<thead>
<tr>
<th>ID</th>
<th>Policy Name</th>
<th>Local Subnet</th>
<th>Remote Subnet</th>
<th>Exchange Mode</th>
<th>Status</th>
<th>Modify</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>policy1</td>
<td>192.168.2.0/24</td>
<td>192.168.1.0/24</td>
<td>IKE</td>
<td>Enabled</td>
<td>Modify, Delete</td>
</tr>
</tbody>
</table>

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.

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

| Policy Name: |  |
| Local Subnet: |  / |
| Remote Subnet: |  / |
| Remote Gateway: | (IP or domain name) |
| Exchange Mode: | □ IKE □ Manual |
| Security Protocol: | ESP |
| Authentication Algorithm: | AUTO |
| Encryption Algorithm: | AUTO |
| IKE Security Policy: | policy1 □ |
| PFS Group: | NONE |
| PFS Lifetime: | 26880 seconds (60-86400) |
| Status: | Enable |

![Figure 4-41](Image)

- **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”.


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


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

<table>
<thead>
<tr>
<th>ID</th>
<th>Name</th>
<th>SPI</th>
<th>Tunnel Initiator</th>
<th>Tunnel Receiver</th>
<th>Security Protocol</th>
<th>AH Auth</th>
<th>ESP Auth</th>
<th>ESP Encr</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Now the list is empty.

![Refresh Button](image)

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.

![PPTP VPN Server Menu](image)

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).

![PPTP Server Settings](image)

Figure 4-44

- **PPTP Server** – Enable or disable the PPTP Server.
- **MPPE Encryption** – Enable or disable MPPE Encryption.
- **IP Range Start** – Enter the start IP address: 192.168.0.200.
- **IP Range End** – Enter the end IP address: 192.168.0.215.

[Save Button]
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

<table>
<thead>
<tr>
<th>ID</th>
<th>Account</th>
<th>Status</th>
<th>Modify</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>123456</td>
<td>Enabled</td>
<td>Modify Delete</td>
</tr>
</tbody>
</table>

- **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

<table>
<thead>
<tr>
<th>Account:</th>
<th>123456</th>
</tr>
</thead>
<tbody>
<tr>
<td>Password:</td>
<td>******</td>
</tr>
<tr>
<td>Confirm Password:</td>
<td>******</td>
</tr>
<tr>
<td>Status:</td>
<td>Enabled</td>
</tr>
</tbody>
</table>

**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).

#### 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 Static Routing

Choose menu “**Static Routing**”, you can configure the static route in the next screen (shown in Figure 4-48). A static route is a pre-determined path that network information must travel to reach a specific host or network.

#### Figure 4-48

- **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 4-48, you will see a new screen shown in Figure 4-49.

**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

<table>
<thead>
<tr>
<th>Destination IP Address:</th>
<th>222.88.88.100</th>
</tr>
</thead>
<tbody>
<tr>
<td>Subnet Mask:</td>
<td>255.255.255.0</td>
</tr>
<tr>
<td>Default Gateway:</td>
<td>222.88.88.1</td>
</tr>
<tr>
<td>Status:</td>
<td>Enabled</td>
</tr>
</tbody>
</table>

![Figure 4-49](image)

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

 совершила

**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 4-48.*

- 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.

### 4.11 Bandwidth Control

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

![Figure 4-50](image)

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 "Control Settings", you can configure the Egress Bandwidth and Ingress Bandwidth in the next screen (shown in Figure 4-51).
Bandwidth Control Settings

Enable Bandwidth Control: [ ]

Line Type:  [ ] ADSL  [ ] Other

Egress Bandwidth:  512 Kbps
Ingress Bandwidth:  2048 Kbps

Save

Figure 4-51

- **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

**Bandwidth Control Rules List**

<table>
<thead>
<tr>
<th>ID</th>
<th>Description</th>
<th>Egress Bandwidth (Kbps)</th>
<th>Ingress Bandwidth (Kbps)</th>
<th>Enable</th>
<th>Modify</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>192.168.0.100 - 192.168.0.199</td>
<td>Min: 100, Max: 1000</td>
<td>Min: 100, Max: 1000</td>
<td>✔️</td>
<td>Modify Delete</td>
</tr>
</tbody>
</table>

Add New  Delete All

Figure 4-52

- **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 4-52, you will see a new screen shown in Figure 4-53

**Step 2:** Enter the information like the screen shown below.
**Bandwidth Control Rule Settings**

Enable: [ ]

**IP Range:**

192.168.0.100 - 192.168.0.199

**Port Range:**

21 -

**Protocol:**

ALL

<table>
<thead>
<tr>
<th>Min Bandwidth(Kbps)</th>
<th>Max Bandwidth(Kbps)</th>
</tr>
</thead>
<tbody>
<tr>
<td>100</td>
<td>1000</td>
</tr>
<tr>
<td>100</td>
<td>1000</td>
</tr>
</tbody>
</table>

[Save] [Back]

Figure 4-53

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

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

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 4-54](image)

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 4-55).

![Figure 4-55](image)
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 4-55, you will see a new screen shown in Figure 4-56.

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

IP & MAC Binding Settings

<table>
<thead>
<tr>
<th>Bind</th>
<th>MAC Address:</th>
<th>IP Address:</th>
</tr>
</thead>
<tbody>
<tr>
<td>✓</td>
<td>00-E0-4C-00-07-BE</td>
<td>192.168.0.4</td>
</tr>
</tbody>
</table>

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 4-55, you will see a new screen shown in Figure 4-57.

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

Find IP & MAC Binding Entry

<table>
<thead>
<tr>
<th>ID</th>
<th>MAC Address</th>
<th>IP Address</th>
<th>Bind</th>
<th>Link</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Figure 4-57

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

Note:

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

Other configurations for the entries as shown in Figure 4-55:

- 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 4-58). 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

<table>
<thead>
<tr>
<th>ID</th>
<th>MAC Address</th>
<th>IP Address</th>
<th>Status</th>
<th>Configure</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>00-E0-4C-00-07-BE</td>
<td>192.168.0.4</td>
<td>Bound</td>
<td>[Load]</td>
</tr>
<tr>
<td>2</td>
<td>00-19-66-19-40-TF</td>
<td>192.168.0.121</td>
<td>Unbound</td>
<td>[Load]</td>
</tr>
</tbody>
</table>

Figure 4-58

Click **Load** to load the specific item to the IP & MAC Binding list (shown in Figure 4-55).
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 4-55).
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 4-59).

![DDNS Configuration](http://example.com/ddns.png)

**Service Provider:**

- Dyndns ([www.dyndns.org](http://www.dyndns.org))

**User Name:**

- username

**Password:**

- ********

**Domain Name:**

- 

**Enable DDNS**

**Connection Status:**

- DDNS not launching!

- Login

- Logout

**Save**

Figure 4-59

**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, you can configure in the next screen (shown in Figure 4-60).

![Figure 4-60](Image)

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, you can configure in the next screen (shown in Figure 4-61).
To set up for Comexe DDNS, follow these instructions:

**Step 1:** Enter the domain name your dynamic DNS service provider offer.

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

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

Click **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.

### 4.13.4 No-IP DDNS

If your dynamic DNS Service Provider is **www.no-ip.com**, you can configure in the next screen (shown in Figure 4-62).
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:

![System Tools](image)

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 4-64).

**Time Settings**

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Time zone</td>
<td>(GMT+08:00) Beijing, Hong Kong, Perth, Singapore</td>
</tr>
<tr>
<td>Date</td>
<td>11 9 2011 (MM/DD/YY)</td>
</tr>
<tr>
<td>Time</td>
<td>14 20 0 (HH/MM/SS)</td>
</tr>
<tr>
<td>NTP Server 1</td>
<td>0.0.0.0 (Optional)</td>
</tr>
<tr>
<td>NTP Server 2</td>
<td>0.0.0.0 (Optional)</td>
</tr>
</tbody>
</table>

Note: Click the “GET GMT” button 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 4-64

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

To configure the system time manually:

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

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

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

To configure the system automatically:

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

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

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

**Note:**

1. This setting will be used for some time-based functions such as firewall. You must specify your time zone once you login to the router successfully, or else, the time limited on these functions will not take effect.
2. The time will be lost if the router is turned off.
3. The router will obtain GMT time automatically from Internet if it has already connected to the Internet.
4.14.2 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 or Tracert
- **IP Address/Domain Name**: 
- **Ping Count**: 4 (1-50)
- **Ping Packet Size**: 64 (4-1472 bytes)
- **Ping Timeout**: 800 (100-2000 milliseconds)
- **Traceroute Hops**: 3 (1-30)

**Diagnostic Results**

The Router is ready.

![Figure 4-65](image)

- **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 4-66).
Firmware Upgrade

- **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 4-67).

Factory Defaults

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

![Restore button](restore.png)

Figure 4-67

Click the **Restore** button to reset all configuration settings to their default values.
Note:
1) The default User Name is admin.
2) The default Password is admin.
3) The default IP Address is 192.168.0.1.
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).

**Backup & Restore**

<table>
<thead>
<tr>
<th>Backup:</th>
<th>Backup</th>
</tr>
</thead>
<tbody>
<tr>
<td>File:</td>
<td>Browse... Restore</td>
</tr>
</tbody>
</table>

**Figure 4-68**

To back up the Router’s current settings:

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

**Figure 4-69**

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

![Figure 4-70](Image)

> **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 4-72). 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: 

Old Password: 

New User Name: 

New Password: 

Confirm New Password: 

Save  Clear All

Figure 4-72

⚠️ 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.
Figure 4-73

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

Click the 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 4-74). This feature allows you to manage your Router from a remote location via the Internet.

- **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 4-75) displays the network traffic of each PC on LAN, including total traffic and current traffic of the last “Packets Statistic interval” seconds.

Table: Statistics

<table>
<thead>
<tr>
<th>Current Statistics Status:</th>
<th>Disabled</th>
<th>Enable</th>
</tr>
</thead>
<tbody>
<tr>
<td>Packets Statistics Interval(5-60):</td>
<td>10 Seconds</td>
<td>Auto-refresh</td>
</tr>
<tr>
<td>Sorted Rules:</td>
<td>Sorted by IP Address</td>
<td>Reset All</td>
</tr>
<tr>
<td>IP Address/MAC Address</td>
<td>Packets</td>
<td>Bytes</td>
</tr>
<tr>
<td>The current list is empty.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

5 entries per page Current No. 1 page

Figure 4-75

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

- 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.
<table>
<thead>
<tr>
<th>IP Address MAC Address</th>
<th>The IP address whose statistics information are displayed</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total</td>
<td>The total amount of packets received and transmitted by the router</td>
</tr>
<tr>
<td></td>
<td>The total amount of bytes received and transmitted by the router</td>
</tr>
<tr>
<td>Current</td>
<td>The total amount of packets received and transmitted in the last “Packets Statistic interval” seconds</td>
</tr>
<tr>
<td></td>
<td>The total amount of bytes received and transmitted in the last “Packets Statistic interval” seconds</td>
</tr>
<tr>
<td>ICMP Tx</td>
<td>The total amount of the ICMP packets transmitted to WAN in the last “Packets Statistic interval” seconds</td>
</tr>
<tr>
<td>UDP Tx</td>
<td>The total amount of the UDP packets transmitted to WAN in the last “Packets Statistic interval” seconds</td>
</tr>
<tr>
<td>TCP SYN Tx</td>
<td>The total amount of the TCP SYN packets transmitted to WAN in the last “Packets Statistic interval” seconds</td>
</tr>
</tbody>
</table>

**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

<table>
<thead>
<tr>
<th>General</th>
</tr>
</thead>
<tbody>
<tr>
<td>Standards and Protocols</td>
</tr>
<tr>
<td>Safety &amp; Emission</td>
</tr>
<tr>
<td>Ports</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>Cabling Type</td>
</tr>
</tbody>
</table>

### Physical and Environment

| Working Temperature | 0℃~40℃ (32℉~104℉) |
| Working Humidity | 10% - 90% RH, Non-condensing |
Appendix B: Preventing Lightning

To avoid damage during a lightning storm and ensure a stable performance, our router has adopted the professional lightning protection technology to prevent the lightning. However, although these measures have been taken to protect TL-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” for the type of WAN connection. Then enter the user name and password in the corresponding field, and finish it by clicking Connect.

   **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.

   **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

<table>
<thead>
<tr>
<th>WAN MAC Address:</th>
<th>00-0A-E8-13-7B-01</th>
<th>Restore Factory MAC</th>
</tr>
</thead>
<tbody>
<tr>
<td>Your PC’s MAC Address:</td>
<td>40-61-06-FD-75-C3</td>
<td>Clone MAC Address</td>
</tr>
</tbody>
</table>

![Figure 3](image)

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**.
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.

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

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

<table>
<thead>
<tr>
<th>Web Management Port</th>
<th>88</th>
</tr>
</thead>
<tbody>
<tr>
<td>Remote Management IP Address</td>
<td>255.255.255.255</td>
</tr>
</tbody>
</table>

Save

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 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 Table](image)

<table>
<thead>
<tr>
<th>ID</th>
<th>Service Port</th>
<th>IP Address</th>
<th>Protocol</th>
<th>Status</th>
<th>Modify</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>21</td>
<td>192.168.0.100</td>
<td>TCP</td>
<td>Enabled</td>
<td>Modify/Delete</td>
</tr>
<tr>
<td>2</td>
<td>80</td>
<td>192.168.0.101</td>
<td>TCP</td>
<td>Enabled</td>
<td>Modify/Delete</td>
</tr>
<tr>
<td>3</td>
<td>1720</td>
<td>192.168.0.102</td>
<td>ALL</td>
<td>Enabled</td>
<td>Modify/Delete</td>
</tr>
</tbody>
</table>

Add New... Enable All Disable All Delete All

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 configures the TCP/IP parameters for all PCs 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.