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.

FCC STATEMENT

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

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

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

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

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

FCC RF Radiation Exposure Statement

This equipment complies with FCC RF radiation exposure limits set forth for an uncontrolled environment. This device and its antenna must not be co-located or operating in conjunction with any other antenna or transmitter.

"To comply with FCC RF exposure compliance requirements, this grant is applicable to only Mobile Configurations. The antennas used for this transmitter must be installed to provide a separation distance of at least 20 cm from all persons and must not be co-located or operating in conjunction with any other antenna or transmitter."

CE Mark Warning

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

National Restrictions

2400.0-2483.5 MHz

Country	Restriction	Reason/remark
Bulgaria		General authorization required for outdoor use and public service
France	Outdoor use limited to 10 mW e.i.r.p. within the band 2454-2483.5 MHz	Military Radiolocation use. Refarming of the 2.4 GHz band has been ongoing in recent years to allow current relaxed regulation. Full implementation planned 2012
Italy		If used outside of own premises, general authorization is required
Luxembourg	None	General authorization required for network and service supply(not for spectrum)
Norway	Implemented	This subsection does not apply for the geographical area within a radius of 20 km from the centre of Ny-Ålesund
Russian Federation		Only for indoor applications

Package contents

The following contents should be found in your box:

- One TD-W8920G 108M Wireless ADSL2+ Router
- One DC power Adapter for TD-W8920G 108M Wireless ADSL2+ Router
- Quick Installation Guide
- One RJ45 cable
- Two RJ11 cables
- One ADSL splitter
- One Resource CD for TD-W8920G 108M Wireless ADSL2+ Router, including:
  - This User Guide
  - Other Helpful Information

Note:
If any of the listed contents are damaged or missing, please contact the retailer from whom you purchased the TD-W8920G 108M Wireless ADSL2+ Router for assistance.

COMMENT

Chapter 1. About This User Guide

1.1 Purpose

For helping user know about TD-W8920G 108M Wireless ADSL2+ Router better, use it accurately and adequately, maintain it expediently, we write this User Guide. This Guide introduces the product comprehensively, including the product's functions, parameters and specifications. It also explains how to configure and use these functions accurately.

1.2 Conventions

The Router or TD-W8920G mentioned in this User guide stands for TD-W8920G 108M Wireless ADSL2+ Router without any explanations.

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

You can set the parameters according to your demand.

1.3 Overview of this User Guide

Chapter 1: About This User Guide
Chapter 2: Product Overview
Chapter 3: Hardware Installation Guide
Chapter 4: Quick Installation Guide
Chapter 5: Basic Router Configuration
Chapter 6: Appendix

Chapter 2. Product Overview

2.1 Overview of the Router

Thank you for choosing the **TD-W8920G 108M Wireless ADSL2+ Router**. The Router is designed to provide a simple and cost-effective ADSL Internet connection for a private Ethernet or 802.11g, 802.11b wireless network.

The Router is easy to use. The TD-W8920G connects to an Ethernet LAN or computers via standard Ethernet ports. The ADSL connection is made using ordinary telephone line with standard connectors. Multiple workstations can be networked and connected to the Internet using a single Wide Area Network (WAN) interface and single global IP address. The advanced security enhancements, **IP Filtering** and **MAC Filtering** can help protect your network from potentially devastating intrusions by malicious agents from the outside of your network. **Parental Control** provides flexible access control so that parents or network administrators can establish restricted access policies for children or staff.

The Router is easy to install and manage. **Quick Setup** of the Web-based Utility is supplied and friendly help messages are provided for every step. Network and Router management is done through the Web-based Utility which can be accessed through local Ethernet using any web browser. Remote management is provided so that you may configure the Router through WAN port by the use of any Web browser.

ADSL

The **TD- W8920G 108M Wireless ADSL2+ Router** utilizes integrated ADSL2+ transceiver and high speed MIPS CPU. The Router supports full-rate ADSL2+ connectivity conforming to the ITU and ANSI specifications.

In addition to the basic DMT physical layer functions, the ADSL2+ PHY supports dual latency ADSL2+ framing (fast and interleaved) and the I.432 ATM Physical Layer.

The **TD- W8920G 108M Wireless ADSL2+ Router** is a complete plug-and-play solution. The Router integrates 4-port switch, firewall and NAT-Router. Its design is dedicated to Small Office/Home Office (SOHO) wireless network solutions.

Wireless

In the most attentive wireless security, the Router provides multiple protection measures. It can be set to turn off the wireless network name (SSID) broadcast so that only stations that have the SSID can be connected. The Router provides wireless LAN 64/128/152-bit WEP encryption security, WPA/WPA2 and WPA-PSK/WPA2-PSK authentication, as well as TKIP/AES encryption security.

The router adopts **2x to 3x eXtended Range™ WLAN transmission technology** so that transmission distance is 2-3 times of traditional IEEE 802.11g/b solutions. It is compatible with all IEEE 802.11g and IEEE 802.11b products. In addition, it also adopts **108M Super G™ WLAN Transmission Technology**, which offers the highest throughput performance available on the

market today, and data rates of up to 108Mbps. In dynamic 108M mode, the router can attach IEEE 802.11b, 802.11g and 108Mbps Super G™ devices at the same time in an integrated environment.

2.2 Main Features

- 4 10/100Mbps Auto-Negotiation RJ45 LAN ports (Auto MDI/MDIX), 1 RJ11 port.
- Quick response semi-conductive surge protect circuit, reliable surge-protect function.
- AFE to support Annex A/B/C/I/J/K/M, and L deployments.
- Provides external splitter.
- Multi-user sharing a high-speed Internet connection
- Connecting the internet on demand and disconnecting from the Internet when idle for PPPoE.
- Provides **WPA/WPA2, WPA-PSK/WPA2-PSK** data security, **TKIP/AES** encryption security.
- Provides 64/128/152-bit **WEP** encryption security and wireless LAN ACL (Access Control List).
- Adopts 2x to 3x eXtended Range™ wireless LAN transmission technology.
- Adopts Advanced DMT modulation and demodulation technology.
- Adopts 108M Super G™ wireless LAN transmission technology.
- Supports access control, parents and network administrators can establish restricted access policies based on time of day for children or staff.
- Supports Virtual Server, Port Triggering and DMZ host.
- Supports UPnP, Dynamic DNS, Static Routing.
- Supports bridge mode and Router function.
- Supports Web management.
- Supports firmware upgrade.
- Supports Flow Statistics.
- Supports SIP ALG.
- Built-in firewall supporting IP address filtering, MAC address filtering and parental control.
- Built-in DHCP server.

2.3 Supporting Protocol

- - Complies with ANSI T1.413
- - Complies with ITU G.992.1 (G.DMT) - Annex A/B/C
- - Complies with ITU G.992.2 (G.Lite) - Annex A/B/C
- - Complies with ITU G.992.3 (ADSL 2) - Annex A/B/C/M and Annex L (RE-DSL)

- - Complies with ITU G.992.5 (ADSL 2+) - Annex A/B/C and Annex L (RE-DSL)
- - Complies with IEEE 802.11b
- - Complies with IEEE 802.11g
- - Complies with IEEE 802.3, IEEE 802.3u
- - Supports RFC 2684 (EoA)(Bridged* and Router)
- - Supports RFC1577**:** IPoA (IP over ATM)
- - Supports RFC2364**:** PPPoA (PPP over ATM)
- - Supports RFC2516**:** PPPoE (PPP over Ethernet)

Note:
"*" Needs third-party software.

2.4 Transmit Data-rate

- Maximum Download Speed**:** 24Mbps（ADSL2+), 8Mbps（ADSL).
- Maximum Upload Speed**:** 1Mbps.
- Supports 108/54/48/36/24/18/12/9/6Mbps and 11/5.5/2/1Mbps data transfer rates.

Chapter 3. Hardware Installation Guide

3.1 The Front Panel

The Router's LEDs are located on the front panel.

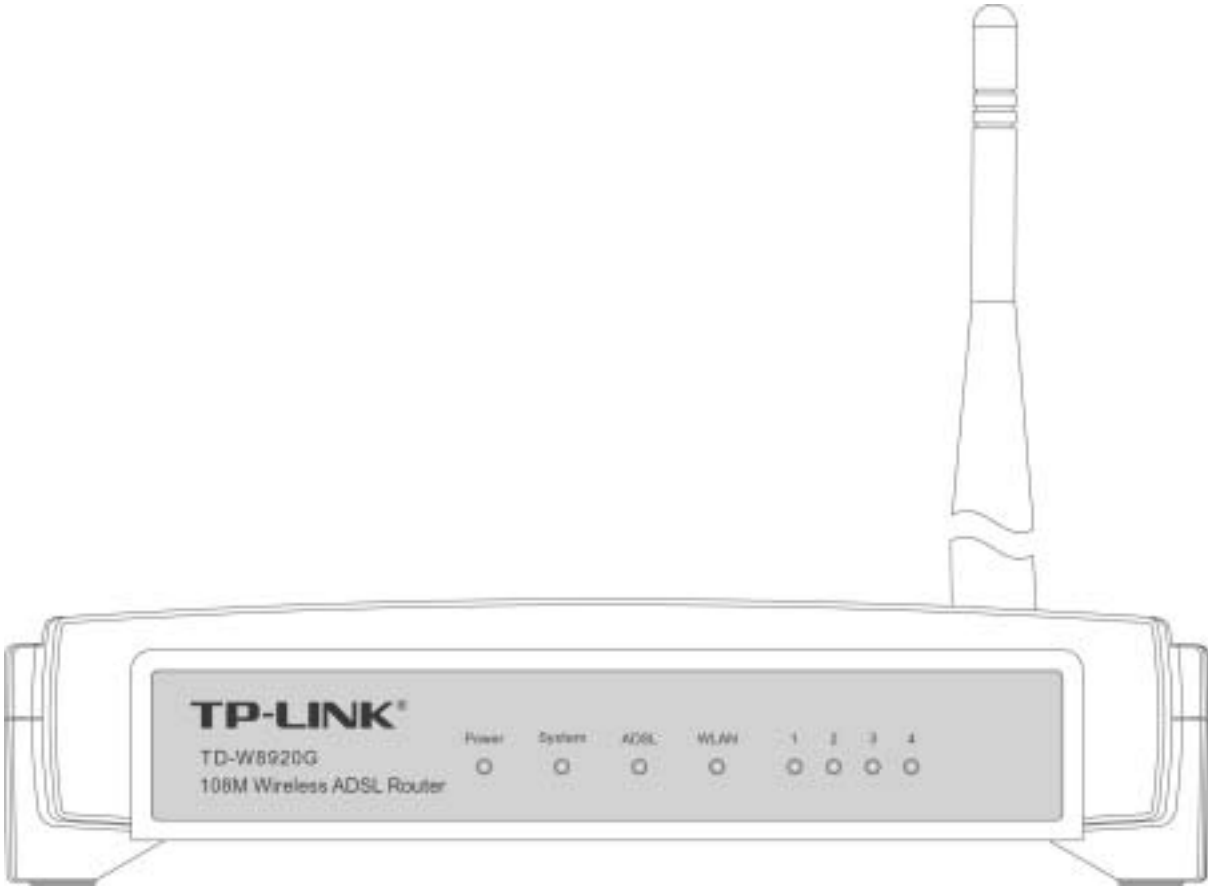

Figure 3-1

The LED indicators on the front panel include the **Power**, **System**, **ADSL**, **WLAN** and **1-4 (LAN)**. The ADSL, WLAN and 1-4 (LAN) indicators monitor link status and activity (Link/Act).

3.2 LED Explanation

Name	Status	Description
Power	Off	No Power
	On	Power on
System	Off	The Router has an error
	On	The Router is initializing
	Flashing	The Router is working properly
ADSL	Off	Disconnected the LINE port
	On	Connected the LINE port to ISP network
	Slow flash	Connecting to the ISP network
	Quick flash	Sending or receiving data

WLAN	Off	The Wireless function is disabled
	Slow flash	The Wireless function is enabled
	Quick flash	Sending or receiving data over wireless network
(1-4) LAN	Off	There is no device linked to the corresponding port
	On	Connected to a device through the corresponding port
	Flashing	Sending or receiving data over corresponding port

3.3 The Back Panel

The Router's ports, where the cables are connected, and RESET button are located on the back panel.

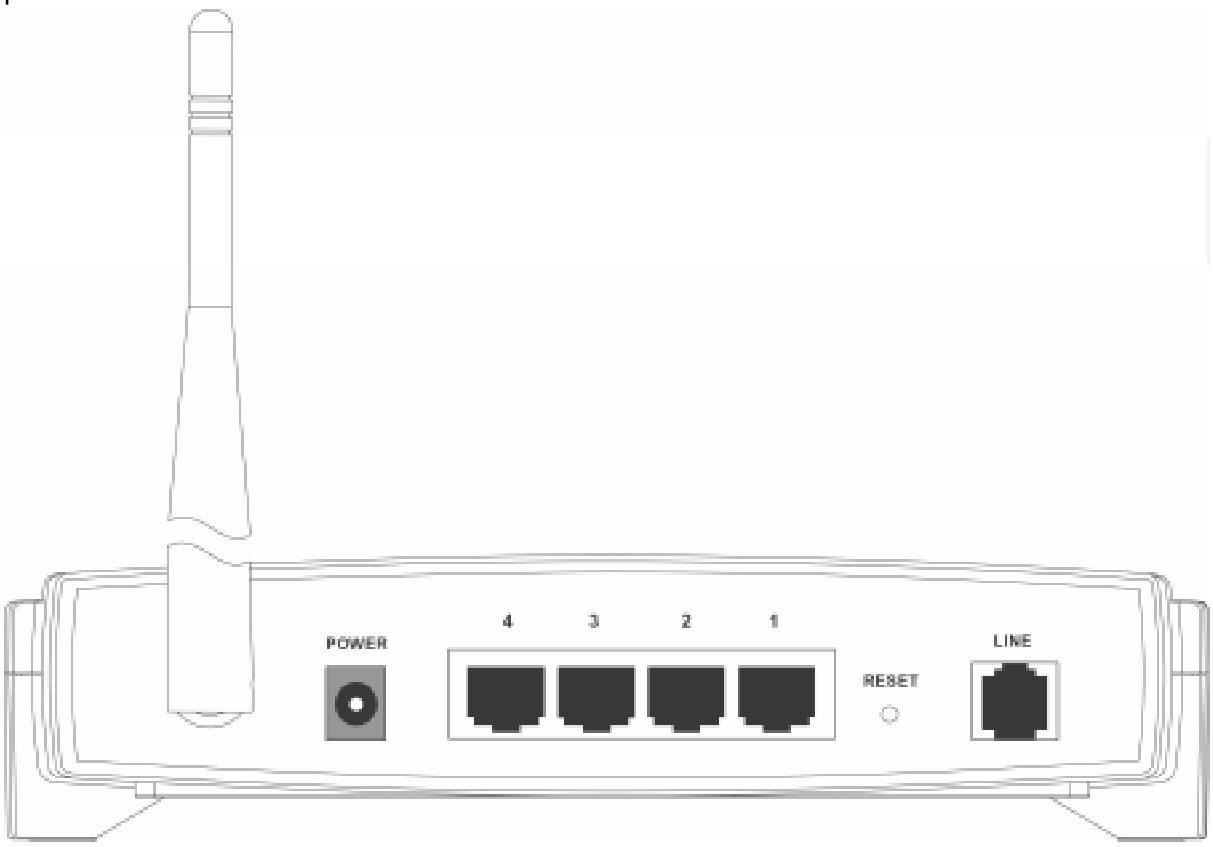

Figure 3-2

- **Line:** Connect to the Modem Port of Splitter or to the telephone line.
- **Reset Button:** There are two ways to reset the Router's factory defaults. Press the reset button of the Router, and then power on the Router, hold reset button pressed down for about five seconds, or restore the default setting from “Management **-** Settings **-** Restore Default “of the Router's Web-based Utility.
- **1, 2, 3, 4 (LAN):** Through these ports, you can connect the Router to your PCs and the other Ethernet network devices.
- **Power:** The Power plug is where you will connect the power adapter.
- **Antenna:** Used for wireless operation and data transmit.

3.4 System Requirements

- Make sure your computer has a Networking Interface Card (either wired or wireless is ok)

before connecting the Router to your computer.

- An operating system supporting the TCP/IP protocol.
- Broadband Internet Access (ADSL).
- Web browser, such as Microsoft Internet Explorer 5.0 or later, Netscape Navigator 6.0 or later.

3.5 Installation Environment Requirements

- The Router should not be located where it will be exposed to moisture or excessive heat.
- Place the Router in a location where it can be connected to the various devices as well as to a power source.
- Make sure the cables and power cord are placed safely out of the way so they do not create a tripping hazard.
- Designed to go up to 100 meters indoors and up to 300 meters outdoors for wireless connection.
- The Router can be placed on a shelf or desktop.
- Operating temperature**:** 0℃~40℃ (32°F~104°F).
- Operating Humidity**:** 10% ~ 90% RH Non-congealing.

3.6 Connecting the Router

Before installing the Router, please make sure your broadband service provided by your ISP is available. If there is any problem, please contact with your ISP. 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. Locate an optimum location for the Router. The best place is usually near the center of the area in which your PC will be wirelessly connected. The place had better accord with the Installation Environment Requirements.
2. Adjust the direction of the antenna. Normally, upright is a good direction.
3. Connect your PC and Switch/Hub in your LAN to the LAN Ports of the Router. (If you have a wireless NIC and want to have wireless connection, please skip this step.)
4. Connect the telephone line to the Line port on the Router.
5. Connect the DC power adapter to the DC power plug of the Router, and the other end into an electrical outlet. The Router will start to work automatically.

3.6.1 The Best Location for Wireless Network Connection

The operating distance or range of your wireless connection varies significantly based on the physical placement of the Router. For best results, place your Router.

- Near the center of the area in which your wireless stations will operate.
- In an elevated location such as a high shelf.
- Away from the potential sources of interference, such as PCs, microwaves, and cordless phones.
- Have the Antenna in the upright position.
- Away from large metal surfaces.

Note:

If do not follow these guidelines, there may be significant performance degradation and you may not be able to connect to the Router wirelessly.

3.6.2 Wired network connection

Wired network connections are provided through the **Line** port and LAN ports which are on the back of the Router. See the Back Panel picture above and the illustrations below for examples.

3.6.2.1. Connect ADSL Line

Use the ADSL cable included with the Router to connect it to a telephone wall socket or receptacle. Plug one end of the cable into the **Line** port (RJ11 receptacle) on the rear panel of the Router and insert the other end into the RJ11 wall socket. If you are using a low pass filter device, follow the instructions included with the device or given to you by your service provider. The ADSL connection represents the WAN interface, the connection to the Internet. It is the physical link to the service provider's network backbone and ultimately to the Internet.

3.6.2.2. Hub or Switch to Router Connection

Connect the Router to an uplink port (MDI-II) on an Ethernet hub or switch with a straight-through cable If you wish to reserve the uplink port on the switch or hub for another device, connect to other MDI-X ports (1x, 2x, etc.) with a crossed cable.

3.6.2.3. Computer to Router Connection

You can connect the Router directly to a 10/100BASE-TX Ethernet adapter installed on a PC using the Ethernet cable-10/100BASE-TX.

The illustration below shows the Router connected to Ethernet LAN devices, Wireless LAN devices and the Internet. You can connect the Router directly to a 10/100BASE-TX Ethernet adapter installed on a PC using the Ethernet cable provided as shown in this diagram.

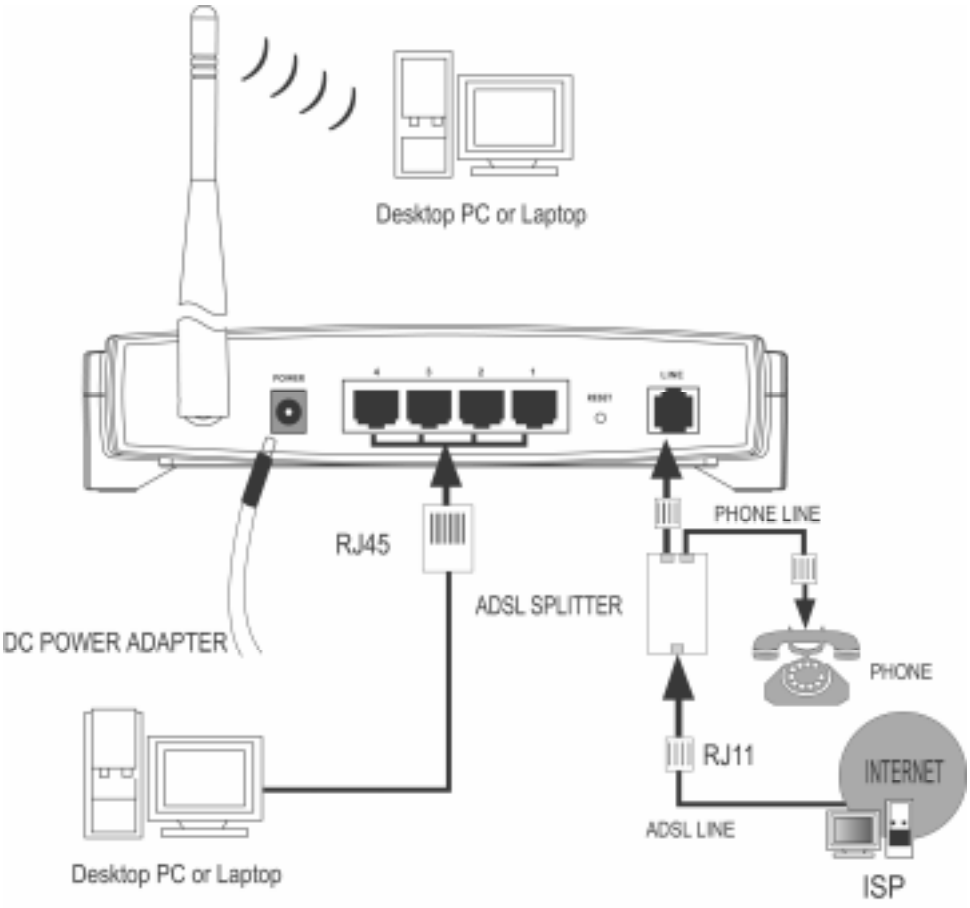
Desktop PC or Laptop
RJ45
PHONE LINE
ADSL SPLITTER
DC POWER ADAPTER
PHONE
RJ11
INTERNET
ADSL LINE
Desktop PC or Laptop
ISP

Figure 3-3

Chapter 4. Quick Installation Guide

After connecting the Router to your network, you should configure it. This chapter describes how to quickly configure the basic functions of your Router. These procedures only take you a few minutes. You can access the Internet via the Router immediately after successfully configuring.

4.1 Configure the Router

1. Login to Home Page

To use the web-based utility, launch a suitable web browser and direct it to the IP address of the Router. Type **http://192.168.1.1** in the address bar of the browser.

A dialog box prompts for User name and Password. Type in the default User name **admin** as well as Password **admin** and then click the **OK** button to access the **Quick Setup** screen.

Figure 4-1

Note:
Do not mix up the user name and password with your ADSL account user name and password which needed for PPP connections.

2. The default screen shows as below. Change the VPI or VCI values which are used to define a unique path for your connection. **If you have been given specific settings for this to configuration, type in the correct values assigned by your ISP.** Click “Next”.

Figure 4-2

3. On the **Connection Type** screen, you can select a connection type (PPPoA, PPPoE, MER, IPoA or Bridging), which is provided by your ISP. We select PPPoE mode (For example), and then click “Next “to continue.

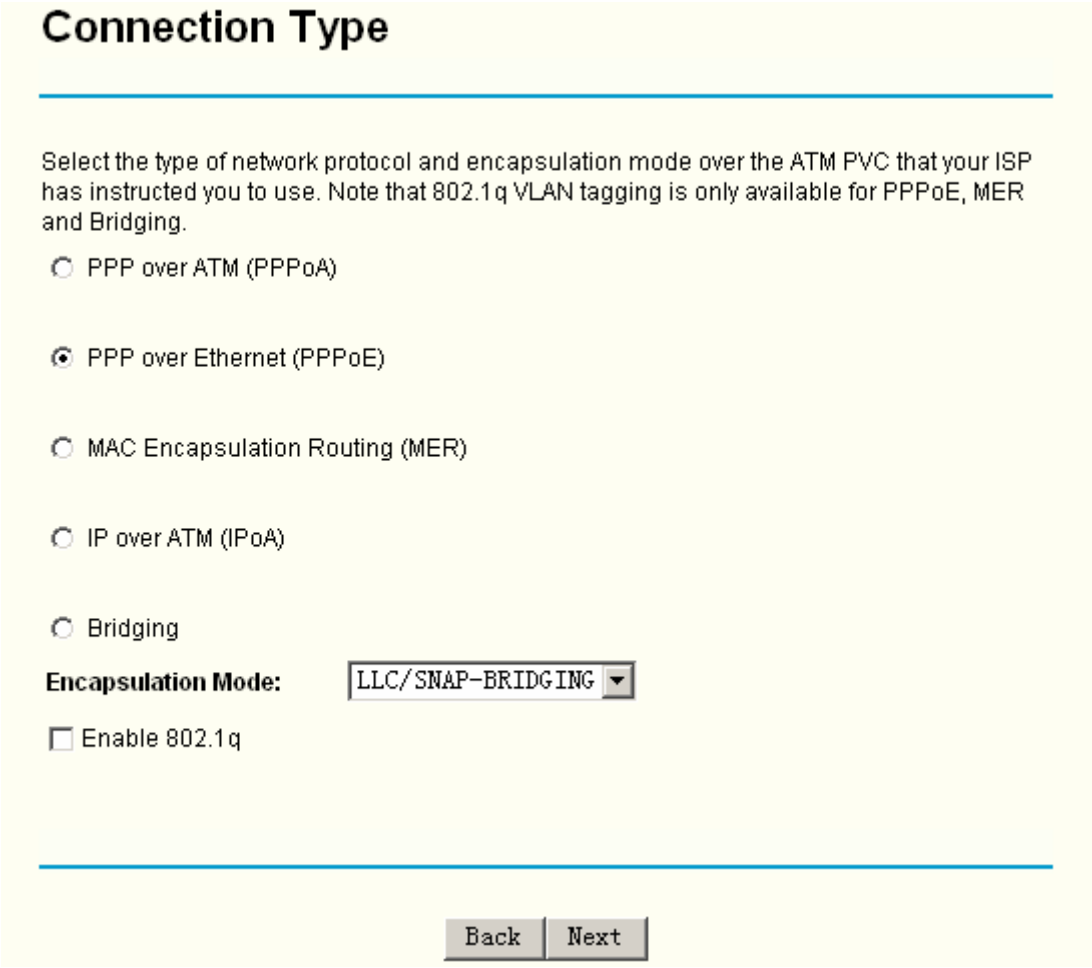

Figure 4-3

4. Enter the **PPP Username** and **PPP Password** provided by your ISP. If PPPoE Service

Name was provided by your ISP, enter the Service Name. Click “Next” to continue.

Figure 4-4

5. Use the default setting of this screen click “Next” to continue.

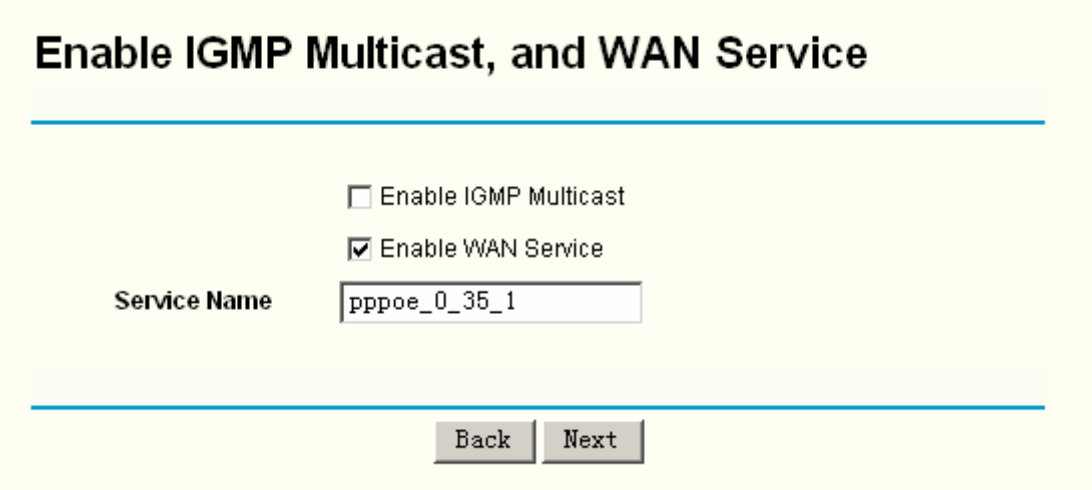

Figure 4-5

6. Use the default IP Address 192.168.1.1 and Subnet Mask 255.255.255.0. Use the default setting of “**Enable DHCP Server**”, and click “Next” to continue.

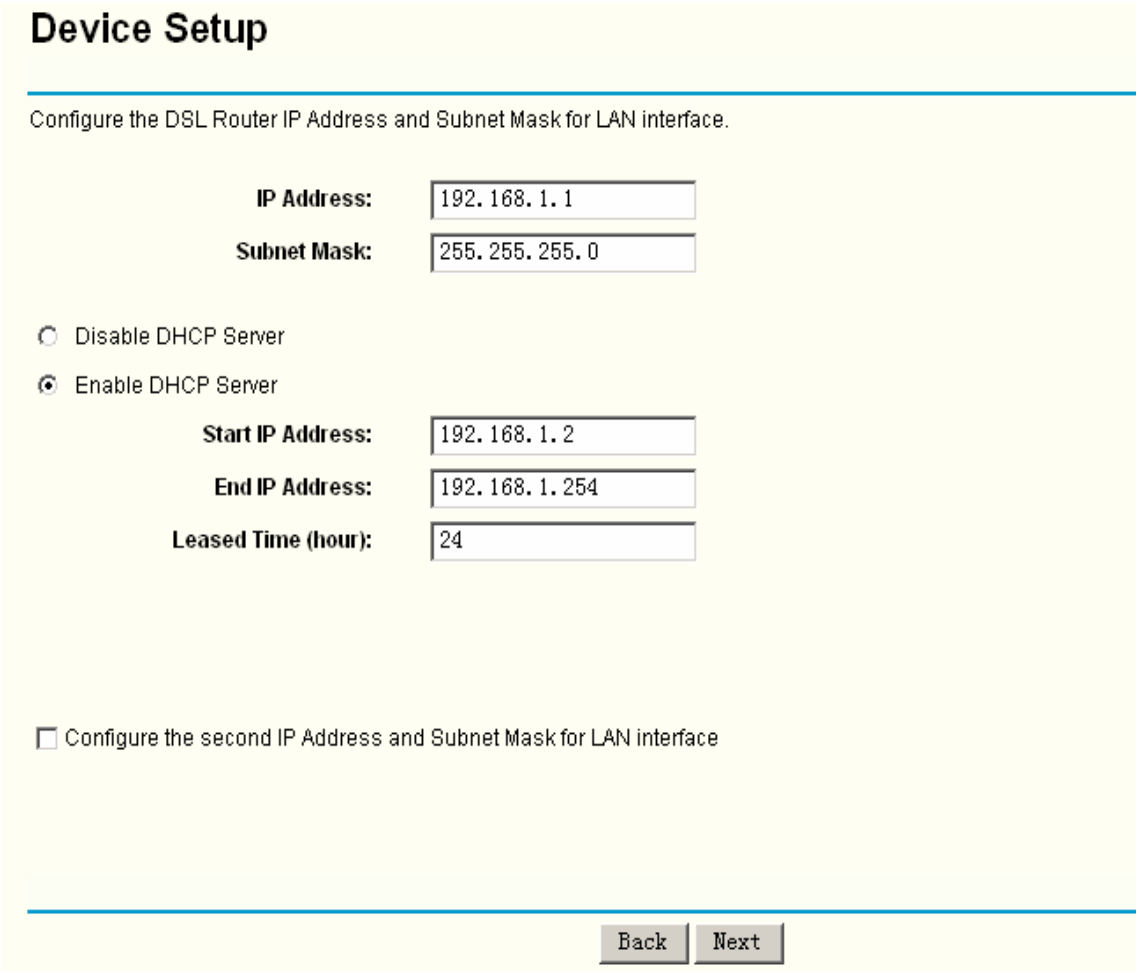

Figure 4-6

7. Use the default setting “**Enable Wireless**”. Default SSID is “TP-LINK”, then click “Next”.

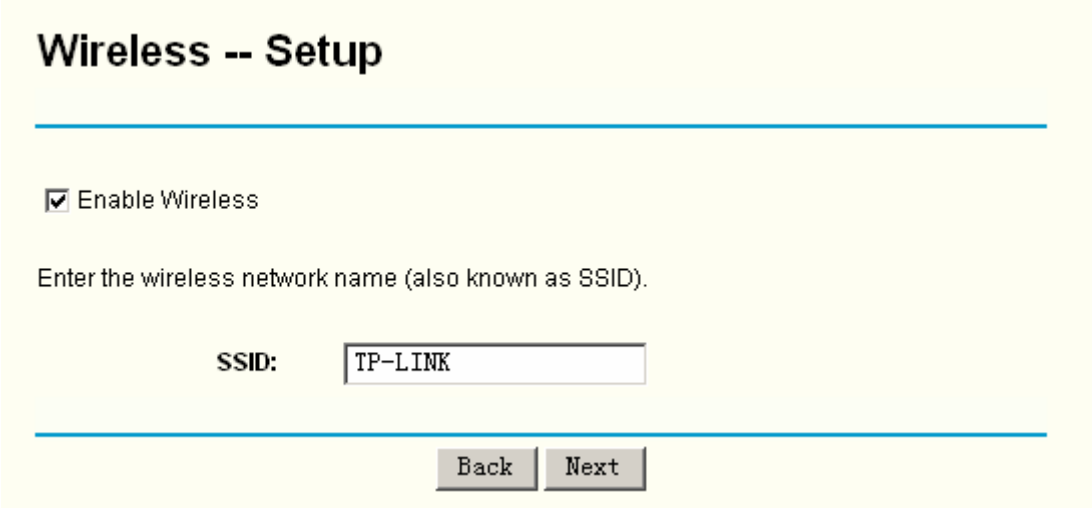

Figure 4-7

8. You will see the **WAN Setup-Summary** screen below, click "**Save/Reboot**" to save these settings and reboot the Router.

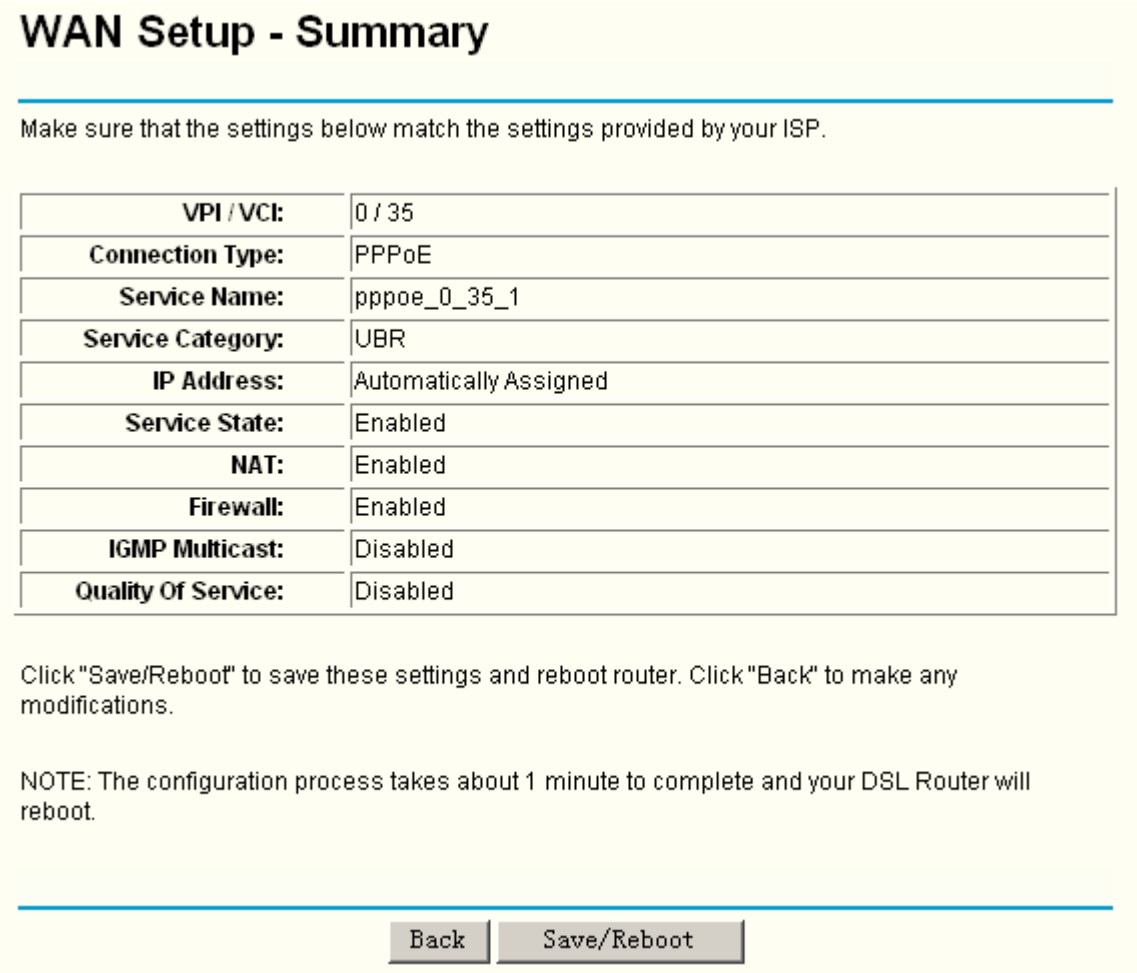

Figure 4-8

Note:
The reboot process will take a while to complete, please wait before reopening your web browser.

4.2 Configure PC

Your PC needs a network adapter. You may directly connect your adapter to the Router, or you may connect your adapter to a Hub/Switch, and then connect the Hub/Switch to the Router.

Follow the instructions below to configure a computer running Windows XP to be a DHCP client.

1. From the **Start** menu on your desktop, go to **Settings**, and then click on Network Connections.

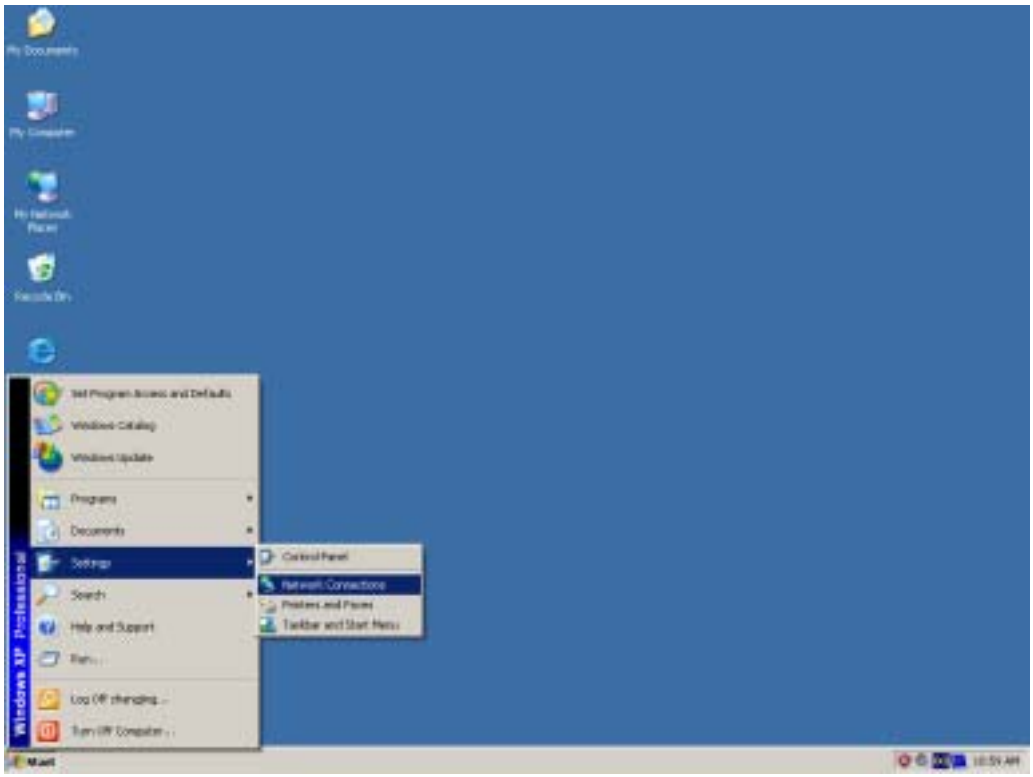

Figure 4-9

2. In the **Network Connections** window, right-click on LAN (Local Area Connection), then click Properties.

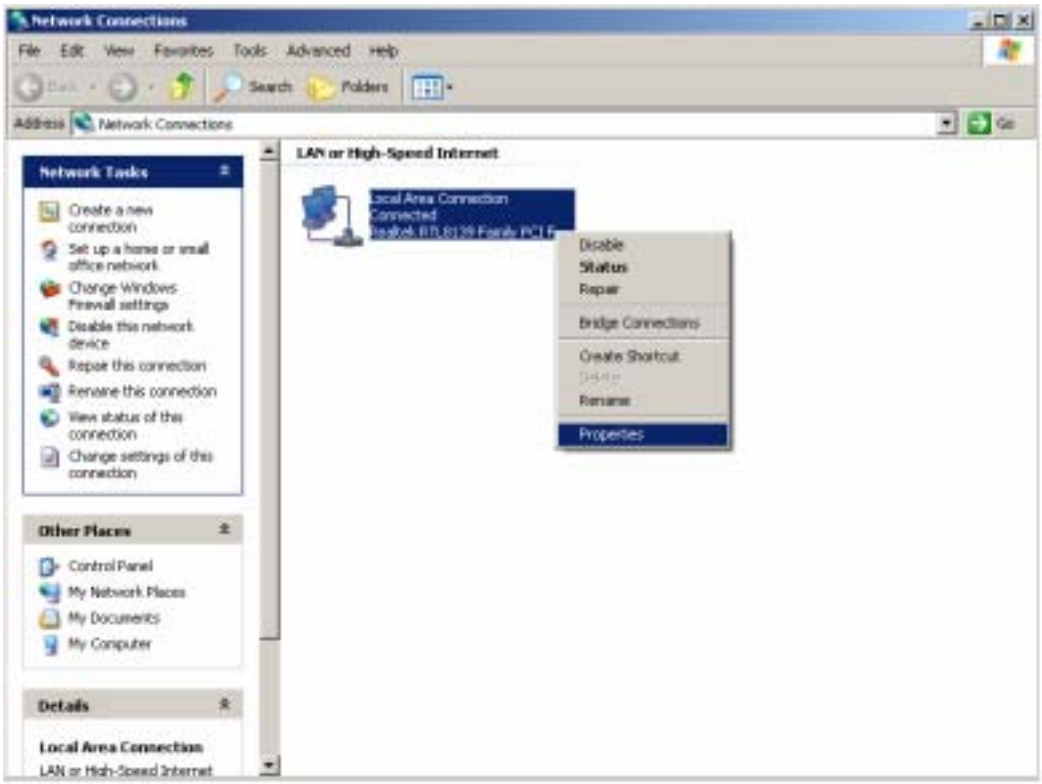

Figure 4-10

3. In the **General** tab of **Internet Protocol (TCP/IP) Properties** menu, highlight Internet Protocol (TCP/IP) under “This connection uses the following items:” by clicking on it once.

Click on the Properties button.

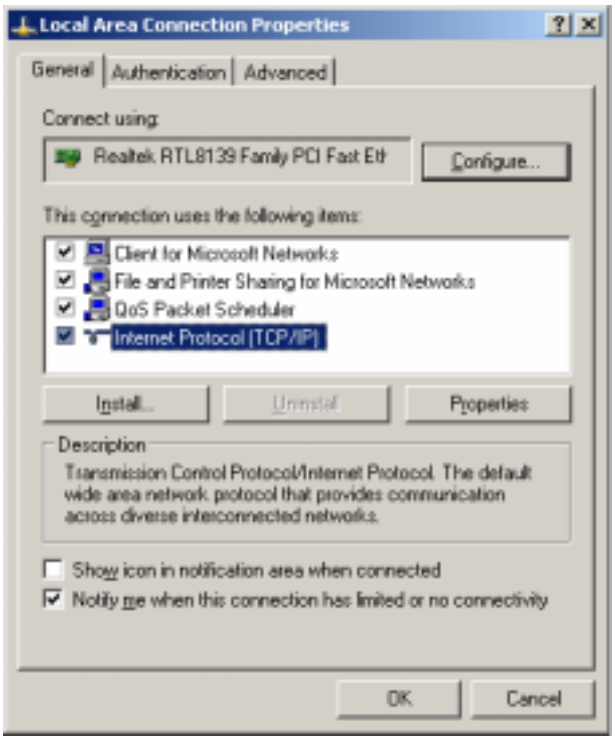

Figure 4-11

4. Select “Obtain an IP address automatically” by clicking the radio-button. Click OK

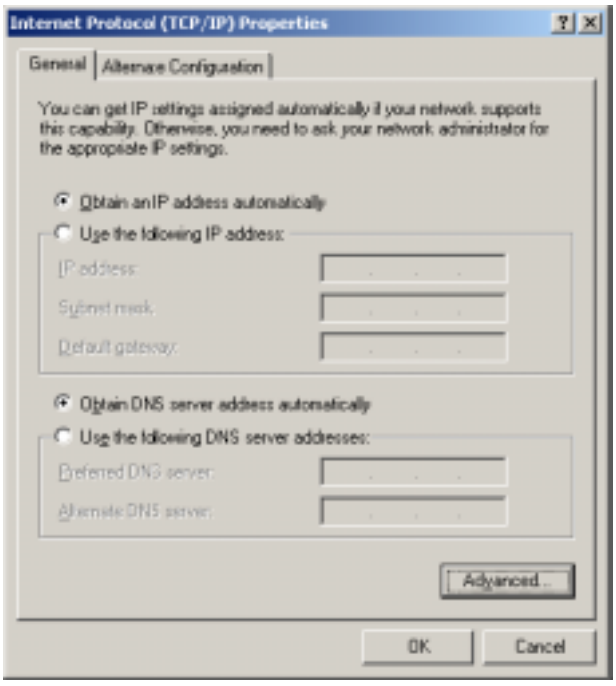

Figure 4-12

➢ Configure the IP address manually

Open TCP/IP Properties of the LAN card in your PC, enter the IP address as 192.168.1.* (* is any value between 2 to 254, Subnet mask is 255.255.255.0, Gateway is 192.168.1.1, DNS address is the value provided by ISP).

- Now, you can run the Ping command in the command prompt to verify the network connection between your PC and the Router. The following example is in Windows XP Operating System.

Open a command prompt, From the Start menu on your desktop, select run tab, type **cmd** in the field, and type *ping 192.168.1.1* on the screen that appears, and then press Enter.

If the result displayed is similar to that shown in figure below, the connection between your PC and the Router has been established.

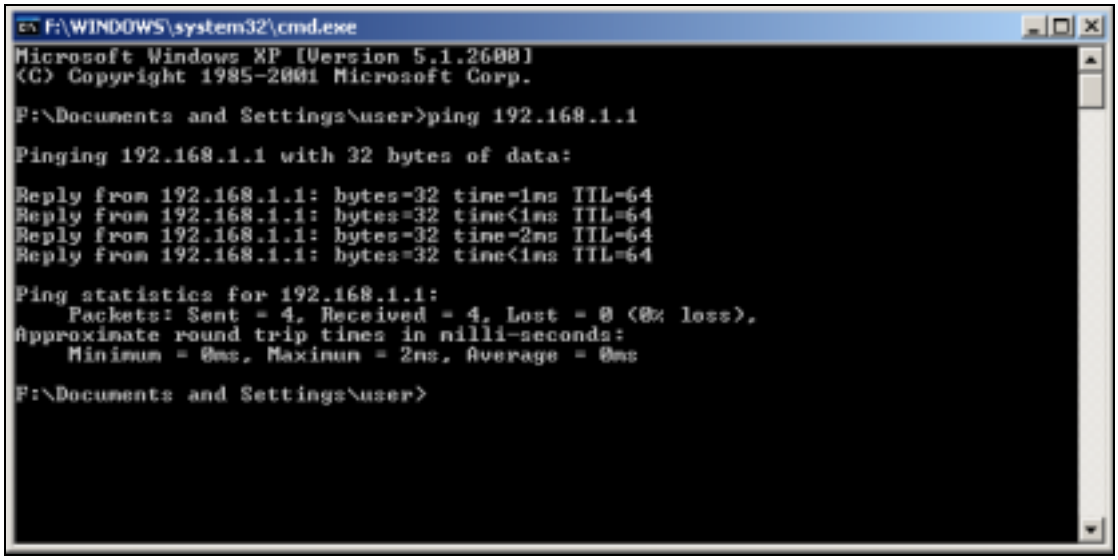

Figure 4-13

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

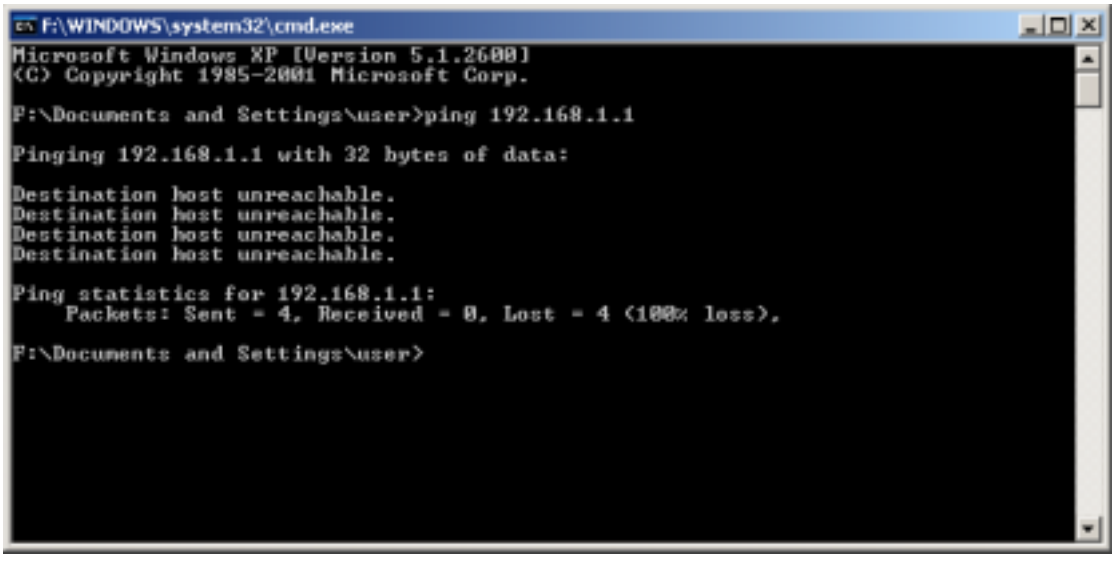

Figure 4-14

Please check it following these steps:

1. If the connection between your PC and the Router is correct?

Note:

The 1/2/3/4 LEDs of LAN port which you link to on the Router and LEDs on your PC's adapter should be lit.

2. If the TCP/IP configuration for your PC is correct?

Note:

If the Router's IP address is 192.168.1.1, your PC's IP address must be within the range of 192.168.1.2 ~ 192.168.1.254, the gateway must be 192.168.1.1.

For more details of configuring the Router, please refer to Chapter 5

Chapter 5. Basic Router Configuration

This User Guide recommends using the “Quick Installation Guide” for first-time installation of the TD-W8920G 108M Wireless ADSL2+ Router. For advanced users, if you want to know more about the TD-W8920G and make use of its functions adequately, you need to read this chapter and configure the Router’s advanced settings though the Web-based Utility.

This chapter will describe each web page on the Utility and each page’s key functions. The Utility can be accessed via your web browser though the use of a computer connected to the Router. You may configure the TD-W8920G 108M Wireless ADSL2+ Router’s settings though the Web–based Utility.

5.1 Login

After your successful login, you will see the Login screen (shown in Figure 5-1).

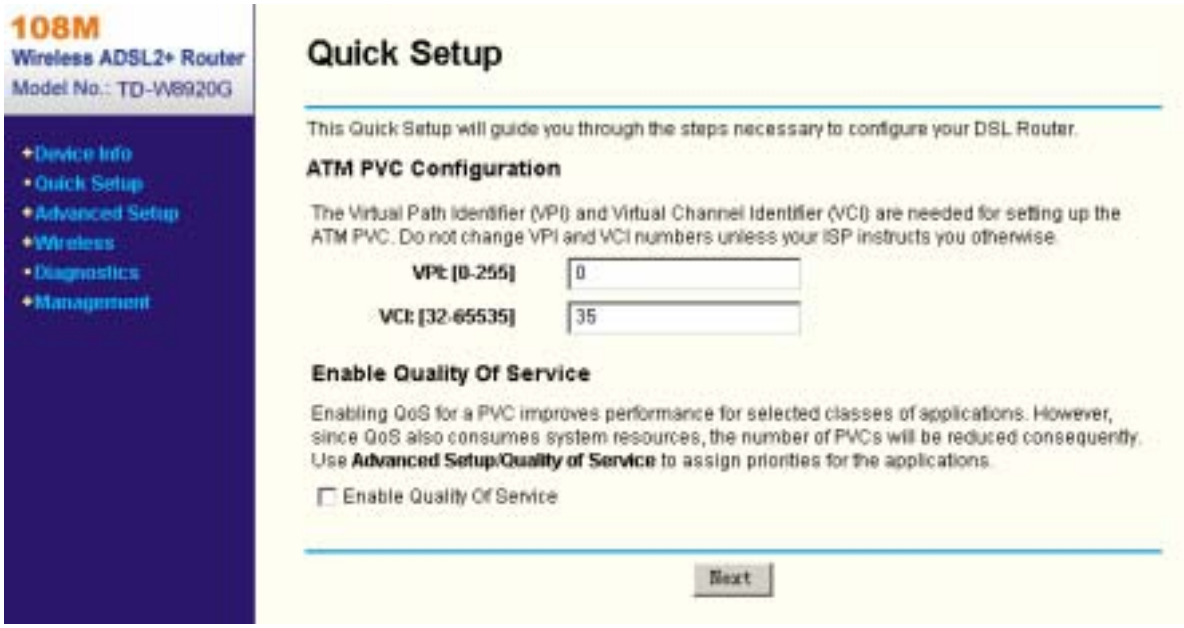

Figure 5-1

There are six main menus shown on the screen, they are **Device Info**, **Quick Setup**, **Advanced Setup**, **Wireless**, **Diagnostics** and **Management**. Additional menus will be available after you click one of the main menus. Click one of the main menus, and you will be able to configure the corresponding function.

5.2 Device Info

Choose “**Device Info**” menu, there are six submenus under the main menu: **Summary**, **WAN**, **Statistics**, **Route**, **ARP** and **DHCP**. This Device Info section mainly introduces the elementary information about the Router and its current settings in use. Click any of them, and you will be able to view the corresponding information.

Choose “**Device Info**”→“**Summary**”, you will see the Summary screen (shown in Figure 5-2)

The first table indicates the information about the version including Software and Hardware, the second table displays the current status of the TD-W8920G connection, this information will vary depending on the settings of the Router configured on the Advanced Setup screen.

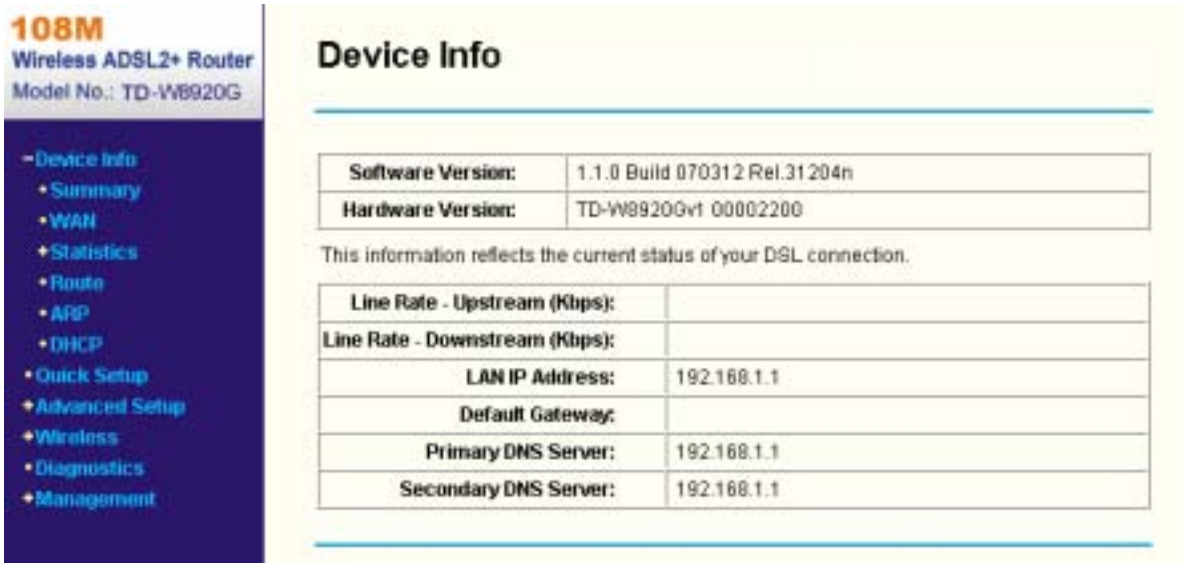

Figure 5-3

Note:

Click the other submenus under the main menu **Device Info**, you will be able to view the corresponding information about **WAN**, **Statistics**, **Route**, **ARP** and **DHCP**.

5.3 Quick Setup

Please refer to the **Chapter 4** to get the detailed information.

5.4 Advanced Setup

Choose "**Advanced Setup**", there are many submenus under the main menu. Among the submenus, **WAN**, **LAN**, **Routing**, **DSL** and **Port Mapping** are default menus, while **NAT**, **Security**, **Quality of Service** and **DNS** will appear only when you select some corresponding functions, click any one of them, and you will be able to configure the corresponding function.

This Advanced Setup section mainly introduces how to configure the Router for adequate use. The detailed explanations for each subsection are provided below.

5.4.1 WAN

Choose "**Advanced Setup**"→"**WAN**", and you will see the WAN screen (shown in Figure 5-4), the section shows the configuration information of WAN port.

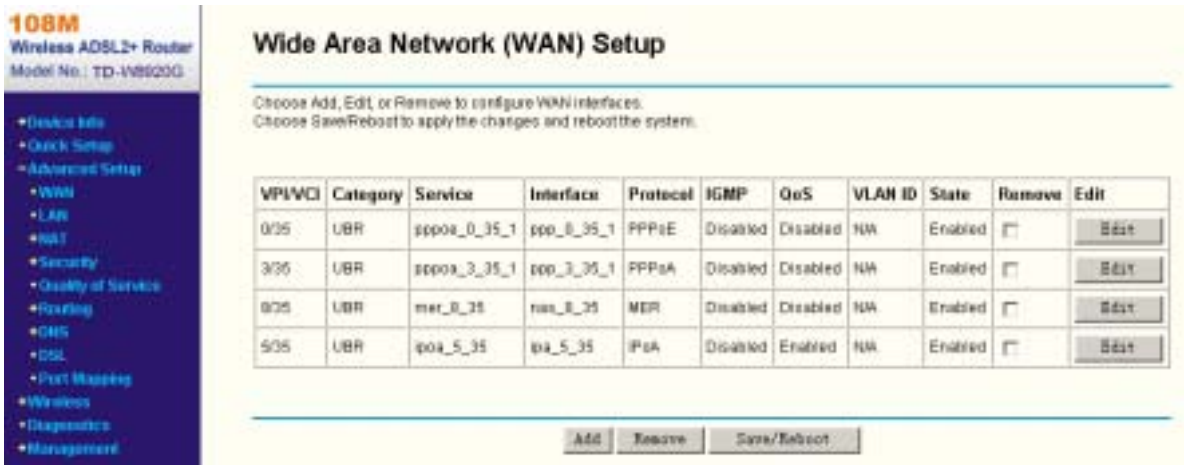

Figure 5-4

- **WAN Port Information Table:** This table describes the WAN port settings and the relevant manipulation to each interface.
- **Remove:** Select the check box in the table (shown in Figure 5-4) and then click the **Remove** tab, the corresponding interface will be deleted in the table.
- **Add:** Click the **Add** button, you can add a new interface in the next screen (shown in Figure 5-5).
- **Save/Reboot:** If you are sure of the settings, choose **Save/Reboot** to apply the changes and reboot the system.

Note:

You have to reboot to activate the WAN interface and further configuration services over this interface. Click the **Save/Reboot** button to implement it.

Follow the instructions below to Add or Edit an ATM PVC

1. Click the **Add** button on the screen above (shown in Figure 5-4), then you will see the next screen as follows (Figure 5-5):

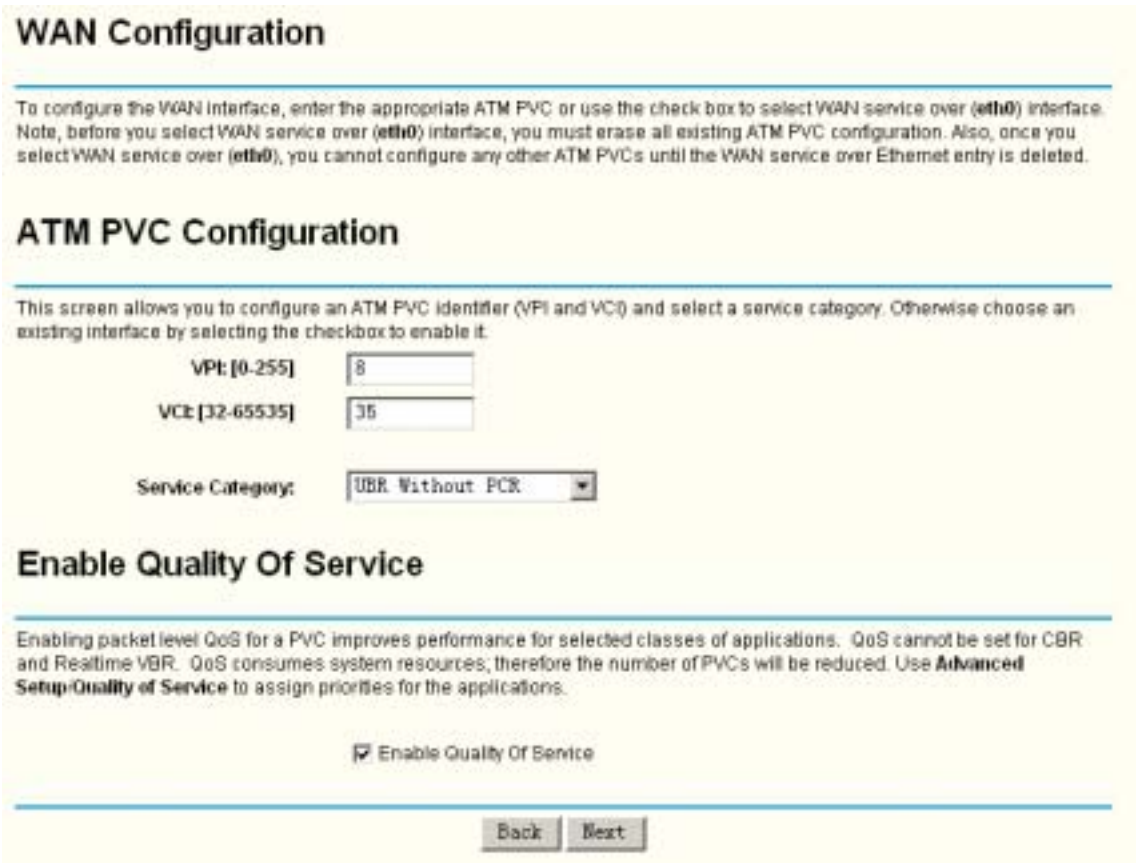

Figure 5-5

1. Follow the instructions below to configure the **ATM PVC** on the screen (shown in Figure 5-5). Make sure you have the necessary information before you configure it.
   1) Enter the **VPI** and **VCI** values provided by your ISP, they should not be changed unless you have been instructed to change it by your ISP.
   2) Select the type of the service assigned by your ISP in the drop-down list. The default type is **UBR Without PCR**.
   3) If you want to adopt **QoS** (Quality of Service) for the connection, please select the **Enable Quality Of Service** check box.
   4) Click the **Next** button for the further configuration in the next screen (shown in Figure 5-6), or else click the **Back** button to go to the previous screen.

Note:

Enabling packet level QoS for PVC improves performance for selected classes of applications. While QoS consumes system resources; therefore the number of PVC(s) will be reduced. Besides this, it cannot be set for the connection type of CBR and Real-time VBR. If you select the QoS service, the Quality of Service menu will be added to the Web-based Utility, the detailed configuration will be described in **5.4.5 Quality of Service**.

2. Select the **Connection Type** in the next screen (shown in Figure 5-6).

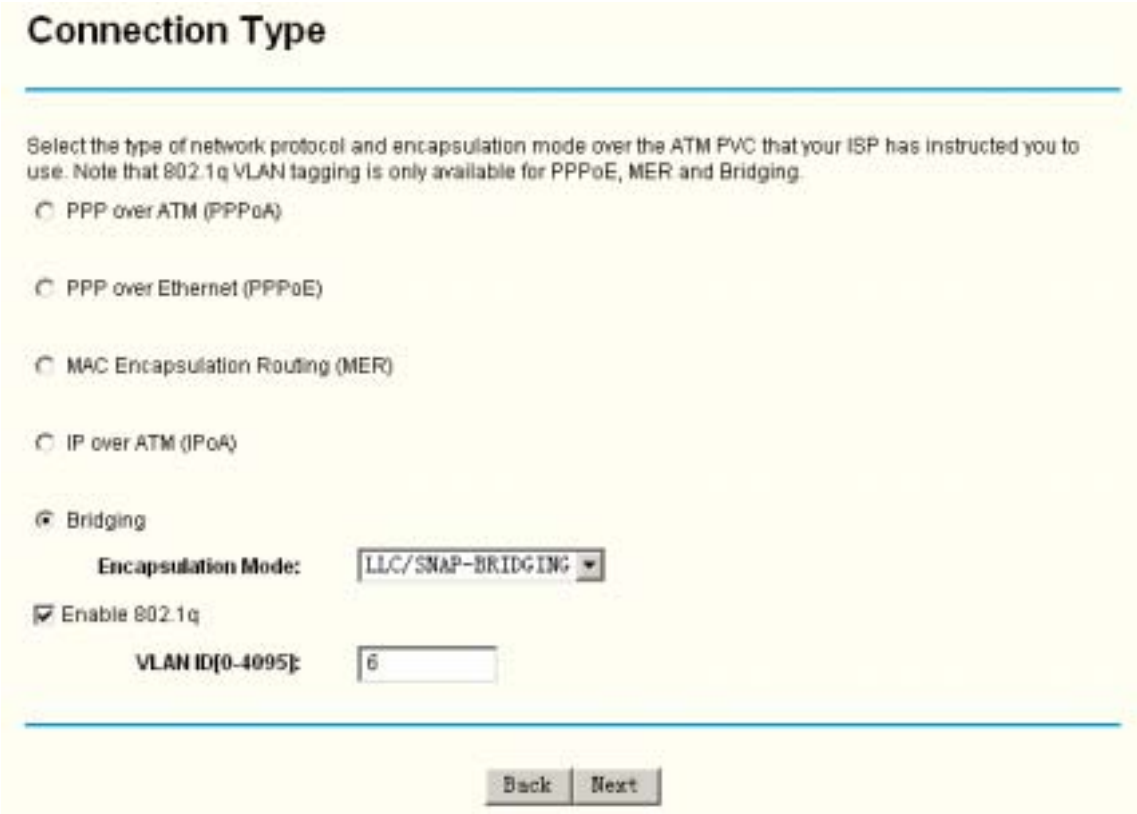

Figure 5-6

1) Select the **Connection Type** and **Encapsulation Mode** your ISP has instructed you to use, the default connection type is Bridging.
2) If you want to add to an assigned VLAN, please select the **Enable 802.1q** check box, and enter the **VLAN ID**.
3) Click the **Next** button to go to the next screen to make further configurations for the WAN Port, or else click the **Back** button to go to the previous screen to make modifications.

Note:

802.1q VLAN tagging is only available for the connection type of **PPPoE**, **MER** and **Bridging**.

After you select the **Connection Type**, please follow the instructions below to complete the further configuration of WAN Interface. There are five different configurations for the connection types, which are **PPPoA**, **PPPoE**, **MER**, **IPoA** and **Bridge**. You can select the corresponding types according to your needs. Note that this User Guide adopts different VPI, VCI and QoS to introduce further configuration for the different connection types below, if you need to change the configuration of ATM PVC (VPI, VCI and QoS), you should go to the previous screen (shown in Figure 5-5) to configure them again.

1. PPPoA

If you choose connection type **PPPoA** on the screen above (shown in Figure 5-6), you will see the screen below (shown in Figure 5-7). Follow the instructions to configure the WAN Interface.

Figure 5-7

1) Enter the **PPP Username** and **PPP Password** provided by your ISP exactly, select the **Authentication Method** in the drop-down list, the default method is **AUTO**, you can leave it as a default setting.
2) If you wish to active the “Connect on Demand” function, click the **Dial on the demand** radio-button, and enter the **Inactivity timeout** value, the range is from 1 to 4320 minutes. Then the Router will cut off the Internet connection after it has been inactive for a specific period of time (Inactivity Timeout). If your Internet connection is 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.
3) If you are required to use a permanent IP address, select the option **Static IP Address** and enter the value in the text box.
4) Click the **Next** button to go to the next screen below (shown in Figure 5-8), or else click the **Back** button to return to the previous screen to make modifications.

Note:

If you are not sure about the **PPP IP extension** and **PPP Debug Mode**, please don’t select this option.

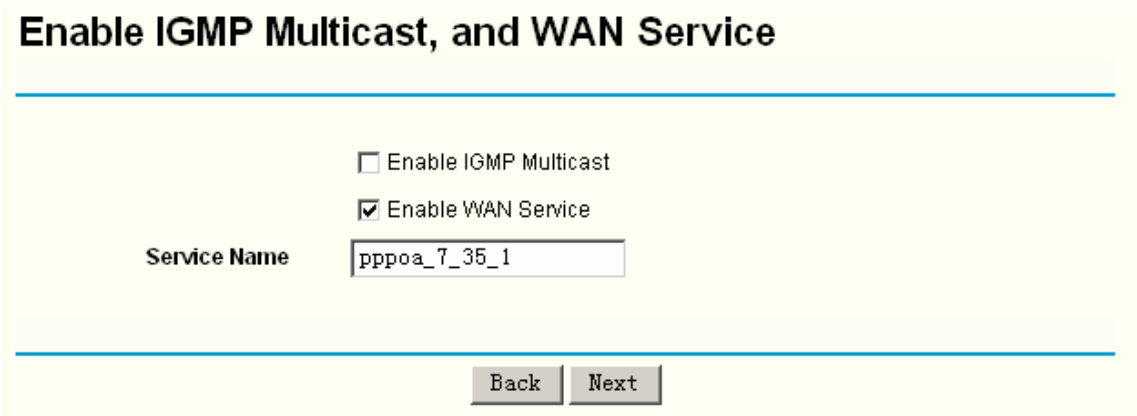

Figure 5-8

5) Enable the **IGMP Multicast** and **WAN Service** on the screen above, if you are not sure about the IGMP, just leave the default setting. Note that if you want to adopt the PPPoA service, you have to select the **Enable WAN Service** option in the screen above, or else the service will not take effect.
6) Click the **Next** button, and you will see the next screen which displays the detailed settings you've made (shown in Figure 5-9).

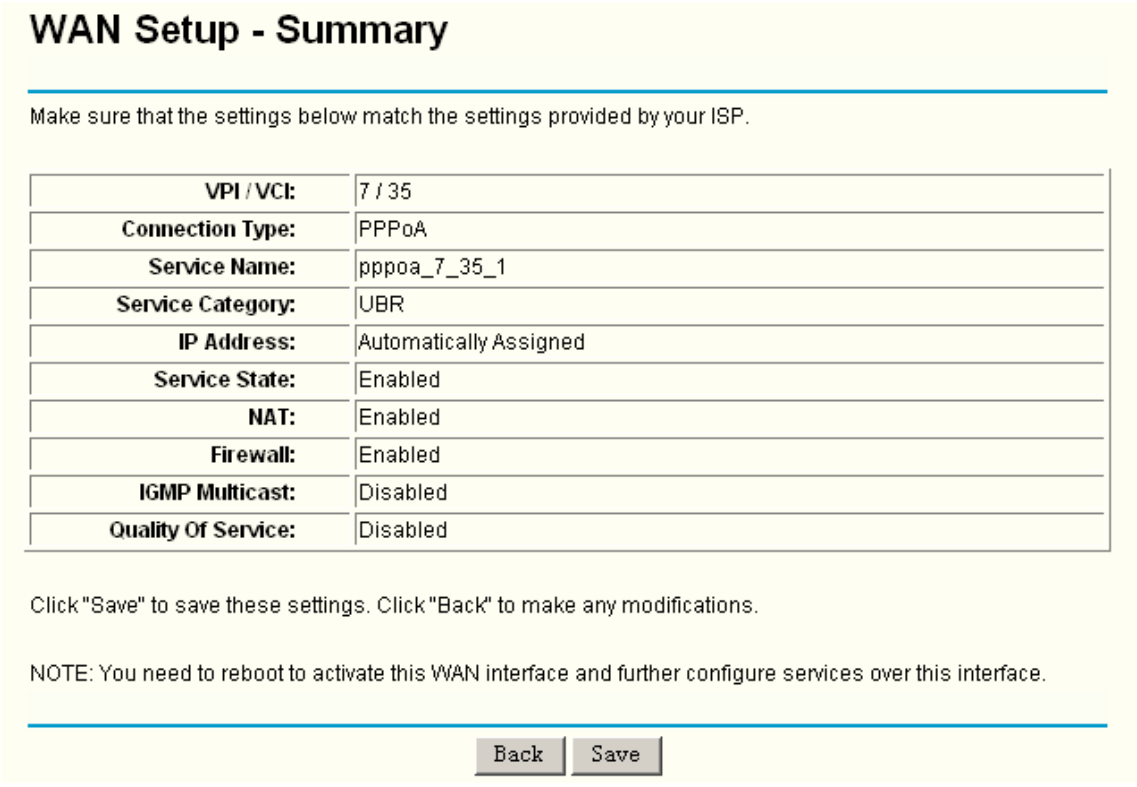

Figure 5-9

7) If you are sure about the configuration, click the **Save** button to save these settings, otherwise click the **Back** button to return to the previous screen to make modifications. The information is same as the information in Figure 5-4.

2. PPPoE

If you choose **PPPoE** in the previous screen (shown in Figure 5-6), the configuration is similar to **PPPoA**, the only difference is that you should set the **PPPoE Service Name** on

the corresponding screen. You can refer to **Chapter 4** to achieve the configuration for the connection type.

3. MER

If you choose **MER** in the previous screen (shown in Figure 5-6), you can see the screen (shown in Figure 5-10). Follow the instructions to configure the connection.

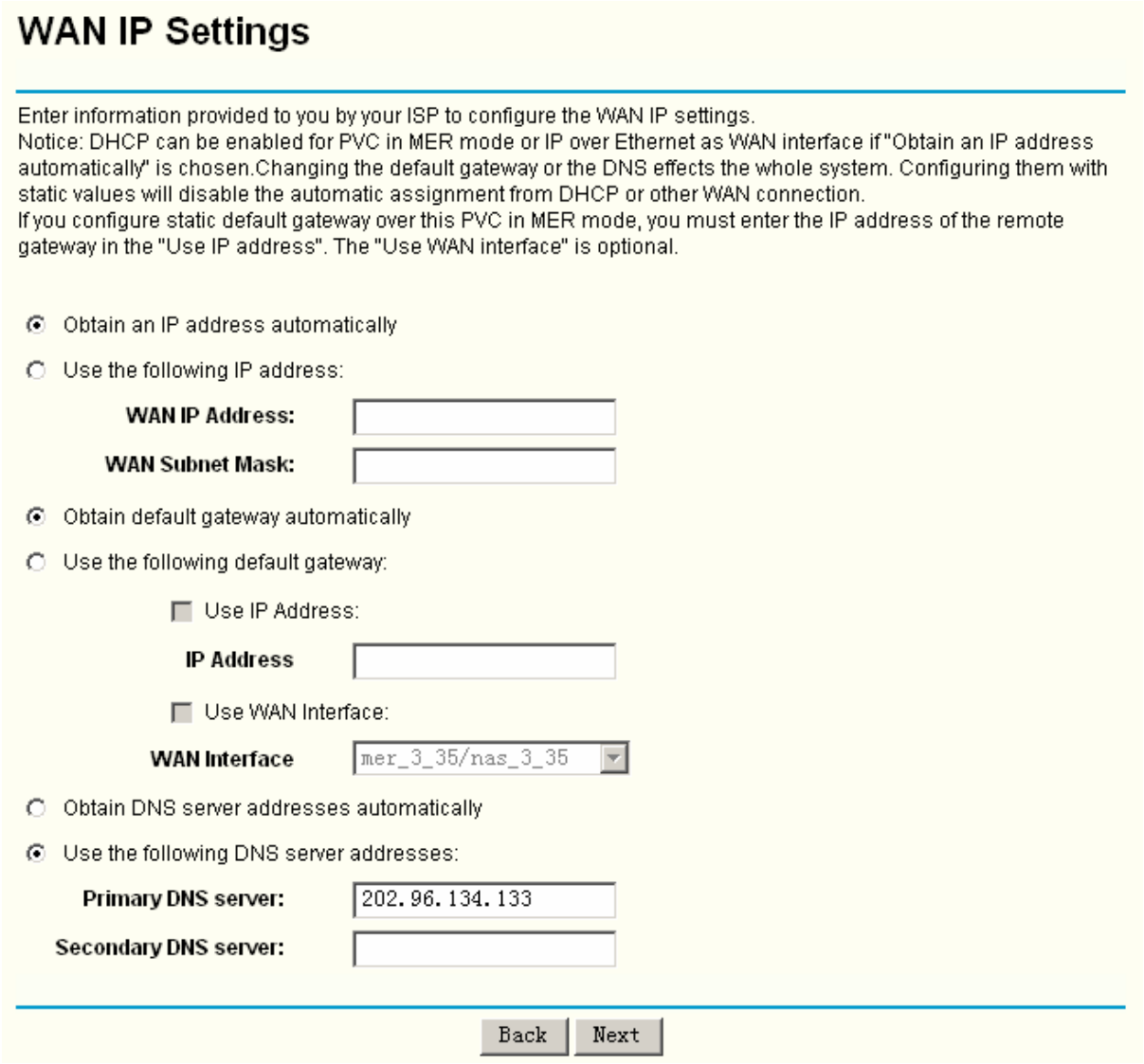

Figure 5-10

1) Configure the **WAN IP Address**. If you are provided a dynamic IP Address, please select **obtain an IP address automatically**, and then the Router will automatically get IP parameters from your ISP. If you are provided with a static IP Address, please select **Use the following IP Address**, and then enter the **WAN IP Address** and **WAN Subnet Mask**.
2) Configure the **default gateway**. If you are provided a dynamic gateway address, please select **obtain default gateway automatically**, and then the Router will automatically get gateway parameters from your ISP. If you are provided with a static gateway, please select **Use the following default gateway**, and then enter the gateway address.
3) Configure the DNS. If you are provided dynamic DNS server addresses, please select **obtain DNS server addresses automatically**, then the Router will automatically get

DNS server addresses from your ISP. If you are provided static DNS server addresses, please select **Use the following DNS server addresses**, then enter the DNS Server addresses. In this case, you will be provided at least one DNS server address.

4) Click the **Next** button, and you will see the screen (shown in Figure 5-11). You can also click the **Back** button to return to the previous screen to make modifications. On the screen below, you can Enable the **NAT**, **Firewall**, **IGMP Multicast** and **WAN Service**, if you are not sure about the settings, just leave the default settings.

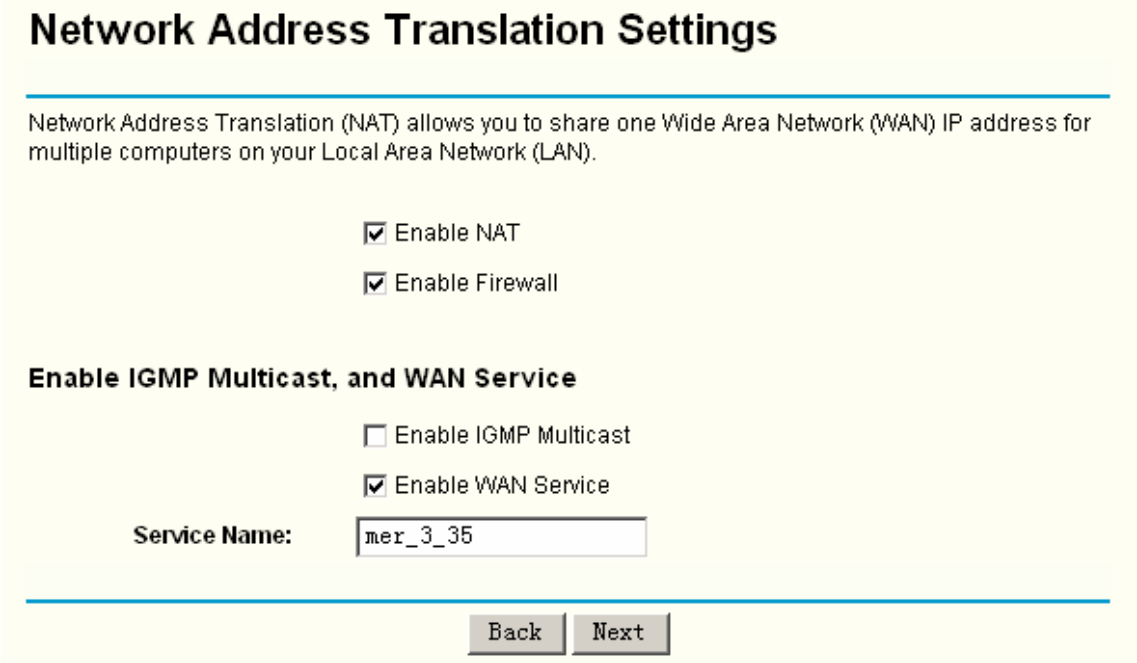

Figure 5-11

- **Enable NAT:** This technology translates the IP addresses of a local area network to a different IP address for the Internet. If this Router is hosting your network's connection to the Internet, please select the check box. If another Router exists in your network, you don't need to select the option.
- **Enable Firewall:** A firewall enhances network's security. Select the option to use a firewall, or else without a firewall.
- **Enable IGMP Multicast:** This is disabled by default. This setting will not allow IGMP (Internet Group Management Protocol) packets to be forwarded to the LAN. IGMP is used to manage multicasting on TCP/IP networks. Most users will not need to enable this. Some ISPs use IGMP to perform remote configuration for client devices, such as the Router. If you are unsure, check with your ISP.
- **Enable WAN Service:** If you want to adopt the MER service, you have to select the option in the screen above, or else the service will not take effect.
- **service name:** You can enter the service name in the text box or leave the default name.

Note:

If you select the **NAT** and **Security** check box on the screen (shown in Figure 5-11), the **NAT** and **Security** menu will be added to the Web-based Utility. We will describe the detailed configuration in **5.4.3 NAT** and **5.4.4 Security**.

5) Click the **Next** button, and you will see the next screen which displays the detailed settings you've made (shown in Figure 5-12). Or else click the **Back** button to return to

the previous screen to make modifications.

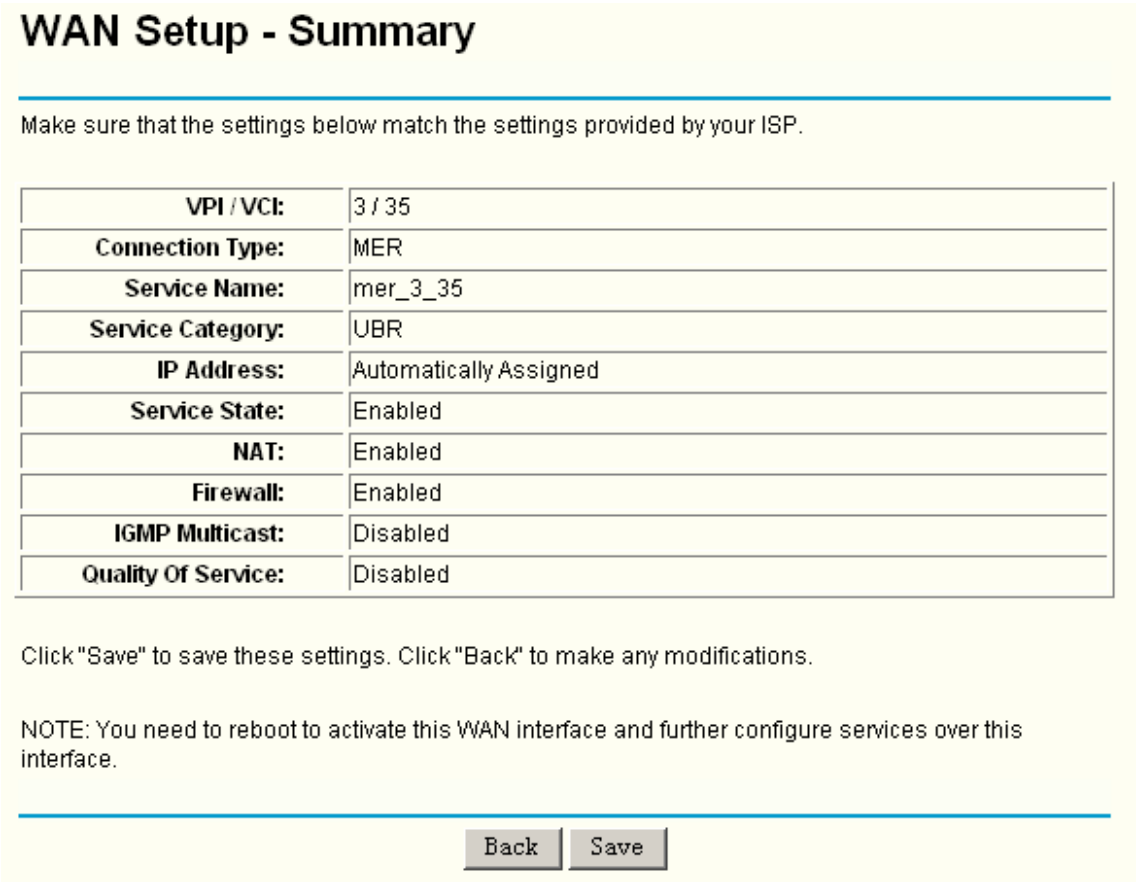

Figure 5-12

6) If you are sure about the configuration, click the **Save** button to save these settings, otherwise click the **Back** button to return to the previous screen to make modifications. The information of the figure shows above is same as the information in the Figure 5-4.

4. IPoA

If you choose **IPoA** in the previous screen (shown in Figure 5-6), the configuration is similar to **MER**.

5. Bridge

If you choose **Bridging** in the previous screen (shown in Figure 5-6), a screen will be displayed as shown below (shown in Figure 5-13).

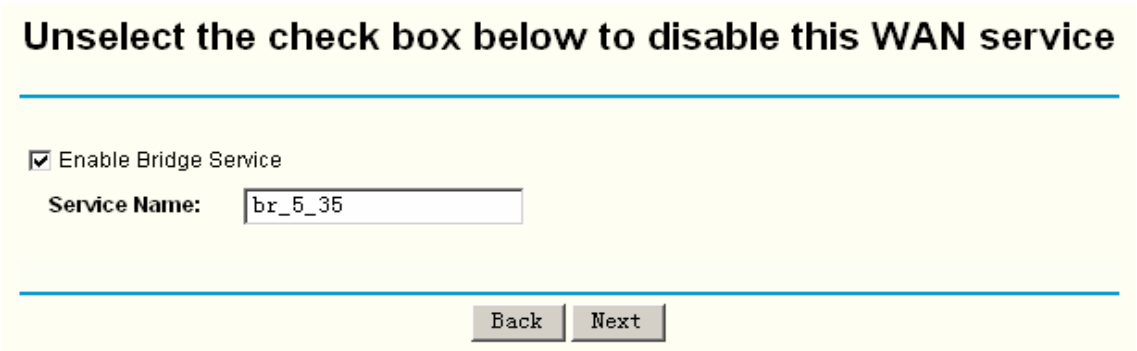

Figure 5-13

1) If you want to adopt the Bridge service, you have to select the **Enable Bridge Service** option in the screen above, or else the service will not take effect
2) Enter the service name in this screen, otherwise leave the default setting.
3) Click the **Next** button, and you will see the next screen which displays the detailed settings you've made (shown in Figure 5-14). Or else click the **Back** button to return to the previous screen to make modifications.

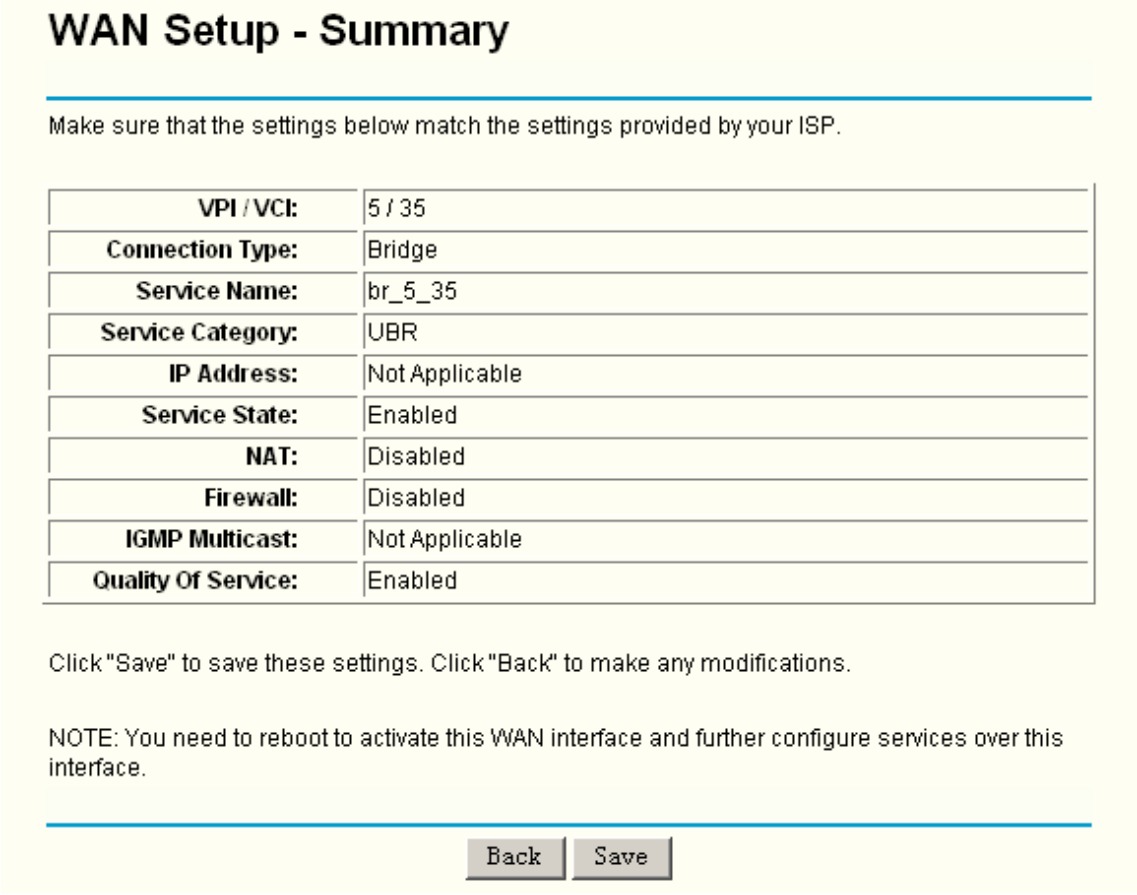

Figure 5-14

4) If you are sure about the configuration, click the **Save** button to save these settings, otherwise click the **Back** button to return to the previous screen to make modifications. The information of the figure shows above is same as the information in the Figure 5-4.

5.4.2 LAN

Choose "**Advanced Setup**"→"**LAN**", and you will see the LAN screen (shown in Figure 5-15)，the section allows you to configure the Router's LAN ports settings.

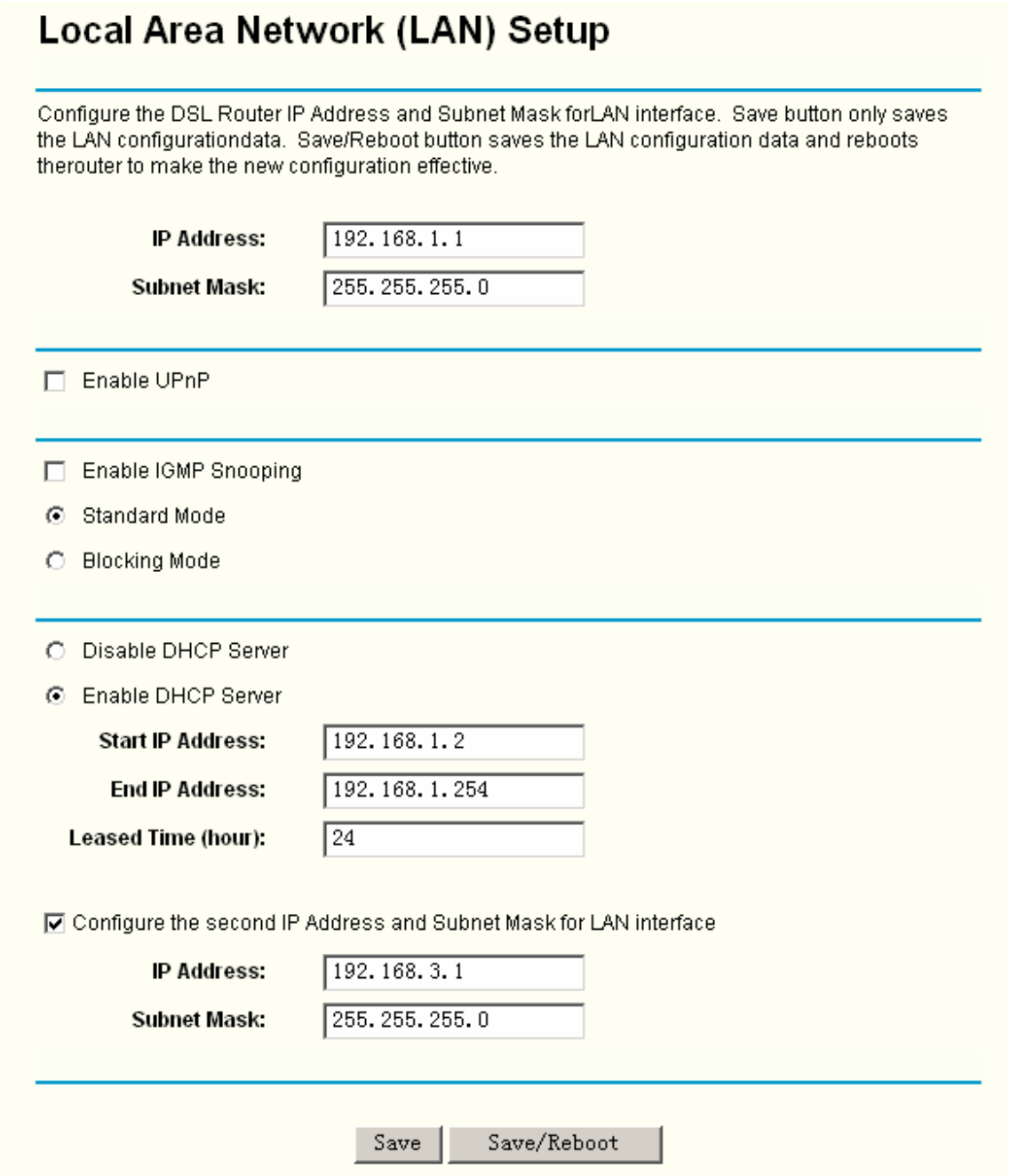

Figure 5-15

- **IP Address:** You can configure the Router's IP Address and Subnet Mask for LAN Interface.
  - **IP Address:** Enter the Router's local IP Address, then you can access to the Web-based Utility via the IP Address, the default value is 192.168.1.1.
  - **Subnet Mask:** Enter the Router's Subnet Mask, the default value is 255.255.255.0.
- **Enable UPnP:** If you need the UPnP function, select the check box to enable it.
- **Enable IGMP Snooping:** If you select the option, please choose the IGMP Mode**::** Standard Mode or Blocking Mode.
- **DHCP Server:** These settings allow you to configure the Router's Dynamic Host Configuration Protocol (DHCP) server function. The DHCP server is enabled by default for the Router's Ethernet LAN interface. DHCP service will supply IP settings to computers which

are configured to automatically obtain IP settings that are connected to the Router though the Ethernet port. When the Router is set for DHCP, it becomes the default gateway for DHCP client connected to it. Keep in mind that if you change the IP address of the Router, you must change the range of IP addresses in the pool used for DHCP on the LAN.

- **Start IP Address:** Enter a value for the DHCP server to start with when issuing IP addresses. Because the default IP address for the Router is 192.168.1.1, the default Start IP Address is **192.168.1.2**, and the Start IP Address must be 192.168.1.2 or greater, but smaller than 192.168.1.254.
- **End IP Address:** Enter a value for the DHCP server to end with when issuing IP addresses. The End IP Address must be smaller than 192.168.1.254. The default End IP Address is **192.168.1.254**.
- **Leased Time (hour):** The Leased Time 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 hours, then the user will be "leased" this dynamic IP address. After the dynamic IP address has expired, the user will be automatically assigned a new dynamic IP address. The default is **24** hours.

➢ **Configure the second IP Address and Subnet Mask:** You can configure the Router's second IP Address and Subnet Mask for LAN Interface though which you can also access to the Web-based Utility as the default IP Address and Subnet Mask.

Note:

UPnP, DHCP Server and the second IP Address are not available for the connection type of **Bridge** here, they won't display on the screen above since only Bridge is selected.

5.4.3 NAT

When you select **PPPoA** or **PPPoE** for the WAN Setup, or when you select **Enable NAT** (shown in Figure 5-11) for the type of **MER** or **IPoA** connection, you will see the **NAT** menu in the Web-based Utility (shown in Figure 5-16).

Figure 5-16

Choose "**Advanced Setup**"→"**NAT**", there are four submenus under the main menu**: Virtual Servers**, **Port Triggering**, **DMZ Host** and **ALG**. Click any of them, and you will be able to configure the corresponding function.

5.4.3.1. Virtual Servers

Choose "**Advanced Setup**"→"**NAT**"→"**Virtual Servers**", you can set up virtual servers on the screen below (shown in Figure 5-17).

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 the Internet to this service port will be redirected to the computer specified by the server IP. Any PC that was used for a virtual server must have a static or reserved IP Address because its IP Address may change when using the DHCP function.

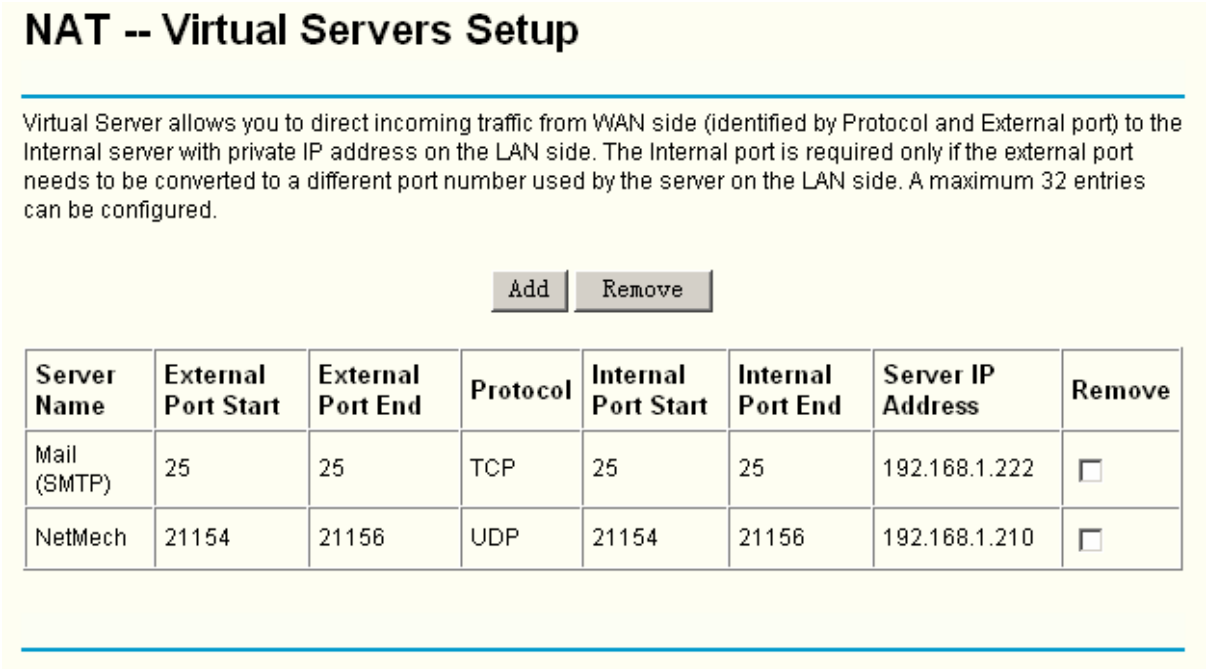

Figure 5-17

- **Virtual Server Table:** The table indicates the information about the Virtual Server entries.
  - **Server Name:** This is the name of the **Virtual Server**. It is exclusive and must be filled in.
  - **External Port Start:** The base number of External Ports. You can type a service port or leave it blank.
  - **External Port End:** The end number of External Ports. You can type a service port or leave it blank.
  - **Protocol:** The protocol used for this application, **TCP**, **UDP**, or **TCP/UDP**.
  - **Internal Port Start:** The base number of Internal Ports. You can type a service port or leave it blank.
  - **Internal Port End:** The end number of Internal Ports. You can type a service port or leave it blank.
  - **Server IP Address:** The IP Address of the PC providing the service application.
- **Add:** Click the **Add** button to add a new entry.
- **Remove:** Select the check box in the table (shown in Figure 5-17) and then click the **Remove** button, then the corresponding entry will be deleted in the table.

To setup a virtual server entry:

1. Click the **Add** button on the screen above (pop-up Figure 5-17), and then you will set the new Virtual Server in the next screen (shown in Figure 5-18).

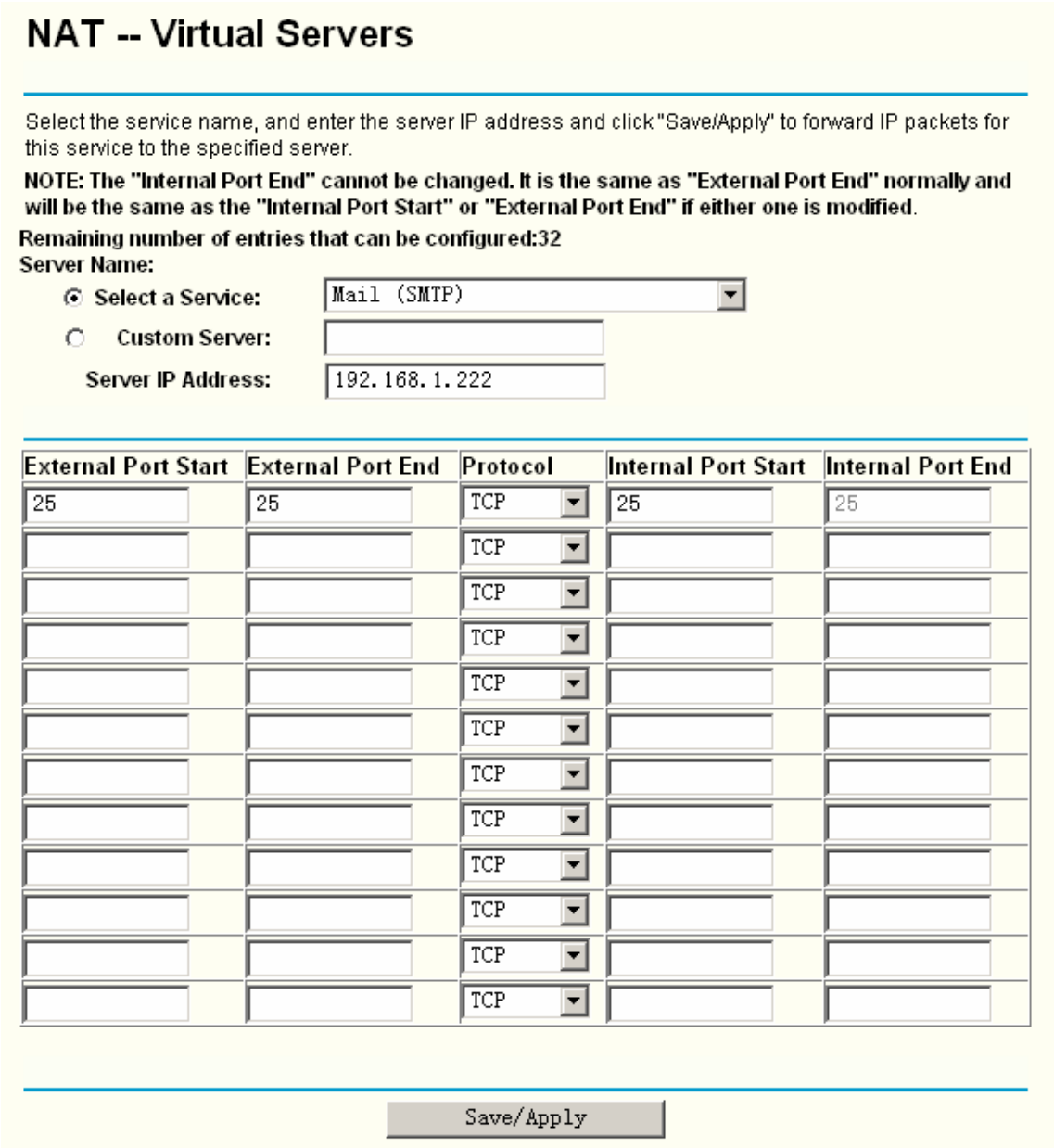

Figure 5-18

2. Select the service which you want to use from the drop-down list. If the list does not have the service you need, type the name of the custom service in the text box.
3. Type the IP Address of the computer in the **Server IP Address** text box.
4. Enter the External Port Start, External Port End, Internal Port Start and Internal Port End in the table, and then select the protocol used for this Virtual Server, **TCP**, **UDP** or **All**.
5. Click the **Save/Apply** button to enable virtual server.

Note:

If you select the service from the drop-down list, the External Port Start, External Port End, Internal Port Start, Internal Port End and the Protocol will be added in the table automatically. You only need to enter the Server IP Address for the Virtual Server.

5.4.3.2. Port Triggering

Choose "**Advanced Setup**"→"**NAT**"→"**Port Triggering**", you can set Port Triggering on the screen (shown in Figure 5-19).

Some applications require that specific ports in the Router's firewall should be opened for access by remote devices. Port Trigger dynamically opens up the 'Open Ports' in the firewall when an application on the LAN initiates a TCP/UDP connection to a remote device using the triggering ports. The Router allows the remote party from the WAN side to establish new connections back to the application on the LAN side using the open ports. A maximum 32 entries can be configured.

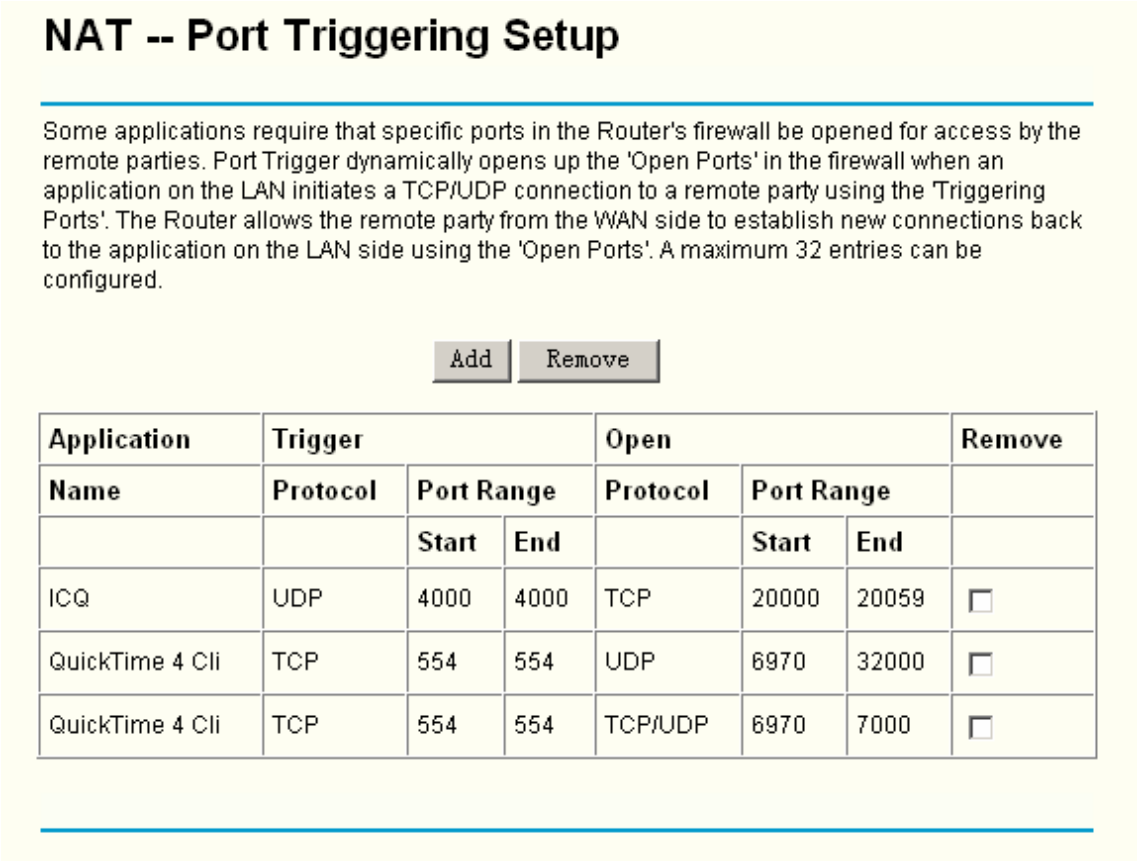

Figure 5-19

- **Port Triggering Table:** The table indicates the information about the Port Triggering entries.
  - **Application (Name):** This is the name of the **Port Triggering**. It is exclusive and must be filled.
  - **Trigger:** It includes the Protocol and the Start and End value of the Trigger Ports.
  - **Open:** It includes the Protocol and the Start and End value of the Open Ports
- **Add:** Click the button to add a new entry.
- **Remove:** Select the check box in the table (shown in Figure 5-19) and then click the **Remove** button, then the corresponding entry will be deleted in the table.

To add a new Port Triggering:

1. Click the **Add** button (pop-up Figure 5-19), and then you will set the new Port Triggering in the next screen (shown in Figure 5-20).

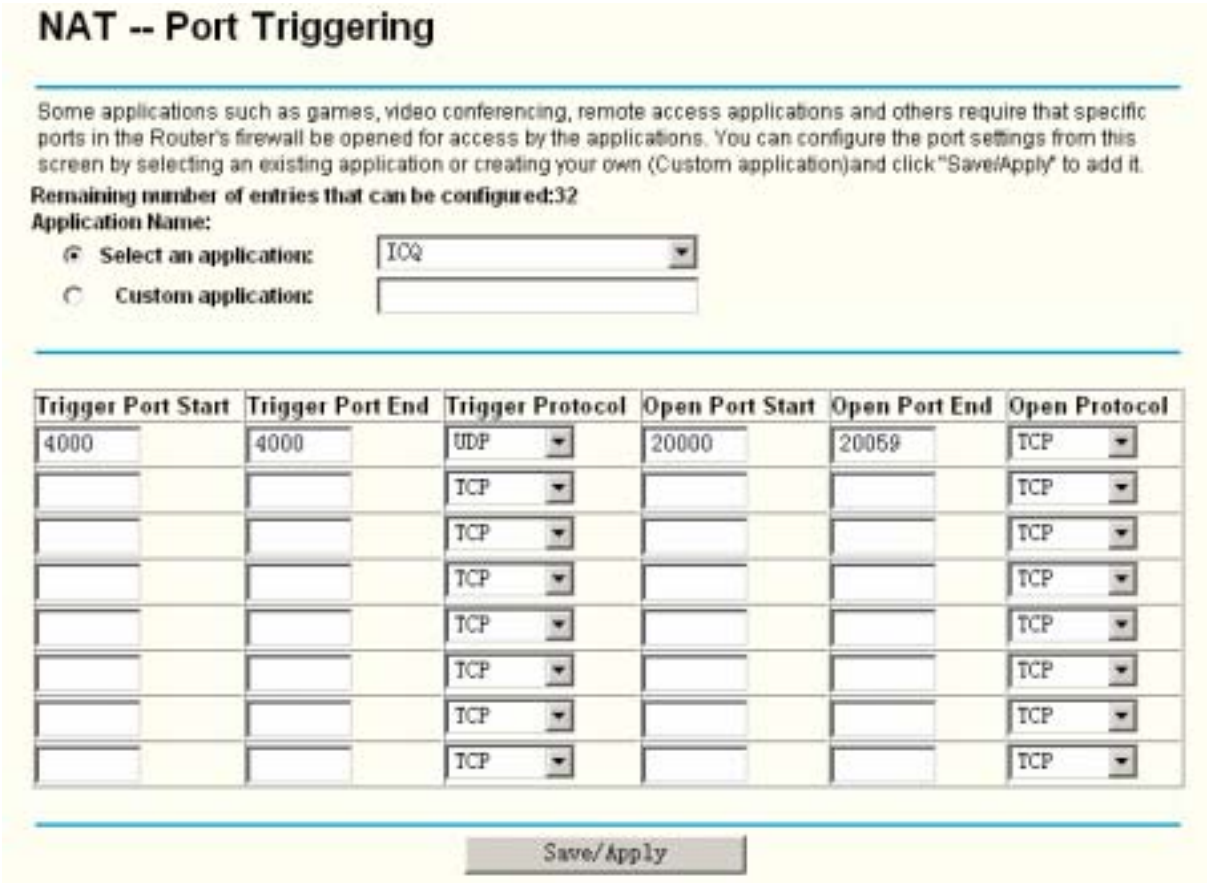

Figure 5-20

2. Select the application from the drop-down list. If the list does not have the application that you want, select the **Custom application** radio-button, and type the name of the custom application in the text box.
3. Enter the **Trigger Port Start**, **Trigger Port End**, **Open Port Start** and **Open Port End** in the table, and then select the **Trigger protocol** and **Open protocol**, **TCP**, **UDP** or **All**.
4. Click the **Save/Apply** button to enable the settings.

Note:

If you select the application from the drop-down list, the External Port Start, External Port End, Internal Port Start, Internal Port End and the Protocol will be added in the table automatically.

5.4.3.3. DMZ Host

Choose "**Advanced Setup**"→"**NAT**"→"**DMZ Host**", you can set up DMZ Host on the screen (shown in Figure 5-21).

The DMZ host feature can make a local host be exposed to the Internet for a special-purpose service, such as online gaming or video conferencing.

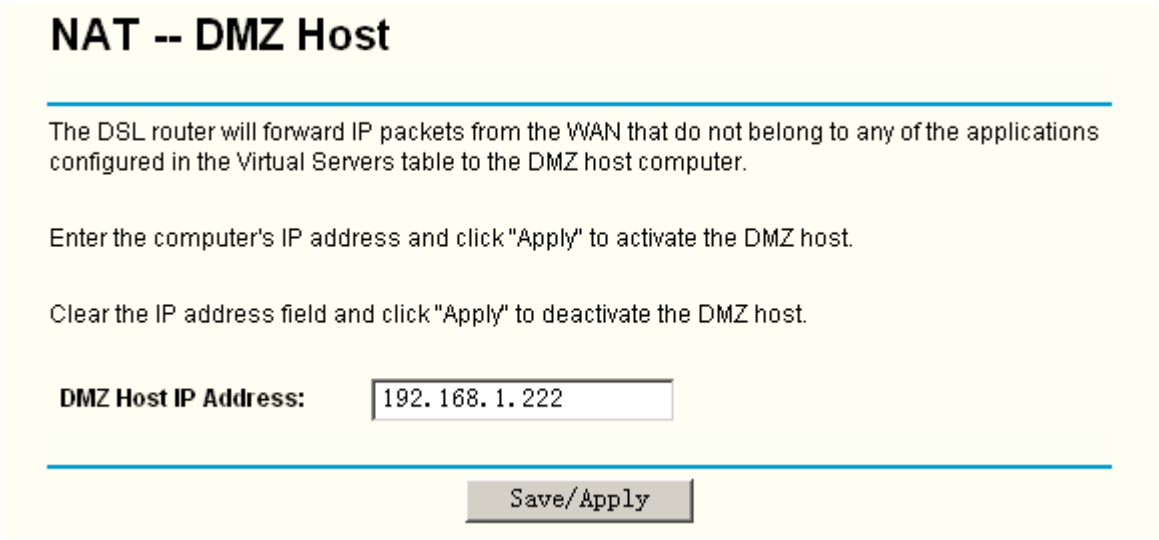

Figure 5-21

To add a new DMZ Host:

You can enter the computer's IP address and then click **Save/Apply** to activate the DMZ host you set on this page.

Note:

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 while using the DHCP function.

5.4.3.4. ALG

Choose "**Advanced Setup**"→"**NAT**"→"**ALG**", you can Enable SIP (Session Initiation Protocol) on the ALG (Application Level Gateway) screen (shown in Figure 5-22).

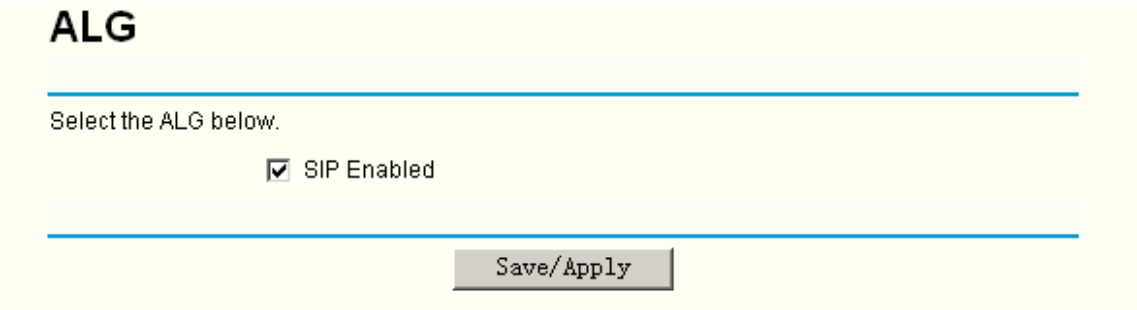

Figure 5-22

5.4.4 Security

When you select the **Enable Security** function (shown in Figure 5-11) for the connection type of **MER** or **IPoA** for the WAN Setup, or when you setup **Bridge**, **PPPoA or PPPoE** mode for WAN interface, you will see the **Security** menu in the Web-based Utility (shown in Figure 5-23). It includes **IP Filtering**, **MAC Filtering** (only effective in Bridge mode) and **Parental Control** submenus.

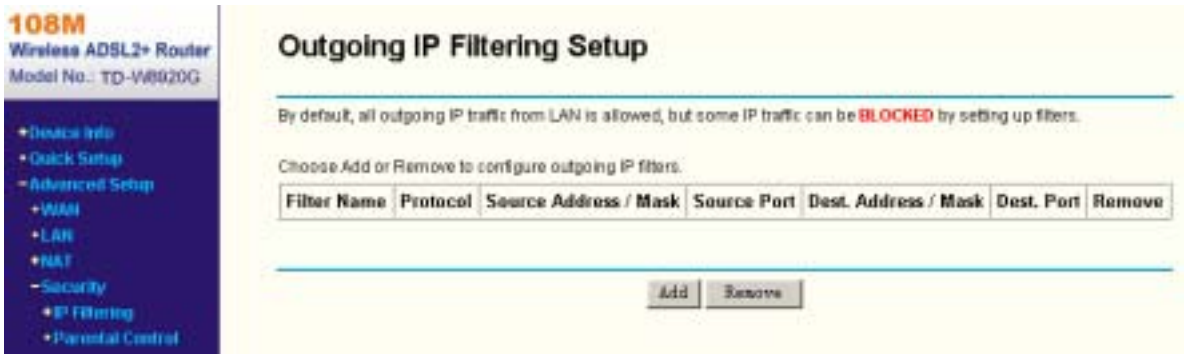

Figure 5-23

5.4.4.1. IP Filtering

The IP address filtering feature makes it possible for administrators to control user's access to the Internet, which is based on user's IP. The IP address filtering includes **Outgoing** and **Incoming**, the detailed descriptions are provided below.

IP Filtering - Outgoing

Choose "**Advanced Setup**"→"**Security**"→"**IP Filtering**"→"**Outgoing**", you can configure Outgoing Filtering rules on the screen (shown in Figure 5-24).

The Outgoing IP Filtering feature allows you to control some IP traffic from LAN to access to some specifically addresses. By default, all outgoing IP traffic from LAN is allowed, but some IP traffic can be **BLOCKED** by setting up filters.

Figure 5-24

Setup an Outgoing IP Filtering rule:

1. Click the **Add** button (pop-up Figure 5-24), then you will set the new rule in the next screen (shown in Figure 5-25).

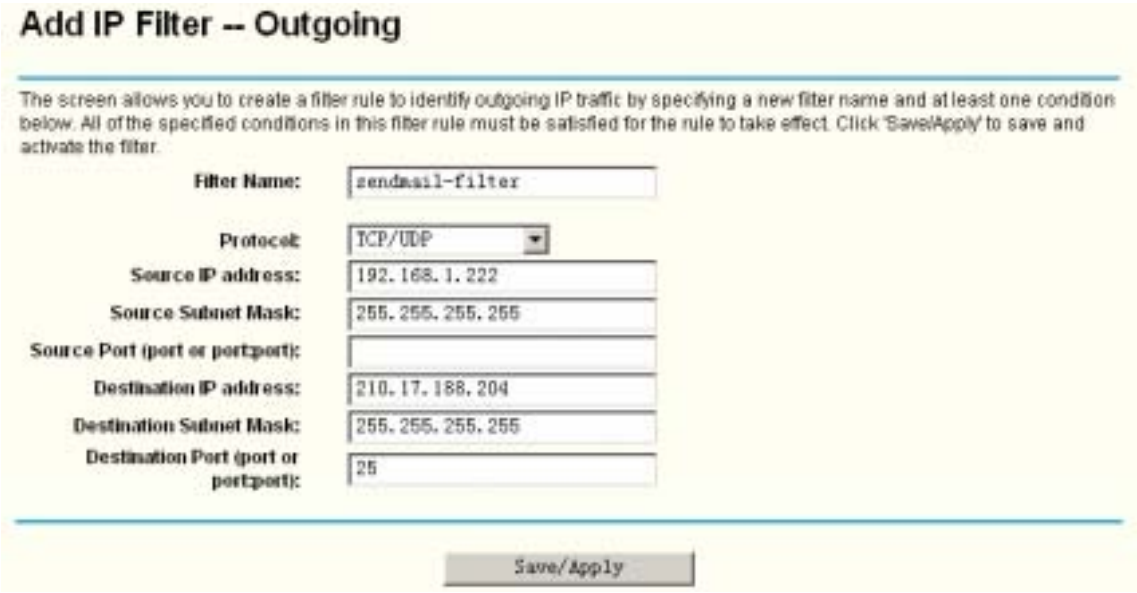

Figure 5-25

2. Enter the **Filter name** for the rule, it is exclusive and must be filled.
3. Select the **protocol: TCP/UDP**, **TCP**, **UDP** or **ICMP** in the drop-down list for the connection between the Source IP address and Destination IP address.
4. Enter a **Source IP Address** in dotted-decimal notation format and then type the **Source Subnet Mask** and **Source Port** (port or port**:** port) in the text boxes separately.
5. Enter a **Destination IP Address** in dotted-decimal notation format and then type the **Destination Subnet Mask** and **Destination Port** (port or port**:** port) in the text boxes separately.
6. Click the **Save/Apply** button to save this entry.

Note:

When you add an Outgoing IP Filtering entry, you must configure at least one condition on the screen above except the Filter name. If you leave the Protocol blank, it means that the rule is effective to all protocols, if you leave the Source IP Address and/or Destination IP Address blank, it suggests that all Source IP Addresses and/or Destination IP Addresses are controlled by the rule, if you leave the Source Port and/or Destination Port blank, it suggests that all Source Ports and/or Destination Ports are controlled by the rule.

IP Filtering - Incoming

Choose "**Advanced Setup**"→"**Security**"→"**IP Filtering**"→"**Incoming**", you can configure Incoming Filtering rules on the screen (shown in Figure 5-26).

The Incoming IP Filtering feature allows some IP traffic from WAN to access some local addresses. By default, all incoming IP traffic from the WAN is blocked when the firewall is enabled. However, some IP traffic can be **ACCEPTED** by setting up filters.

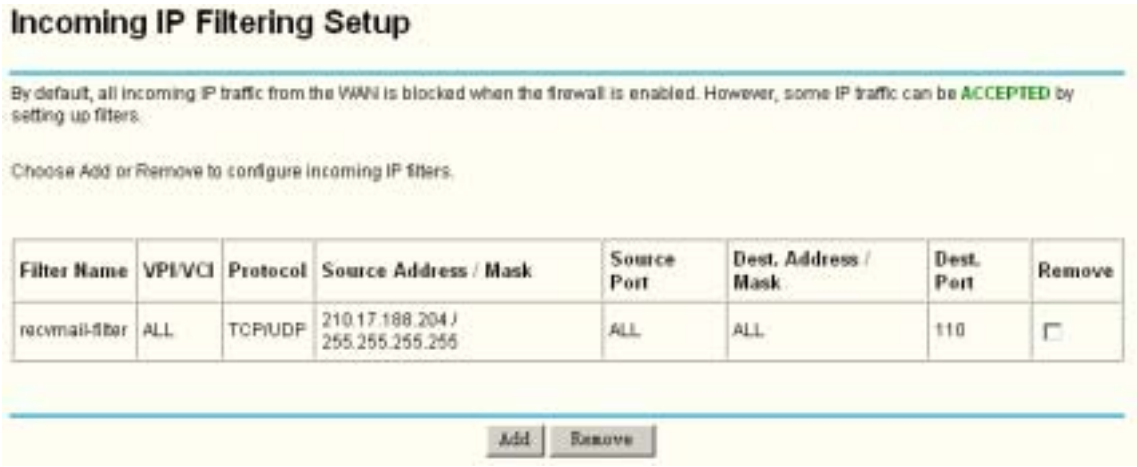

Figure 5-26

Setup an Incoming IP Filtering rule:

1. Click the **Add** button (pop-up Figure 5-26), and then you will set the new rule in the next screen (shown in Figure 5-27).

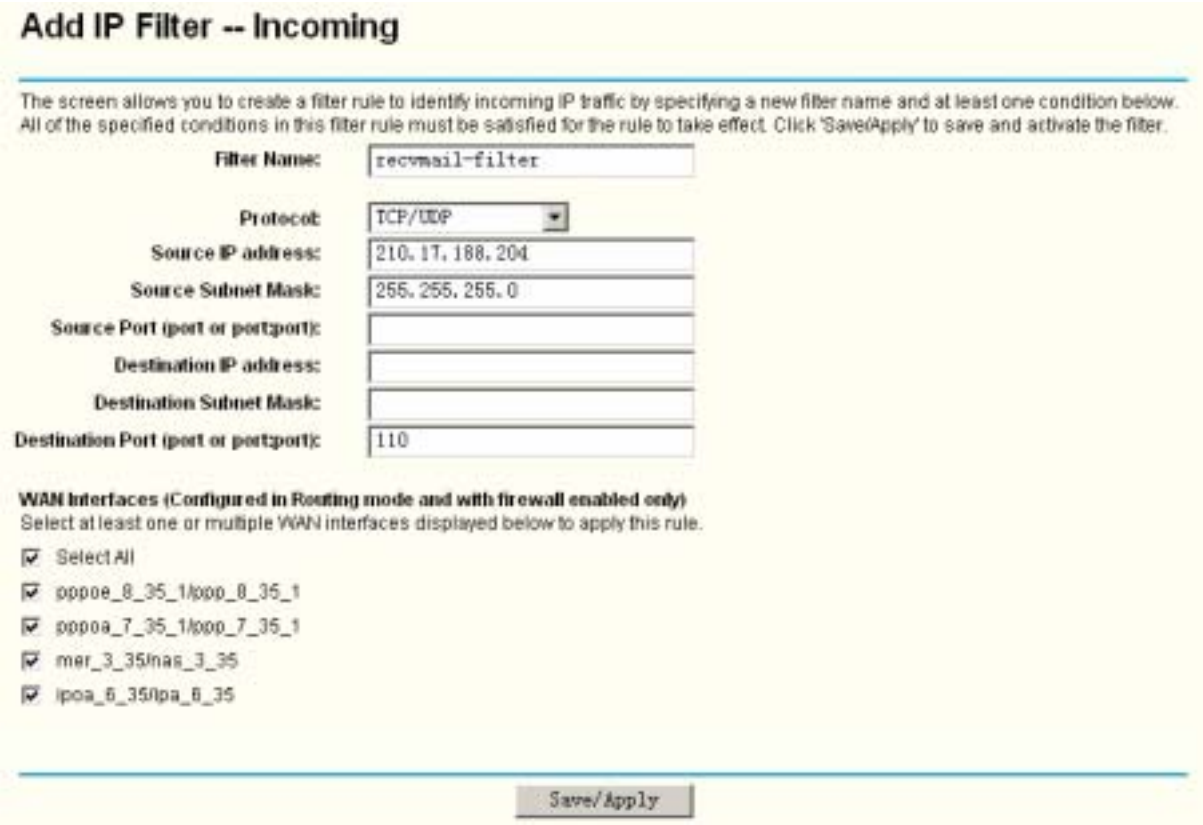

Figure 5-27

2. Enter the **Filter name** for the rule, it is exclusive and must be filled in.
3. Select **Protocol** in the drop-down list, enter **Source IP address**, **Source Subnet Mask**, **Source Port**, **Destination IP address**, **Destination Subnet Mask**, and **Destination Port** for the rule.
4. Select at least one WAN interfaces displayed below to apply this rule.
5. Click the **Save/Apply** button to save this entry.

Note:

When you add a Incoming IP Filtering entry, you must configure at least one condition on the screen above except the Filter name. If you leave **Protocol** blank, it means that the rule is effective to all protocols, if you leave the Source IP address and/or Destination IP address blank, it suggests that all Source IP addresses and/or Destination IP addresses are controlled by the rule, if you leave the Source Port and/or Destination Port blank, it suggests that all Source Ports and/or Destination Ports are controlled by the rule.

5.4.4.2. MAC Filtering

Choose "**Advanced Setup**"→"**Security**"→"**MAC Filtering**", you can configure MAC Filtering rules on the screen (shown in Figure 5-28). The section allows you to control access to the Internet by users on your local network based on their MAC Address.

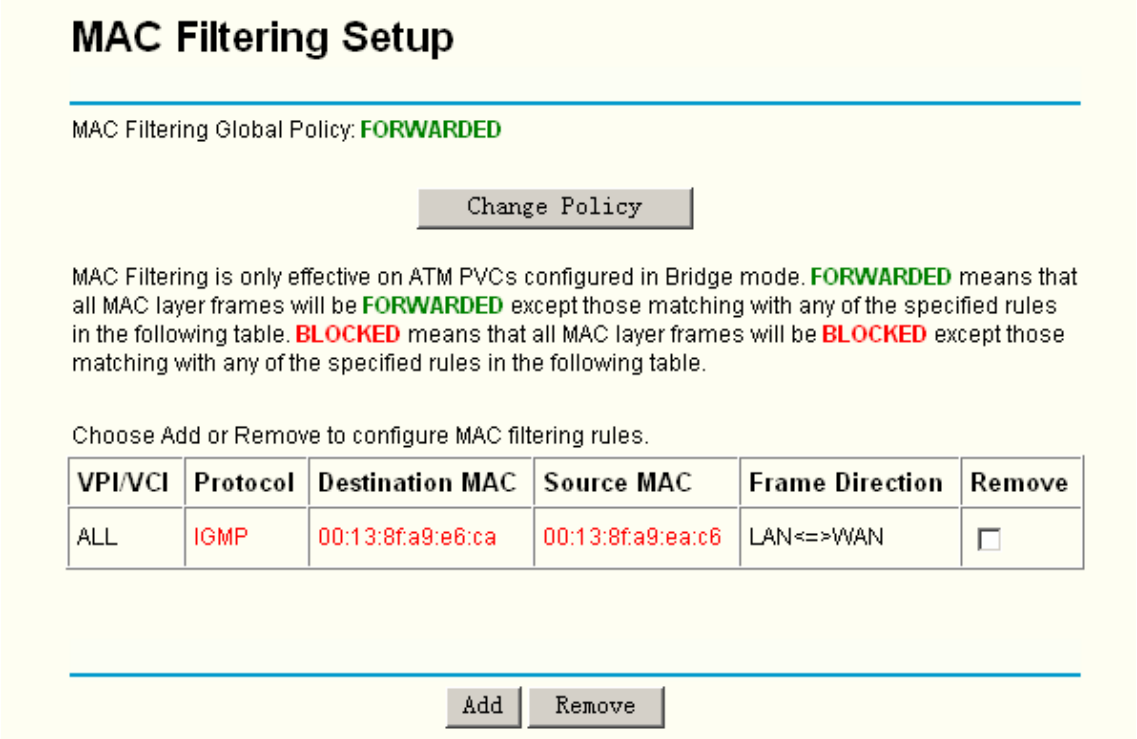

Figure 5-28

- **Change Policy:** There are two policies for the MAC filters**: FORWARDED** and **BLOCKED**. Click the button to change from one policy to another. When you select **FORWARDED**, it means that all MAC layer frames will be **forwarded** except those matching with any of the specified rules in the table (shown in Figure 5-28). While **BLOCKED** means that all MAC layer frames will be **blocked** except those matching with any of the specified rules in the table above.
- **Add:** Click the **Add** button, and then you can add a new MAC Filter in the next screen (shown in Figure 5-28).
- **Remove:** Select the check box in the table (shown in Figure 5-28) and then click the **Remove** button, and then the corresponding entry will be deleted in the table.

To setup a MAC Filtering rule:

1. Click the **Add** button (pop-up Figure 5-28), then you will set the new rule in the next screen (shown in Figure 5-29).

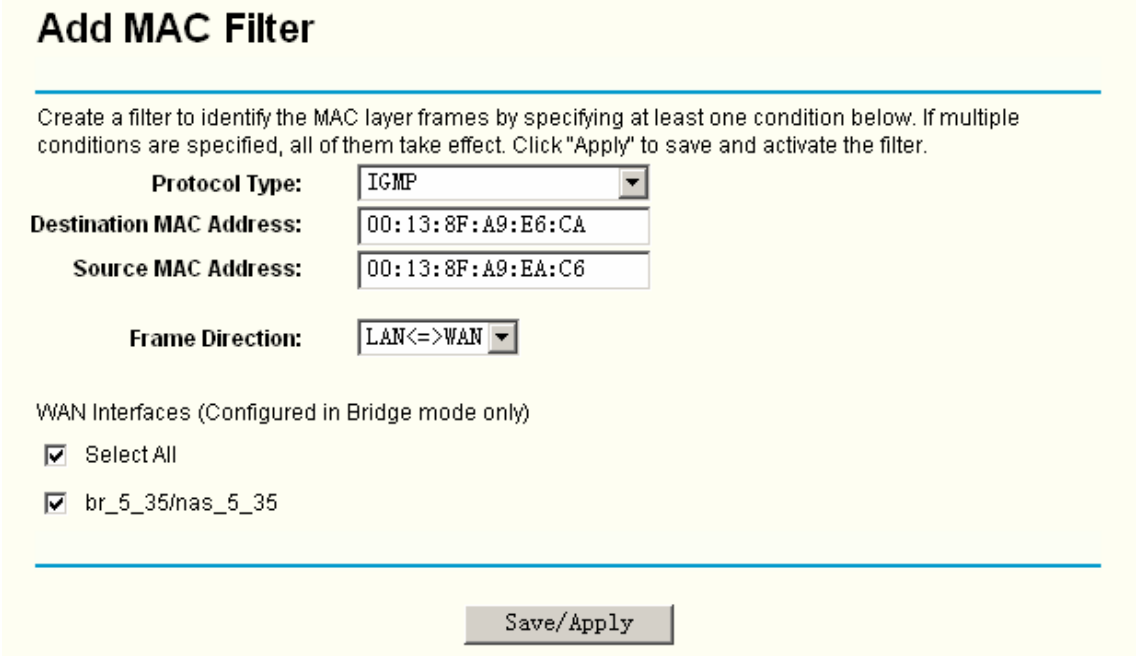

Figure 5-29

2. Select **Protocol Type** in the drop-down list for the rule.
3. Enter **Destination MAC Address** and **Source MAC Address** in the text box.
4. Select **Frame Direction** in the drop-down list for the rule.
5. Select the **WAN interfaces**, you can leave the default settings also.
6. Click the **Save/Apply** button to save this entry.

Note:
MAC Filtering is only effective on ATM PVC(s) configured in Bridge mode.

5.4.4.3. Parental Control

Choose "**Advanced Setup**"→"**Security**"→"**Parental Control**". You can configure the Parental Control rules on the screen (shown in Figure 5-30). This section allows you add time of day restriction to a special LAN device connected to the Router.

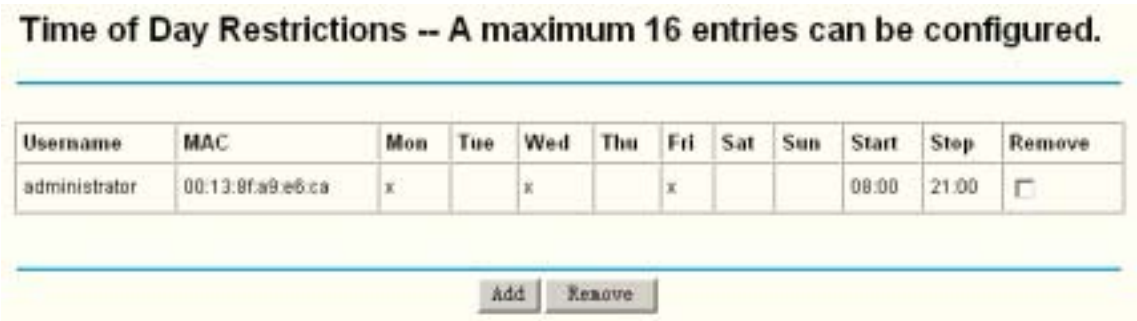

Figure 5-30

To setup a Parental Control rule:

1. Click the **Add** button (pop-up Figure 5-30), and then you will set the new rule in the next screen (shown in Figure 5-31).

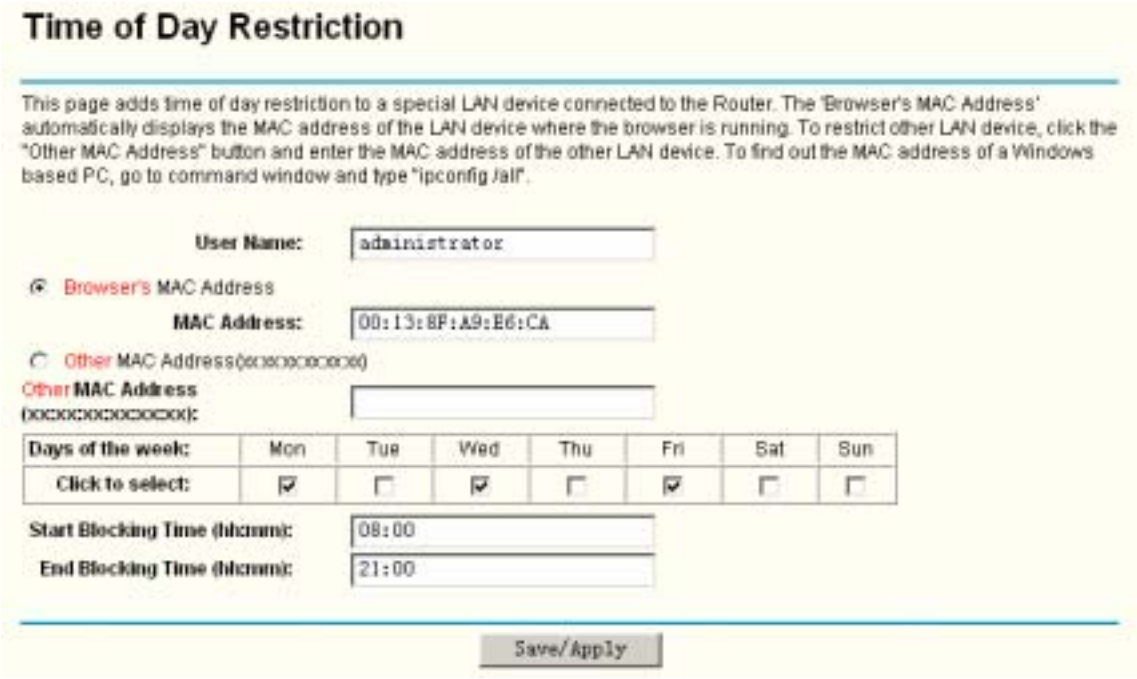

Figure 5-31

2. Enter the **User Name** of the LAN device connected to the Router.
3. To restrict the device where the browser is running, select the **Browser's MAC Address** radio-button, its MAC Address has automatically displayed in the text box. To restrict other LAN devices, click the **Other MAC Address** radio-button and enter the MAC address of the other LAN device.
4. Select the day when the rule will take effect in the table.
5. Enter the **Start Blocking Time** and **End Blocking Time** in the text box separately, and then the device controlled will then be unable to connect to the internet during that time.
6. Click the **Save/Apply** button to save this entry.

5.4.5 Quality of Service

When you select **Enable Quality Of Service** check box (shown in Figure 5-5) for the WAN configuration, the **Quality Of Service** menu will be added to the Web-based Utility. Choose "**Advanced Setup**"→"**Quality Of Service**", you can configure QoS (Quality of Service) on the screen (shown in Figure 5-32).

Figure 5-32

Click the **Add** button, and you can configure the QoS on the next screen (shown in Figure 5-33).

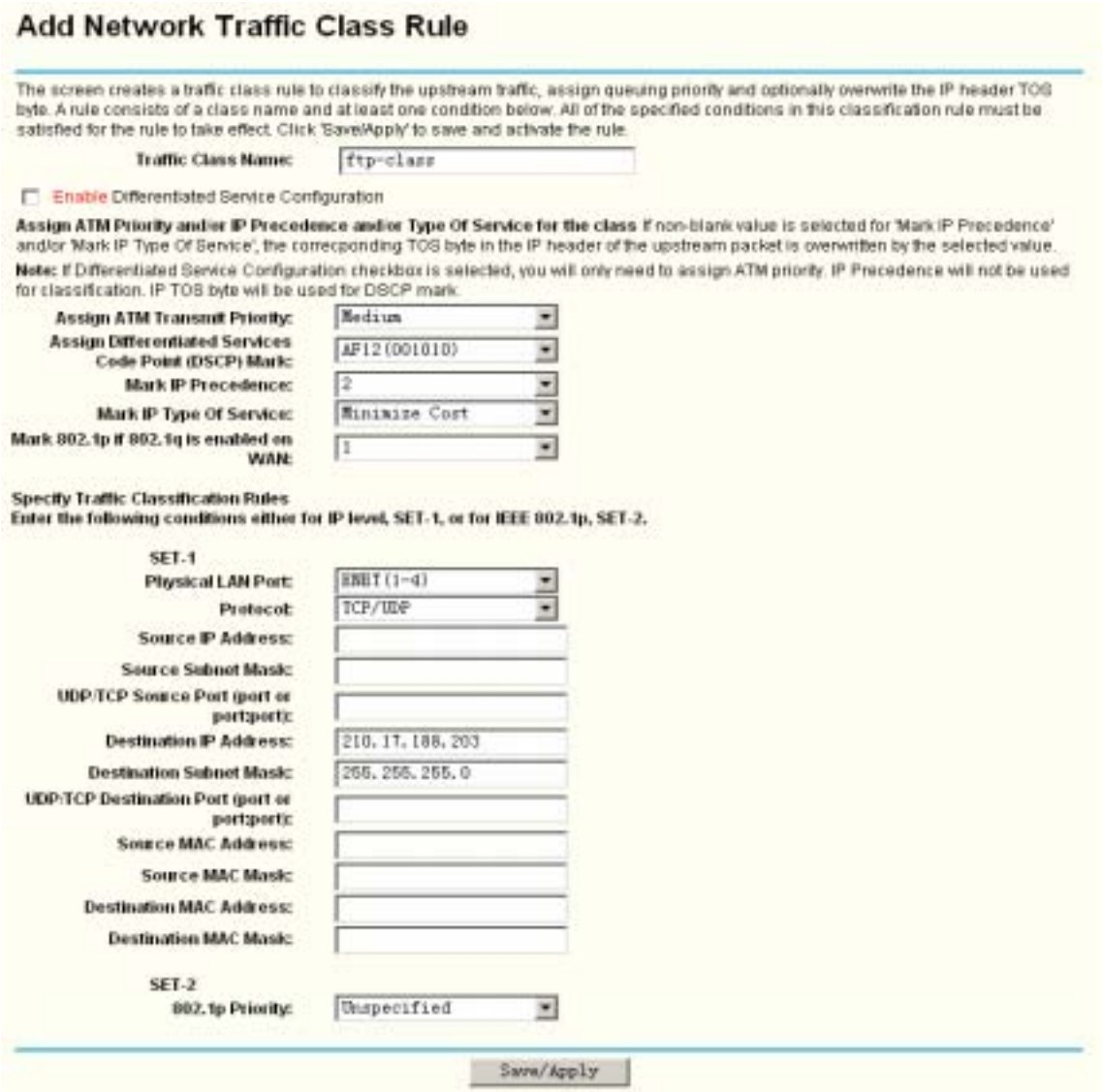

Figure 5-33

After you specify the condition, click the **Save/Apply** button to save the entry.

Note:
A rule must be consisting of a class name and at least one condition above. All of the specified conditions in this classification rule must be satisfied with the rule to take effect.

5.4.6 Routing

Choose "**Advanced Setup**"→"**Routing**", it includes three menus**: Default Gateway**, **Static Route and RIP (**shown in Figure 5-34). The detailed descriptions are provided below.

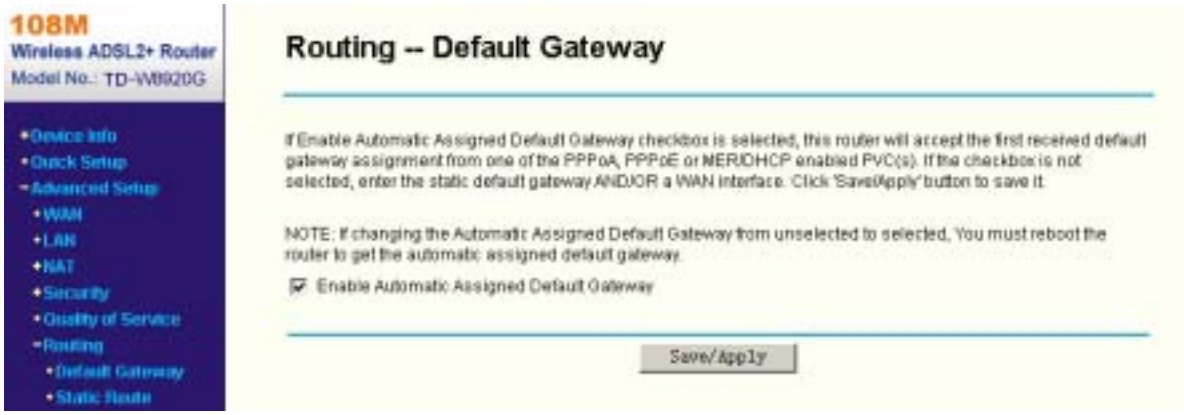

Figure 5-34

5.4.6.1. Default Gateway

Choose "**Advanced Setup**"→"**Routing**"→"**Default Gateway**", you can see the Default Gateway screen, this screen allows you to configure the default gateway (shown in Figure 5-35).

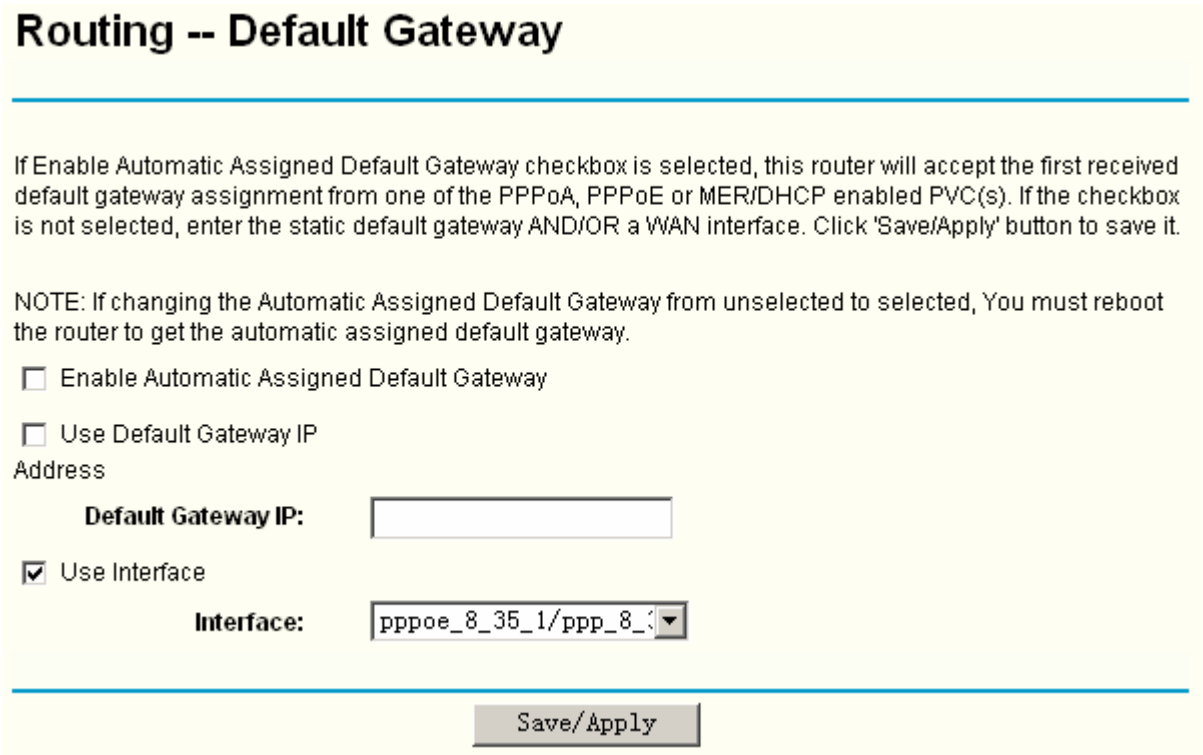

Figure 5-35

If the **Enable automatic Assigned Default Gateway** check-box is selected, this Router will accept the first received default gateway assignment from one of **PPPoA, PPPoE** or **MER/DHCP** enabled PVC(s). If the check-box is not selected, enter the static **Default Gateway IP** and/or a WAN **Interface**, you can leave the WAN Interface default. Then click **Save/Apply** button to save it.

Note:
If changing the Automatic Assigned Default Gateway from unselected to selected, you have to reboot the Router to get the automatically assigned default gateway.
Default Gateway IP address should be specified since MER Interface is selected when you select the **Enable automatic Assigned Default Gateway** check box.

5.4.6.2. Static Route

Choose "**Advanced Setup**"→"**Routing**"→"**Static Route**". You can see the Static Route screen, this screen allows you to configure the static routes (shown in Figure 5-36). A static route is a pre-determined path that network information must travel to reach a specific host or network.

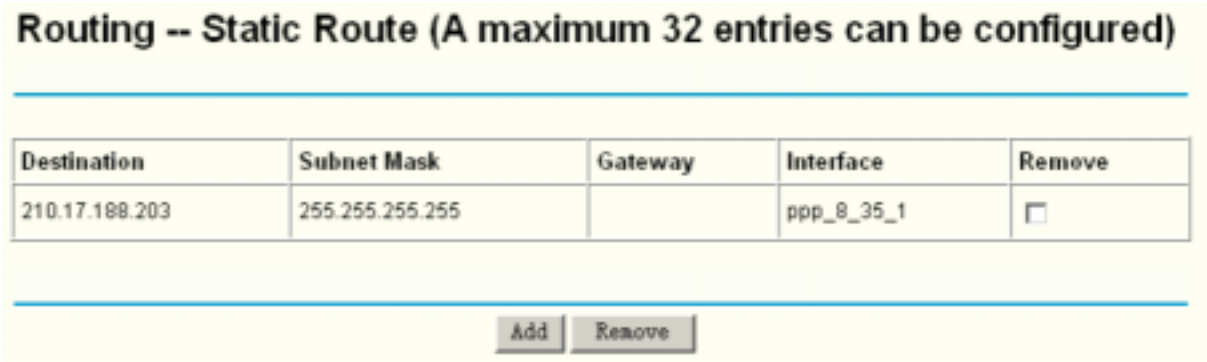

Figure 5-36

To add static routing entries:

1. Click the **Add** button (pop-up Figure 5-37), and you will see the screen below (shown in Figure 5-37).

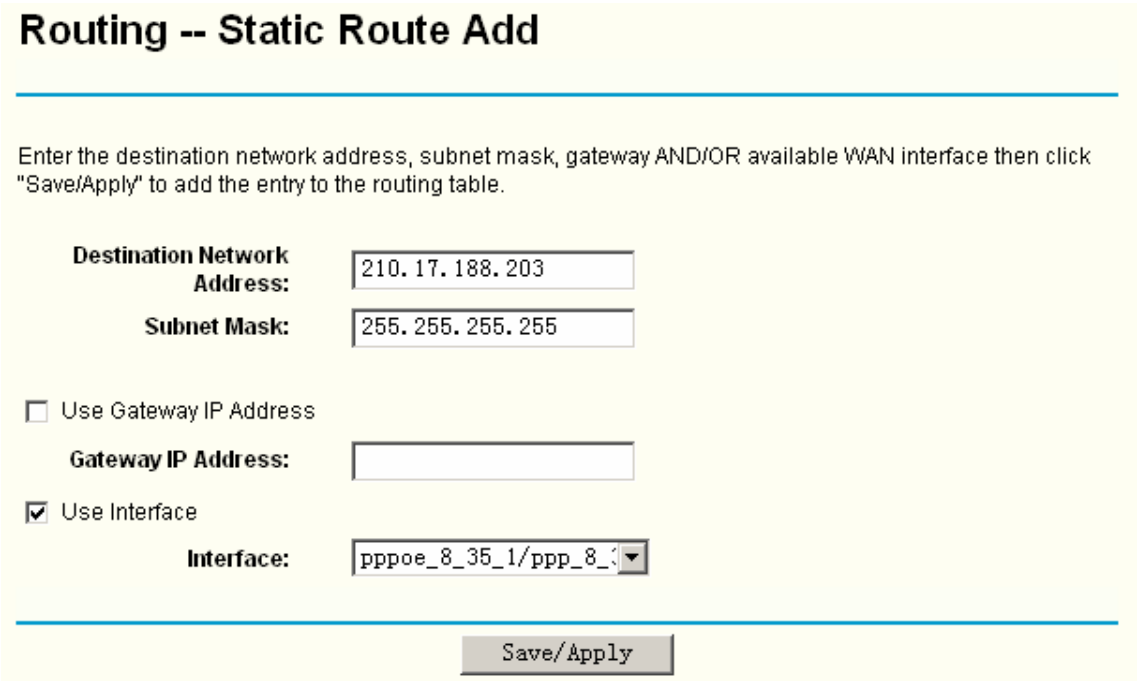

Figure 5-37

2. Enter the following data:

- **Destination Network Address:** The **Destination Network 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.
- **Gateway IP Address:** If the **Use Gateway IP Address** checkbox is selected, you should type the Gateway address exactly in the text box, or else, the default Gateway address will be adopted for the Static Route.
- **Use Interface:** If the **Use Interface** checkbox is selected, you should select the Interface name in the text box, or else, the default Use Interface will be adopted for the Static Route.

3. Click the **Save/Apply** button to save it.

To remove a static routing entry:

1. Select the **Remove** check box according to the entry in the Figure 5-36.
2. Click the **Remove** button, and the entry will be deleted.

Note:

Default Gateway IP address should be specified since MER Interface is selected

5.4.6.3. RIP

Choose "**Advanced Setup**"→"**Routing**"→"**RIP**", you can see the RIP (Routing Information Protocol) screen, this screen allows you to configure the RIP (shown in Figure 5-38).

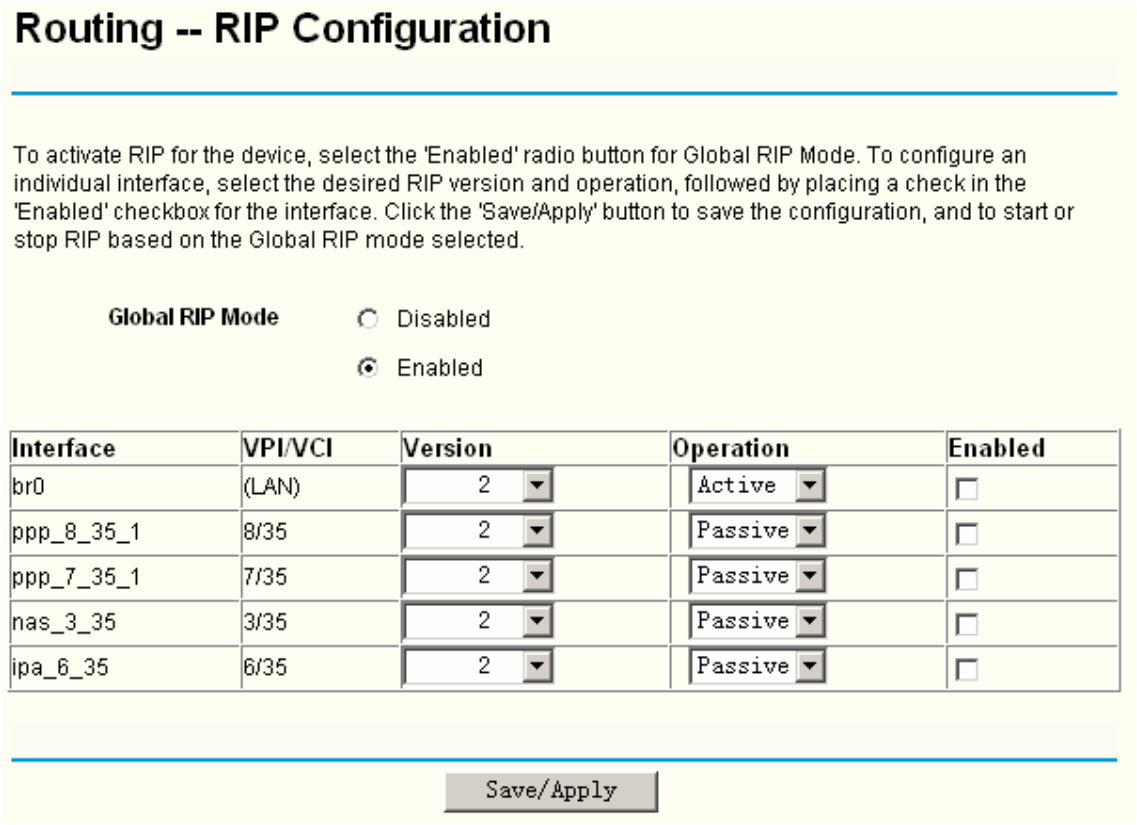

Figure 5-38

To activate RIP for the device, select the **Enabled** radio-button for **Global RIP Mode**. To configure an individual interface, select the desired RIP version and operation, followed by placing a check in the **Enabled** checkbox for the interface.

If you are sure about the settings, click the **Save/Apply** button to save the configuration.

5.4.7 DNS

When you select the connection type **PPPoE, PPPoA**, **MER** or **IPoA** for WAN configuration, you will see the **DNS** menu in the Web-based Utility (shown in Figure 5-39). It includes **DNS Server** and **Dynamic DNS** submenus.

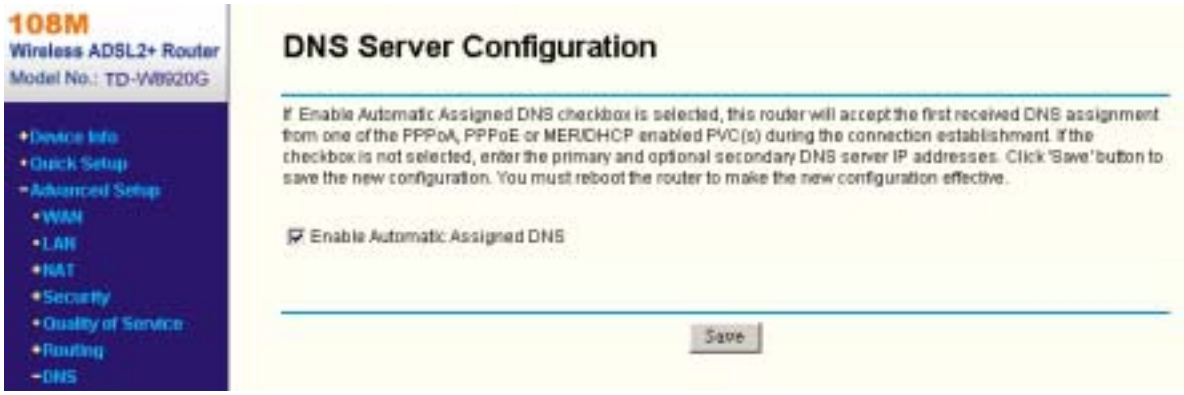

Figure 5-39

5.4.7.1. DNS Server

Choose "**Advanced Setup**"→"**DNS**"→"**DNS Server**". You can see the **DNS Server** screen, this screen allows you to configure the DNS Server Addresses (shown in Figure 5-40).

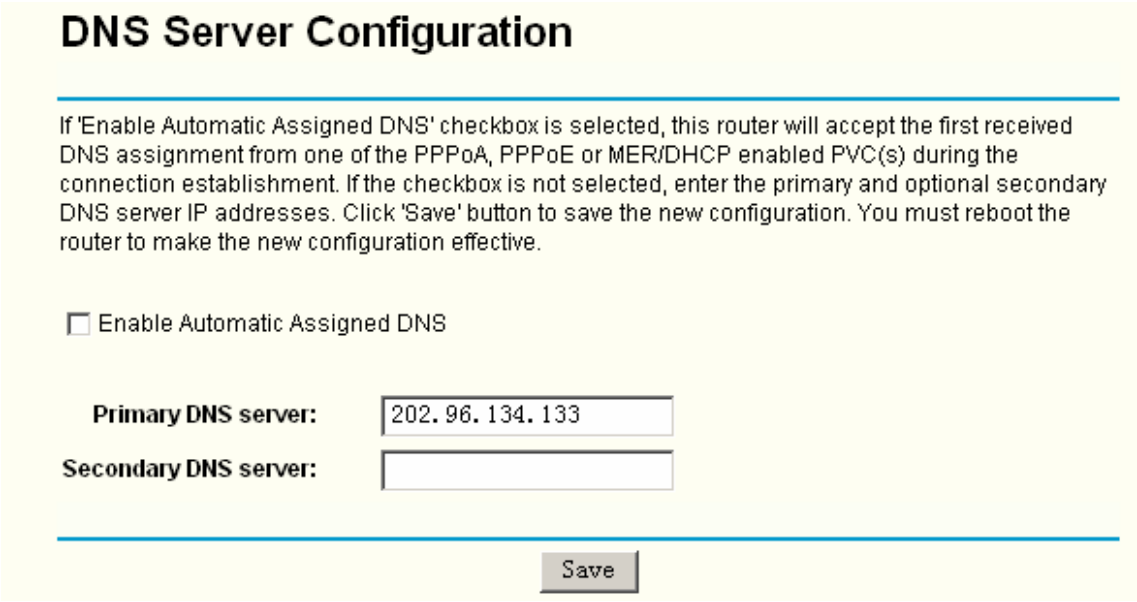

Figure 5-40

If you select **Enable Automatic Assigned DNS**, this Router will accept automatically the first received DNS assignment from one of **PPPoA**, **PPPoE** or **MER/DHCP** enabled PVC(s) during the connection establishment. If the checkbox is not selected, please enter the primary and /or optional secondary DNS server IP addresses provided by your ISP. Then click the **Save** button to save the new configuration.

Note:
You have to reboot the Router to make the new configuration take effect.

5.4.7.2. Dynamic DNS

Choose "**Advanced Setup**"→"**DNS**"→"**Dynamic DNS**", you can see the **Dynamic DNS** screen, this screen allows you to configure the Dynamic DNS (shown in Figure 5-41).
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. The Dynamic DNS service allows you to alias a dynamic IP address to a static hostname in any of the many domains, allowing your Router to be more easily accessed from various locations on the Internet.

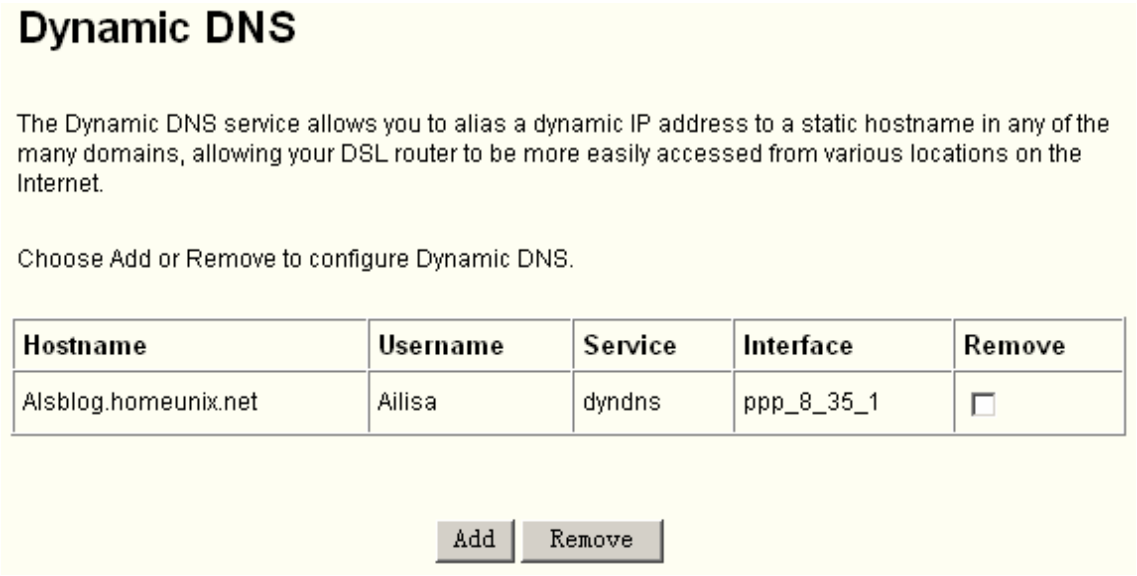

Figure 5-41

To setup DDNS, follow these instructions:

1. Click the **Add** button (pop-up Figure 5-41), then you will set the DDNS in the next screen (shown in Figure 5-42).

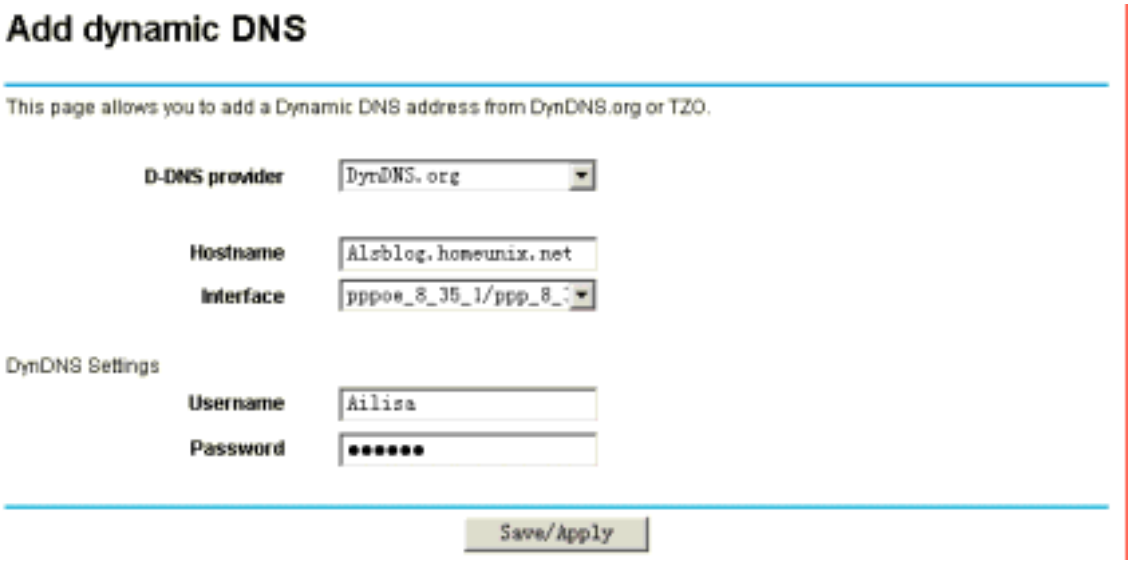

Figure 5-42

2. Select **D-DNS provider** in the drop-down list.
3. Enter the Hostname of the DNS Server, and select the corresponding Interface for the DDNS, you can leave it default.
4. Type the **User Name** and **Password** for your DDNS account.
5. Click the **Save/Apply** button to save the entry.

5.4.8 DSL

Choose "**Advanced Setup**"→"**DSL**", you can see the DSL Settings screen, this screen allows you to configure the DSL (shown in Figure 5-43).

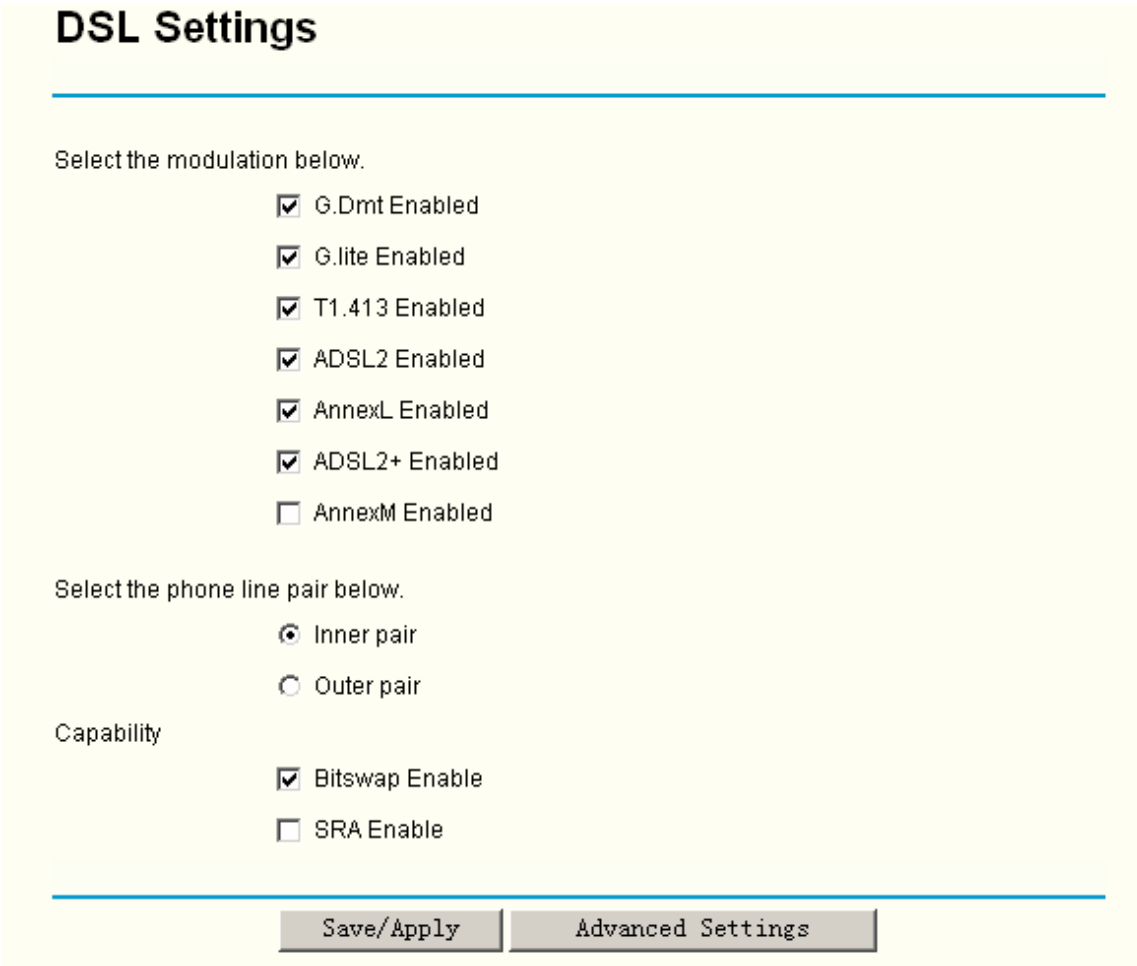

Figure 5-43

You can select the modulation type, phone line pair and the capability of Bitswap or SRA. After you set them up, click the **Save/Apply** button to save the configurations.

5.4.9 Port Mapping

Choose "**Advanced Setup**"→"**Port Mapping**", you can see the Port Mapping screen, this screen allows you to configure the Dynamic DNS (shown in Figure 5-44).

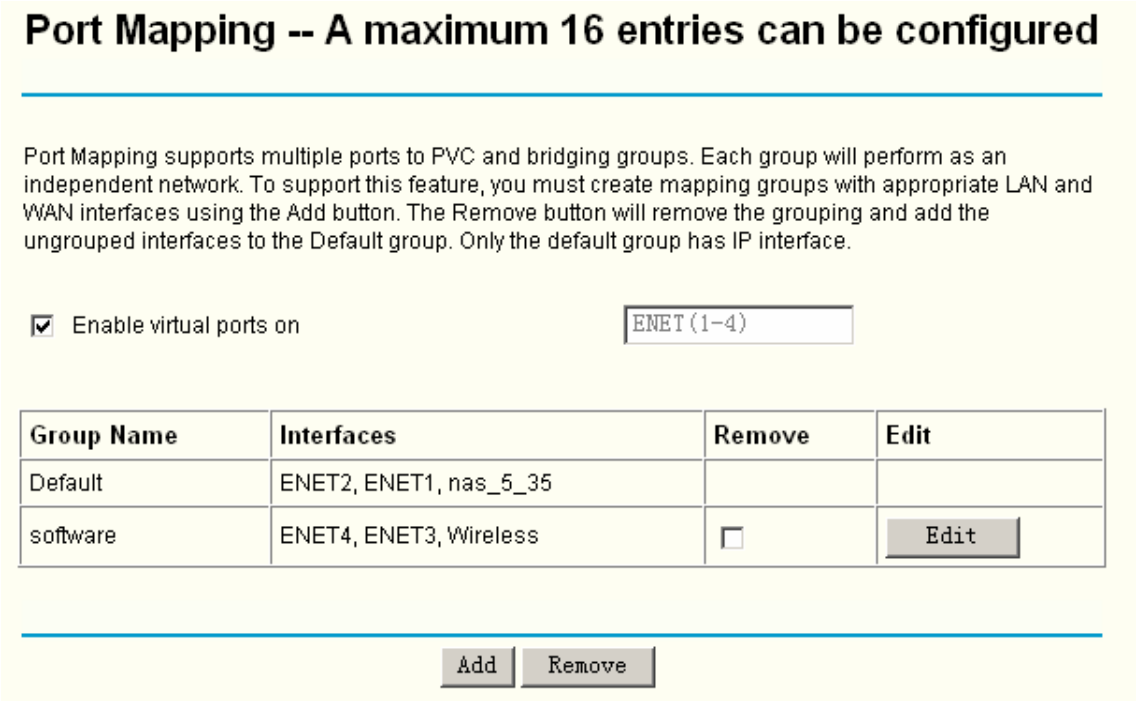

Figure 5-44

Click the **Add/Edit** button, and then you can configure the Port Mapping in the next screen (shown in Figure 5-45). After you configure the settings, click the **Save/Apply** button to save it.

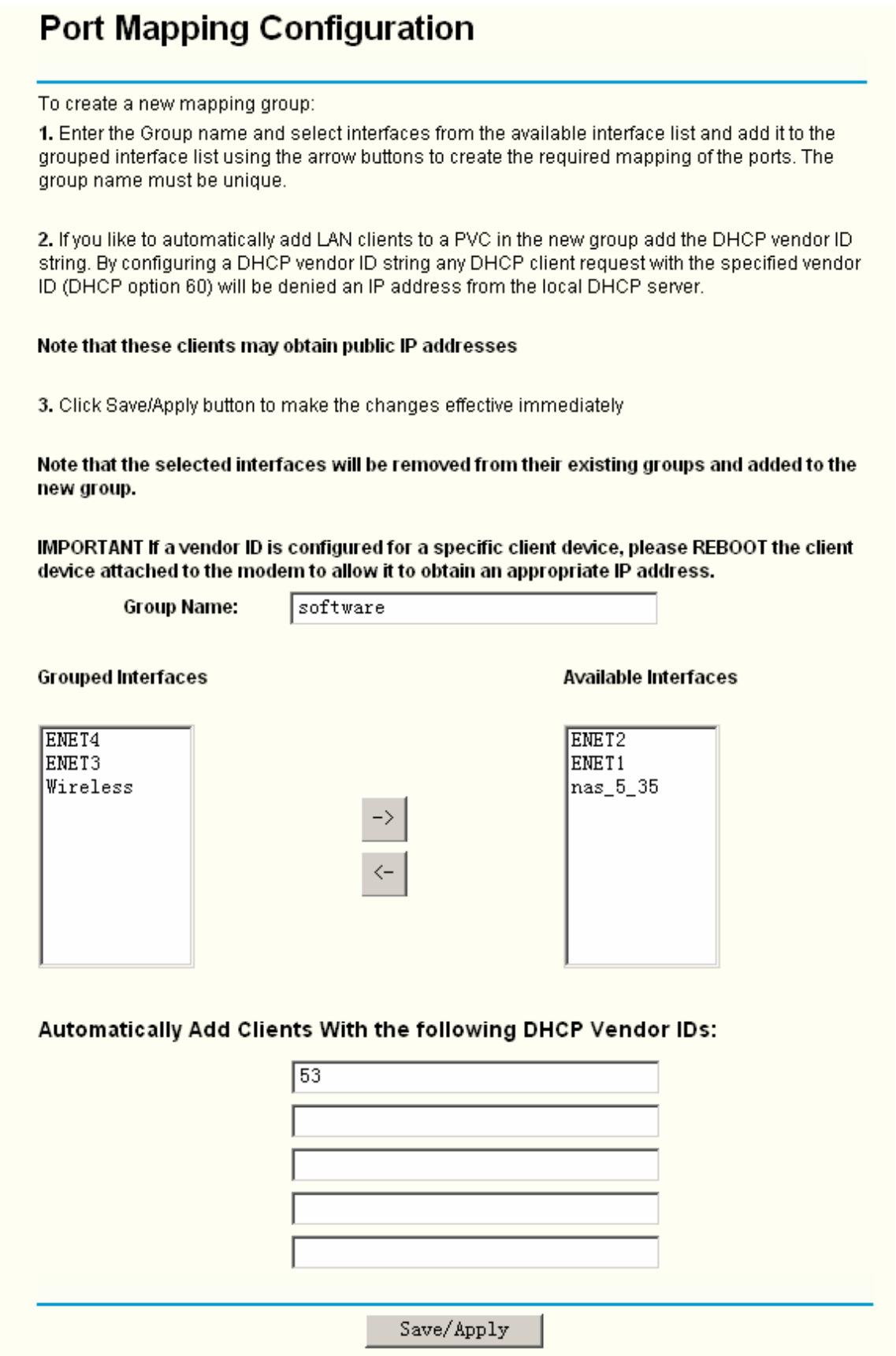
Port Mapping Configuration
To create a new mapping group:
1. Enter the Group name and select interfaces from the available interface list and add it to the grouped interface list using the arrow buttons to create the required mapping of the ports. The group name must be unique.
2. If you like to automatically add LAN clients to a PVC in the new group add the DHCP vendor ID string. By configuring a DHCP vendor ID string any DHCP client request with the specified vendor ID (DHCP option 60) will be denied an IP address from the local DHCP server.
Note that these clients may obtain public IP addresses
3. Click Save/Apply button to make the changes effective immediately
Note that the selected interfaces will be removed from their existing groups and added to the new group.
IMPORTANT If a vendor ID is configured for a specific client device, please REBOOT the client device attached to the modem to allow it to obtain an appropriate IP address.
Group Name:
software
Grouped Interfaces
Available Interfaces
ENET4
ENET3
Wireless
->
<-
ENET2
ENET1
nas_5_35
Automatically Add Clients With the following DHCP Vendor IDs:
53
Save/Apply

Figure 5-45

5.5 Wireless LAN Configuration

The menus used to configure Wireless LAN settings available in the Wireless directory including Basic, Security, MAC Filter, Advanced, and Statistics menus. The Wireless Basic, Security, MAC Filter, Advanced, and Statistics are described below.

5.5.1 Wireless – Basic

Choose "**Wireless**"→"**Basic**", you will see the screen of **Wireless-Basic** settings shown as below. The basic settings for wireless networking are set on this screen.

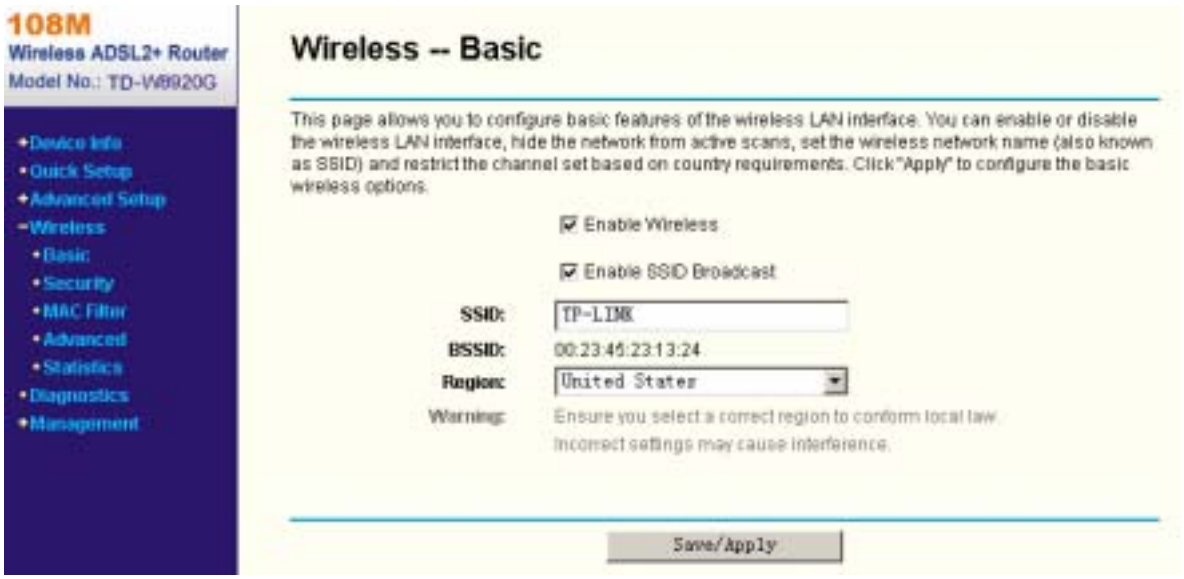

Figure 5-46

This page allows you to configure basic features of the wireless LAN interface. You can enable or disable the wireless LAN interface, hide the network from active scans, set the wireless network name (also known as SSID) and restrict the channel set based on Region requirements.

- **Enable Wireless:** If you want to use wireless features, you must select "Enable Wireless". If you deselect "Enable Wireless" option, all the Wireless settings below will be disabled.
- **Enable SSID Broadcast:** When wireless clients survey the local area for wireless networks to associate with, they will detect the SSID broadcast by the Router. To broadcast the Router's SSID, keep the default setting, if you don't want to broadcast the Router's SSID, unselect this option.
- **SSID:** Wireless network name shared among all points in a wireless network. The SSID must be identical for all devices in the wireless network. It is case-sensitive and must not exceed 32 characters (use any of the characters on the keyboard). Make sure this setting is the same for all stations in your wireless network. Type the desired SSID in the space provided.
- **BSSID:** Show the MAC address of the Router.
- **Region:** Restrict the channel set and transmit power.

Click "**Apply**" to configure the basic wireless options.

5.5.2 Wireless – Security

Choose "**Wireless**"→"**Security**", you will see the screen of **Wireless-Security** settings shown as below.

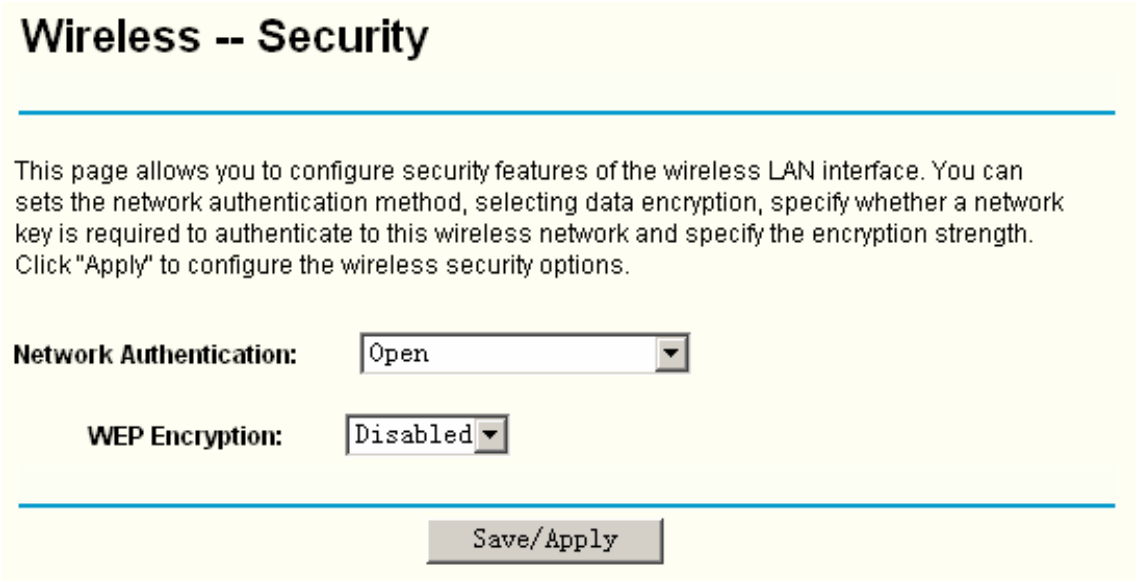

Figure 5-47

This page allows you to configure security features of the wireless LAN interface. You can set the network authentication method, selecting data encryption, specify whether a network key is required to authenticate to this wireless network and specify the encryption strength.

- **Network Authentication:** Select an authentication type from the drop-down list. Options available are: Open, Shared, WPA, WPA-PSK, WPA2, WPA2-PSK, Mixed WPA2/WPA, and Mixed WPA2/WPA-PSK.

Note:

For most users, it is recommended to use the default Wireless LAN Performance settings. Any changes made to these settings may adversely affect your wireless network. Under certain circumstances, changes may benefit performance. Carefully consider and evaluate any changes to these wireless settings.

5.5.2.1. WEP Encryption

WEP is a basic encryption method offering three levels of encryption, 152-bit is stronger than 64-bit and 128-bit encryption. If you select enable from the drop-down list of **WEP Encryption**, you will see the screen shown as below.

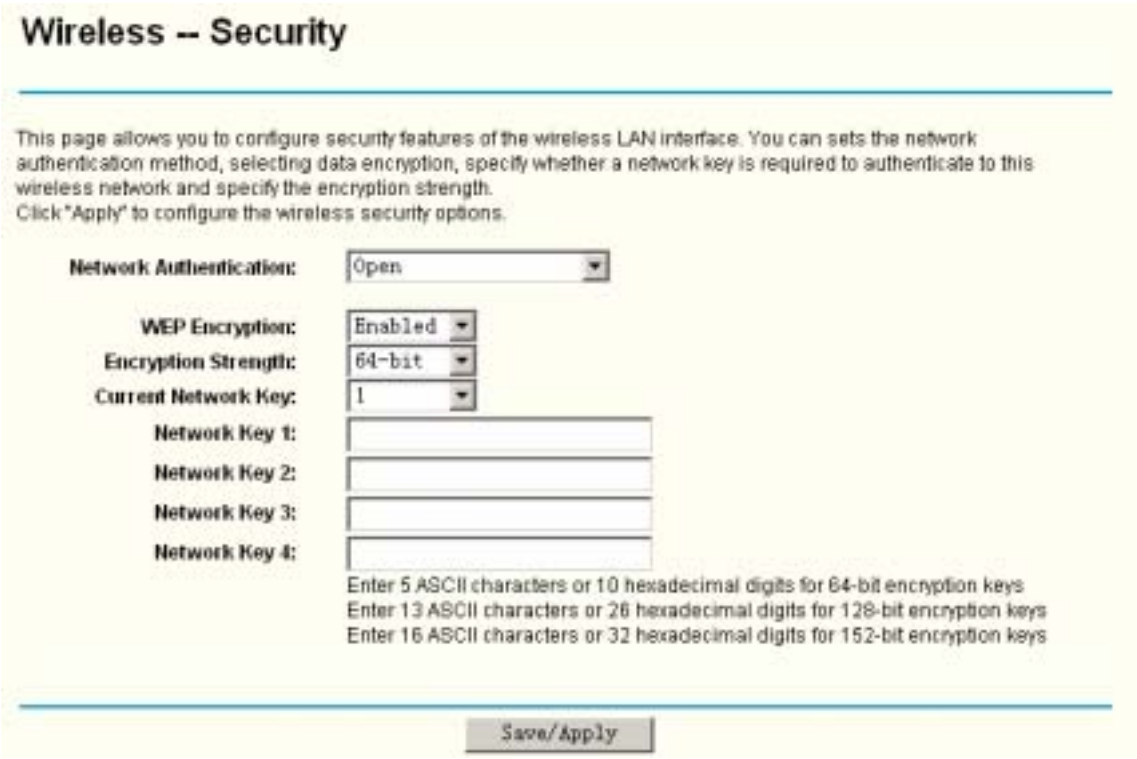

Figure 5-48

- **Encryption strength:** Select the appropriate level of encryption, 64-bit, 128-bit or 152-bit.
- **Current Network Key:** To indicate which WEP key to use, select a transmission key number.
- **Network Key 1-4:** If you want to manually enter the WEP keys, then enter them in the network Key 1-4 fields.

Configure WEP Encryption

WEP can use different methods of Authentication. Choose the Authentication Type from drop-down list Open or Shared.

- Select **Open** to allow any wireless station to associate with the access point.
- Select **Shared** to only allow stations using a shared key encryption to associate with it. Shared key requires additional configuration of the keys to be used. Follow the instructions below to configure the Shared Keys.

WEP Encryption is disabled by default. To enable WEP, select the Enable option. Configure the Encryption Keys as below:

1. Encryption strength: Select 64-bit (enter 5 ASCII characters or 10 hexadecimal digits in the Network Key list), 128-bit (enter 13 ASCII characters or 26 hexadecimal digits in the Network Key list), or 152-bit (enter 16 ASCII characters or 32 hexadecimal digits in the Network Key list).
2. Current Network Key: Select 1.
3. In Network key 1 list, enter 5 ASCII characters or 10 hexadecimal digits for 64-bit encryption keys, enter 13 ASCII characters or 26 hexadecimal digits for 128-bit encryption keys, enter 16 ASCII characters or 32 hexadecimal digits for 152-bit encryption keys.
4. Click the **Save/Apply** button to save the new configuration.

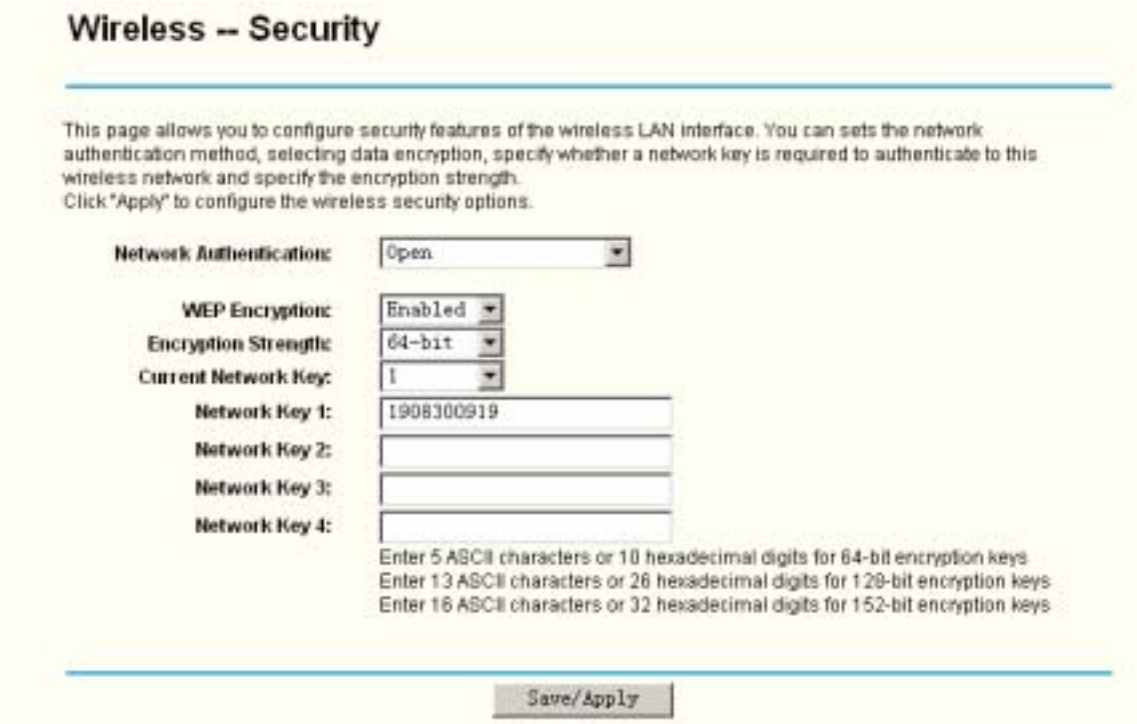

Figure 5-49

Note:

We use **Encryption Strength** 64-bit, **Current Network Key** selected "1" and enter 10 hexadecimal digits"1908300919" in the **Network Key 1** for example, Configure the settings as Figure 5-49 shown above.

5.5.2.2. WPA

WPA security for wireless communication has been developed to overcome some of the shortcomings of WEP. WPA combines the key generation with the authentication services of a RADIUS server.

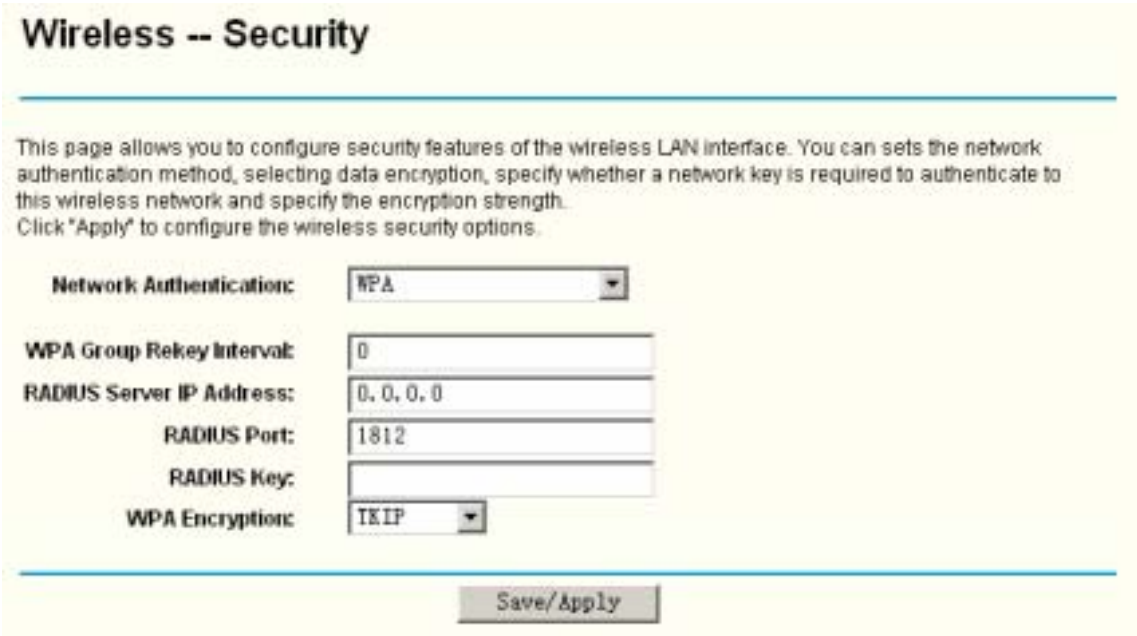

Figure 5-50

- **WPA Group ReKey Interval:** Enter the Key Renewal period, which tells the Router how often it should change encryption keys.
- **RADIUS Server IP Address:** The IP address of the RADIUS server.
- **RADIUS Port:** The port of the RADIUS server. The default number is 1812.
- **RADIUS key:** The password of the RADIUS Server.
- **WPA Encryption:** Select the encryption you want to use: Automatic, TKIP or AES (AES is an encryption method stronger than TKIP).

Configure WPA settings

1. Select the WPA option from the Network Authentication drop-down list. The menu will change to offer the appropriate settings.
2. Change the WPA Group Rekey Interval as desired.
3. Type in the IP address of the RADIUS server used in the RADIUS Server IP Address field.
4. Change the RADIUS Port if necessary.
5. Type in the password in the RADIUS Key field.
6. Use the default setting TKIP of WPA Encryption.
7. Click the **Save/Apply** button to save the new configuration.

Figure 5-51

5.5.2.3. WPA-PSK

WPA-PSK requires a shared key and does not use a separate server for authentication. PSK keys can be ASCII or Hex type.

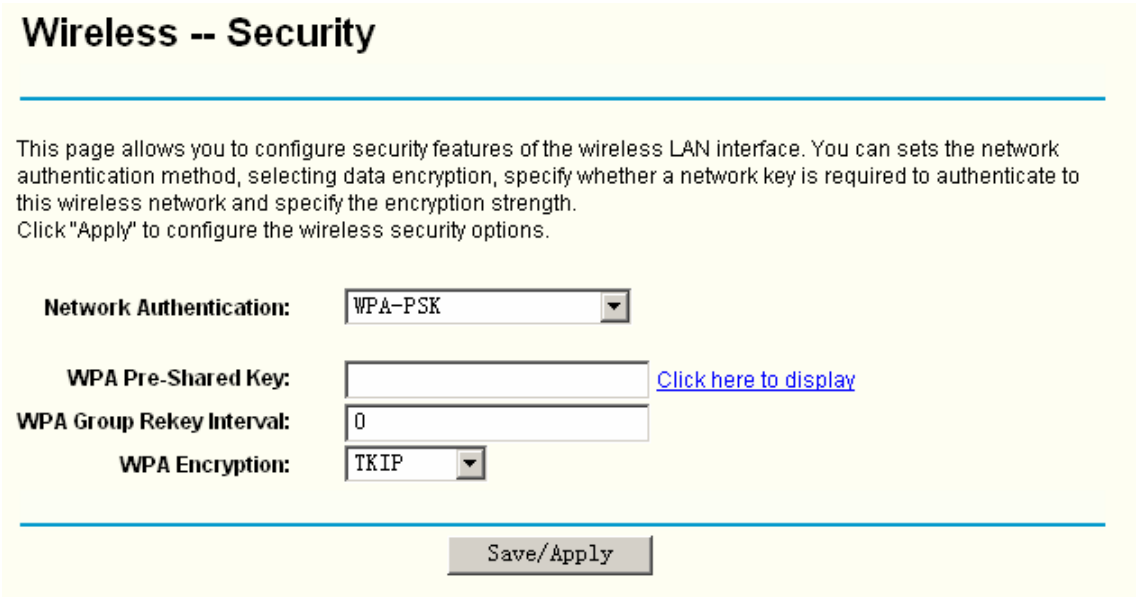

Figure 5-52

- **WPA Pre-Shared Key:** Enter the key shared by the Router and your other network devices. It must have 8-63 ASCII characters or 64 Hexadecimal digits.
- **Click here to display:** Click it to show you the WPA Pre-Shared Key.

Configure WPA-PSK settings

1. Select the WPA-PSK option. The menu will change to offer the appropriate settings as the picture show above.
2. WPA-PSK requires a shared key. Type the key in the space provided. PSK keys can be ASCII or Hex type.
3. Change the Group Key Interval as desired or use the default setting.
4. Click the **Save/Apply** button to save the new configuration.

Figure 5-53

Note:

If you click the option "Click here to display", the Figure 5-54 will pop-up, and it shows the password you have set.

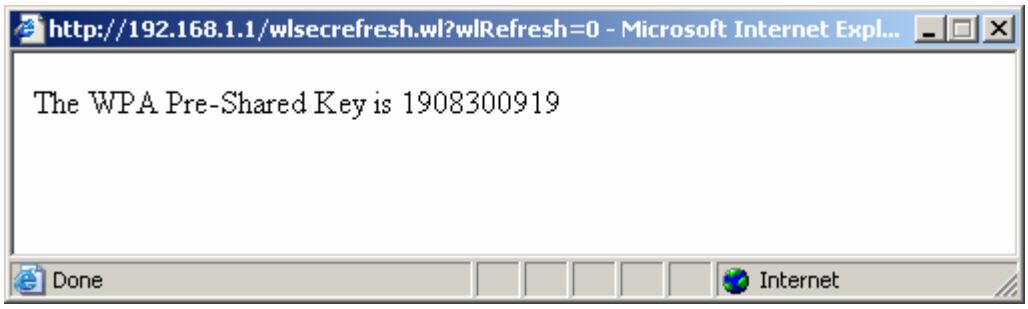

Figure 5-54

5.5.2.4. WPA2

To configure WPA2 settings, select the WPA2 option from the drop-down list. The menu will change to offer the appropriate settings. The steps of these settings are similar to WPA settings.

Figure 5-55

5.5.2.5. WPA2-PSK

To configure WPA2-PSK settings, select the WPA2-PSK option from the drop-down list. The menu will change to offer the appropriate settings. WPA2-PSK requires a shared key and does not use a separate server for authentication. PSK keys can be ASCII or Hex type.

Figure 5-56

5.5.2.6. Mixed WPA2/WPA

To configure Mixed WPA2/WPA settings, select the Mixed WPA2/WPA option from the drop-down list. The menu will change to offer the appropriate settings. The steps to these settings are similar to those for WPA-PSK.

Figure 5-57

5.5.2.7. Mixed WPA2/WPA-PSK

To configure Mixed WPA2/WPA-PSK settings, select the Mixed WPA2/WPA-PSK option from the drop-down list. The menu will change to offer the appropriate settings. The steps of this setting are the same with WPA-PSK.

Figure 5-58

5.5.3 Wireless -- MAC Filter

Choose "**Wireless**"→"**MAC Filter**", you will see the screen of **Wireless-MAC Filter** settings shown as below.

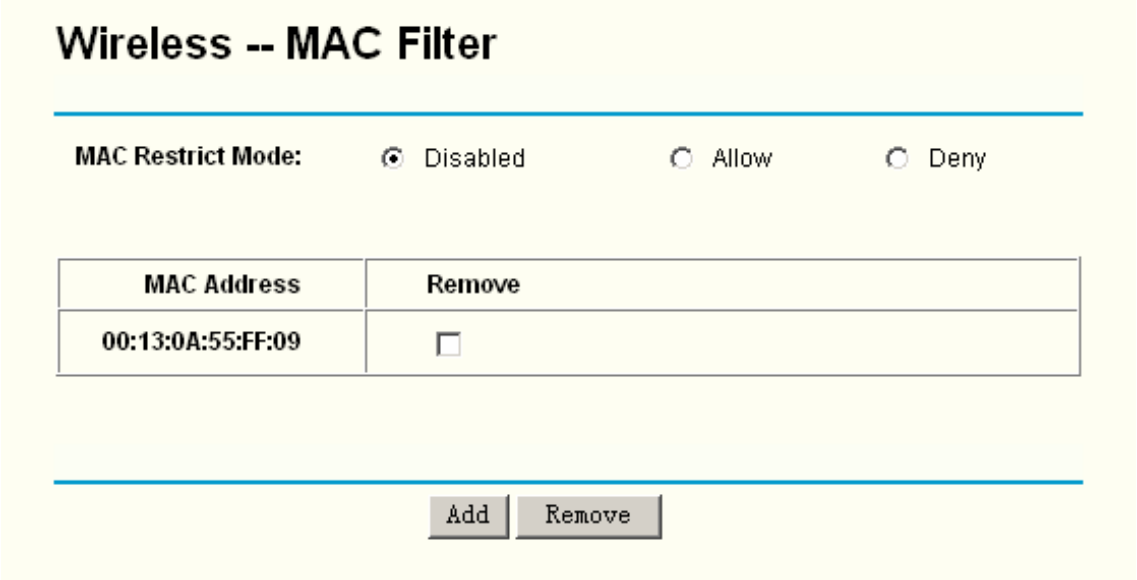

Figure 5-59

Wireless access can be filtered by using the MAC addresses of the wireless devices transmitting within your network's RADIUS. To filter wireless users by MAC Address, either permitting or blocking access. If you do not wish to filter users by MAC Address, select Disabled.

- **Allow:** Click this button to allow wireless access by the devices listed on this screen.
- **Deny:** Click this button to block wireless access from the devices listed on this screen.
- **Add:** Click this button to add the MAC Address.
- **Remove:** Click this button to remove the item of the MAC Address.

When you click the **Add** button, the pop-up picture shown below, and then you can type the MAC Address in the **MAC Address** field.

Note:

The form of MAC Address must be "**xx:xx:xx:xx:xx:xx**", like "**00:13:0A:55:FF:09**".

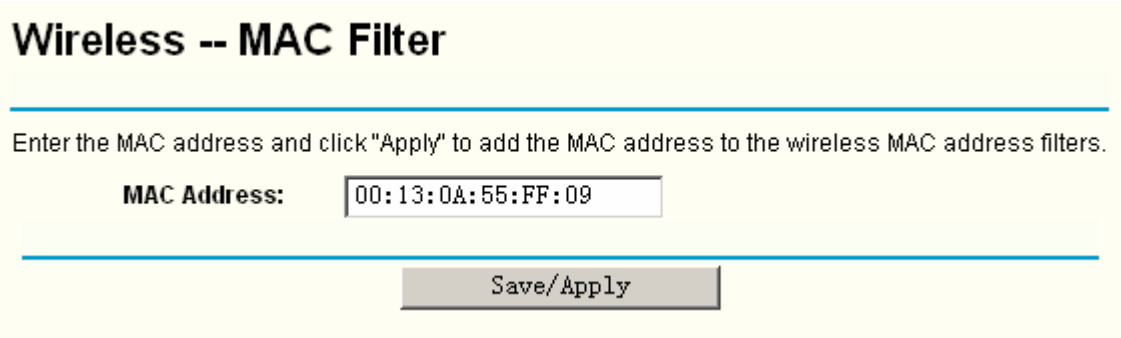

Figure 5-60

When you finished making changes to the MAC Filter List screen, click the **Save/Apply** button to save the changes.

5.5.4 Wireless – Advanced

Choose "**Wireless**"→"**Advanced**", you will see the screen of **Wireless-Advanced** settings shown as below.

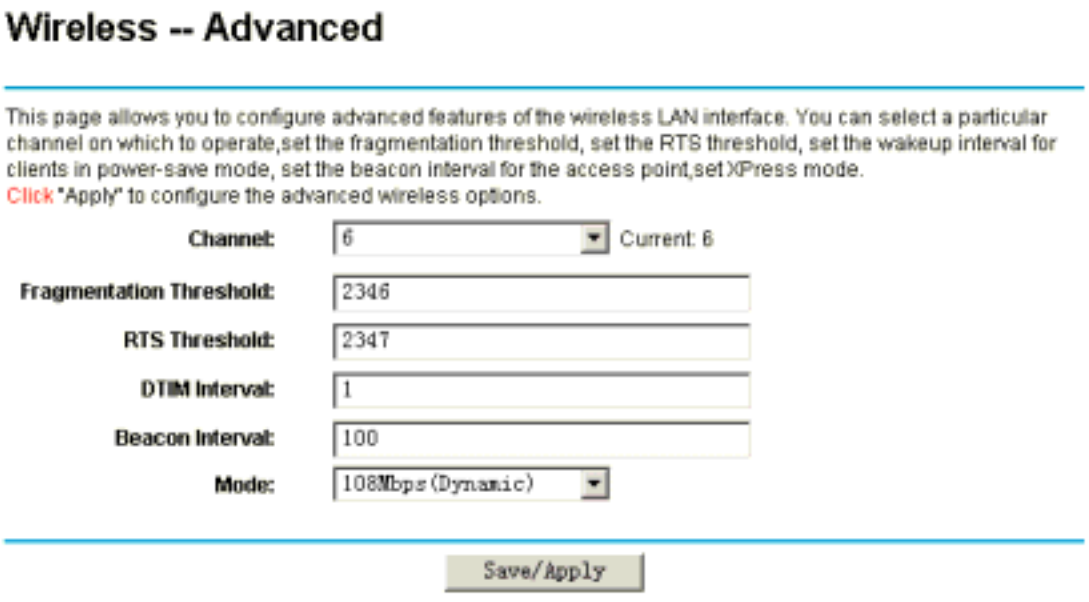

Figure 5-61

- **Channel:** Select the channel you want to use from the drop-down List of Channel. This field determines which operating frequency will be used. It is not necessary to change the wireless channel unless you notice interference problems with another nearby access point.
- **Fragmentation Threshold:** This value specifies the maximum size for a packet before data is fragmented into multiple packets. If you experience a high packet error rate, you may slightly increase the Fragmentation Threshold. Setting the Fragmentation Threshold too low may result in poor network performance. Only minor reduction of the default value is recommended. In most cases, it should remain at its default value of 2346.
- **RTS Threshold:** Should you encounter inconsistent data flow, only minor reduction of the

default value 2347 is recommended. If a network packet is smaller than the preset RTS threshold size, the RTS/CTS mechanism will not be enabled. The Router sends Request to Send (RTS) frames to a particular receiving station and negotiates the sending of a data frame. After receiving an RTS, the wireless station responds with a Clear to Send (CTS) frame to acknowledge the right to begin transmission. In most cases, keep its default value of 2347.

- **DTIM Interval:** This value, between 1 and 255, indicates the interval of the Delivery Traffic Indication Message (DTIM). A DTIM field is a countdown field informing clients of the next window for listening to broadcast and multicast messages. When the Router has buffered broadcast or multicast messages for associated clients, it sends the next DTIM with a DTIM Interval value. Its clients hear the beacons and awaken to receive the broadcast and multicast messages. The default value is **1**.
- **Beacon Interval:** Enter a value between 20-1000 milliseconds. The Beacon Interval value indicates the frequency interval of the beacon. A beacon is a packet broadcast by the Router to synchronize the wireless network. The default value is 100.
- **Mode:** In the drop-down list you can select “11Mbps (802.11b)”, “54Mbps (802.11g)”, and “108Mbps (Dynamic)”. "54Mbps (802.11g)", which allows both 802.11g and 802.11b wireless stations to connect to the Router, “108Mbps (Dynamic)” allows Super G™, 802.11g and 802.11b wireless stations connect to the router.

5.5.5 Wireless – Statistics

Choose “**Wireless**”→”**Statistics**”, you will see the screen of **Wireless-Statistics** setting shown as below.

Figure 5-62

This page shows authenticated wireless stations and their status.

- **BSSID:** Displays the connected wireless station's MAC address.
- **Associated:** Displays whether the wireless station has associated with the access point.
- **Authorized:** Displays the information of Authentication.

5.6 Diagnostics

Choose “**Diagnostics**”, you will see the Diagnostics screen. This section describes the result of the test for the ENET (Ethernet) Connection, Wireless Connection and ADSL Synchronization. You can refer to the **Help** menu to get more information about the corresponding test.

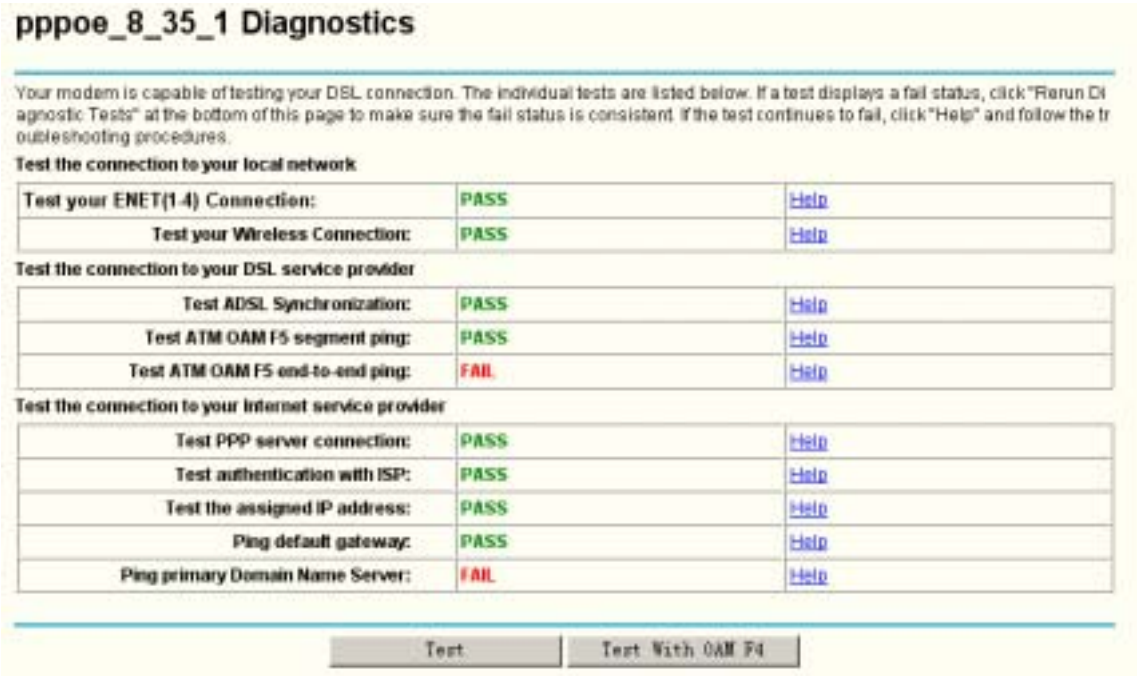

Figure 5-63

5.7 Management

Choose “**Management**”, there are six submenus under the main menu. They are **Settings**, **System Log**, **TR-069 client**, **Internet Time**, **Access Control**, **Update Software** and **Reboot**. Click any of them, and you will be able to configure the corresponding function.

5.7.1 Settings

This section provides three important functions for managing the Router; they are **Backup**, **Update** and **Restore Default** (shown in Figure 5-64). The detailed manipulations are described below.

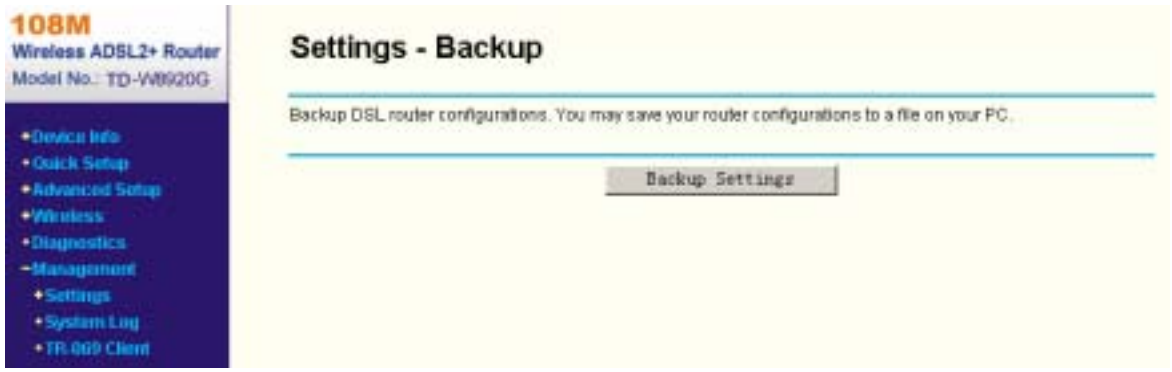

Figure 5-64

5.7.1.1. Backup

Choose "**Management**"→"**Settings**"→"**Backup**", you can see the **Backup** screen, this screen (shown in Figure 5-65) allows you to save the current configuration of the Router as a backup file.

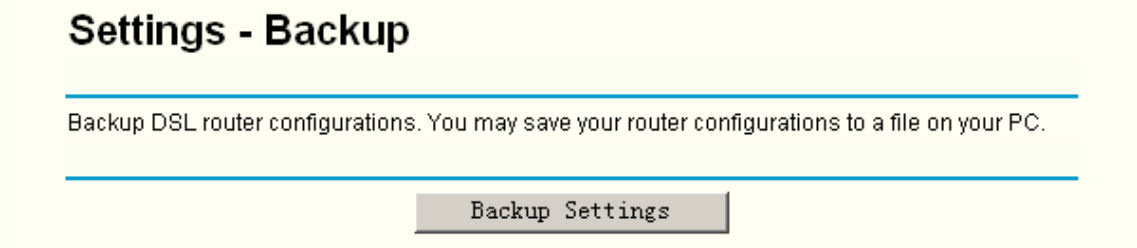

Figure 5-65

To back up the Router's current settings:

1. Click the **Backup Settings** button on the screen above (pop-up Figure 5-65), the following screen will then appear (shown in Figure 5-66).

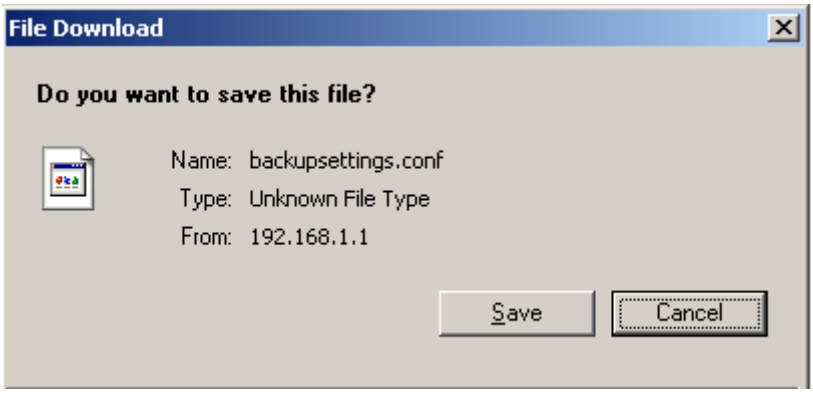

Figure 5-66

2. Click the **Save** button, and save the file as the appointed file (shown in Figure 5-67).

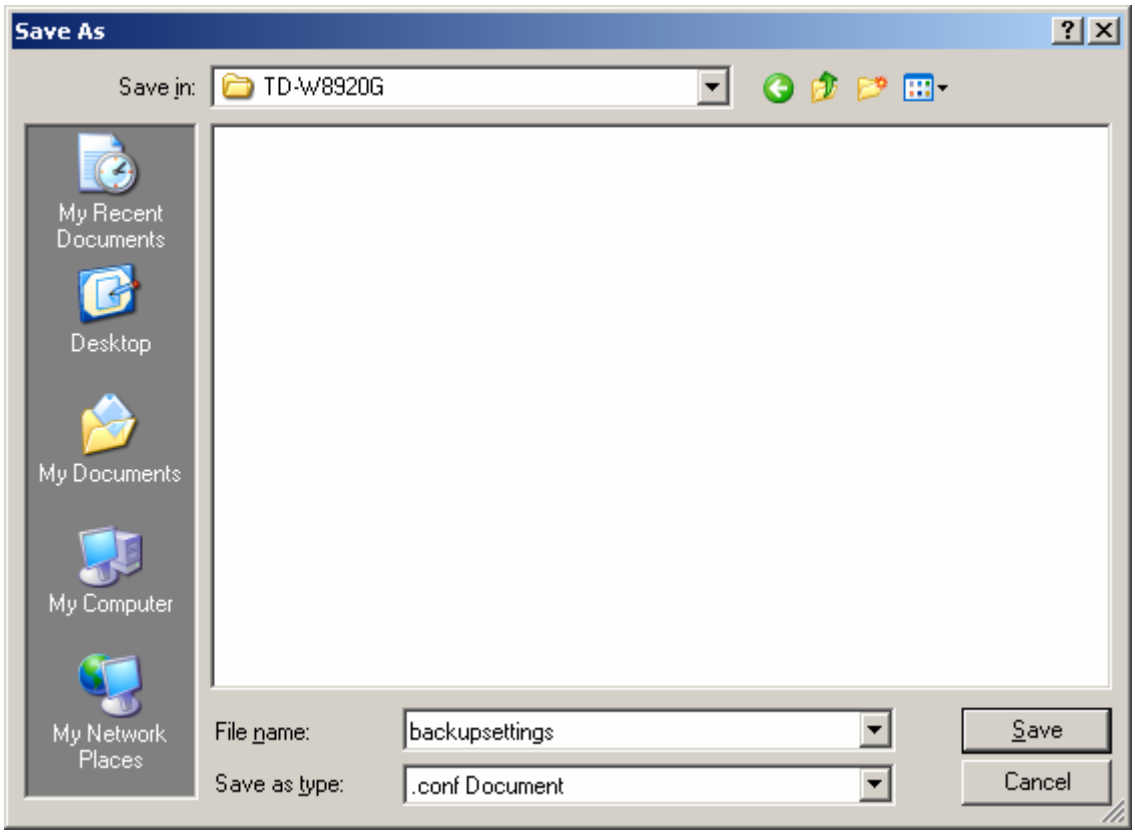

Figure 5-67

5.7.1.2. Update

Choose "**Management**"→"**Settings**"→"**Update**", you can see the **Update** screen, this screen (shown in Figure 5-68) allows you to update the Router's settings.

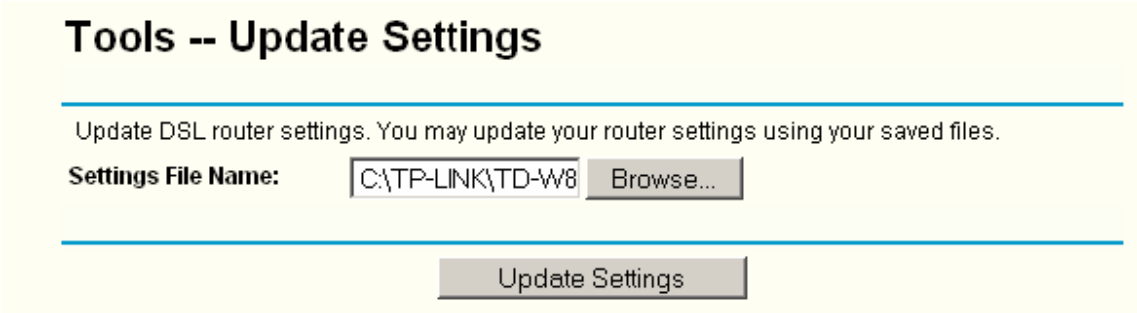

Figure 5-68

To update the Router's settings:

1. Click the **Browse** button to locate the update file for the device, and you can also enter the exact path to the Setting file in the text box.
2. After you have selected the file for updating the settings, click the **Update Settings** button.

Note:

The Router will reboot upon completion. This process will take a while, don't turn off the Router or press the **Reset** button while processing.

5.7.1.3. Restore Default

Choose "**Management**"→"**Settings**"→"**Restore Default**", you can see the **Restore Default** screen, this screen (shown in Figure 5-69) allows you to restore the Router's configuration to the factory defaults on the screen.

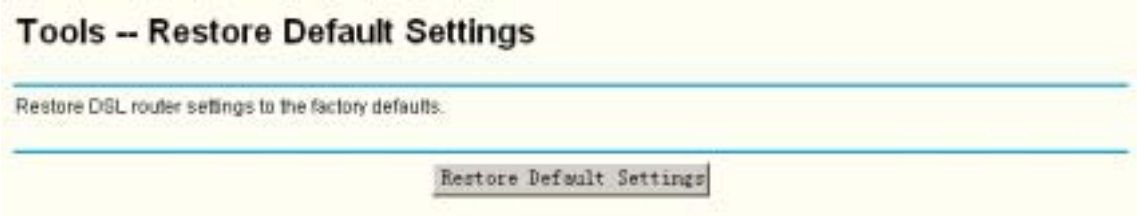

Figure 5-69

- **Restore Default Settings:** Click this button to restore the Router's configuration to the factory defaults, and then follow the on-screen instructions to complete it.
- **Account and Password:** The default **account name** and its **password** are both admin.
- The default **IP Address:** 192.168.1.1.
- The default **Subnet Mask:** 255.255.255.0.

5.7.2 System Log

Choose "**Management**"→"**System Log**", you can see the **System Log** screen, this screen (shown in Figure 5-70) allows you to view the system log and configure the system log options.

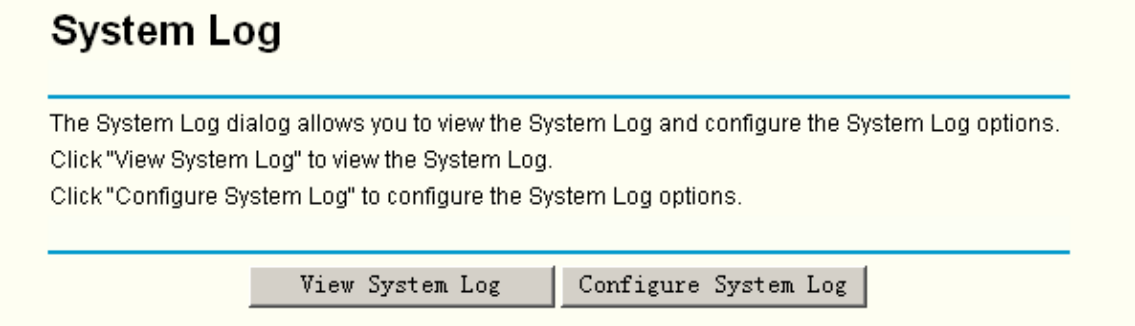

Figure 5-70

To View the System Log:

Click the **View System Log** button, you will see the screen (shown in Figure 5-71) which displays the Router's recent logs.

Figure 5-71

- **Refresh:** Click the button, the information in the table will be updated.
- **Close:** Click the button, the screen will be closed.

To Configure the System Log Settings:

Click the **Configure System Log** button (shown in Figure 5-70), you will see the screen below (shown in Figure 5-72).

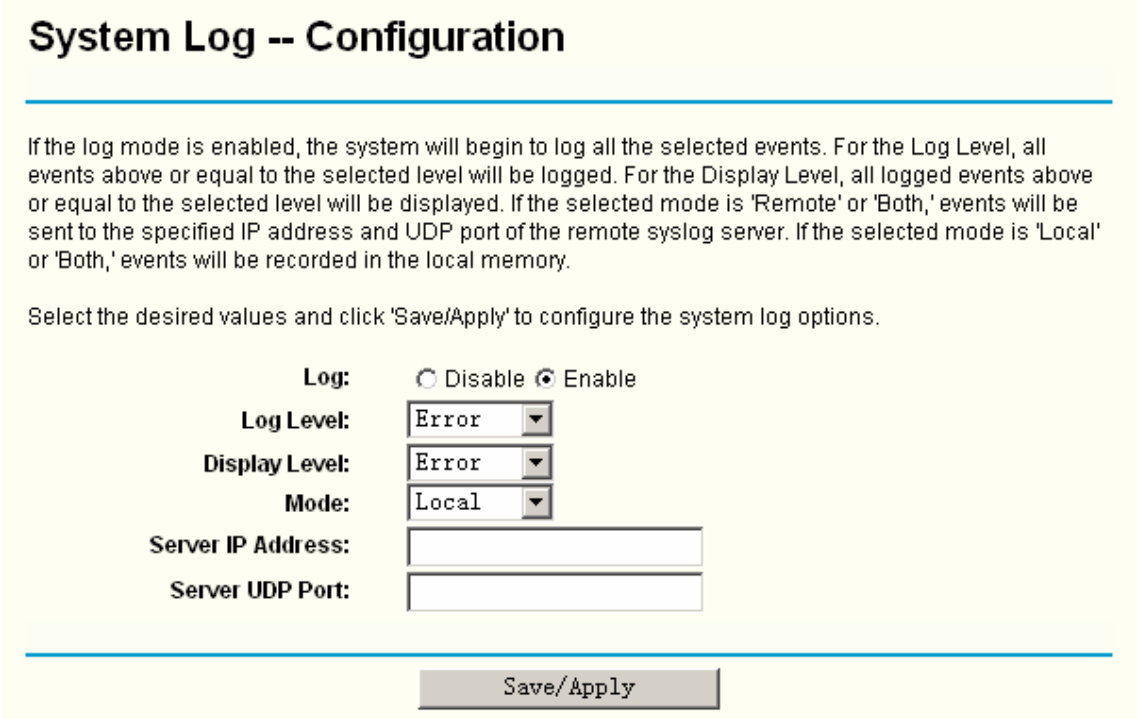

Figure 5-72

- **Disable/Enable:** Select the **Enable** to log the events, if you don't want to log these events, please select **Disable**.
- **Log Level:** Select the Log level in the drop-down list, for the Log level, all events above or equal to the selected level will be logged.
- **Display Level:** Select the Display level in the drop-down list, for the Display Level, all logged events above or equal to the selected level will be displayed.
- **Mode:** Select the mode to record the events. If the selected mode is **Local,** events will be

recorded in the local memory. If the selected mode is **Remote**, events will be sent to the specified IP address and UDP port of the remote system log server. If the selected mode is **Both**, events will be sent to the local memory and the remote system log server.

- **Server IP Address:** Type the address of the server you want to record the events.
- **Server UDP Port:** Type the UDP Port of the server.

5.7.3 TR-069 client

Choose "**Management**"→"**TR-069 client**", you can see the TR-069 client - Configuration screen, this screen (shown in Figure 5-73).

TR-069（WAN Management Protocol）allows a Auto-Configuration Server (ACS) to perform auto-configuration, provision, collection, and diagnostics to this device.

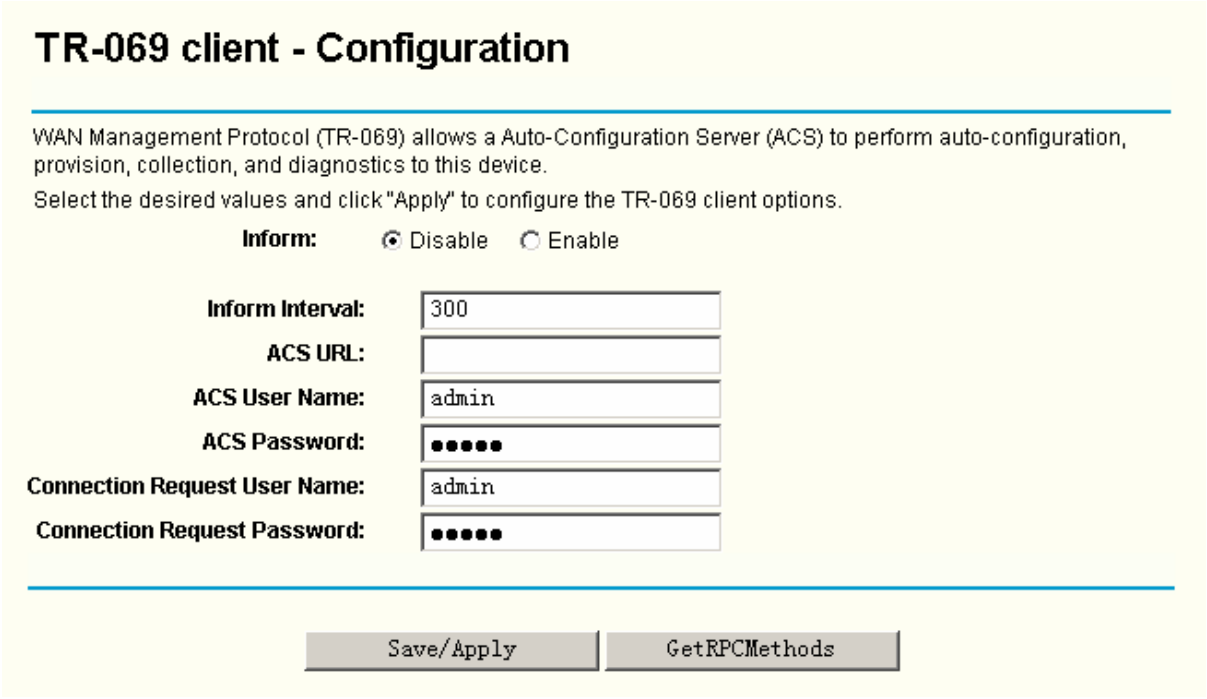

Figure 5-73

- **Inform:** You can select the checkbox to disable or enable the **Inform Interval.**
- **Inform Interval:** Type the interval time of your Router contact with the **ACS**.
- **ACS URL:** Please accept this information from your ISP. And through **ACS** (Auto-Configuration Server) you can perform auto-configuration, provision, collection, and diagnostics to this router.
- **ACS User Name:** Please accept this User Name information from your ISP.
- **ACS Password:** Please accept the Password information from your ISP.

Note:

If you want to log on the **ACS**, you must owned the **ACS User Name** and **ACS Password**.

- **Connection Request User Name:** Type the Connection Request User Name, set it yourself.
- **Connection Request Password:** Type the Connection Request Password, set it yourself.

Note:

The Connection Request User Name and Connection Request Password used for **ACS** log on the Router and manage it.

- **GetRPCMethods:** Click this button to contact with **ACS**.

Note:

RPC- Remote **P**rocedure **C**alls

Select the desired values and click "Save/Apply" to configure the TR-069 client options.

5.7.4 Internet Time

Choose "**Management**"→"**Internet Time**", you can see the Time settings screen, this screen (shown in Figure 5-74) allows you to set the time for the Router.

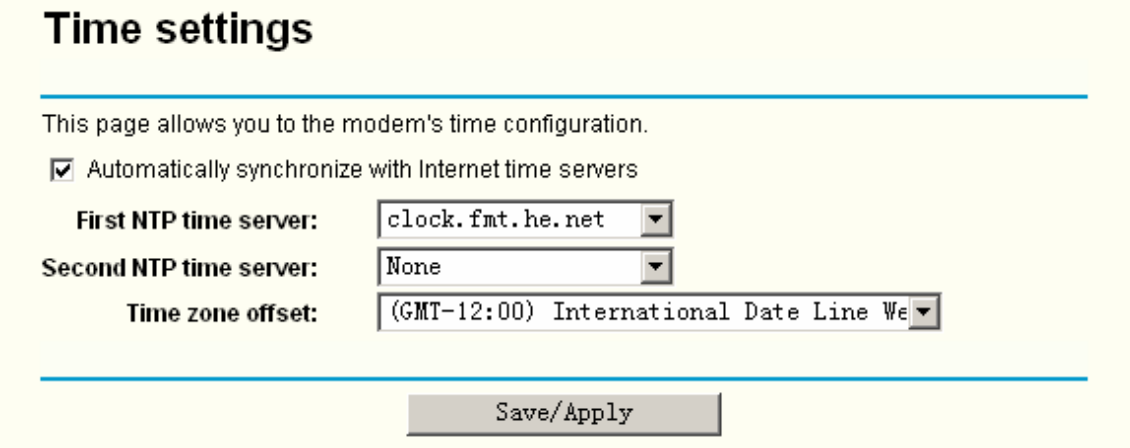

Figure 5-74

To set the Router's time:

1. Select automatically synchronize with Internet time servers.
2. Select the First NTP time server and/or the Second NTP time server in the drop-down list severally.
3. Select your local time zone.
4. Click **Save/Apply** button.

Note:

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, if not, the time limited on these functions will not take effect.

The time will be lost if the Router is turned off.

The Router will obtain the time automatically from Internet if it has already connected to Internet.

5.7.5 Access Control

This section provides three submenus including **Services**, **Addresses** and **Password** (shown in Figure 5-75), the detailed descriptions are provided below.

Figure 5-75

5.7.5.1. Services

Choose "**Management**"→"**Access Control**"→"**Services**", you can see the **Services** screen, this screen (shown in Figure 5-76) allows you to select the services for LAN Ports and WAN Port. After you have completed, click the **Save/Apply** button to make sure your selection.

Figure 5-76

Note:

WAN are not available for the connection type of **Bridge** here, they won't display on the screen above since only Bridge is selected.

5.7.5.2. IP Addresses

Choose "**Management**"→"**Access Control**"→"**IP Addresses**", you can see the **IP Address** screen, this screen (shown in Figure 5-77) allows you to configure the IP Address for managing the Router.

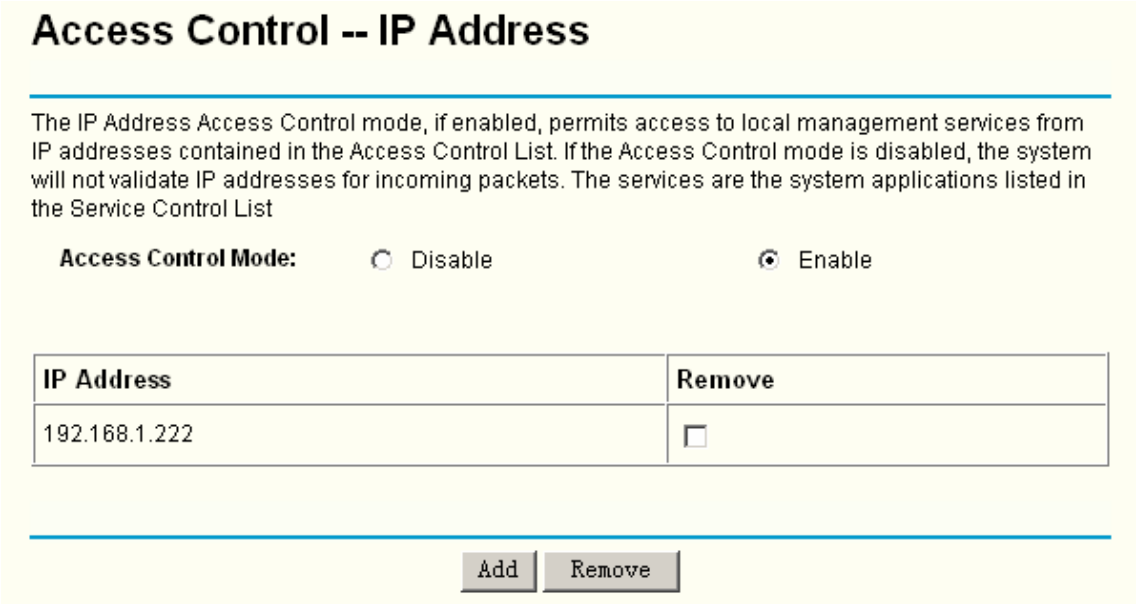

Figure 5-77

To add the IP Address:

1. Click the **Add** button. You can add a new IP Address in the next screen (shown in Figure 5-78).

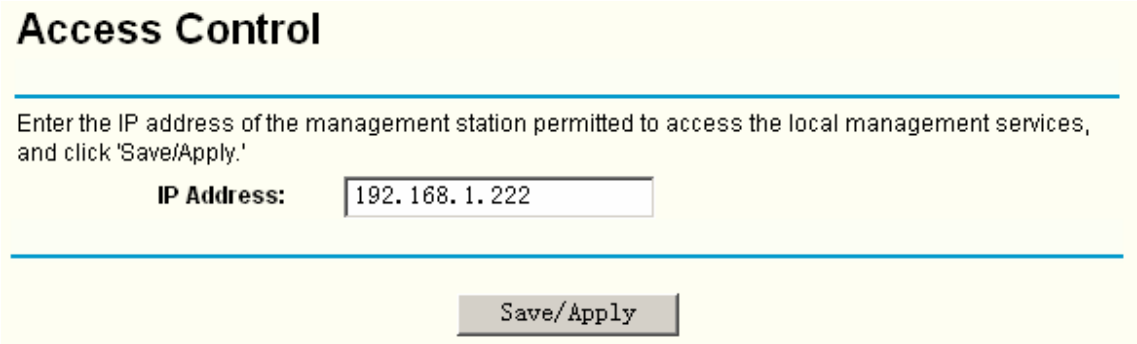

Figure 5-78

2. Enter the IP address of the management station permitted to access the local management services.
3. Click the **Save/Apply** button to save the IP Address.
4. Enable the **Access Control Mode** (shown in Figure 5-77).

Note:

If **Enabled**, the Router will permit access to local management services from IP addresses contained in the Access Control List. If the Access Control mode is **Disabled**, the function will not validate, and all IP addresses can access to local management services. The services are the system applications listed in the Service Control List.

5.7.5.3. Passwords

Choose "**Management**"→"**Access Control**"→"**Password**", you can see the screen (shown in Figure 5-79) which allows you to change the factory default password of the Router.

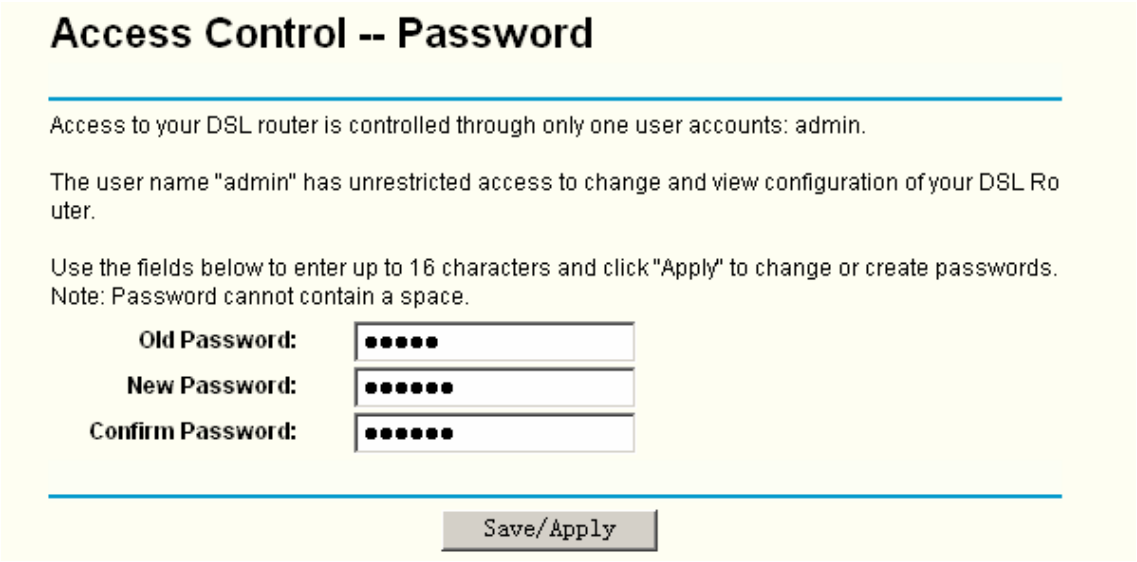

Figure 5-79

To change the password:

1. Enter the **Old Password** in the text box.
2. Enter the **New Password** and **Confirm Password**. The Confirm Password should be the same as the New Password.
3. Click the **Save/Apply** button to make your change take effect.

Note:

The password cannot contain a space, and its maximum length is 16 characters.

5.7.6 Update Software

Choose "**Management**"→"**Update Software**", you can see the screen (shown in Figure 5-80) which allows you to upgrade the latest version software to keep the Router up to date.

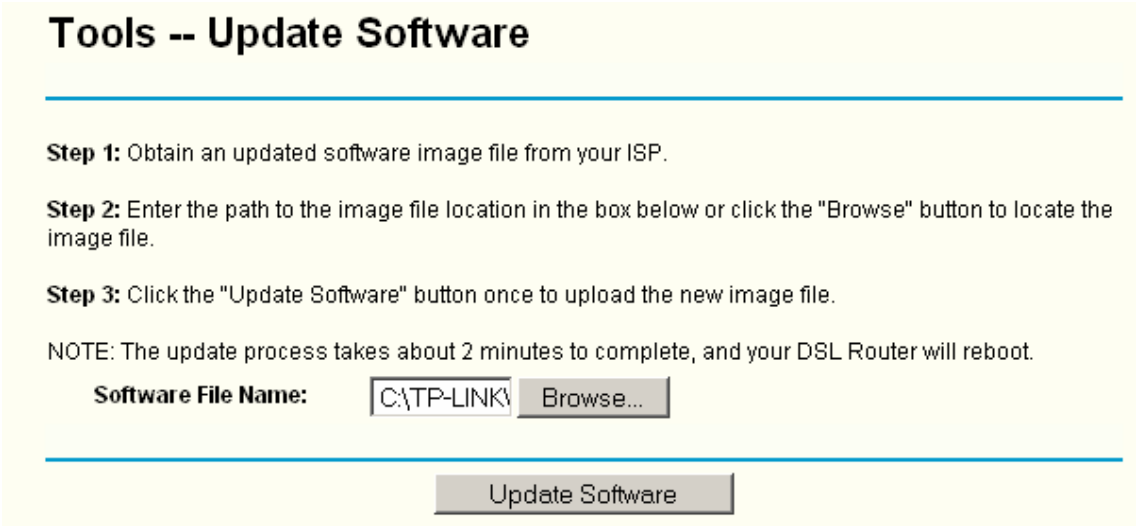

Figure 5-80

- **Browse:** Click the button to locate the latest software for the device.
- **Update Software:** After you have selected the latest software, click the button.

To update the Router's software:

1. Download the latest software upgrade file from the TP-LINK website (www.tp-link.com).
2. Click **Browse** to view the folders and select the image file or enter the exact path to the image file location in the text box.
3. Click the **Update Software** button.

Note:

Do not turn off the Router or press the **Reset** button while the software is being updated.
The Router will reboot after the Upgrading is finished.

5.7.7 Reboot

Choose "**Management**"→"**Reboot**", you can see the screen (shown in Figure 5-81) which allows you to reboot the Router.

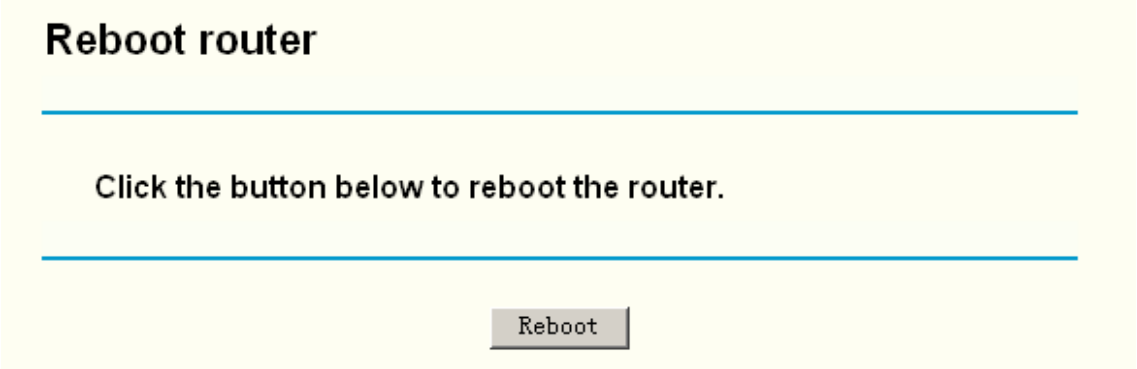

Figure 5-81

Note:

After you clicked the **Reboot** button, please wait for a while before reopening your web browser.
Do not turn off the Router or press the **Reset** button while the Router is rebooting.
If necessary, reconfigure your PC's IP address to match your new configuration.

Chapter 6. Appendix

Appendix A: Glossary

108M Super G™ WLAN Transmission Technology - 108M Super G™ WLAN Transmission Technology employs multiple performance-enhancing techniques including packet bursting, fast frames, data compression, and dynamic turbo mode that combine to improve the throughput and range of wireless networking products. Users can experience link rates of up to 108Mbps, twice the industry-standard maximum data link rate of 54Mbps, while preserving full compatibility with traditional 802.11g or 802.11b networks. 108M Super G™ products offer the highest throughput performance available on the market today. In dynamic 108M mode, the device can attach 802.11b, 802.11g and 108Mbps Super G™ devices at the same time in an integrated environment.

2x to 3x eXtended Range™ WLAN Transmission Technology - The WLAN device with 2x to 3x eXtended Range™ WLAN transmission technology make its sensitivity up to 105 dB, which gives users the ability to have robust, longer-range wireless connections. With this range-enhancing technology, a 2x to 3x eXtended Range™ based client and access point can maintain a connection at as much as three times the transmission distance of traditional 802.11b and 802.11g products, for a coverage area that is up to nine times greater. A traditional 802.11b and 802.11g product transmission distance is about 300m, a 2x to 3x eXtended Range™ based client and access point can maintain a connection transmission distance may be up to 830m.

Access Point - A device that allows wireless-equipped computers and other devices to communicate with a wired network. Also used to expand the range of a wireless network.

Ad-hoc Network - An ad-hoc network is a group of computers, each with a wireless adapter, connected as an independent IEEE 802.11 wireless LAN. Ad-hoc wireless computers operate on a peer-to-peer basis, communicating directly with each other without the use of an access point. Ad-hoc mode is also referred to as an Independent Basic Service Set (IBSS) or as peer-to-peer mode, and is useful at a departmental scale or SOHO operation.

AES (Advanced **E**ncryption **S**tandard**) -** A security method that uses symmetric 128-bit block data encryption.

ACS (Auto-**C**onfiguration **S**erver**) -** Through **ACS** (Auto-Configuration Server) you can perform auto-configuration, provision, collection, and diagnostics to the device.

ATM (Asynchronous **T**ransfer **M**ode**) -** ATM is a cell based transfer mode that requires variable length user information to be segmented and reassembled to/from short, fixed length cells. It uses two different methods for carrying connectionless network interconnect traffic, routed and bridged Protocol Data Units (PDUs), over an ATM network.

Bridging - A device that connects different networks.

Browser - An application program that provides a way to look at and interact with all the information on the World Wide Web.

DDNS (**D**ynamic **D**omain **N**ame **S**ystem) **-** Allows the hosting of a website, FTP server, or e-mail

server with a fixed domain name (e.g., www.xyz.com) and a dynamic IP address.

Default Gateway - A device that forwards Internet traffic from your local area network.

DHCP - A networking protocol that allows administrators to assign temporary IP addresses to network computers by “leasing” an IP address to a user for a limited amount of time, instead of assigning permanent IP addresses.

DMZ (**D**e**m**ilitarized **Z**one) **-** Removes the Router's firewall protection from one PC, allowing it to be “seen” from the Internet.

DNS (**D**omain **N**ame **S**erver) **-** The IP address of your ISP's server, which translates the names of websites into IP addresses.

Domain - A specific name for a network of computers.

DSL (**D**igital **S**ubscriber **L**ine) **-** An always-on broadband connection over traditional phone lines.

Dynamic IP Address - A temporary IP address assigned by a DHCP server.

EAP (Extensible **A**uthentication **P**rotocol**) -** A general authentication protocol used to control network access. Many specific authentication methods work within this framework.

Encryption - Encoding data transmitted in a network.

Ethernet - IEEE standard network protocol that specifies how data is placed on and retrieved from a common transmission medium.

Firewall - A set of related programs located at a network gateway server that protects the resources of a network from users from other networks.

Gateway - A device that interconnects networks with different, incompatible communications protocols.

IEEE 802.11b - The IEEE 802.11b standard specifies a wireless networking at 11 Mbps using direct-sequence spread-spectrum (DSSS) technology and operating in the unlicensed radio spectrum at 2.4GHz, and WEP encryption for security. IEEE 802.11b networks are also referred to as Wi-Fi networks.

IEEE 802.11g - Specification for wireless networking at 54 Mbps using direct-sequence spread-spectrum (DSSS) technology, using OFDM modulation and operating in the unlicensed radio spectrum at 2.4GHz, and backward compatibility with IEEE 8021b devices, and WEP encryption for security.

Infrastructure Network - An infrastructure network is a group of computers or other devices, each with a wireless adapter, connected as an IEEE 802.11 wireless LAN. In infrastructure mode, the wireless devices communicate with each other and to a wired network by first going through an access point. An infrastructure wireless network connected to a wired network is referred to as a Basic Service Set (BSS). A set of two or more BSS in a single network is referred to as an Extended Service Set (ESS). Infrastructure mode is useful at a corporation scale, or when it is necessary to connect the wired and wireless networks.

IP Address - The address used to identify a computer or device on a network.

IPoA (IP and **ARP** over **ATM) -** A protocol that provides extensions to the IP Group for handling IP over ATM flows.

ISP (**I**nternet **S**ervice **P**rovider) **-** A company that provides access to the Internet.

LAN - The computers and networking products that make up your local network.

MAC (**M**edia **A**ccess **C**ontrol) **Address -** The unique address that a manufacturer assigns to each networking device.

NAT (**N**etwork **A**ddress **T**ranslation) **-** NAT technology translates IP addresses of a local area network to a different IP address for the Internet.

MER (MAC Encapsulation **R**outing**) - MER** allows IP packet to be carried as bridged frames. There are many applications, such as IPoA, DSL networks and other frame-based network. Depending on your equipment, they can be either bridged or routed within the network.

Network - A series of computers or devices connected for the purpose of data sharing, storage, and/or transmission between users.

Ping (**P**acket **I**nternet **G**roper) **-** An Internet utility used to determine whether a particular IP address is online.

Port - The connection point on a computer or networking device used for plugging in cables or adapters.

PPPoE (**P**oint to **P**oint **P**rotocol **o**ver **E**thernet) **-** PPPoE stands for Point to Point protocol over Ethernet, this protocol is used as a type of broadband connection that provides authentication (username and password) in addition to data transport.

PPPoA (Point to **P**oint **P**rotocol over **ATM) -** PPPoA stands for Point to Point protocol over ATM, this protocol is also used as a type of broadband connection that provides authentication (username and password) in addition to data transport.

RADIUS (Remote **A**uthentication **D**ial**-I**n **U**ser **S**ervice**) -** A protocol that uses an authentication server to control network access.

RJ45 (Registered **J**ack**-45) -** An Ethernet connector that holds up to eight wires.

Router - A networking device that connects multiple networks together.

RPC (Remote **P**rocedure **C**alls**) -** RPC is a powerful technique for constructing distributed, client-server based applications. It is based on extending the notion of convention, or local procedure calling, so that the called procedure need not exist in the same address space as the calling procedure. The two processes may be on the same system, or they may be on different systems with a network connecting them. By using RPC, programmers of distributed applications avoid the details of the interface with the network. The transport independence of RPC isolates the application from the physical and logical elements of the data communications mechanism and allows the application to use a variety of transports.

Server - Any computer whose function in a network is to provide user access to files, printing, communications, and other services.

SOHO (Small Office/Home Office) - Market segment of professionals who work at home or in

small offices.

SSID - A Service Set Identification is a thirty-two character (maximum) alphanumeric key identifying a wireless local area network. For the wireless devices in a network to communicate with each other, all devices must be configured with the same SSID. This is typically the configuration parameter for a wireless PC card. It corresponds to the ESSID in the wireless Access Point and to the wireless network name.

Static IP Address - A fixed address assigned to a computer or device that is connected to a network.

Static Routing - Forwarding data in a network via a fixed path.

Subnet Mask - An address code that determines the size of the network.

TCP (Transmission **C**ontrol **P**rotocol**) -** A network protocol for transmitting data that requires acknowledgement from the recipient of data sent.

TCP/IP (Transmission **C**ontrol **P**rotocol/**I**nternet **P**rotocol**) -** A set of instructions PCs use to communicate over a network.

TKIP (Temporal **K**ey **I**ntegrity **P**rotocol**) -** a wireless encryption protocol that provides dynamic encryption keys for each packet transmitted.

UDP (User Datagram Protocol) - A network protocol for transmitting data that does not require acknowledgement from the recipient of the data that is sent.

VCI (Virtual **C**hannel **I**dentifier**) - The identifier of the VC contained in the ATM cell header.**

VPI (Virtual **P**ath **I**dentifier**) - The identifier of the VP contained in the ATM cell header.**

Update - To replace existing software or firmware with a newer version.

VLAN (Virtual **L**ocal **A**ir **N**etwork**) -** Logical subgroups that constitute a Local Area Network (LAN). This is done in software rather than defining a hardware solution.

VLAN ID (0-4095) - Indicates the ID number of the VLAN being configured. Up to 256 VLANs can be created.

WAN (**W**ide **A**rea **N**etwork) **-** Networks that cover a large geographical area.

Web-based Utility - The web page that allows you to manage the Router.

WEP (Wired **E**quivalent **P**rivacy**) -** A data privacy mechanism based on a 64-bit or 128-bit or 152-bit shared key algorithm, as described in the IEEE 802.11g standard.

Wi-Fi - A trade name for the IEEE 802.11b wireless networking standard, given by the Wireless Ethernet Compatibility Alliance (WECA, see http://www.wi-fi.net), an industry standards group promoting interoperability among IEEE 802.11b devices.

WLAN (Wireless **L**ocal **A**rea **N**etwork**) -** A group of computers and associated devices communicate with each other wirelessly, which network serving users are limited in a local area.

WPA (Wi-Fi Protected **A**ccess**) -** A wireless security protocol use TKIP (Temporal Key Integrity Protocol) encryption, which can be used in conjunction with a RADIUS server.

Appendix B: Specifications

Supporting Standards and Protocols		ANSI T1.413, ITU G.992.1, ITU G.992.2, ITU G.992.3, ITU G.992.5, IEEE 802.11b，IEEE 802.11g，IEEE 802.3, IEEE 802.3u, TCP/IP, IPoA , PPPoA , PPPoE, SNTP, HTTP, DHCP, ICMP, NAT
Ports	LAN Ports	4 10/100M Auto-Negotiation RJ45 ports（Auto MDI/MDIX)
	Line Ports	1 RJ11 port
Network Medium		10Base-T: UTP category 3, 4, 5 cable
		100Base-TX: UTP category-5
LED	LAN/WAN	1,2,3,4(LAN), WLAN, ADSL
	Others	Power, System
Dimensions (L x W x H)		186×146×44（mm), 7.32 × 5.75 × 1.73 (inch)
Working Environment		Working Temperature: 0℃ ~ 40℃
		Storage Temperature: -40℃ ~ 70℃
		Working Humidity: 10% ~ 90% RH (non-condensing)
		Storage Humidity: 10% ~ 90% RH (non-condensing)

Appendix C: Contact Information

For help with the installation or operation of the TP-LINK TL-W8920G 108M Wireless ADSL2+ Router, please visit our website.
http://www.tp-link.com