TP-LINK®

User Guide

TD-W8950ND

150Mbps Wireless Lite N ADSL2+ Modem Router

Rev: 1.0.0
1910010316

COPYRIGHT & TRADEMARKS

http://www.tp-link.com

FCC STATEMENT

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

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

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

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

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

Note: The manufacturer is not responsible for any radio or tv interference caused by unauthorized modifications to this equipment. Such modifications 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

CE 1588 ⓘ

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

This device is intended for home and office use in all EU countries (and other countries following the EU directive 1999/5/EC) without any limitation except for the countries mentioned below:

Country	Restriction	Reason/remark
Bulgaria	None	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	None	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	None	Only for indoor applications

Note: Please don’t use the product outdoors in France.

DECLARATION OF CONFORMITY

For the following equipment:

Product Description: 150Mbps Wireless Lite N ADSL2+ Modem Router

Model No.: TD-W8950ND

Trademark: **TP-LINK**

We declare under our own responsibility that the above products satisfy all the technical regulations applicable to the product within the scope of Council Directives:

Directives 1999/5/EC

The above product is in conformity with the following standards or other normative documents

ETSI EN 300 328 V1.7.1: 2006

ETSI EN 301 489-1 V1.8.1:2008& ETSI EN 301 489-17 V2.1.1:2009

EN60950-1:2006

Recommendation 1999/519/EC

EN62311:2008

Directives 2004/108/EC

The above product is in conformity with the following standards or other normative documents

EN 55022:2006 +A1:2007

EN 55024:1998+A1:2001+A2:2003

EN 61000-3-2:2006

EN 61000-3-3:1995+A1:2001+A2:2005

Directives 2006/95/EC

The above product is in conformity with the following standards or other normative documents

EN60950-1:2006

Directive（ErP） 2009/125/EC

Audio/Video, information and communication technology equipment- Environmentally conscious design

EN62075:2008

Person is responsible for marking this declaration:

Yang Hongliang

Product Manager of International Business

TP-LINK TECHNOLOGIES CO., LTD

South Building, No.5 Keyuan Road, Central Zone, Science & Technology Park, Nanshan, Shenzhen, P. R. China

CONTENTS

Package Contents

The following contents should be found in your package:

- One TD-W8950ND 150Mbps Wireless Lite N ADSL2+ Modem Router
- One Power Adapter for TD-W8950ND 150Mbps Wireless Lite N ADSL2+ Modem Router
- Quick Installation Guide
- One RJ45 cable
- Two RJ11 cables
- One ADSL splitter
- One Resource CD for TD-W8950ND 150Mbps Wireless Lite N ADSL2+ Modem Router, including:
  - This User Guide
  - Other Helpful Information

☞ **Note:**

Make sure that the package contains the above items. If any of the listed items are damaged or missing, please contact with your distributor.

Chapter 1. Product Overview

Thank you for choosing the **TD-W8950ND 150Mbps Wireless Lite N ADSL2+ Modem Router**.

1.1 Overview of the Router

The TD-W8950ND 150Mbps Wireless Lite N ADSL2+ Modem Router integrates 4-port Switch. The Wireless Lite N Router delivers exceptional range and speed, which can fully meet the need of Small Office/Home Office (SOHO) networks and the users demanding higher networking performance.

The TD-W8950ND 150Mbps Wireless Lite N ADSL2+ Modem 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 router provides up to 150Mbps wireless connection with other 802.11n wireless clients. The incredible speed makes it ideal for handling multiple data streams at the same time, which ensures your network stable and smooth. The performance of this 802.11n wireless Router will give you the unexpected networking experience at speed 650% faster than 802.11g. It is also compatible with all IEEE 802.11g and IEEE 802.11b products.

With multiple protection measures, including SSID broadcast control and wireless LAN 64/128 WEP encryption, Wi-Fi protected Access (WPA2-PSK, WPA-PSK), as well as advanced Firewall protections, the TD-W8950ND 150Mbps Wireless Lite N ADSL2+ Modem Router provides complete data privacy.

The Router provides flexible access control, so that parents or network administrators can establish restricted access policies for children or staff.

The Router provides flexible access control, so that parents or network administrators can establish restricted access policies for children or staff. It also supports Virtual Server and DMZ host for Port Triggering, and then the network administrators can manage and monitor the network in real time with the remote management function.

Since the Router is compatible with virtually all the major operating systems, it is very easy to manage. Quick Setup Wizard is supported and detailed instructions are provided step by step in this user guide. Before installing the Router, please look through this guide to know all the Router's functions.

1.2 Main Features

- Make use of IEEE 802.11n wireless technology to provide a wireless data rate of up to 150Mbps
- One RJ11 LINE port, four 10/100M Auto-Negotiation RJ45 LAN ports, supporting Auto MDI/MDIX
- Provides WPA/WPA2, WPA-PSK/WPA2-PSK authentication, TKIP/AES encryption security
- Shares data and Internet access for users, supporting Dynamic IP/Static IP/PPPoE Internet access
- Supports Virtual Server, Port Triggering and DMZ host
- Supports UPnP, Dynamic DNS, Static Routing
- Provides Automatic-connection and Scheduled Connection on certain time to the Internet
- Connects Internet on demand and disconnects from the Internet when idle for PPPoE
- Built-in NAT and DHCP server supporting static IP address distributing
- Supports Stateful Packet Inspection
- Supports VPN Passthrough
- Supports access control, parents and network administrators can establish restricted access policies based on time of day for children or staff
- Provides 64/128/152-bit WEP encryption security and wireless LAN ACL (Access Control List)
- Supports Flow Statistics
- High speed and asymmetry data transmit mode, provides safe and exclusive bandwidth
- Support All ADSL industrial standards
- Compatible with all mainstream DSLAM (CO)
- Provide integrated access of internet and route function which face to SOHO user
- Advanced DMT modulation and demodulation
- Real-time Configuration and device monitoring
- Quick response semi-conductive surge protect circuit, provides reliable ESD and surge-protect function
- Supports ADSL dual latency (fast path and interleaved path)
- Quick response semi-conductive surge protect circuit, reliable surge-protect function
- AFE to support Annex A 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
- Supports bridge mode and Router function
- Supports Web management and firmware upgrade
- Supports QSS (Quick Secure Setup)

1.3 Panel Layout

1.3.1 The Front Panel

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

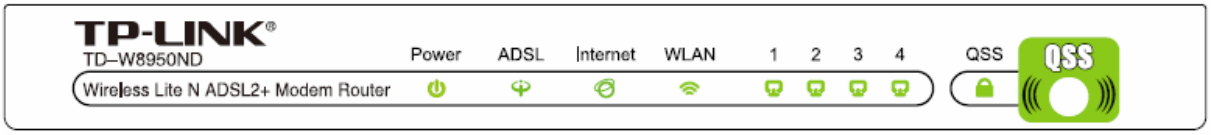


Figure 1-1

The Router's LEDs and the QSS button are located on the front panel (View from left to right).

Name	Status	Description
Power	On	Power is on
	Off	Power is off
ADSL	On	The LINE port has connected to ISP's network
	Flashing	The LINE port is connecting to the ISP's network
	Off	The LINE port is disconnected
Internet	On	A successful PPP connection has been established
	Flashing	Data is being transferred over the Internet
	Off	There is no successful PPP connection or the Router works on Bridge mode
WLAN	Off	The Wireless function is disabled
	Flashing	The Wireless function is enabled
LAN 1-4	On	There is a device linked to the corresponding port but there is no activity
	Flashing	There is an active device linked to the corresponding port
	Off	There is no device linked to the corresponding port
QSS	On	A wireless device has been successfully added to the network by QSS function.
	Flashing	A wireless device is connecting to the network by QSS function.
	Off	No wireless device is added to the network by QSS function.

☞ **Note:**

After a device is successfully added to the network by QSS function, the QSS LED will keep on for about 5 minutes and then turn off.

1.3.2 The Back Panel

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

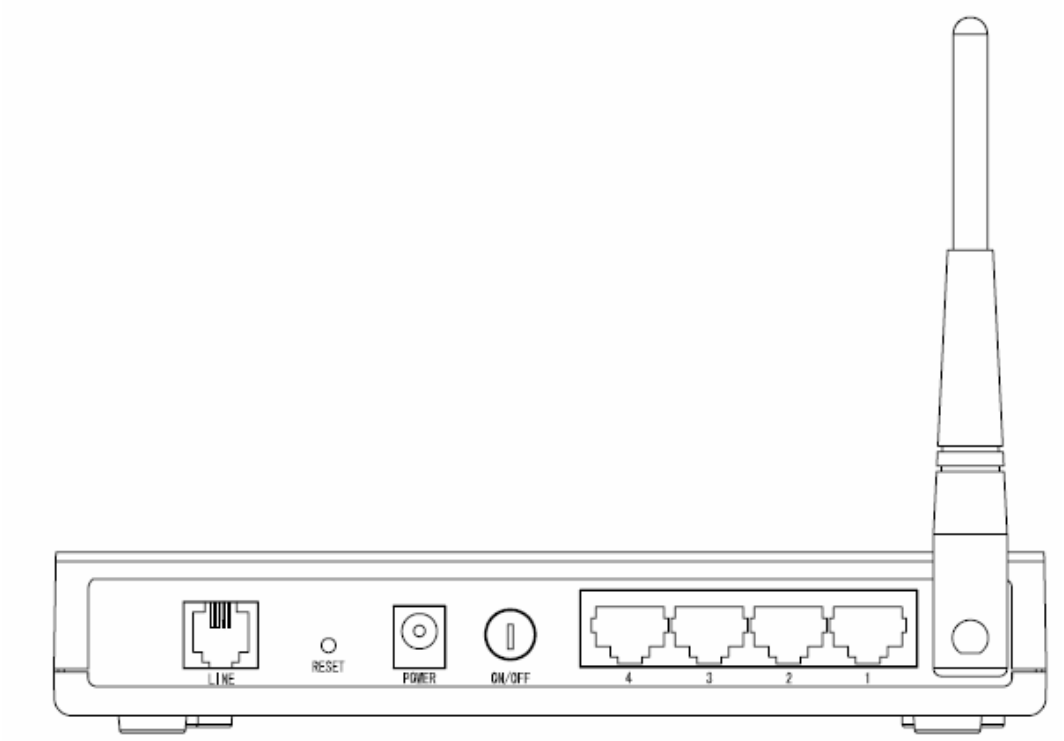


Figure 1-2

- LINE: Connect to the Modem Port of Splitter or to the telephone line.
- Reset: There are two ways to reset the Router's factory defaults.

1) Use the Restore Default function on Management -> Settings -> Restore Default page in the router's Web-based Utility.
2) Use the Factory Default RESET button: With the Router powered on, use a pin to press and hold the RESET button for at least 5 seconds. And the Router will reboot to its factory default settings.

- POWER: The Power plug is where you will connect the power adapter.
- ON/OFF: The switch for the power.
- 1, 2, 3, 4 (LAN): The ports (1, 2, 3, 4) connect the Router to the local PC(s).
- Wireless Antennas: To receive and transmit the wireless data.

Chapter 2. Connecting the Router

2.1 System Requirements

- Broadband Internet Access Service (DSL/Cable/Ethernet).
- PCs with a working Ethernet Adapter and an Ethernet cable with RJ45 connectors.
- TCP/IP protocol on each PC.
- Web browser, such as Microsoft Internet Explorer, Mozilla Firefox or Apple Safari.

2.2 Installation Environment Requirements

- Place the Router in a well ventilated place far from any heater or heating vent
- Avoid direct irradiation of any strong light (such as sunlight)
- Keep at least 2 inches (5 cm) of clear space around the Router
- Operating temperature: 0℃~40℃ (32℉~104℉)
- Operating Humidity: 10% ~ 90% RH (non-condensing)

2.3 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 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 at the center of your wireless network.
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. Or you can access the Internet and make calls at the same time by using a separate splitter to divide the data and voice. The external splitter has three ports:
   - LINE: Connect to the wall jack
   - PHONE: Connect to the phone sets
   - MODEM: Connect to the ADSL LINE port of device

   Plug one end of the twisted-pair ADSL cable into the ADSL LINE port on the rear panel of device. Connect the other end to the MODEM port of the external splitter.
5. Connect the power adapter to the power plug of the Router, and the other end into an electrical outlet. The electrical outlet shall be installed near the device and shall be easily accessible.
6. Turn on the ON/OFF switch to power the device. It will start to work automatically.

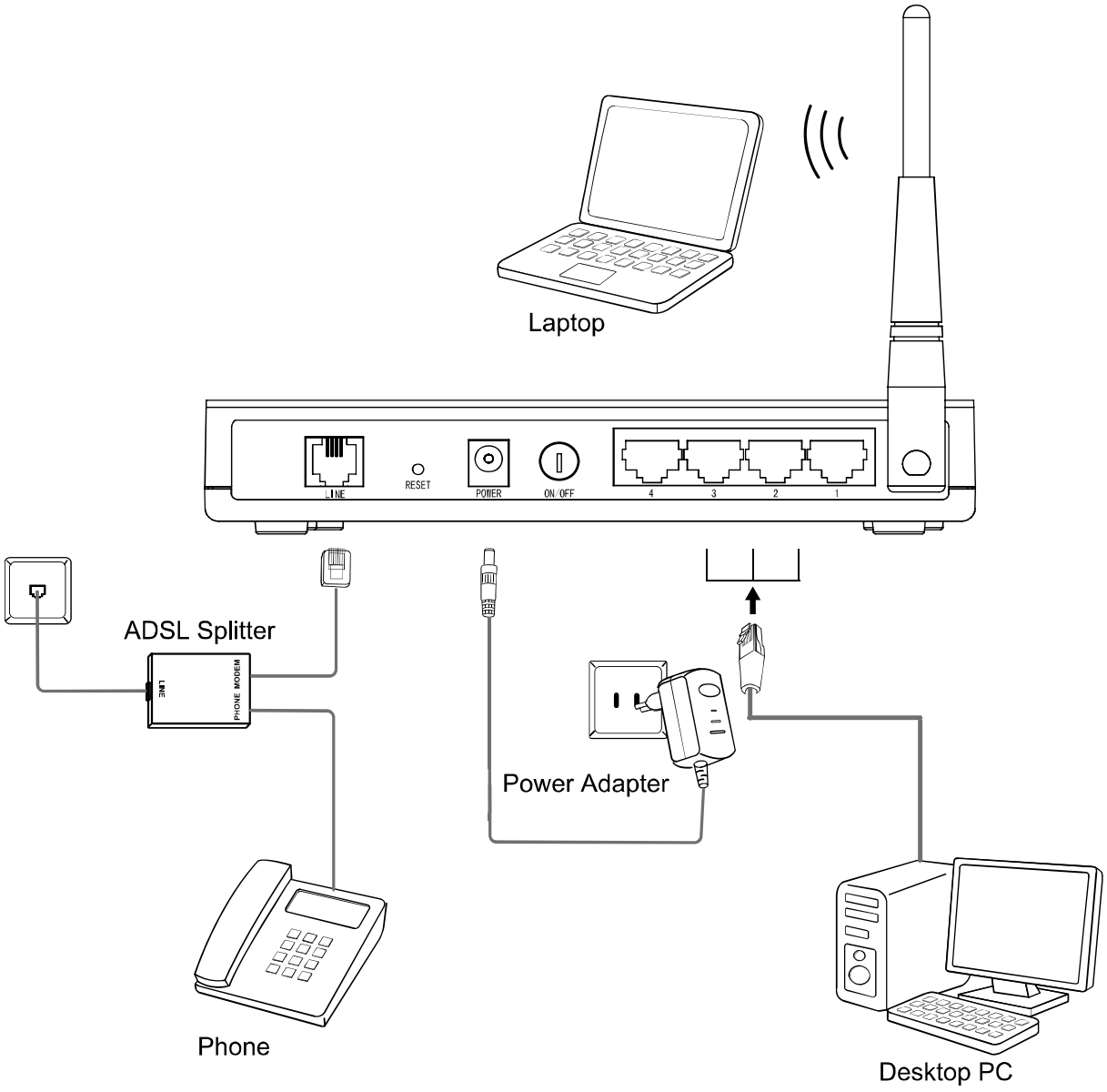

Laptop
LINE
RESET
POWER
ON/OFF
4
3
2
1
ADSL Splitter
LINE
PHONE MODEM
Power Adapter
Phone
Desktop PC

Figure 2-1

Chapter 3. Quick Installation Guide

This chapter will show you how to configure the basic functions of your TD-W8950ND 150Mbps Wireless Lite N ADSL2+ Modem Router using Quick Setup Wizard within minutes.

3.1 TCP/IP Configuration

The default IP address of the Router is 192.168.1.1. And the default Subnet Mask is 255.255.255.0. These values can be changed as you desire. In this guide, we use all the default values for description.

Connect the local PC to the LAN ports of the Router. And then you can configure the IP address for your PC in the following two ways.

1. Configure the IP address manually

1) Set up the TCP/IP Protocol for your PC. If you need instructions as to how to do this, please refer to "Appendix B: Configuring the PC".

2) Configure the network parameters. The IP address is 192.168.1.xxx ("xxx" is any number from 2 to 254), Subnet Mask is 255.255.255.0, and Gateway is 192.168.1.1 (The Router's default IP address).

2. Obtain an IP address automatically

1) Set up the TCP/IP Protocol in "Obtain an IP address automatically" mode on your PC. If you need instructions as to how to do this, please refer to "Appendix B: Configuring the PC".

2) Then the built-in DHCP server will assign IP address for the PC.

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 OS.

Open a command prompt, and type *ping 192.168.1.1*, and then press Enter.

3. If the result displayed is similar to the Figure 3-1, it means the connection between your PC and the Router has been established well.

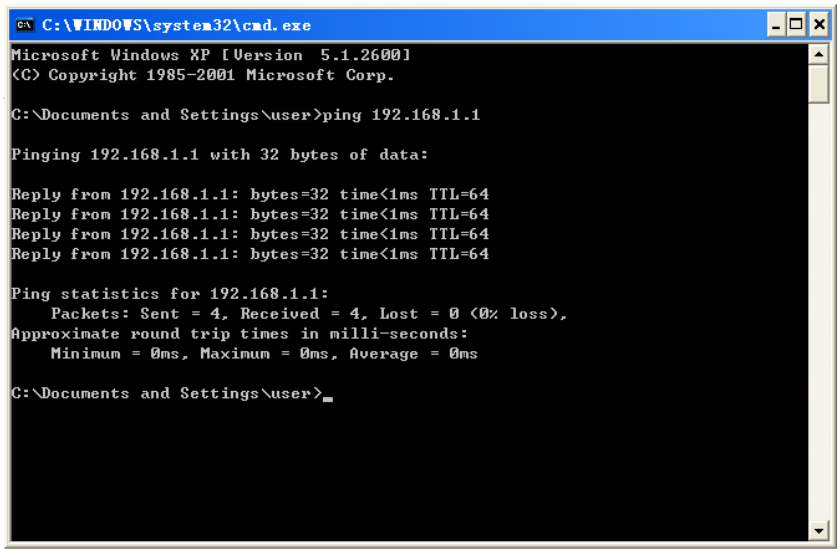


Figure 3-1 Success result of Ping command

➢ If the result displayed is similar to the Figure 3-2, it means the connection between your PC and the Router is failed.

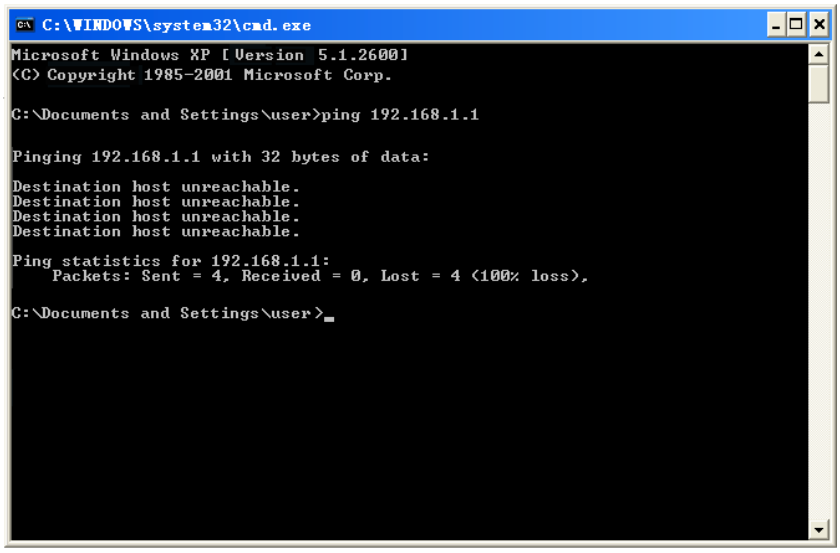


Figure 3-2 Failure result of Ping command

Please check the connection following these steps:

1. Is the connection between your PC and the Router correct?

☞ **Note:**

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

2. Is the TCP/IP configuration for your PC 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.

3.2 Quick Installation Guide

With a Web-based utility, it is easy to configure and manage the TD-W8950ND 150Mbps Wireless Lite N ADSL2+ Modem Router. The Web-based utility can be used on any Windows, Macintosh or UNIX OS with a Web browser, such as Microsoft Internet Explorer, Mozilla Firefox or Apple Safari.

1. To access the configuration utility, open a web-browser and type in the default address http://192.168.1.1 in the address field of the browser.

Figure 3-3

After a moment, a login window will appear, similar to the Figure 3-4. Enter admin for the User Name and Password, both in lower case letters. Then click the OK button or press the Enter key.

Figure 3-4

Note:

1) Do not mix up the user name and password with your ADSL account user name and password which are needed for PPP connections.

2) If the above screen does not pop up, it means that your Web-browser has been set to a proxy. Go to Tools menu→Internet Options→Connections→LAN Settings, in the screen that appears, cancel the Using Proxy checkbox, and click OK to finish it.

2. After your successful login, you will see the Login screen as shown in Figure 3-5. Click Quick Setup menu to access Quick Setup Wizard.

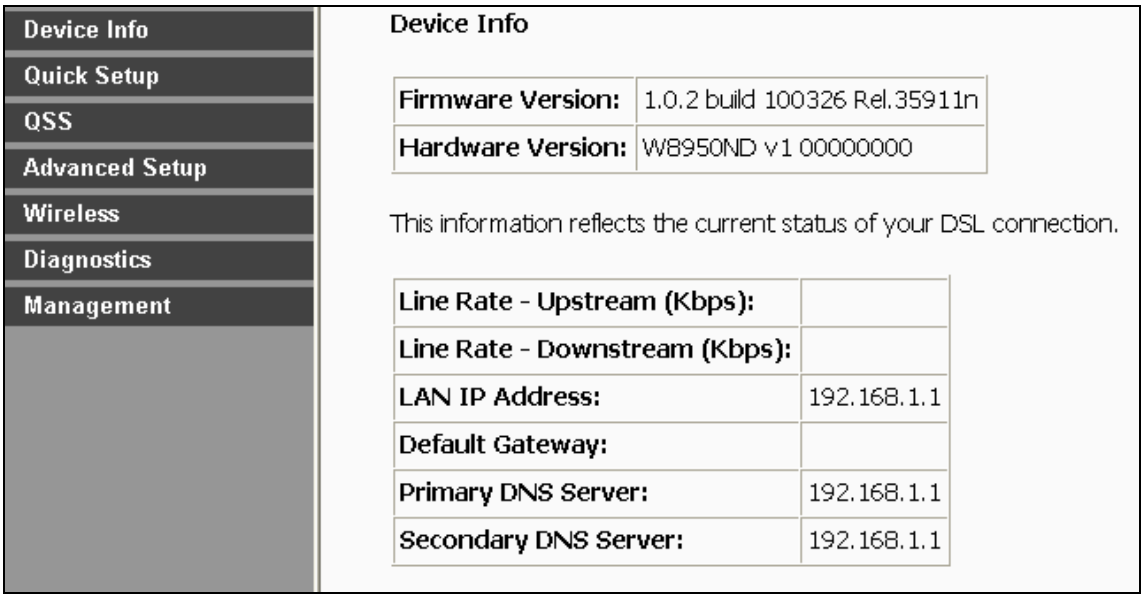


Figure 3-5

3. 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, and then click Next.

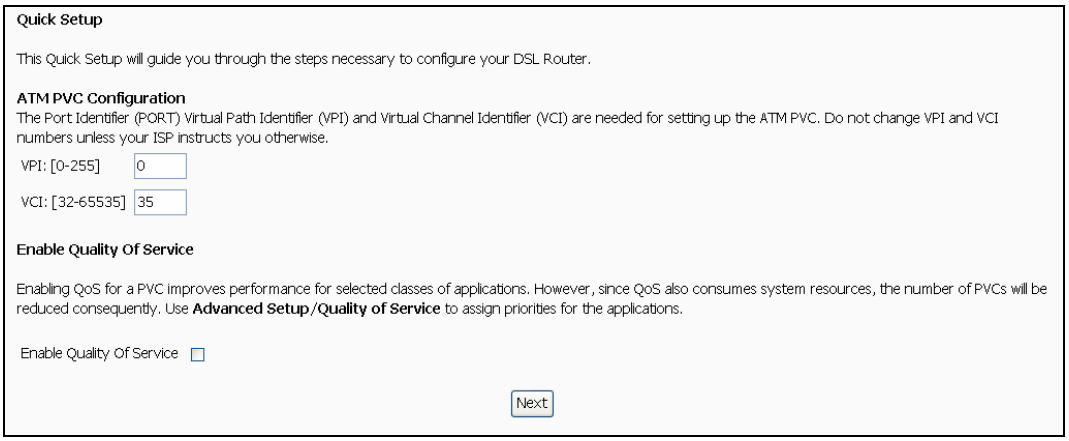


Figure 3-6

4. The Connection Type page will display. Here we select PPPoE WAN Link Type for example.

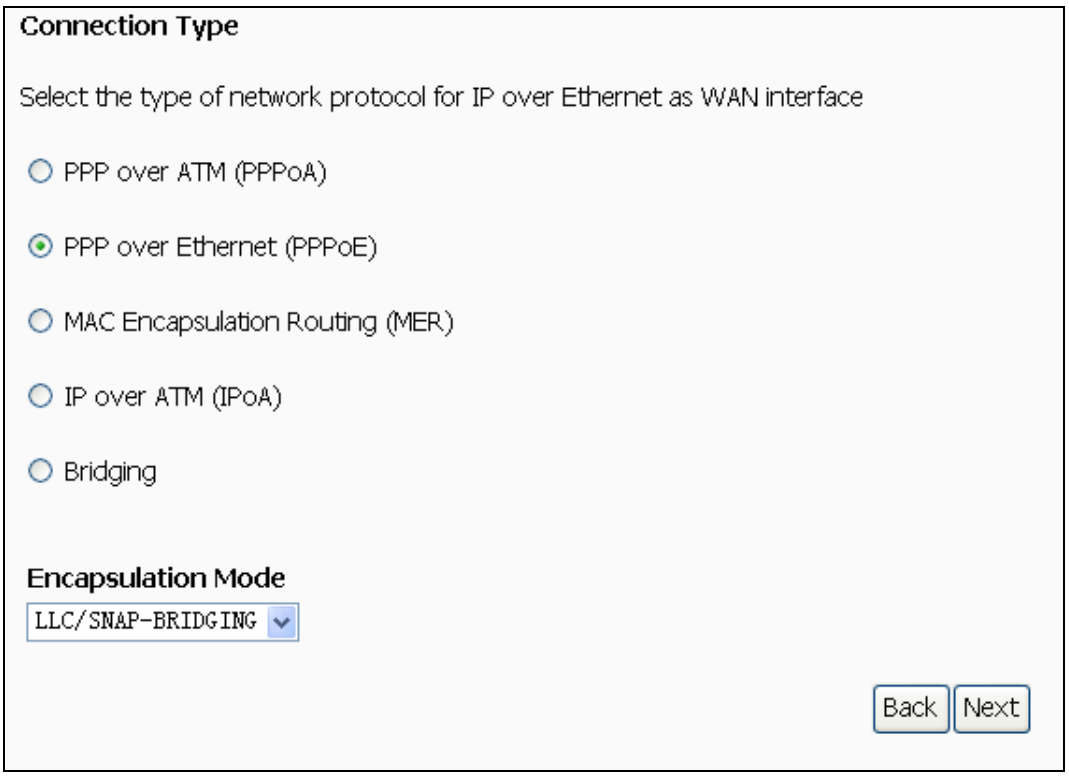


Figure 3-7

5. Enter the Username and Password given by your ISP and click Next to continue.

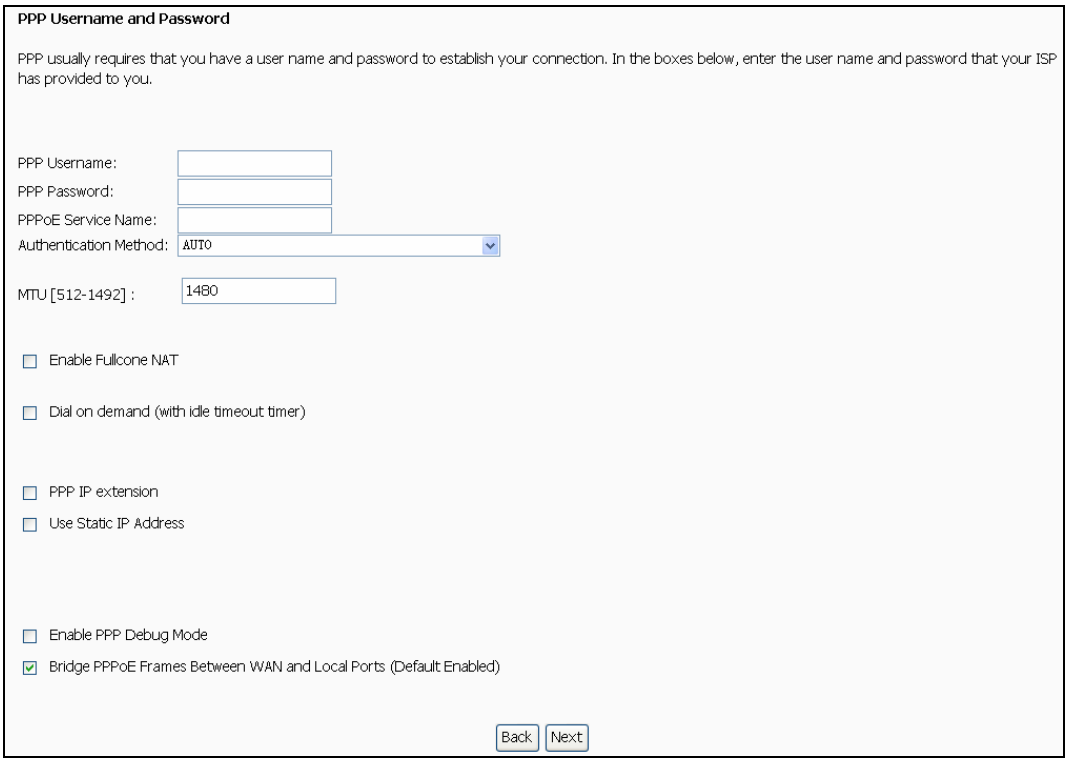


Figure 3-8

6. The following page will display. Keep the default settings and click Next to continue.

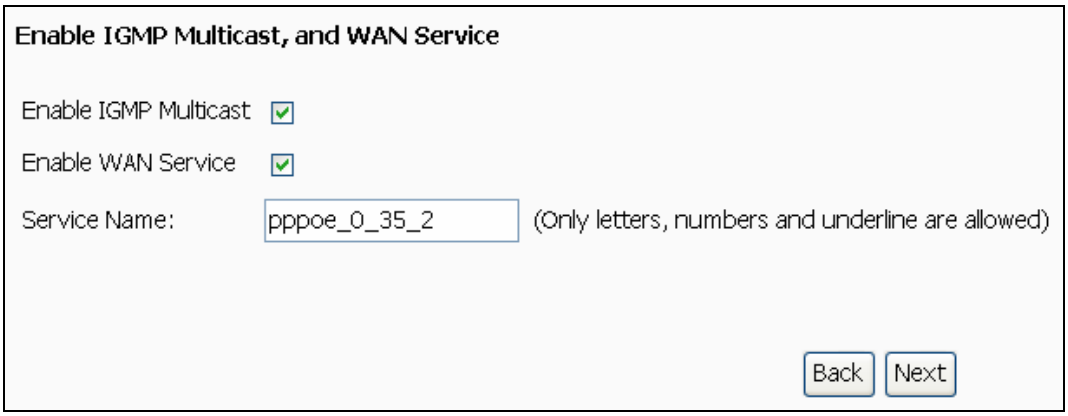


Figure 3-9

7. The Wireless -- Setup page will display. Click Next to continue.

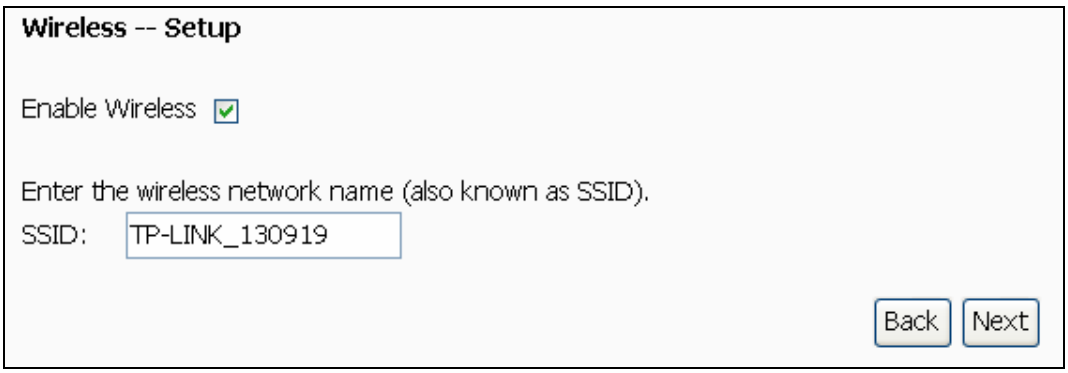


Figure 3-10

8. You will see the Summary screen below, click Save/Reboot to save these settings.

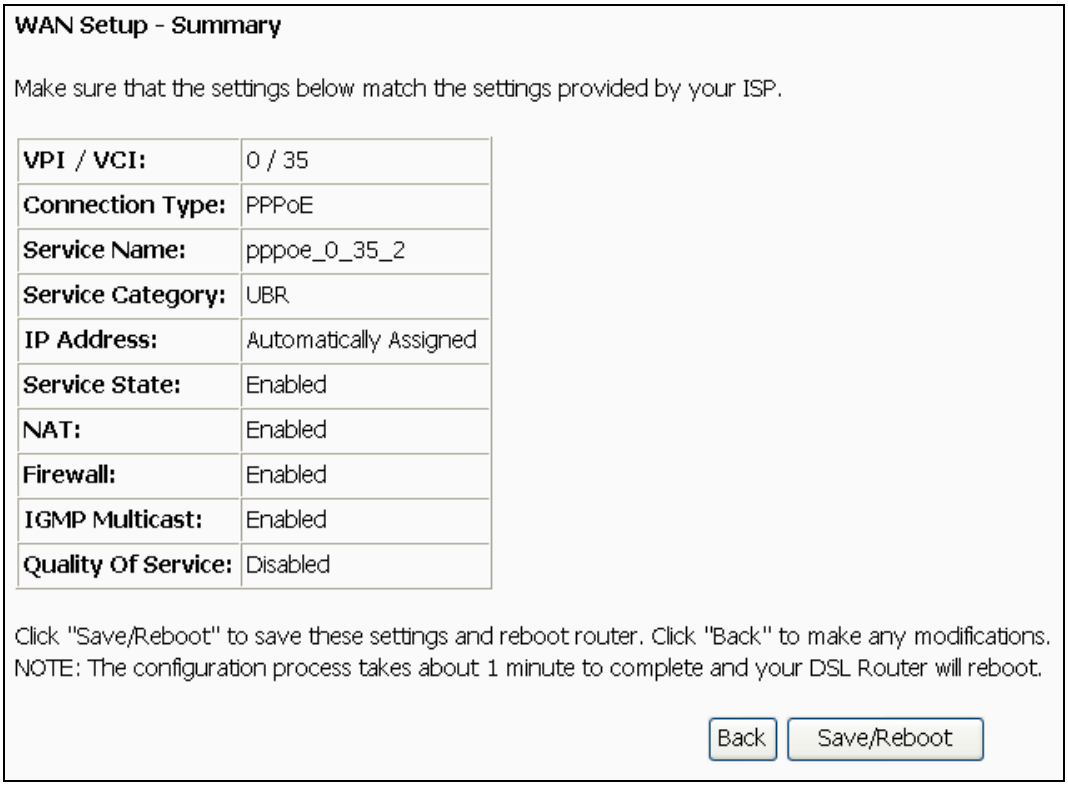


Figure 3-11

9. Now, your ADSL Modem Router has been configured and is rebooting. Please do not power off the Router while it's rebooting. After successfully rebooting, the Router will return to the Device Info page.

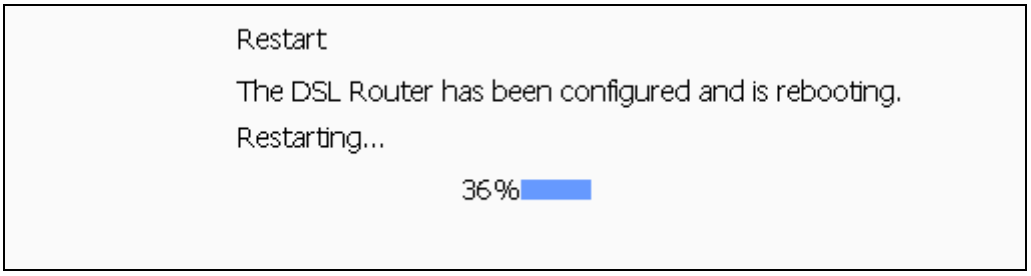


Figure 3-12

Note:

The Quick Setup Wizard will guide you to configure the WAN Service over ATM interface.

Chapter 4. Configuring the Router

This chapter will show each Web page's key function and the configuration way.

4.1 Login

After your successful login, you will see the six main menus on the left of the Web-based utility. On the right, there are the corresponding explanations and instructions.

The detailed explanations for each Web page's key function are listed below.

4.2 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 4-1). The first table indicates the information about the version including Software and Hardware. The second table displays the current status of the TD-W8950ND connection. This information will vary depending on the settings of the Router configured on the Advanced Setup screen.

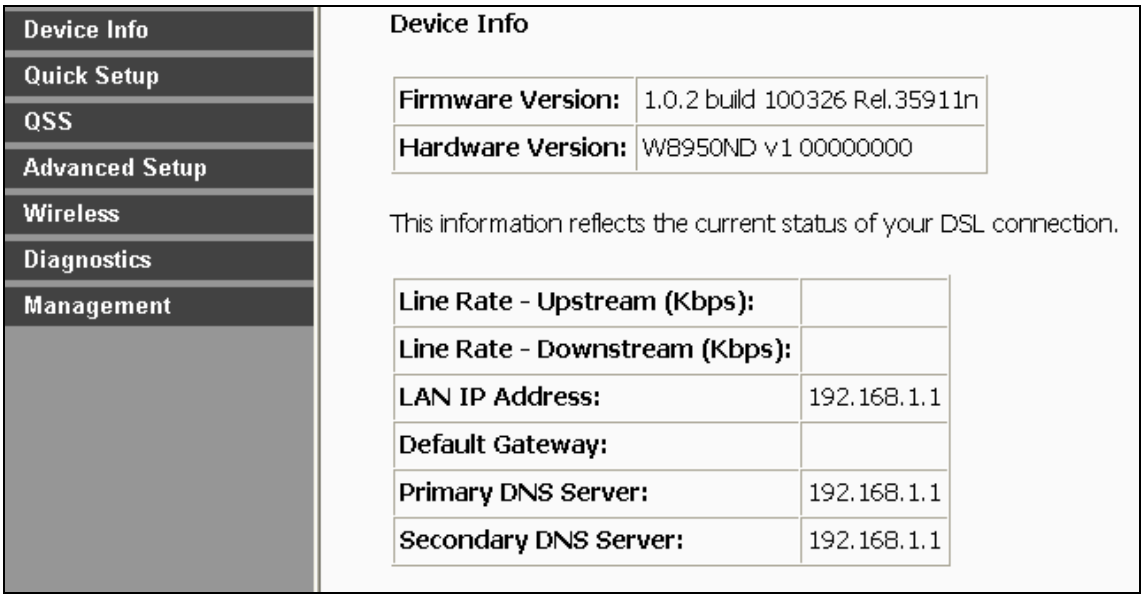


Figure 4-1

Note:

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

4.3 Quick Setup

Please refer to Section 3.2 Quick Installation Guide.

4.4 QSS

This section will guide you add a new wireless device to an existing network quickly by QSS (Quick Secure Setup) function.

a). Choose menu “QSS”, you will see the next screen (shown in Figure 4-2).

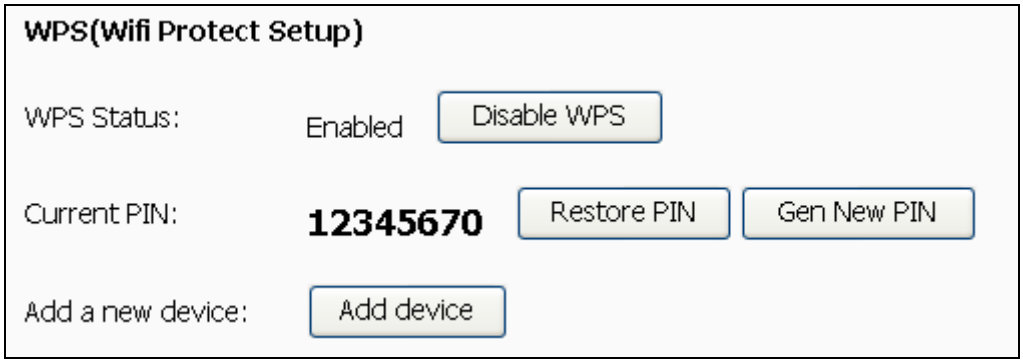


Figure 4-2 QSS

- WPS Status - Enable or disable the QSS function here.
- Current PIN - The current value of the Router's PIN displayed here. The default PIN of the Router can be found in the label or User Guide.
- Restore PIN - Restore the PIN of the Router to its default.
- Gen New PIN - Click this button, and then you can get a new random value for the Router's PIN. You can ensure the network security by generating a new PIN.
- Add device - You can add the new device to the existing network manually by clicking this button.

b). To add a new device:

If the wireless adapter supports Wi-Fi Protected Setup (WPS), you can establish a wireless connection between wireless adapter and Router using either Push Button Configuration (PBC) method or PIN method.

Note:

To build a successful connection by QSS, you should also do the corresponding configuration of the new device for QSS function meanwhile.

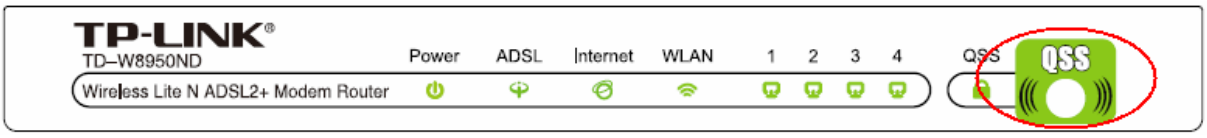
For the configuration of the new device, here takes the Wireless Adapter of our company for example.

I. By PBC

If the wireless adapter supports Wi-Fi Protected Setup and the Push Button Configuration (PBC) method, you can add it to the network by PBC with the following two methods.

Method One: Hardware push button.

Step 1: Press the QSS button on the front panel of the Router.



Step 2: Press and hold the QSS button of the adapter directly for 2 or 3 seconds.

Step 3: Wait for a while until the next screen of adapter appears. Click **Finish** to complete the QSS configuration.

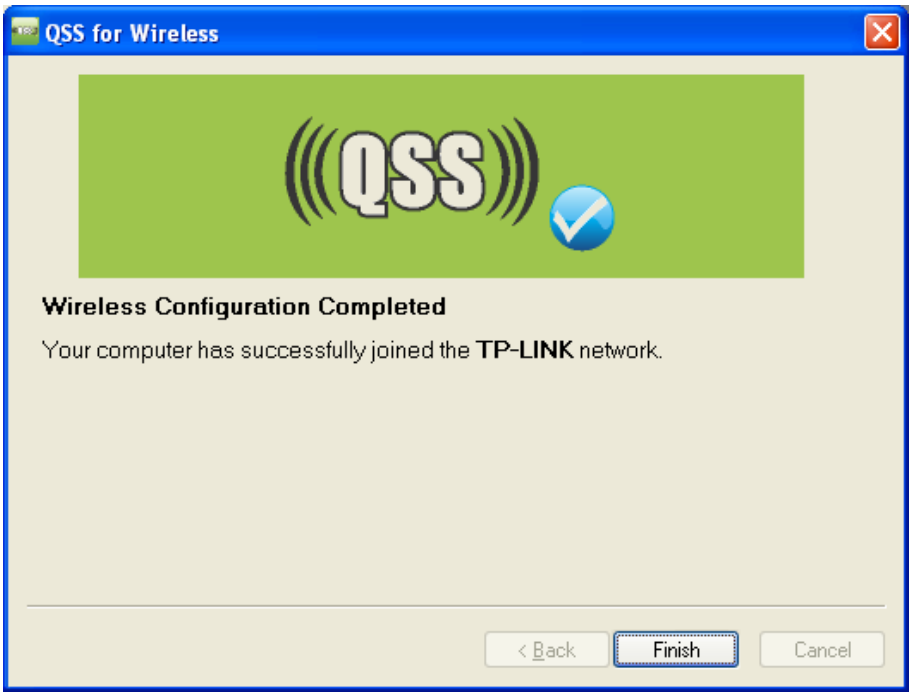
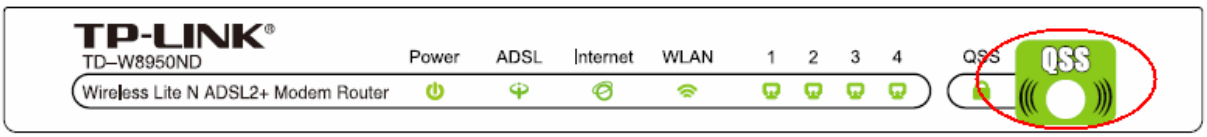


Figure 4-3

Method Two:

Step 1: Press the QSS button on the front panel of the Router.



Step 2: For the configuration of the wireless adapter, please choose “Push the button on my access point” in the configuration utility of the QSS as below, and click **Next**.

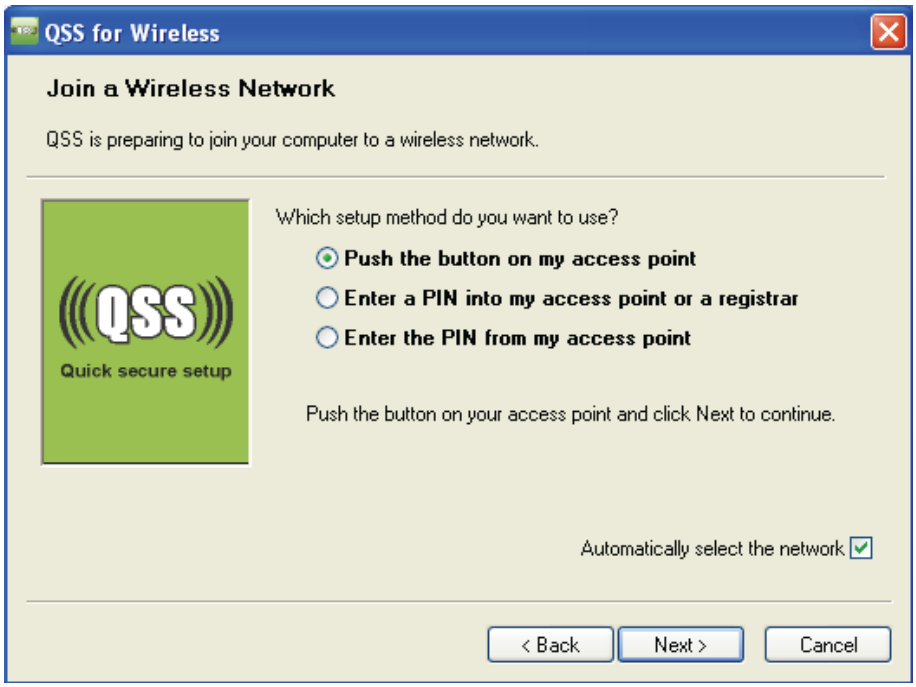


Figure 4-4

Step 3: Wait for a while until the next screen appears. Click **Finish** to complete the QSS configuration.

Figure 4-5

Method Three:

Step 1: Keep the default QSS Status as Enabled and click the Add device button in Figure 4-2, then the following screen will appear.

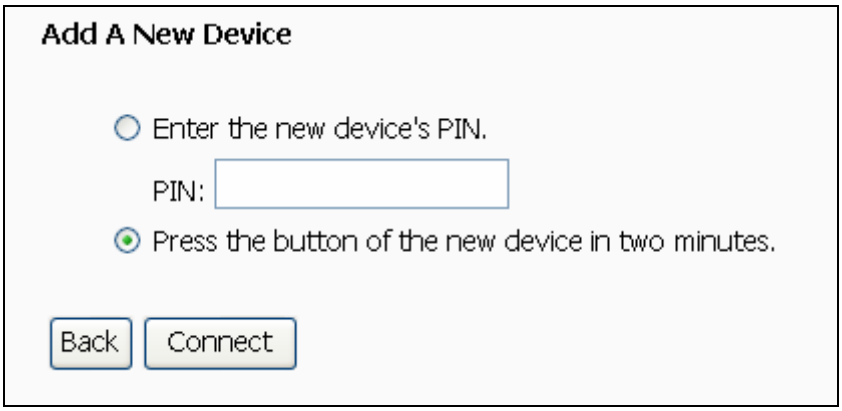
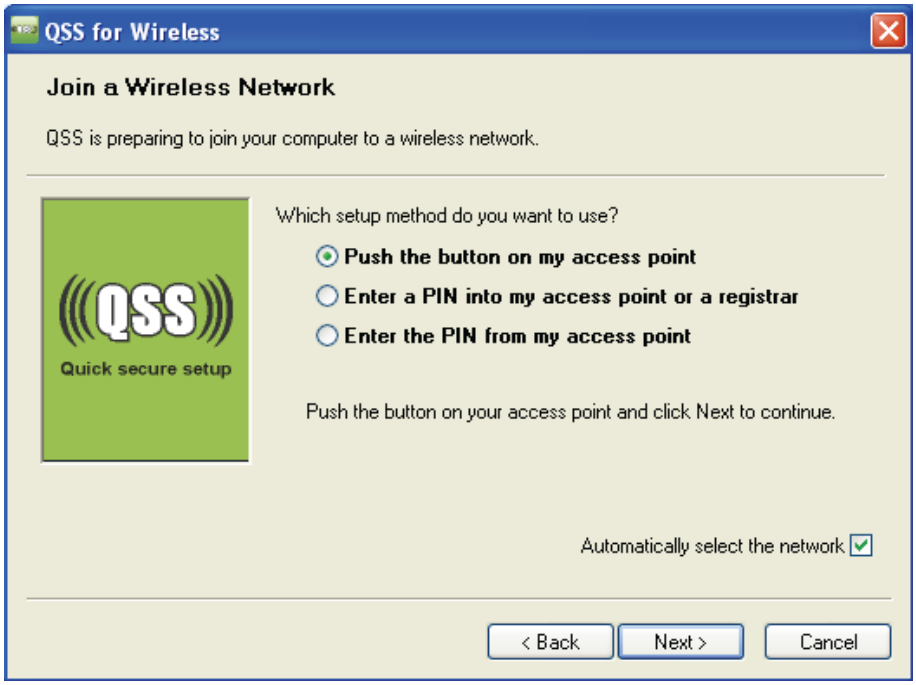


Figure 4-6 Add A New Device

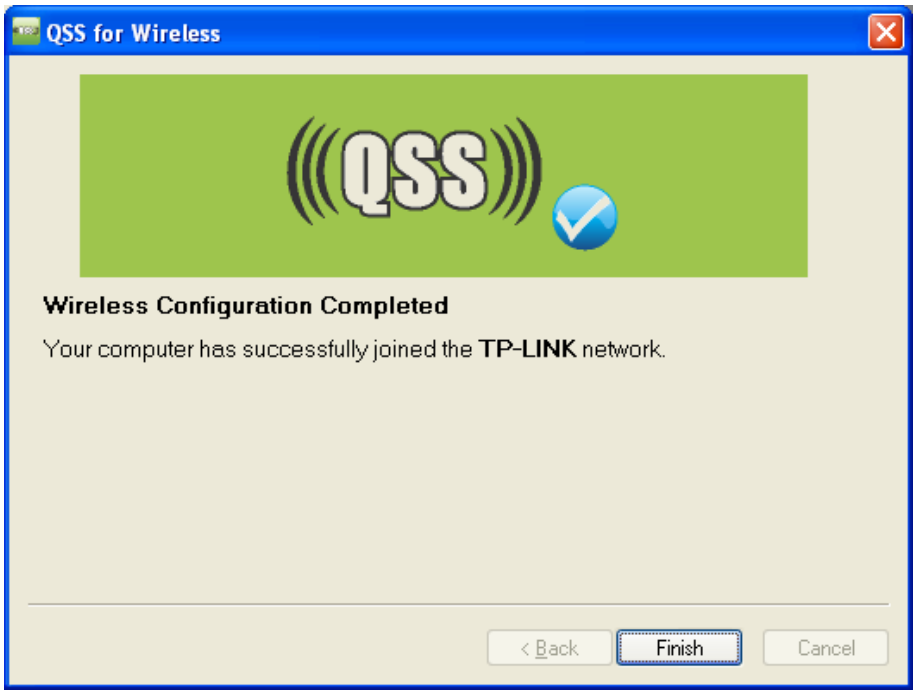
Step 2: Choose Press the button of the new device in two minutes and click Connect.

Step 3: For the configuration of the wireless adapter, please choose Push the button on my access point in the configuration utility of the QSS as below, and click **Next**.



The QSS Configuration Screen of Wireless Adapter

Step 4: Wait for a while until the next screen appears. Click **Finish** to complete the QSS configuration.



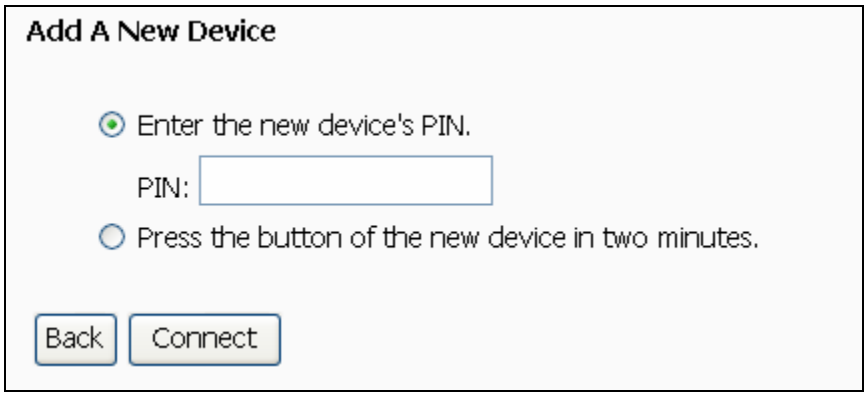
The QSS Configuration Screen of Wireless Adapter

II. By PIN

If the new device supports Wi-Fi Protected Setup and the PIN method, you can add it to the network by PIN with the following two methods.

Method One: Enter the PIN into my Router

Step 1: Keep the default QSS Status as Enabled and click the Add device button in Figure 4-2, then the following screen will appear.

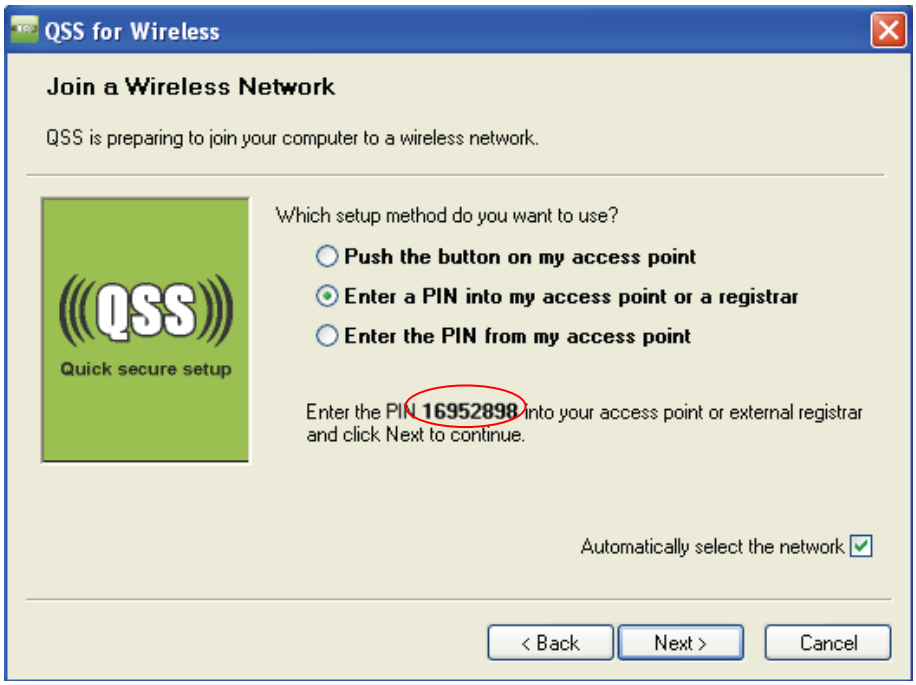


Step 2: Choose **Enter the new device's PIN** and enter the PIN code of the wireless adapter in the field behind PIN in the above figure. Then click Connect.

☞ **Note:**

The PIN code of the adapter is always displayed on the QSS configuration screen

Step 3: For the configuration of the wireless adapter, please **choose Enter a PIN into my access point or a registrar** in the configuration utility of the QSS as below, and click Next.



The QSS Configuration Screen of Wireless Adapter

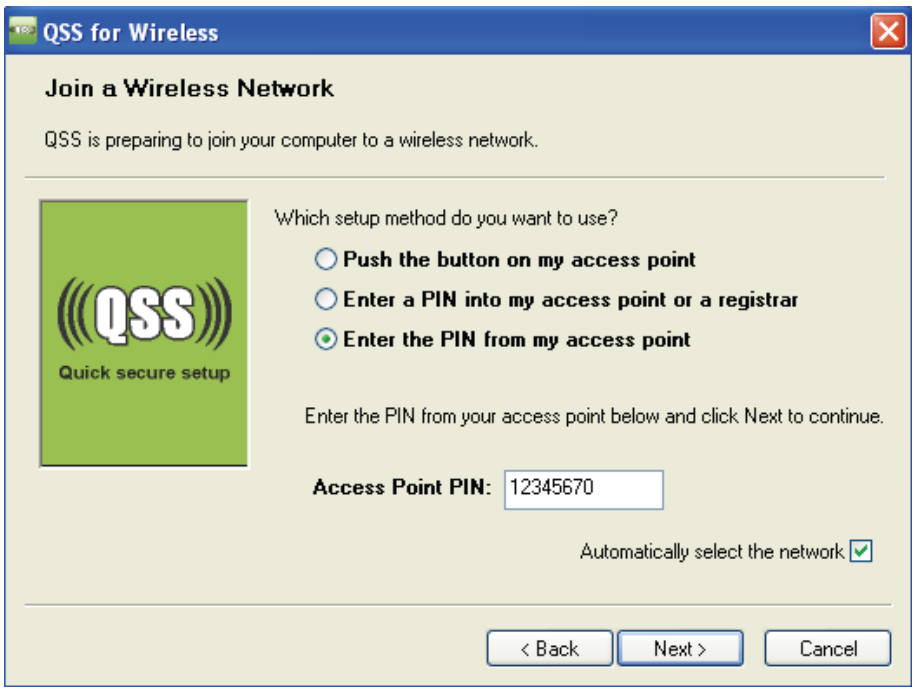
Note:

In this example, the default PIN code of this adapter is 16952898 as the above figure shown.

Method Two: Enter the PIN from my Router

Step 1: Get the Current PIN code of the Router in Figure 4-2 (each Router has its unique PIN code. Here takes the PIN code 12345670 of this Router for example).

Step 2: For the configuration of the wireless adapter, please choose Enter a PIN from my access point in the configuration utility of the QSS as below, and enter the PIN code of the Router into the field behind Access Point PIN. Then click **Next**.

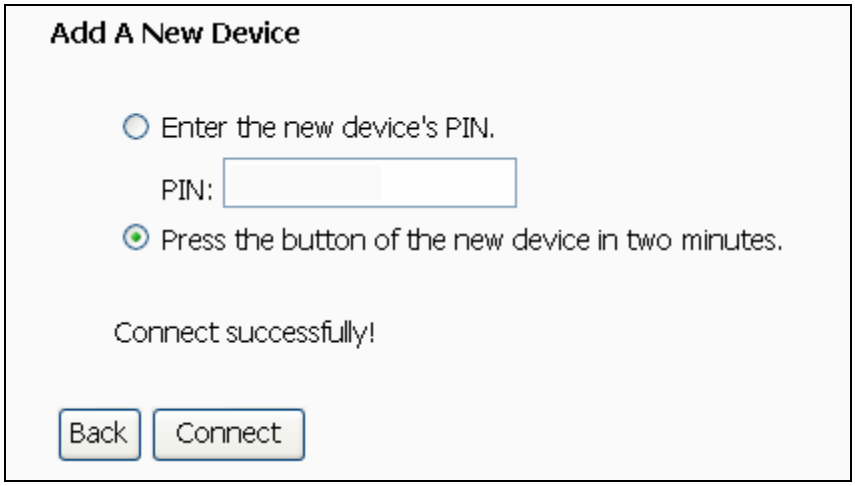


The QSS Configuration Screen of Wireless Adapter

Note:

The default PIN code of the Router can be found in its label or the QSS configuration screen as Figure 4-2.

c). You will see the following screen when the new device successfully connected to the network.



Note:

1） The status LED on the Router will light green all the time if the device has been successfully added to the network.

2） The QSS function cannot be configured if the Wireless Function of the Router is disabled. Please make sure the Wireless Function is enabled before configuring the QSS.

4.5 Advanced Setup

Choose “Advanced Setup”, and you can see the submenus as shown in Figure 4-7

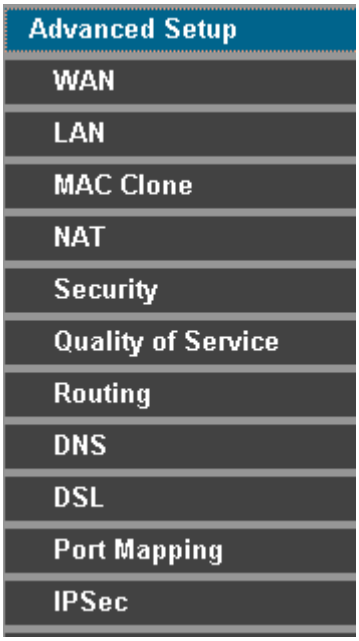


Figure 4-7

4.5.1 WAN

Choose “Advanced Setup”→”WAN”, and you will see the page of Wide Area Network (WAN) Setup as shown Figure 4-8

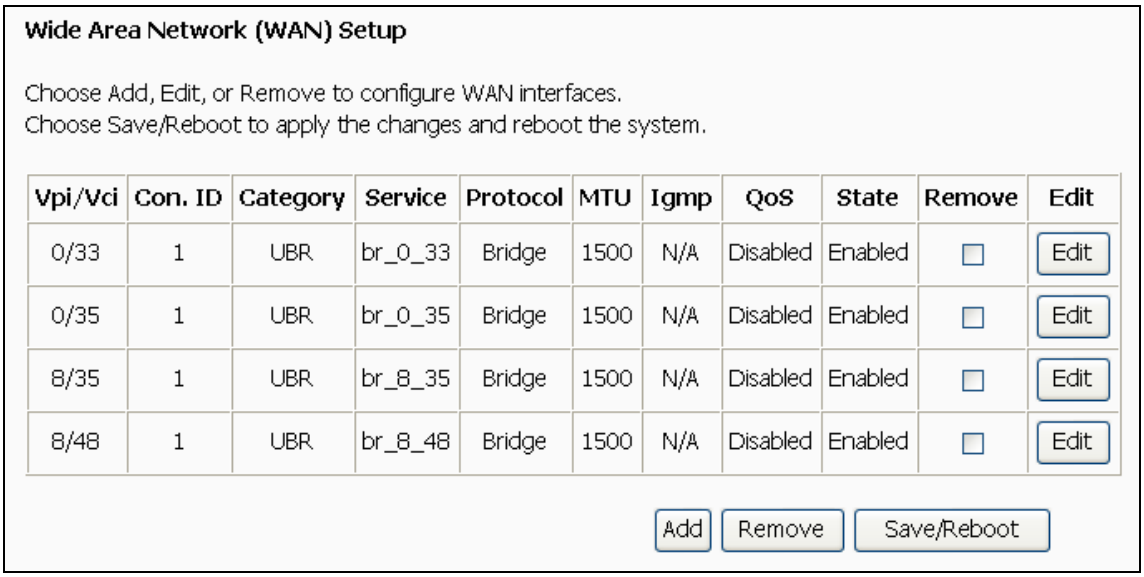


Figure 4-8

There are 4 PVC links in the WAN setup page. Click the Add button or choose the appropriate PVC according to your need. Then you will enter the page of ATM PVC Configuration as shown in Figure 4-9.

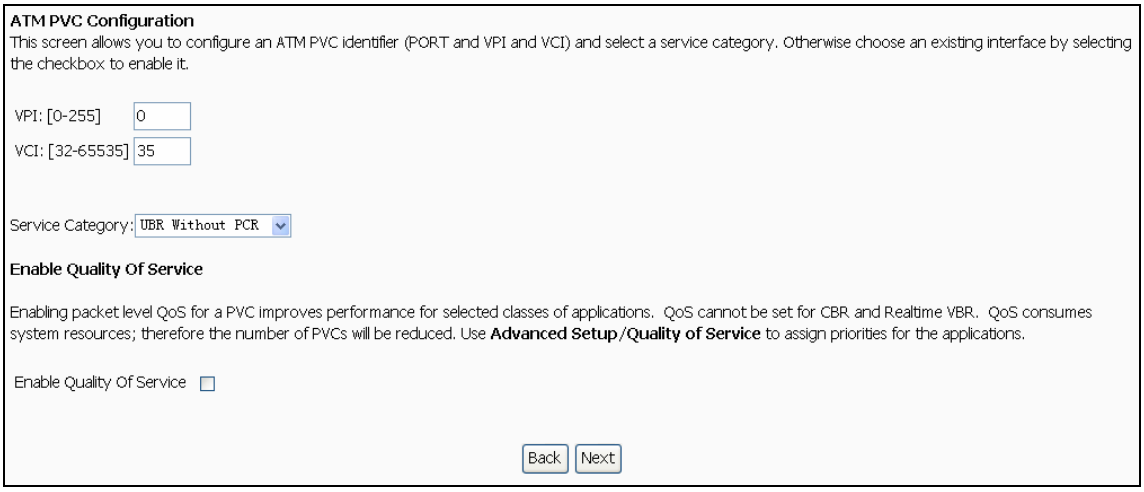


Figure 4-9

Enter VPI/VCI value and service category provided by your ISP. Click Next to enter the next step. You will see the Figure 4-10.

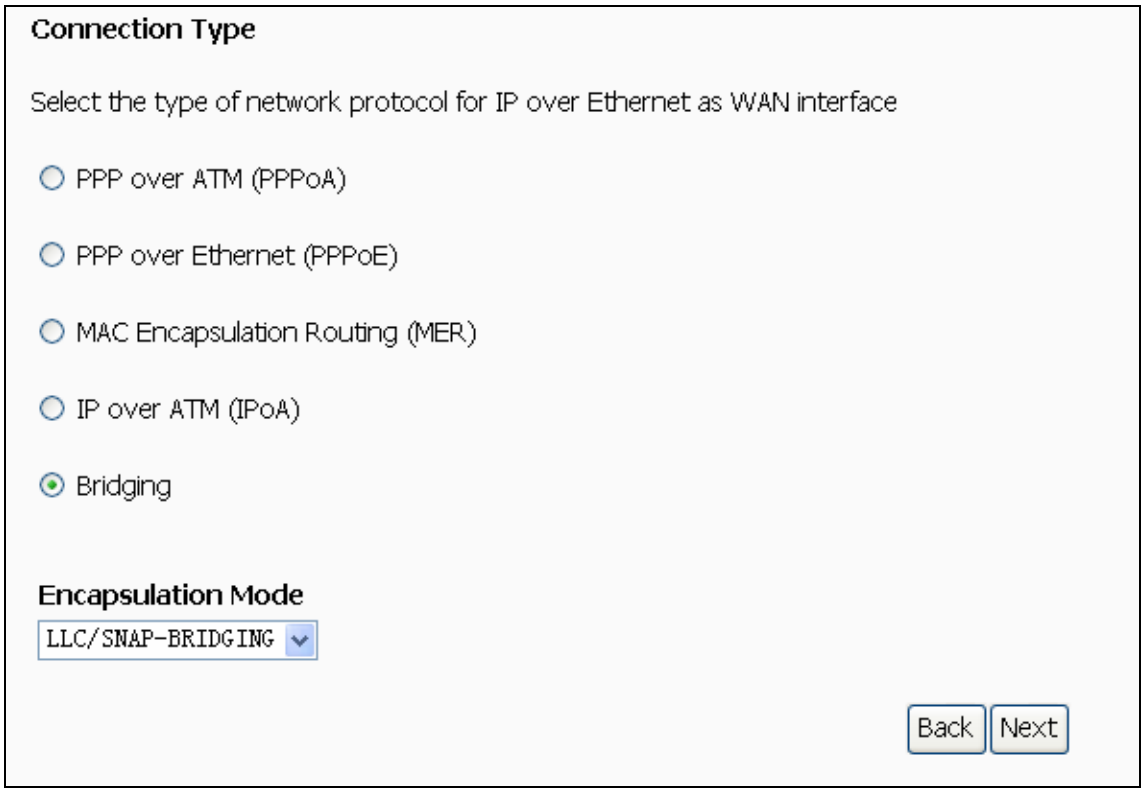


Figure 4-10

After choosing the proper protocol, enter the correct parameters supported by your ISP. Enable the configurations, and then you will go to the Internet.

☞ **Note:**

The type of network protocol selected may be different in different areas. There are five types, so you should ask your ISP to acquire the Connection Type and Encapsulation Mode.

➢ PPP over ATM (PPPoA)

If you select the protocol of PPP over ATM (PPPoA), you will see the Figure 4-11.

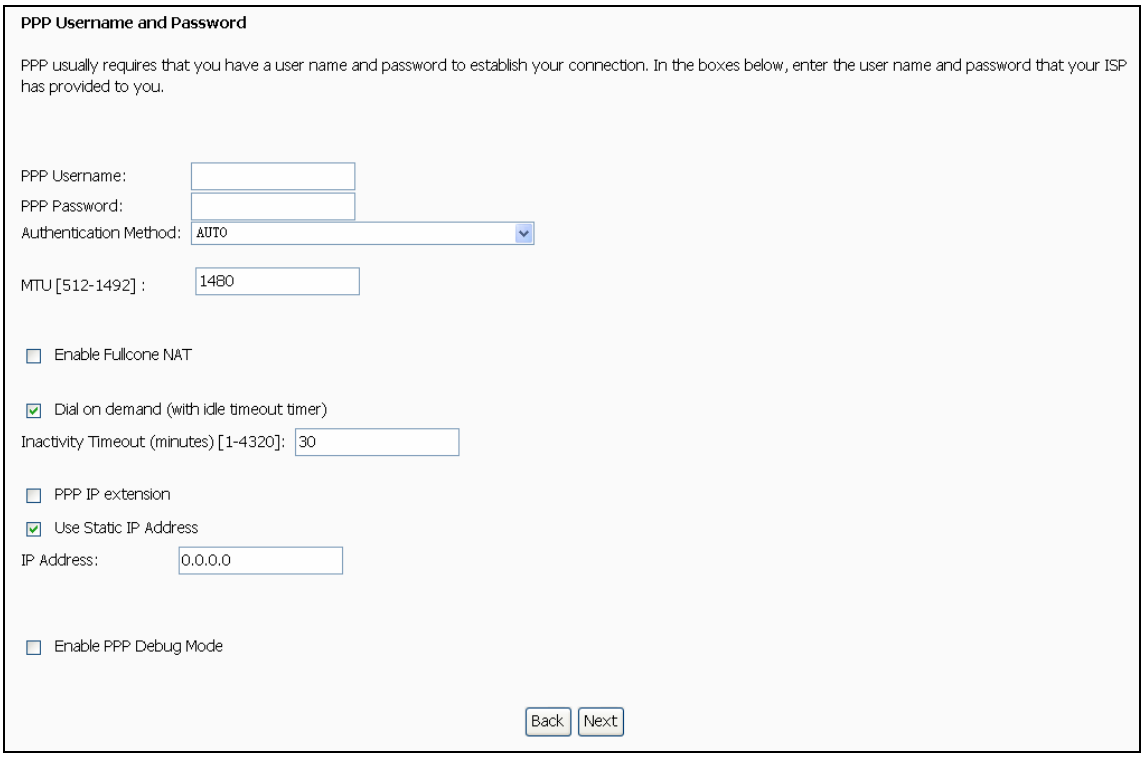


Figure 4-11

- PPP Username: Enter your username for your PPPoA connection to identify and verify your account to the ISP.
- PPP Password: Enter your password for your PPPoA connection.
- Authentication Method: Choose a method of authentication, AUTO, PAP, CHAP, or MSCHAP.
- MTU: The default MTU value is 1480 Bytes. It is not recommended that you change the default value unless required by your ISP. The value should be between 512 and 1492.
- Enable Fullcone NAT: Check this box to enable the Fullcone NAT function. The default value is disabled.
- Dial on demand: If you check this box, the Internet connection can be terminated automatically after a specified inactivity period (Inactivity Timeout) and be re-established when you attempt to access the Internet again. The default value of Inactivity Timeout is 15. The value should be between 1 and 4320.
- PPP IP extension: If this box is checked, the IP address obtained by the Router will be assigned to the computer, and the NAT and Firewall will be disabled.
- Use Static IP Address: Check this box to use the static IP address to dial. The default value is disabled.
- Enable PPP Debug Mode: Check this box to enable the debug mode. The default value is disabled.

Click Next button in Figure 4-11, and then you will see Figure 4-12. Check or uncheck the Enable WAN Service box according to your needs.

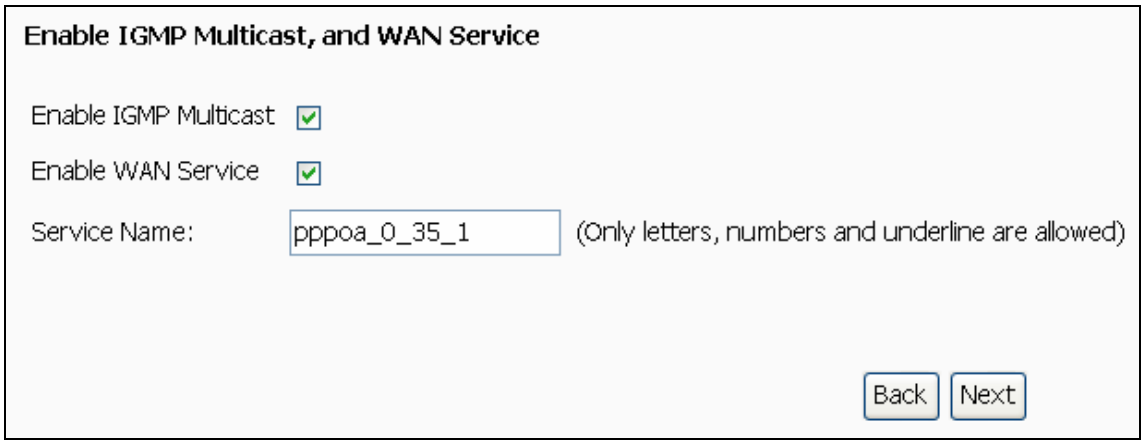


Figure 4-12

Click the Next button to enter the next step as shown in Figure 4-13. Click Save to complete the configuration.

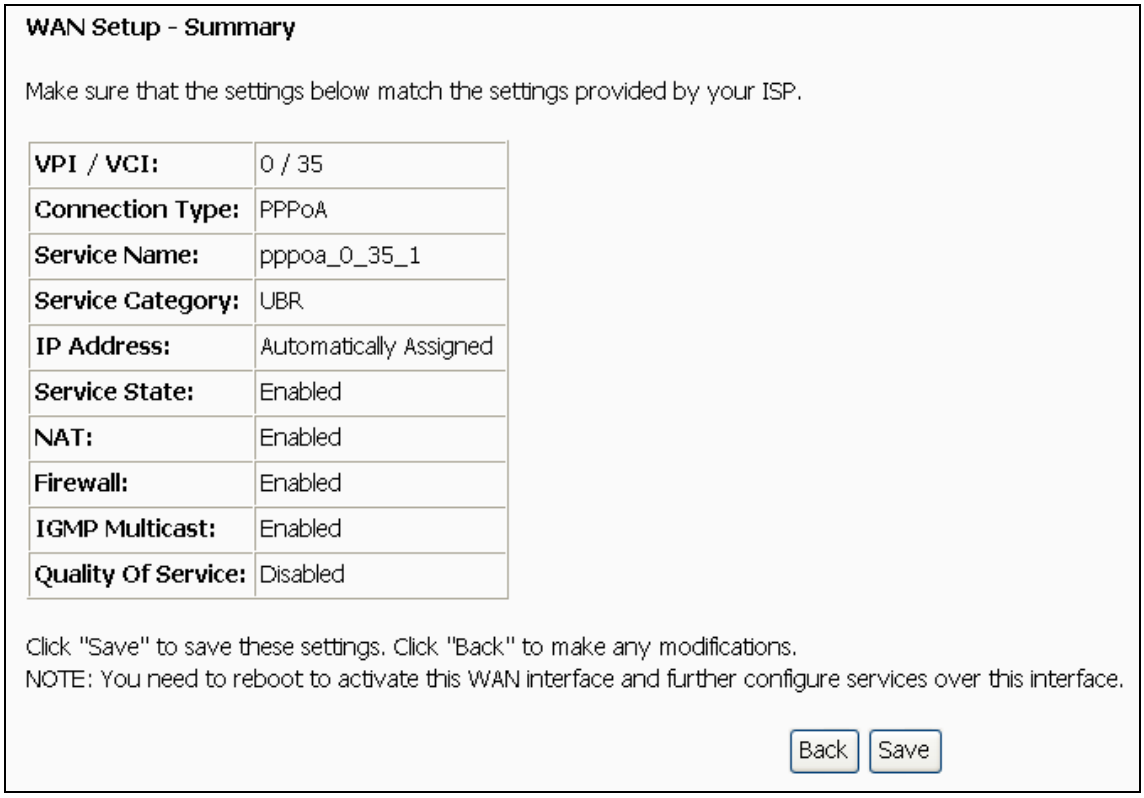


Figure 4-13

- PPP over Ethernet (PPPoE)

If you select the protocol of PPP over Ethernet (PPPoE), you will see the Figure 4-14.

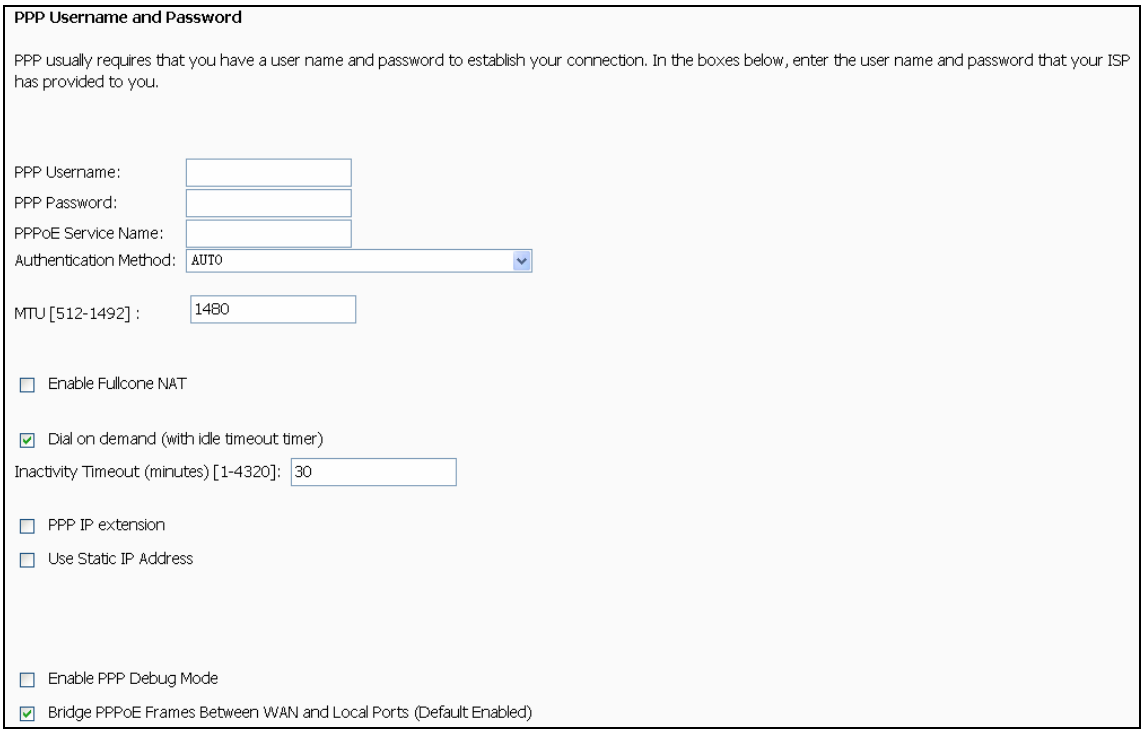


Figure 4-14

- PPP Username: Enter your username for your PPPoE connection to identify and verify your account to the ISP.
- PPP Password: Enter your password for your PPPoE connection.
- PPPoE Service Name: Enter a name for the PPPoE connection for recognition.
- Authentication Method: Choose a method of authentication, AUTO, PAP, CHAP, or MSCHAP.
- MTU: The default MTU value is 1480 Bytes. It is not recommended that you change the default value unless required by your ISP. The value should be between 512 and 1492.
- Enable Fullcone NAT: Check this box to enable the Fullcone NAT function. The default value is disabled.
- Dial on demand: If you check this box, the Internet connection can be terminated automatically after a specified inactivity period (Inactivity Timeout) and be re-established when you attempt to access the Internet again. The default value of Inactivity Timeout is 30. The value should be between 1 and 4320.
- PPP IP extension: If this box is checked, the IP address obtained by the Router will be assigned to the computer, and the NAT and Firewall will be disabled.
- Use Static IP Address: Check this box to use the static IP address to dial. The default value is disabled.
- Enable PPP Debug Mode: Check this box to enable the debug mode. The default value is disabled.
- Bridge PPPoE Frames Between WAN and Local Ports: If you check this box, you can establish dial-up connection in this Router or on the PC. By default, the checkbox is selected.

Click Next button in Figure 4-14, and then you will Figure 4-15. Check or uncheck the Enable WAN Service box according to your needs.

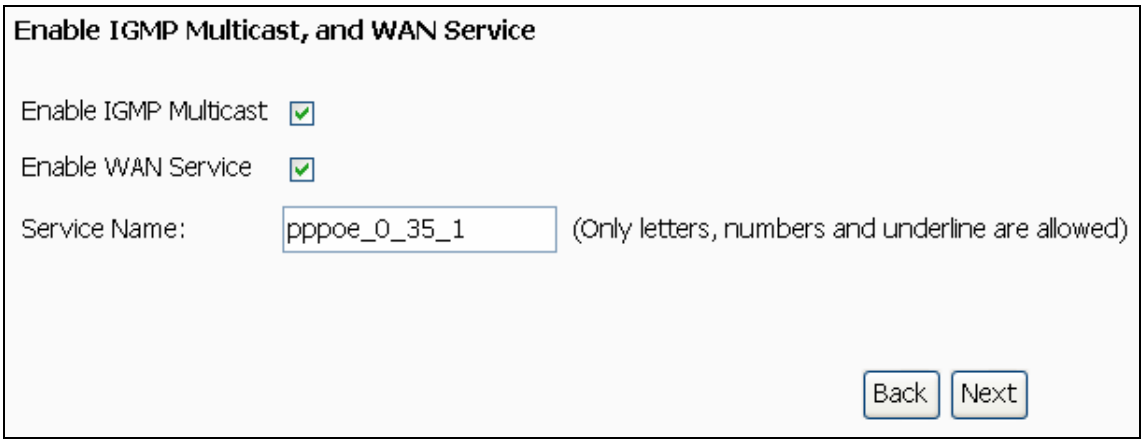


Figure 4-15

Click the Next button to enter the next step as shown in Figure 4-16. Click Save to complete the configuration.

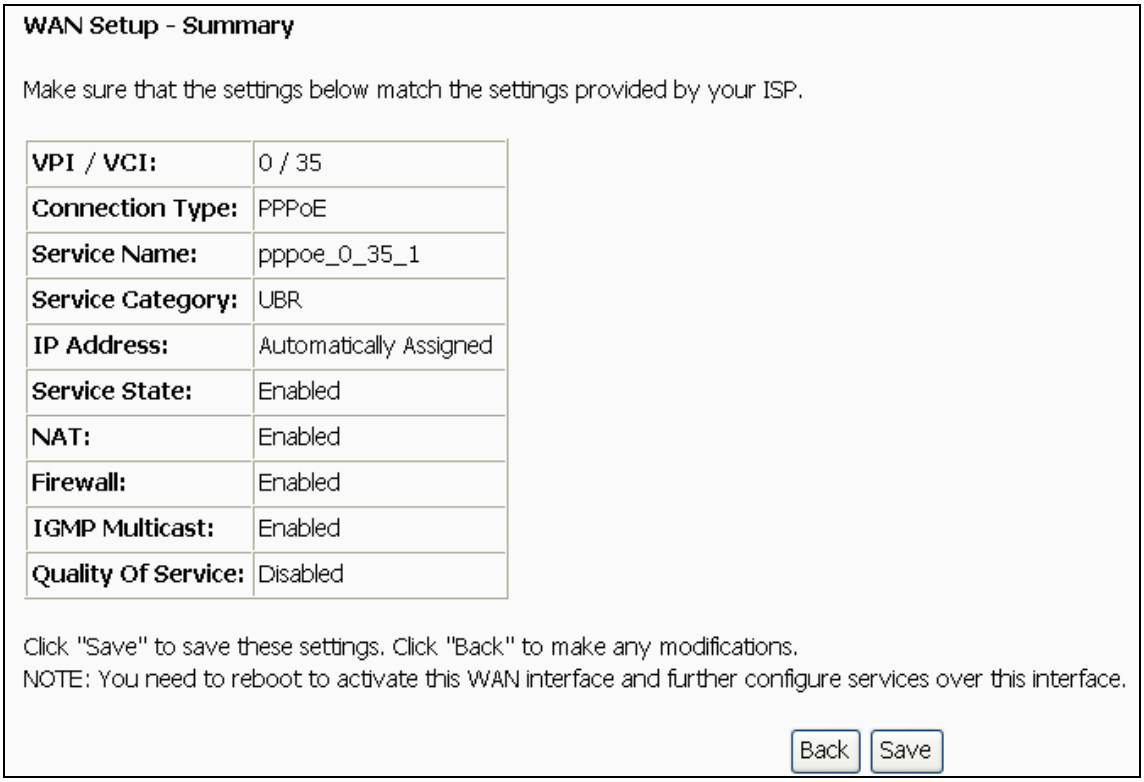


Figure 4-16

- MAC Encapsulation Routing (MER)

If you select the protocol of MAC Encapsulation Routing (MER), you will see the page as shown in Figure 4-17.

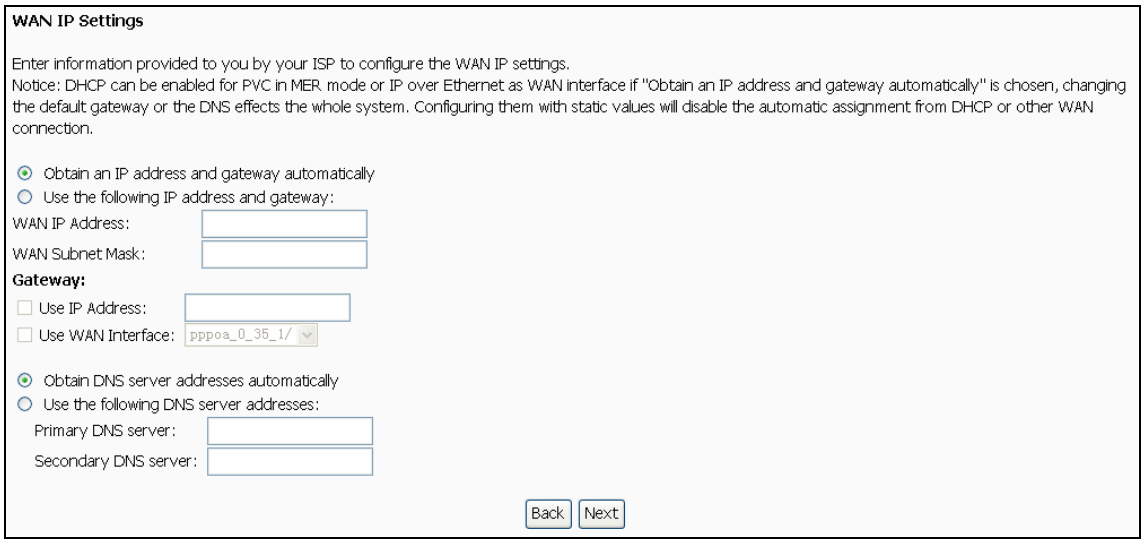


Figure 4-17

- Obtain an IP address automatically: This radio button is checked by default. You can obtain the IP address automatically.
- Use the following IP address and gateway: Check this radio button to enter the information provided by your ISP to configure the WAN IP settings.
- Obtain DNS server addresses automatically: This radio button is checked by default. It's recommended that you keep the default settings to allow the Router to obtain the default DNS server addresses automatically.
- Use the following DNS server addresses: Check this radio button then you can enter the primary DNS server and secondary DNS server. This is not recommended by default.

☞ **Note:**

1) DHCP can be enabled for PVC in MER mode as WAN interface if "Obtain an IP address automatically" is chosen.
2) Changing the default gateway or the DNS will affect the whole system. Configuring them with static values will disable the automatic assignment from DHCP or other WAN connection.
3) If you configure static default gateway over this PVC in MER mode, you must enter the IP address of the remote gateway in the "Use IP address". The "Use WAN interface" is optional.

Click Next button in Figure 4-17, and then you will see the Figure 4-18. Check or uncheck the Enable WAN Service box according to your needs.

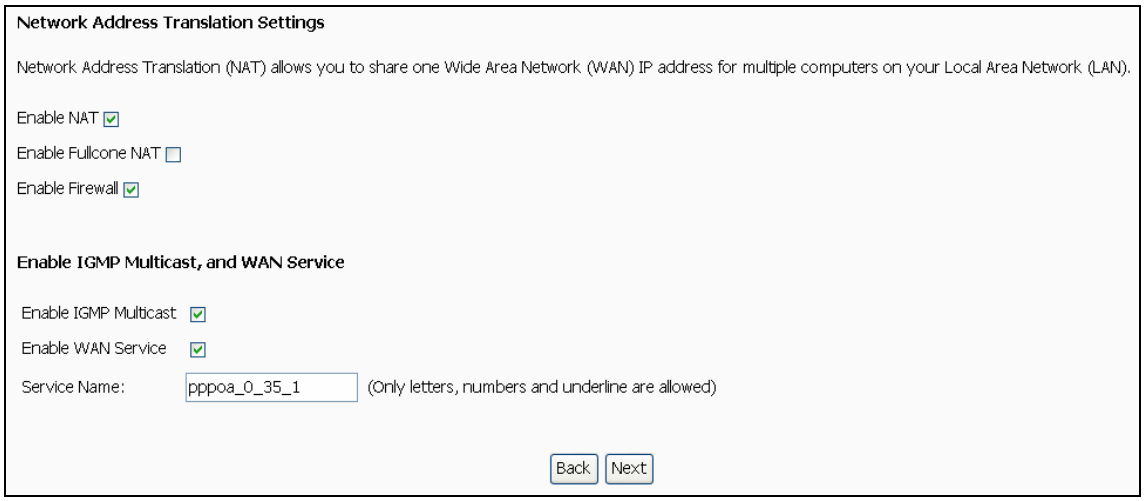


Figure 4-18

Click the Next button to enter the next step as shown in Figure 4-19. Click Save to complete the configuration.

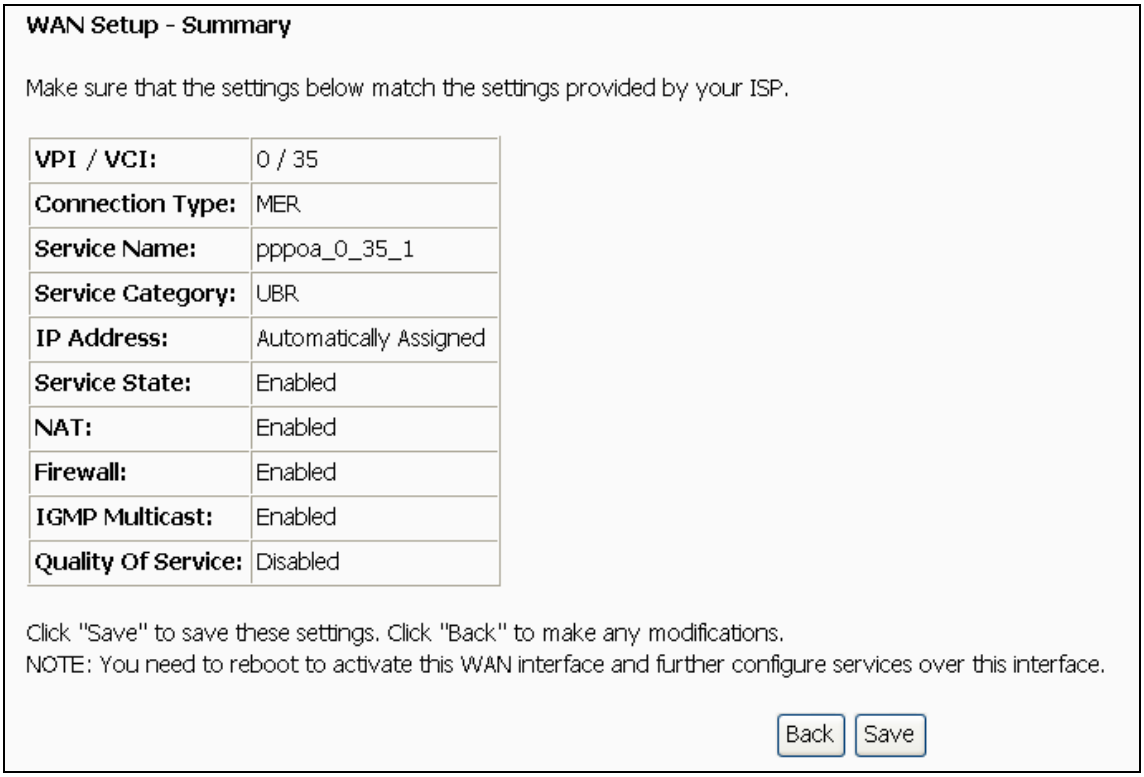


Figure 4-19

- IP over ATM (IPoA)

If you select the protocol of IP over ATM (IPoA), you will see the Figure 4-20. Enter the parameters provided by your ISP.

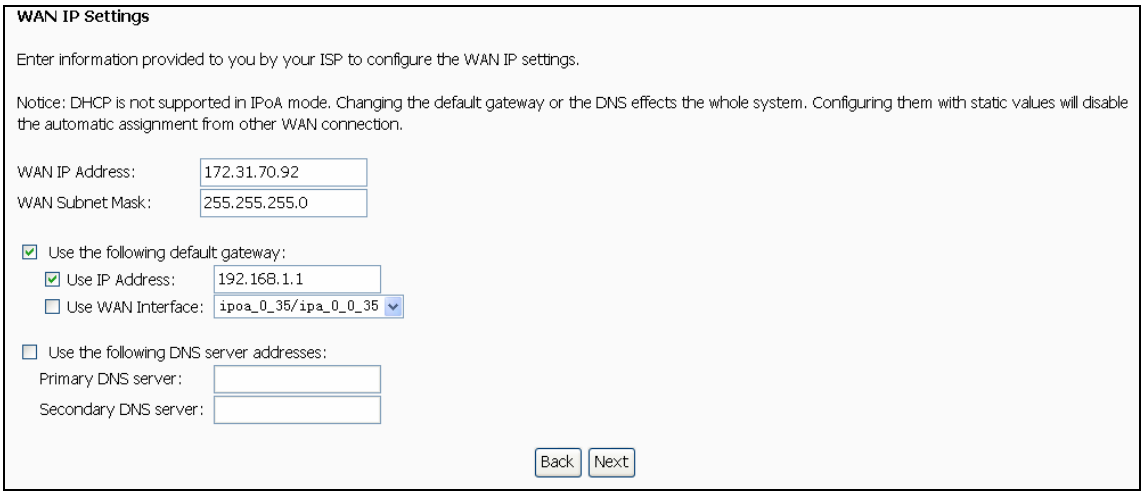


Figure 4-20

- WAN IP Address: Enter the IP Address provided by your ISP.
- WAN Subnet Mask: Enter the subnet mask provide by your ISP.
- Use the following default gateway: Check this radio button then you can choose Use IP Address or Use WAN Interface. If you have any problems, please ask your ISP for the information.
- Use the following DNS server addresses: Check this radio button then you can enter the primary DNS server and secondary DNS server. If you have any problems, please ask your ISP for the information.

Note:

1) DHCP is not supported in IPoA mode.
2) Changing the default gateway or the DNS will affect the whole system. Configuring them with static values will disable the automatic assignment from other WAN connection.

Click Next in Figure 4-20, and then you will see the Figure 4-21.

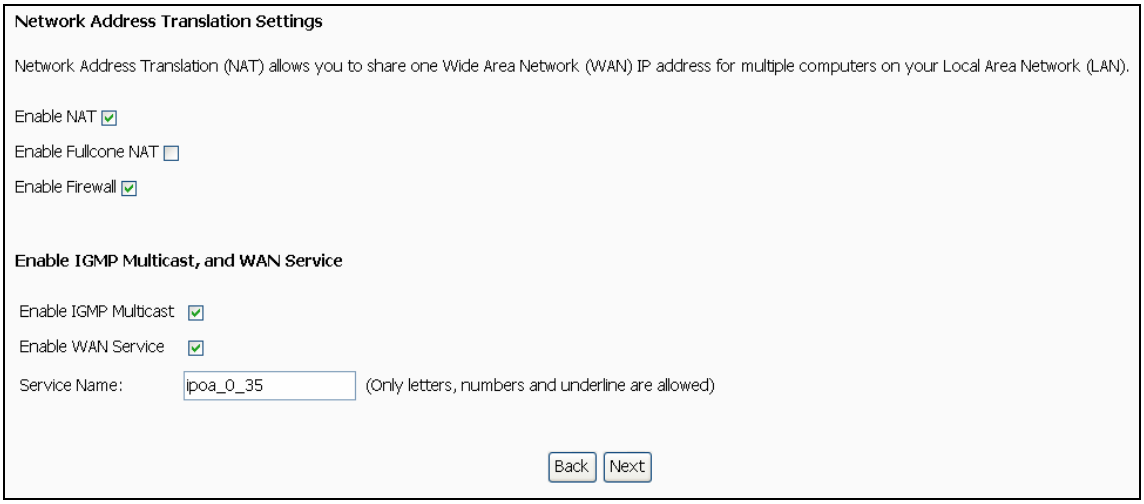


Figure 4-21

Check or uncheck the Enable WAN Service box according to your needs. Click the Next button to enter the next step as shown in Figure 4-22, and click Save to complete the configuration.

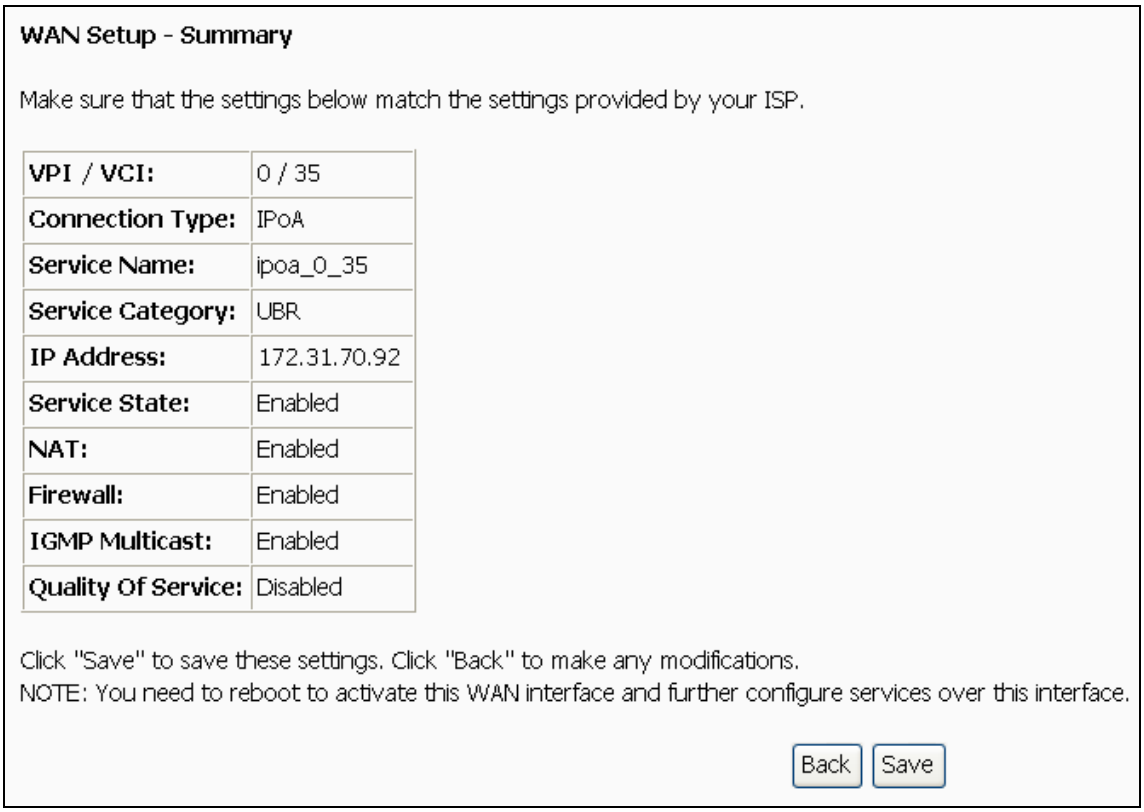


Figure 4-22

- Bridging

If you select the Bridging protocol, you will see the Figure 4-23. Click the Next button.

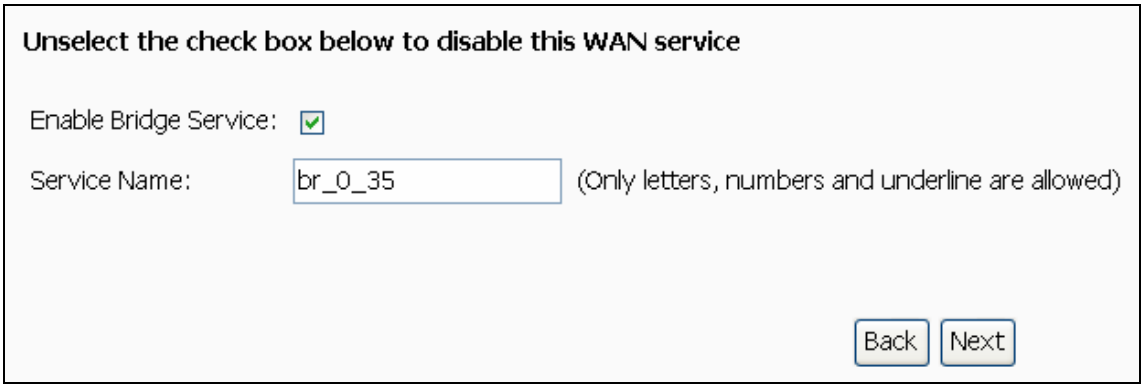


Figure 4-23

Then you will see the Figure 4-24. Click Save to complete the configuration

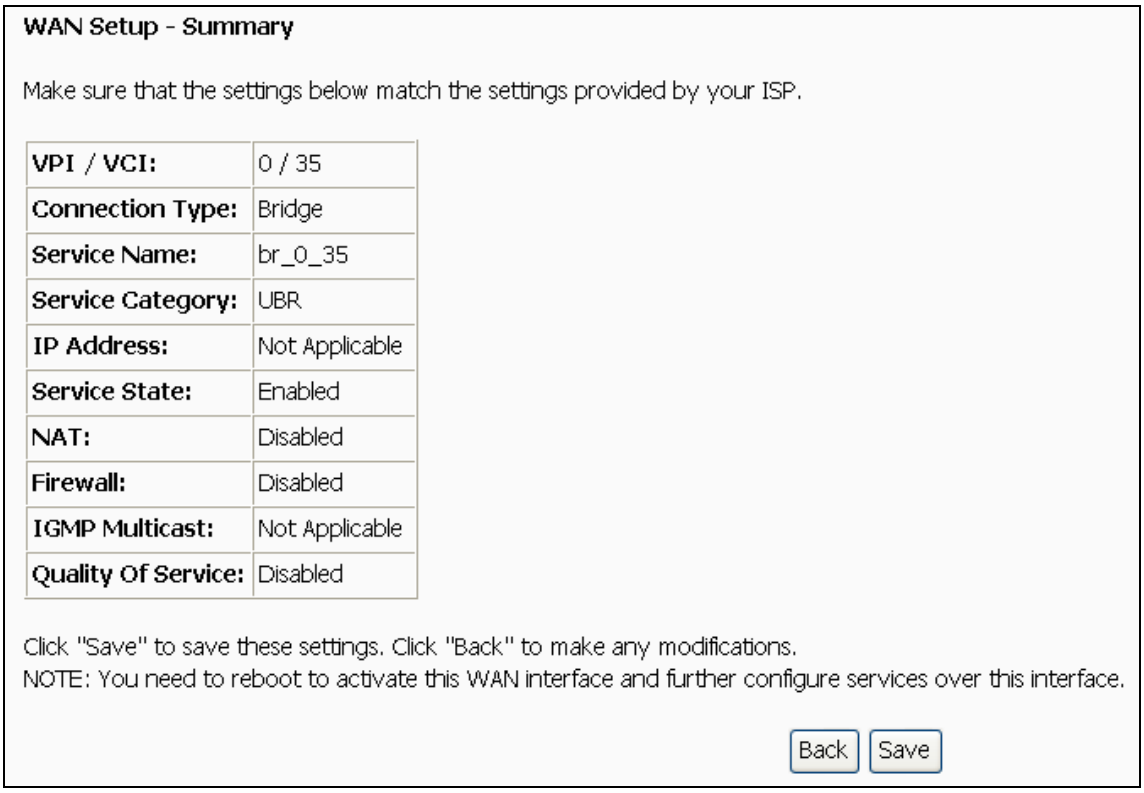


Figure 4-24

Note:

After completing any setup, the new setup must be saved and the Router must be restarted for the configuration to go into effect. Please click the Save/Reboot button to restart as shown in Figure 4-25.

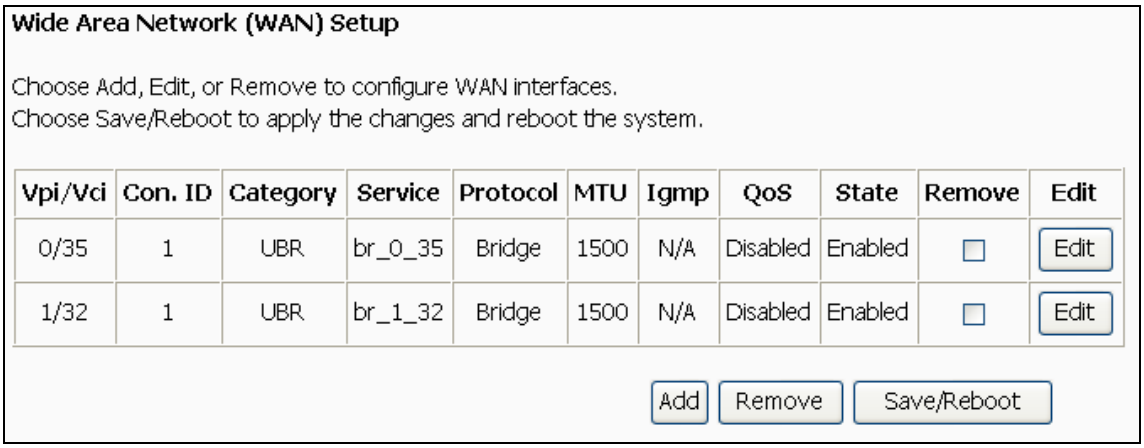


Figure 4-25

Note:

All of the above setup is under windows XP OS.

4.5.2 LAN

Choose “Advanced Setup→LAN” menu, and you can see and configure the Local Area Network (LAN) parameters in the screen as shown in Figure 4-26.

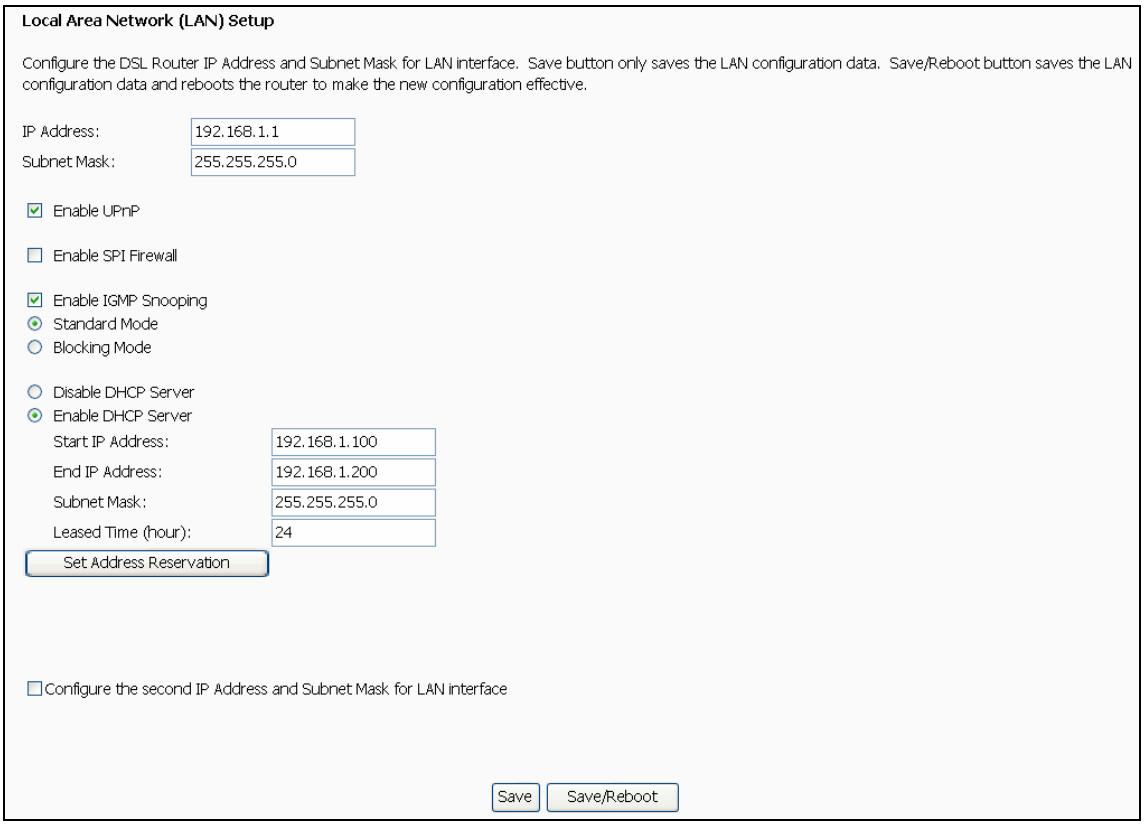


Figure 4-26

- IP Address - Enter an IP address for the Router. Then you can access the Web-based Utility via this IP address. The default setting is 192.168.1.1.
- Subnet Mask - An address code that determines the size of the network. Normally use 255.255.255.0 as the subnet mask.

Note:

1) If you change the IP Address of LAN, you must use the new IP Address to log in the Router.
2) If the new LAN IP Address you set is not in the same subnet, the IP Address pool of the DHCP server will change accordingly at the same time，while the Virtual Server and DMZ Host will not take effect until they are re-configured.

- Enable SPI Firewall: Check this box to enable the SPI Firewall function. The default value is disabled.
- Enable IGMP Snooping: By default this option is enabled. With this function enabled, the Router can listen to the IGMP messages transmitted from the LAN to the WAN, and track the IGMP messages and the registered port.
- Disable/Enable DHCP Server - Disable or Enable the DHCP server. DHCP stands for Dynamic Host Configuration Protocol. The DHCP Server will automatically assign dynamic IP addresses to the computers on the network. If you disable the Server, you must have another DHCP server within your network or else you must configure the computer manually. The following options are available only when DHCP Server is enabled.
  - Start IP Address - Specify an IP address for the DHCP Server to start with when assigning IP addresses. 192.168.1.100 is the default start address

- End IP Address - Specify an IP address for the DHCP Server to end with when assigning IP addresses. 192.168.1.200 is the default end address.
- Sunet Mask: An address code that determines the size of the network. Normally use 255.255.255.0 as the subnet mask.
- Leased Time (hour) - The Lease Time is the amount of time a network user will be allowed connection to the Router with their current dynamic IP address. Enter the amount of time, in hours, and the user will be "leased" this dynamic IP address. After the time is up, the user will be automatically assigned a new dynamic IP address. The default value is 24 hours.

➢ Set Address Reservation - Click this button, you can view and add a reserved address for clients via the Address Reservation page as shown in Figure 4-26. When you specify a reserved IP address for a PC on the LAN, that PC will always receive the same IP address each time when it accesses the DHCP server. Reserved IP addresses should be assigned to servers that require permanent IP settings.

➢ Configure the second IP Address and Subnet Mask for LAN interface - Check this box, and you can configure a second IP address and subnet mask for the LAN interface.

➢ Save - Clicking this button only saves the LAN configuration data.

➢ Save/Reboot - Clicking this button not only saves the LAN configuration data but also reboots the Router to make the new configuration take effect.

To Reserve an IP address：

1. Click the Set Address Reservation button shown in Figure 4-26 to enter the screen as shown in Figure 4-27.

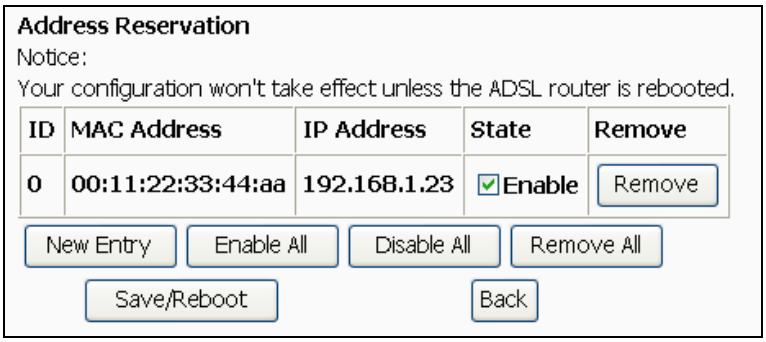


Figure 4-27

2. Click the New Entry button in Figure 4-27. Then Figure 4-28 will pop up.

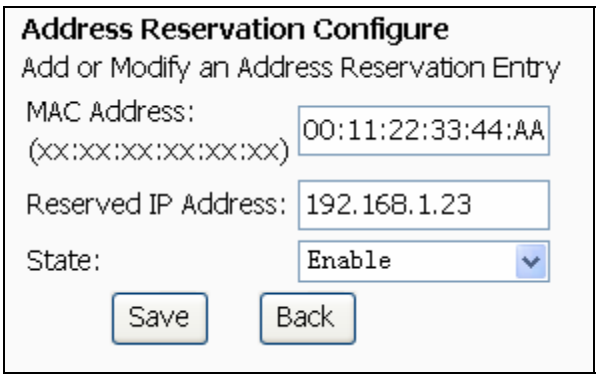


Figure 4-28

3. Enter the MAC address in XX:XX:XX:XX:XX:XX format and reserved IP address in dotted-decimal notation of the computer for which you want to reserve an IP address.

   Note:

   The MAC Address and IP Address added in Figure 4-28 are used for illustrating. They may be different to your circs.

4. Select Enable from the State drop-down list.
5. Click the Save button, then you will go back to the Address Reservation screen and see the new entry as shown in Figure 4-27.
6. Click Save/Reboot button to save the settings and reboot the Router.

Note:

The function won't take effect until the router reboots.

4.5.3 MAC Clone

Choose “Advanced Setup→MAC Clone” menu, you can configure the MAC address of the WAN on the screen below..

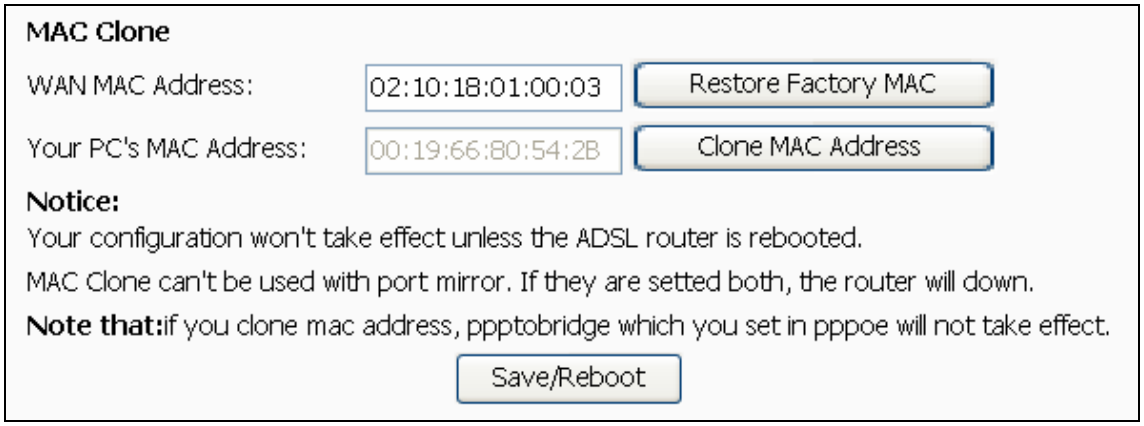


Figure 4-29

Some ISPs require that you register the MAC Address of your adapter. Changes are rarely needed here.

- WAN MAC Address - This field displays the current MAC address of the WAN port. If your ISP requires you to register the MAC address, please enter the correct MAC address into this field in XX:XX:XX:XX:XX:XX format (X is any hexadecimal digit).
- Your PC's MAC Address - This field displays the MAC address of the PC that is managing the Router. If the MAC address is required, you can click the Clone MAC Address button and this MAC address will be filled in the WAN MAC Address field.

Click Restore Factory MAC to restore the MAC address of WAN port to the factory default value.

Click the Save/Reboot button to save your settings.

Note:

1) Only the PC on your LAN can use the MAC Address Clone function.
2) Your configuration won't take effect unless the ADSL Router is rebooted.
3) MAC Clone can't be used with port mirror. If they are set both, the Router will be down.

4.5.4 NAT

NAT (Network Address Translation) allows you to share one WAN (Wide Area Network) IP address for multiple computers on your LAN (Local Area Network).

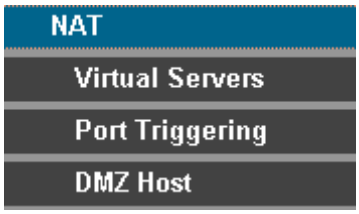


Figure 4-30

Note:

When you select PPPoA or PPPoE for the WAN Setup, or when you select Enable NAT for the type of IPoA and IPoE connection, you will see the NAT menu in the Web-based Utility (shown in Figure 4-31).

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

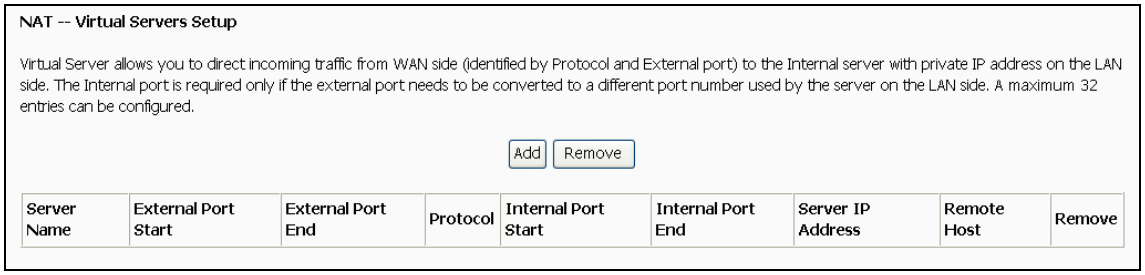


Figure 4-31

4.5.4.1 Virtual Servers

Choose “Advanced Setup→NAT→Virtual Servers”, you can set up virtual servers on the screen below (shown in Figure 4-32).

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.

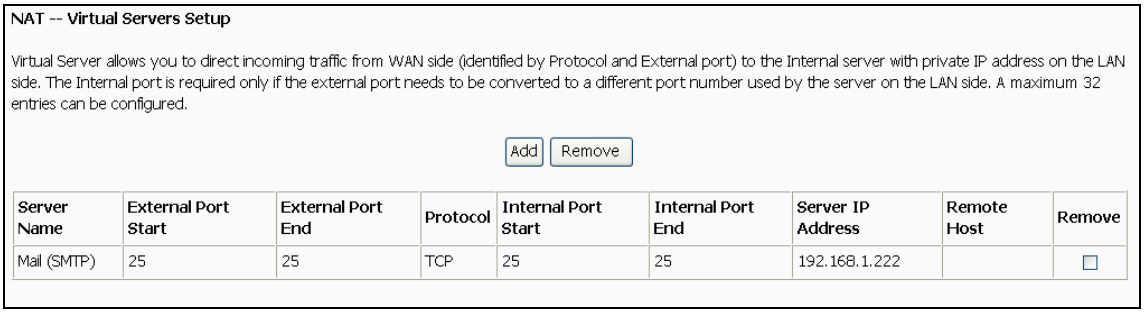


Figure 4-32

- 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.
  - Remote Host: The PC can enjoy the service application.
- Add: Click the Add button to add a new entry.
- Remove: Select the check box in the table (shown in Figure 4-32) and then click the Remove button, then the corresponding entry will be deleted in the table.

To add a virtual server entry:

1. Click the Add button on the preceding screen Figure 4-32, and then you will see the new Virtual Server in the next screen as shown in Figure 4-33.

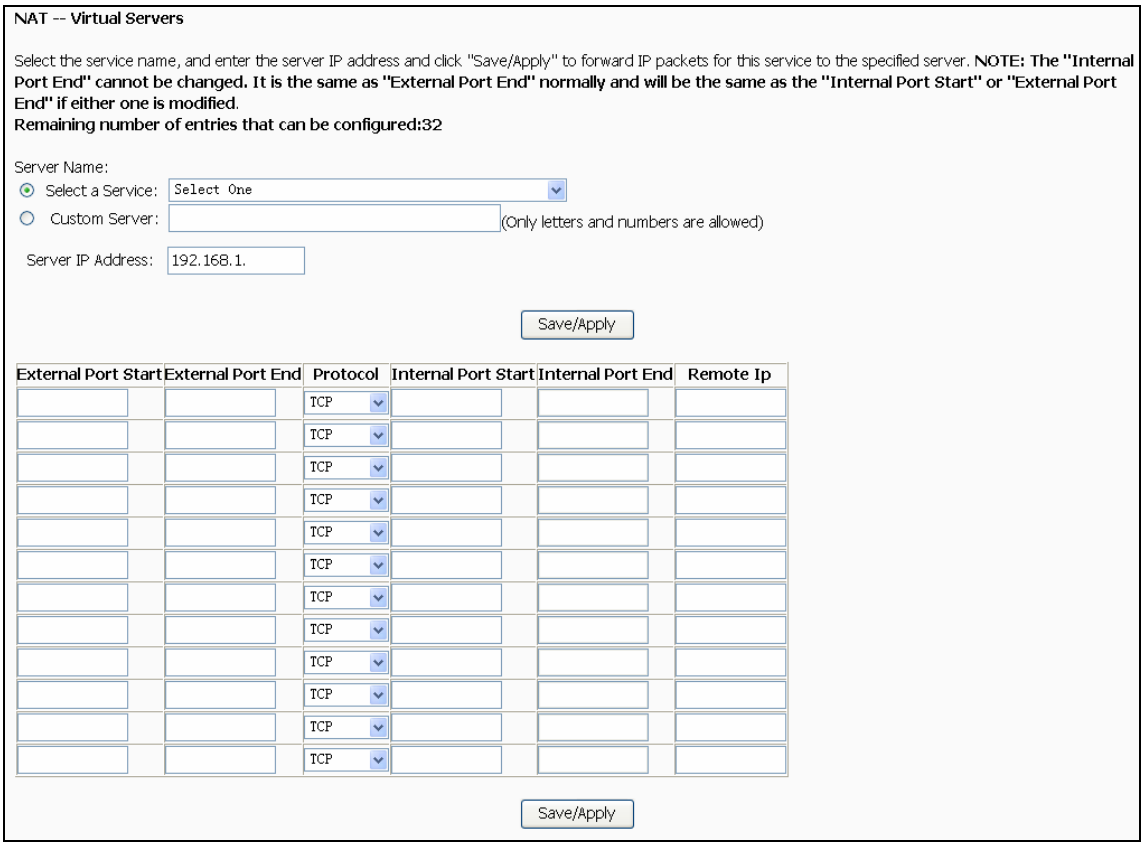


Figure 4-33

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 Save/Apply to enable virtual server and then you will see your setting as shown in Figure 4-32.

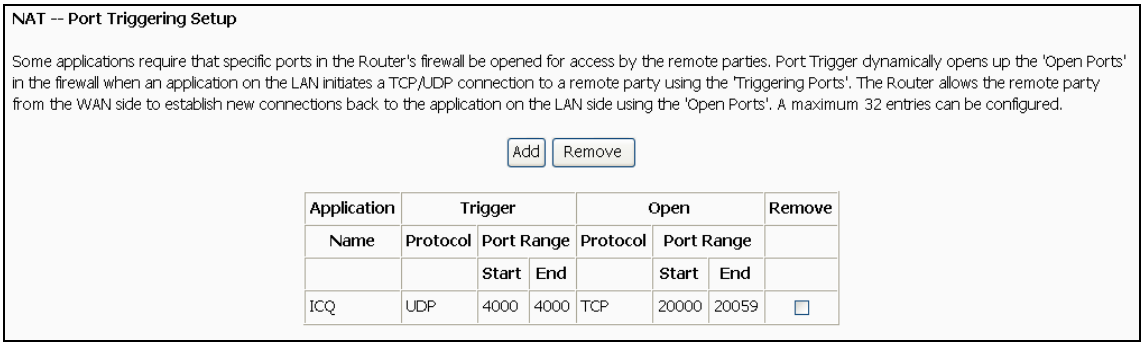
Note:

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.

4.5.4.2 Port Triggering

Choose “Advanced Setup→NAT→Port Triggering”, you can set Port Triggering on the screen (shown in Figure 4-34).

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.


NAT -- Port Triggering Setup

Some applications require that specific ports in the Router's firewall be opened for access by the remote parties. 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 party 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.

Add Remove

Application	Trigger			Open			Remove
Name	Protocol	Port Range		Protocol	Port Range		
		Start	End		Start	End	
ICQ	UDP	4000	4000	TCP	20000	20059	☐

Figure 4-34

- 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 4-34) 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 in Figure 4-34, and then you will see the new Port Triggering in the next screen as shown in Figure 4-35.

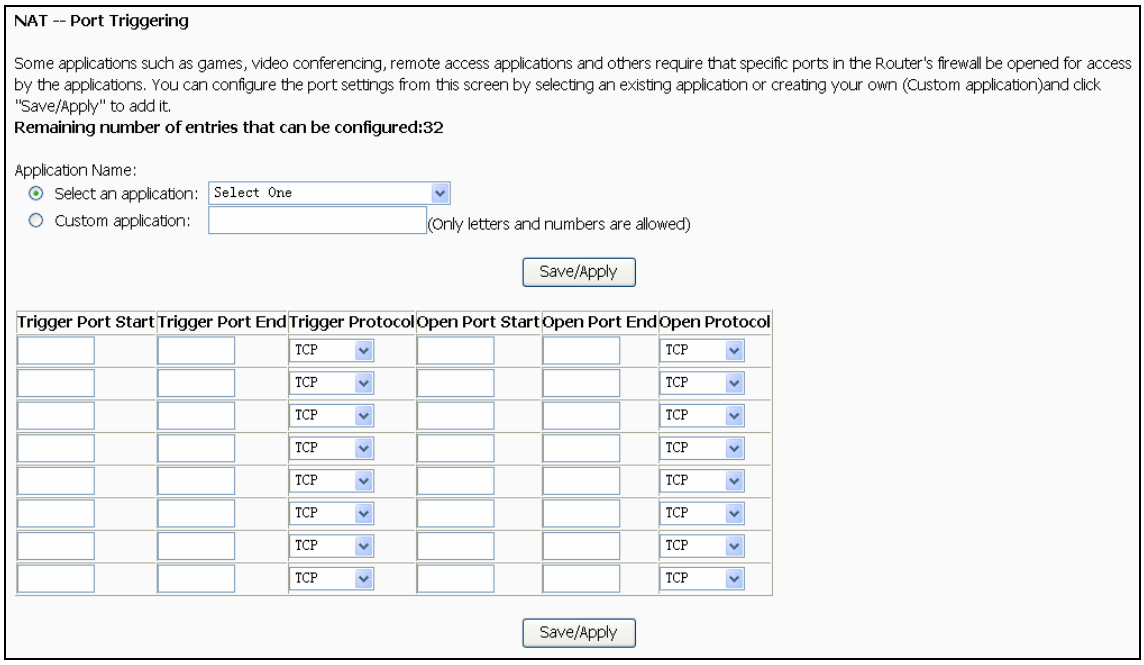


Figure 4-35

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 Save/Apply to enable the settings and then you will see you settings as shown in Figure 4-34.

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.

4.5.4.3 DMZ Host

Choose “Advanced Setup→NAT→DMZ Host”, you can set up DMZ Host on the screen (shown in Figure 4-36).

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.

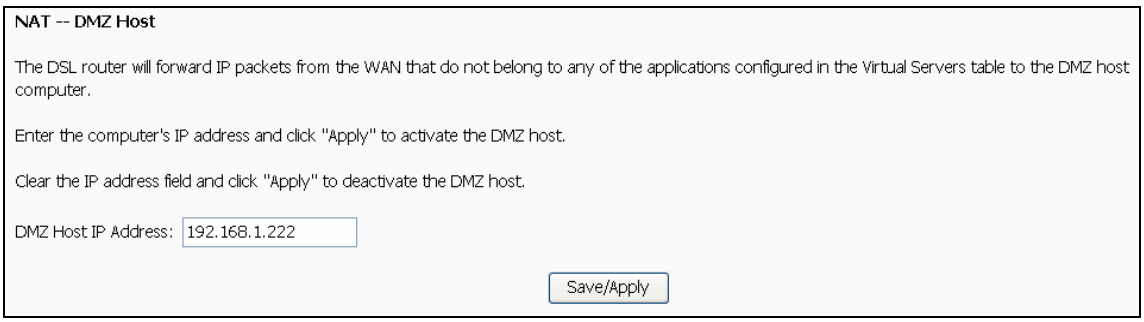


Figure 4-36

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.

4.5.5 Security

Choose “Advanced Setup→Security” menu, you can do some security configurations for your Router. There are two submenus under the Security menu as shown in Figure 4-37.

Figure 4-37

When you select the connection type PPPoE, PPPoA or IPoA for WAN configuration, you will see the more submenus in the Web-based Utility shown as Figure 4-38.

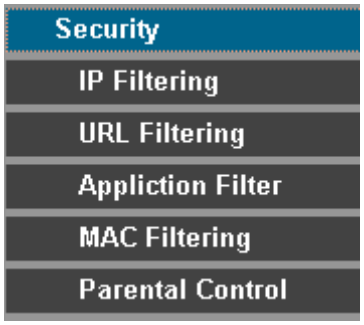


Figure 4-38

4.5.5.1 MAC Filtering

Choose “Security→MAC Filtering” menu, you can configure the MAC filtering rule in the next screen similar to Figure 4-39. The MAC Address Filtering feature allows you to control the access of users on your local network basing on their MAC addresses.

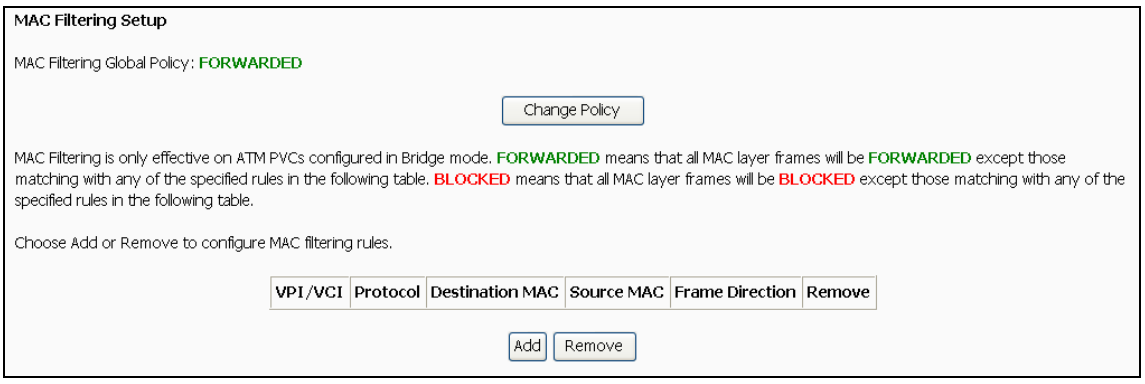


Figure 4-39

MAC Filtering Global Policy - The default setting is FORWARDED.

- FORWARDED means that all MAC layer frames will be forwarded except those matching with any of the specified rules in the following table.
- BLOCKED means that all MAC layer frames will be blocked except those matching with any of the specified rules in the following table.

You can change the policy by clicking the Change Policy button to go to the Change MAC Filtering Global Policy page as shown in Figure 4-40.

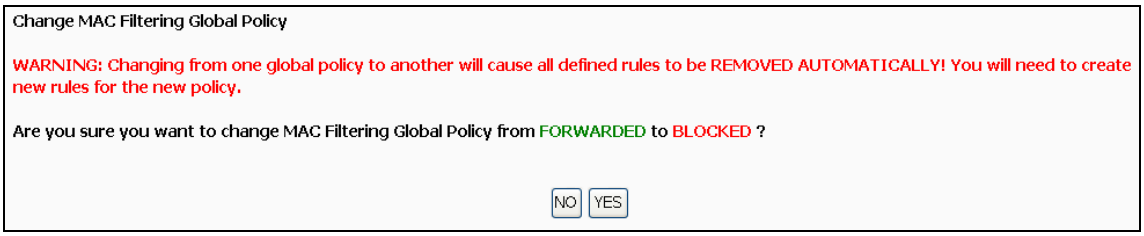


Figure 4-40

To add a new entry, follow the steps below.

1. Click the Add button in Figure 4-39 to go to the Add MAC Filter page as shown in Figure 4-41.
2. Select the protocol type.
3. Enter the destination MAC address.
4. Enter the source MAC address.
5. Select the frame direction.
6. Select the WAN interfaces.
7. Click Save/Apply to save your settings.

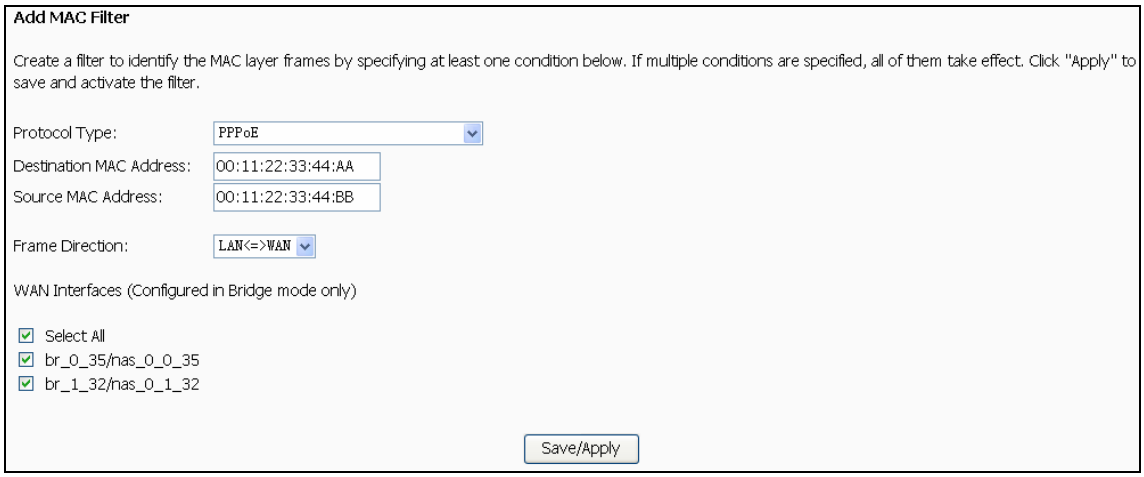


Figure 4-41

To remove an existing entry, follow the steps below.

1. Check the Remove box as shown in Figure 4-39 in the entry you want to remove.
2. Click the Remove button.

4.5.5.2 IP Filtering

There are two submenus under IP Filtering.

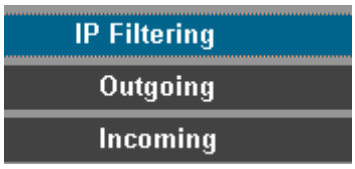


Figure 4-42

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 4-43).

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.

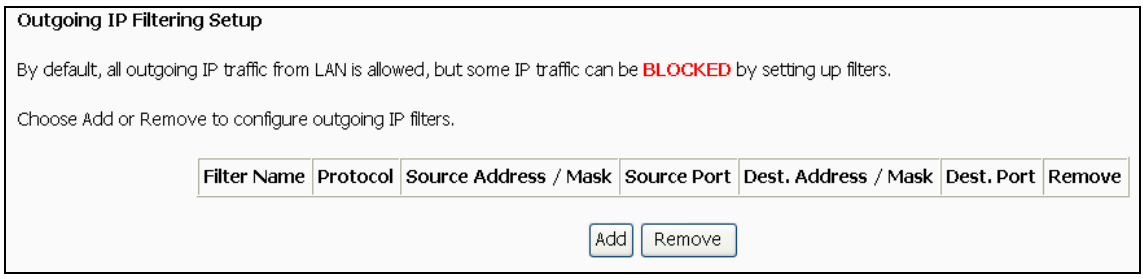


Figure 4-43

Setup an Outgoing IP Filtering rule:

1. Click the Add button in Figure 4-43, and you will see the next screen as shown in Figure 4-44.

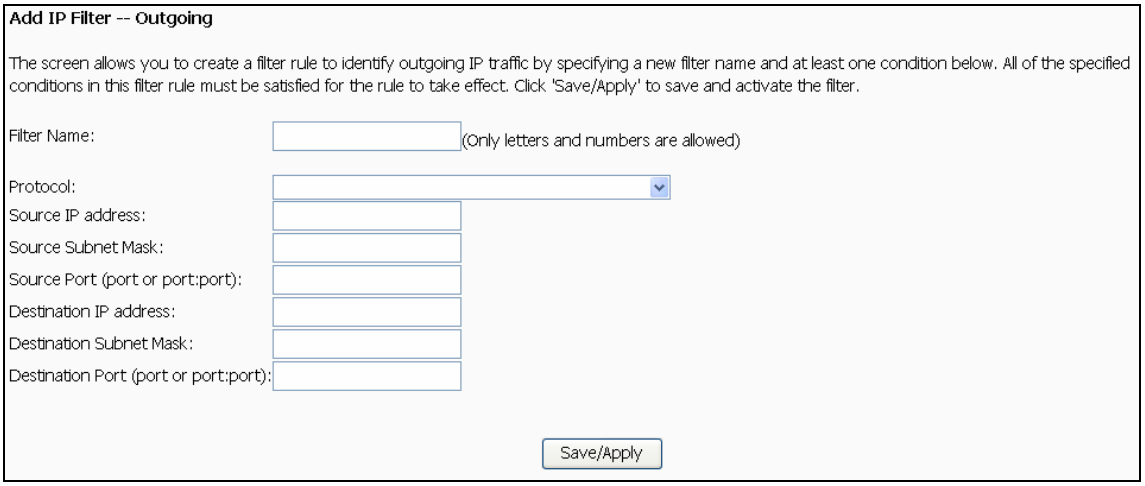


Figure 4-44

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 Save/Apply to save this entry.

☞ **Note:**

When you add an Outgoing IP Filtering entry, you must configure at least one condition on the preceding screen 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 as shown in Figure 4-45.

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.

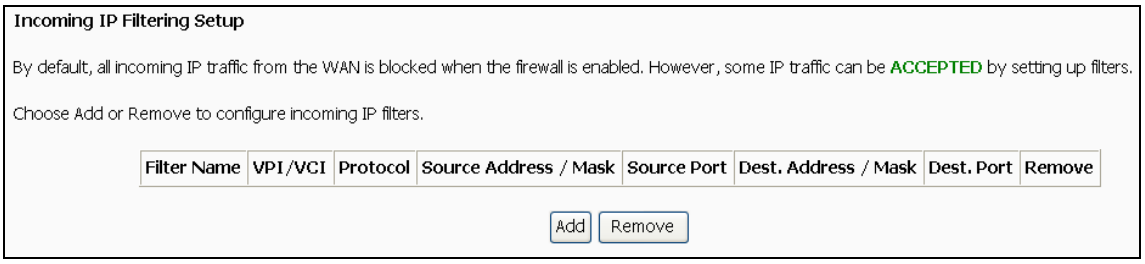


Figure 4-45

Setup an Incoming IP Filtering rule:

1. Click the Add button in Figure 4-45, and then you will see Figure 4-46.

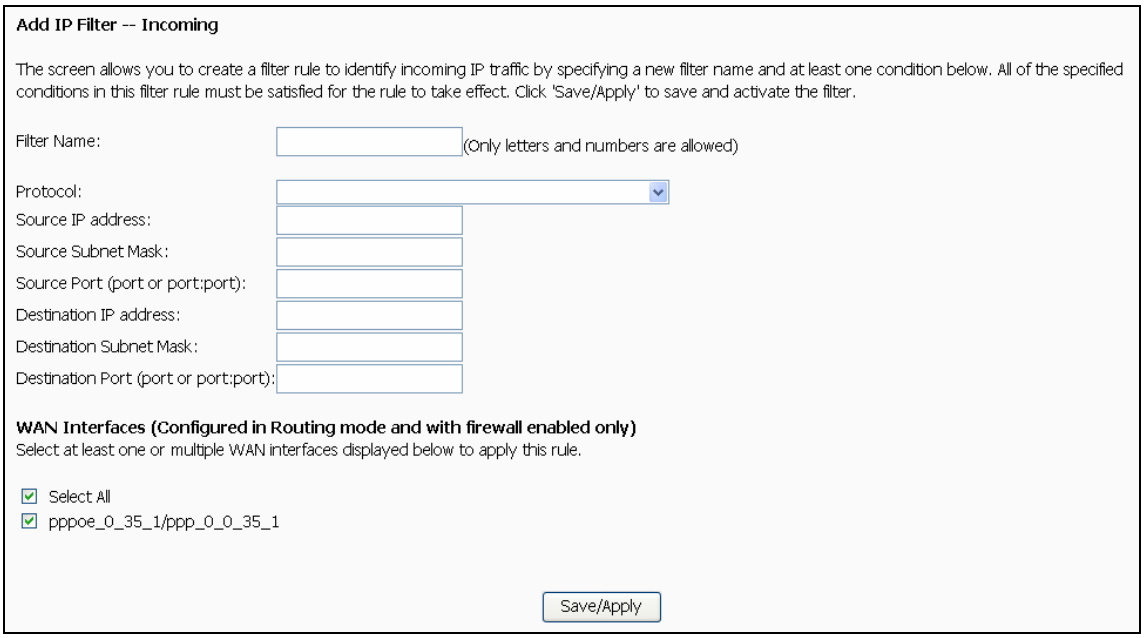


Figure 4-46

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 Save/Apply to save this entry.

Note:

When you add an Incoming IP Filtering entry, you must configure at least one condition on the preceding screen 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.

4.5.5.3 URL Filtering

This section allows you to configure the filter rules based on URL to control the computers in the LAN to access the specified port.

Figure 4-47

URL Filtering Global Policy - The default setting is FORWARDED.

- FORWARDED means that all MAC layer frames will be forwarded except those matching with any of the specified rules in the following table.
- BLOCKED means that all MAC layer frames will be blocked except those matching with any of the specified rules in the following table.

You can change the policy by clicking the Change Policy button to go to the Change MAC Filtering Global Policy page as shown in Figure 4-48.

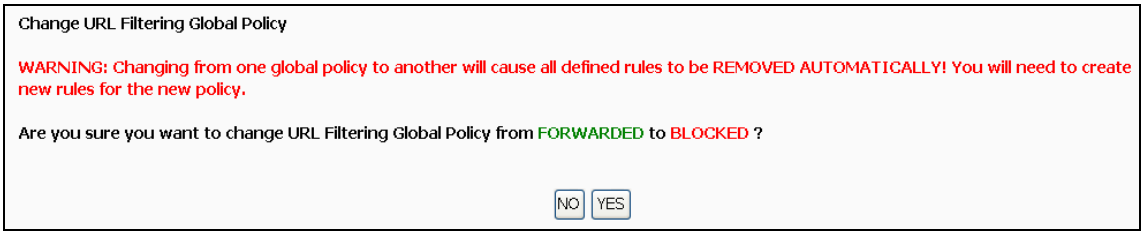


Figure 4-48

To add a new entry, follow the steps below.

1. Click the Add button in Figure 4-47 to go to the Add MAC Filter page as shown in Figure 4-49.
2. Enter the start IP address.
3. Enter the end IP address.
4. Enter the desire URL address.
5. Click Save/Apply to save your settings.

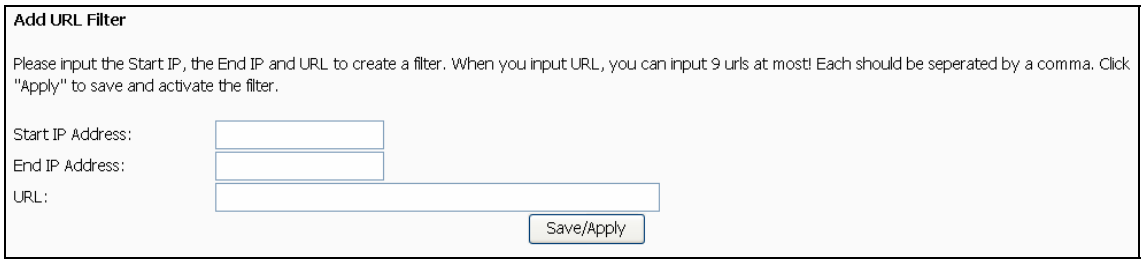


Figure 4-49

To remove an existing entry, follow the steps below.

1. Check the Remove box as shown in Figure 4-47 in the entry you want to remove.
2. Click the Remove button.

4.5.5.4 Application Filter

Choose “Security→Application Filtering” menu, you can select the desired application to filter.

Figure 4-50

Select the desired application and click Save/Apply to make the setting effective.

4.5.5.5 Parental Control

Choose “Security→Parental Control” menu, you can configure the parental control rule in the screen as shown in Figure 4-51. The Parental Control function can be used to restrict the time of Internet surfing for the child.

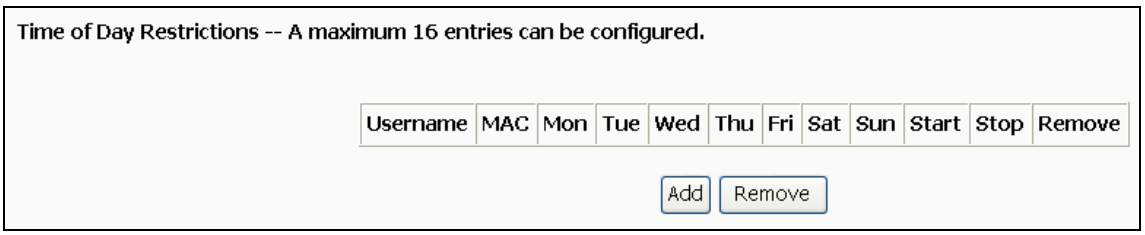


Figure 4-51

For example: If you don’t want your child_1 to surf the Internet from 18:00 to 20:00 on weekdays. You can follow the steps below.

1. Click the Add button in Figure 4-51 to go to the Time of Day Restriction page as shown in Figure 4-52.
2. Create a User Name for your child, for example child_1.
3. If you want to restrict the Browser’s surfing time, check the Browser’s MAC Address radio button. If you want to restrict other user’s surfing time, check the Other MAC Address radio button and enter the MAC address of the user’s computer, for example 00:11:22:33:44:CC.
4. Select the day or days you need.
5. Enter the Start Blocking Time and End Blocking Time both in hh:mm format.
6. Click Save/Apply button. Then you will go back to the Time of Day Restrictions page and see the list as shown in Figure 4-51.

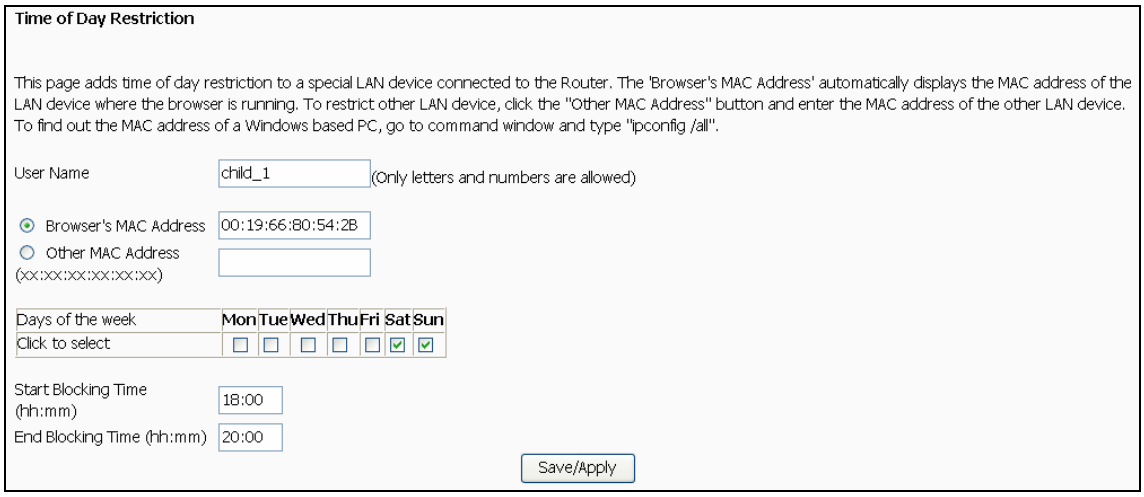


Figure 4-52

To remove an existing entry, follow the steps below.

1. Check the box in the Remove column of the entry as shown in Figure 4-51.
2. Click the Remove button below.

4.5.6 Quality of Service

Choose “Advanced Setup→Quality of Service”, you can enable QoS (Quality of Service) on the screen shown in Figure 4-53. QoS helps to prioritize data as it enters your router. By attaching special identification marks or headers to incoming packets, QoS determines which queue the packets enter, based priority. This is useful when there are certain types of data you want to give higher priority, such as voice data packets give higher priority than Web data packets. This option will provide better service of selected network traffic over various technologies.

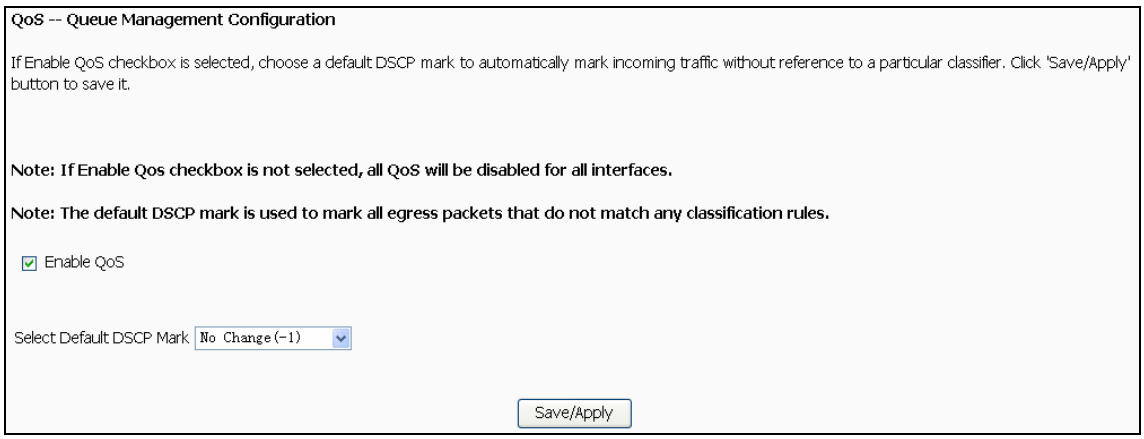


Figure 4-53

Select the Enable QoS checkbox to enable all QoS for all interfaces.

Select a Default DSCP Mark from drop-down list to automatically mark incoming traffic without reference to a particular classifier.

Click Save/Apply to save the current configuration.

☞ **Note:**

The default DSCP mark is used to mark all egress packets that do not match any classification rules.

4.5.6.1 Queue Config

Choose “Advanced Setup→Quality of Service→Queue Config”, you can set configure QoS queues on the screen below.

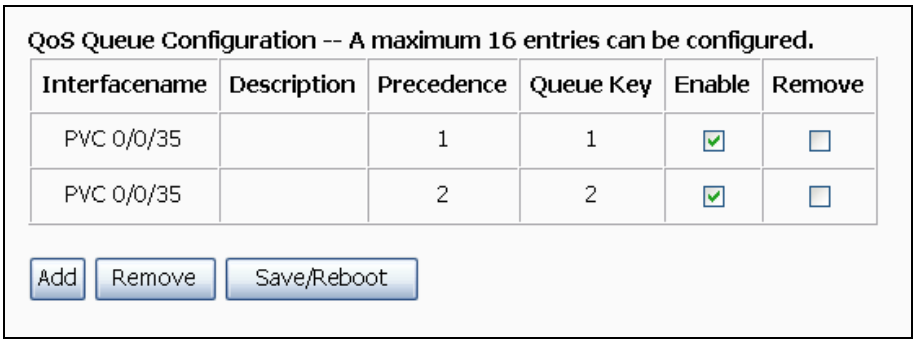


Figure 4-54

Click the Add button in Figure 4-54, and you can configure the QoS queue entry on the next screen as shown in Figure 4-55.

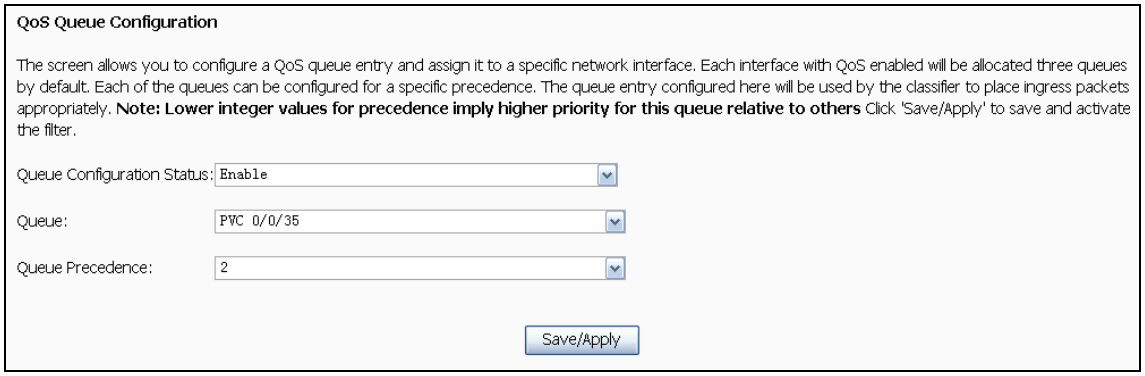


Figure 4-55

- Queue Configuration Status: Enable or disable the queue configuration.
- Queue: Select a QoS queue entry from the drop-down list.
- Queue Precedence: Specify precedence for this QoS queue entry.

After you specify the condition, click Save/Apply to save the entry and then you will see you settings as shown in Figure 4-54.

Note:

1) Lower integer values for precedence imply higher priority for this queue relative to others.
2) The queue entry configured here will be used by the classifier to place ingress packets appropriately.

4.5.6.2 QoS Classification

This section will guide you to create a traffic class rule to classify the upstream traffic, assign queue which defines the precedence and the interface and optionally overwrite the IP header DSCP byte.

A rule consists of a class name and at least one condition below. All of the specified conditions in this classification rule must be satisfied for the rule to take effect.

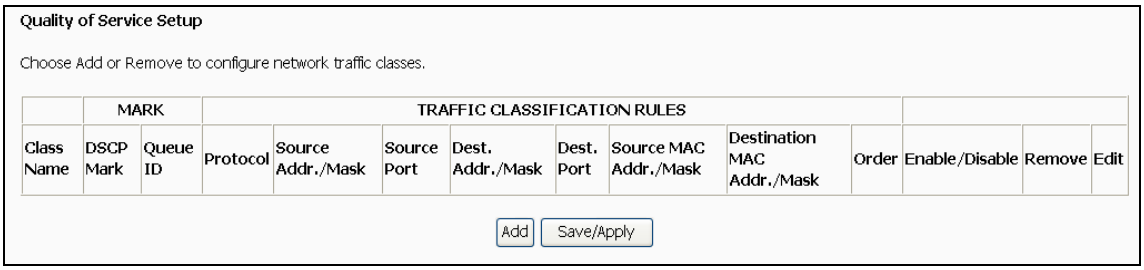


Figure 4-56

Click the Add button Figure 4-56, and you can configure the QoS on the next screen.

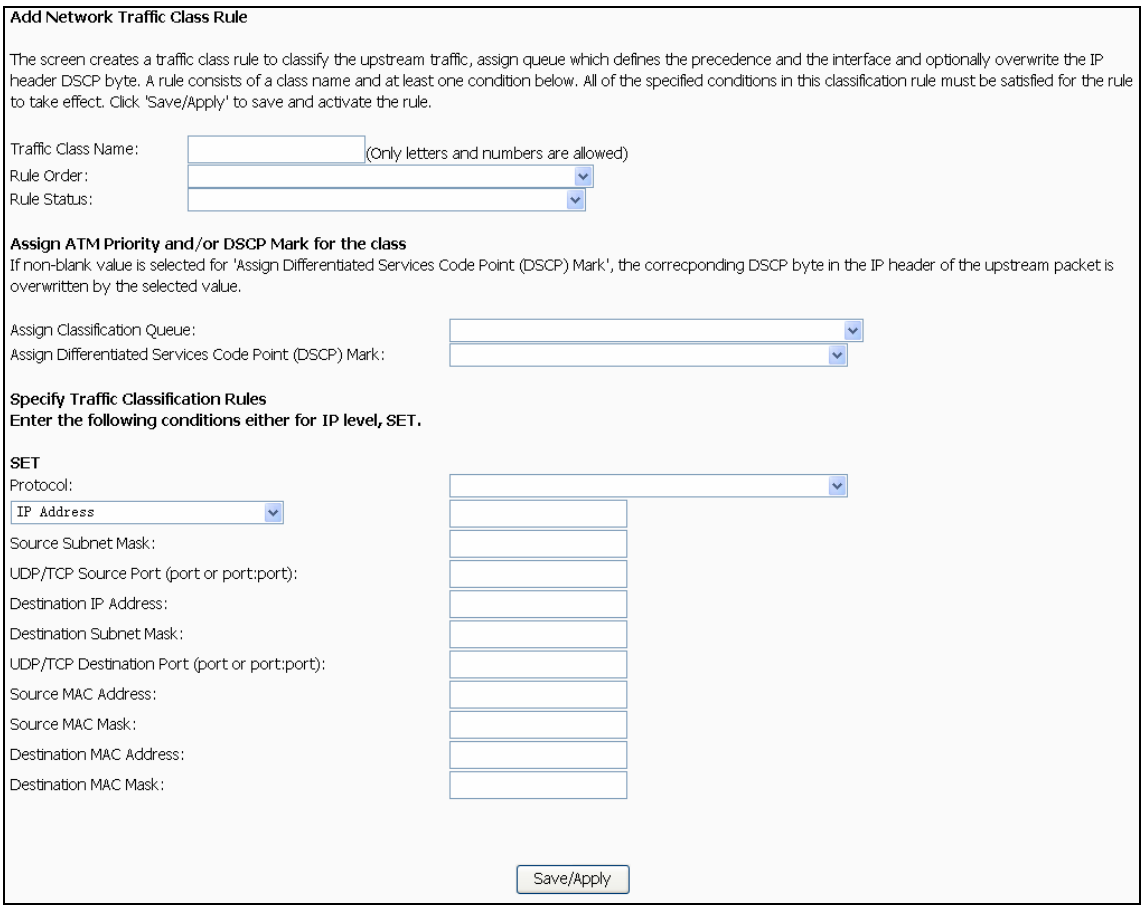


Figure 4-57

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

4.5.7 Routing

Choose “Advanced Setup→Routing” menu, you can see two submenus under the Routing menu as shown in Figure 4-58.

Figure 4-58

4.5.7.1 Default Gateway

Choose “Routing→Default Gateway” menu, you can configure the Default Gateway routing in the next screen as shown in Figure 4-59.

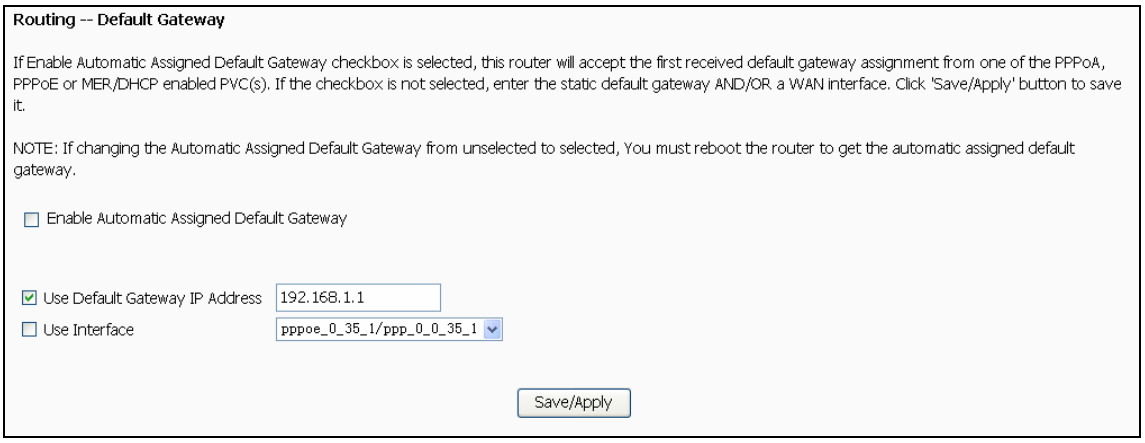


Figure 4-59

- Enable Automatic Assigned Default Gateway - Select this checkbox, and then the Router will accept the first received default gateway assignment from one of the PPPoA, PPPoE or MER/DHCP enabled PVC(s). If this checkbox is not selected, you have to enter the static default gateway and/or an interface. Click Save/Apply to save your configurations.

Note:

If changing the Enable Automatic Assigned Default Gateway from unselected to selected, you must reboot the Router to get the automatic assigned default gateway.

4.5.7.2 Static Route

Choose “Routing→Static Route” menu, you can view and add the Static Route entry in the next screen as shown in Figure 4-60. A static route is a pre-determined path that network information must travel to reach a specific host or network.

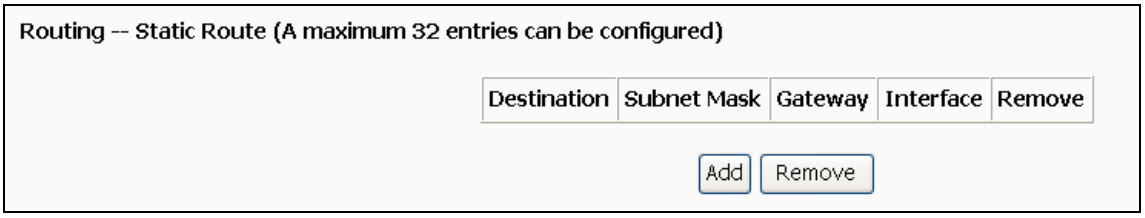


Figure 4-60

To add a new entry, follow the steps below.

1. Click the Add button in Figure 4-60 to go to the Static Route Add page as shown in Figure 4-61.
2. Enter the IP address of the destination network. This parameter specifies the IP network address of the final destination.
3. Enter the Subnet Mask for the destination.
4. Select the Use Gateway IP Address checkbox and enter the IP address of the gateway. The gateway is an immediate neighbor of your ADSL Router that will forward the packet to the destination. On the LAN, the gateway must be a router on the same segment as your Router; over Internet (WAN), the gateway must be the IP address of one of the remote nodes.

5. Click Save/Apply to save your configurations. Then you will go back to Figure 4-60 and see your new entry.

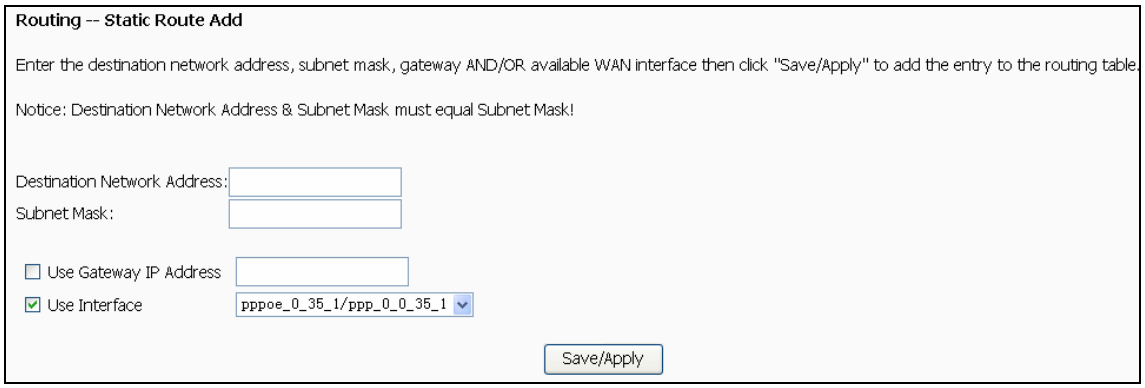


Figure 4-61

4.5.8 DNS

When you select the connection type PPPoE, PPPoA or IPoA for WAN configuration, you will see the DNS menu in the Web-based Utility (shown in Figure 4-62). It includes DNS Server and Dynamic DNS submenus.

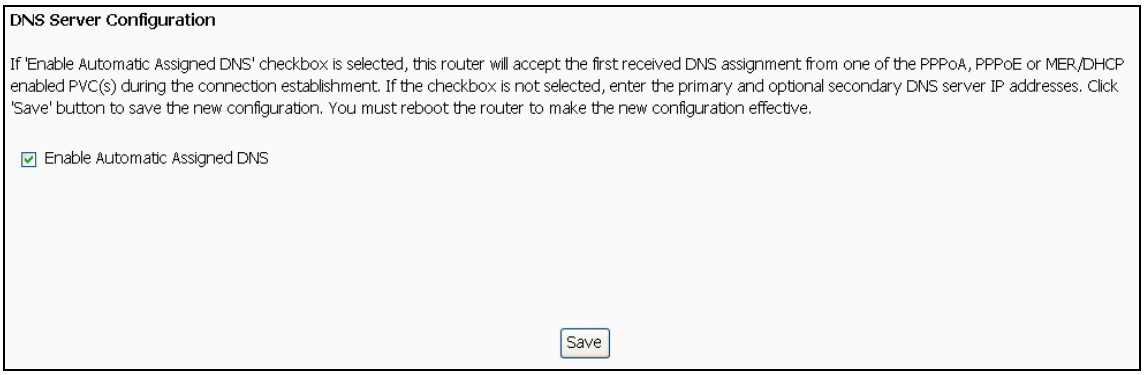


Figure 4-62

4.5.8.1 DNS Server

Choose “Advanced Setup→DNS→DNS Server”, and you can see the DNS Server Configuration screen. Deselect the checkbox before Auto DNS Server, and then you will be able to manually configure the DNS Server Addresses as shown in Figure 4-63.

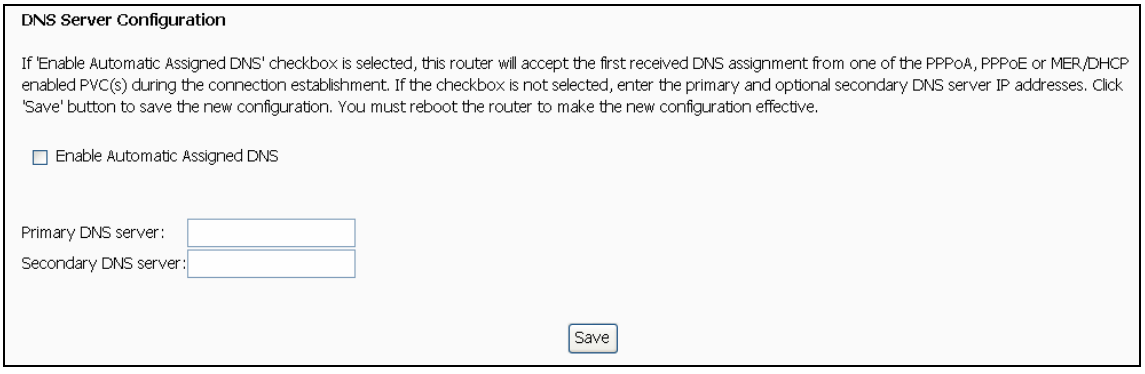


Figure 4-63

Enter the primary and /or secondary DNS server IP addresses provided by your ISP.

Click the Apply/Save button to save the new configuration.

4.5.8.2 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 4-64).

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.

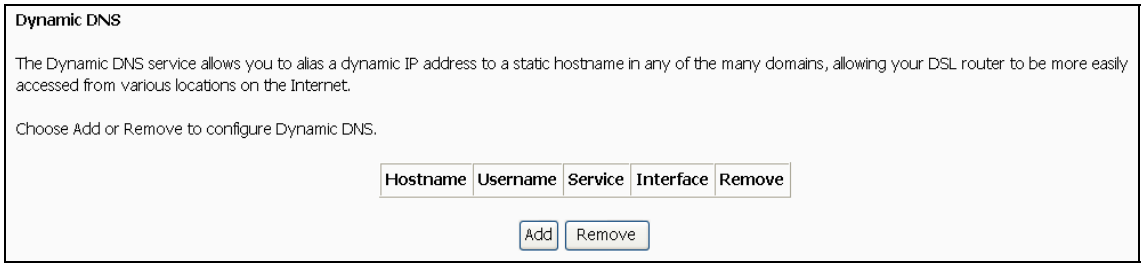


Figure 4-64

To add a DDNS entry:

1. Click the Add button (pop-up Figure 4-64), and then you will set the DDNS in the next screen (shown in Figure 4-65).

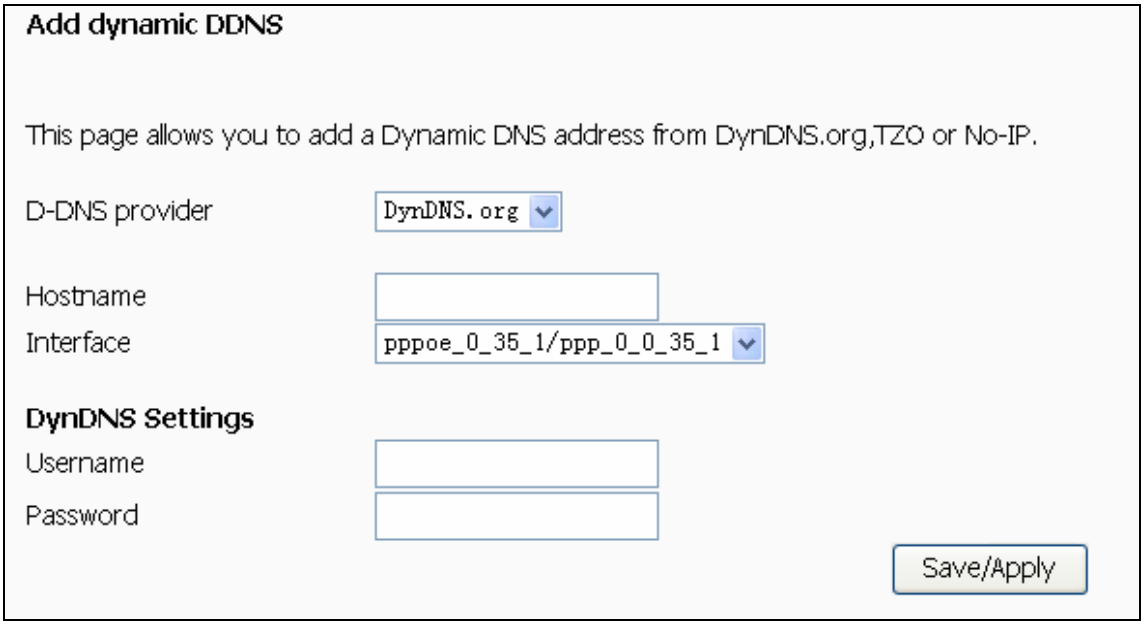


Figure 4-65

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.

Click Save/Apply to save the entry and then you will see your settings as shown in Figure 4-64.

4.5.9 DSL

Choose “Advanced Setup→DSL” menu, you can view and configure the parameters in the screen as shown in Figure 4-66.

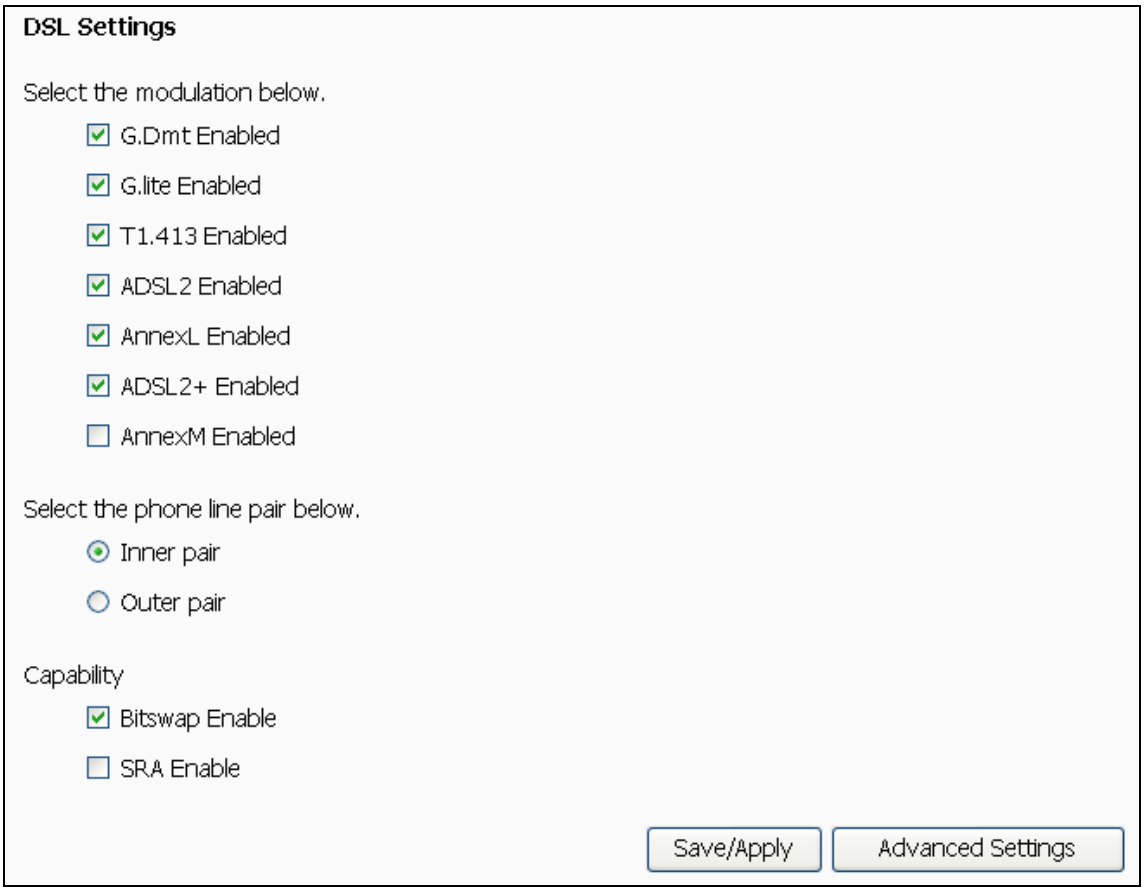


Figure 4-66

If you want to make some advanced settings, click Advanced Settings button in Figure 4-66 to go to the DSL Advanced Settings page as shown in Figure 4-67.

Figure 4-67

If you want to select the tone, click the Tone Selection button to go to the ADSL Tone Settings page as shown in Figure 4-68.

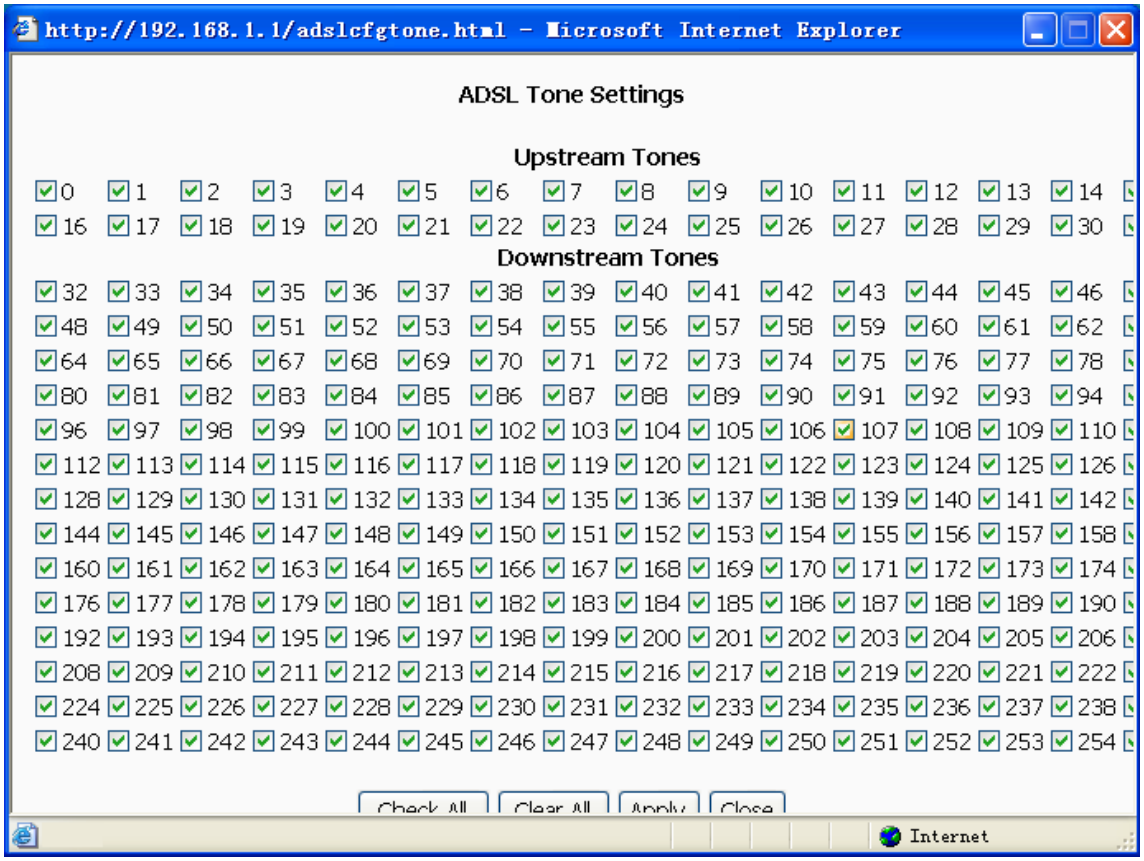


Figure 4-68

4.5.10 Port Mapping

Choose “Advanced Setup→Port Mapping” menu, you can view and configure the parameters in the screen as shown in Figure 4-69.

Port Mapping supports multiple ports to PVC and bridging groups. Each group will perform as an independent network.

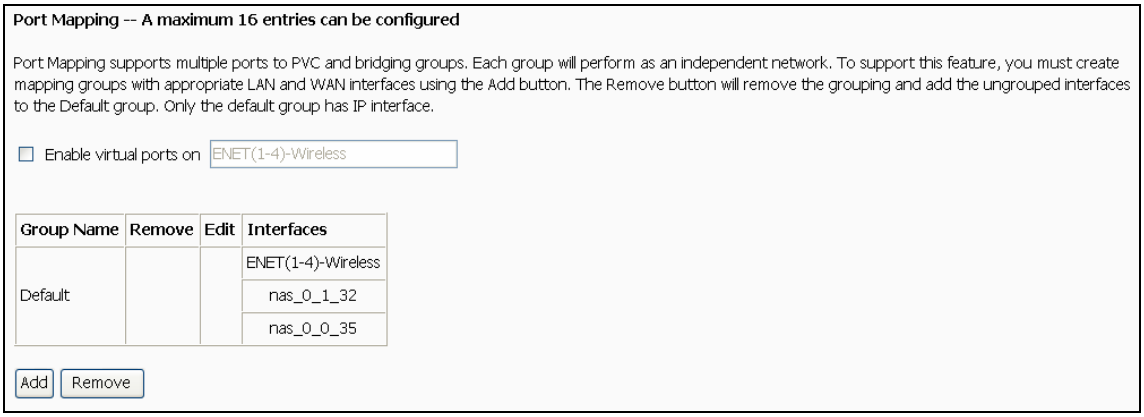


Figure 4-69

To add a Port Mapping group:

1. Click the Add button, and Figure 4-70 pop up, and then you will set the port mapping group.

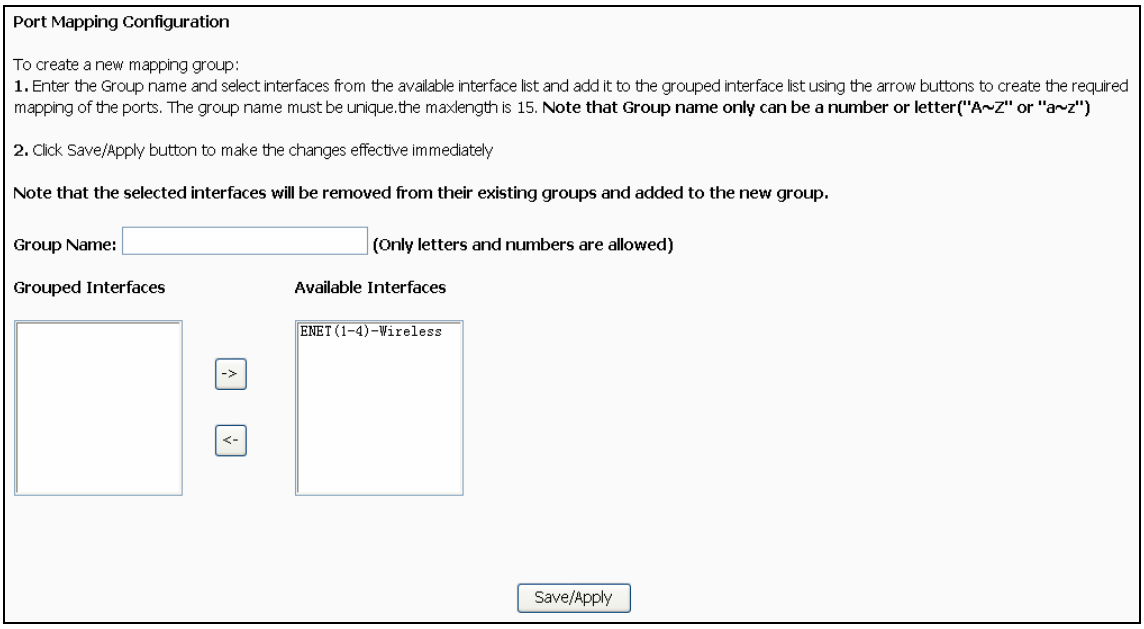


Figure 4-70

2. 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. The max length is 15.

Click Save/Apply button to make the changes effective immediately

☞ **Note:**

Group name only can be a number or letter 0("A~Z" or "a~z").

4.5.11 IPSec

Choose “Advanced Setup→IPSec”, you can Add/Remove or Enable/Disable the IPSec tunnel connections on the screen as shown in Figure 4-71.

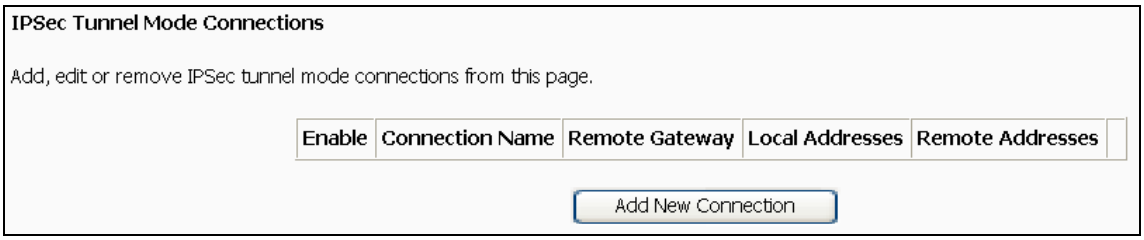
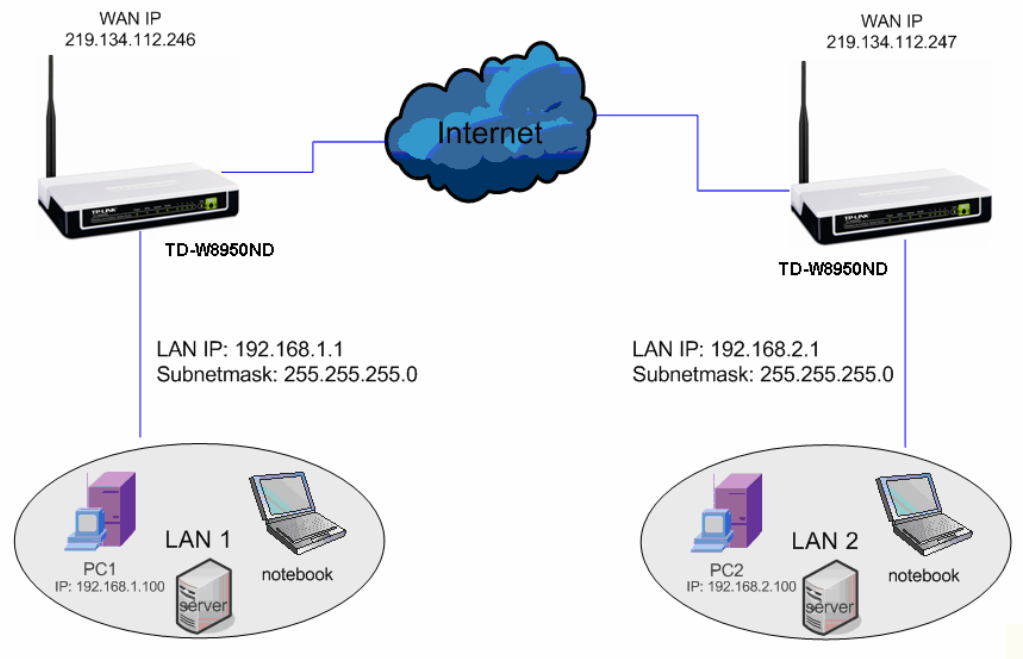


Figure 4-71

This section will guide you to configure a VPN tunnel between two TD-W8950NDs. The topology is as follows.



Note:

You could also use other VPN Routers to set VPN tunnels with TD-W8950ND. TD-W8950ND supports up to 10 VPN tunnels simultaneously.

Click Add New Connection in Figure 4-71 and then you will enter the screen shown in Figure 4-72.

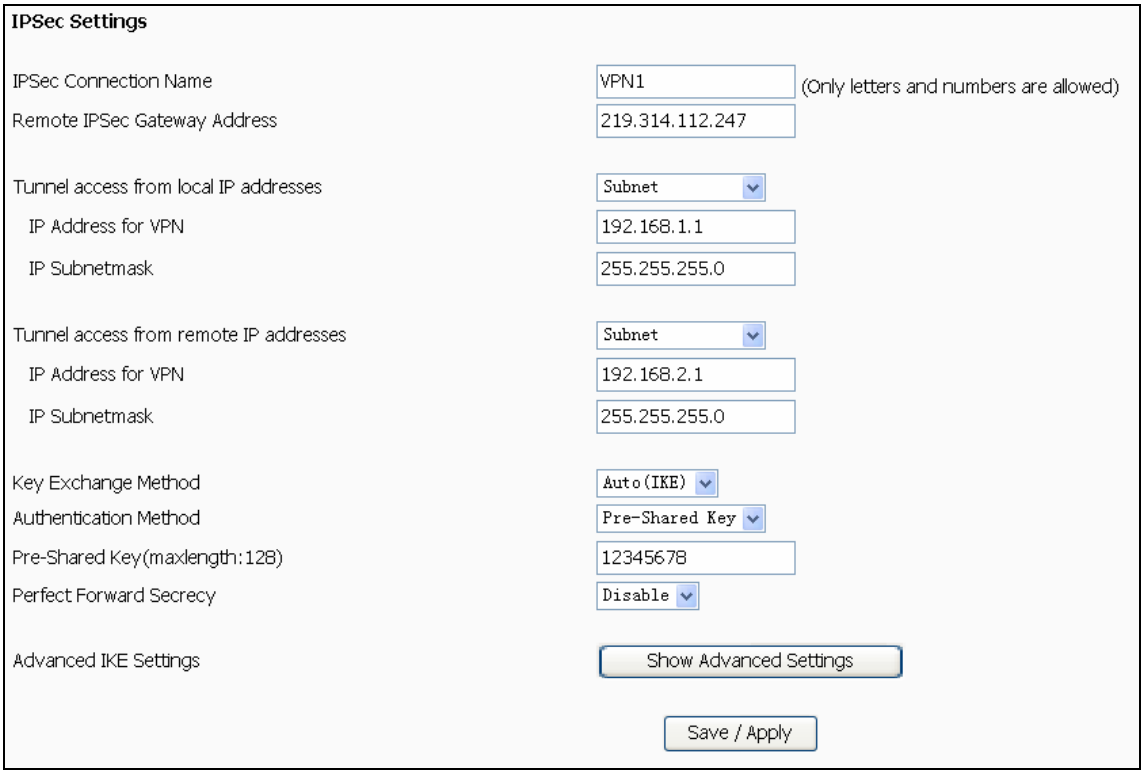


Figure 4-72

- IPSec Connection Name: Enter a name for your VPN.

- Remote IPSec Gateway Address: Enter the destination gateway IP address in the box which is the public WAN IP or Domain Name of the remote VPN server endpoint. (For example: Input 219.134.112.247 in Device1, Input 219.134.112.246 in Device 2)
- Tunnel access from local IP addresses: Choose Subnet if you want the Whole LAN to join the VPN network, or else choose Single Address if you want single IP to join the VPN network.
- IP Address for VPN: Enter the IP address of your LAN. (For example: Input 192.168.1.1 in Device1, Input 192.168.2.1 in Device2)
- IP Subnetmask: Enter the Subnet mask of your LAN. (For example: Input 255.255.255.0 in both Device1 and Device2)
- Tunnel access from remote IP addresses: Choose Subnet if you want the Remote Whole LAN to join the VPN network, or else choose Single Address if you want single IP to join the VPN network.
- IP Address for VPN: Enter the IP address of the Remote LAN. (For example: Input 192.168.2.1 in Device1,Input 192.168.1.1 in Device2)
- IP Subnetmask: Enter the subnetmask of the remote LAN. (For example: Input 255.255.255.0 in both Device1 and Device2)
- Key Exchange Method: Select Auto (IKE) or Manual.
- Authentication Method: Select Pre-Shared Key (recommended) or Certificate (X.509).
- Pre-Shared Key: Input the Pre-Shared key for Authentication. (For example: Input 12345678)
- Perfect Forward Secrecy: PFS is an additional security protocol.

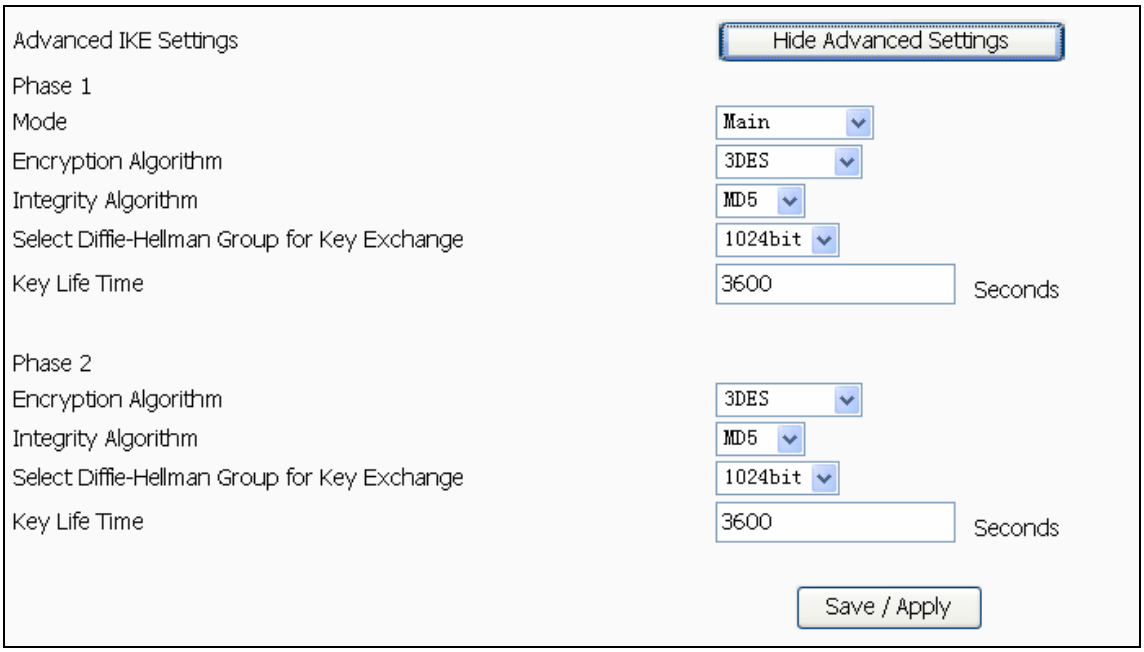
We recommend you leave the Advanced Settings as default value.

After complete the basic settings and click Save/Apply in both Device1 and Device2, PCs in LAN1 could conmmunicate with PCs in remote LAN2. (For example: You can ping the IP address of PC2 which is 192.168.2.100 in PC1)

☞ **Note:**

The VPN Servers Endpoint from both ends must use the same pre-shared keys and Perfect Forward Secrecy settings.

Click Show Advanced Settings and then you can configure the Advanced Settings.



- Main Mode: Select Main Mode to configure the standard negotiation parameters for IKE phase1.
- Aggressive Mode: Select Aggressive Mode to configure IKE phase1 of the VPN Tunnel to carry out negotiation in a shorter amount of time. (Not Recommended-Less Secure)

Note:

The difference between the two is that aggressive mode will pass more information in fewer packets, with the benefit of slightly faster connection establishment, at the cost of transmitting the identities of the security firewall in the clear. When using aggressive mode, some configuration parameters such as Diffie-Hellman groups, and PFS can not be negotiated, resulting in a greater importance of having "compatible" configuration on both ends.

- Key Life Time:

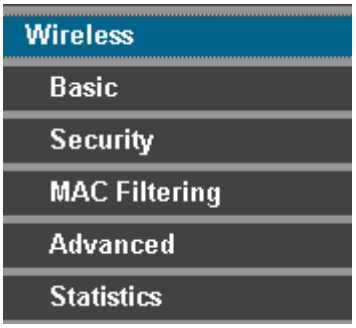
Enter the number of seconds for the IPSec lifetime. It is the period of time to pass before establishing a new IPSec security association (SA) with the remote endpoint. The default value is 3600.

Note:

If you want to change the default settings of Advanced Settings, please make sure that both VPN server endpoints use the same Encryption Algorithm, Integrity Algorithm, Diffie-Hellman Group and Key Life time in both phase1 and phase2.

4.6 Wireless

Choose “Wireless”, there are five submenus to configure Wireless LAN settings. Click any of them, and you will be able to configure the corresponding function. The detailed explanations for each submenu are provided below.



4.6.1 Basic

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 4-73

- SSID: Enter a value of up to 32 characters. The same name of SSID (Service Set Identification) must be assigned to all wireless devices in your network. Considering your wireless network security, the default SSID is set to be (XXXXXX indicates the last unique six numbers of each Router’s MAC address). This value is case-sensitive. For example, *TEST* is NOT the same as *test*.

- Channel: This field determines which operating frequency will be used. The default channel is set to Auto, so the AP will choose the best channel automatically. It is not necessary to change the wireless channel unless you notice interference problems with another nearby access point.
- Region: Select your region from the pull-down list. This field specifies the region where the wireless function of the Router can be used. It may be illegal to use the wireless function of the Router in a region other than one of those specified in this field. If your country or region is not listed, please contact your local government agency for assistance.

When you select your local region from the pull-down list, click the Save button, then the Note Dialog appears. Click OK.

Note Dialog

Note:

Limited by local law regulations, version for North America does not have region selection option.

- Mode: Select the desired mode. The default setting is 11bgn mixed.

11b only: Select if all of your wireless clients are 802.11b.

11g only: Select if all of your wireless clients are 802.11g.

11n only: Select only if all of your wireless clients are 802.11n.

11bg mixed: Select if you are using both 802.11b and 802.11g wireless clients.

11bgn mixed: Select if you are using a mix of 802.11b, 11g, and 11n wireless clients.

Select the desired wireless mode. When 802.11g mode is selected, only 802.11g wireless stations can connect to the Router. When 802.11n mode is selected, only 802.11n wireless stations can connect to the AP. It is strongly recommended that you set the Mode to 802.11b&g&n, and all of 802.11b, 802.11g, and 802.11n wireless stations can connect to the Router.

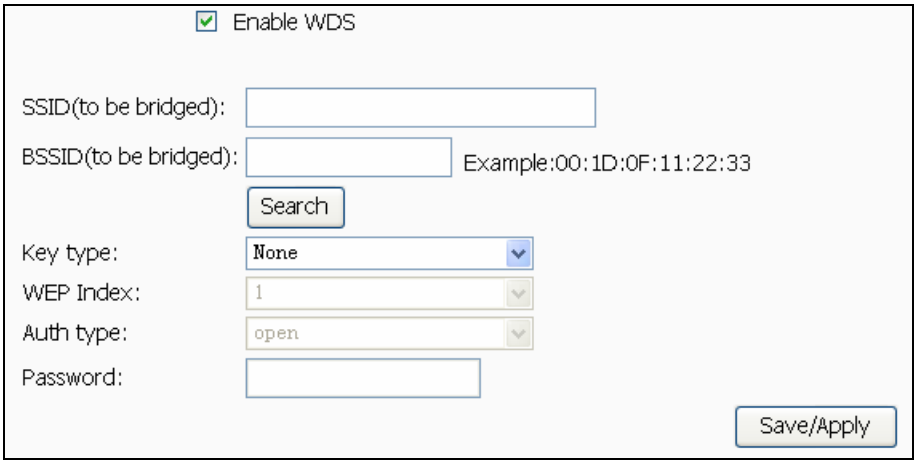
- Channel width: Select any channel width from the pull-down list. The default setting is automatic, which can adjust the channel width for your clients automatically.

Note:

If 11b only, 11g only, or 11bg mixed is selected in the Mode field, the Channel Width selecting field will turn grey and the value will become 20M, which is unable to be changed.

- Enable Wireless Router Radio: The wireless radio of this Router can be enabled or disabled to allow wireless stations access.
- 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. If you select the Enable SSID Broadcast checkbox, the Wireless Router will broadcast its name (SSID) on the air.
- Enable WDS: Check this box to enable WDS. With this function, the Router can bridge two or

more WLANs. If this checkbox is selected, you will have to set the following parameters as shown below. Make sure the following settings are correct



- SSID(to be bridged): The SSID of the AP your Router is going to connect to as a client. You can also use the search function to select the SSID to join.
- BSSID(to be bridged): The BSSID of the AP your Router is going to connect to as a client. You can also use the search function to select the BSSID to join.
- Search: Click this button, you can search the AP which runs in the current channel.
- Key type: This option should be chosen according to the AP's security configuration.It is recommended that the security type is the same as your AP's security type
- WEP Index: This option should be chosen if the key type is WEP(ASCII) or WEP(HEX).It indicates the index of the WEP key.
- Auth Type: This option should be chosen if the key type is WEP(ASCII) or WEP(HEX).It indicates the authorization type of the Root AP.
- Password: If the AP your Router is going to connect needs password, you need to fill the password in this blank.

Click Apply/Save to save your settings.

4.6.2 Security

Choose menu “Wireless→Security”, you can configure the security settings of your wireless network.

There are five wireless security modes supported by the Router: WEP (Wired Equivalent Privacy), WPA (Wi-Fi Protected Access), WPA2 (Wi-Fi Protected Access 2), WPA2-PSK (Pre-Shared Key), WPA-PSK (Pre-Shared Key).

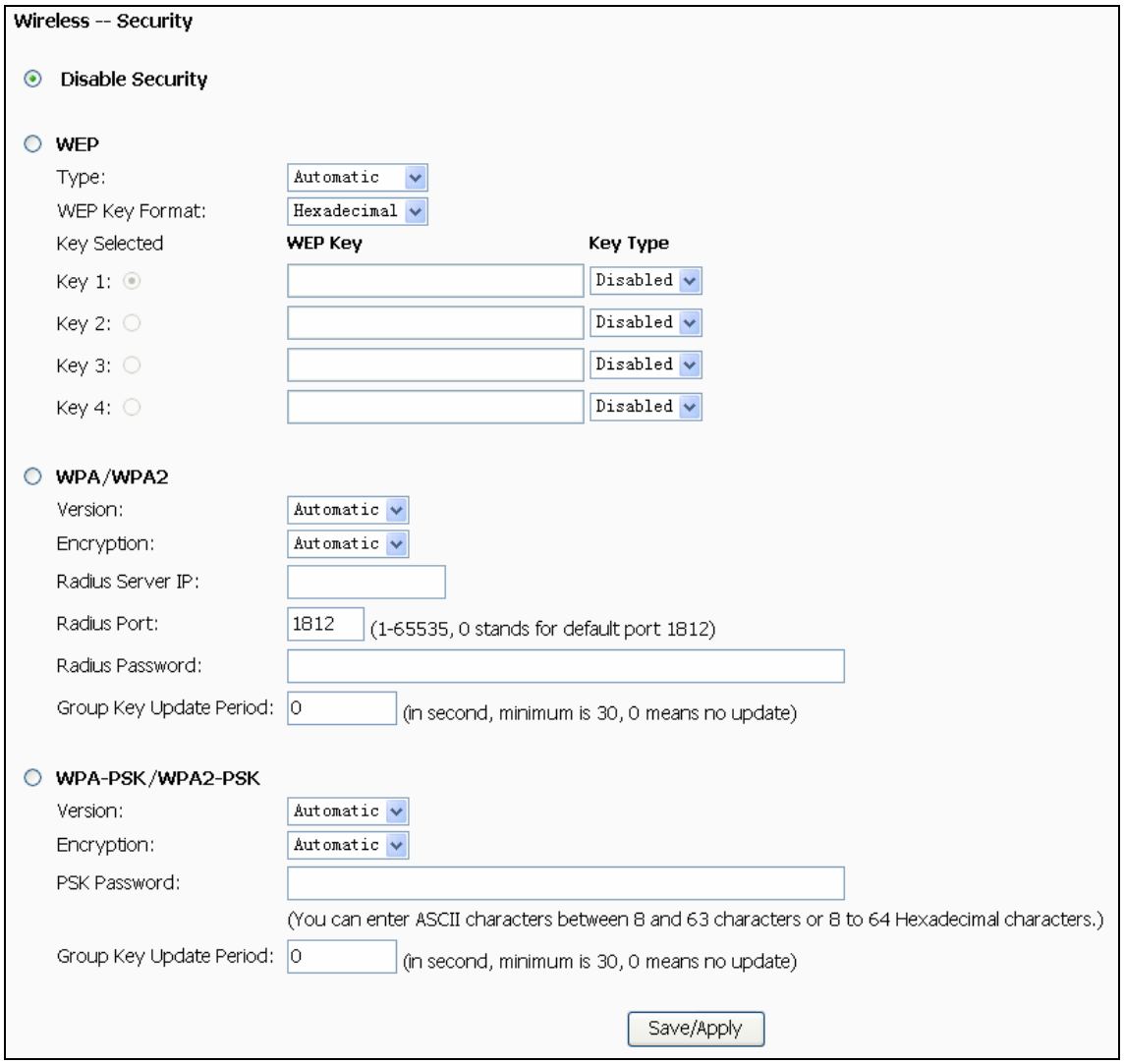


Figure 4-74

- Disable Security: If you do not want to use wireless security, select this check box, but it's strongly recommended to choose one of the following modes to enable security.
- WEP: It is based on the IEEE 802.11 standard. If you select this check box, you will find a notice in red as show in Figure 4-75.

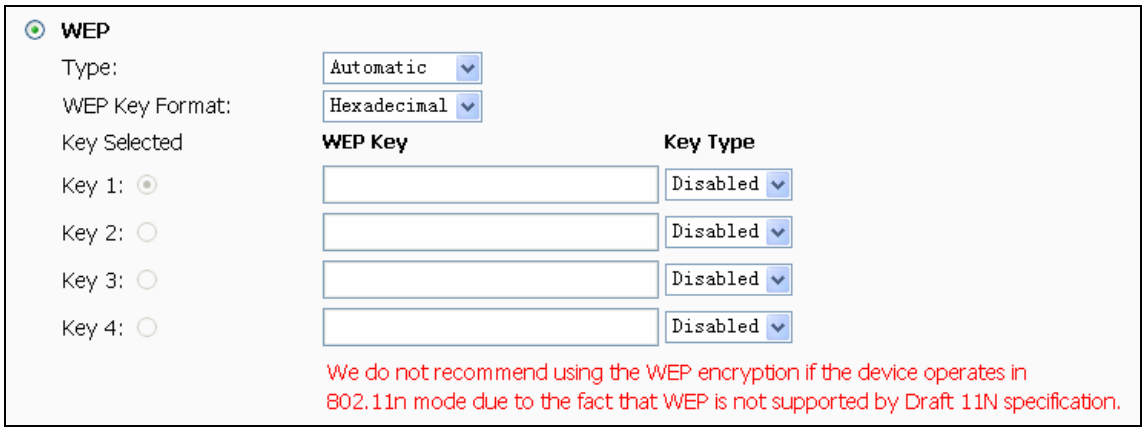


Figure 4-75

- Type: you can choose the type for the WEP security on the pull-down list. The default setting is Automatic, which can select Open System or Shared Key authentication type automatically based on the wireless station's capability and request.
- WEP Key Format: Hexadecimal and ASCII formats are provided. Hexadecimal format stands for any combination of hexadecimal digits (0-9, a-f, A-F) in the specified length. ASCII format stands for any combination of keyboard characters in the specified length.
- WEP Key: Select which of the four keys will be used and enter the matching WEP key that you create. Make sure these values are identical on all wireless stations in your network.
- Key Type: You can select the WEP key length (64-bit, or 128-bit, or 152-bit.) for encryption. "Disabled" means this WEP key entry is invalid.

64-bit: You can enter 10 hexadecimal digits (any combination of 0-9, a-f, A-F, zero key is not promoted) or 5 ASCII characters.

128-bit: You can enter 26 hexadecimal digits (any combination of 0-9, a-f, A-F, zero key is not promoted) or 13 ASCII characters.

152-bit: You can enter 32 hexadecimal digits (any combination of 0-9, a-f, A-F, zero key is not promoted) or 16 ASCII characters.

Note:

If you do not set the key, the wireless security function is still disabled even if you have selected Shared Key as Authentication Type.

➢ WPA /WPA2: It's based on Radius Server.

- Version: you can choose the version of the WPA security on the pull-down list. The default setting is Automatic, which can select WPA (Wi-Fi Protected Access) or WPA2 (WPA version 2) automatically based on the wireless station's capability and request.
- Encryption: You can select either Automatic, or TKIP or AES.

Note:

If you check the WPA/WPA2 radio button and choose TKIP encryption, you will find a notice in red as shown in Figure 4-76

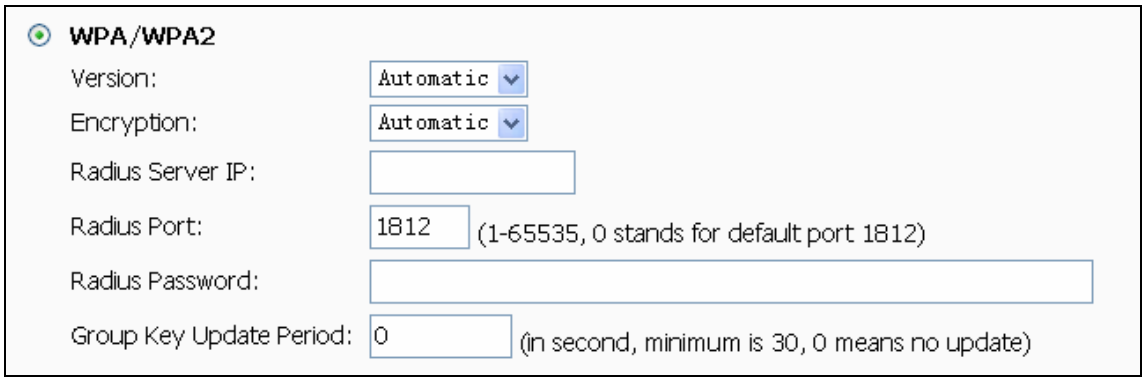


Figure 4-76

- Radius Server IP: Enter the IP address of the Radius Server.
- Radius Port: Enter the port that radius service used.
- Radius Password: Enter the password for the Radius Server.
- Group Key Update Period: Specify the group key update interval in seconds. The value

should be 30 or above. Enter 0 to disable the update.

➢ WPA-PSK/WPA2-PSK: It's the WPA/WPA2 authentication type based on pre-shared passphrase.

- Version: you can choose the version of the WPA-PSK security on the drop-down list. The default setting is Automatic, which can select WPA-PSK (Pre-shared key of WPA) or WPA2-PSK (Pre-shared key of WPA) automatically based on the wireless station's capability and request.
- Encryption: When WPA-PSK or WPA is set as the Authentication Type, you can select either Automatic, or TKIP or AES as Encryption.

Note:

If you check the WPA-PSK/WPA2-PSK radio button and choose TKIP encryption, you will find a notice in red as shown in Figure 4-19.

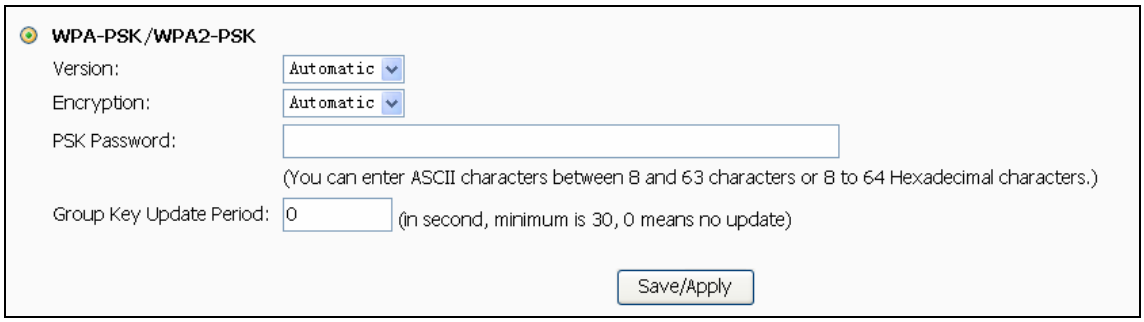


Figure 4-77

- PSK Password: You can enter ASCII characters between 8 and 63 characters or 8 to 64 Hexadecimal characters.
- Group Key Update Period: Specify the group key update interval in seconds. The value should be 30 or above. Enter 0 to disable the update.

Be sure to click the Save button to save your settings on this page.

4.6.3 MAC Filtering

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

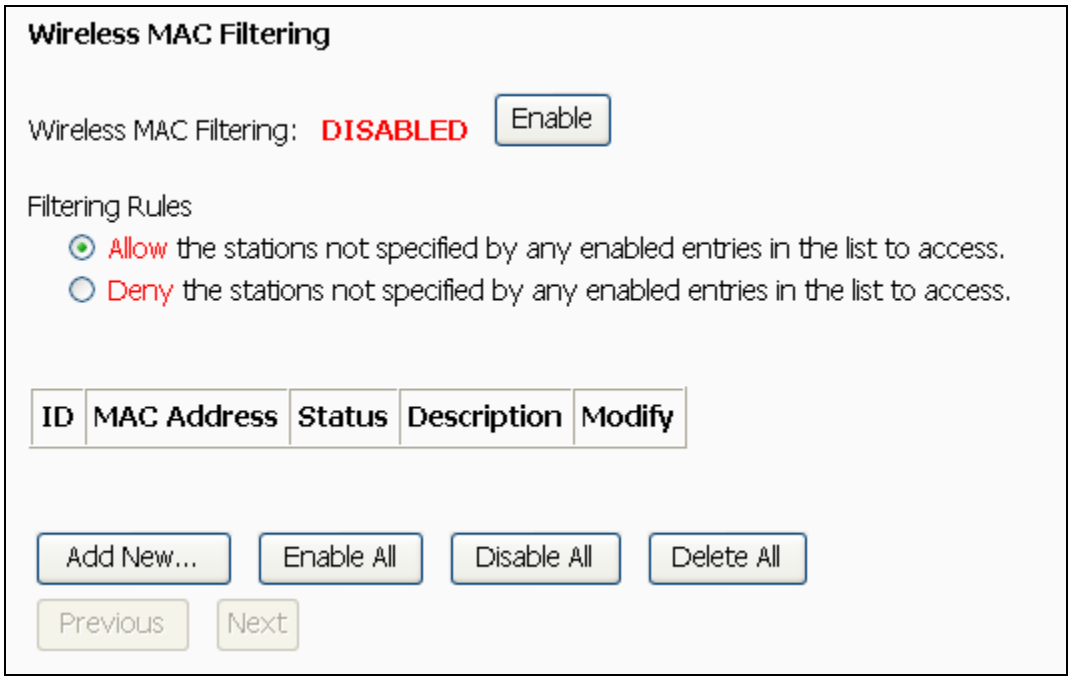


Figure 4-78

To filter wireless users by MAC Address, click Enable. The default setting is Disable.

- MAC Address: The wireless station's MAC address that you want to filter.
- Status: The status of this entry either Enabled or Disabled.
- Description: A simple description of the wireless station.

To Add a Wireless MAC Address filtering entry, click the Add New… button. The "Add or Modify Wireless MAC Address Filtering entry" page will appear, shown in Figure 4-79:

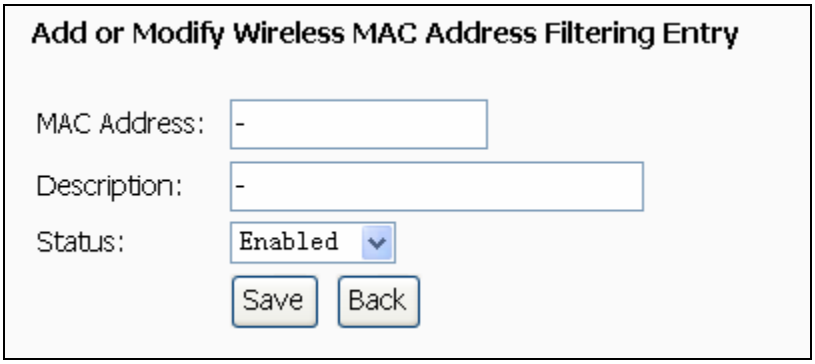


Figure 4-79 Add or Modify Wireless MAC Address Filtering entry

To add or modify a MAC Address Filtering entry, follow these instructions:

1. Enter the appropriate MAC Address into the MAC Address field. The format of the MAC Address is XX:XX:XX:XX:XX:XX (X is any hexadecimal digit). For example: 00:0A:EB:00:07:8A.
2. Enter a simple description of the wireless station in the Description field. For example: Wireless station A.
3. Status - Select Enabled or Disabled for this entry on the Status pull-down list.
4. Click the Save button to save this entry.

To modify or delete an existing entry:

3. Click the Modify in the entry you want to modify. If you want to delete the entry, click the Delete.
4. Modify the information.
5. Click the Save button.

Click the Enable All button to make all entries enabled

Click the Disabled All button to make all entries disabled.

Click the Delete All button to delete all entries

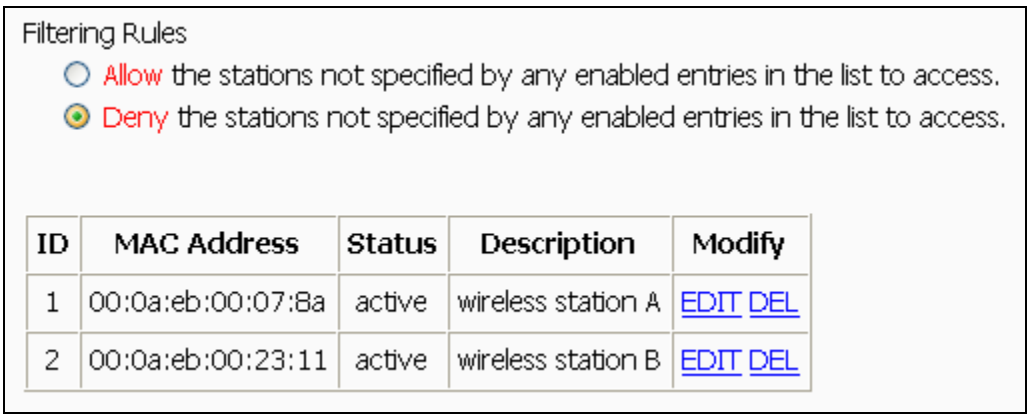
Click the Next button to go to the next page

Click the Previous button to return to the previous page.

For example: If you desire that the wireless station A with MAC address 00-0A-EB-00-07-8A and the wireless station B with MAC address 00-0A-EB-00-23-11 are able to access the Router, but all the other wireless stations cannot access the Router, you can configure the Wireless MAC Address Filtering list by following these steps:

1. Click the Enable button to enable this function.
2. Select the radio button: Deny the stations not specified by any enabled entries in the list to access for Filtering Rules.
3. Delete all or disable all entries if there are any entries already.
4. Click the Add New... button and enter the MAC address 00-0A-EB-00-07-8A /00-0A-EB-00-23-11 in the MAC Address field, then enter wireless station A/B in the Description field, while select Enabled in the Status pull-down list. Finally, click the Save and the Back button.

   The filtering rules that configured should be similar to the following list:



4.6.4 Advanced

Choose “Wireless→Advanced”, you will see the screen of Wireless Advanced settings shown as below.

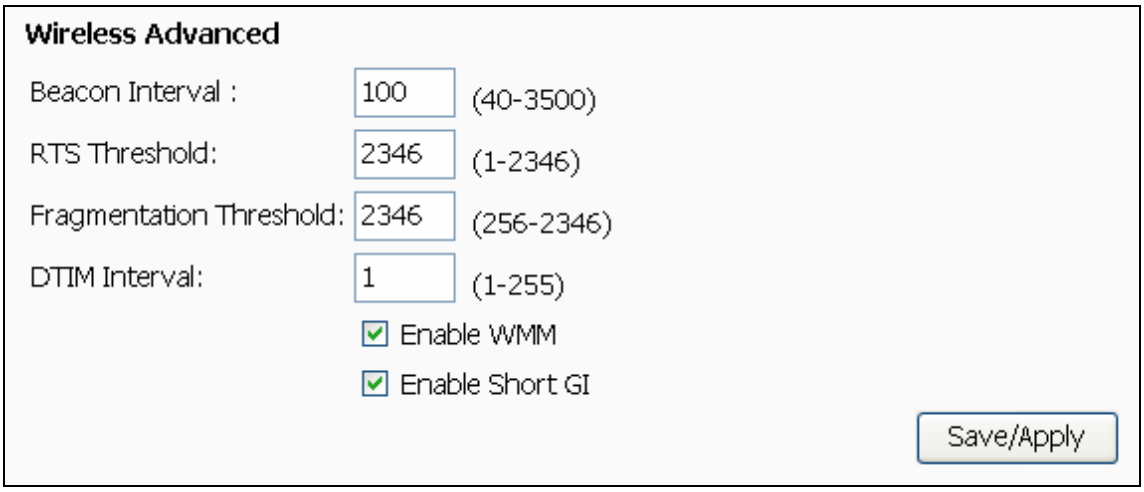


Figure 4-80

- Beacon Interval: Enter a value between 40-3500 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.
- RTS Threshold: Should you encounter inconsistent data flow, only minor reduction of the default value 2346 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 2346.
- 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.
- 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.
- Enable WMM - WMM function can guarantee the packets with high- priority messages being transmitted preferentially. It is strongly recommended enabled.
- Enable Short GI - This function is recommended for it will increase the data capacity by reducing the guard interval time.

4.6.5 Statistics

Choose menu “Wireless→Wireless Statistics”, you can see the MAC Address, Current Status, Received Packets and Sent Packets for each connected wireless station.

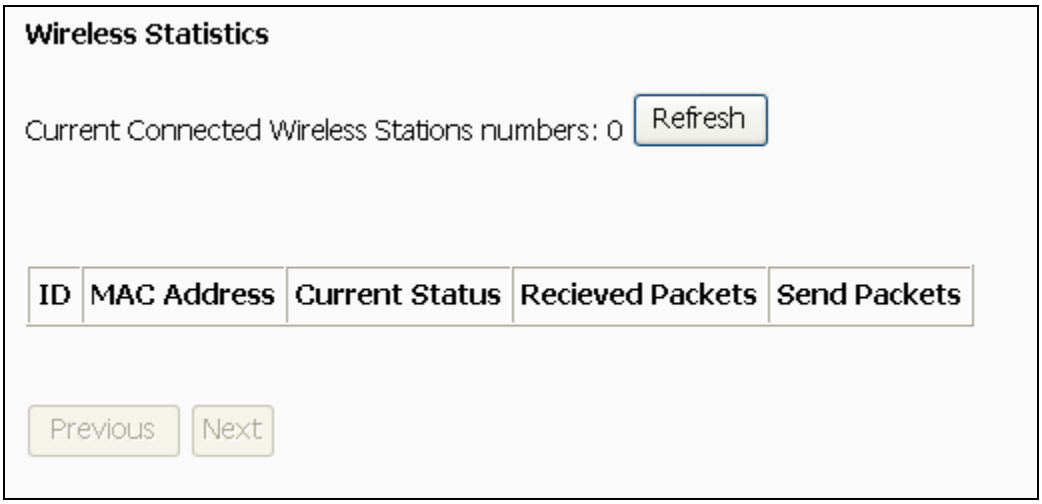


Figure 4-81

- MAC Address - The connected wireless station's MAC address
- Current Status - The connected wireless station's running status, one of STA-AUTH / STA-ASSOC / STA-JOINED / WPA / WPA-PSK / WPA2 / WPA2-PSK / AP-UP / AP-DOWN / Disconnected
- Received Packets - Packets received by the station
- Sent Packets - Packets sent by the station

You cannot change any of the values on this page. To update this page and to show the current connected wireless stations, click on the Refresh button.

If the numbers of connected wireless stations go beyond one page, click the Next button to go to the next page and click the Previous button to return the previous page.

4.7 Diagnostics

Choose “Diagnostics”, and your modem will test your DSL connection. Then you will see the test results for the connectivity to your local network and your DSL service provider similar to the following page.

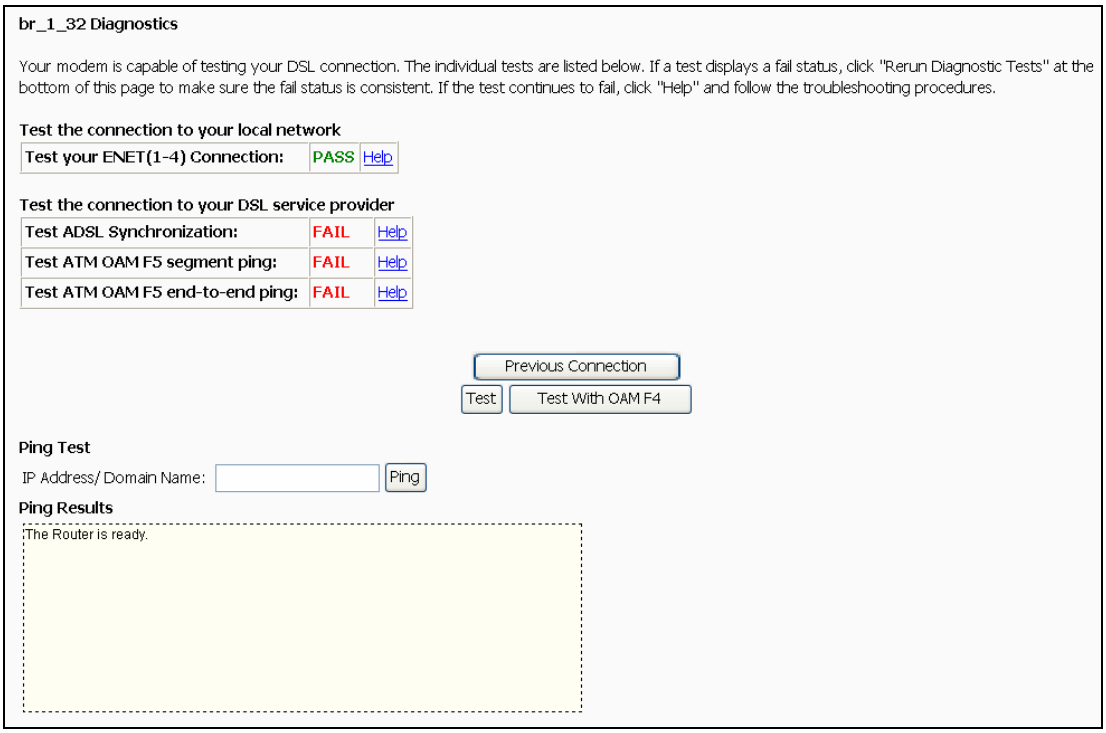


Figure 4-82

4.8 Management

Choose “Management”, and you can see the submenus as shown in Figure 4-83

Figure 4-83

4.8.1 Settings

Choose “Management→Settings” menu, and you will see the submenus as shown in Figure 4-84.

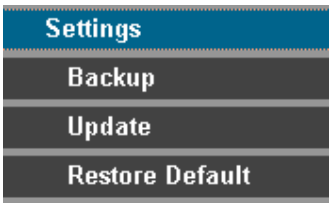


Figure 4-84

4.8.1.1 Backup

Choose “Settings→Backup” menu, and you can save the current configuration of the Router as a backup file in Figure 4-85. Click Backup Settings button to save your current configuration.

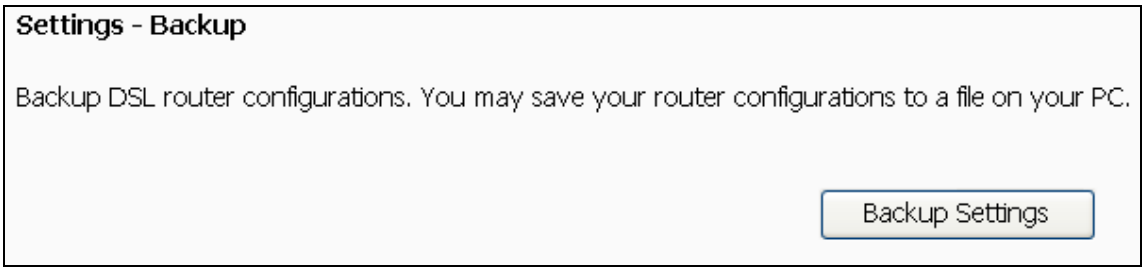


Figure 4-85

4.8.1.2 Update

Choose “Settings→Update” menu, and you can update the settings for the Router as shown in Figure 4-86. Click the Browse… button to find the file you want to update and then click Update Settings to begin the updating.

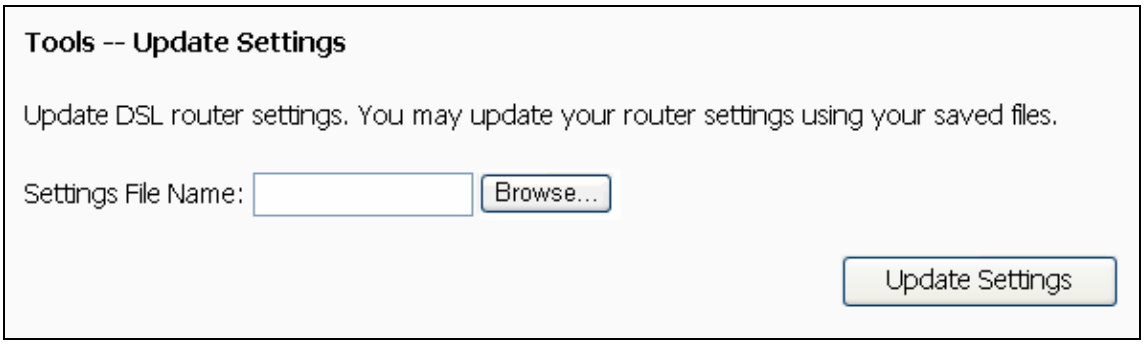


Figure 4-86

4.8.1.3 Restore Default

Choose “Settings→Restore Default” menu, and you can restore the configurations of the Router to its factory default as shown in Figure 4-87. Click the Restore Default Settings button to begin restoring.

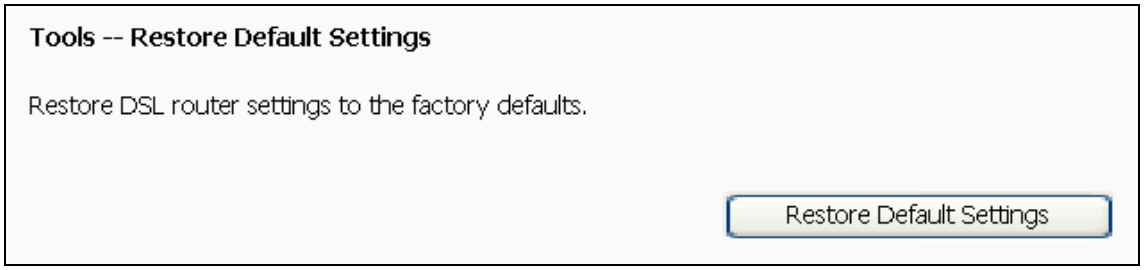


Figure 4-87

4.8.2 System Log

Choose “Management→System Log” menu, and you can view and configure the logs of the Router in Figure 4-88.

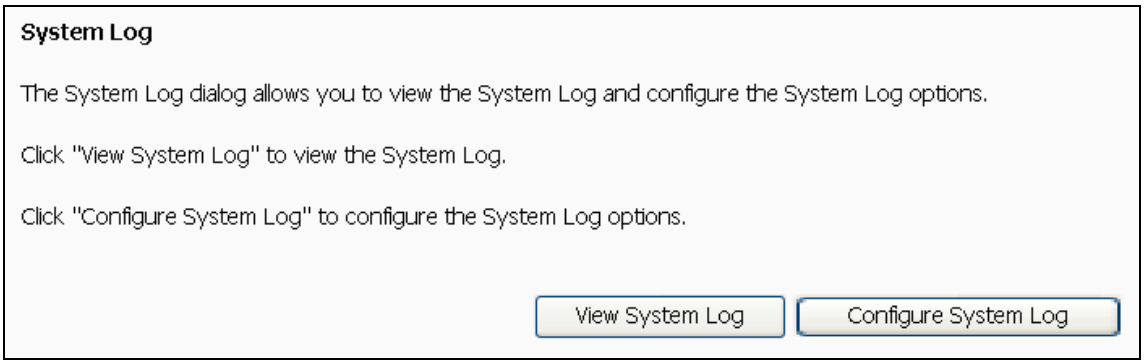


Figure 4-88

Click the View System Log button, and you will go to the System Log page and see the logs similar to Figure 4-89.

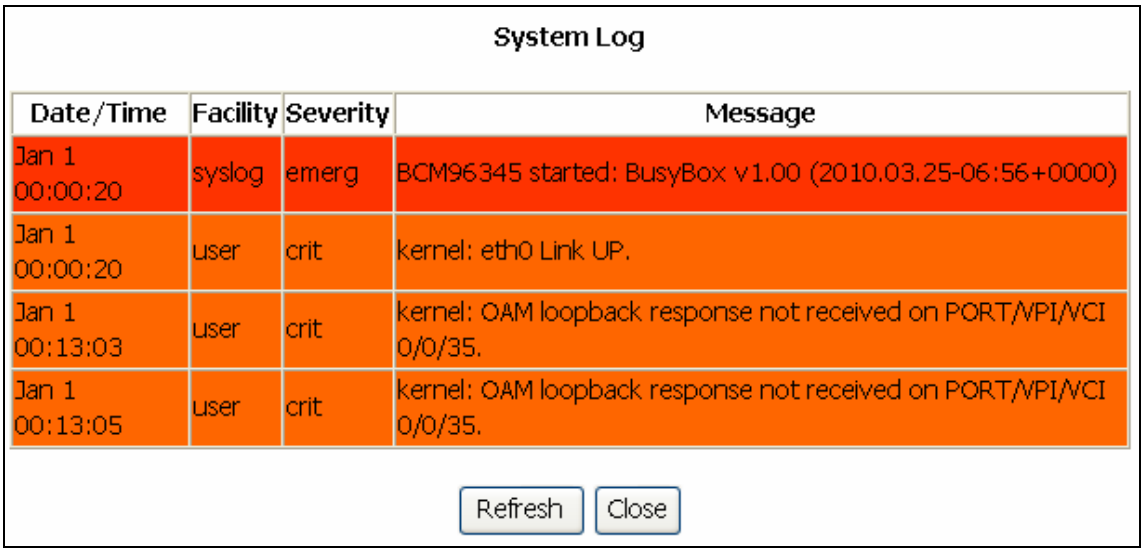


Figure 4-89

Click the Configure System Log button, and you will go to the Configuration page as shown in Figure 4-90.

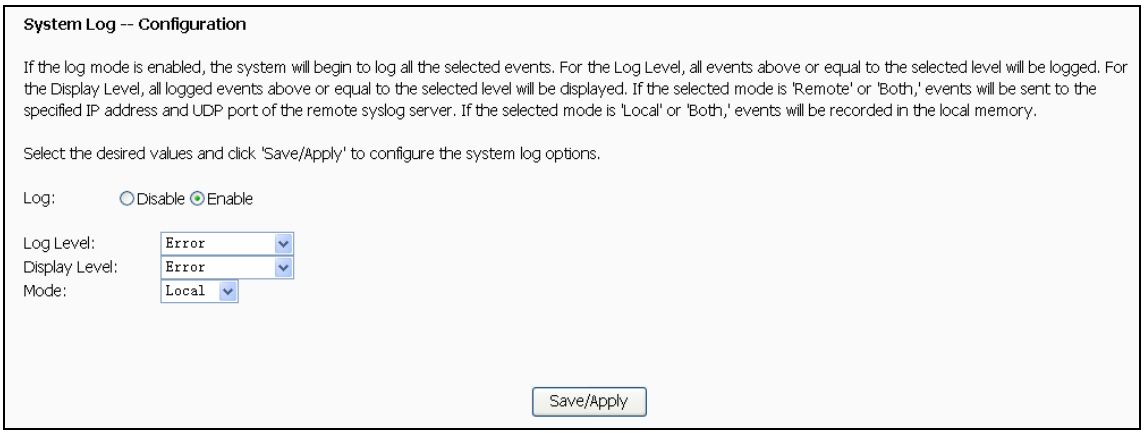


Figure 4-90

- Log - Check the Disable radio button to disable the system log function. The default setting is enabled.
- Log Level - Select the log level, then all the events above or equal to the selected level will be

logged.

- Display Level - All logged events above or equal to the selected level will be displayed.
- Mode - Select Local, Remote or Both. If the selected mode is Remote or Both, events will be sent to the specified IP address and UDP port of the remote syslog server. If the selected mode is Local or Both, events will be recorded in the local memory.

4.8.3 SNMP Agent

Choose “Management→SNMP Agent” menu, and you will go to the SNMP (Simple Network Management Protocol) page as shown in Figure 4-91. SNMP allows a management application to retrieve statistics and status from the SNMP agent in this device. Select the desired values and click Save/Apply to configure the SNMP options.

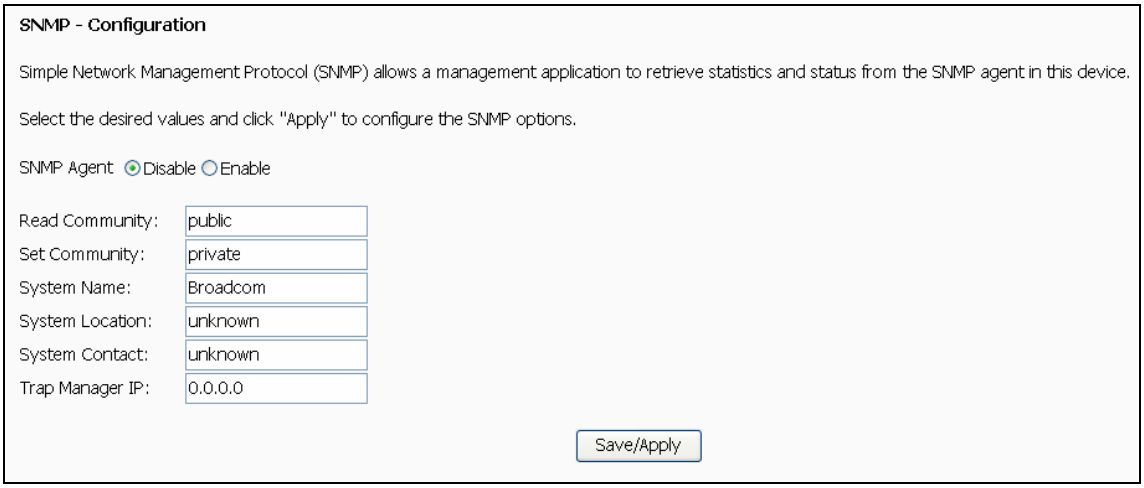


Figure 4-91

4.8.4 TR-069 Client

Choose “Management→TR-069 Client”, you can see the TR-069 client - Configuration screen as shown below.

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

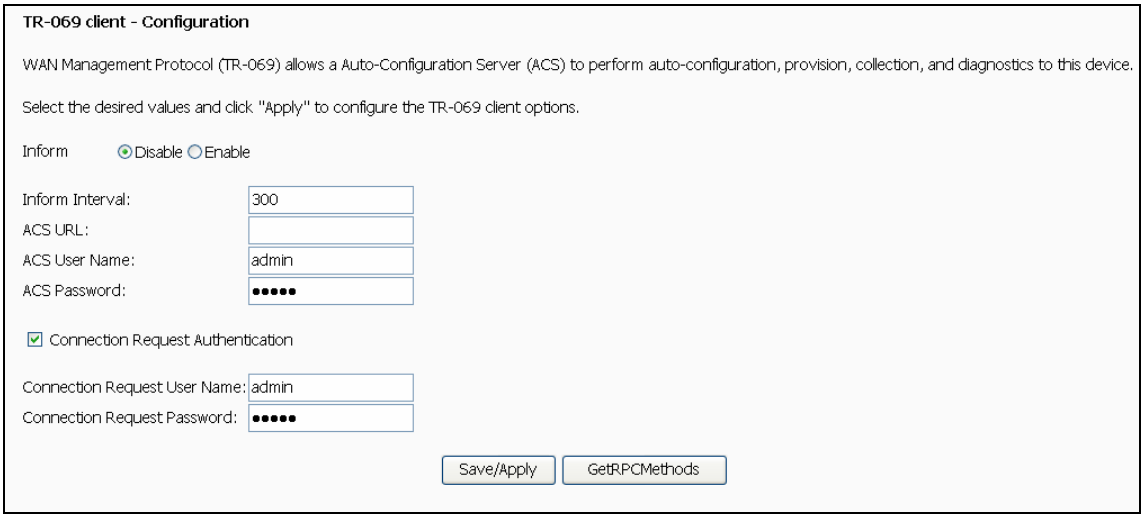


Figure 4-92

- 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 own 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.

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

4.8.5 Internet Time

When you select the connection type PPPoE, PPPoA or IPoA for WAN configuration, you will see the Internet Time in the Web-based Utility. On this page you can configure your router's time.

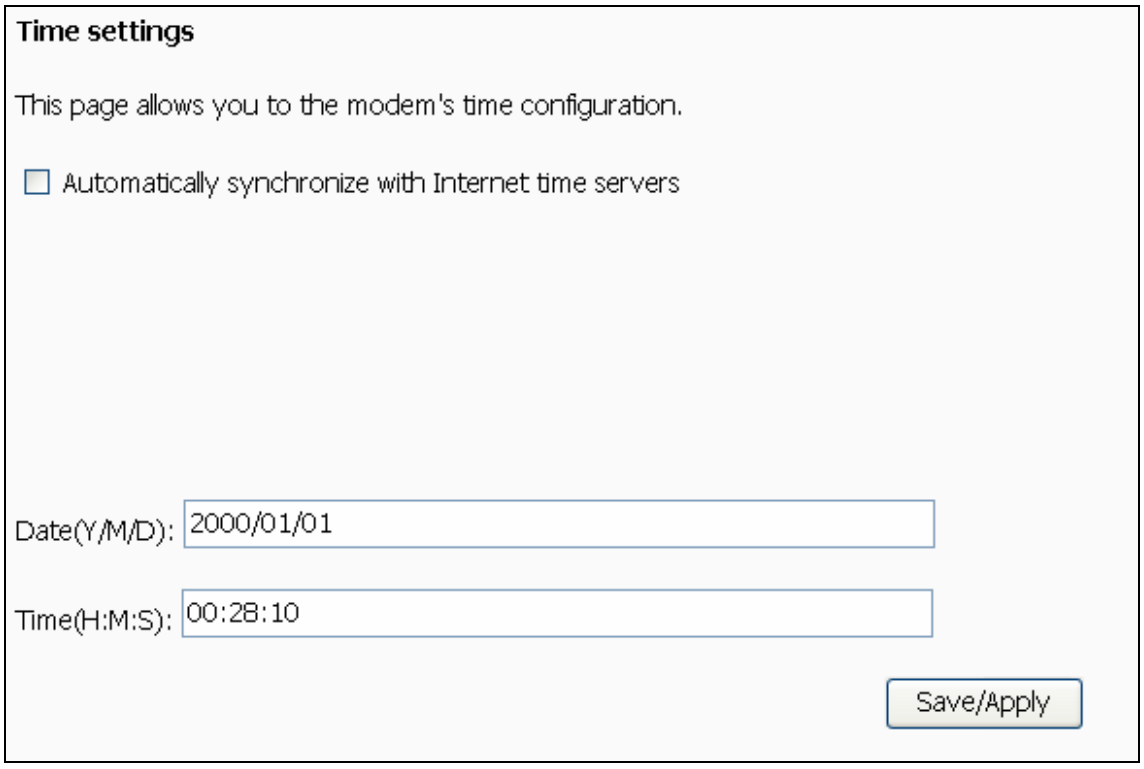


Figure 4-93

- Date: Enter the date.
- Time: Enter the time.

You can also select Automatically synchronize with Internet time servers to make your router synchronize its time with Internet time severs.

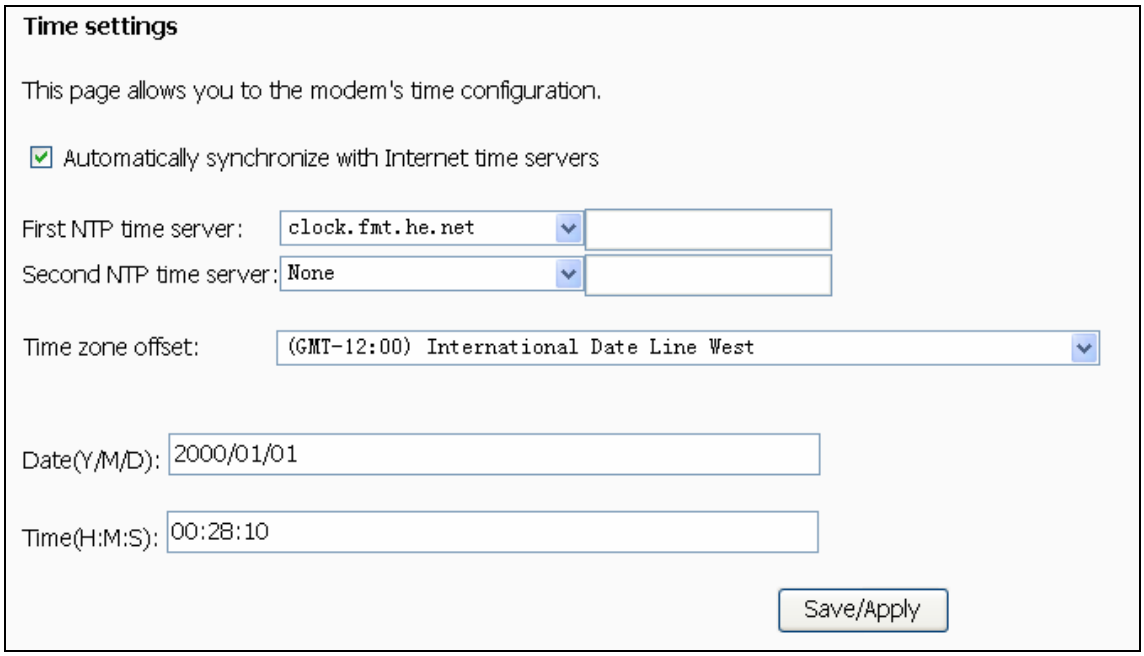


Figure 4-94

- Automatically synchronize with Internet time servers: Select the checkbox to make your router synchronize its time with Internet time severs.
- First/Second NTP time server: Select a time server for your router.
- Time zone offset: Select your time zone.

4.8.6 Access Control

Choose “Management→Access Control” menu, and you will submenus as shown in Figure 4-95.

Figure 4-95

4.8.6.1 Service

Choose “Access Control→Service” menu, and you can enable or disable the services as shown in Figure 4-96. Click Save/Apply to save your configurations.

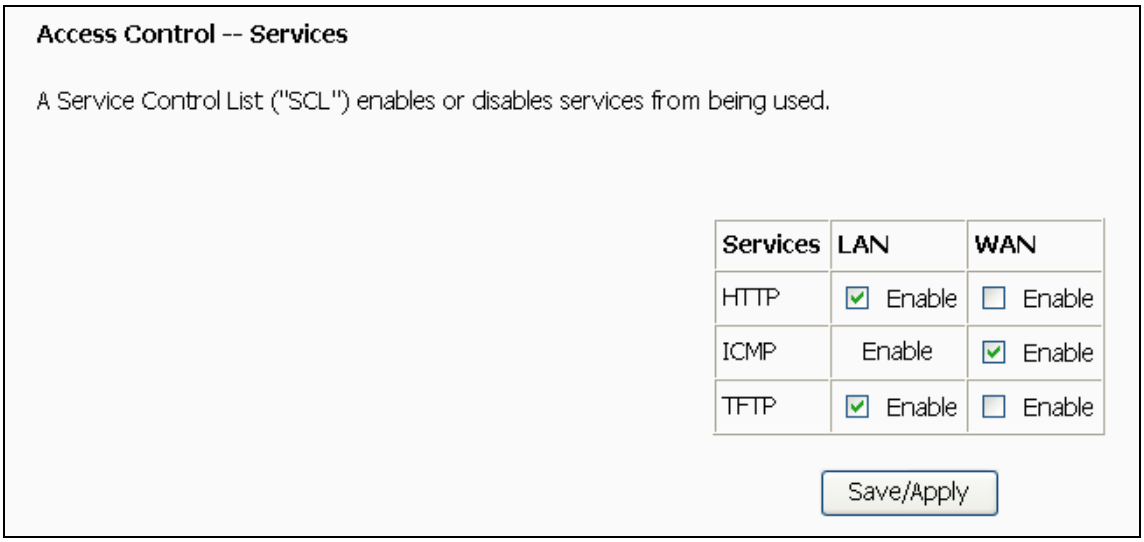


Figure 4-96

4.8.6.2 IP Address

Choose “Access Control→IP Address” menu, and can view and configure the IP address access control in the screen as shown in Figure 4-97. If enabled, only PCs with IP addresses listed are allowed to access the Router.

Figure 4-97

To add a new entry, follow the steps below.

1. Click the Add button in Figure 4-97 to go to the Access Control page in the screen as shown in Figure 4-98.
2. Enter the IP address (e.g. 192.168.1.23) you want to add in the IP Address filed.
3. Click Save/Apply to save your configuration.

Figure 4-98

4.8.6.3 Password

Choose “Access Control→Password” menu, and you can change the factory default password of the Router in the screen as shown in Figure 4-99.

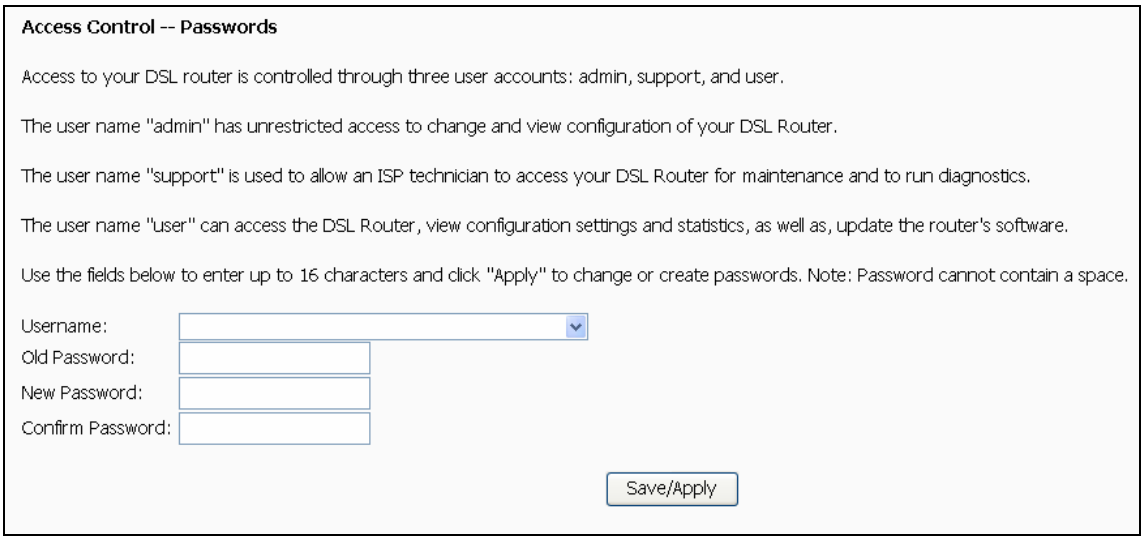


Figure 4-99

4.8.7 Update Software

Choose “Management→Update Software”, you can see the screen (shown in Figure 4-100) which allows you to upgrade the latest version software to keep the Router up to date.

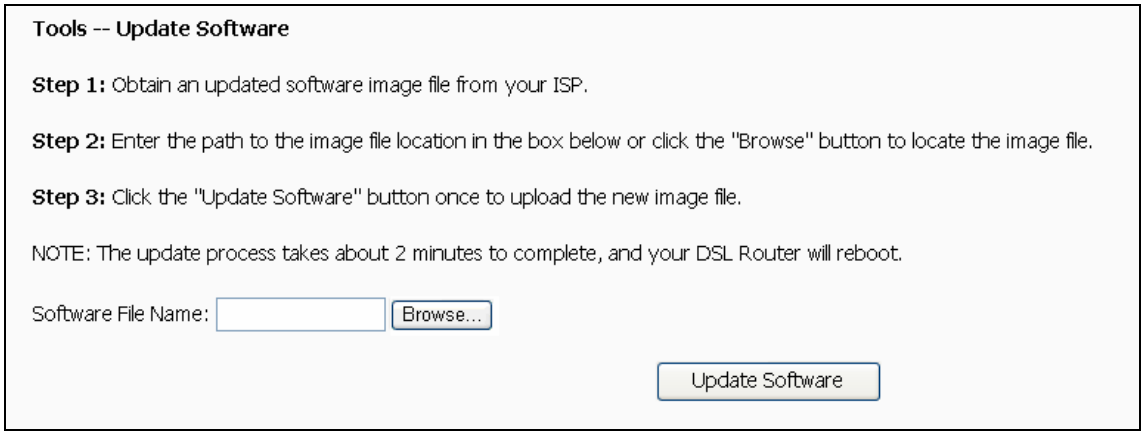


Figure 4-100

- Browse: Click the button to locate the latest software for the device.
- Update Firmware: 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 (http://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 Firmware button.

☞ **Note:**

1) There is no need to upgrade the firmware unless the new firmware has a new feature you want to use. However, when experiencing problems caused by the Router itself, you can try to upgrade the firmware.
2) Before upgrading the Router’s firmware, you should write down some of your customized settings to avoid losing important configuration settings of the Router.

3) Do not turn off the Router or press the Reset button while the software is being updated.

4) The Router will reboot after the Upgrading is finished.

4.8.8 Reboot

Choose “Management→Reboot”, you can see the screen (shown in Figure 4-101) which allows you to reboot the Router.

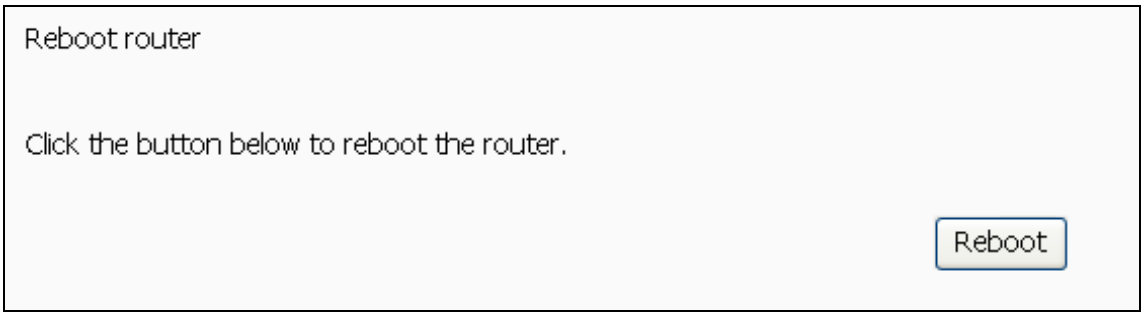


Figure 4-101

☞ **Note:**

1) After you clicked the Reboot button, please wait for a while before reopening your web browser.

2) Do not turn off the Router or press the Reset button while the Router is rebooting.

3) If necessary, reconfigure your PC's IP address to match your new configuration.

Appendix A: FAQ

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

1) First, configure the ADSL Modem configured in RFC1483 bridge model.
2) Connect the Ethernet cable from your ADSL Modem to the WAN port on the Router. The telephone cord plugs into the Line port of the ADSL Modem.
3) Log in to the Router, and configure the WAN connection type as PPPoE connection mode. The detailed steps please refer to section 4.5.1.
4) If your ADSL lease is in “pay-according-time” mode, select “Dial on Demand” for Internet connection mode.

☞ **Note:**

If you are a Cable user, please configure the Router following the above steps.

2. The wireless stations cannot connect to the Router.

1) Make sure the "Enable Wireless Router Radio" is checked.
2) Make sure that the wireless stations' SSID accord with the Router's SSID.
3) Make sure the wireless stations have right KEY for encryption when the Router is encrypted.
4) If the wireless connection is ready, but you can’t access the Router, check the IP Address of your wireless stations.

Appendix B: Configuring the PC

In this section, we'll introduce how to install and configure the TCP/IP correctly in Windows XP. First make sure your Ethernet Adapter is working, refer to the adapter's manual if necessary.

1. Configure TCP/IP component

   1) On the Windows taskbar, click the Start button, and then click Control Panel.

   2) Click the Network and Internet Connections icon, and then click on the Network Connections tab in the appearing window.

   3) Right click the icon that showed below, select Properties on the prompt page.

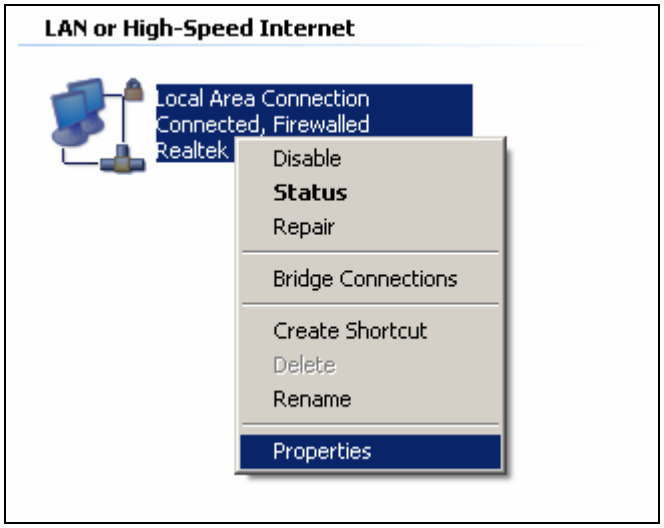


Figure 0-1

   4) In the prompt page that showed below, double click on the Internet Protocol (TCP/IP).

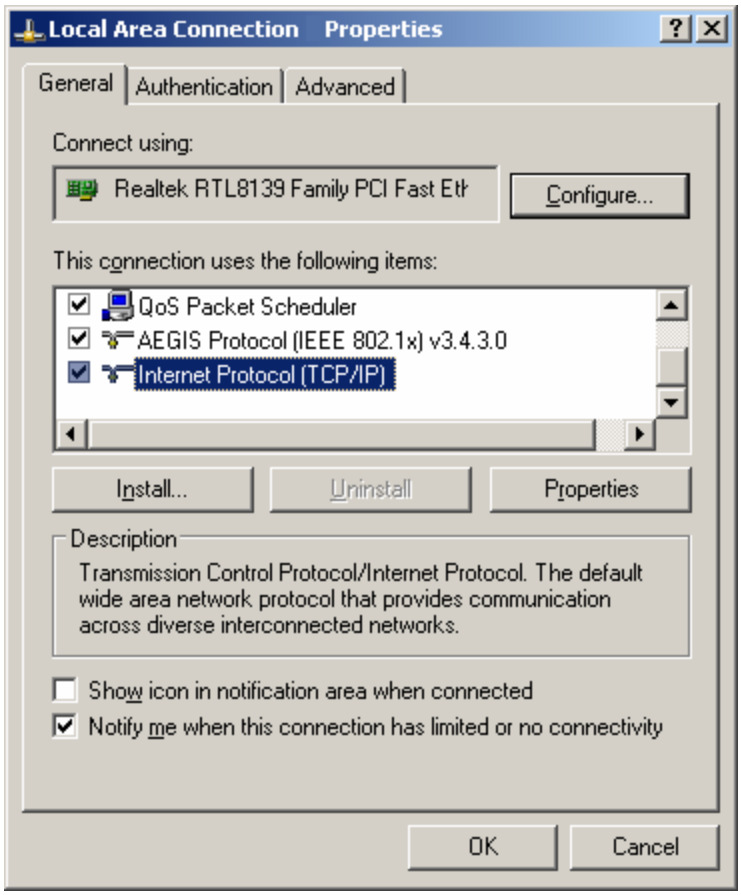


Figure 0-2

5) The following TCP/IP Properties window will display and the IP Address tab is open on this window by default.

Now you have two ways to configure the TCP/IP protocol below:

- Setting IP address automatically

Select Obtain an IP address automatically, Choose Obtain DNS server automatically, as shown in the Figure below:

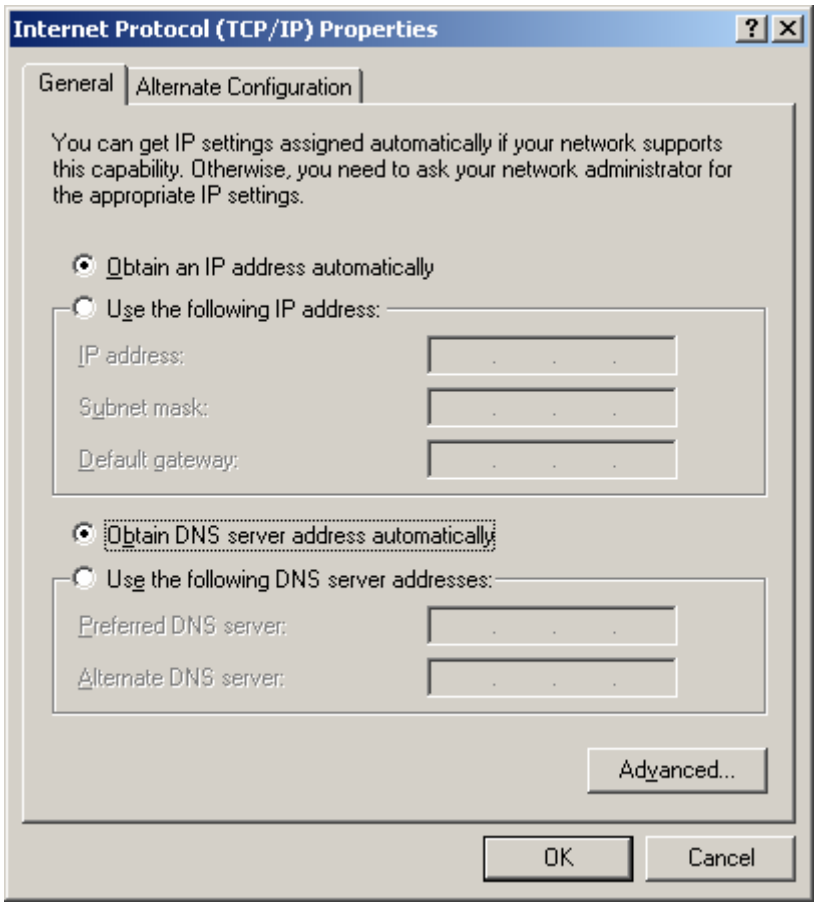


Figure 0-3

Note:

For Windows 98 OS or before, the PC and Router may need to be restarted.

➢ Setting IP address manually

1 Select Use the following IP address radio button. And the following items available.

2 If the Router's LAN IP address is 192.168.1.1, specify the IP address as 192.168.1.x (x is from 2 to 254), and the Subnet mask as 255.255.255.0.

3 Type the Router's LAN IP address (the default IP is 192.168.1.1) into the Default gateway field.

4 Select Use the following DNS server addresses. In the Preferred DNS Server field you can enter the same value as the Default gateway or type the local DNS server IP address.

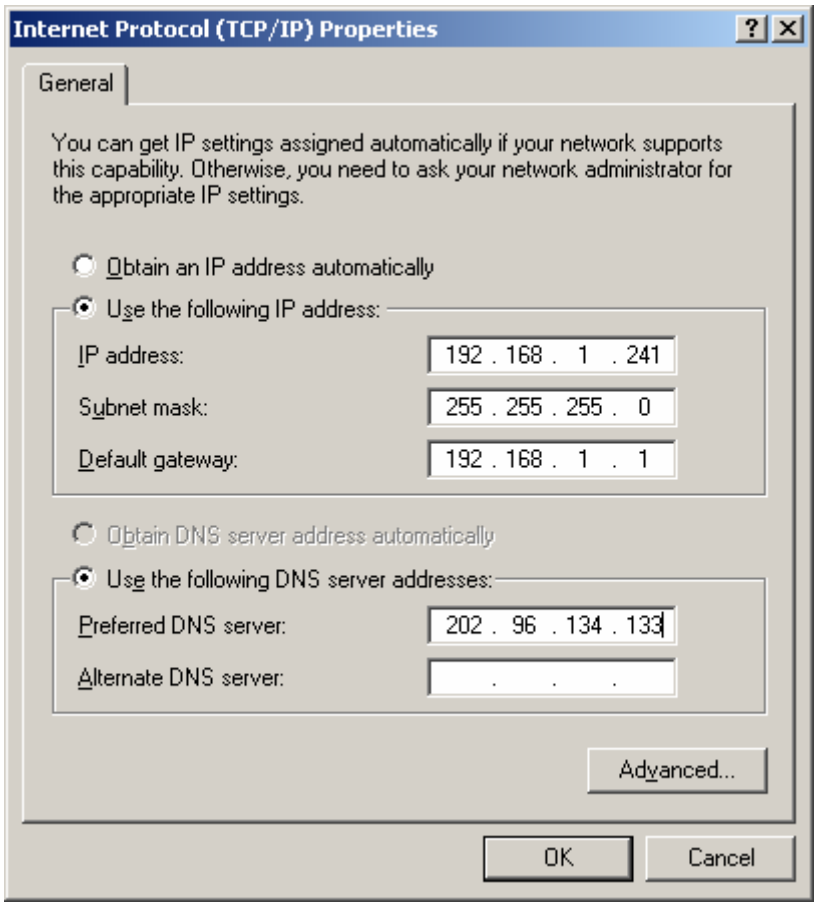


Figure 0-4

Now:

Click OK to keep your settings.

Appendix C: Specifications

General	
Standards	ANSI T1.413, ITU G.992.1, ITU G.992.2, ITU G.992.3, ITU G.992.5, IEEE 802.3, IEEE 802.3u, IEEE 802.11b , IEEE 802.11g , 802.11n
Protocols	TCP/IP, IPoA , PPPoA , PPPoE, SNTP, HTTP, DHCP, ICMP, NAT
Ports	LAN Ports: Four 10/100M Auto-Negotiation RJ45 ports（Auto MDI/MDIX)
	Line Ports: One RJ11 port
Cabling Type	10BASE-T: UTP category 3, 4, 5 cable (maximum 100m) EIA/TIA-568 100Ω STP (maximum 100m)
	100BASE-TX: UTP category 5, 5e cable (maximum 100m) EIA/TIA-568 100Ω STP (maximum 100m)
LED	1,2,3,4(LAN), WLAN, ADSL
	Power, Internet, QSS
Safety & Emissions	FCC, CE

Wireless	
Frequency Band	2.4~2.4835GHz
Radio Data Rate	11n: up to 150Mbps（Automatic） 11g: 54/48/36/24/18/12/9/6Mbps（Automatic） 11b: 11/5.5/2/1Mbps（Automatic）
Frequency Expansion	DSSS(Direct Sequence Spread Spectrum)
Modulation	DBPSK, DQPSK, CCK, OFDM, 16-QAM, 64-QAM
Security	WEP/WPA/WPA2/WPA2-PSK/WPA-PSK
Sensitivity @PER	130M: -68dBm@10% PER 108M: -68dBm@10% PER; 54M: -68dBm@10% PER 11M: -85dBm@8% PER; 6M: -88dBm@10% PER 1M: -90dBm@8% PER

Environmental and Physical		
Temperature.	Operating:	0℃~40℃ (32℉~104℉)
	Storage:	-40℃~70℃(-40℉~158℉)
Humidity	Operating:	10% ~ 90% RH, Non-condensing
	Storage:	5% ~ 90% RH, Non-condensing

Appendix D: Glossary

- 802.11n - 802.11n builds upon previous 802.11 standards by adding MIMO (multiple-input multiple-output). MIMO uses multiple transmitter and receiver antennas to allow for increased data throughput via spatial multiplexing and increased range by exploiting the spatial diversity, perhaps through coding schemes like Alamouti coding. The Enhanced Wireless Consortium (EWC) [3] was formed to help accelerate the IEEE 802.11n development process and promote a technology specification for interoperability of next-generation wireless local area networking (WLAN) products.
- 802.11b - The 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. 802.11b networks are also referred to as Wi-Fi networks.
- 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 802.11b devices, and WEP encryption for security.
- 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 Encryption Standard) - A security method that uses symmetric 128-bit block data encryption.
- ACS (Auto-Configuration Server) - Through ACS (Auto-Configuration Server) you can perform auto-configuration, provision, collection, and diagnostics to the device.
- ATM (Asynchronous Transfer Mode) - 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 (Dynamic Domain Name System) - 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 (Demilitarized Zone) - Removes the Router's firewall protection from one PC, allowing it to be “seen” from the Internet.

- DNS (Domain Name Server) - 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 (Digital Subscriber Line) - An always-on broadband connection over traditional phone lines.
- Dynamic IP Address - A temporary IP address assigned by a DHCP server.
- EAP (Extensible Authentication Protocol) - 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 (Internet Service Provider) - A company that provides access to the Internet.
- LAN - The computers and networking products that make up your local network.
- MAC (Media Access Control) Address - The unique address that a manufacturer assigns to each networking device.
- NAT (Network Address Translation) - NAT technology translates IP addresses of a local area network to a different IP address for the Internet.
- MER (MAC Encapsulation Routing) - 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 (Packet Internet Groper) - 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 (Point to Point Protocol over Ethernet) - 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 Point Protocol 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 Authentication Dial-In User Service) - A protocol that uses an authentication server to control network access.
- RJ45 (Registered Jack-45) - An Ethernet connector that holds up to eight wires.
- Router - A networking device that connects multiple networks together.
- RPC (Remote Procedure Calls) - 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 Control Protocol) - A network protocol for transmitting data that requires acknowledgement from the recipient of data sent.
- TCP/IP (Transmission Control Protocol/Internet Protocol) - A set of instructions PCs use to communicate over a network.
- TKIP (Temporal Key Integrity Protocol) - 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 Channel Identifier) - The identifier of the VC contained in the ATM cell header.
- VPI (Virtual Path Identifier) - The identifier of the VP contained in the ATM cell header.
- Update - To replace existing software or firmware with a newer version.
- VLAN (Virtual Local Air Network) - 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 (Wide Area Network) - Networks that cover a large geographical area.
- Web-based Utility - The web page that allows you to manage the Router.
- WEP (Wired Equivalent Privacy) - 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 Local Area Network) - 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 Access) - A wireless security protocol use TKIP (Temporal Key Integrity Protocol) encryption, which can be used in conjunction with a RADIUS server.