USER MANUAL

DSL-2640B

VERSION 1.0

D-Link®

BROADBAND

Federal Communication Commission Interference 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 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, and (2) this device must accept any interference received, including interference that may cause undesired operation.

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

IMPORTANT NOTE:

FCC Radiation Exposure Statement:

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 20cm between the radiator & your body.

This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

IEEE 802.11b or 802.11g operation of this product in the U.S.A. is firmware-limited to channels 1 through 11.

Table of Contents

Before You Begin

Please read and make sure you understand all the prerequisites for proper installation of your new Router. Have all the necessary information and equipment on hand before beginning the installation.

Package Contents

- DSL-2640B ADSL Router
- Power Adapter
- CD-ROM with User Manual
- One twisted-pair telephone cable used for ADSL connection
- One straight-through Ethernet cable
- One Quick Installation Guide

Warning: The Router must be used with the power adapter included with the device.

System Requirements

- ADSL Internet service

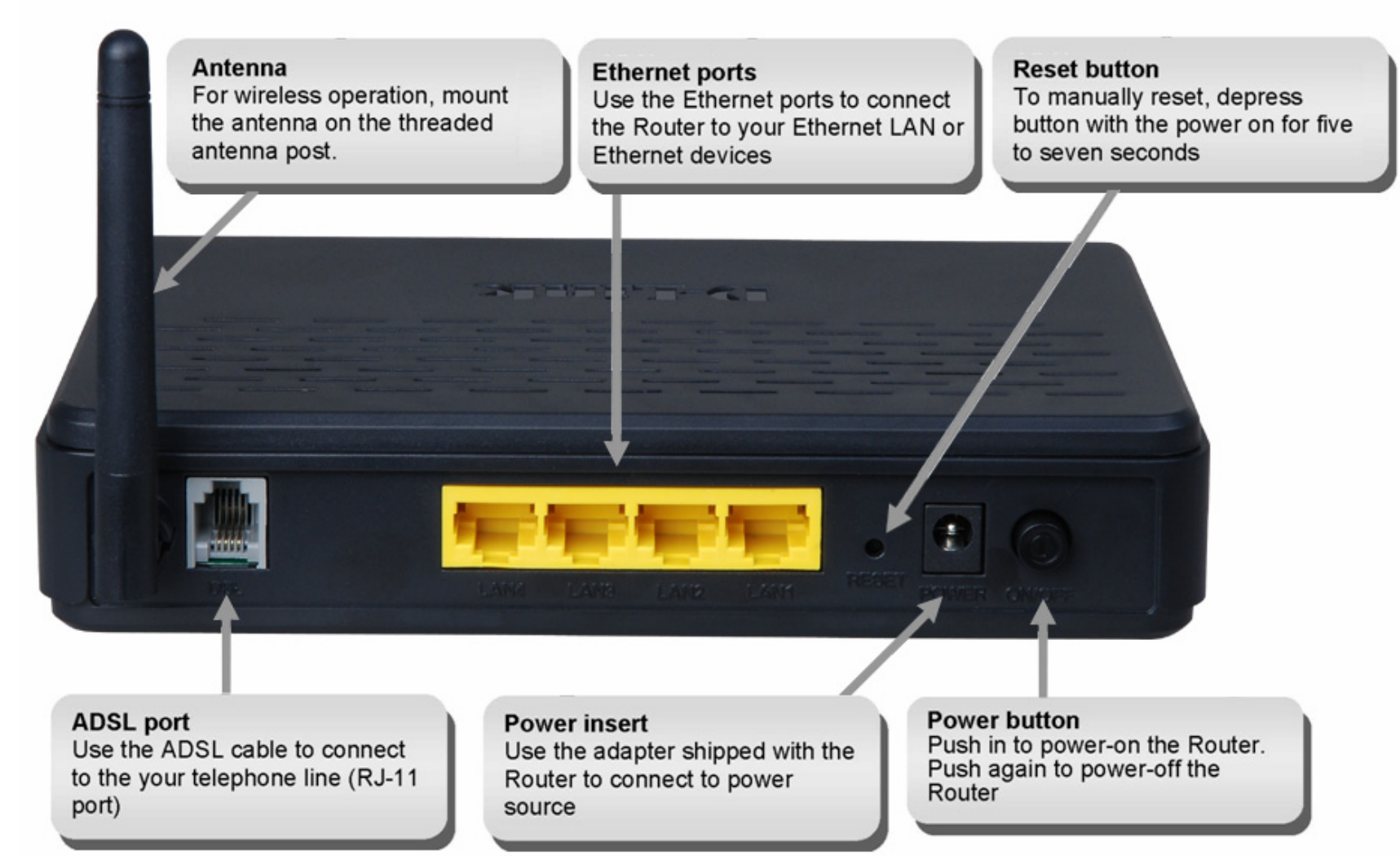
- Computer with:
  - 200 MHz Processor
  - 64MB Memory
  - CD-ROM Drive
  - Ethernet Adapter with TCP/IP Protocol Installed
  - Internet Explorer v6 or later, FireFox v1.5
  - Computer with Windows 2000, Windows XP, or Windows Vista

Features

- **PPP (Point-to-Point Protocol) Security –** The DSL-2640B ADSL Router supports PAP (Password Authentication Protocol) and CHAP (Challenge Handshake Authentication Protocol) for PPP connections. The Router also supports MSCHAP.
- **DHCP Support –** Dynamic Host Configuration Protocol automatically and dynamically assigns all LAN IP settings to each host on your network. This eliminates the need to reconfigure every host whenever changes in network topology occur.
- **Network Address Translation (NAT) –** For small office environments, the DSL-2640B allows multiple users on the LAN to access the Internet concurrently through a single Internet account. This provides Internet access to everyone in the office for the price of a single user. NAT improves network security in effect by hiding the private network behind one global and visible IP address. NAT address mapping can also be used to link two IP domains via a LAN-to-LAN connection.
- **TCP/IP (Transfer Control Protocol/Internet Protocol) –** The DSL-2640B supports TCP/IP protocol, the language used for the Internet. It is compatible with access servers manufactured by major vendors.
- **RIP-1/RIP-2 –** The DSL-2640B supports both RIP-1 and RIP-2 exchanges with other routers. Using both versions lets the Router to communicate with all RIP enabled devices.
- **Static Routing –** This allows you to select a data path to a particular network destination that will remain in the routing table and never “age out”. If you wish to define a specific route that will always be used for data traffic from your LAN to a specific destination within your LAN (for example to another router or a server) or outside your network (to an ISP defined default gateway for instance).
- **Default Routing –** This allows you to choose a default path for incoming data packets for which the destination address is unknown. This is particularly useful when/if the Router functions as the sole connection to the Internet.
- **Precise ATM Traffic Shaping –** Traffic shaping is a method of controlling the flow rate of ATM data cells. This function helps to establish the Quality of Service for ATM data transfer.
- **Full Network Management –** The DSL-2640B incorporates SNMP (Simple Network Management Protocol) support for web-based management and text-based network management.
- **Easy Installation –** The DSL-2640B uses a web-based graphical user interface program for convenient management access and easy set up. Any common web browser software can be used to manage the Router.

Hardware Overview

Connections



LED Indicators

Front Panel

Side Panel

LED	Color	Status	Description
Power	Green	Off	Power not supplied.
		On	Power supplied.
	Red	On	Not bootable or device is malfunction.
LAN 1/2/3/4	Green	Off	No LAN link.
		Blink	Data is being transmitted through the LAN interface.
		On	LAN link is established and active.
WLAN	Green	Off	WLAN is disabled.
		Blink	WLAN traffic is flowing.
		On	WLAN link is established.
DSL	Green	Off	DSL line is disconnected.
		Blink	DSL line is training.
		On	DSL line is connected.
Internet	Green	Off	The device is under the Bridge mode, DSL connection is not present, or the power is off.
		Blink	DSL traffic is flowing.
		On	IP is connected.
	Red	On	The device is attempted to become IP connected, but failed.
WPS (on the side panel)	Blue	Off	Device is ready for new WPS to setup.
		Blink	WPS is successfully triggered
		On	Connection is successfully established between the router and the client, the LED would remain in solid light for 5s.

Installation

This section will walk you through the installation process. Placement of the Wireless ADSL Router is very important. Do not place the Router in an enclosed area such as a closet, cabinet, or in the attic or garage. Place the Wireless ADSL Router in a location where it can be easily connected to Ethernet devices, the telephone line as well as to a power source.

Mounting the Device on the Wall

Step 1 There are two slots on the device bank. Install two screws on the wall according to the positions of the slots. Keep the two screws at the same horizontal level.
Step 2 Gently fasten the two slots with the screws.
Step 3 Slowly take your hands off the device. Ensure that the device is properly mounted on the wall with the support of the screws.

See the following figure:

Installation Notes

In order to establish a connection to the Internet it will be necessary to provide information to the Router that will be stored in its memory. For some users, only their account information (Username and Password) is required. For others, various parameters that control and define the Internet connection will be required. You can print out the two pages below and use the tables to list this information. This way you have a hard copy of all the information needed to setup the Router. If it is necessary to reconfigure the device, all the necessary information can be easily accessed. Be sure to keep this information safe and private.

Low Pass Filters
Since ADSL and telephone services share the same copper wiring to carry their respective signals, a filtering mechanism may be necessary to avoid mutual interference. A low pass filter device can be installed for each telephone that shares the line with the ADSL line. These filters are easy to install passive devices that connect to the ADSL device and/or telephone using standard telephone cable. Ask your service provider for more information about the use of low pass filters with your installation.

Operating Systems
The DSL-2640B uses an HTML-based web interface for setup and management. The web configuration manager may be accessed using any operating system capable of running web browser software, including Windows 98 SE, Windows ME, Windows 2000, Windows XP, and Windows Vista.

Web Browser
Any common web browser can be used to configure the Router using the web configuration management software. The program is designed to work best with more recently released browsers such as Opera, Microsoft Internet Explorer® version 6.0, Netscape Navigator® version 6.2.3, or later versions. The web browser must have JavaScript enabled. JavaScript is enabled by default on many browsers. Make sure JavaScript has not been disabled by other software (such as virus protection or web user security packages) that may be running on your computer.

Ethernet Port (NIC Adapter)
Any computer that uses the Router must be able to connect to it through the Ethernet port on the Router. This connection is an Ethernet connection and therefore requires that your computer be equipped with an Ethernet port as well. Most notebook computers are now sold with an Ethernet port already installed. Likewise, most fully assembled desktop computers come with an Ethernet NIC adapter as standard equipment. If your computer does not have an Ethernet port, you must install an Ethernet NIC adapter before you can use the Router. If you must install an adapter, follow the installation instructions that come with the Ethernet NIC adapter.

Additional Software
It may be necessary to install software on your computer that enables the computer to access the Internet. Additional software must be installed if you are using the device as a simple bridge. For a bridged connection, the information needed to make and maintain the Internet connection is stored on another computer or gateway device, not in the Router itself.

If your ADSL service is delivered through a PPPoE or PPPoA connection, the information needed to establish and maintain the Internet connection can be stored in the Router. In this case, it is not necessary to install software on your computer. It may however be necessary to change some settings in the device, including account information used to identify and verify the connection.

All connections to the Internet require a unique global IP address. For bridged connections, the global IP settings must reside in a TCP/IP enabled device on the LAN

side of the bridge, such as a PC, a server, a gateway device such as a router or similar firewall hardware. The IP address can be assigned in a number of ways. Your network service provider will give you instructions about any additional connection software or NIC configuration that may be required.

Wireless LAN
Computers using the Wireless network can access the Internet or use the embedded 802.1g wireless access point. Wireless workstations must have an 802.1g or 802.1b wireless network card installed to use the Wireless ADSL Router. In addition the workstations must be configured to operate on the same channel and SSID as the Wireless ADSL Router. If wireless security is used, the wireless workstations must be properly configured for the security settings used.

Information you will need from your ADSL service provider

Username
This is the Username used to log on to your ADSL service provider's network. Your ADSL service provider uses this to identify your account.

Password
This is the Password used, in conjunction with the Username above, to log on to your ADSL service provider's network. This is used to verify the identity of your account.

WAN Setting / Connection Type
These settings describe the method your ADSL service provider uses to transport data between the Internet and your computer. Most users will use the default settings. You may need to specify one of the following WAN Setting and Connection Type configurations (Connection Type settings listed in parenthesis):

- PPPoE/PPPoA (PPPoE LLC, PPPoE VC-Mux, PPPoA LLC or PPPoA VC-Mux)
- Dynamic IP Address (1483 Bridged IP LLC, 1483 Bridged IP VC-Mux)
- Static IP Address (1483 Bridged IP LLC, 1483 Bridged IP VC-Mux, 1483 Routed IP LLC (IPoA) or 1483 Routed IP VC-Mux)
- Bridge Mode (1483 Bridged IP LLC or 1483 Bridged IP VC Mux)

Modulation Type
ADSL uses various standardized modulation techniques to transmit data over the allotted signal frequencies. Some users may need to change the type of modulation used for their service. The default DSL modulation (Auto Synch-Up) used for the Router automatically detects all types of ADSL, ADSL2, and ADSL2+ modulation.

Security Protocol
This is the method your ADSL service provider will use to verify your Username and Password when you log on to their network. Your Router supports the PAP and CHAP protocols.

VPI
Most users will not be required to change this setting. The Virtual Path Identifier (VPI) is used in conjunction with the Virtual Channel Identifier (VCI) to identify the data path between your ADSL service provider's network and your computer. If you are setting up the Router for multiple virtual connections, you will need to configure the VPI and VCI as instructed by your ADSL service provider for the additional connections. This setting can be changed in the WAN Settings window of the web management interface.

VCI
Most users will not be required to change this setting. The Virtual Channel Identifier (VCI) used in conjunction with the VPI to identify the data path between your ADSL service provider's network and your computer. If you are setting up the Router for multiple virtual connections, you will need to configure the VPI and VCI as instructed by your ADSL service provider for the additional connections. This setting can be changed in the WAN Settings window of the web management interface.

Information you will need about DSL-2640B

Username
This is the Username needed to access the Router's management interface. When you attempt to connect to the device through a web browser you will be prompted to enter this Username. The default Username for the Router is "**admin**." The user cannot change this.

Password
This is the Password you will be prompted to enter when you access the Router's management interface. The default Password is "**tot**." The user may change this.

LAN IP addresses for the DSL-2640B
This is the IP address you will enter into the Address field of your web browser to access the Router's configuration graphical user interface (GUI) using a web browser. The default IP address is 192.168.1.1. This may be changed to suit any IP address scheme the user desires. This address will be the base IP address used for DHCP service on the LAN when DHCP is enabled.

LAN Subnet Mask for the DSL-2640B
This is the subnet mask used by the DSL-2640B, and will be used throughout your LAN. The default subnet mask is 255.255.255.0. This can be changed later.

Information you will need about your LAN or computer:

Ethernet NIC
If your computer has an Ethernet NIC, you can connect the DSL-2640B to this Ethernet port using an Ethernet cable. You can also use the Ethernet ports on the DSL-2640B to connect to other computer or Ethernet devices.

DHCP Client status
Your DSL-2640B ADSL Router is configured, by default, to be a DHCP server. This means that it can assign an IP address, subnet mask, and a default gateway address to computers on your LAN. The default range of IP addresses the DSL-2640B will assign are from 192.168.1.2 to 192.168.1.254. Your computer (or computers) needs to be configured to obtain an IP address automatically (that is, they need to be configured as DHCP clients.)

It is recommended that you collect and record this information here, or in some other secure place, in case you have to re-configure your ADSL connection in the future.

Once you have the above information, you are ready to setup and configure your DSL-2640B ADSL Router.

Device Installation

The Wireless ADSL Router maintains three separate interfaces, an ADSL, an Ethernet, and a Wireless LAN interface. Place the Wireless ADSL Router in a location where it can be easily connected to Ethernet devices, the telephone line as well as to a power source.

The Router can be placed on a shelf or desktop, ideally you should be able to see the LED indicators on the front if you need to view them for troubleshooting.

Power on Router

The Router must be used with the power adapter included with the device.

1. Connect the power adapter to the **Power Input** (12V DC, 1A) on the back panel of the Wireless ADSL Router and plug the other end of the power adapter to a wall outlet or power strip.
2. Push the **Power Button** to turn the power on.
3. The **Power** LED on the front panel will shine bright green to indicate the device is powered on.
4. If the Ethernet port is connected to a working device, check the **LAN** LED indicator to make sure the connection is valid. The Wireless ADSL Router will attempt to establish the ADSL connection, if the ADSL line is connected and the Wireless ADSL Router is properly configured the **ADSL** LED will light up after several seconds. If this is the first time installing the device, some settings may need to be changed before the Wireless ADSL Router can establish a connection.

Factory Reset Button

The Router may be reset to the original factory default settings by using a ballpoint or paperclip to gently push down the reset button in the following sequence:

1. With the router powered on (check the Power LED to make sure it lights steady green), press and hold down the reset button using a paper clip or similar object for about 6 to 8 seconds.
2. The router will restart. Watch the Power LED to verify that it is restarting.
3. When it is powered on again it is ready to be configured. The whole process takes about 30 seconds.
4. The device settings will be restored to the factory default IP address **192.168.1.1** and the subnet mask is **255.255.255.0**, the default management Username is “admin” and the default Password is “tot.”

Note: *A factory reset will erase the current configuration settings and reset them to the default settings. After it has restarted, log in to the router’s web-based management interface and use the Setup Wizard to configure the basic settings.*

Network Connections

Connect ADSL Line
Use the ADSL cable included with the Router to connect it to a telephone wall socket or receptacle. Plug one end of the cable into the ADSL port (RJ-11 receptacle) on the rear panel of the Router and insert the other end into the RJ-11 wall socket. If you are using a low pass filter device, follow the instructions included with the device or given to you by your service provider. The ADSL connection represents the WAN interface, the connection to the Internet. It is the physical link to the service provider's network backbone and ultimately to the Internet.

Connect Router to Ethernet
The Router may be connected to a single computer or Ethernet device through the 10/100BASE-TX Ethernet port on the rear panel. Any connection to an Ethernet concentrating device such as a switch or hub must operate at a speed of 10/100 Mbps only. When connecting the Router to any Ethernet device that is capable of operating at speeds higher than 10Mbps, be sure that the device has auto-negotiation (NWay) enabled for the connecting port. Use standard twisted-pair cable with RJ-45 connectors. The RJ-45 port on the Router is a crossed port (MDI-X). Follow standard Ethernet guidelines when deciding what type of cable to use to make this connection. When connecting the Router directly to a PC or server use a normal straight-through cable. You should use a crossed cable when connecting the Router to a normal (MDI-X) port on a switch or hub. Use a normal straight-through cable when connecting it to an uplink (MDI-II) port on a hub or switch. The rules governing Ethernet cable lengths apply to the LAN to Router connection. Be sure that the cable connecting the LAN to the Router does not exceed 100 meters.

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

Computer to Router Connection
You can connect the Router directly to a 10/100BASE-TX Ethernet adapter card (NIC) installed on a PC using the Ethernet cable provided.

Wireless Connection to Router
The Router's embedded 802.11g wireless access point should be configured to suit the local wireless network. All 802.11g or 802.11b devices that associate with the Router's wireless access point must have the same SSID and channel. If wireless security is used, the wireless clients must be configured with the correct security information to use the Router. More information on configuring the wireless settings is found later in this manual.

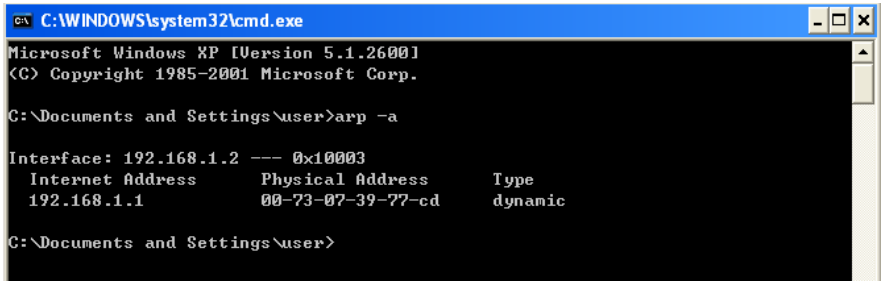
Introduction to Web Configuration

The first time you setup the Router. It is recommended that you configure the WAN connection using a single computer, to ensure that both the computer and the Router are not connected to the LAN. Once the WAN connection operates properly, you may continue to make changes to Router configuration, including IP settings and DHCP setup. This chapter is concerned with using your computer to configure the WAN connection. The following chapter describes the various menus used to configure and monitor the Router, including how to change IP settings and DHCP server setup.

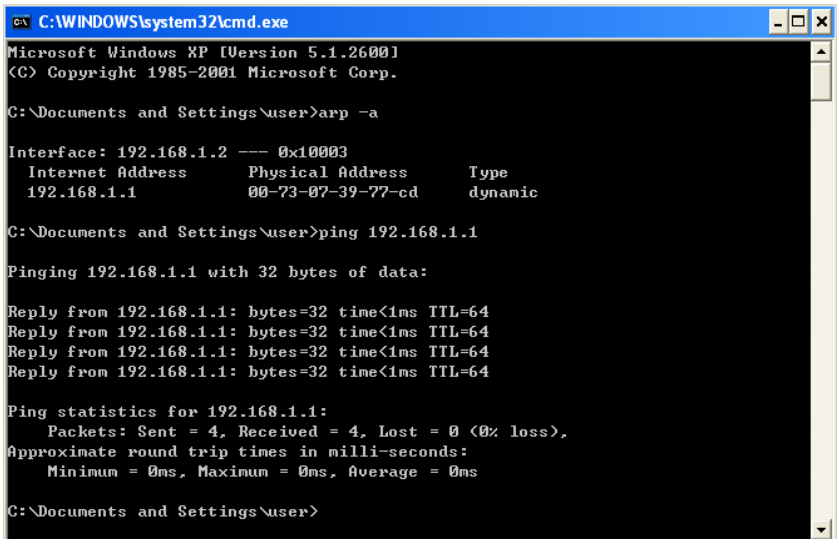
Preparation Before Login

Before accessing the Modem, ensure the communication between PC and Modem is normal. Check the communication as follows.

- Configure the IP address of the PC as 192.168.1.X (2~254), net mask as 255.255.255.0, gateway address as 192.168.1.1 (for customized version, configure them according to the actual version).
- Enter **arp -a** in the DOS window to check whether the PC can read the MAC address of the Modem.



- Ping the management IP address (192.168.1.1 by default) of the Modem. If the PC can read the MAC address of the Modem and can ping through the management IP address of the Modem, that means the communication of the PC and the Modem is normal.



Note: When you manage the Modem through Web, you must keep the Modem power on. Otherwise, the Modem may be damaged.

Logging In to the Modem

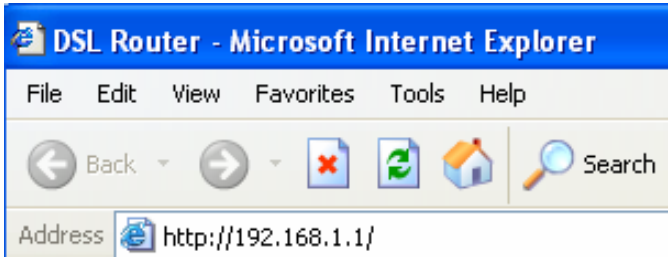
The following description is a detail “How-To” user guide and is prepared for first time users.

First-Time Login

When you log in to the DSL Router for the first time, the login wizard appears.

Step 1 Open a Web browser on your computer.

Step 2 Enter **http://192.168.1.1** (DSL router default IP address) in the address bar. The login page appears.



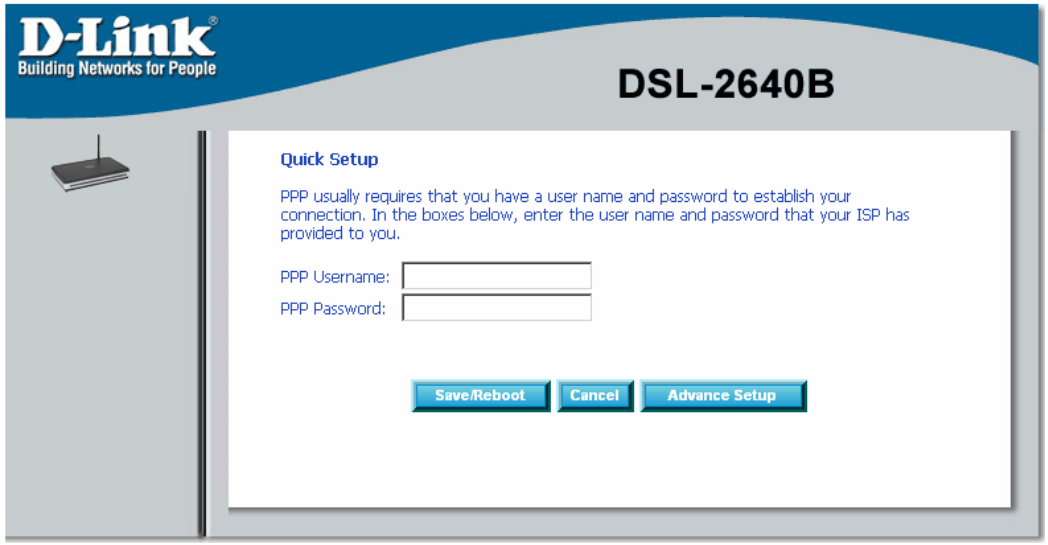
Step 3 Enter a user name and the password. The default username and password are **admin** and **tot**. You need not enter the username and password again if you select the option **Remember my password**. It is recommended to change these default values after logging in to the DSL router for the first time.

Step 4 Click **OK** to log in or click **Cancel** to exit the login page.

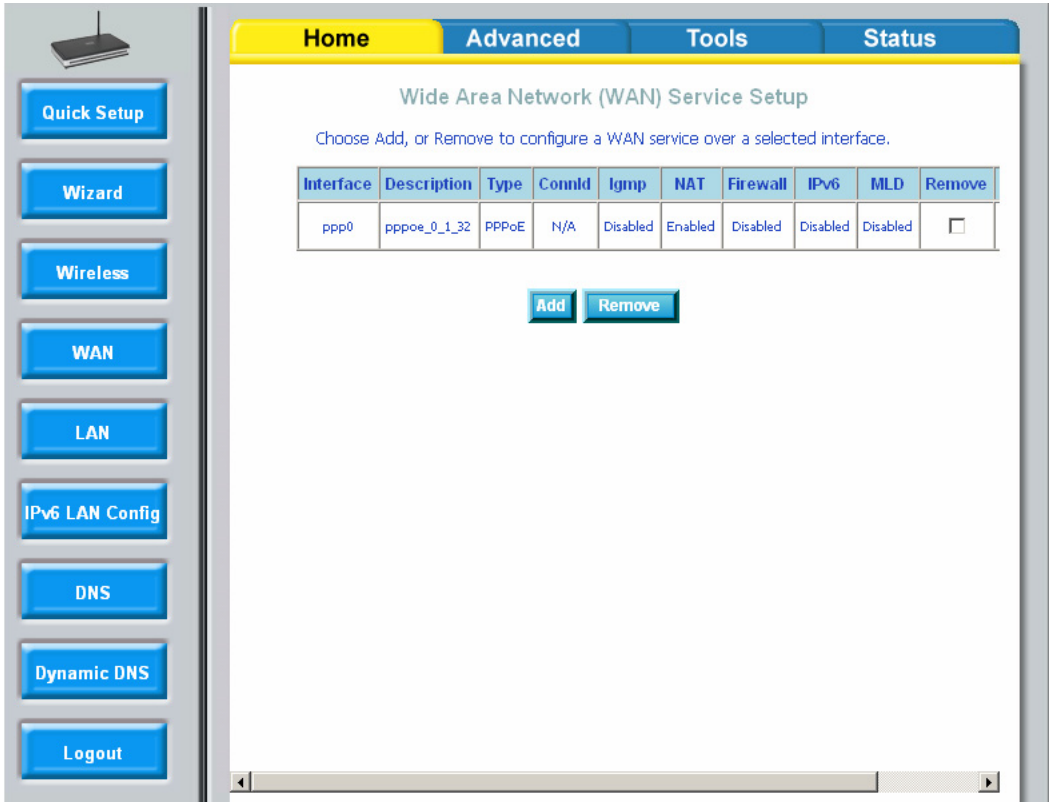
After logging in to the DSL router as a super user, you can query, configure, and modify all configurations, and diagnose the system.

You need to reboot the DSL router to enable your modification or configuration effective in some cases, for example, after you modify the PVC configuration. Some modification, such as adding a static route, takes effect at once, and does not require modem reboot.

After login into the Router, the page shown in the figure appears. In this page, please type “PPP Username” and “PPP Password” provided by your ISP for PPPoE connection.
Click “Save/Reboot” to take the settings into effect.
Click “Cancel” to cancel the configuration.
Note: *If you have not configure the PPP connection, the system will remind you.*



Click “Advance Setup” to login into the home page.
In the left pane, click “**Quick Setup**” to return to the above page.

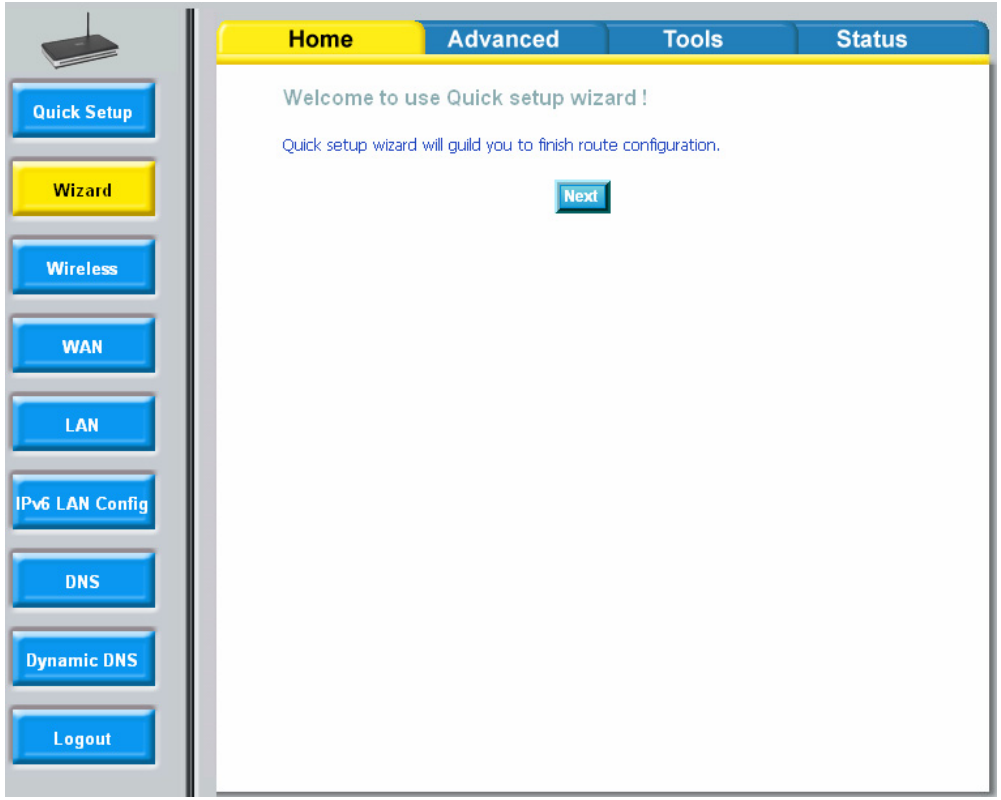


Home Configuration

Wizard

This chapter is concerned with using your computer to configure the WAN connection of IP v4.

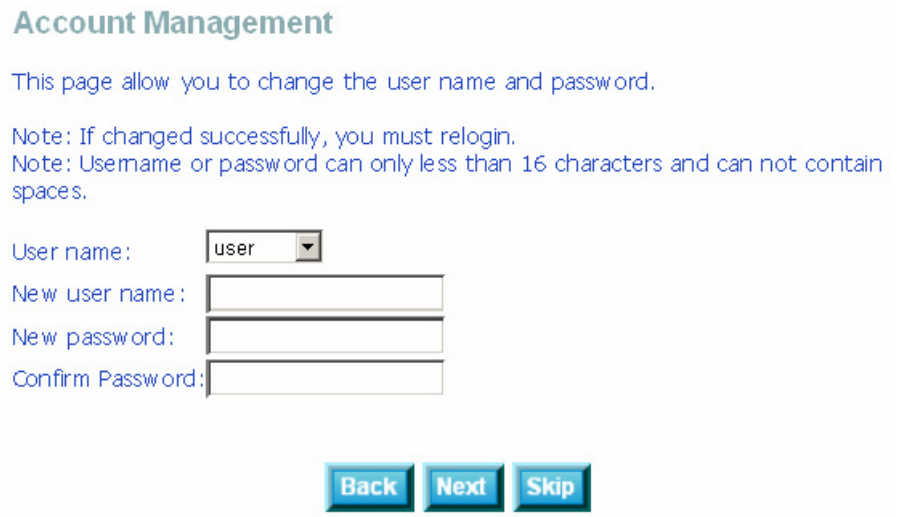
Choose **Home** > **Wizard**, the right page appears.



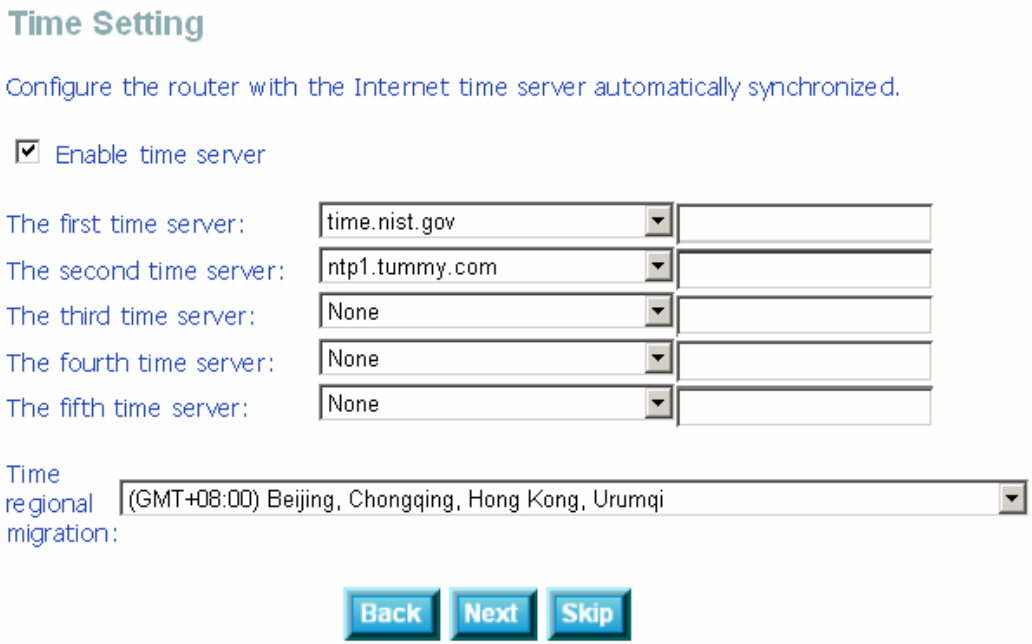
Click **Next**, the right page appears. In this page, there are two users of **user** and **admin**, you can select from the drop-down list. Then you can change the user name and password.

***Note**: If you change the user name and password successfully, you need to relogin. The user name or password can only be less than 16 characters.*

To ignore the step, click **Skip**.

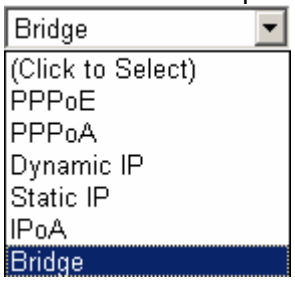


After proper configuration, the right page appears. In this page, you can set the Internet time.
To ignore the step, click **Skip**.



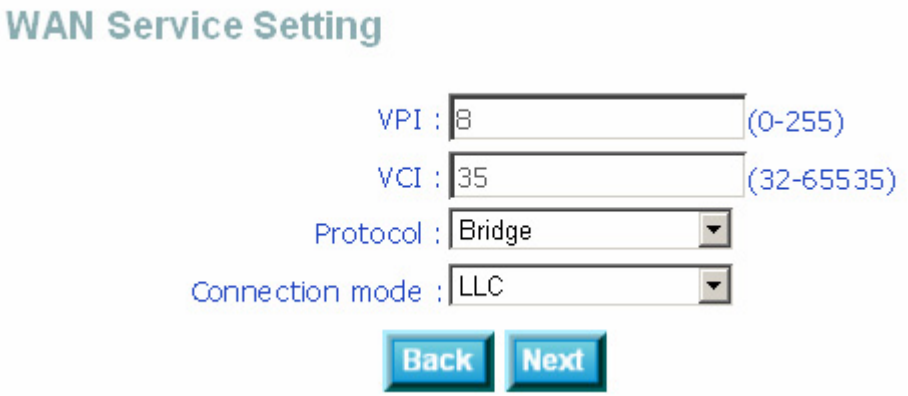
After proper configuration, the right page appears. In this page, you can set the WAN service.

You can select the protocol from the drop-down list:



If you select the **Bridge**, the page is as the right page. Enter the VPI and VCI, then select the connection mode.

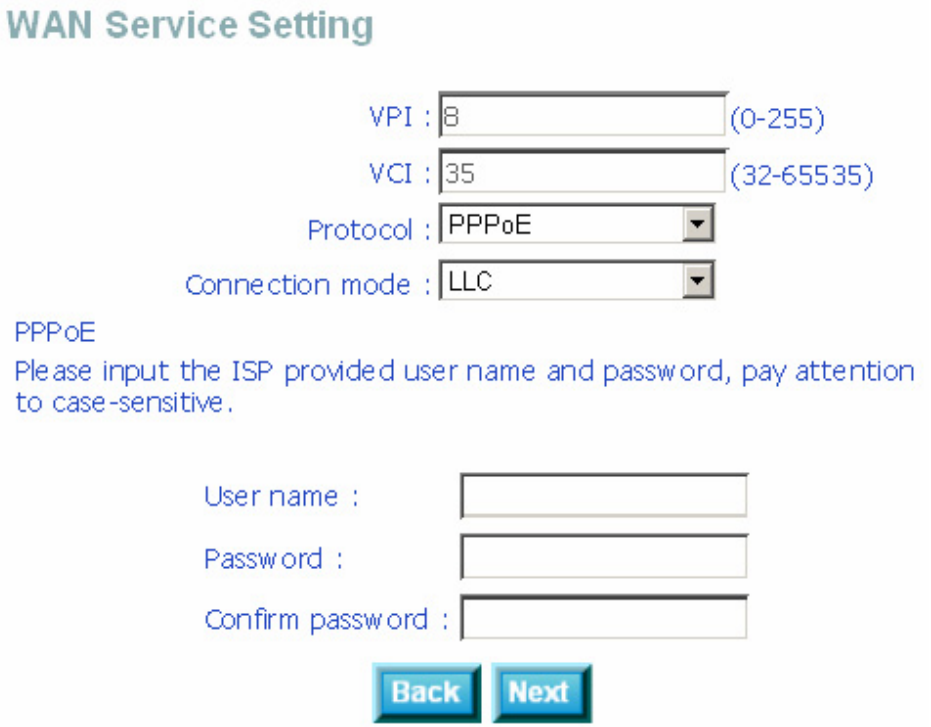
- VPI: The virtual path between two points in an ATM network, ranging from 0 to 255.
- VCI: The virtual channel between two points in an ATM network, ranging from 32 to 65535 (1 to 31 are reserved for known protocols)
- Connection mode: You can choose **LLC** and **VC-Mux**.



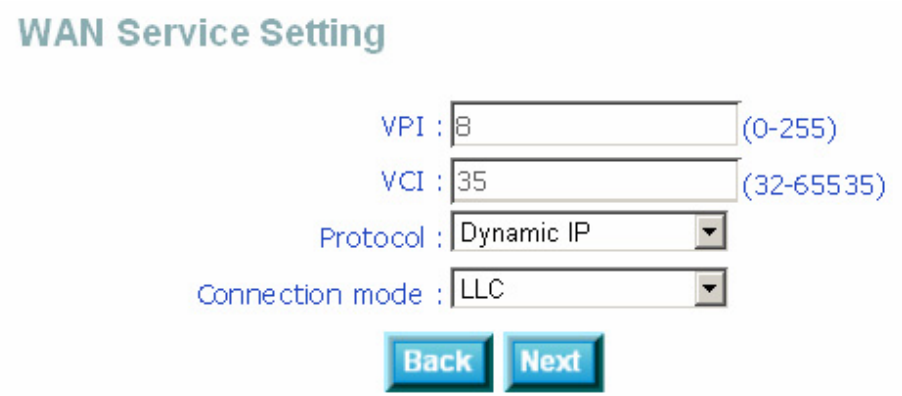
If you select **PPPoE** or **PPPoA** as the protocol, the right page appears.

Your ISP should provide you with the following information:

- PPP Username
- PPP Password

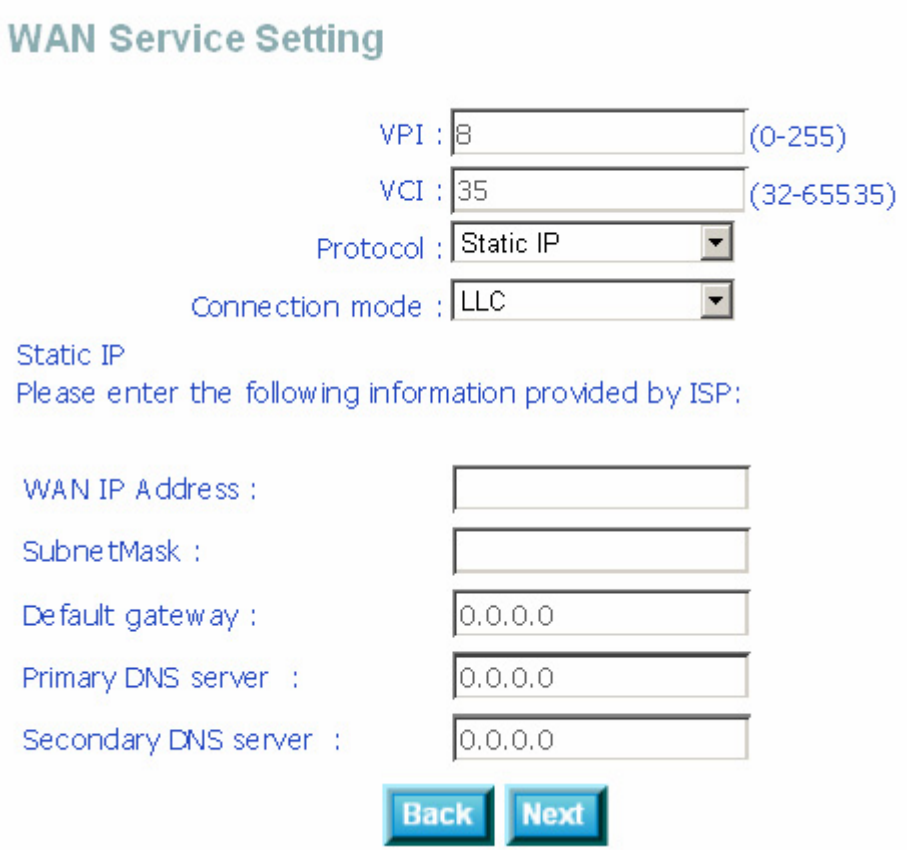


If you select **Dynamic IP** as the protocol, the right page appears.



If you select **Static IP** or **IPoA** as the protocol, the right page appears.
Your ISP should provide you with the following information:

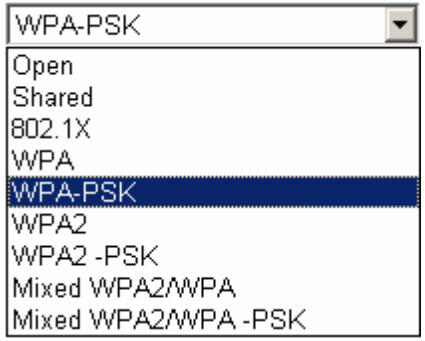
- WAN IP Address
- SubnetMask
- Default gateway
- Primary DNS server
- Secondary DNS server



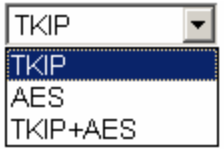
After the WAN service configuration, click Next and the right page appears. In this page, the wireless is enabled by default.

You can set the **SSID**, **WPA Pre-Shared Key**, and **WPA update session Key interval**.

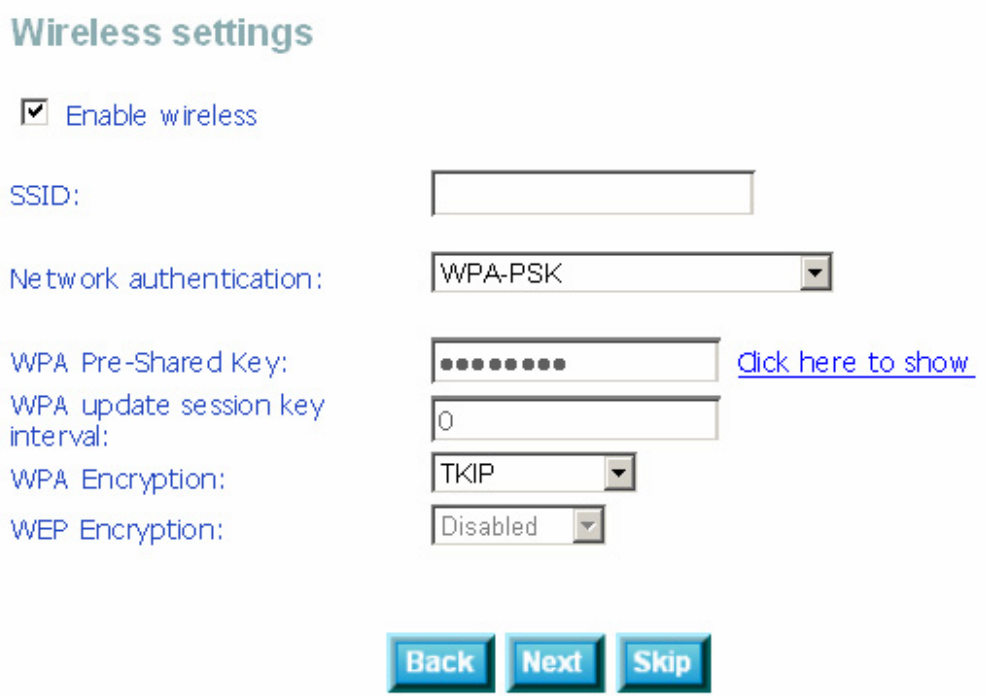
You can select the Network authentication from the drop-down list.



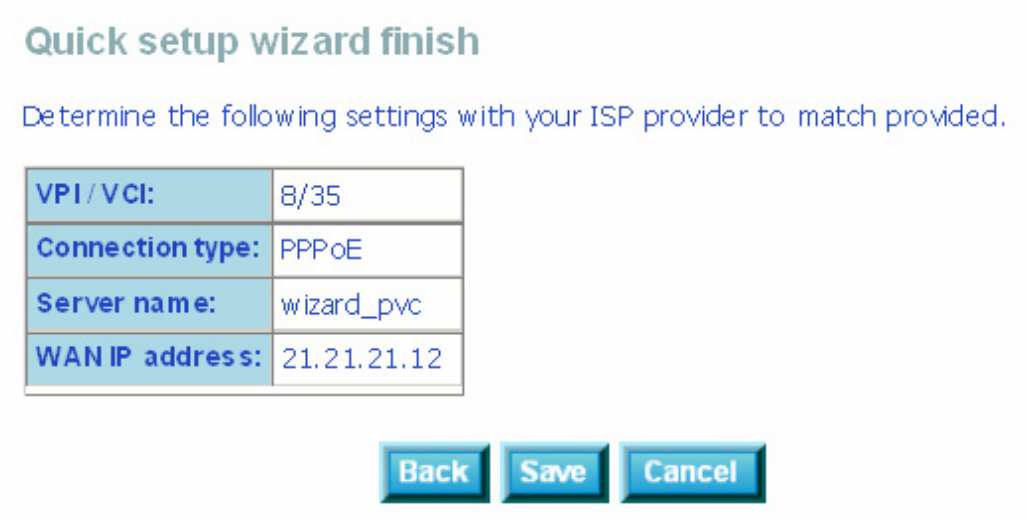
You can select the WPA Encryption from the drop-down list.



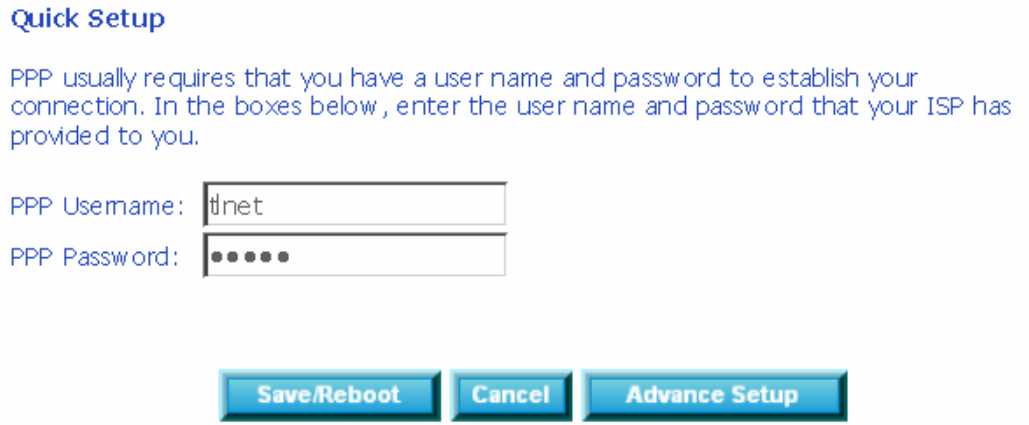
To ignore the step, click **Skip**.



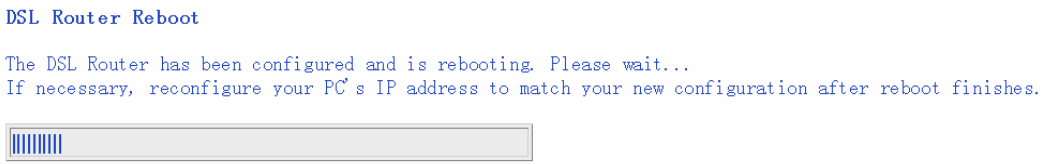
After the proper wireless settings, the quick setup wizard is finished and the right page appears. Check weather the settings match the settings provided by your ISP.



Then it turns to the quick setup page. The quick setup interface is available for the current PVC.
Click **Save/Reboot** to take the settings into effect.
Click **Cancel** to cancel the configuration.
Click **Advance Setup** to continue other settings.
Note: *If you have not configure the PPP connection, the system will remind you.*



Click **Save/Reboot**, the rebooting page appears.



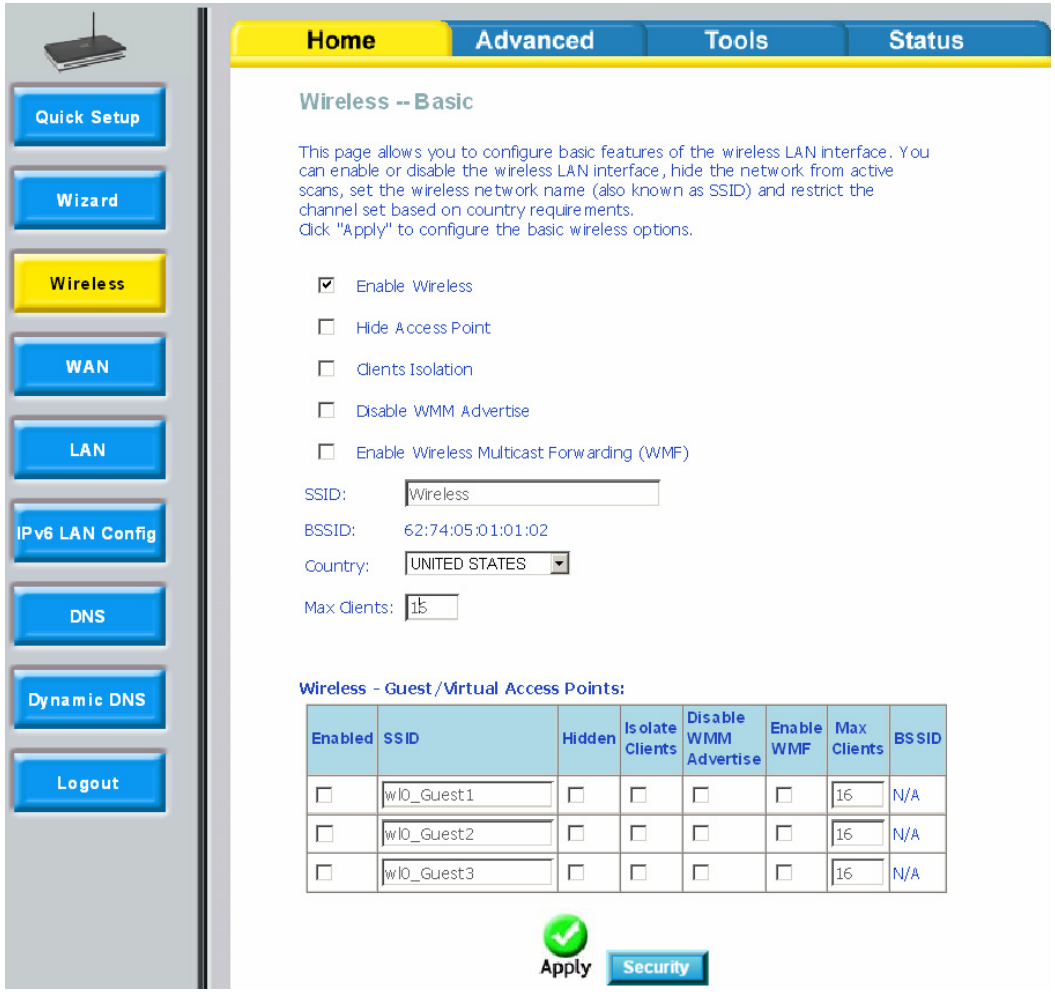
Basic Wireless Configuration

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

Following is a description of the different options:

- **Enable Wireless**: If you want to make wireless be available, you have to check this box first.
- **Hide Access Point**: Check this box if you want to hide any access point for your router, so a station cannot obtain the SSID through passive scanning.
- **Clients Isolation**: When many clients connect to the same access point, they can access each other. If you want to disable the access between clients which connect the same access point, you can check this box.
- **Disable WMM Advertise**: WMM is short for wi-fi multimedia, which can provide high-performance multimedia voice and video data transfers.
- **SSID**: The SSID (Service Set Identification) is the unique name shared among all devices in a wireless network. The SSID must be identical for all devices in the wireless network.
- **Country**: The channel will adjust according to nations to adapt to each nation's frequency provision.
- **Max Clients:** Specifies maximum wireless client stations to be enble to link with AP. Once the clients exceed the max vlaue, all other clients are refused. The value of maximum clients is 16.
- **Wireless - Guest/Virtual Access Points:** If you want to make Guest/Virtual network function be available, you have to check those boxes in the table below. In the current software version, three virtual access points can be configured.

Click **Apply** to save the basic wireless options and make the modification effect.



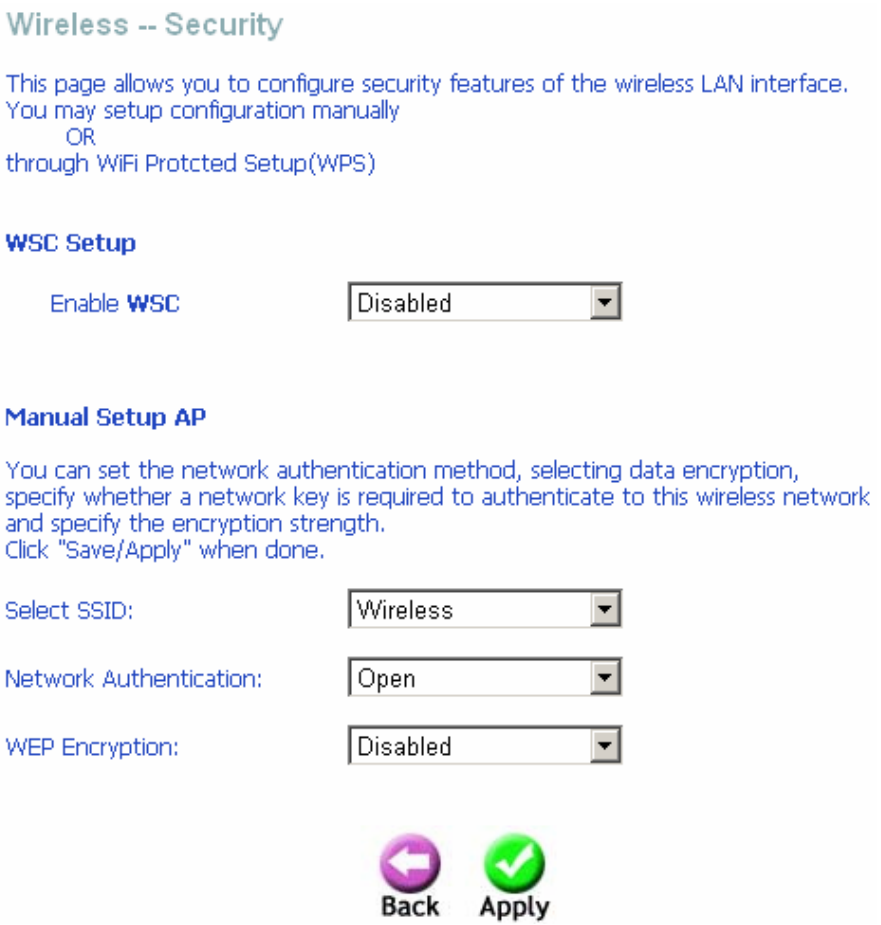
Click **Security** and the right page appears.

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

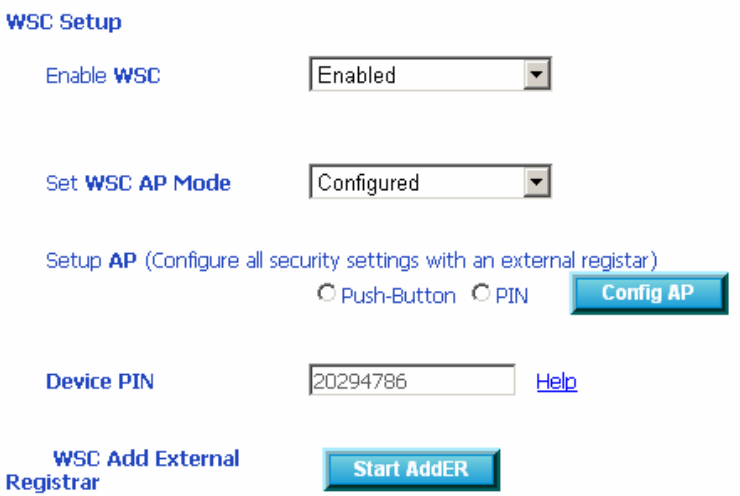
- **WSC Setup:** Wi-Fi Simple Config (WSC) is a new method for setting up residential Wi-Fi (802.11) networks with equal emphasis on security and ease-of-use.

This device is equipped with 802.1X and WPA/WPA2, the latest security standard. It also supports the legacy security standard, that is, WEP. By default, wireless security is disabled and authentication is open. Before enabling the security, consider your network size, complexity, and existing authentication infrastructure and then determine which solution applies to it.

- **Select SSID:** Select the wireless LAN of SSID to configure security features.
- **Network Authentication:** Select the authentication mode for the selected wireless LAN of SSID to be open.
- **WEP Encryption:** Disable WEP Encryption.



- **Enable WSC:** If enable **Manual Setup AP**, you can not enable WSC.
- **Set WSC AP Mode:** If selected Unconfigured, you need to add Client (This feature is available only when WPA-PSK, WPA2 PSK or OPEN mode is configured.), and setup AP (Configure all security settings with an external registar).
- **Device PIN:** Device Pin is generated by AP.
- **WSC Add External Registrar:** If set WSC AP Mode to Configured, this part will show, and you can add external registrar.



Manual Setup AP

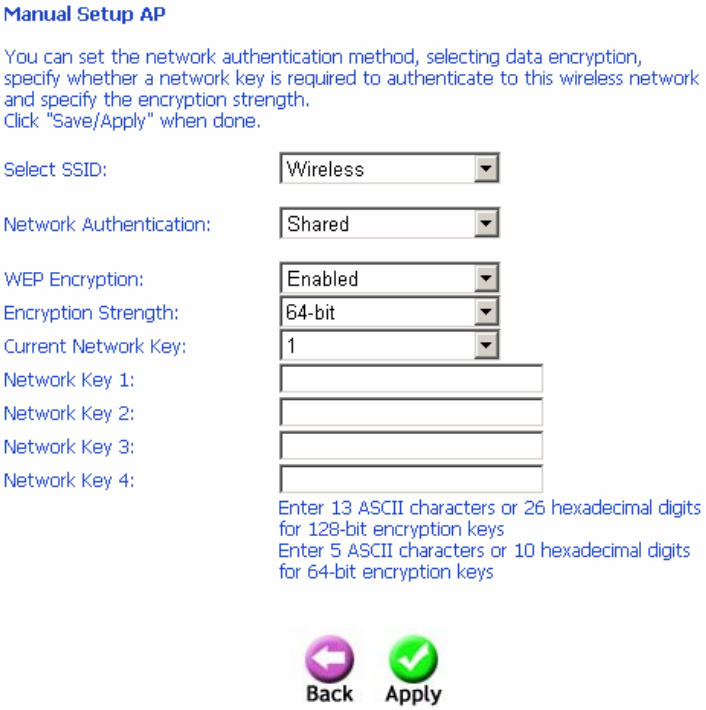
This device is equipped with 802.1X and WPA/WPA2 (Wi-Fi Protected Access), the latest security standard. It also supports the legacy security standard, WEP (Wired Equivalent Privacy).

If you select the “Shared” as the Network Authentication, you can select **64-bit** or **128-bit** as the Encryption Strength.

- **64-bit WEP**: Enter 5 ASCII characters or 10 hexadecimal digits for 64-bit encryption keys. You can set 4 types of the WEP key.
- **128-bit WEP**: Enter 13 ASCII characters or 26 hexadecimal digits for 128-bit encryption keys. You can set 4 types of the WEP key.

The authentication modes are as follows: 802.1X, WPA, WPA-PSK,WPA2, WPA2 –PSK, Mixed WPA2/WPA, Mixed WPA2/WPA –PSK.

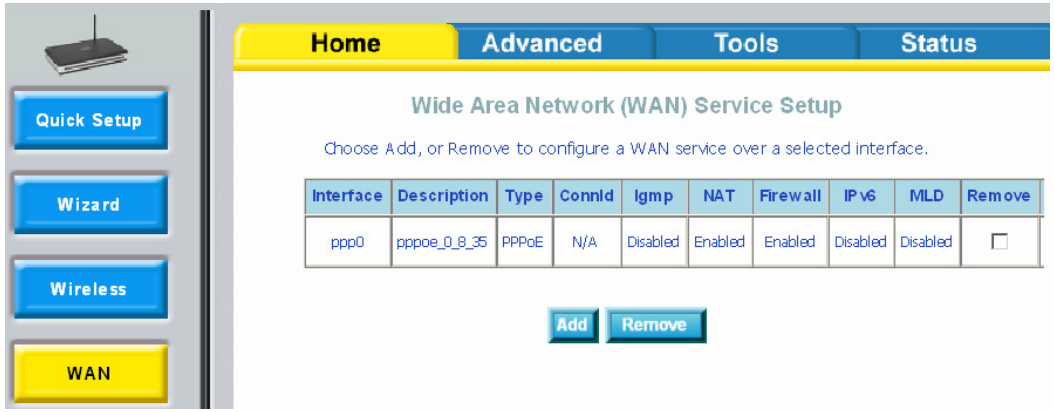
After proper configuration, click **Apply** to save the wireless security options and make the modification effect.



WAN Configuration

Click **WAN** and the right page appears, so you can modify and configure the WAN interface.

Click **Add** or **Remove** to configure WAN interface.

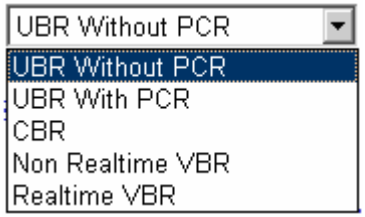


Internet Connection Type - PPP over Ethernet (PPPoE)

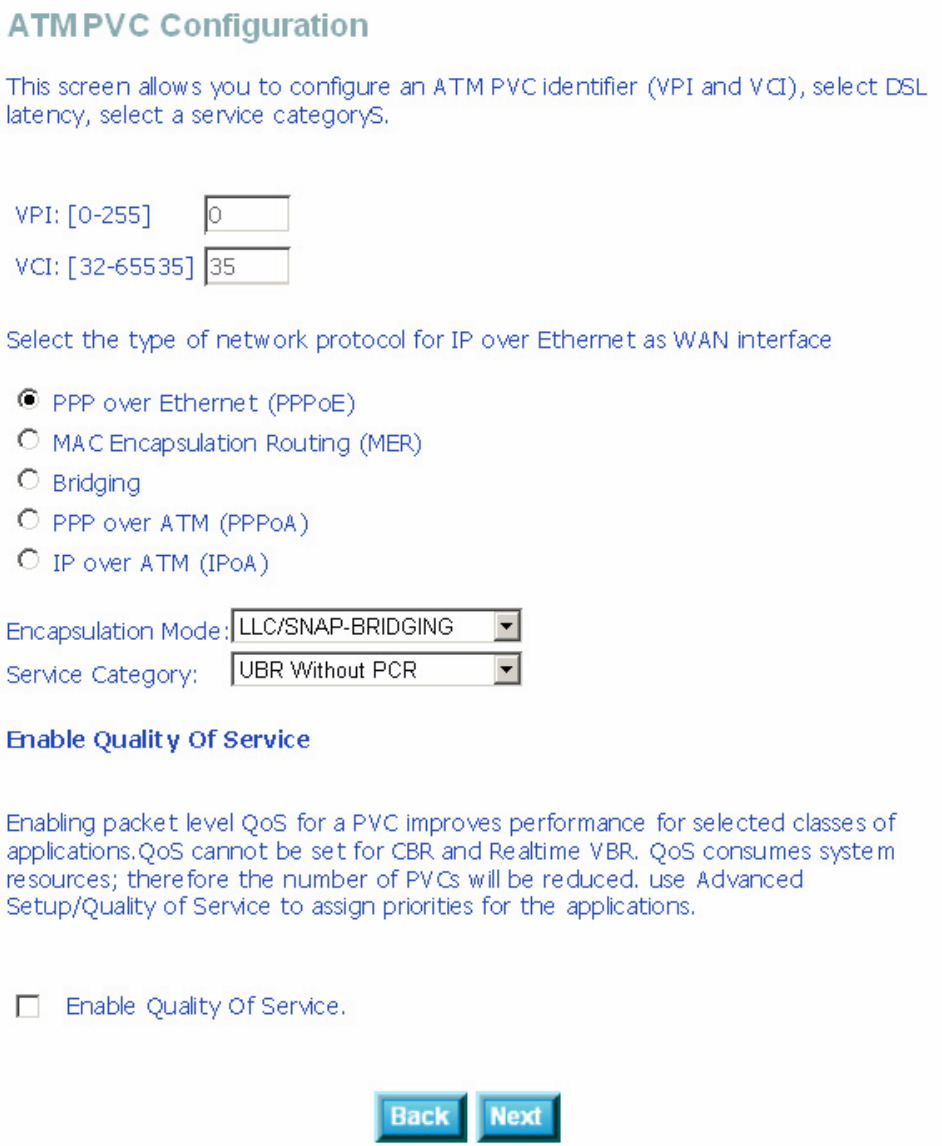
Click **Add** to add the WAN interface.

- **VPI**: Virtual path between two points in an ATM network. Its valid value range is from 0 to 255.
- **VCI**: Virtual channel between two points in an ATM network. Its valid value range is from 32 to 65535 (1 to 31 are reserved for known protocols).
- **Encapsulation Mode**: You can select it from the drop-down list.

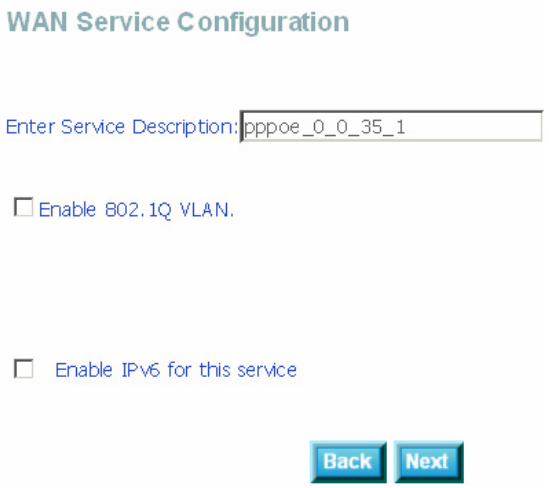
- **Service Category**: You can select it from the drop-down list.



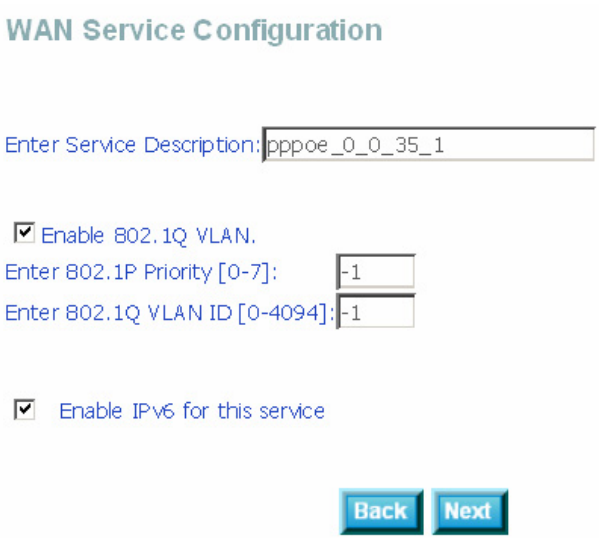
- **Enable Quality Of Service**: Enable or disable QoS.



After proper configuration, click **Next** and the right page appears.
In this page, you can set the service description, enable 802.1Q VLAN and IPv6.



If you enable 802.1Q VLAN and IPv6, the right page appears.
After proper configuration, click **Next**.

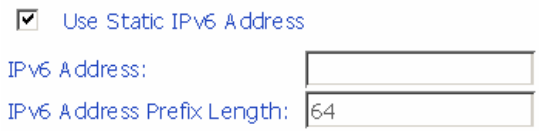


In this page, you can modify the PPP username, PPP password, and authentication method.

- **PPP Username:** The correct user name that your ISP provides to you.
- **PPP Password:** The correct password that your ISP provides to you.
- **PPPoE Service Name:** If your ISP provides it to you, please enter it. If not, do not enter any information.
- **Authentication Method:** The value can be AUTO, PAP, CHAP, or MSCHAP. Usually, you can select AUTO.
- **Dial on demand (with idle timeout timer):** If this function is enabled, you need to enter the idle timeout time. Within the preset minutes, if the modem does not detect the flow of the user continuously, the modem automatically stops the PPPOE connection. Once it detects the flow (like access to a webpage), the modem restarts the PPPoE dialup. If this function is disabled, the modem performs PPPoE dial-up all the time. The PPPoE connnection does not stop, unless the modem is powered off and DSLAM or uplink equipment is abnormal.
- **PPP IP extension:** If you want to configure DMZ Host, you should enable it at first.
- **Use Static IPv4 Address:** If this function is disabled, the modem obtains an IP address assigned by an uplink equipment such as BAS, through PPPoE dial-up. If this function is enabled, the modem uses this IP address as the WAN IP address.

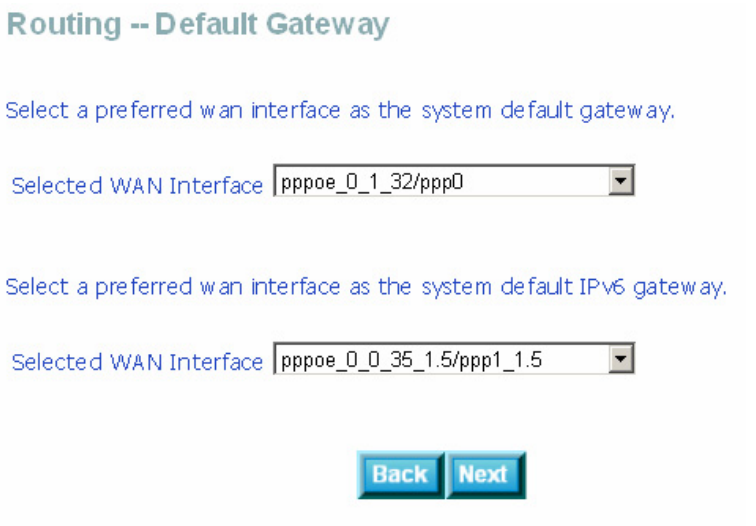
- **IEnable NAT:** Select the checkbox to apply Fullcone NAT mode.

- Use Static IPv6 Address: Enable to use a static IPv6 address. Enter the address in the **IPv6 Address** field.

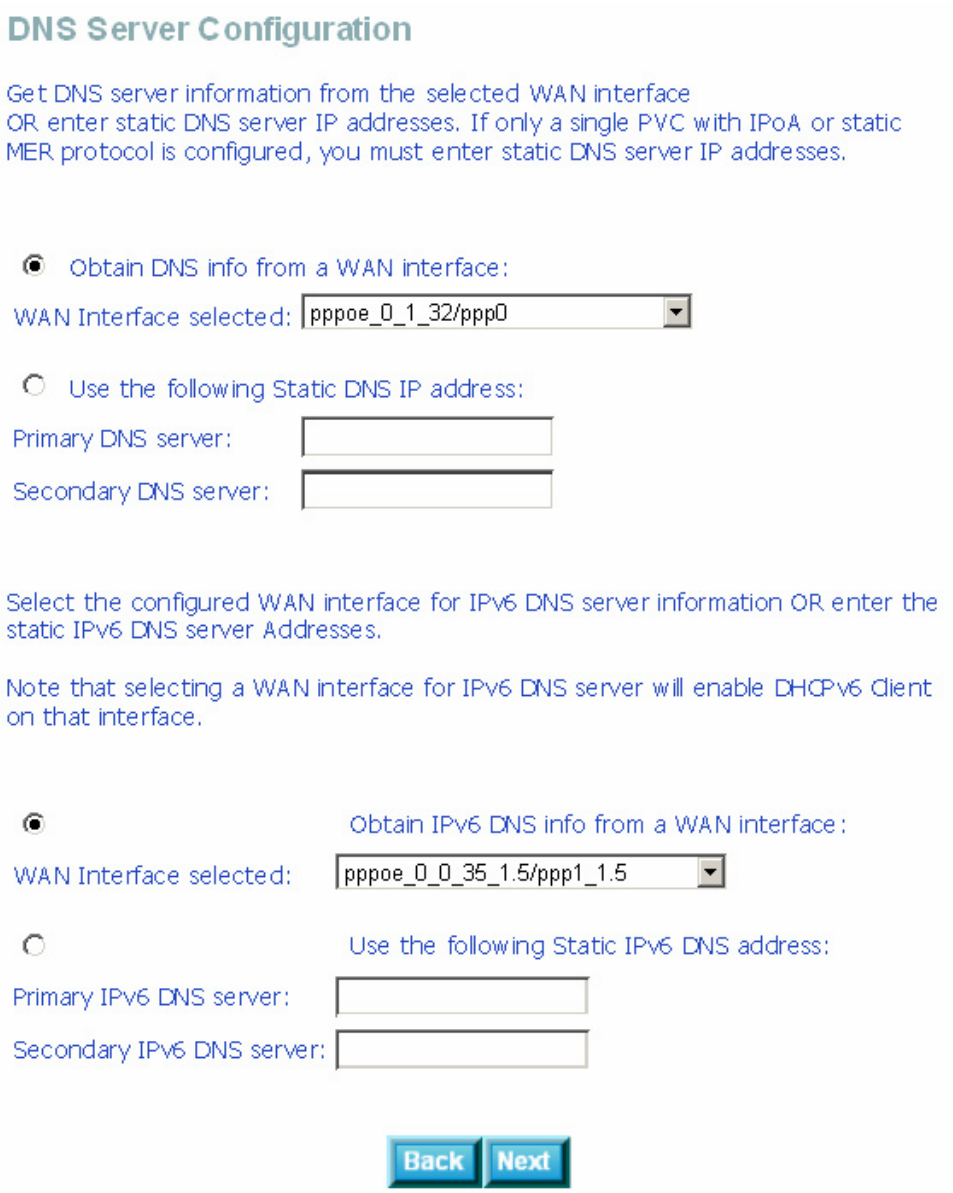


- **GMP Multicast:** IGMP proxy. For example, if you want PPPoE mode to support IPTV, enable it.

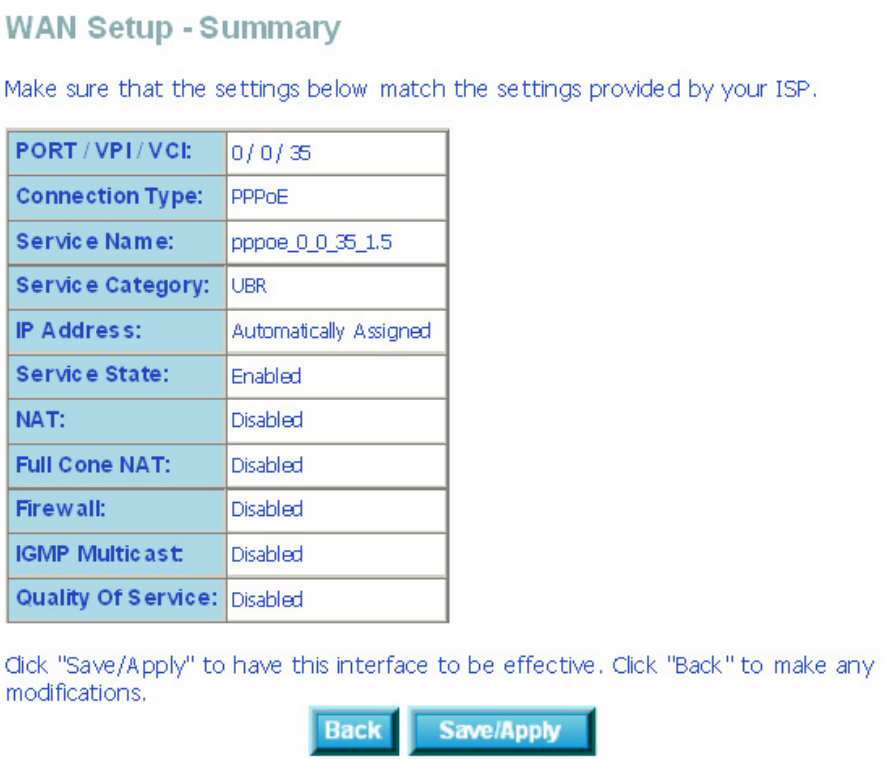
After enter the PPP Username and PPP Password, click **Next**, and the right page appears. In this page, select a preferred WAN interface as the system default gateway.



Click **Next,** and the right page appears.
In this page, you can get DNS server information from the selected WAN interface or enter static DNS server IP addresses. If only a single PVC with IPoA or static MER protocol is configured, you must enter static DNS server IP addresses.



Click **Next**, and the right page appears.
In this page, it shows all the configurations. Click **Back** to make any modifications.
Click **Save/ Apply** to all the configurations. Then it turns to the **Quick Setup** page.

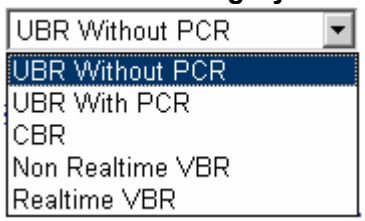


Internet Connection Type - MAC Encapsulation Routing (MER)

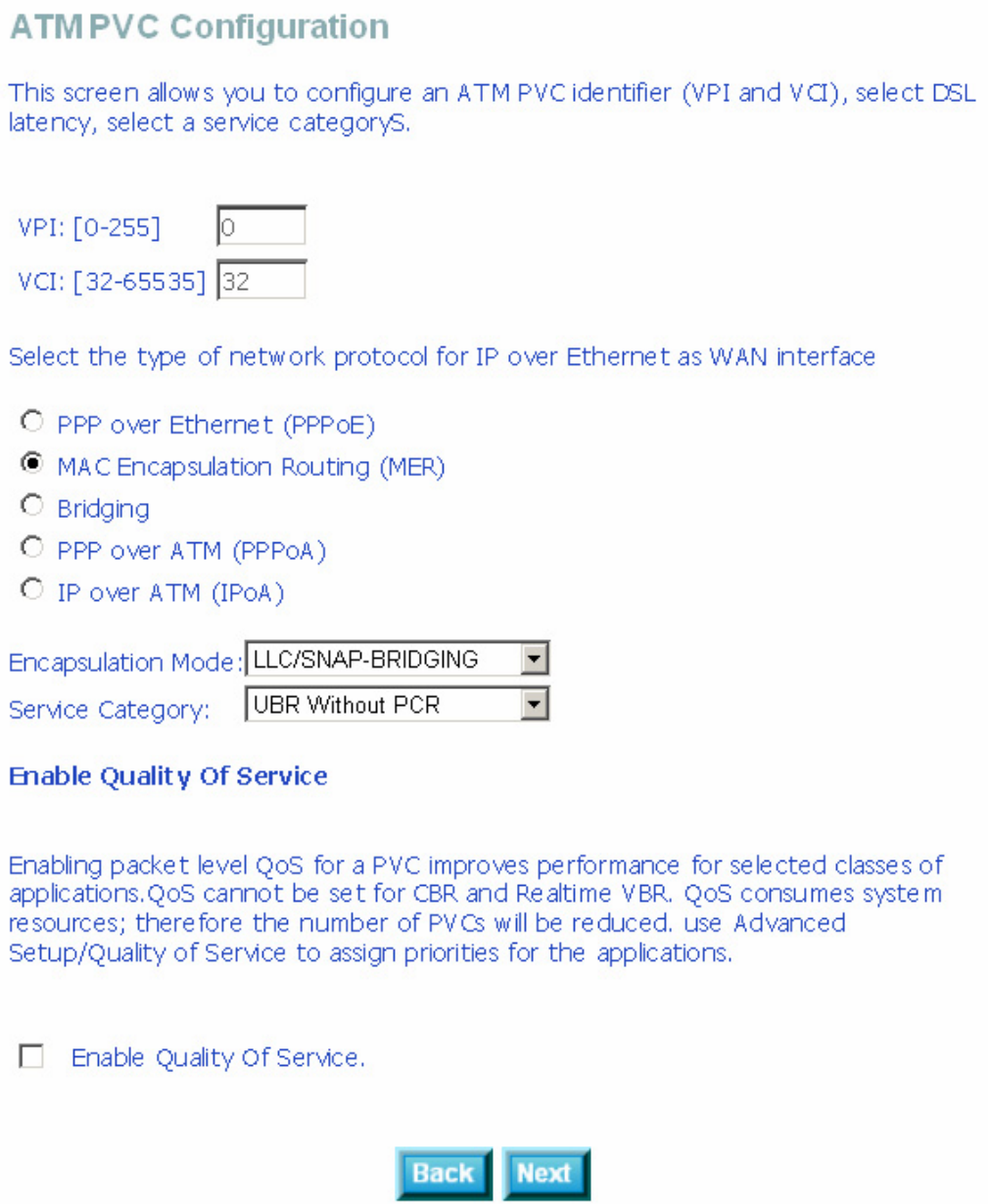
Click **Add** to add the WAN interface.

- **VPI**: Virtual path between two points in an ATM network. Its valid value range is from 0 to 255.
- **VCI**: Virtual channel between two points in an ATM network. Its valid value range is from 32 to 65535 (1 to 31 are reserved for known protocols).
- **Encapsulation Mode**: You can select it from the drop-down list.

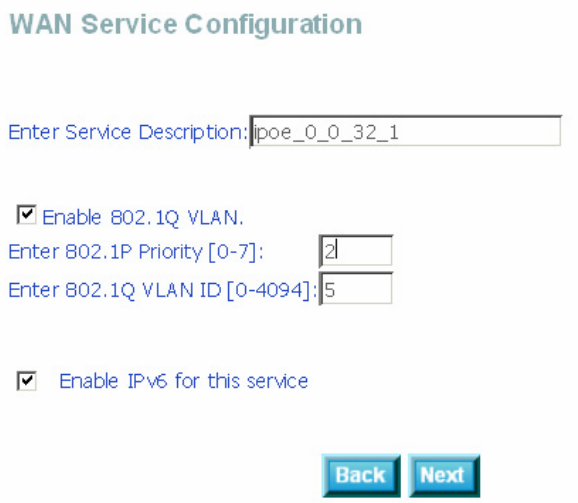
- **Service Category**: You can select it from the drop-down list.



- **Enable Quality Of Service**: Enable or disable QoS.

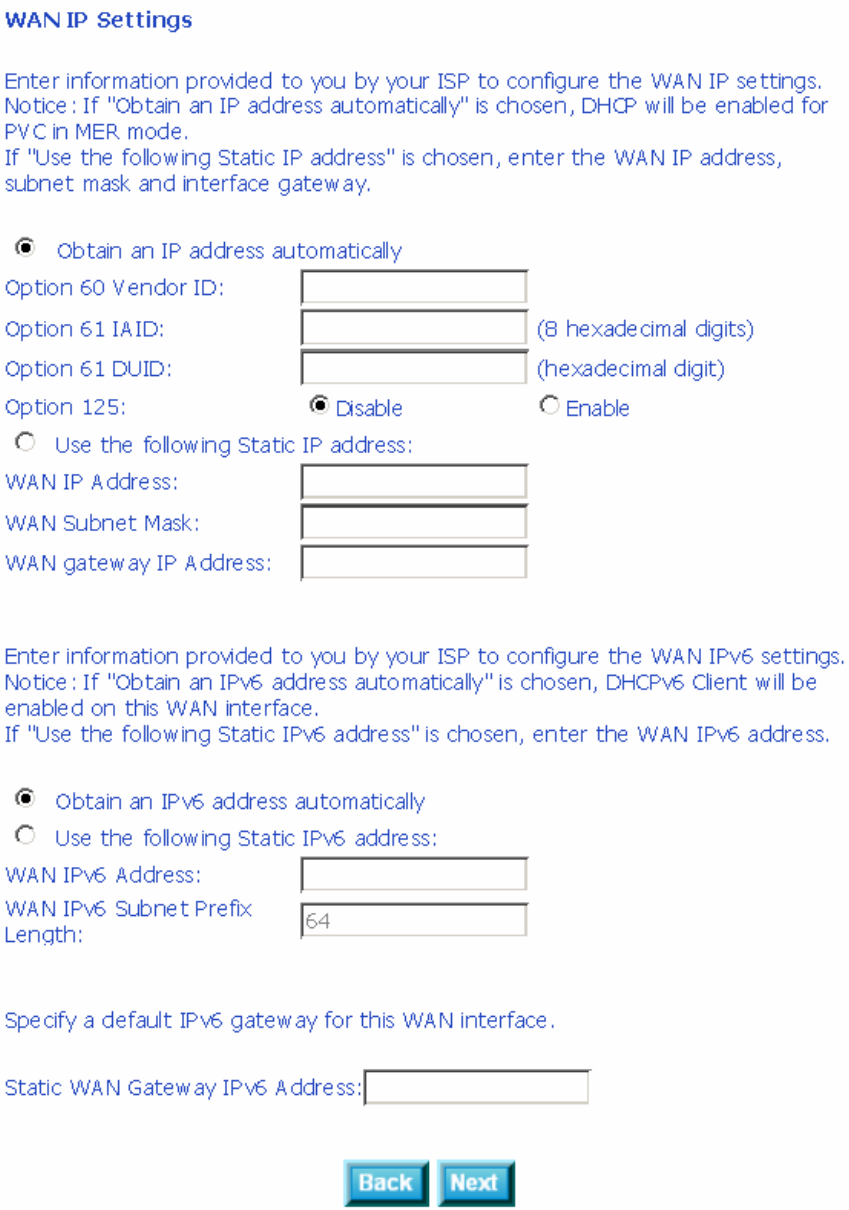


After proper configuration, click **Next** and the right page appears.
In this page, you can set the service description, enable 802.1Q VLAN and IPv6.



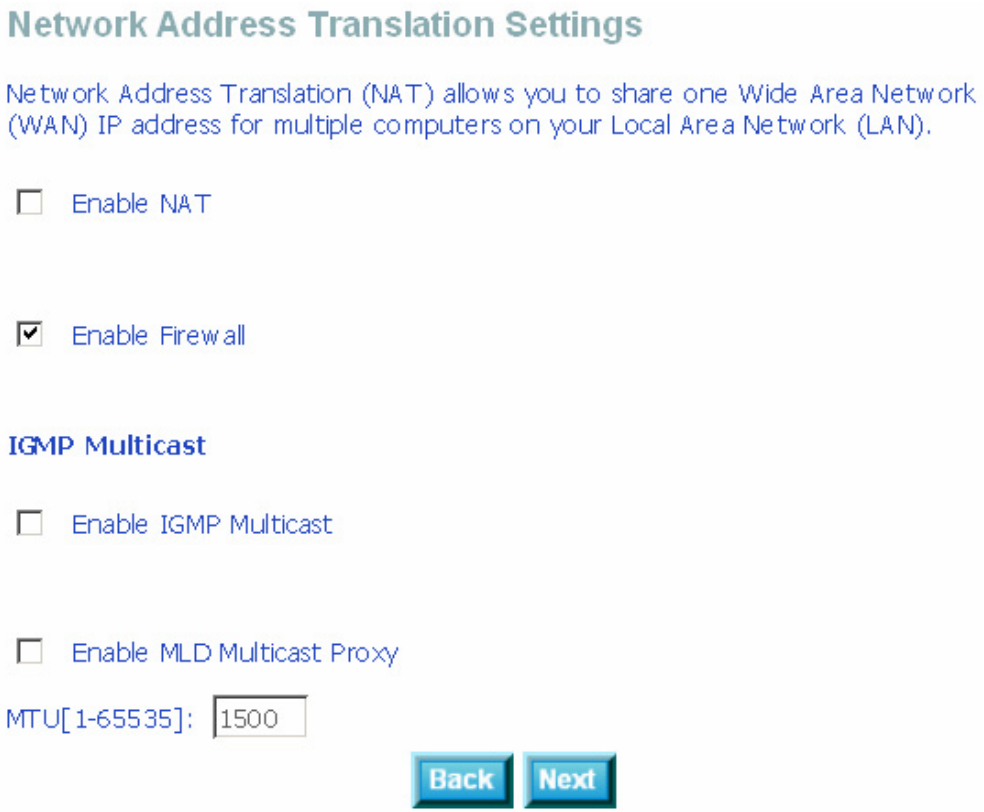
After proper configuration, click **Next** and the right page appears.

Field	Description
Obtain an IP address automatically	Select to obtain an IP address automatically for the WAN IP. DHCP will be enabled for PVC in MER mode.
Option 60 Vendor ID	Contact your ISP for information.
Option 61 IAID	Contact your ISP for information.
Option 61 DUID	Contact your ISP for information.
Option 125	Contact your ISP for information.
Use the following Static IP address	Select to use a specified static IP address for the WAN IP, subnet mask, and interface gateway.
WAN IP Address	Enter a static IP address.
WAN Subnet Mask	Enter a subnet mask.
WAN gateway IP Address	Enter the gateway IP address.
Obtain an IPv6 address automatically	Select to obtain an IP address automatically for the WAN IP. DHCP will be enabled for PVC in MER mode.
Use the following Static IPv6 address	Select to use a specified static IPv6 address for the WAN IP, subnet mask, and interface gateway.
WAN IPv6 Address	Enter a static IPv6 address.
WAN IPv6 Subnet Prefix Length	Enter a subnet mask.
Static WAN Gateway IPv6 Address	Enter the gateway IPv6 address.

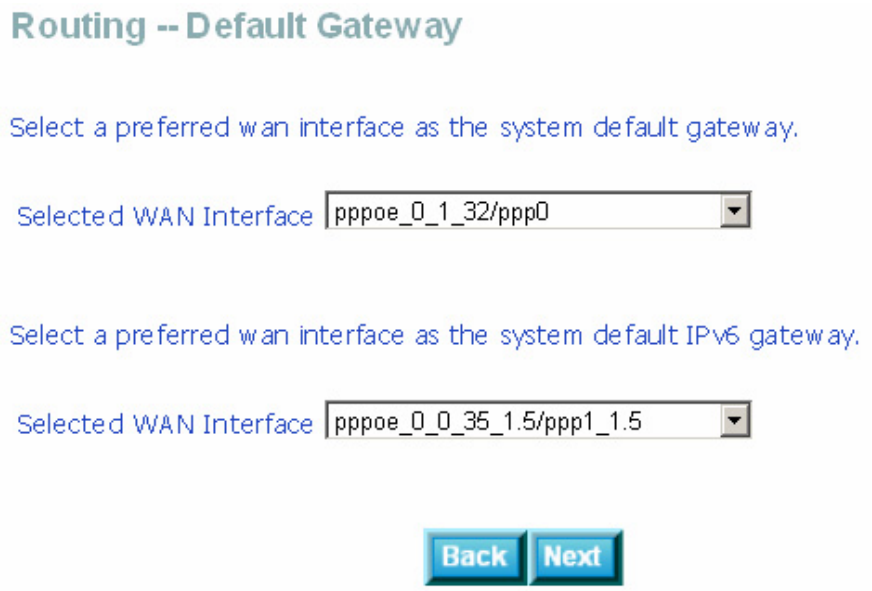


After proper configuration, click **Next** and the right page appears.

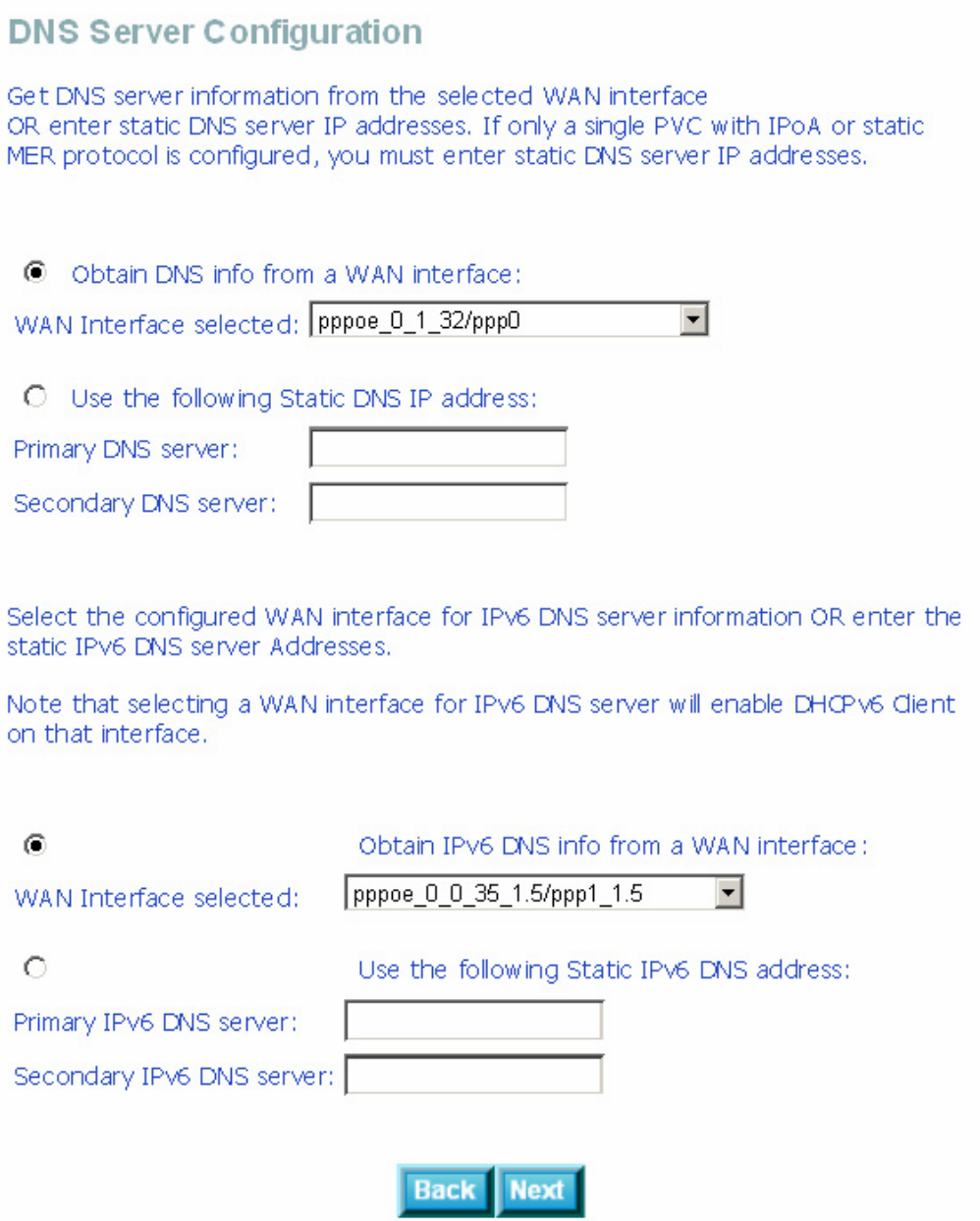
Field	Description
Enable NAT	Indicates if NAT is enabled or disabled.
Enable Firewall	Indicates if the firewall is enabled or disabled.
Enable IGMP Multicast	Indicates if IGMP multicast is enabled or disabled.
Enable MLD Multicast Proxy	Indicates if MLD is enabled or disabled.
MTU(1-65535)	Indicates if multicast listener discovery proxy for IPv6 is enabled or disabled.
Back	Click to return to the previous configuration screen
Next	Click to proceed to the Routing – Default Gateway window.



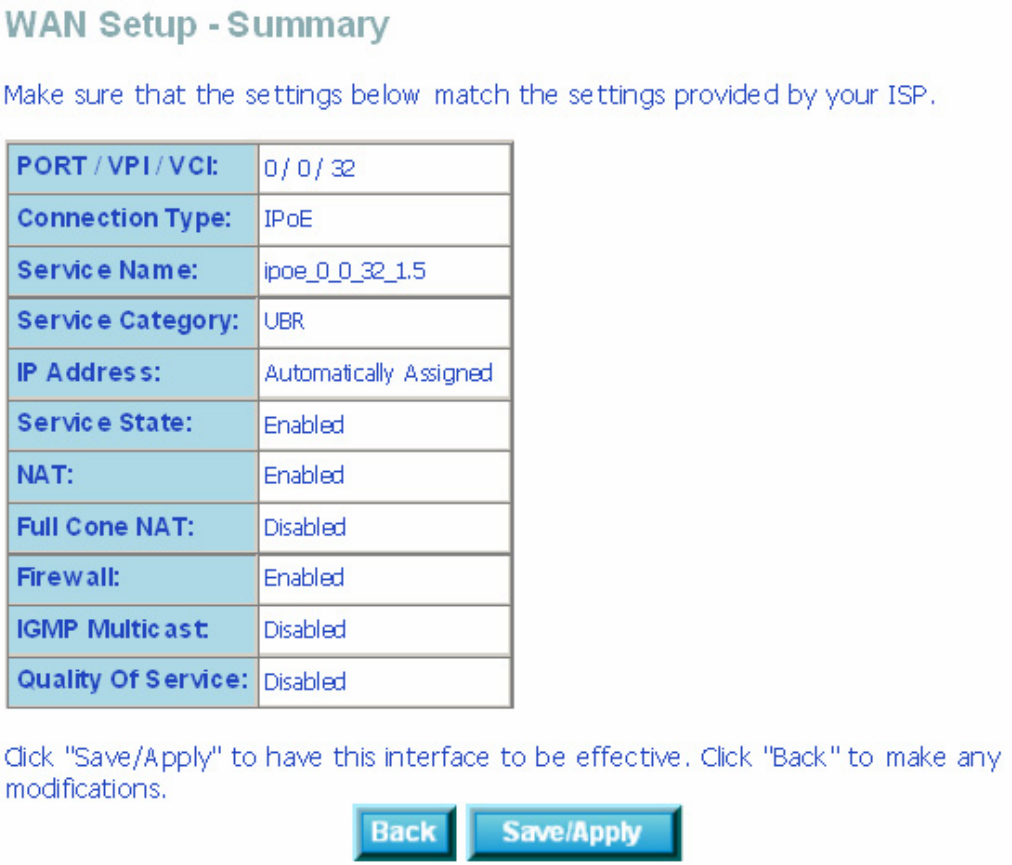
After proper configuration, click **Next** and the right page appears.
In this page, select a preferred WAN interface as the system default gateway.



After proper configuration, click **Next** and the right page appears.
In this page, you can get DNS server information from the selected WAN interface or enter static DNS server IP addresses. If only a single PVC with IPoA or static MER protocol is configured, you must enter static DNS server IP addresses.



Click **Next**, and the right page appears.
In this page, it shows all the configurations. Click **Back** to make any modifications.
Click **Save/ Apply** to all the configurations. Then it turns to the **Quick Setup** page.

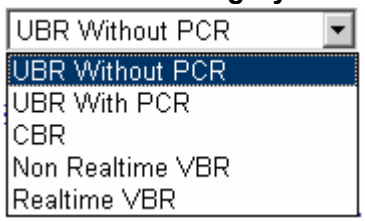


Internet Connection Type – Bridging

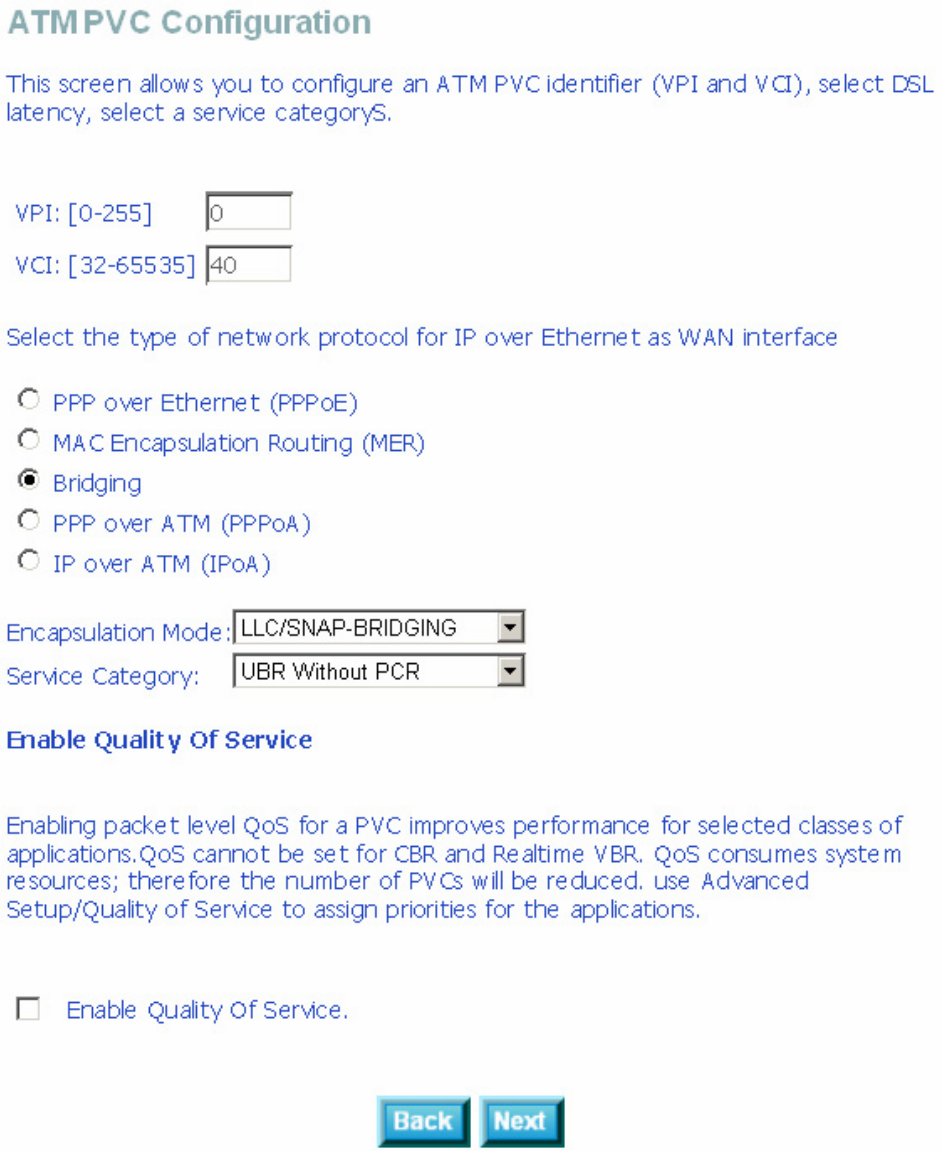
Click **Add** to add the WAN interface.

- **VPI**: Virtual path between two points in an ATM network. Its valid value range is from 0 to 255.
- **VCI**: Virtual channel between two points in an ATM network. Its valid value range is from 32 to 65535 (1 to 31 are reserved for known protocols).
- **Encapsulation Mode**: You can select it from the drop-down list.

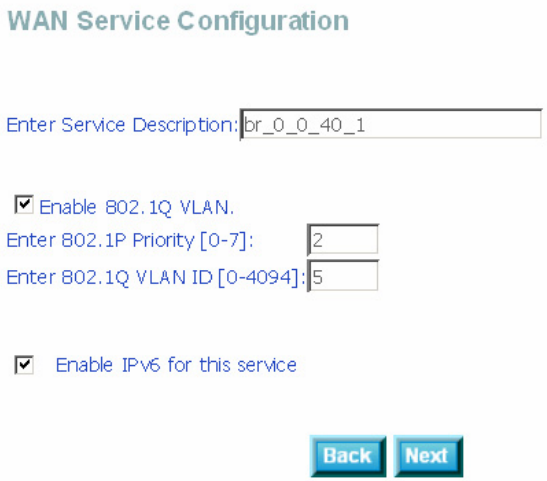
- **Service Category**: You can select it from the drop-down list.



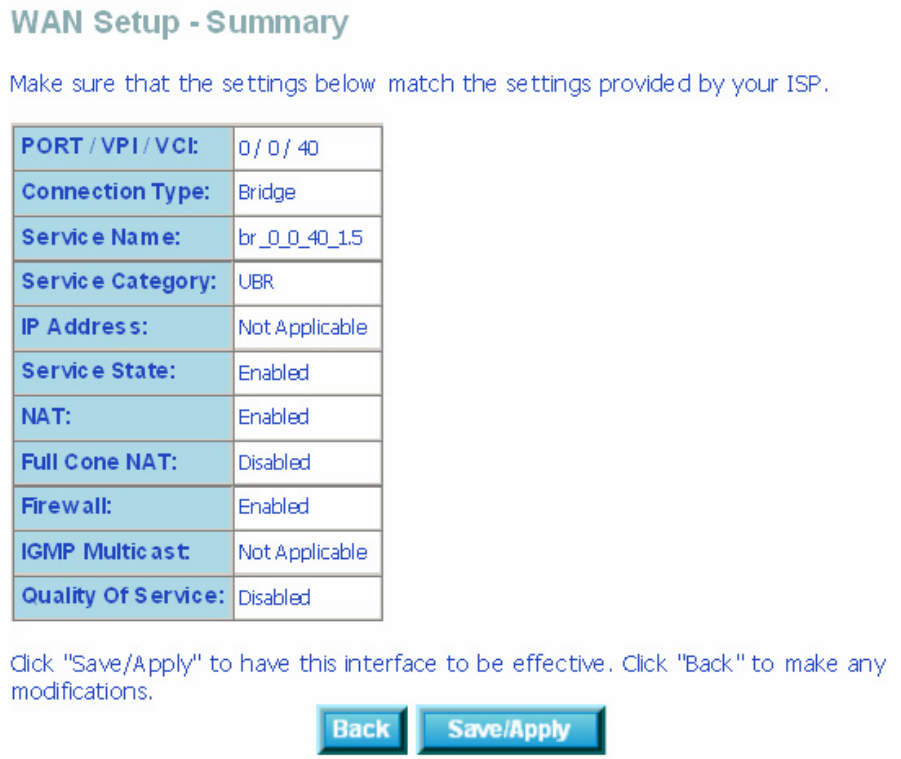
- **Enable Quality Of Service**: Enable or disable QoS.



After proper configuration, click **Next** and the right page appears.
In this page, you can set the service description, enable 802.1Q VLAN and IPv6.



Click **Next**, and the right page appears.
In this page, it shows all the configurations. Click **Back** to make any modifications.
Click **Save/ Apply** to all the configurations. Then it turns to the **Quick Setup** page.

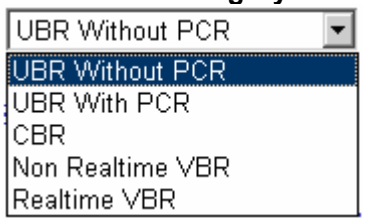


Internet Connection Type - PPP over ATM (PPPoA)

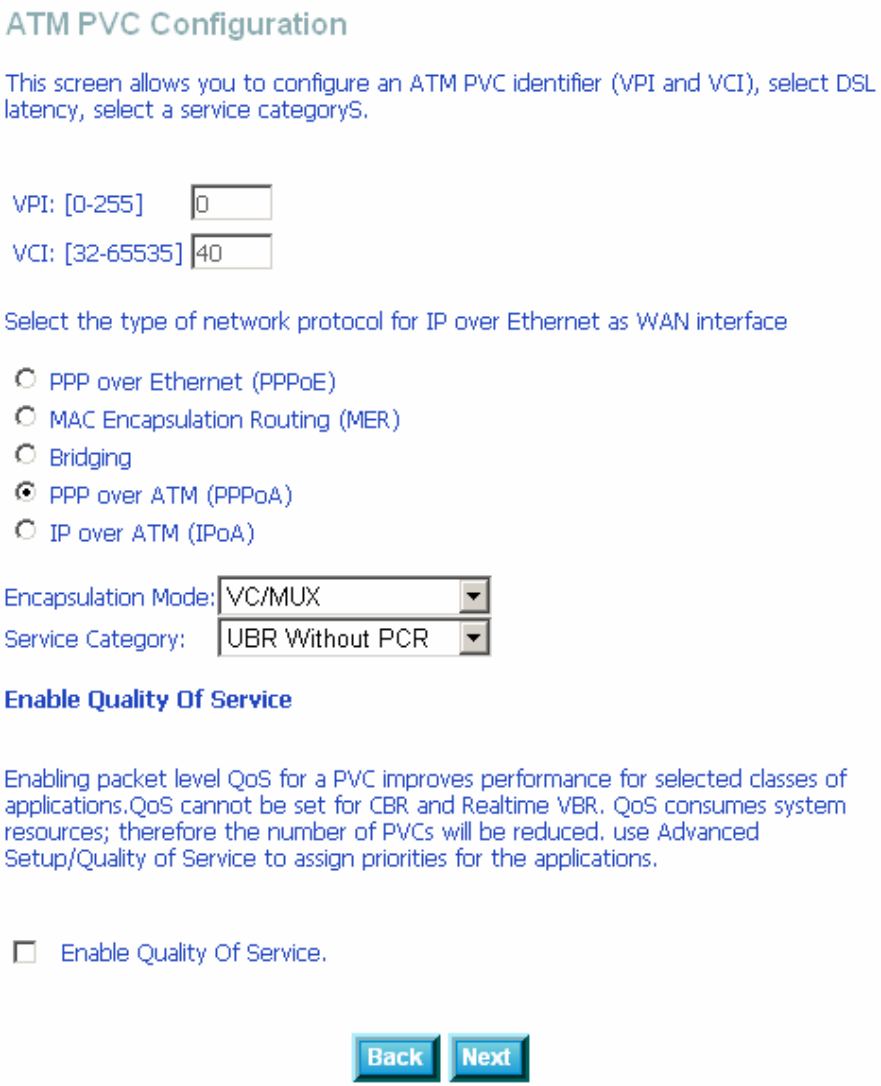
Click **Add** to add the WAN interface.

- **VPI**: Virtual path between two points in an ATM network. Its valid value range is from 0 to 255.
- **VCI**: Virtual channel between two points in an ATM network. Its valid value range is from 32 to 65535 (1 to 31 are reserved for known protocols).
- **Encapsulation Mode**: You can select it from the drop-down list.

- **Service Category**: You can select it from the drop-down list.



- **Enable Quality Of Service**: Enable or disable QoS.



After proper configuration, click **Next** and the right page appears. In this page, you can set the service description.

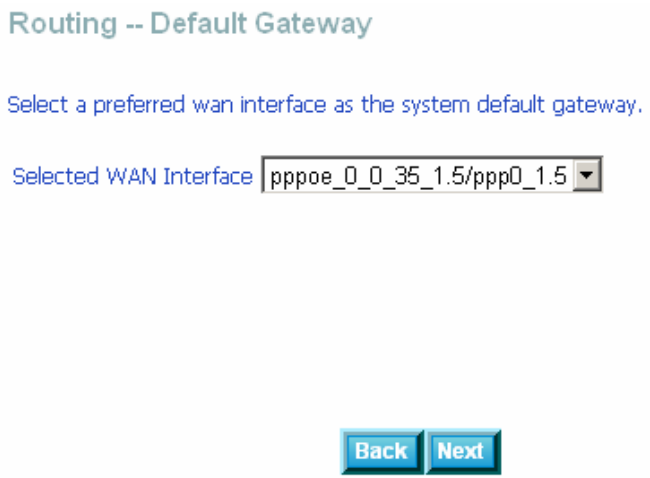
In this page, you can modify the PPP username, PPP password, and authentication method.

- **PPP Username:** The correct user name that your ISP provides to you.
- **PPP Password:** The correct password that your ISP provides to you.
- **PPPoE Service Name:** If your ISP provides it to you, please enter it. If not, do not enter any information.
- **Authentication Method:** The value can be AUTO, PAP, CHAP, or MSCHAP. Usually, you can select AUTO.
- **Dial on demand (with idle timeout timer):** If this function is enabled, you need to enter the idle timeout time. Within the preset minutes, if the modem does not detect the flow of the user continuously, the modem automatically stops the PPPOE connection. Once it detects the flow (like access to a webpage), the modem restarts the PPPoE dialup. If this function is disabled, the modem performs PPPoE dial-up all the time. The PPPoE connnection does not stop, unless the modem is powered off and DSLAM or uplink equipment is abnormal.
- **PPP IP extension:** If you want to configure DMZ Host, you should enable it at first.
- **Use Static IPv4 Address:** If this function is disabled, the modem obtains an IP address assigned by an uplink equipment such as BAS, through PPPoE dial-up. If this function is enabled, the modem uses this IP address as the WAN IP address.

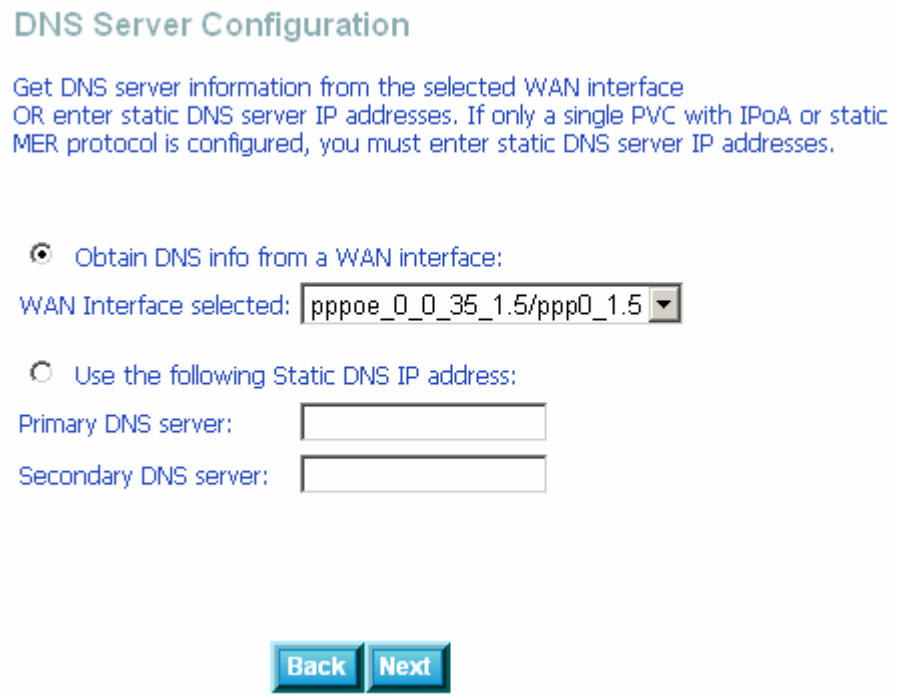
- **IEnable NAT:** Select the checkbox to apply Fullcone NAT mode.

- **IGMP Multicast:** IGMP proxy. For example, if you want PPPoE mode to support IPTV, enable it.

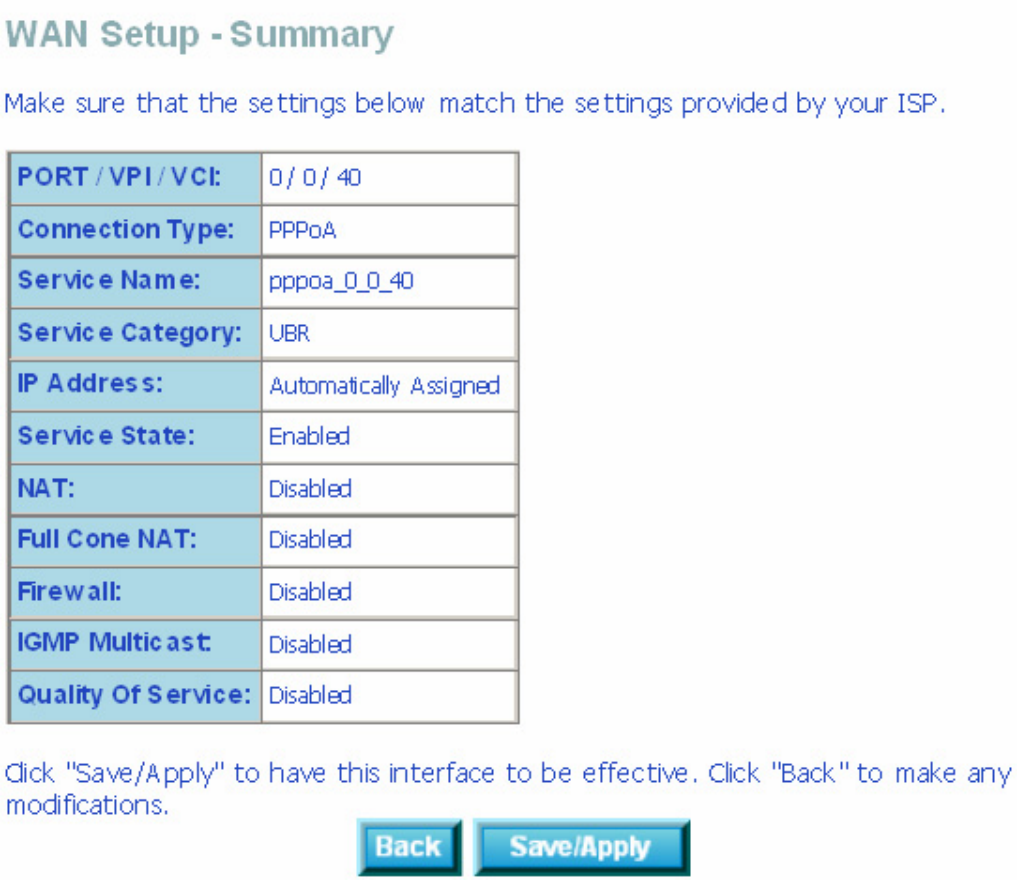
After enter the PPP Username and PPP Password, click **Next**, and the right page appears. In this page, select a preferred WAN interface as the system default gateway.



Click **Next,** and the right page appears.
In this page, you can get DNS server information from the selected WAN interface or enter static DNS server IP addresses. If only a single PVC with IPoA or static MER protocol is configured, you must enter static DNS server IP addresses.



Click **Next**, and the right page appears.
In this page, it shows all the configurations. Click **Back** to make any modifications.
Click **Save/ Apply** to all the configurations. Then it turns to the **Quick Setup** page.

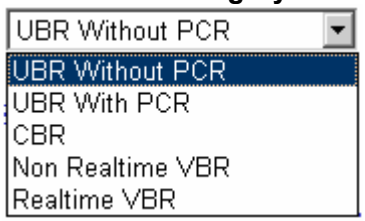


Internet Connection Type - IP over ATM (IPoA)

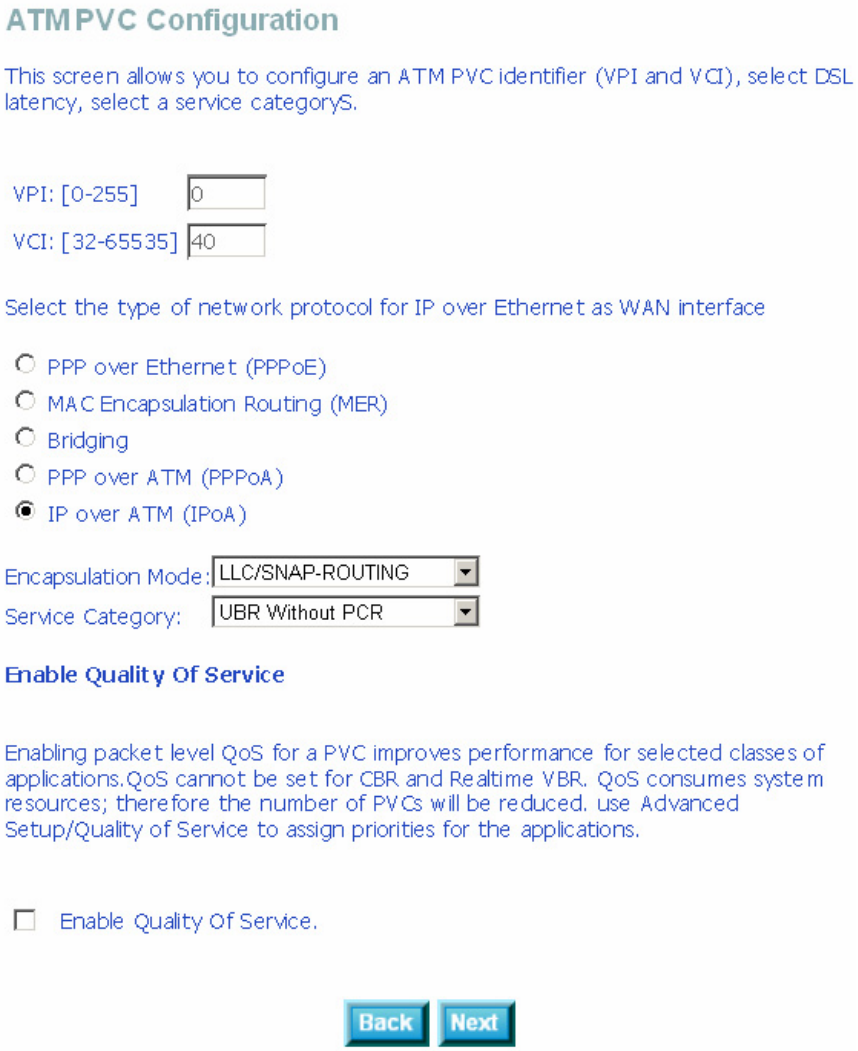
Click **Add** to add the WAN interface.

- **VPI**: Virtual path between two points in an ATM network. Its valid value range is from 0 to 255.
- **VCI**: Virtual channel between two points in an ATM network. Its valid value range is from 32 to 65535 (1 to 31 are reserved for known protocols).
- **Encapsulation Mode**: You can select it from the drop-down list.

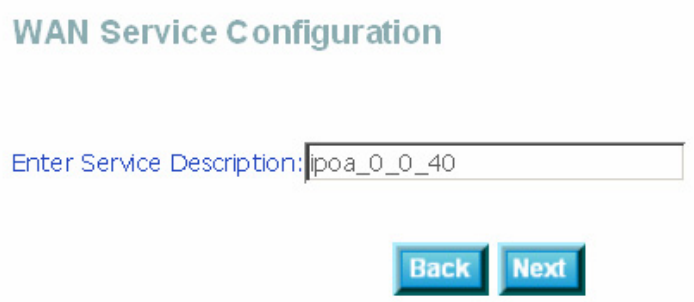
- **Service Category**: You can select it from the drop-down list.



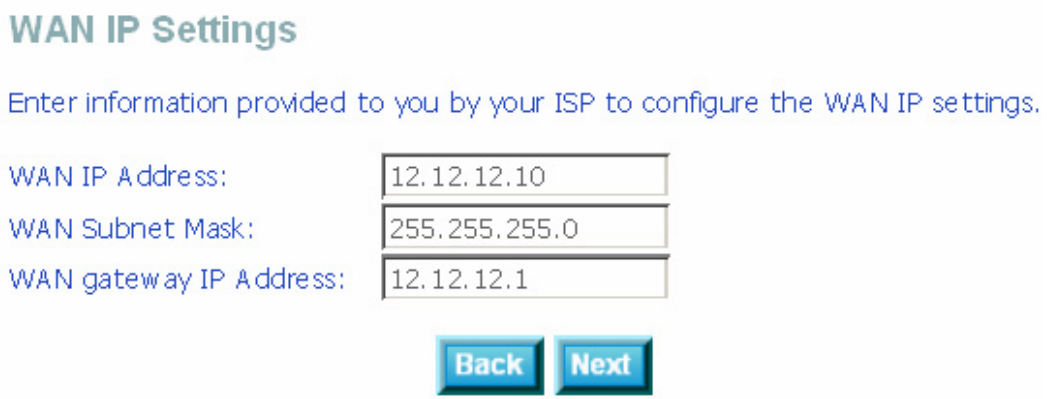
- **Enable Quality Of Service**: Enable or disable QoS.



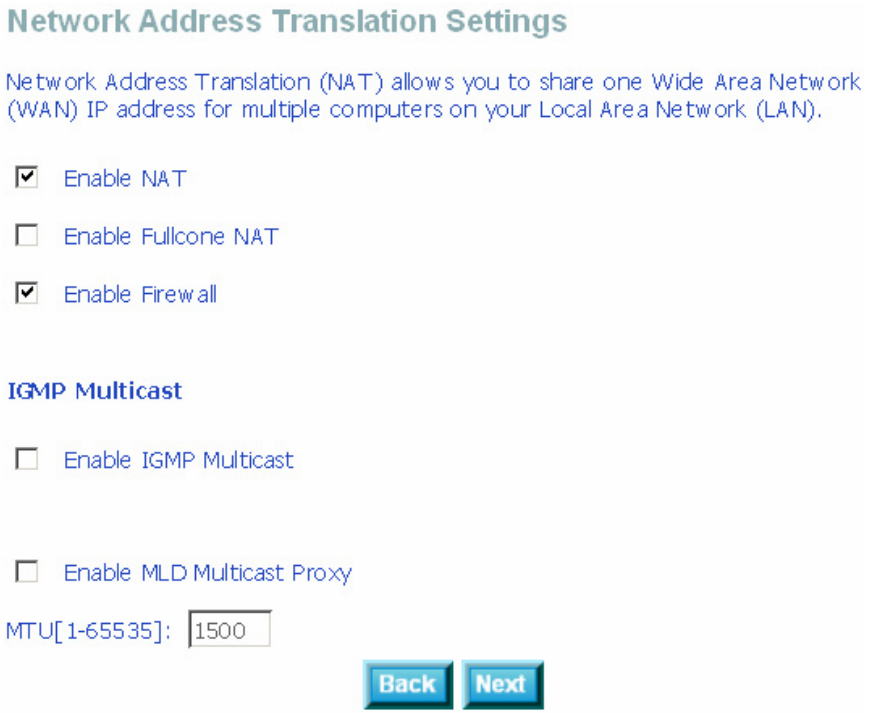
After proper configuration, click **Next** and the right page appears.
In this page, you can set the service description.



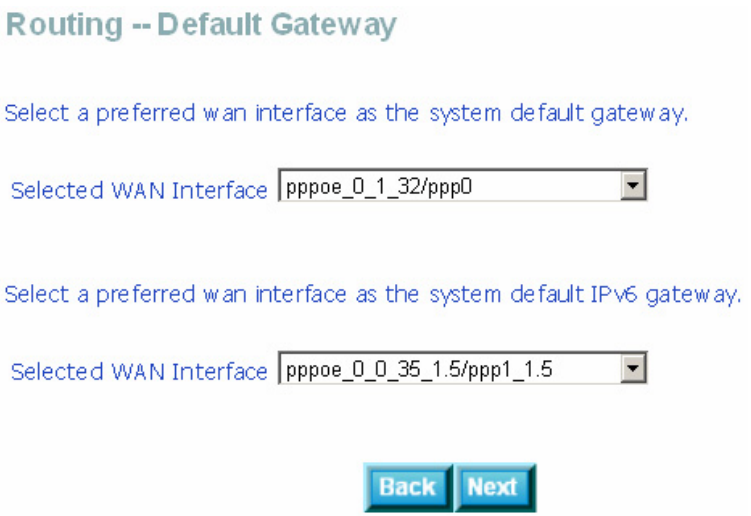
After proper configuration, click **Next** and the right page appears.
In this page, enter the information provided by your ISP for WAN IP settings.



After proper configuration, click **Next** and the right page appears.

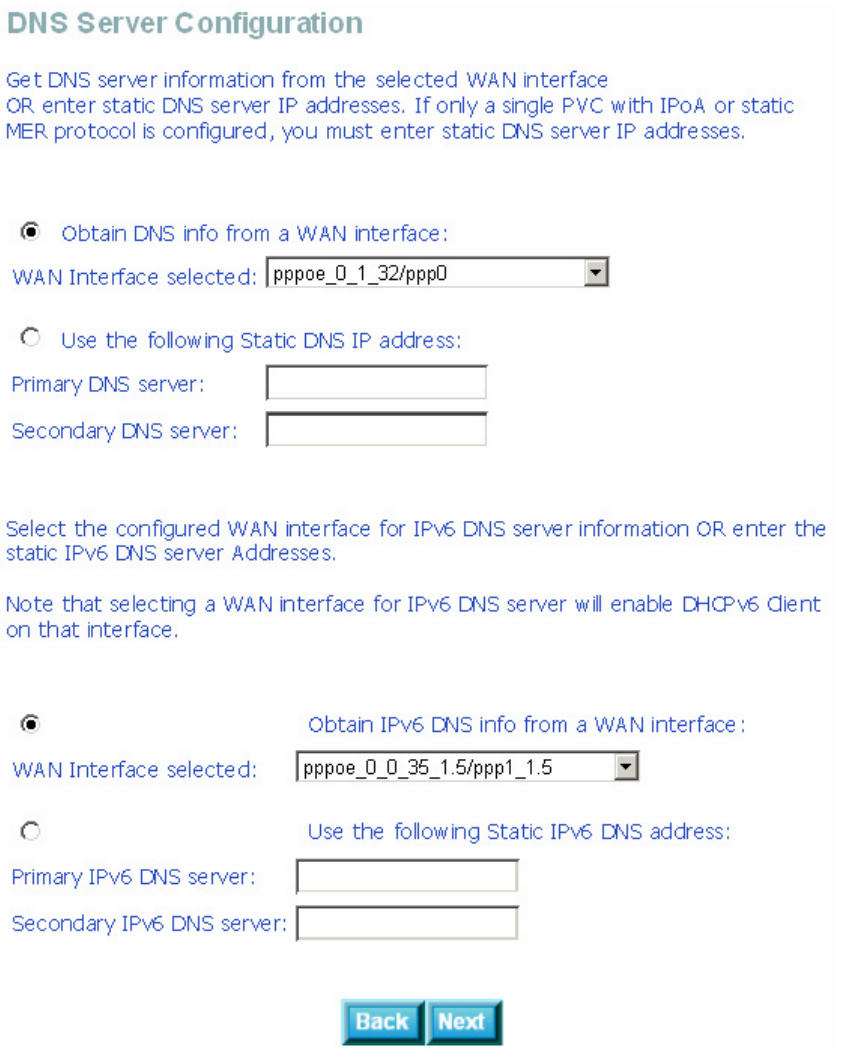


Click **Next**, and the right page appears. In this page, select a preferred WAN interface as the system default gateway.

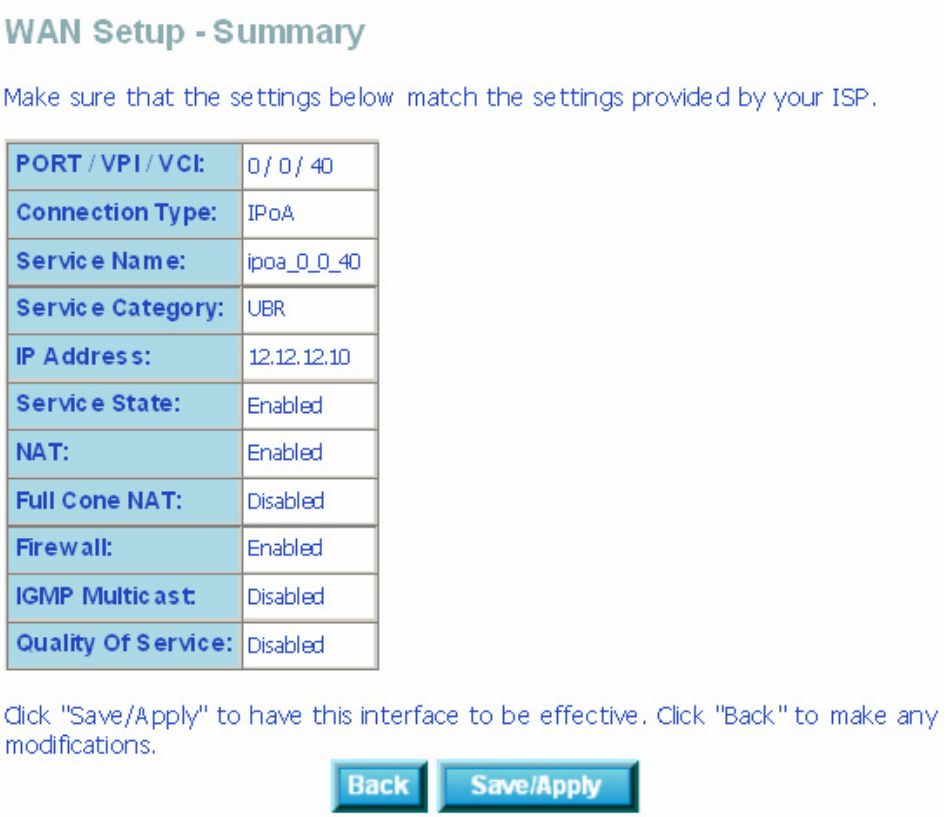


Click **Next,** and the right page appears.

In this page, you can get DNS server information from the selected WAN interface or enter static DNS server IP addresses. If only a single PVC with IPoA or static MER protocol is configured, you must enter static DNS server IP addresses.



Click **Next**, and the right page appears.
In this page, it shows all the configurations. Click **Back** to make any modifications.
Click **Save/ Apply** to all the configurations. Then it turns to the **Quick Setup** page.

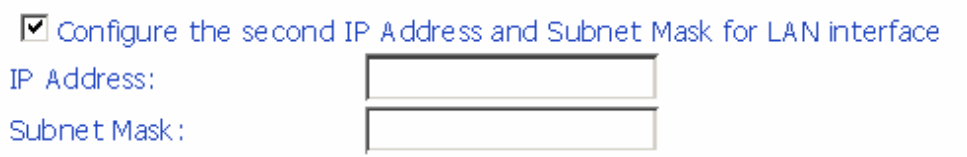


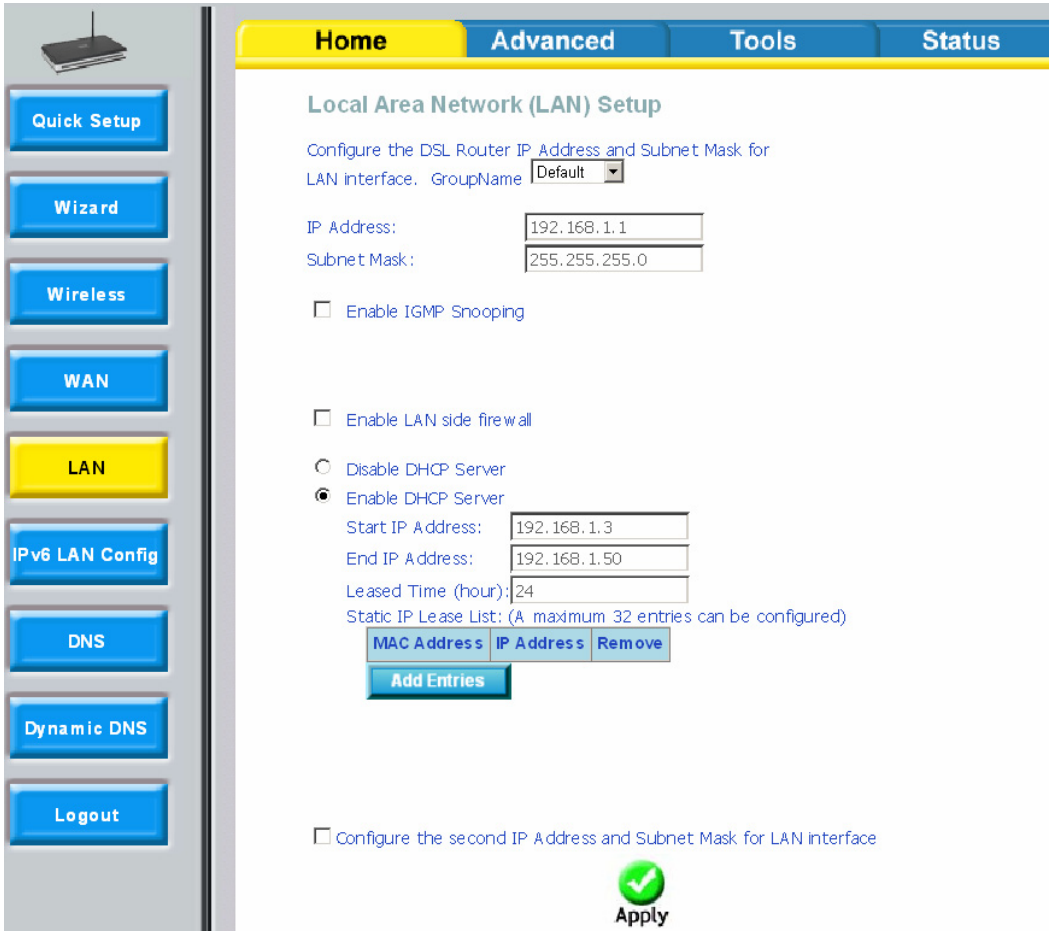
LAN Configuration

In this page, you can configure an IP address for the DSL Router and enable DHCP server. The preset IP address is 192.168.1.1.
If you enable the IGMP Snooping, the following figure appears.

Click **Add Entries**, the following figure appears.

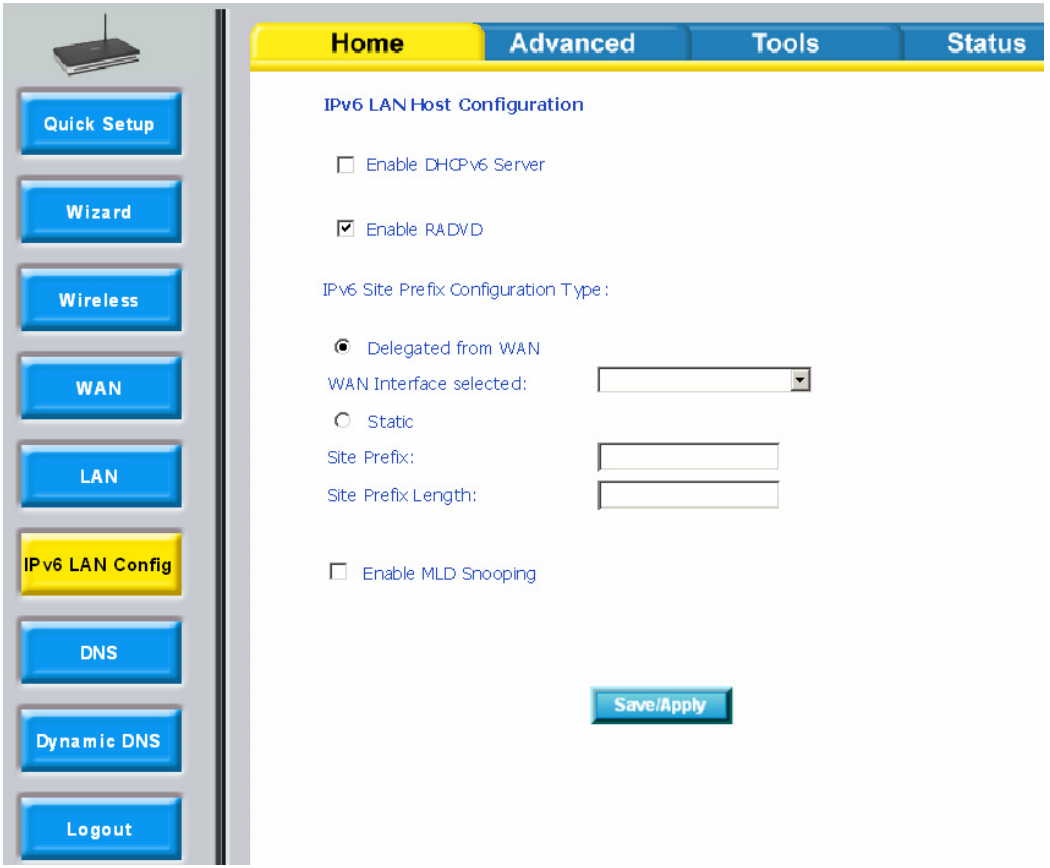
If you want to configure the second IP, please select the check box.





IPv6 LAN Configuration

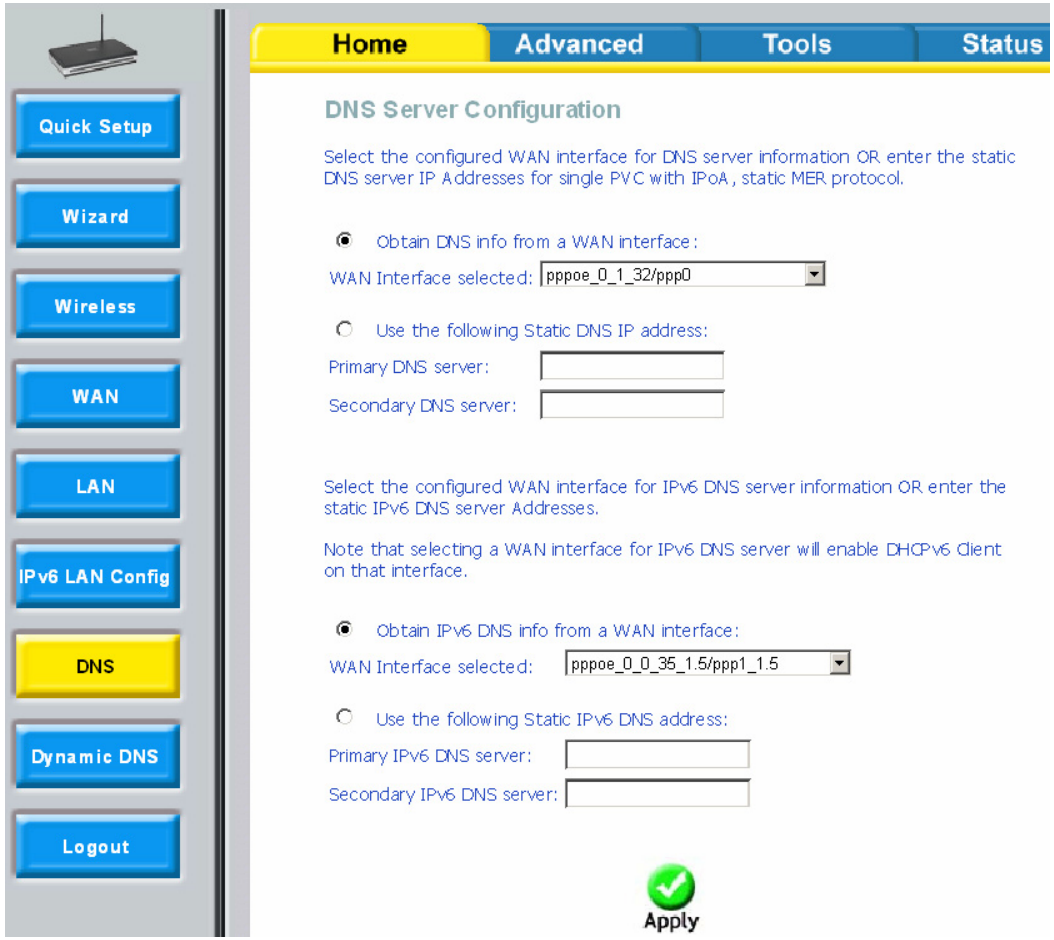
Field	Description
Enable DHCPv6 Server	Select the checkbox to enable the DHCPv6 Server. WIDE-DHCPv6 is an open-source implementation of dynamic host configuration protocol for IPv6 (DHCPv6).
Enable RADVD	Select the checkbox to enable RADVD. The router advertisement daemon (RADVD) is run by Linux or BSD systems acting as IPv6 routers. It sends router advertisement messages, specified by RFC2461, to a local Ethernet LAN periodically and when requested by a node sending a router solicitation message. These messages are required for IPv6 stateless auto-configuration.
Delegated from WAN	Select the Delegated from WAN radio button to have the IPv6 site prefix configuration type delegated from a WAN interface selected from the drop-down list.
Static	Select Static to specify a static IPv6 site prefix.
Site Prefix	Enter the IPv6 site prefix.
Site Prefix Length	Specify the length of the IPv6 site prefix.
Enable MLD Snooping	Select the checkbox to enable multicast listener discovery snooping.
Save/Apply	Click to save your changes.



DNS Configuration

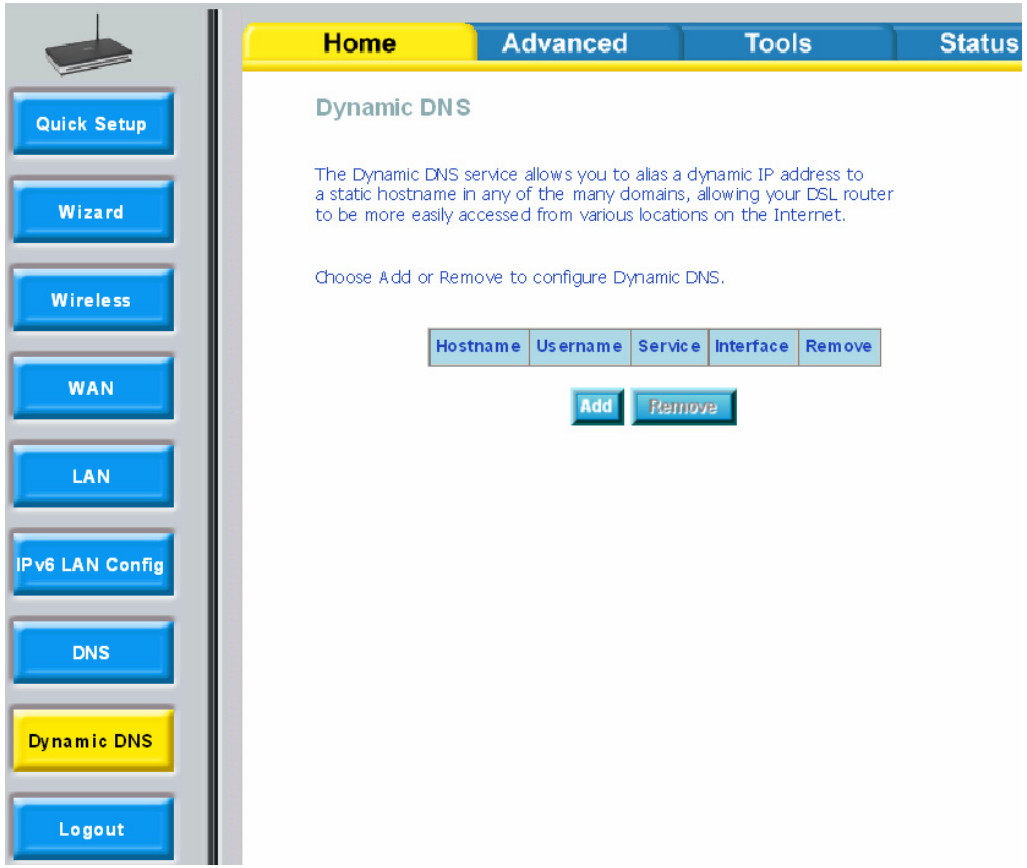
Field	Description
Obtain DNS info from a WAN interface	Select to obtain DNS info from a WAN interface.
WAN interface selected	Select a WAN interface for obtaining DNS info.
Use the following Static DNS IP address	Select to use the following static DNS IP address.
Primary DNS server	Enter a primary static DNS IP address.
Secondary DNS server	Enter a secondary static DNS IP address.
Apply	Click to save changes.

Note: *If you do not enable the IPv6 in the WAN configuration, the DHCPv6 Client will not be displayed.*



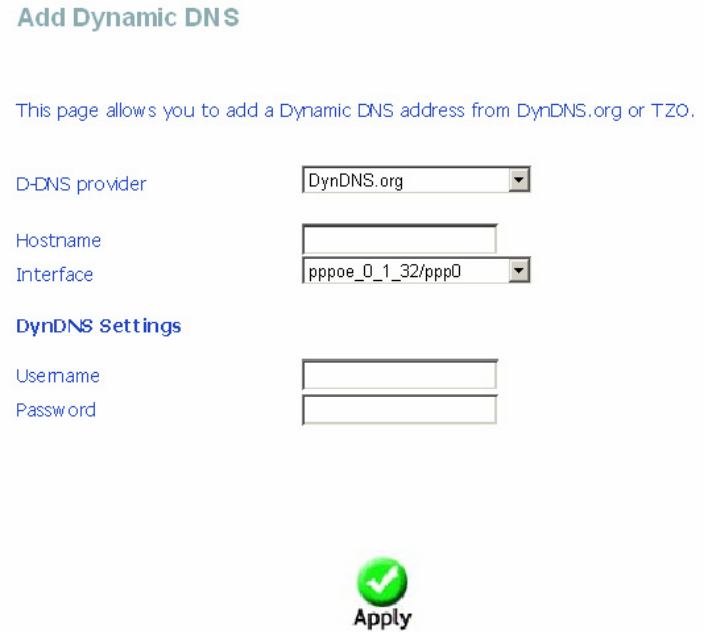
Dynamic DNS

Field	Description
Hostname (read-only)	The hostname of the server.
Username (read-only)	The access username of the DDNS service.
Service (read-only)	The service name of the selected WAN service.
Interface (read-only)	The selected WAN service.
Remove	Enable the check-box to select the DDNS service to be removed.
Add	Click to add a DDNS service. The Add Dynamic DNS window opens.
Remove	Click to remove the selected DDNS service(s).

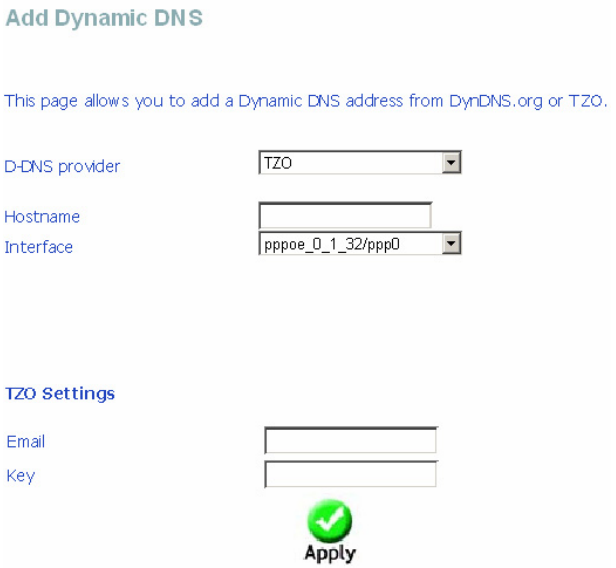


Click **Add,** the right page appears.
You can select the **D-DNS provider** from the drop-down list.

Field	Description
D-DNS provider	Select a DDNS service provider.
Hostname	Enter the hostname of the server.
Interface	Select a routing WAN service.
Username	Enter the access username of the DDNS service.
Password	Enter the password.
Apply	Click to save changes.

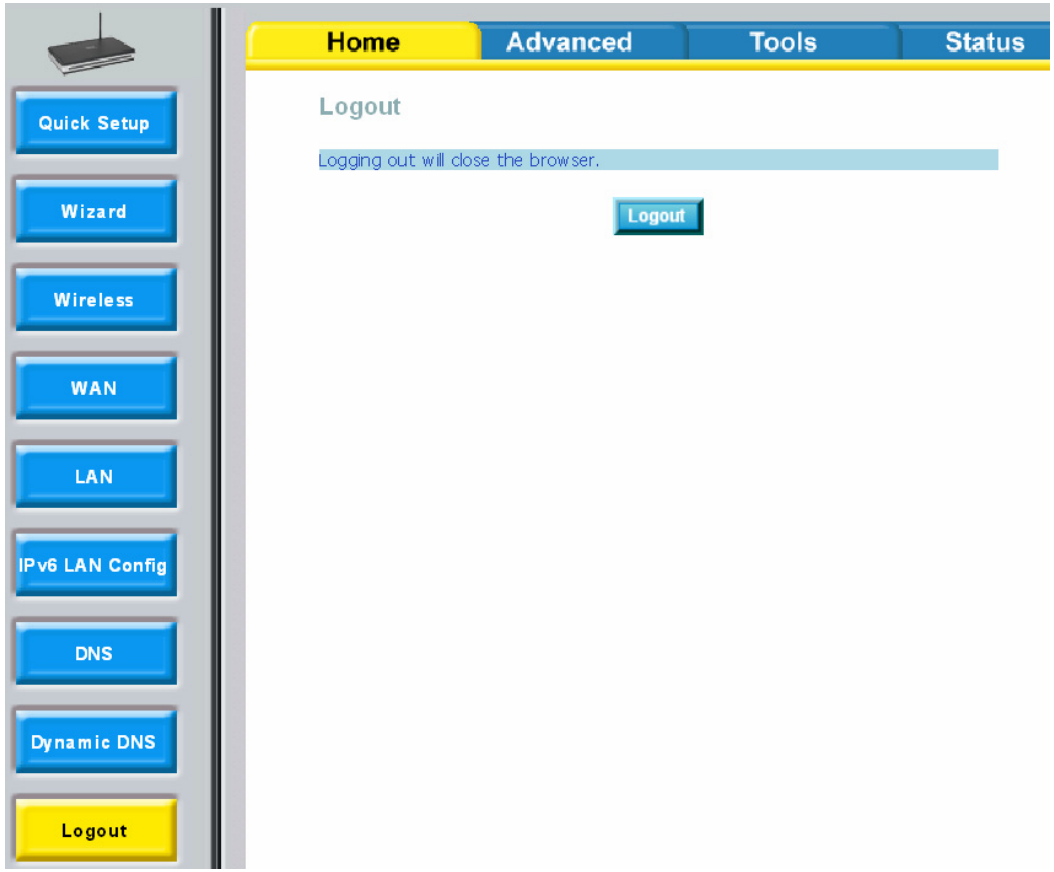


If you select the TZO as the D-DNS provider, the right page appears.
In this page, you should enter the email and key.



Logout

If you want to Logout, please click **Logout**.

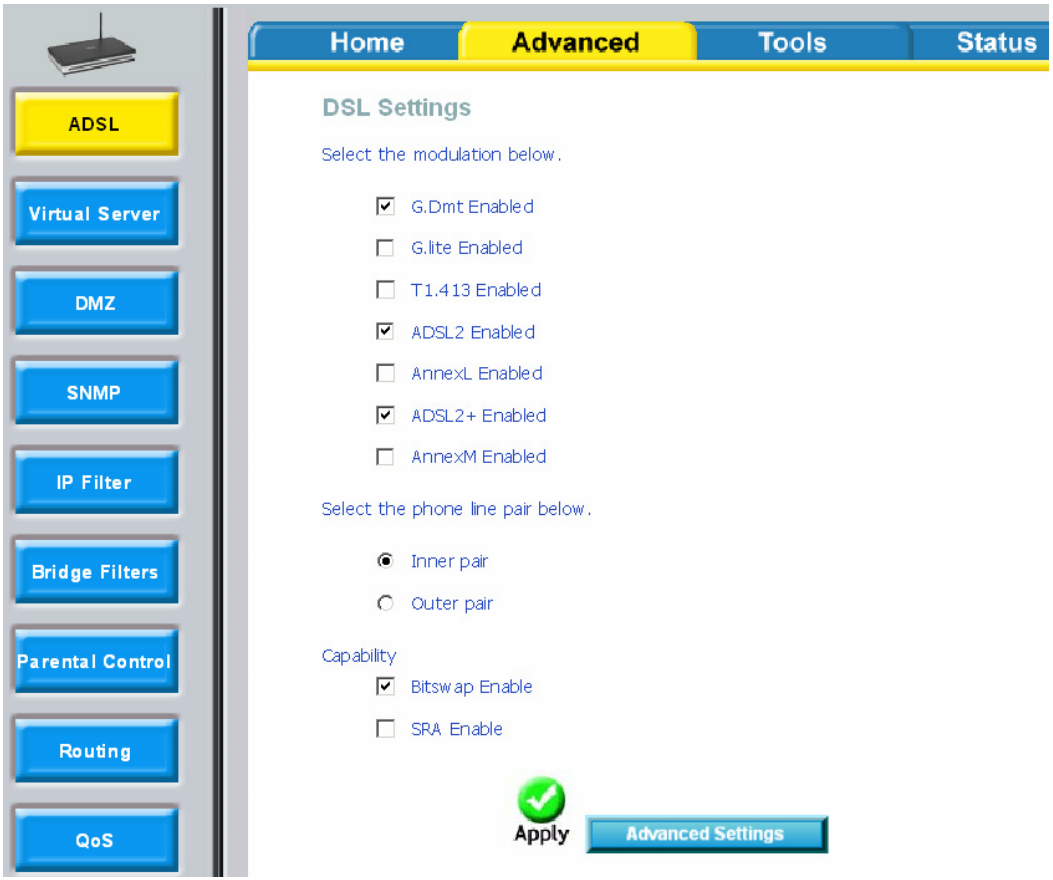


Advanced Configuration

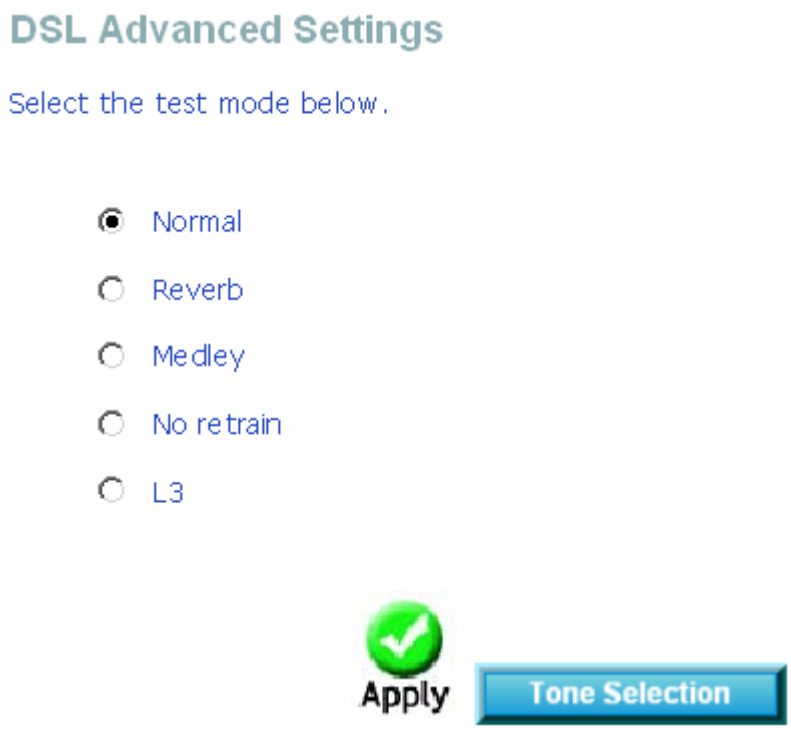
ADSL Configuration

This page allows you to select the desired modulation, phone line pair, and capability. Carry out the following to configure the DSL Settings:

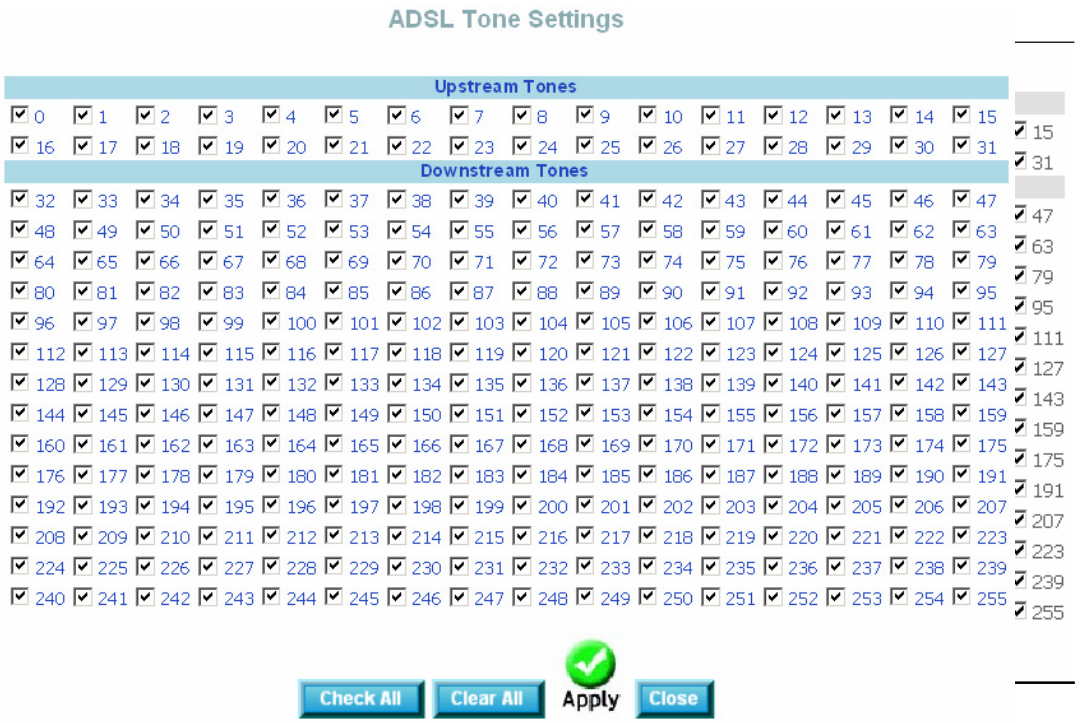
- Tick the text boxes of the modulation types you want to enable.
- Choose the **Inner pair** or **Outer pair** option by clicking the appropriate radio button.
- Tick the text boxes of the capability options you want to enable.
- Click the **Save/Apply** button when you are finished.



Click **Advanced Settings** to select a DSL test mode.
Select the desired DSL test mode and then click the **Apply** button.



Click the **Tone Selection** button to modify the upstream and downstream tones. Select the appropriate upstream and downstream tones for your ADSL connection. Click the **Apply** button to let your settings take effect.



NAT-Virtual Server Configuration

By default, DSL router blocks all external users from connecting to or communicating with your network. Therefore, the system is safe from hackers who may try to intrude into the network and damage it.

However, you may want to expose your network to the Internet in limited and controlled ways in order to enable some applications to work from the LAN (for example, game, voice, and chat applications) and to enable Internet access to servers in the home network. The port forwarding feature supports both functionalities. This topic is also referred as Local Servers.

The port forwarding page is used to define applications that require special handling by DSL router. All you need to do is to select the application protocol and the local IP address of the computer that is using or providing the service. If required, you may add new protocols in addition to the most common ones provided by DSL router.

For example, if you wanted to use a file transfer protocol (FTP) application on one of your PCs, you would simply select FTP from the list and enter the local IP address or host name of the designated computer. All FTP-related data arriving at DSL router from the Internet henceforth is forwarded to the specific computer.

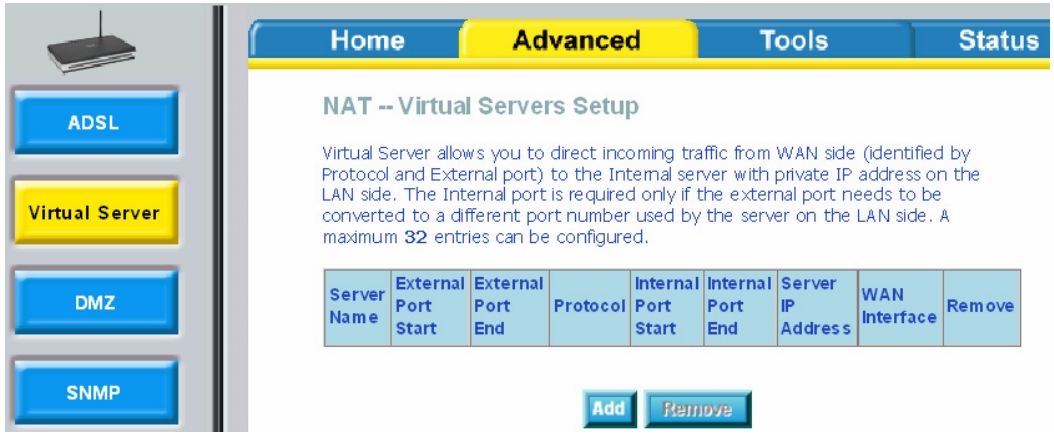
Similarly, you can grant Internet users access to servers inside your home network, by identifying each service and the PC that provide it. This is useful, for example, if you want to host a Web server inside your home network.

When an Internet user points his/her browser to DSL router external IP address, the gateway forwards the incoming HTTP request to your Web server. With one external IP address (DSL router main IP address), different applications can be assigned to your LAN computers, however each type of application is limited to use one computer.

For example, you can define that FTP uses address X to reach computer A and Telnet also uses address X to reach computer A. But attempting to define FTP to use address X to reach both computer A and B fails. DSL router, therefore, provides the ability to add additional public IP addresses to port forwarding rules, which you must obtain from your ISP, and enter into the IP addresses pool. Then, you can define FTP to use address X to reach computer A and address Y to reach computer B.

Additionally, port forwarding enables you to redirect traffic to a different port instead of the one to which it was designated. For example, if you have a Web server running on your PC on port 8080 and you want to grant access to this server to any one who accesses DSL router via HTTP.

Click Virtual Server, and the right page appears. The port forwarding (virtual server) page is used to define applications that require special handling by DSL router.



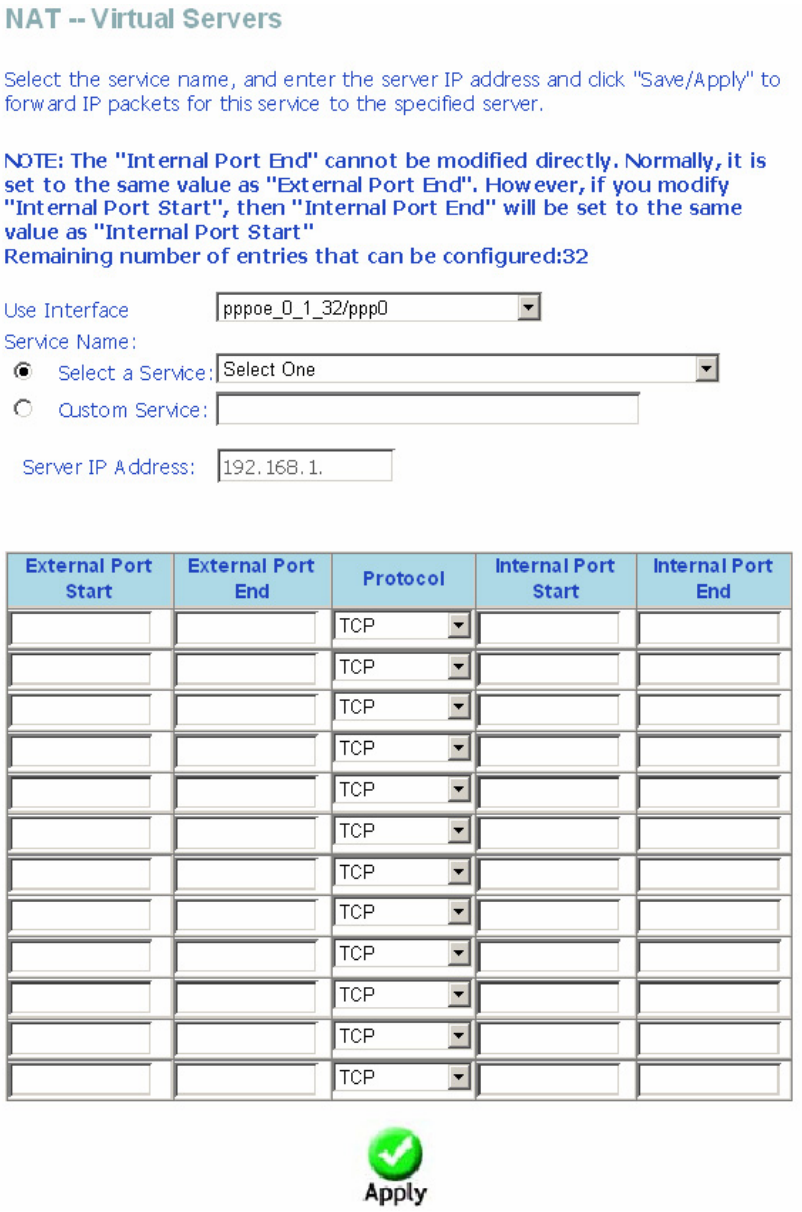
To set up virtual servers for a service, click **Add**.

- Select the use Interface like that pppoe_0_1_32/ppp0 and select a service or enter a custom server.
- Set **Server IP Address**.
- Enter the Server IP address of the computer that provides the service (the server in the **Local Host** field). Note that unless an additional external IP address is added, only one LAN computer can be assigned to provide a specific service or application.
- Set **External Port Start** and **External Port End**.
- Select **Protocol**.
- Set **Internal Port Start** and **Internal Port End**.
- Enter **Remote IP**.
- Click **Apply** to apply the settings.

If the application you require is not in the list, manually enter the information.

Deleting Virtual Servers:

- Select the **Remove** check box.
- Click **Remove** to remove the settings.



DMZ Host

The demilitarized military zone (DMZ) host feature allows one local computer to be exposed to the Internet. This function is applicable for:

- Users who want to use a special-purpose Internet service, such as an on-line game or video conferencing program, that is not presented in the port forwarding list and for which no port range information is available.
- Users who are not concerned with security and wish to expose one computer to all services without restriction.

***Note**: A DMZ host is not protected by the firewall and may be vulnerable to attack. This may also put other computers in the home network at risk. Hence, when designating a DMZ host, you must consider the security implications and protect it if necessary.*

You can set up a client in your local network as a so-called DMZ host. Your device then forwards all incoming data traffic from the Internet to this client. You can, for example, operate your own Web server on one of the clients in your local network and make it accessible to Internet users. As the exposed host, the local client is directly visible to the Internet and therefore particularly vulnerable to attacks (for example, hacker attacks). Enable this function only when necessary (for example, to operate a Web server) and when other functions (for example, port forwarding) are inadequate. In this case, you should take appropriate measures for the clients concerned.

***Note**: Only one PC per public IP address can be set up as an exposed host.*

Adding a DMZ Host

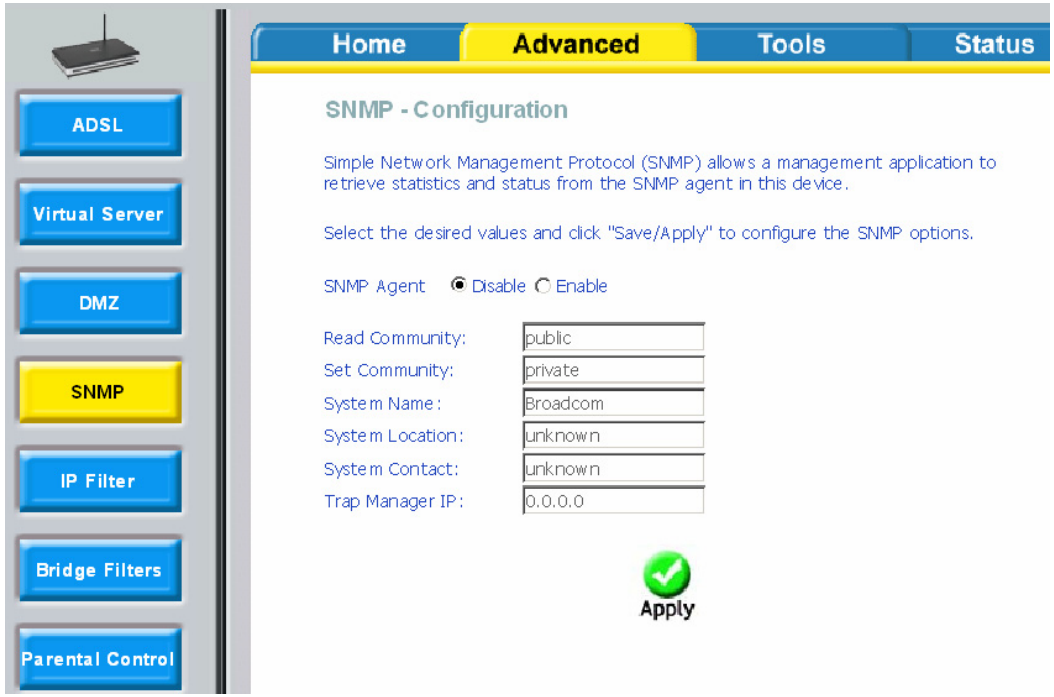
- To set up a PC as a DMZ host, click **DMZ**.
- Enter the local IP address of the PC that is to be enabled as an exposed host.
- Click **Apply** to apply the settings.

Remove DMZ host

- Clear the DMZ Host Address.
- Click **Apply** to apply the settings.

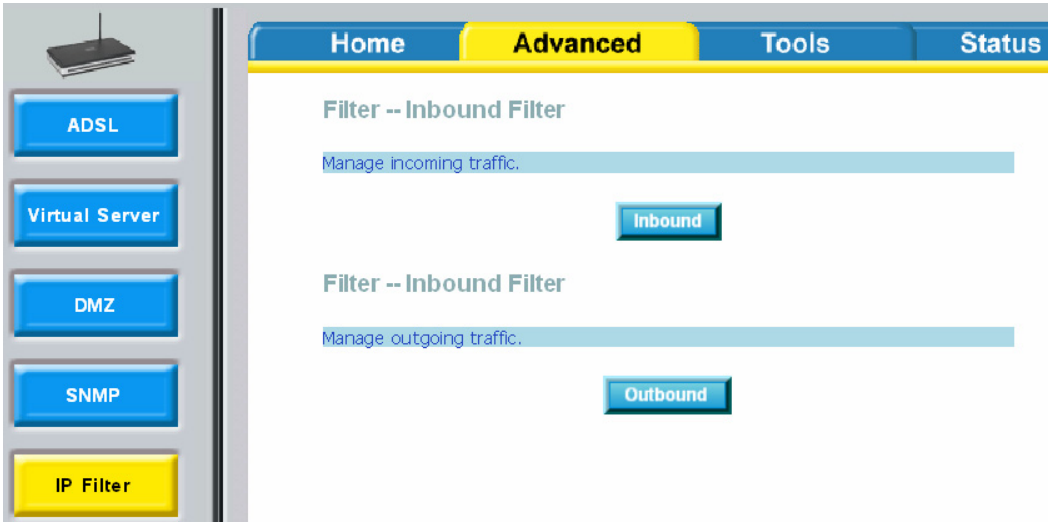
SNMP Configuration

Click **SNMP** and the right page appears.
Click **Enable** to open SNMP function, enter the configuration that your ISP has provided to you. Then click **Apply**.



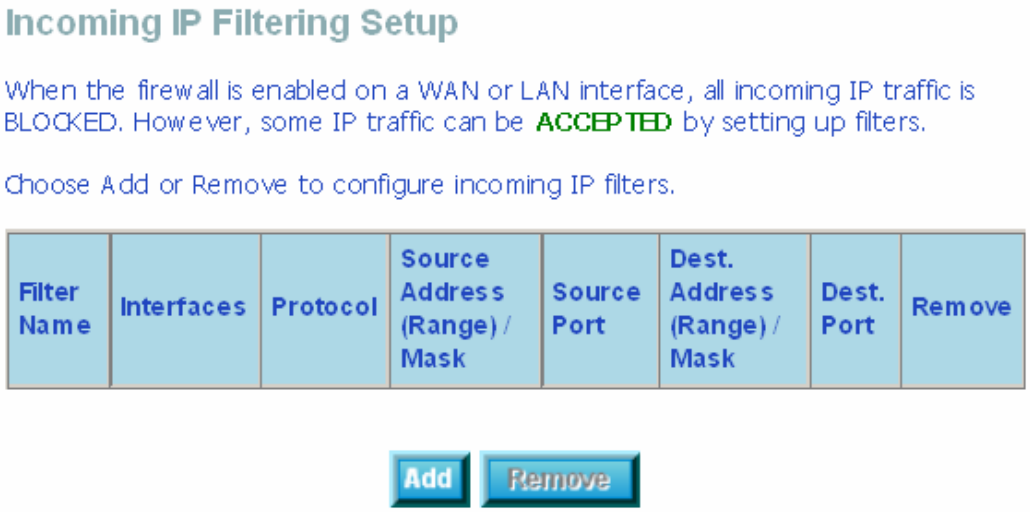
IP Filter Configuration

Click **IP Filter** and the right page appears. By default, the firewall is enabled. The firewall is used to block document transmissions between the Internet and your PC. It serves as a safety guard and permits only authorized documents to be sent to the LAN.



Incoming IP Filtering

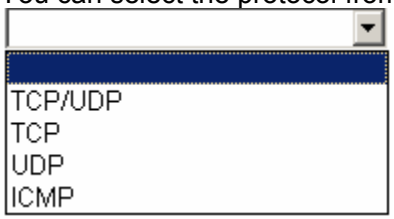
Click **Inbound**, the right page appears.
By default, all incoming IP traffic from the WAN is blocked when the firewall is enabled. However, some IP traffic can be accepted by setting up filters.

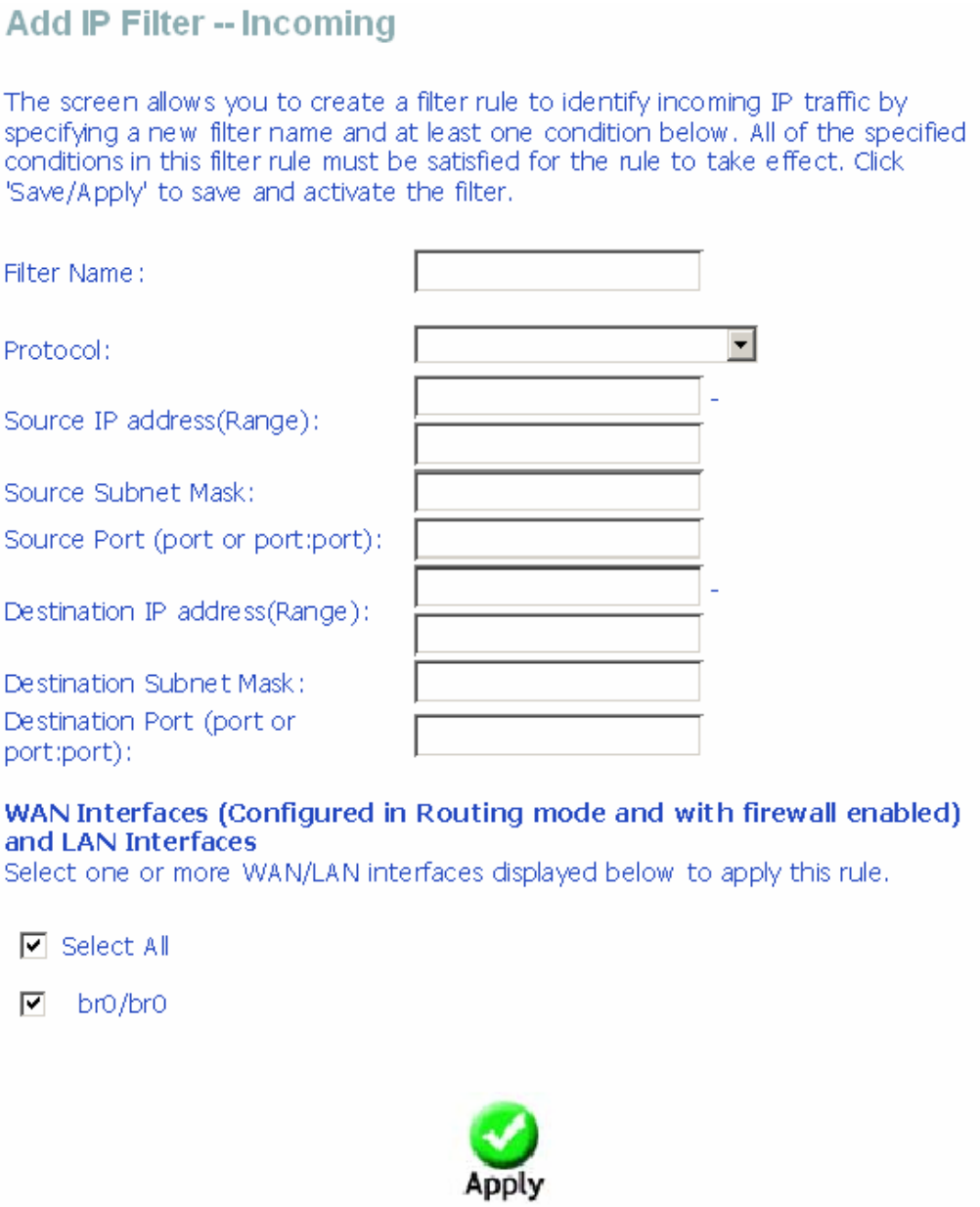


Click **Add**, the right page appears. In this page, you can create a filter rule to identify incoming IP traffic by specifying a new filter name and at least one condition. All specified conditions in this filter rule must comply with the rule. Click **Apply** to save and activate the filter.

You should select at least one WAN interface to apply this rule.

You can select the protocol from the drop-down list.

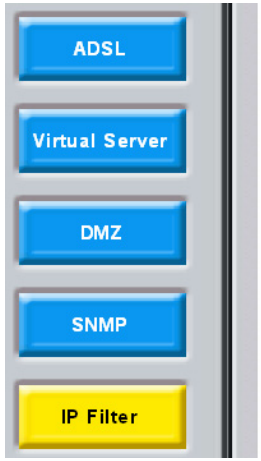


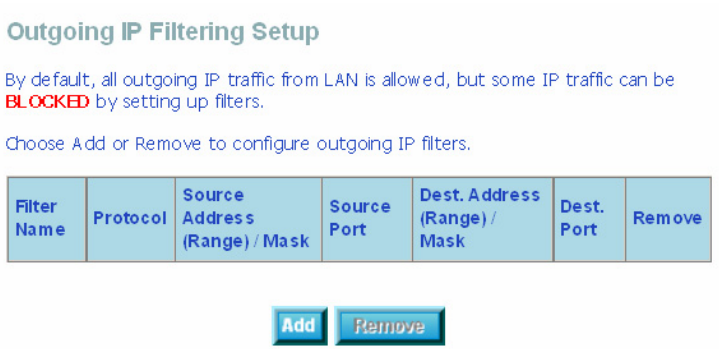


Outgoing IP Filtering

Click **Outboud**, and the right page appears.

By default, all outgoing IP traffic from LAN is allowed, but some IP traffic can be blocked by setting up filters.



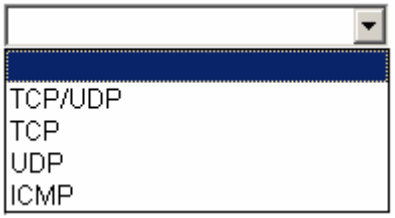


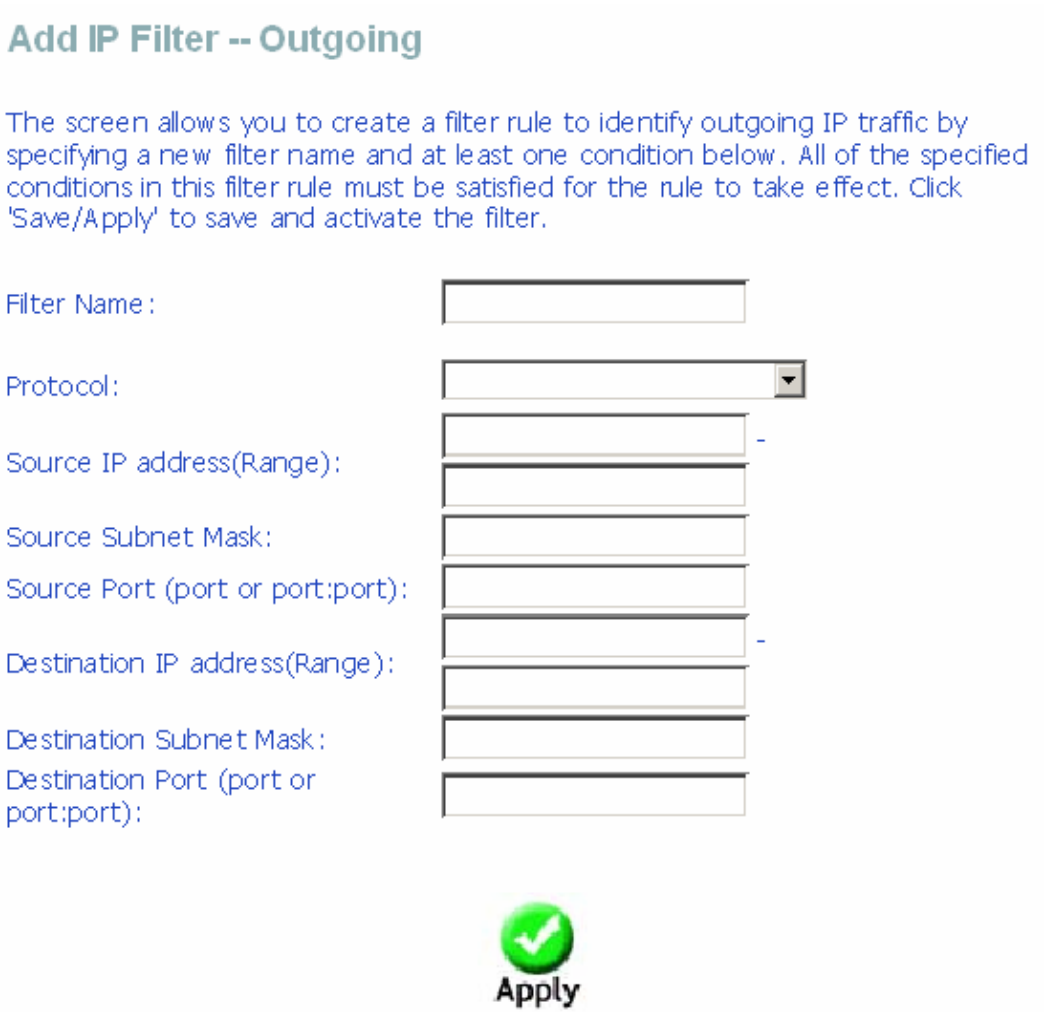
Click **Add** and the page for defining the IP filtering rule appears.

In this page, you can create a filter rule to identify outgoing IP traffic by specifying a new filter name and at least one condition. All specified conditions in the filtering rule must be complied with the rule to take effect.

Click **Apply** to save and activate the filter.

You can select the protocol from the drop-down list.



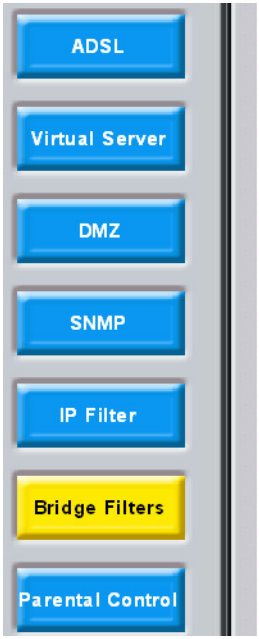


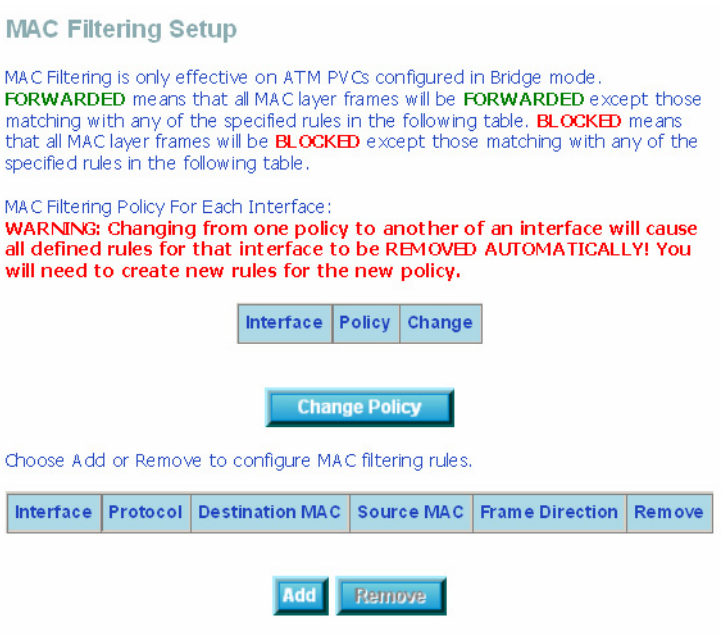
Bridge Filter Configuration

Click **Bridge Filters** and the right page apperas.

MAC Filtering is only effective on ATM PVCs configured in Bridge mode. Forwarded means that all MAC layer frames are forwarded except those matching with any of the specified rules in the following table. Blocked means that all MAC layer frames are blocked except those matching with any of the specified rules in the following table.

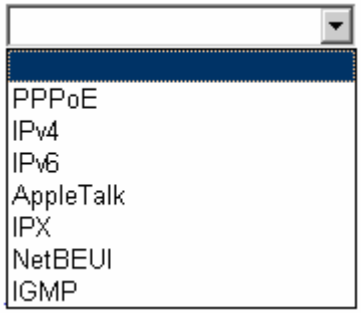
Click **Change Policy** and the following page apperas.Then you can change the MAC Filtering Global Policy from FORWARDED to BLOCKED.



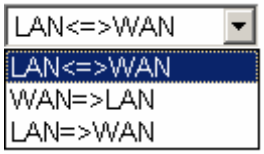


Click **Add**, the right page appears.

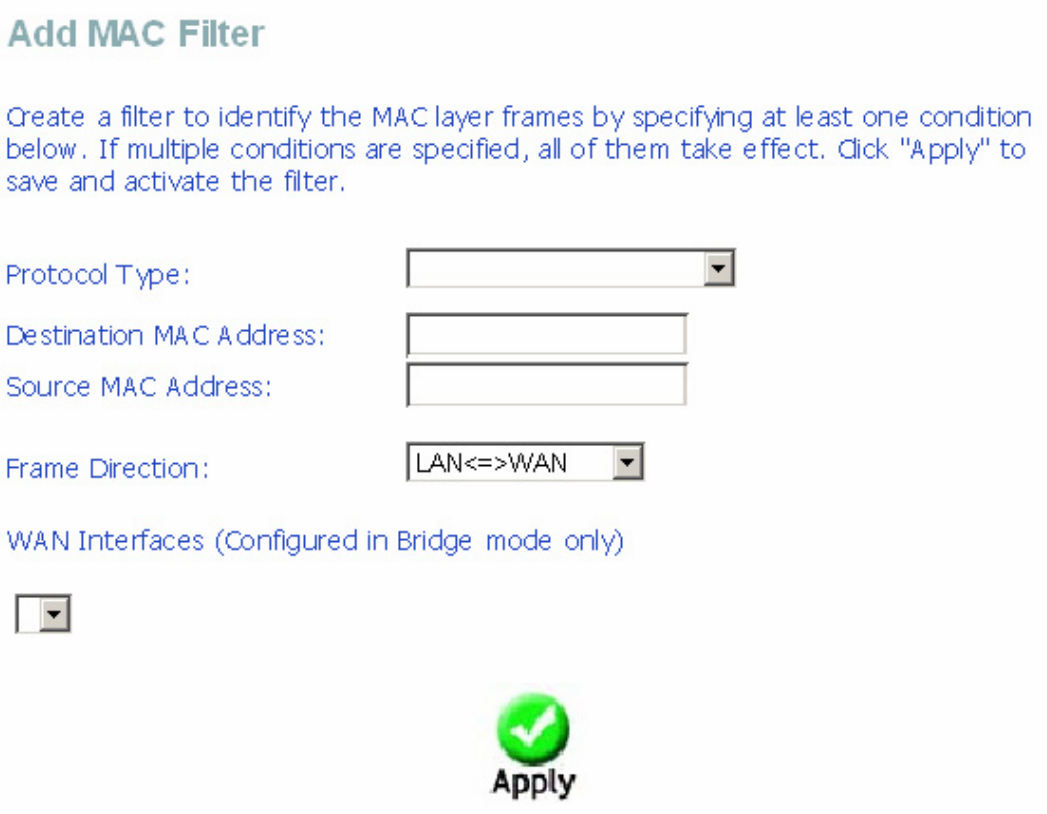
You can select the protocol type from the drop-down list.



You can select the protocol type from the drop-down list.



After proper configuration, click **Apply**.

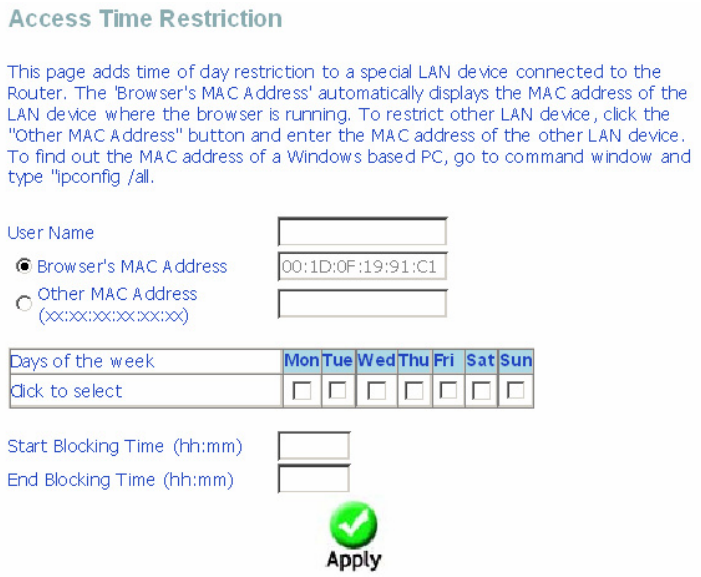


Parental Control

Click **Parental Control** and the right page appears.

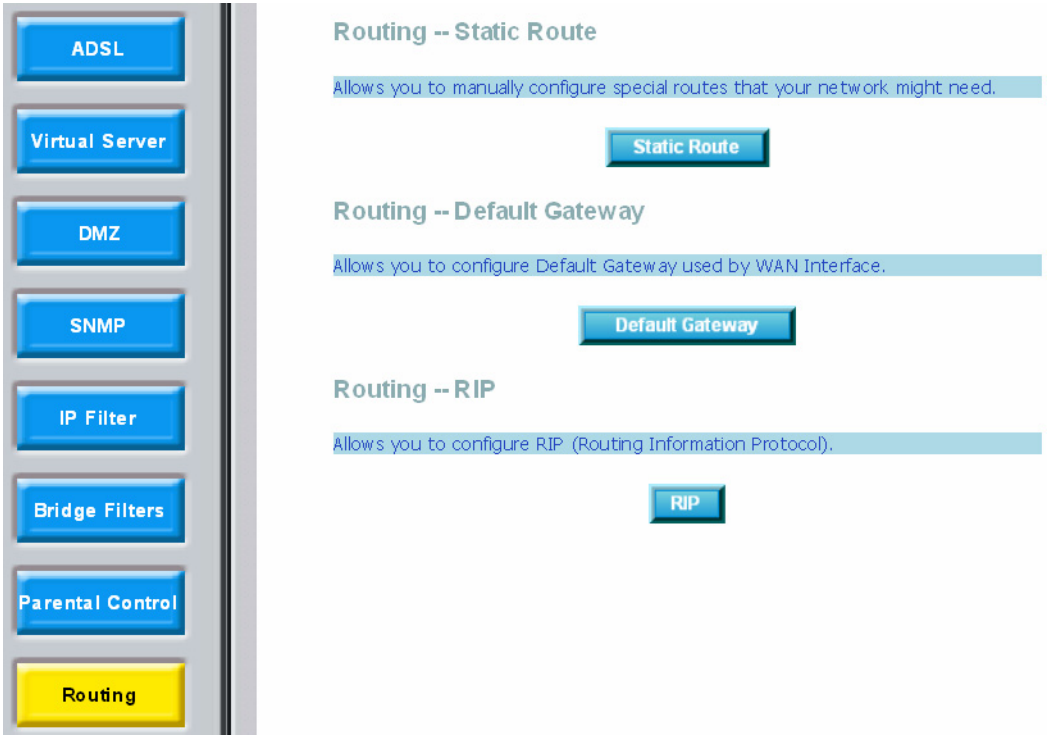
Click **Add**, the right page appears.

In this page, you can add time of day restriction to a special LAN device connected to the Router. The **Browser's MAC Address** automatically displays the MAC address of the LAN device where the browser is running. To restrict other LAN device, click **Other MAC Address** and enter the MAC address of the another LAN device. To obtain the MAC address of a Windows based PC, enter **ipconfig /all** in the DoS window.



Routing Configuration

Click **Routing** and the right page appears.

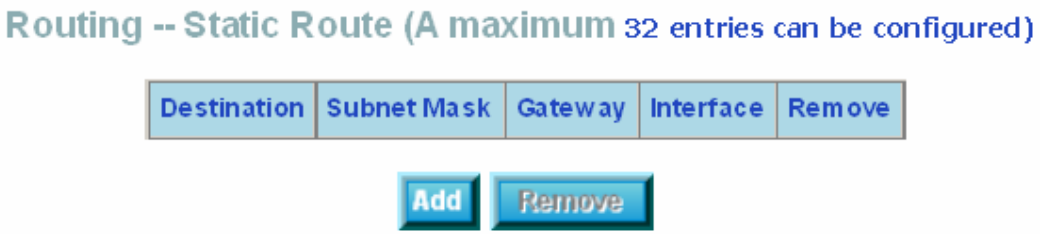


Static Route Configuration

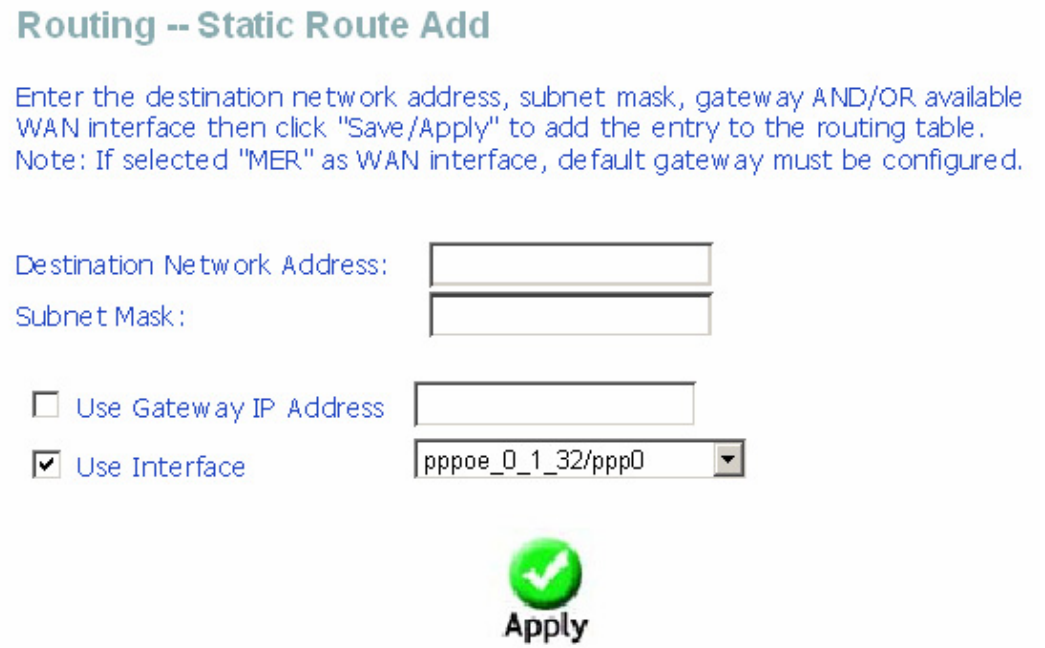
Click **Static Route**, the right page appears.

In this interface, you can query the preset static routes, delete an existing static route, or add a new static route. By default, the system has no static route information.

- **Destination**: The IP address to which packets are transmitted.
- **Subnet Mask**: The subnet mask of the destination IP address.
- **Gateway**: The gateway that the packets pass by during transmission.
- **Interface**: The interface that the packets pass through on the modem.



Click **Add** to add the static routing. Enter the destination network address, subnet mask, gateway AND/OR available WAN interface, then click **Apply** to add the entry to the routing table.

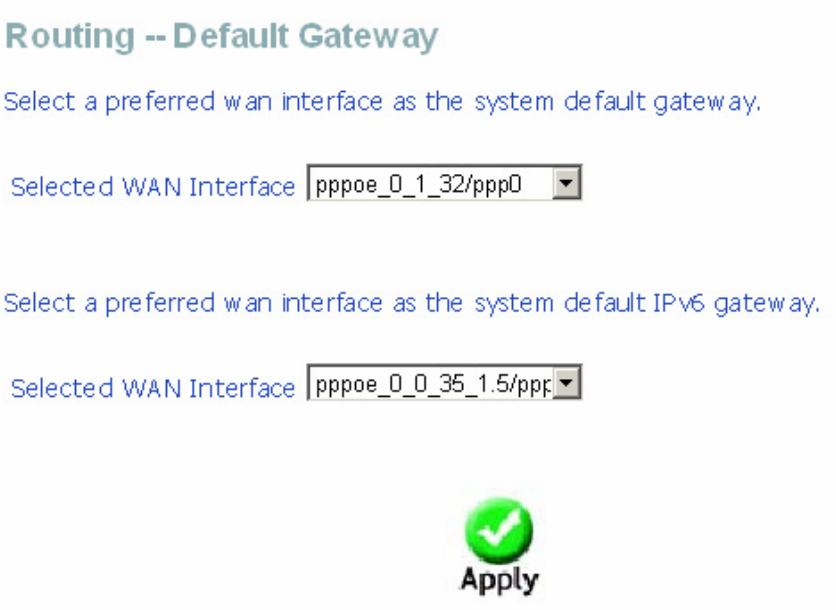


Default Gateway

Click **Default Gateway** to choose the default gateway.

In this page, you can modify the default gateway settings.

If you select **Enable Automatic Assigned Default Gateway**, this router can accept the first received default gateway assignment from one of the PPPoA, PPPoE or MER/DHCP enabled PVC(s). If the check box is not selected, you need to enter the static default gateway and/or a WAN interface. Then, click **Apply**.

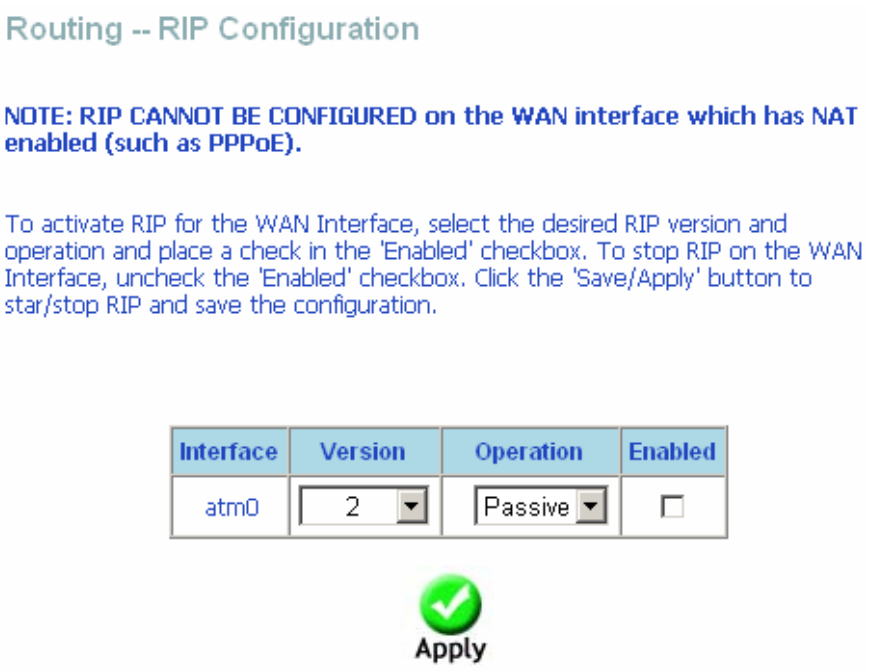


RIP

In the Routing page, click **RIP** and the right page appears.

- To activate RIP for the device, select **Enabled** for Global RIP Mode.
- To configure an individual interface, select the desired RIP version and operation, followed by selecting the **Enabled** checkbox for the interface.

Click **Apply** to save the configuration, and to start or stop RIP based on the Global RIP mode selected.

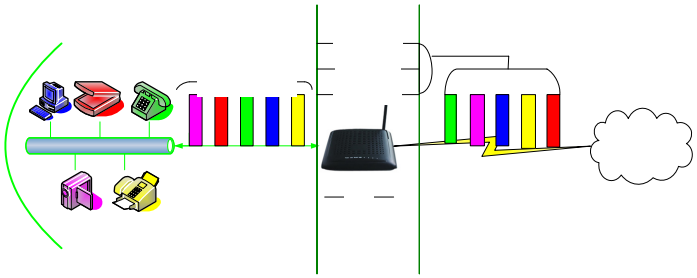


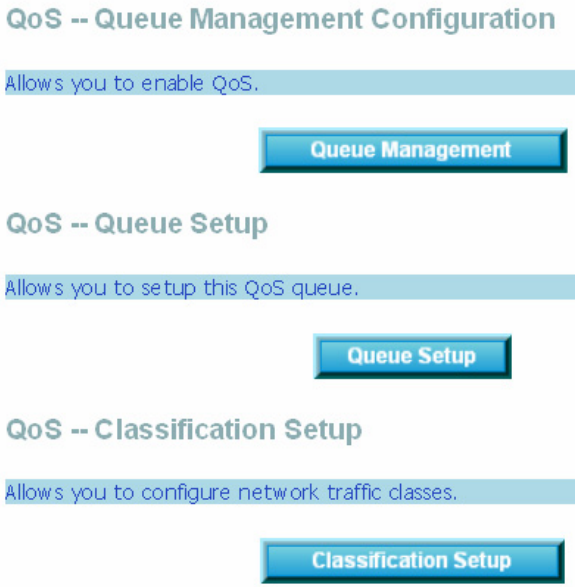
QoS

Many communication and multimedia applications require large, high-speed bandwidths to transfer data between the local network and the internet. However, for many applications there is often only one internet connection available with limited capacity. QoS divides this capacity between the different applications and provides undelayed, continuous data transfer in situation where data packets with higher priority are given preference.

Network QoS is an industry-wide set of standards and mechanisms for ensuring high-quality performance for critical applications. By using QoS mechanisms, network administrators can use existing resources efficiently and ensure the required level of service without reactively expanding or over-provisioning their networks.

Traditionally, the concept of quality in networks meant that all network traffic was treated equally. The result was that all network traffic received the network's best effort, with no guarantees for reliability, delay, variation in delay, or other performance characteristics. With best-effort delivery service, however, a single bandwidth-intensive application can result in poor or unacceptable performance for all applications. The QoS concept of quality is one in which the requirements of some applications and users are more critical than others, which means that some traffic needs preferential treatment.

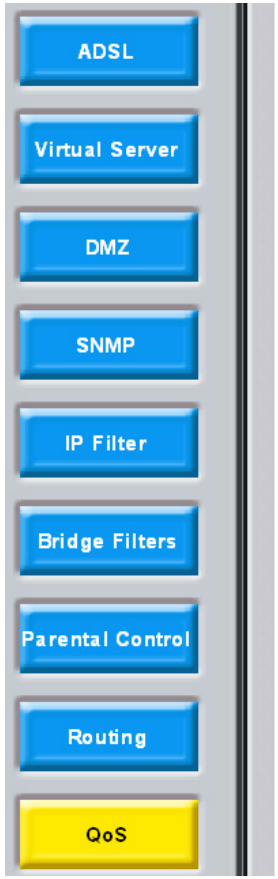


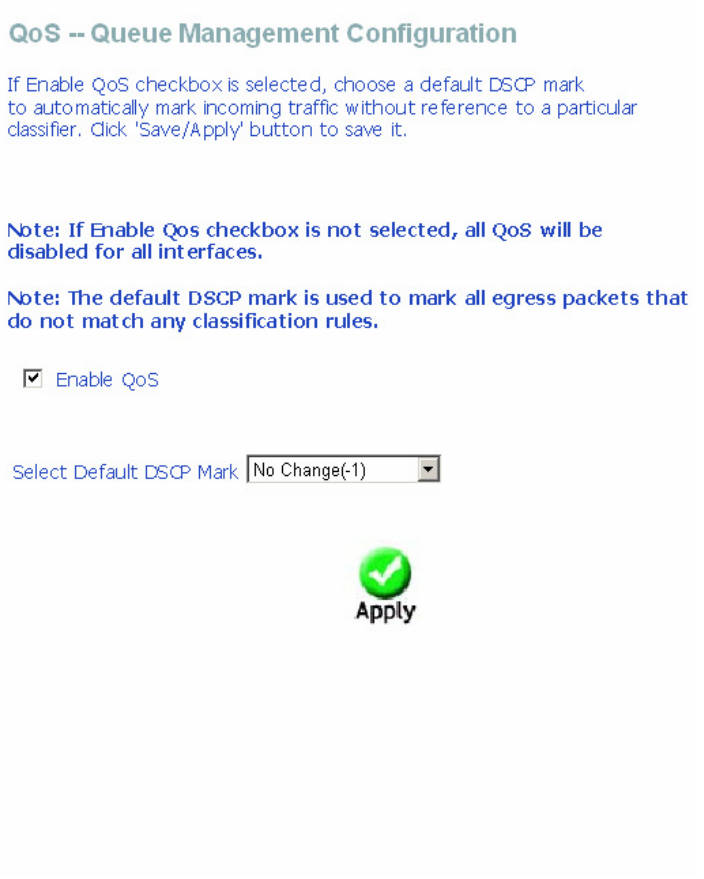


Queue Management

In the **QoS page**, click **Queue Management**, and the right page appears.

In this page, you can perform QoS queue management configuration. By default, the system enables QoS and sets a default DSCP mark to automatically mark incoming traffic without reference to particular classifier.



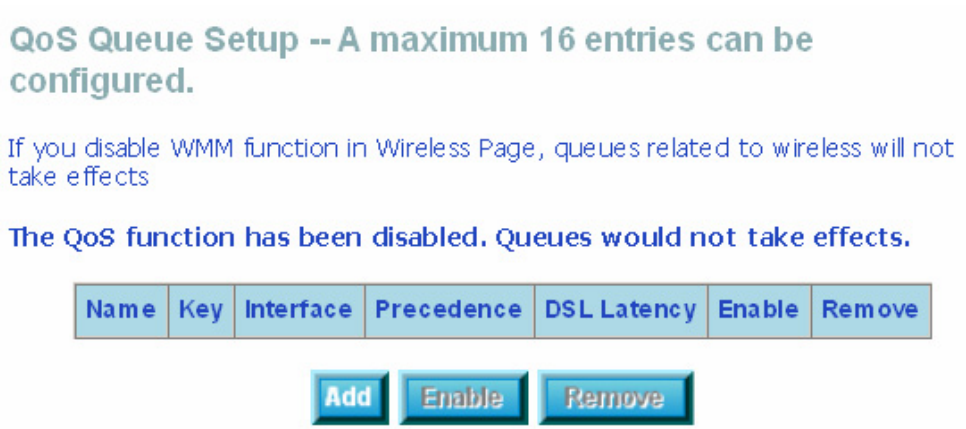


Queue Setup

In the **QoS page**, click **Queue Setup**, and the right page appears.
In this page, you can configure QoS queue. A maximum of 16 entries can be configured.

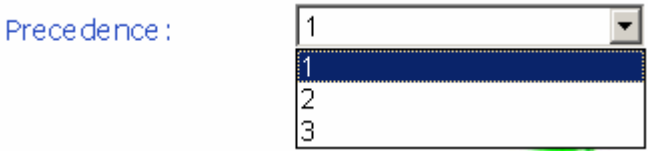
QoS Queue Setup can allocate four queues. Each of the queues can be configured for a precedence value (Lower integer values for precedence imply higher priority for this queue relative to others). The queue entry configured is used by the classifier to place ingress packets appropriately.

Note: *Lower integer values for precedence imply higher priority for this queue relative to others.*

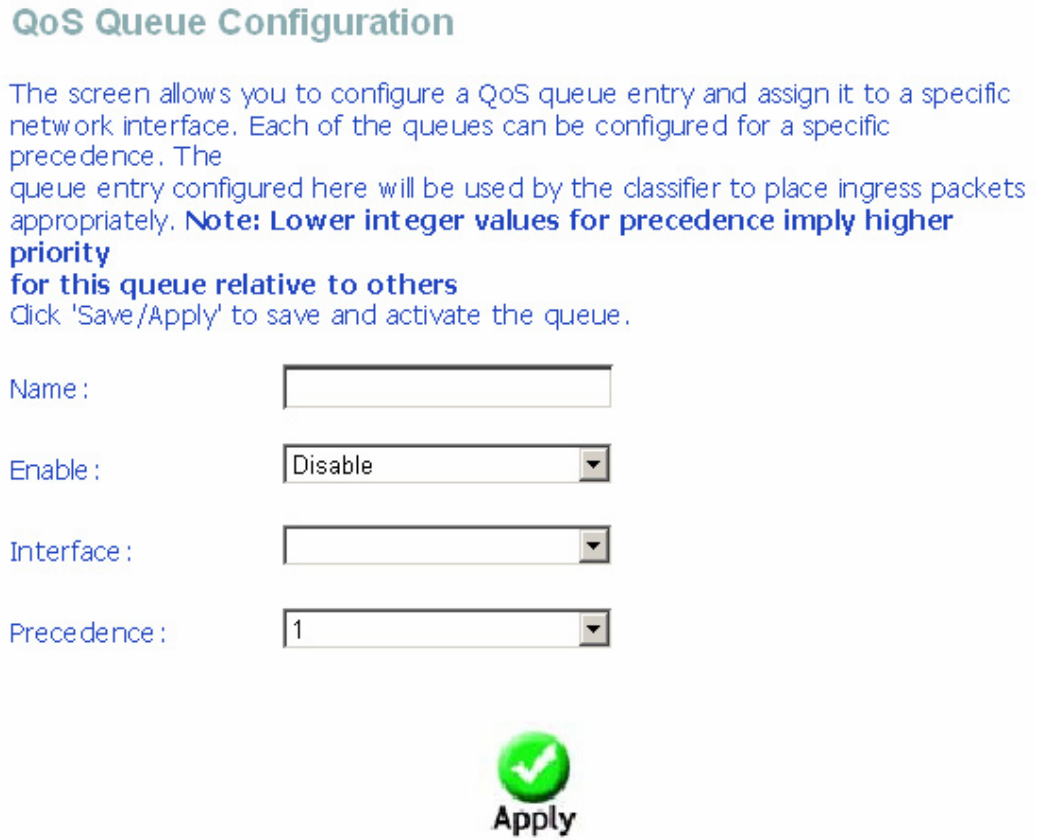


Click **Add** to set the queue.

Precedence: Select an integer value for queue precedence. After you select an integer value, the queue entry appropriately places to ingress packets. Lower integer values for precedence imply higher priority for this queue relative to others.

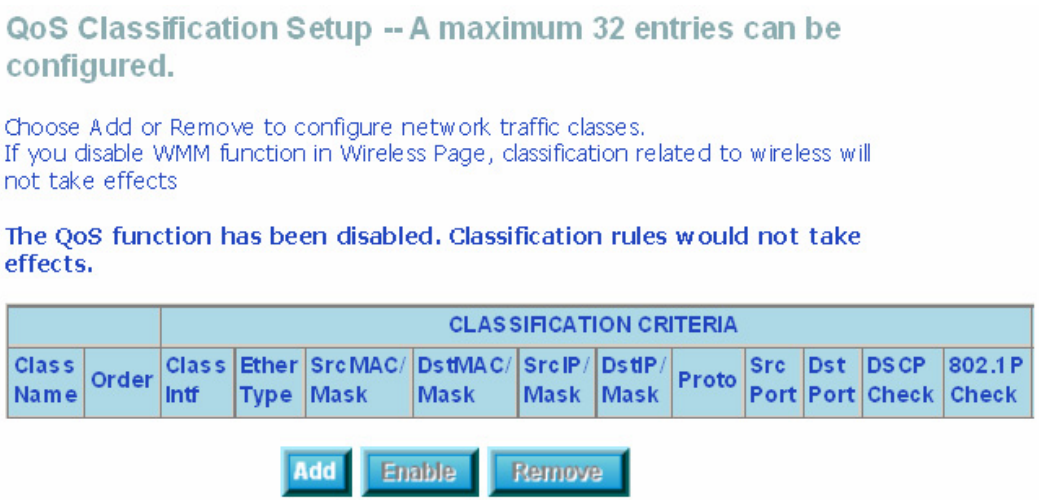


After proper configuration, click **Apply**.



Classification Setup

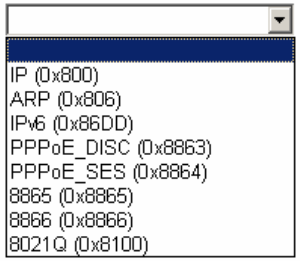
Click **Classification Setup** and the right page appears. In this page, you can configure network traffic classes.

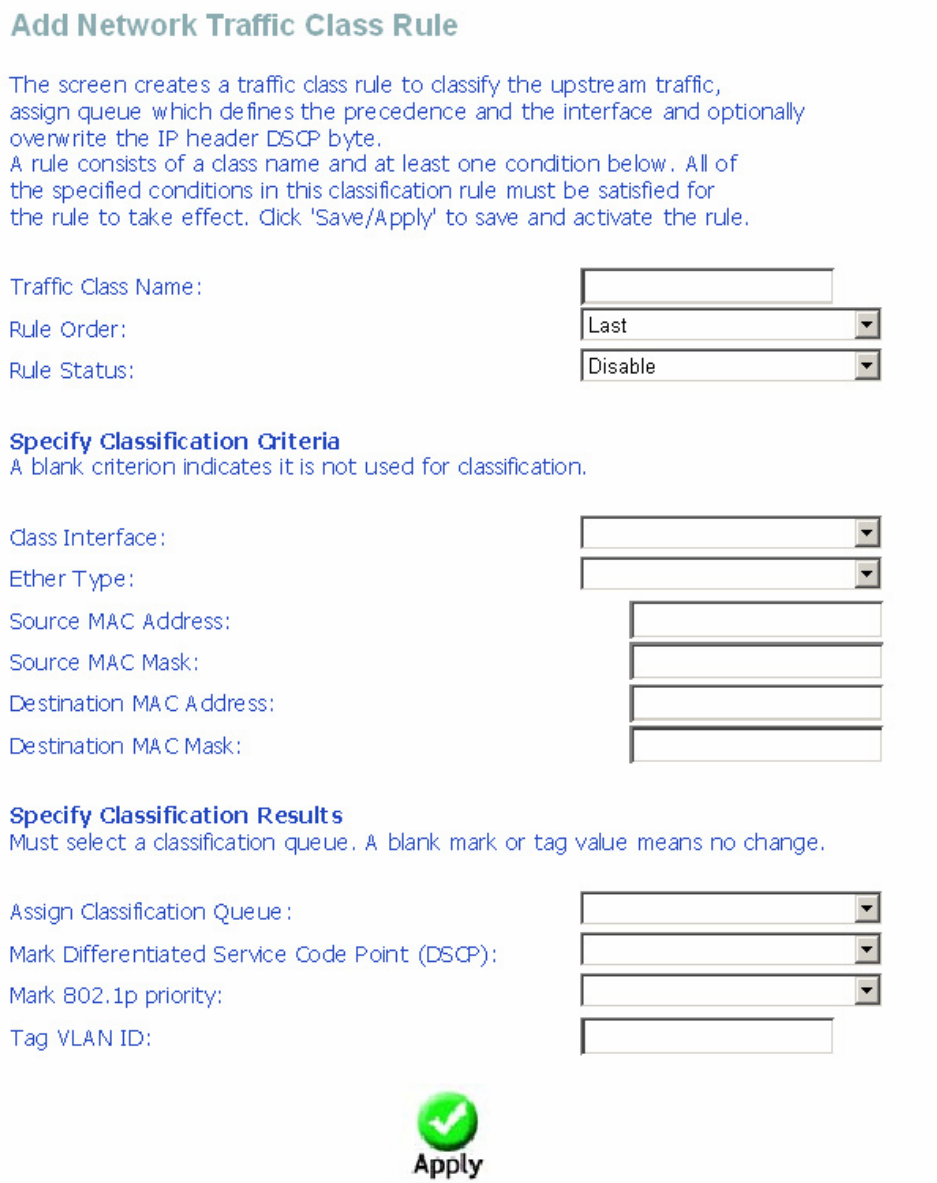


Click **Add** and the right page appears.

- **Traffic Class Name**: Enter a name of the class.
- **Rule Order**: Select order for queue.
- **Rule Status**: Enable or disable this traffic class rule.
- **Assign Classification Queue**: Select a classification queue.
- **Mark 802.1p priority**: Select an 802.1p priority number (0~7) that serves as the 802.1p value. Where level 7 is the highest one.

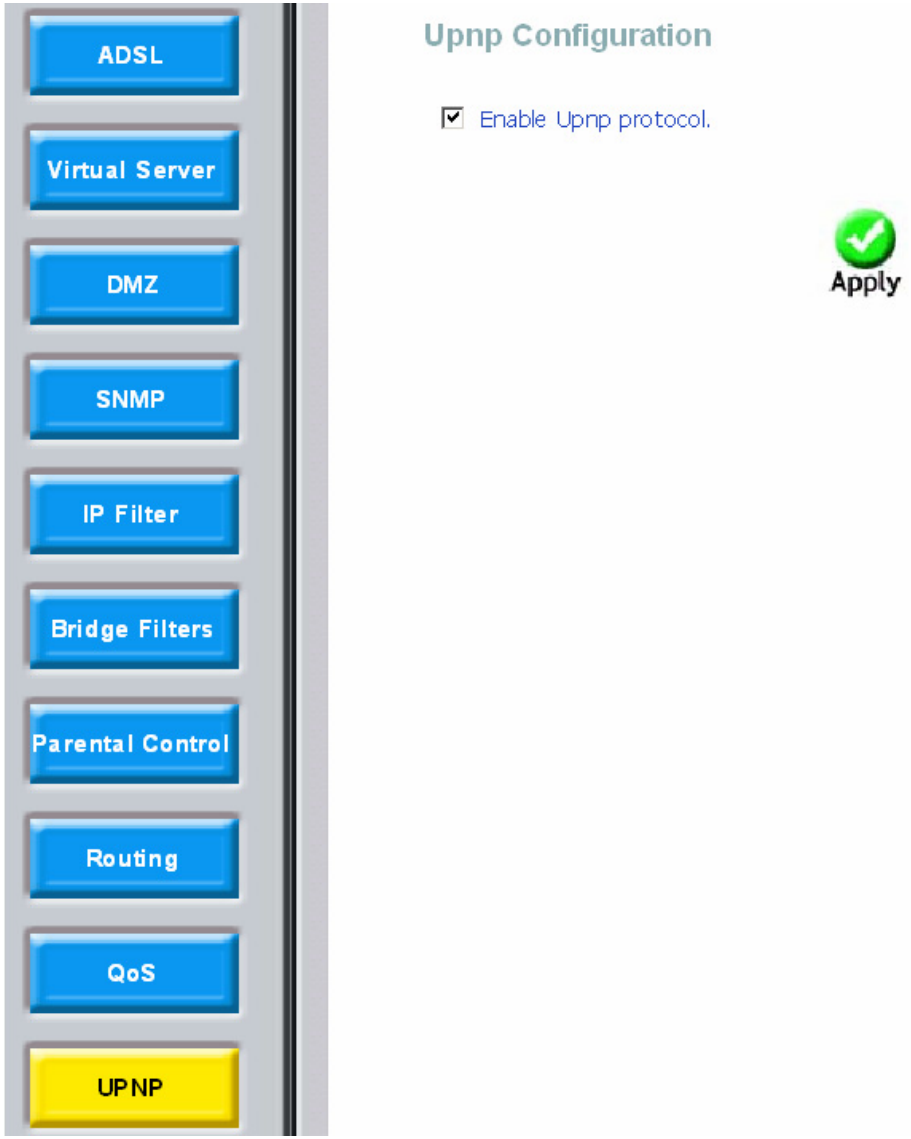
You can select the **Enter Type** from the drop-down list.





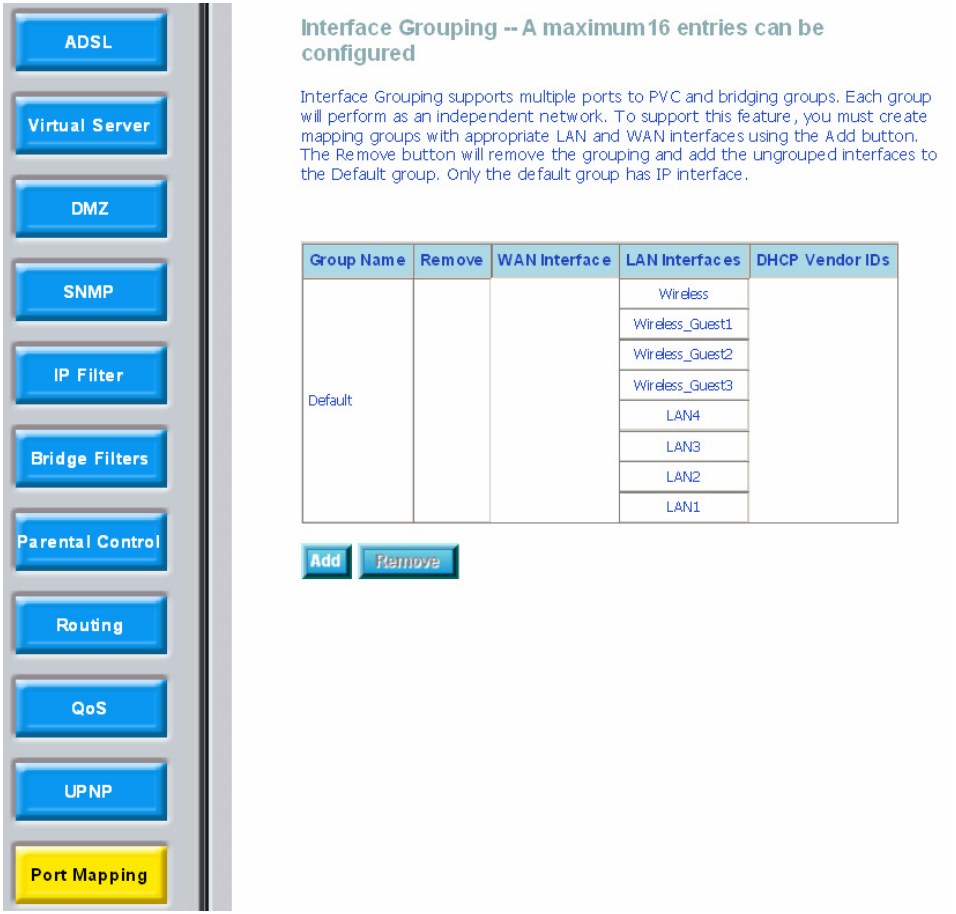
UPNP Configuration

In the **UPNP Configuration** page, you can enable the UPNP protocol.

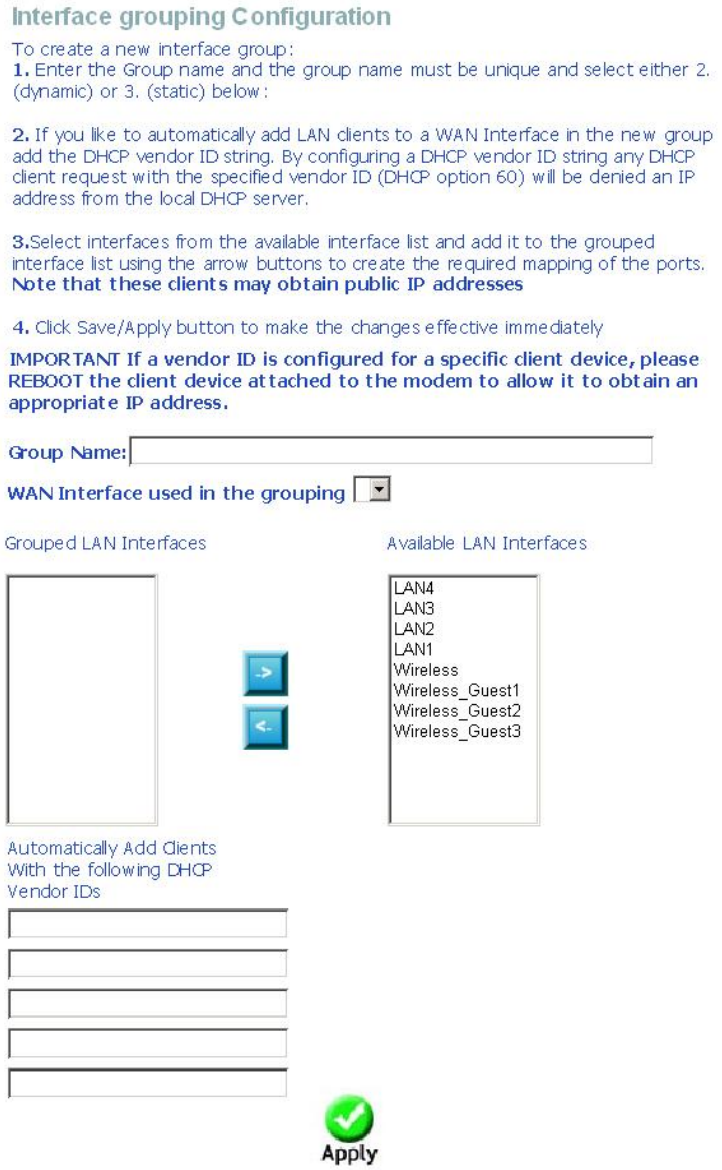


Port Mapping

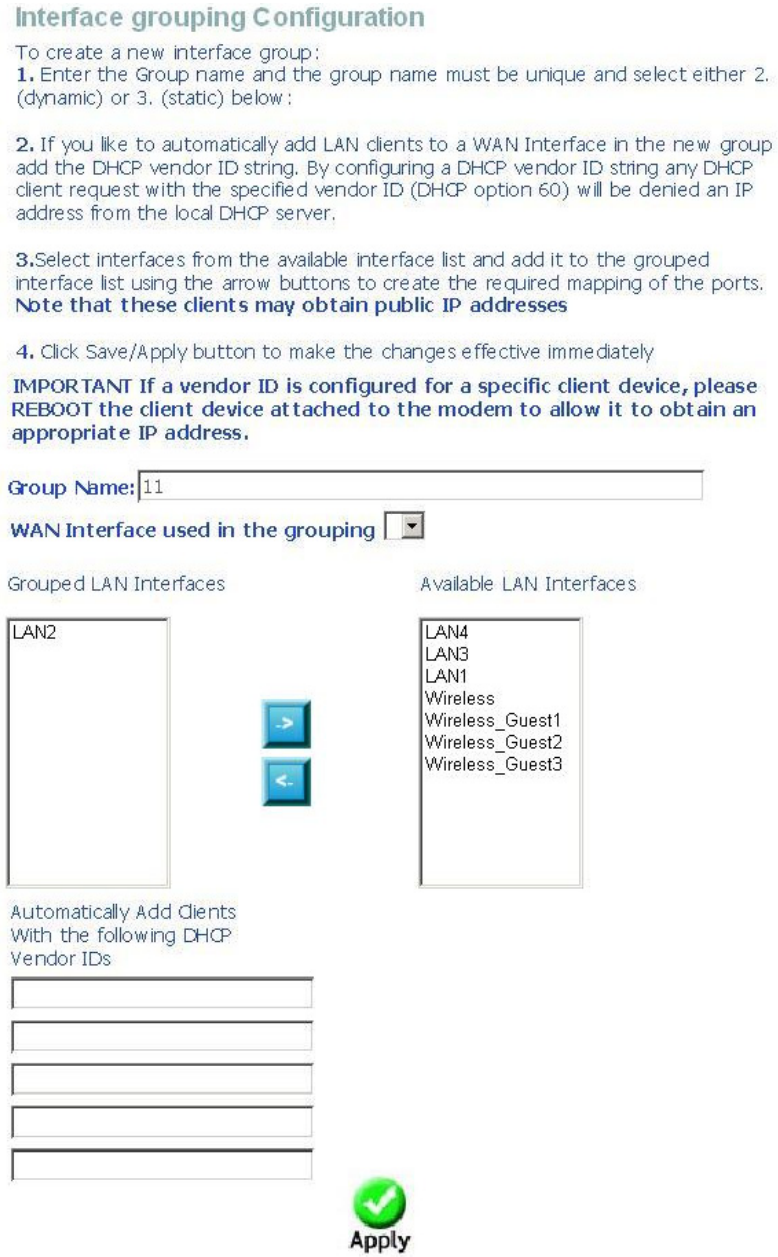
Click **Port Mapping**, the right page appears.
Note: *If you want to set Port Mapping, you need to enable the **LAN Ports** first.*



To create a new mapping group, click **Add.**

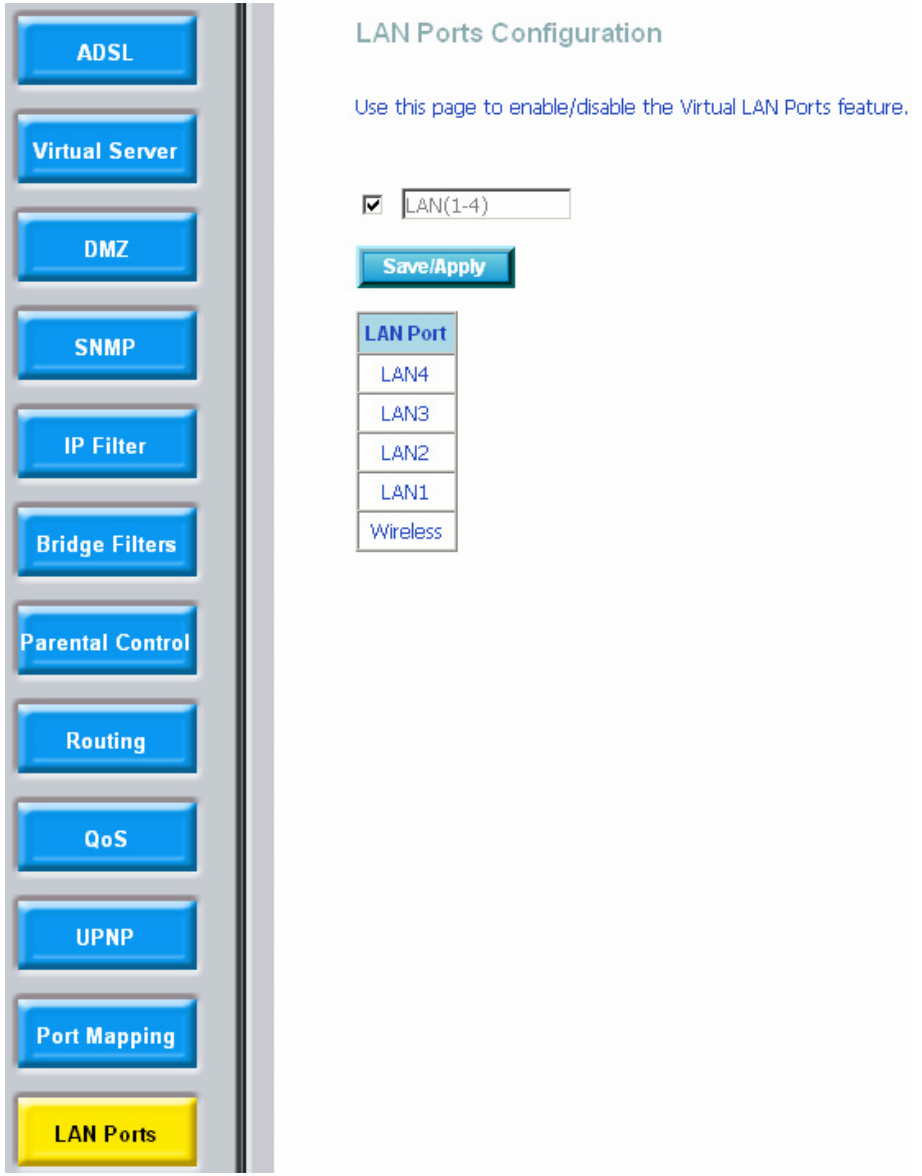


Field	Description
Group Name	Enter the Group name. It must be unique.
WAN Interface used in the grouping	Select interfaces from the available interface list.
Grouped LAN interfaces	Select an interface from the available interface list and add it to the grouped interface list using the arrow buttons to create the required mapping of the ports. The group name must be unique. **Note:** These clients may obtain public IP addresses. **Note:** The selected interfaces are removed from their existing groups and added to the new group.
Automatically Add Clients with the following DHCP Vendor IDs	If a vendor ID is configured for a specific client device, reboot the client device attached to the modem to allow it to obtain an appropriate IP address. (For example, the windows 2000/XP default DHCP client's vender ID is MSFT 5.0.).
Apply	Click to save changes.



LAN Ports

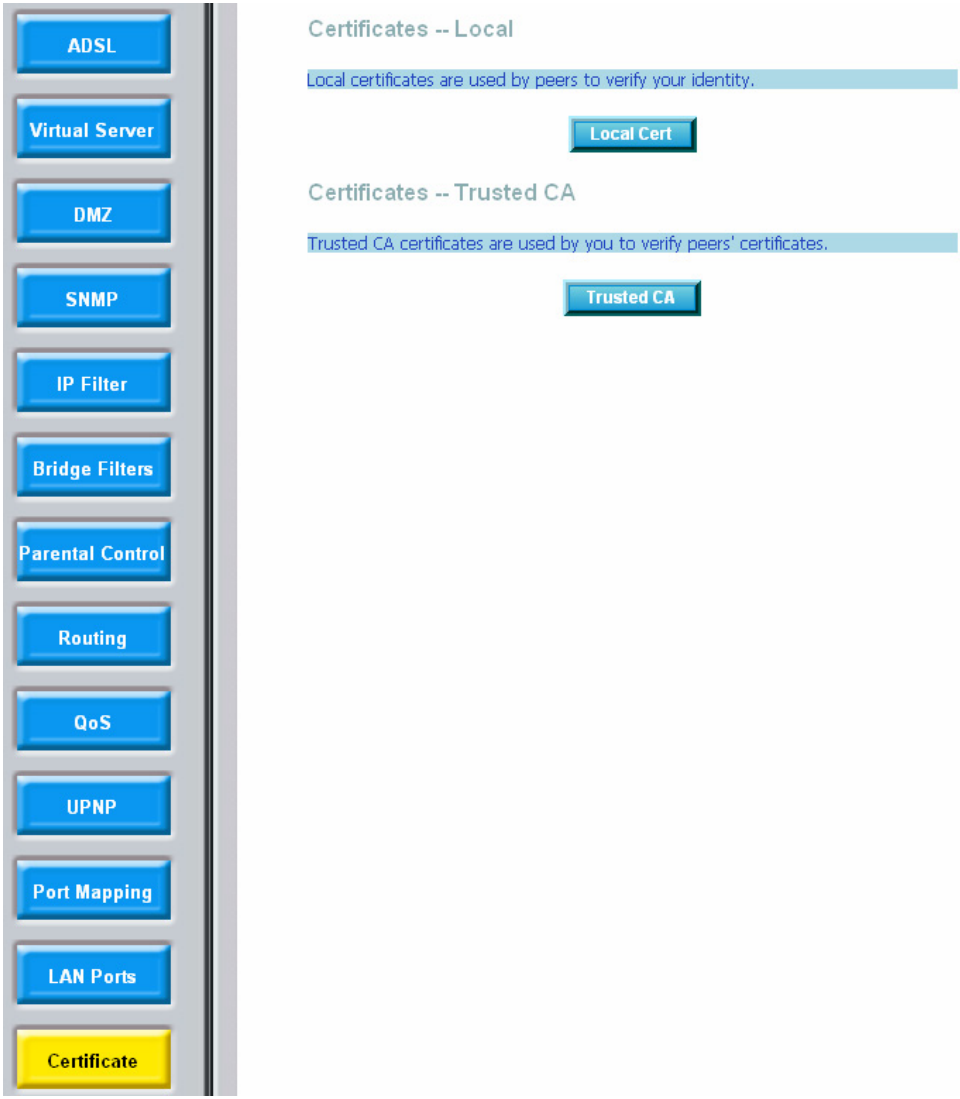
Click **LAN Ports** and the right page appears.



Certificate

Click **Certificate**, the right page appears.

In this page, **LocalCert** means local certificates. **TrustedCA** means trusted Certificate Authority certificates. Local certificates preserve the identity of the modem. CA certificates are used by the modem to very certificates from other hosts.

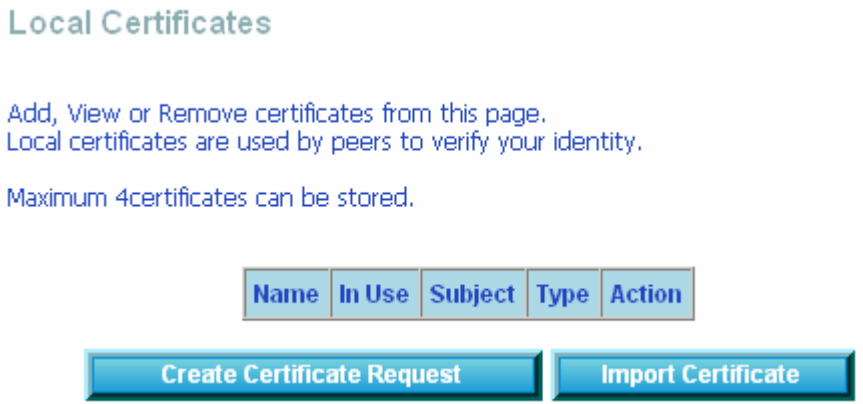


Local Certificate

Click **Local Certificate,** the right page appears.

Local certificates can be created by two ways:

- Create a new certificate request, have it signed by a certificate authority and load the signed certificate.
- Import an existing signed certificate directly.



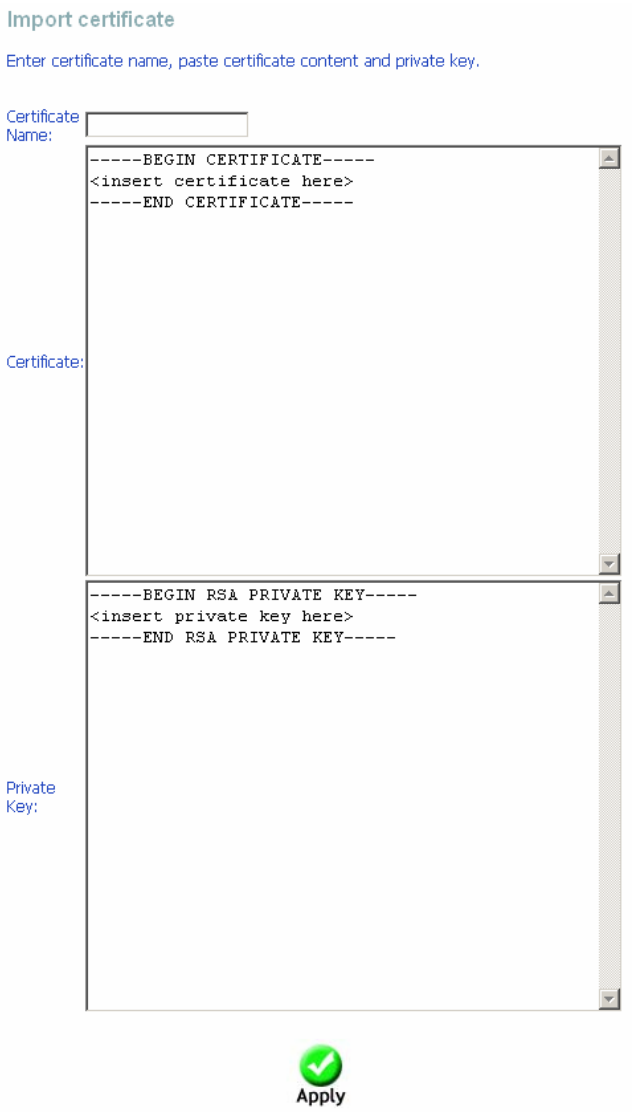
Create New Local Certificate

Click **Create Certificate Request,** the right page appears.

- **Certificate name:** Creates an SSL certificate in the specified certificate repository (administrator's or domain's repository) by using a private key file and a corresponding certificate file.
- **Common Name:** The common name is the "fully qualified domain name," (or FQDN) used for DNS lookups of your server (for example, www.mydomain.com). Browsers use this information to identify your Web site. Some browsers will refuse to establish a secure connection with your site if the server name does not match the common name in the certificate. Please do not include the protocol specifier "http://" or any port numbers or pathnames in the common name. Do not use wildcard characters such as * or ?, and do not use an IP address.
- **Organization Name:** The name of the organization to which the entity belongs (such as the name of a company).
- **State/Province Name:** This is the name of the state or province where your organization's head office is located. Please enter the full name of the state or province.
- **Country/Region Name:** This is the two-letter ISO abbreviation for your country (for example, GB for the United Kingdom).

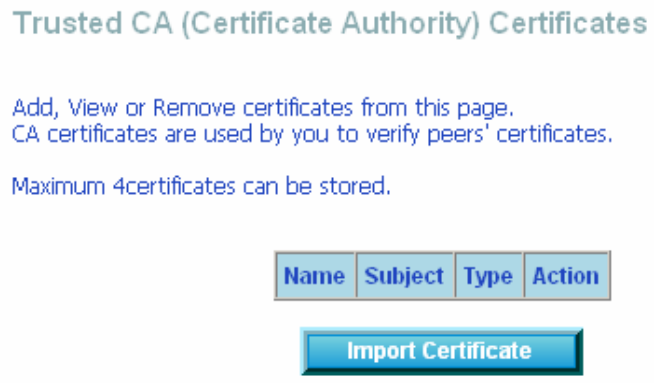
Import Certificate

To import existing certificate, click **Import Certificate** and paste both certificate and corresponding private key.

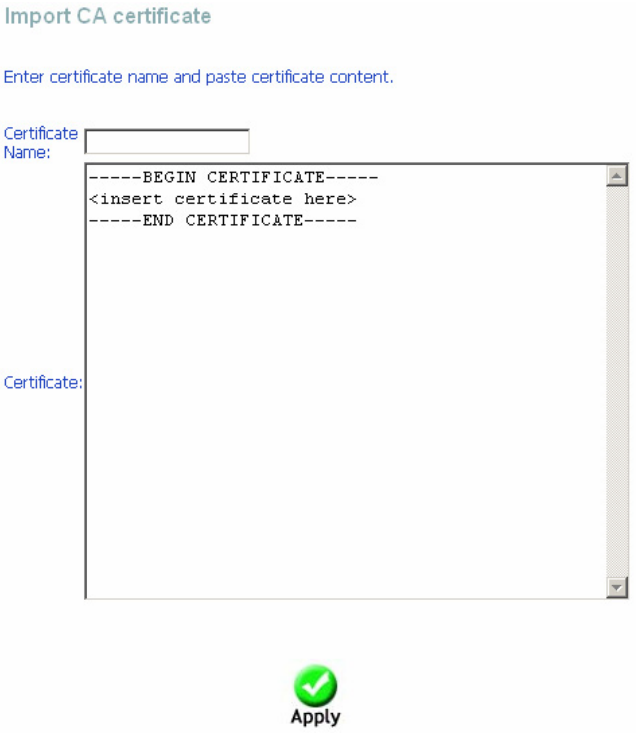


Trusted CA

Click **Trusted CA** and the right page appears. CA certificates are used by you to verify certificates of peers. It can store maximum 4 certificates.

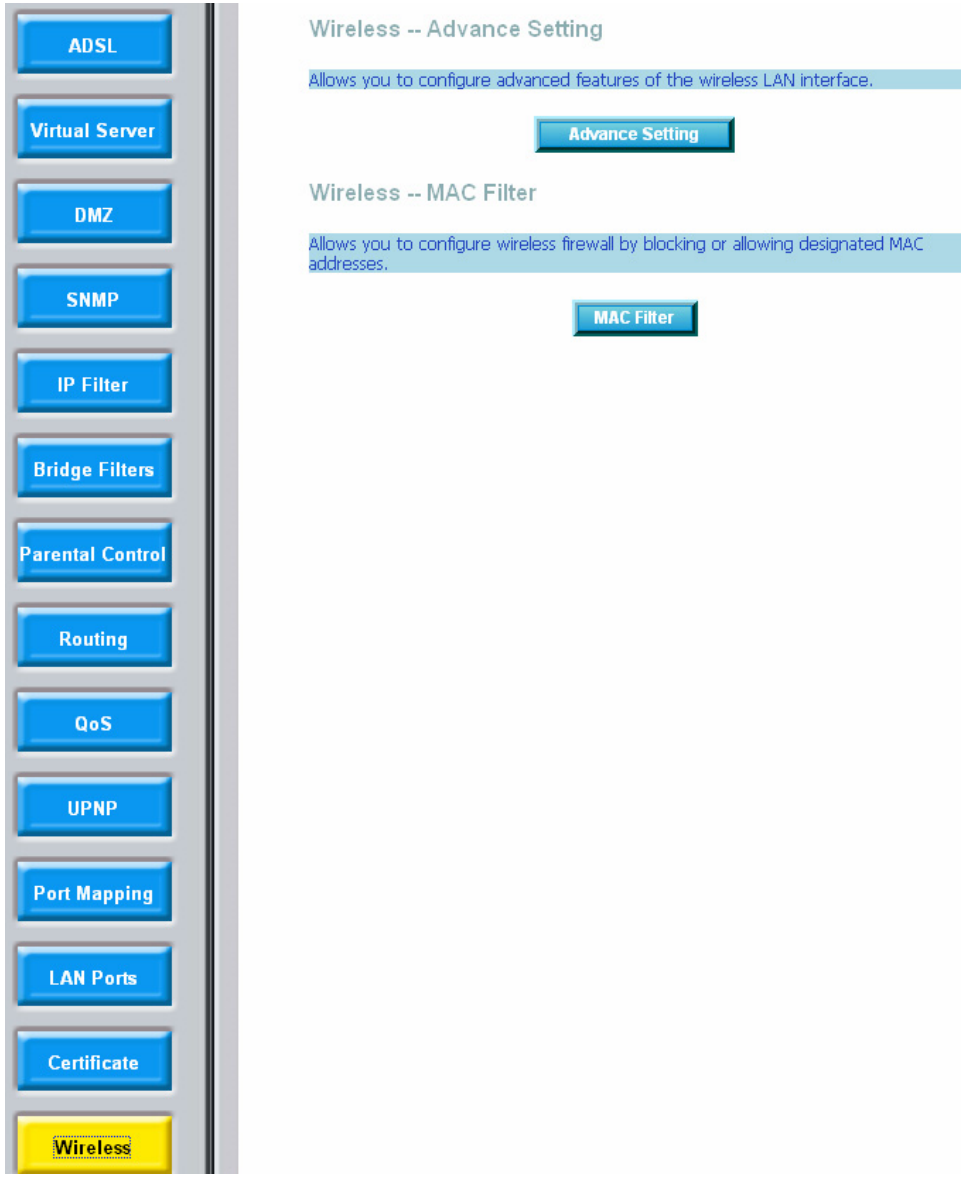


Click **Import Certificate** and the following page appears. Then you can enter certificate name, paste certificate content.



Wireless Configuration

Click **Wireless**, the right page appears.
In this page, you can select to configure **Advanced Setting** or **MAC Filter**.

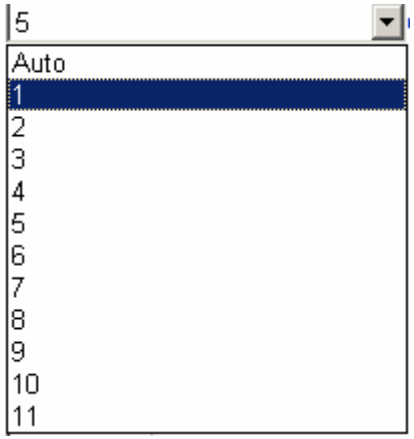


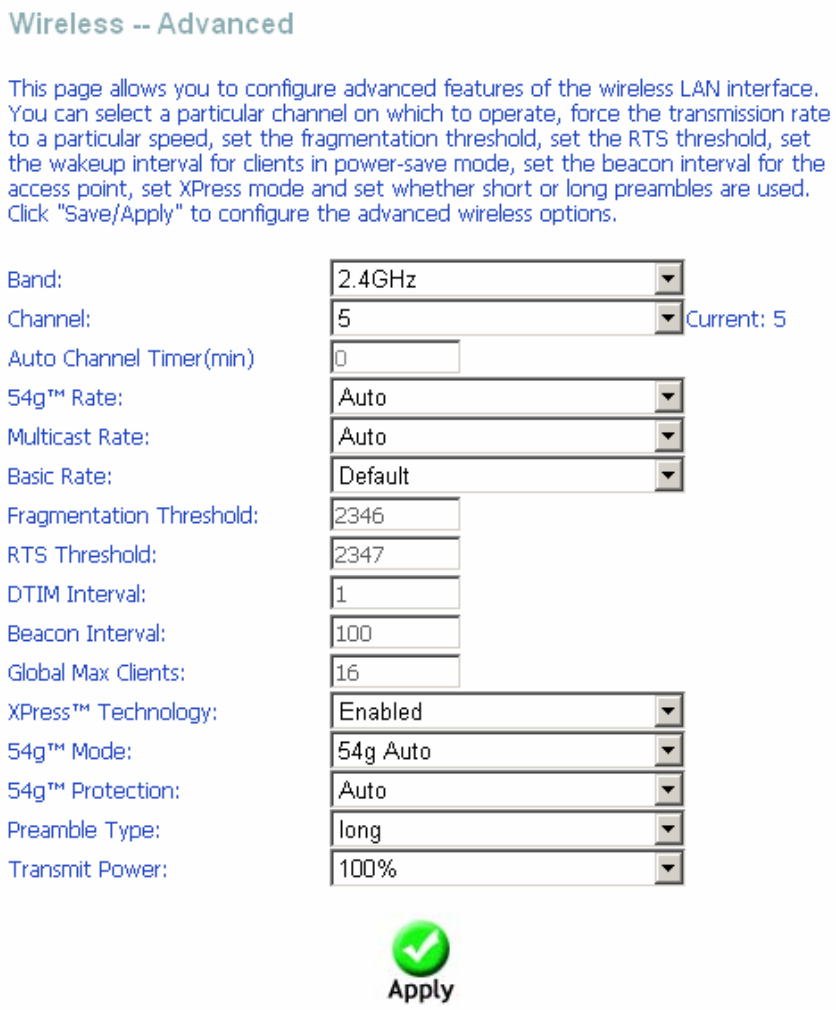
Wireless - Advanced Setting

Click **Advance Setting**, the right page appears.

This page allows you to configure advanced features of the wireless LAN interface. You can select a particular channel on which to operate, force the transmission rate to a particular speed, set the fragmentation threshold, set the RTS threshold, set the wakeup interval for clients in power-save mode, set the beacon interval for the access point, set XPress mode and set whether short or long preambles are used.

You can select the channel from the drop-down list.





- **Band:** Select 802.11b/g using wireless frequency band range. The radio frequency remains at 2.4 GHz.
- **Channel:** Fill in the appropriate channel to correspond with your network settings. 5 is the default channel. All devices in your wireless network must use the same channel in order to work correctly. This router supports auto channeling functionality.
- **Auto Channel Timer(min):** Specifies the timer of auto channelling.

- **54g™ Rate:** Select the transmission rate for the network. The rate of data transmission should be set depending on the speed of your wireless network. You can select from a range of transmission speeds, or you can select **Auto** to have the Router automatically use the fastest possible data rate and enable the Auto-Fallback feature. Auto-Fallback will negotiate the best possible connection speed between the Router and a wireless client. The default value is **Auto**.
- **Multicast Rate:** Select the multicast transmission rate for the network. The rate of data transmission should be set depending on the speed of your wireless network. You can select from a range of transmission speeds, or you can select **Auto** to have the Router automatically use the fastest possible data rate and enable the Auto-Fallback feature. Auto-Fallback will negotiate the best possible connection speed between the Router and a wireless client. The default value is **Auto**.
- **Basic Rate:** Select the basic transmission rate ability for the AP.
- **Fragmentation Threshold:** Packets that are larger than this threshold are fragmented into multiple packets. Try to increase the fragmentation threshold if you encounter high packet error rates. Do not set the threshold too low, since this can result in reduced networking performance.
- **RTS Threshold:** This value should remain at its default setting of 2347.Should you encounter inconsistent data flow, only minor reductions are recommended. Should you encounter inconsistent data flow, only minor reduction of the default value, 2347, is recommended. If a network packet is smaller than the preset RTS threshold size, the RTS/CTS mechanism will not be enabled. The Router sends Request to Send (RTS) frames to a particular receiving station and negotiates the sending of a data frame. After receiving an RTS, the wireless station responds with a Clear to Send (CTS) frame to acknowledge the right to begin transmission. The RTS Threshold value should remain at its default value of 2347.
- **DTIM Interval:** (Delivery Traffic Indication Message) Enter a value between 1 and 255 for the Delivery Traffic Indication Message (DTIM.) A DTIM is a countdown informing clients of the next window for listening to broadcast and multicast messages.
- **Beacon Interval:** Beacon is a packet of information that is sent from a connected device to all other devices where it announces its availability and readiness. A beacon interval is a period of time (sent with the beacon) before sending the beacon again. The beacon interval may be adjusted in milliseconds (ms). Default (100) is recommended.
- **Global Max Clients:** Default value is 16.
- **XPress™ Technology:** Select Enable or Disable. This is a special accelerating technology for IEEE802.11g. The defaule is Disabled.
- **54g™ Mode:** Compatible with IEEE 802.11b, IEEE 802.11g. Select a Standards from the drop-down list box. Its default setting is 54g Auto. The drop-down list box includes below mode.
- **54g™ Protection**: The 802.11g standards provide a protection method so 802.11g and 802.11b devices can co-exist in the same network without “speaking” at the same time. Do not disable 54g Protection if there is a possibility that a 802.11b device may need to use your wireless network. In Auto Mode, the wireless device will use RTS/CTS to improve 802.11g performance in mixed 802.11g/802.11b networks. Turn protection off to maximize 802.11g throughput under most conditions.
- **Preamble Type**: Preambles are a sequence of binary bits that help the receivers synchronize and ready for receipt of a data transmission. Some older wireless systems like 802.11b implementation use shorter preambles. If you are having difficulty connecting to an older 802.11b device, try using a short preamble. You can select short preamble only if the 54g mode is set to 802.11b.
- **Transmit Power:** Adjust the transmission range here. This tool can be helpful for security purposes if you wish to limit the transmission range.

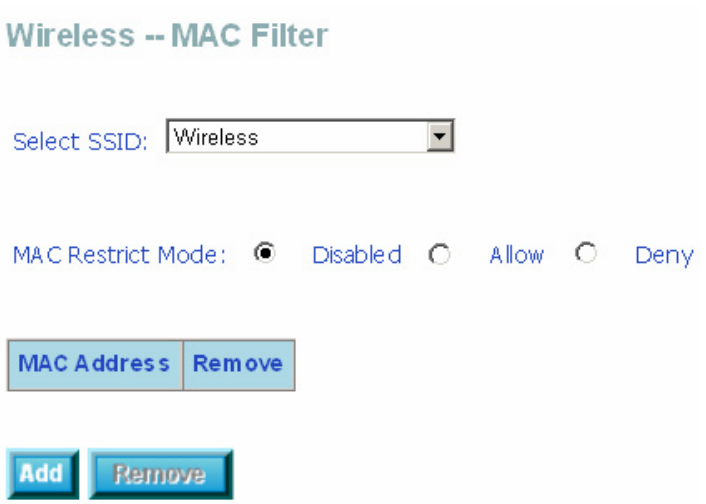
Click **Apply** to make the changes take effect.

MAC Filter

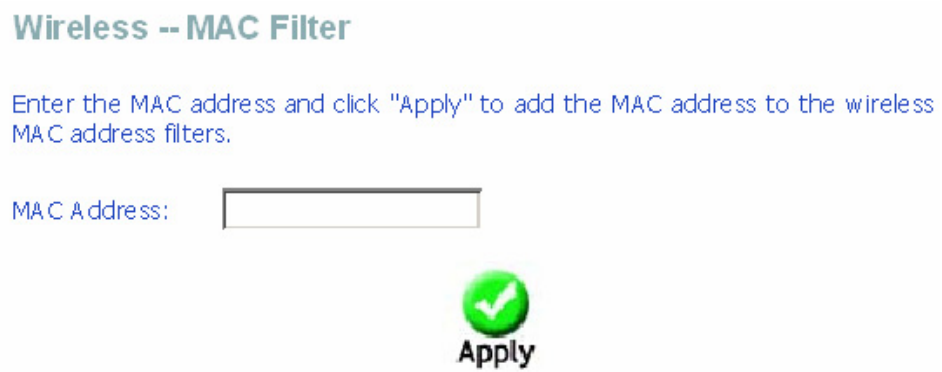
The page allows you to create a list of MAC addresses that are banned or allowed association with the wireless access point.

MAC Restrict Mode: The function can be turn on/off, Check **Disabled** to disable this function. Vice versa, to enable the function. After enabling the function, you can filter wireless users according to their MAC address, either allowing or denying access. Check **Allow** to make any wireless MAC address in the Wireless Access Control List can be linked to. And Check **Deny** to banned any wireless MAC address in the Wireless Access Control List to be linked to.

- **Add a MAC Access Control:** To add a new MAC address to your wireless MAC address filters, click **Add** to show next page. Type in the MAC Address in the entry field provided. Click **Save/Apply** to add the MAC address to the list. The MAC address appears listed in the table below.
- **Remove a MAC Access Control:** Select the **Remove** checkbox in the right column of the list for the MAC address to be removed and click **Remove**.



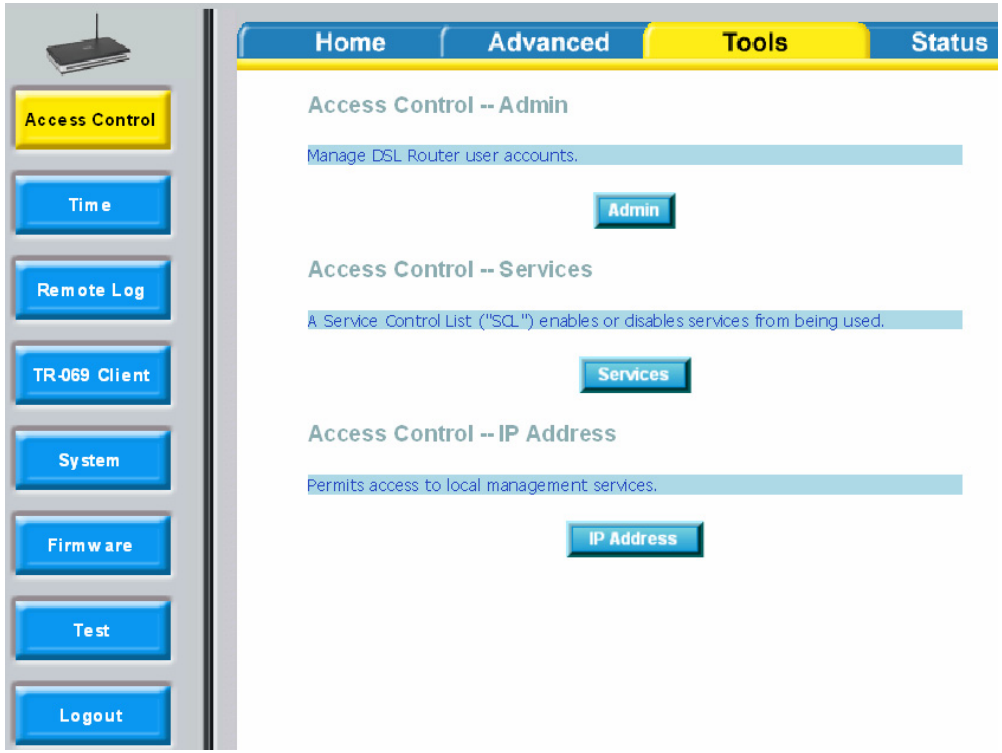
Choose **Allow** and click **Add**, the right page appears.



Tools Configuration

Access Control

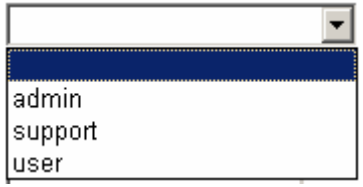
Choose **Tools** > **Access Control** and the right page appears.

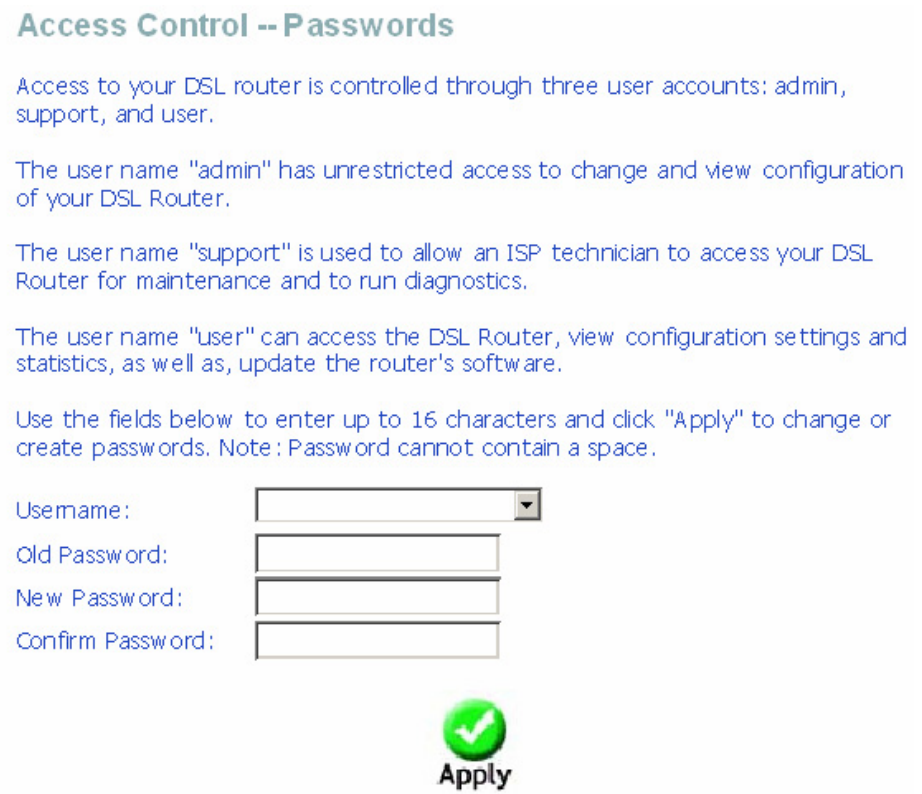


Access Control – Passwords

Click **Admin** and the right page appears. In this page, you can modify the accounts passwords.

You can select the Username from the drop-down list.

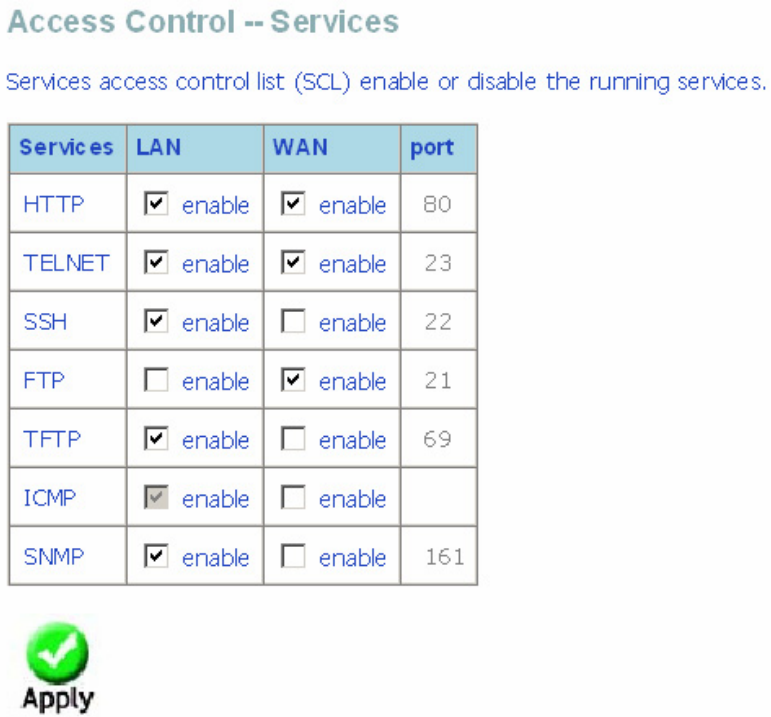




Access Control – Services

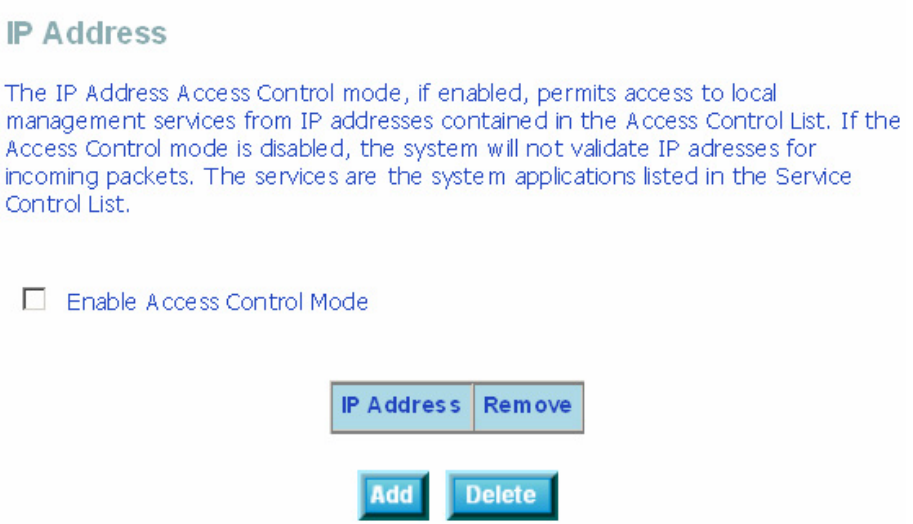
Click **Services** and the right page appears. In this page, you can enable or disable the services. And the LAN side and WAN side can have different configurations.

***Note**: If the connection is PPPoE PVC, you can view the information of WAN side.*

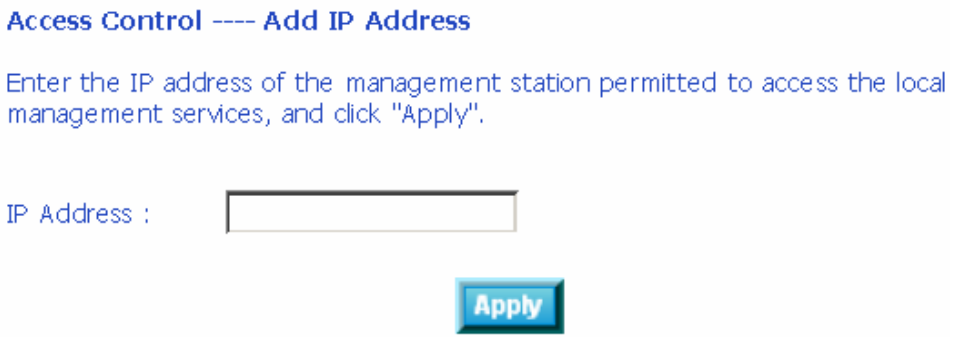


Access Control -- IP Addresses

Click **IP Address** and the right page appears.
If enabled, permits access to local management services from IP addresses contained in the Access Control List.
If the Access Control mode is disabled, the system does not validate IP addresses for incoming packets. The services are the system applications listed in the Service Control List.

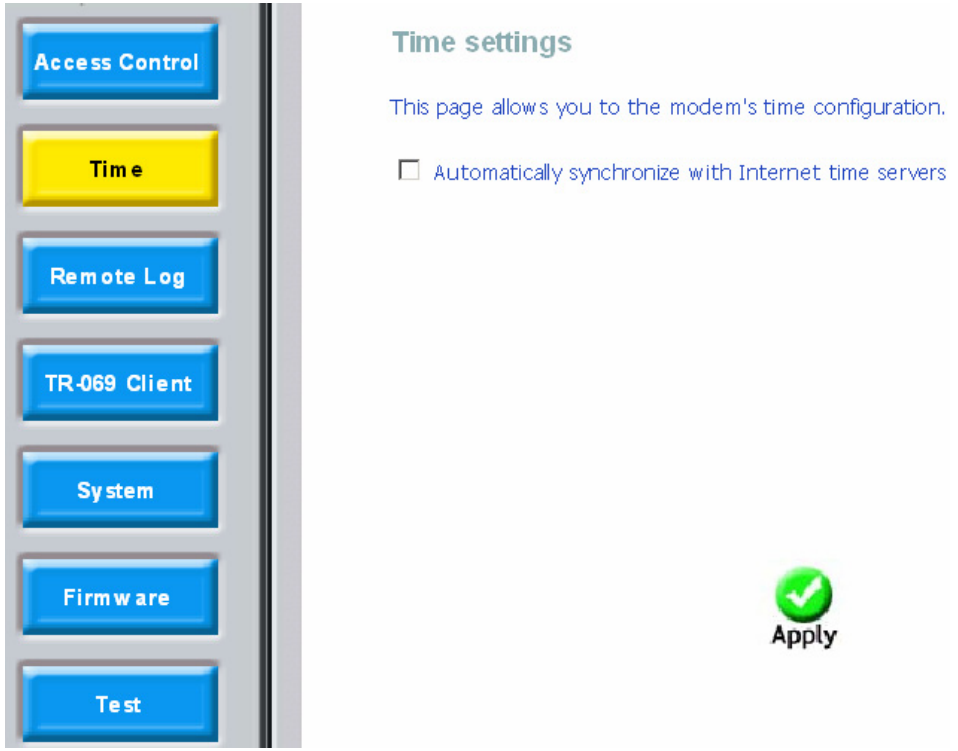


Click **Add** to show the following interface. In the interface input the IP address of the management station permitted to access the local management services, and click **Apply**.

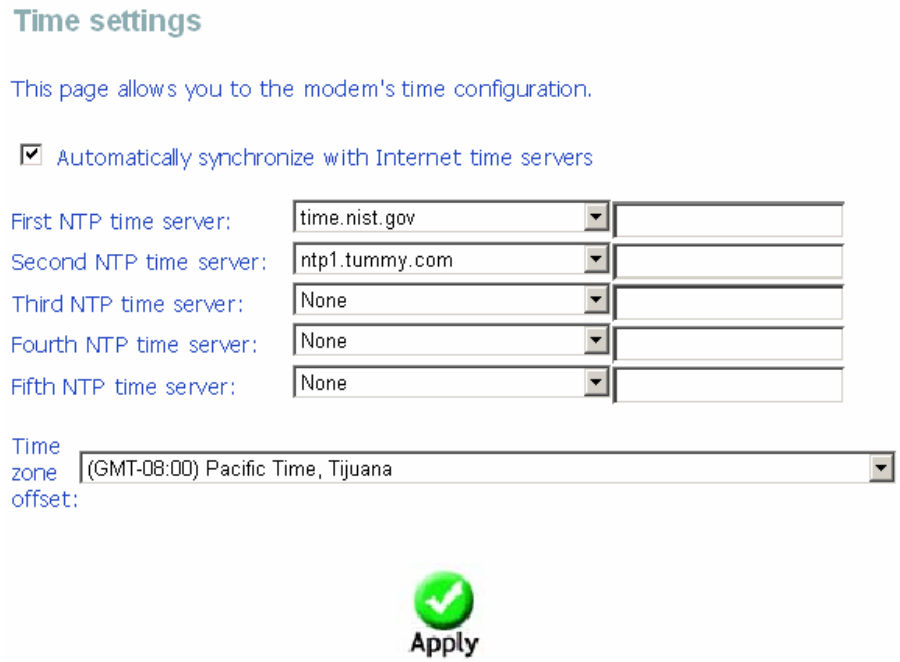


Internet Time

Click **Time** and the right page appears. In this page, the modem can synchronize with Internet time servers.

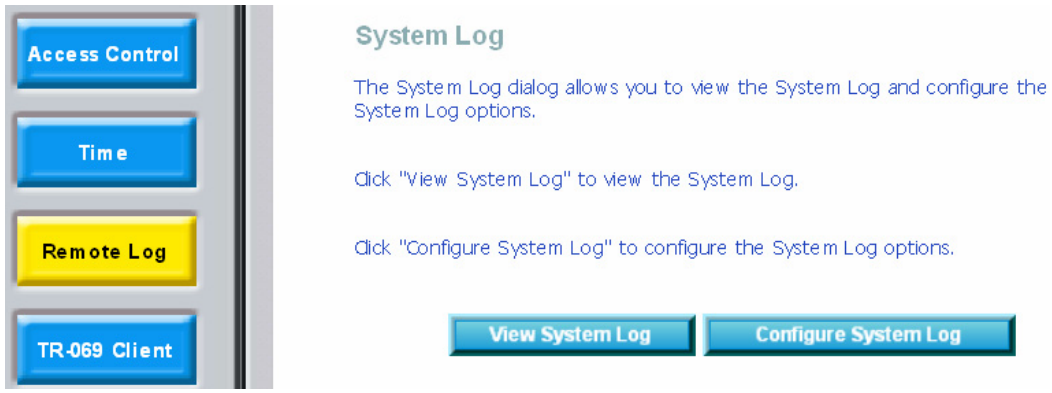


After enable **Automatically synchronize with Internet time servers**, the right page appears. Enter proper configurations and click **Apply**.



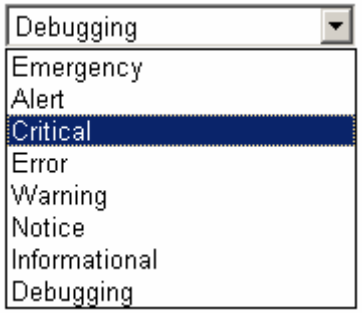
System Log

Click **Remote Log** and the right page appears. The system log dialog allows you to view the system log and configure the system log options.

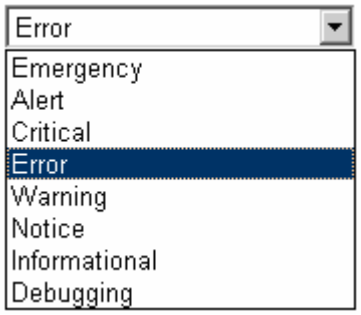


Click **Configure System Log** to show the following interface. You can enable or disable the system log and then select the log level, display level and mode, and click **Apply** to end your configurations.

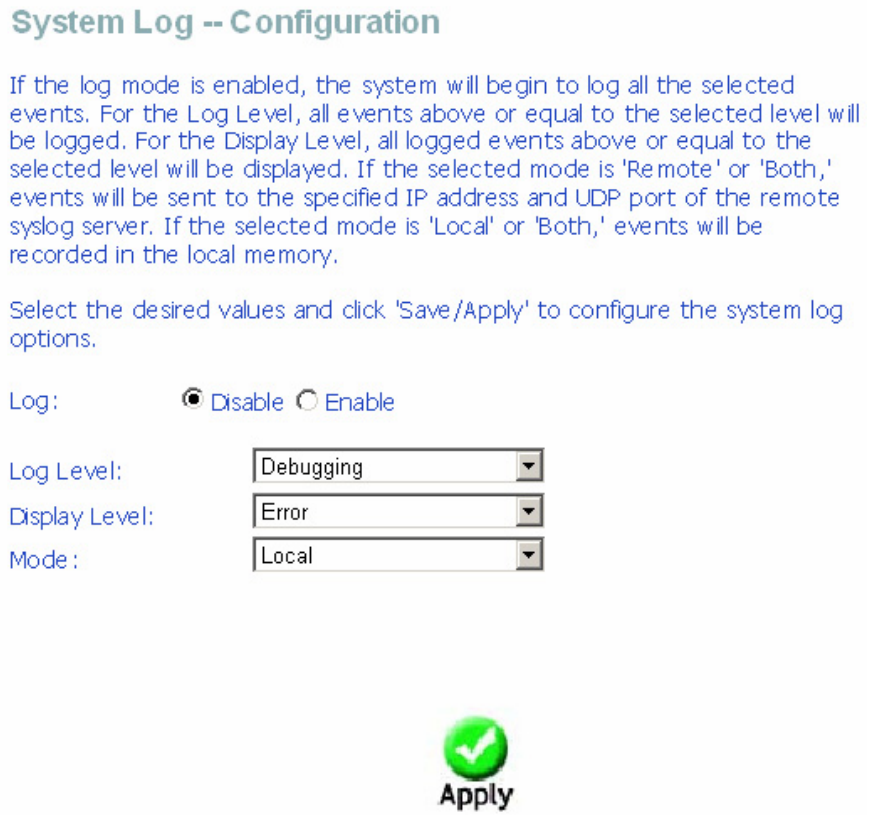
You can select **Log Level** from the drop-down list.



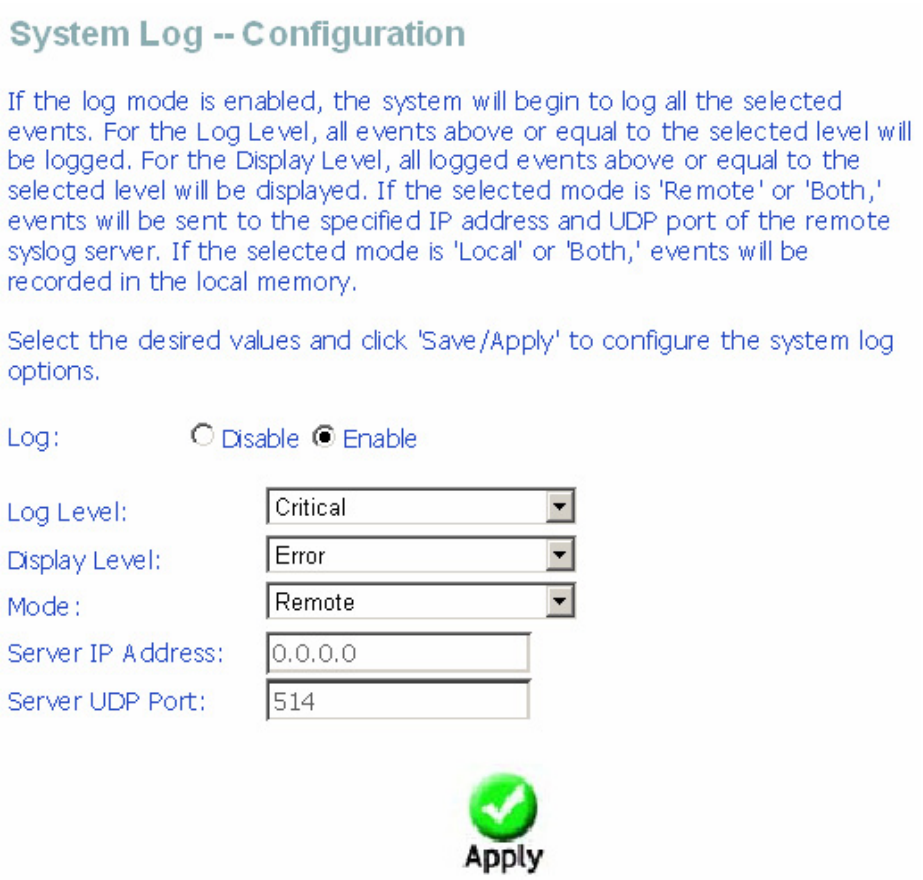
You can select **Display Level** from the drop-down list.



You can select **Mode** from the drop-down list.



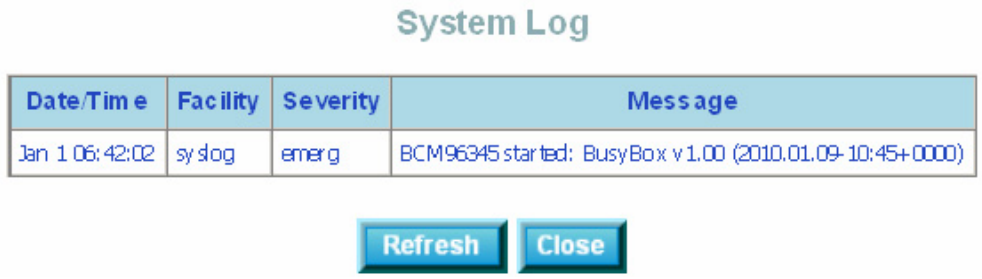
If you select **Remote** or **Both**, all events are transmitted to the specified UDP port of the specified log server.



After operations under **Configure System Log**, click **View System Log** to query the system logs. In this example, the **View System Log** is the default.

***Note**: The log and display of the system events are above the set level. If you intend to record all information, you need to set the levels as Debugging.*

Click **Refresh** to refresh the system event logs or click **Close** to exit from this page.

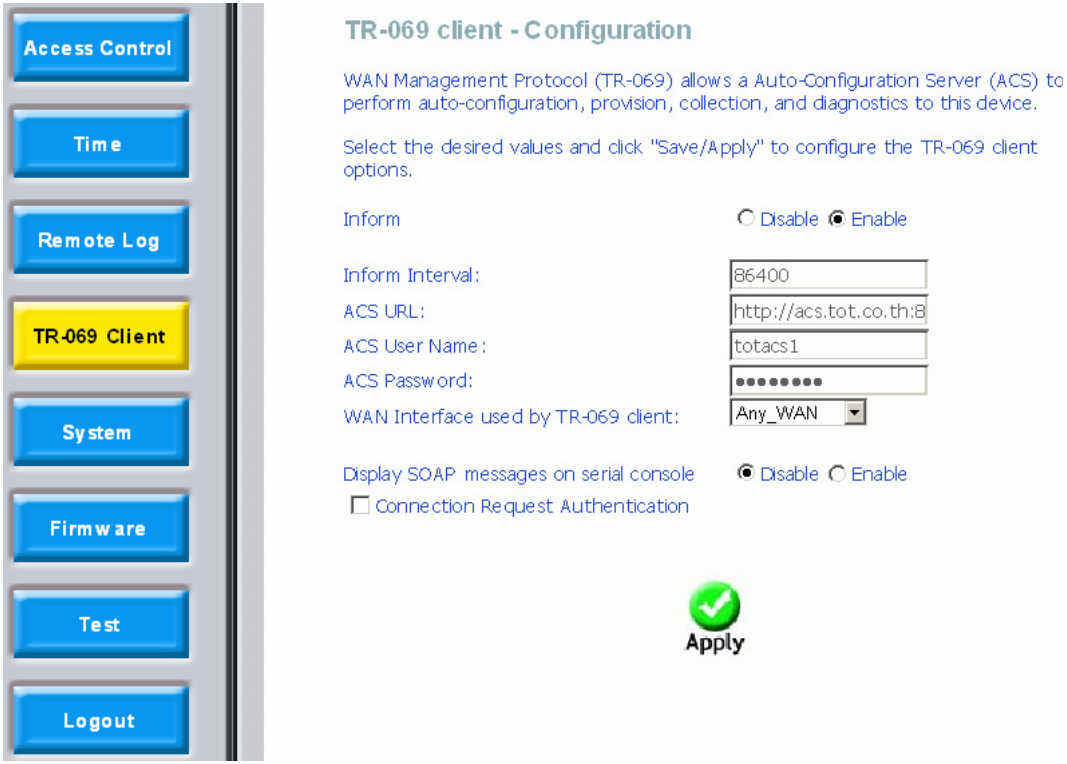


TR-069 Client

Click **TR-069 Client** and the right page appears.

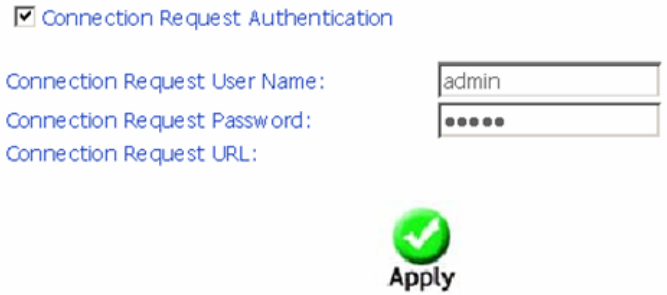
- **Inform:** If the **Enable** option is selected,the CPE accepts the commands from ACS, the CPE does not accept the commands from ACS when the **Disable** option is selected.
- **Inform Interval:** How many seconds does the CPE inform the ACS to connect.
- **ACS URL:** Enter the ACS URL.
- **ACS User Name:** The ACS user name is that the TR-069 Service provide to you.
- **ACS Password:** The ACS password is that the TR-069 Service provide to you.
- **Display SOAP messages on serial console:** When select **Enable** option, the SOAP information displays on the serial console, when select **Disable**, it does not.

Click **Apply** to save the he configuration.



- **Connection Request Authentication:** If this checkbox is selected, you need to enter the Connection Request User Name and the Connection Request Password. Or you needn't to enter.
- **Connection Request User Name:** the connection user name that the TR-069 Service provides to you.
- **Connection Request Password:** the Connection Request Password that the TR-069 Service provides to you.

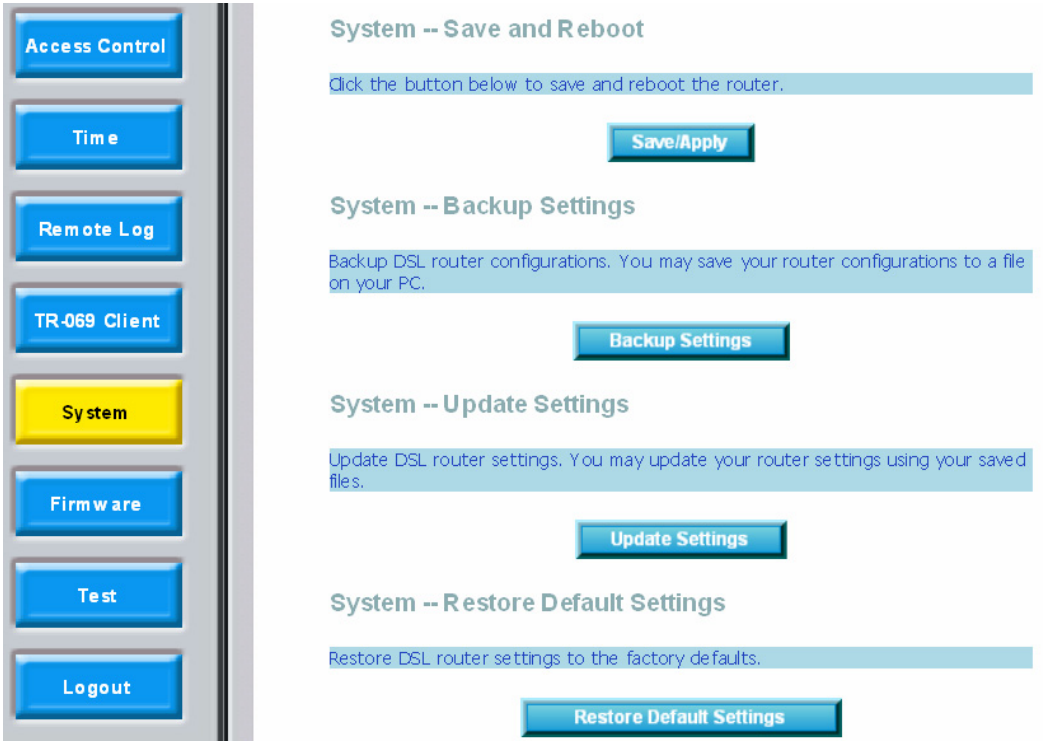
Click **Apply** to save the he configuration.



System Settings

Click System and the right page appears.
In this page, you can operate the following configuration.

- Save and reboot
- Backup settings
- Update settings
- Restore default settings

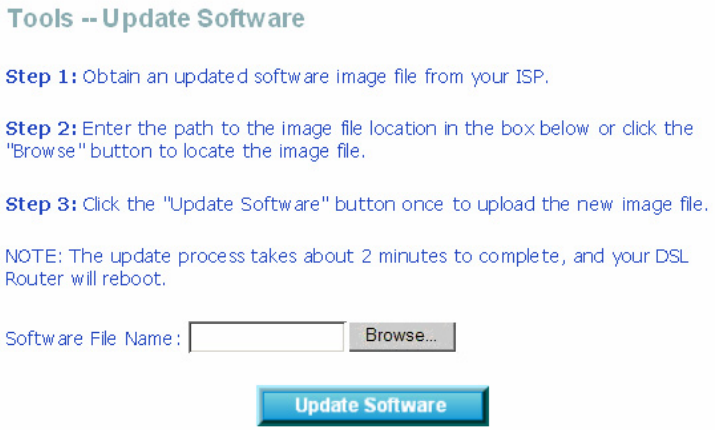


Update Firmware

Click **Firmware** and the right page appears. In this page, you can update the router firmware. Click **Browse** to find the right version file and click **Update Software** to update.

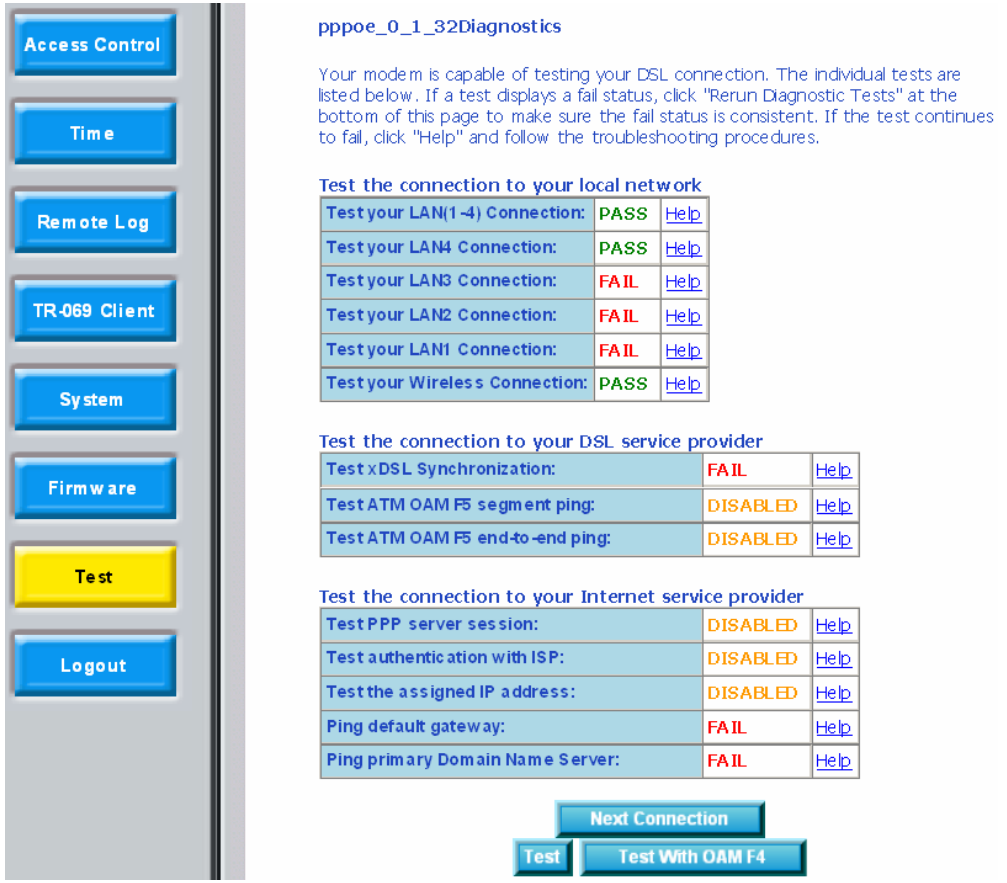
***Note**: Do not turn off your modem during firmware updates. When the update is finished, the modem reboots automatically. Do not turn off your modem either before the reboot is over. You must guarantee the update software is right and accurate. It is strictly forbidden to use other software for updates.*

After update software, it is suggested to restore the router to the factory defaults and configure it again.



Test

Your router is capable of testing your DSL connection. The individual tests are listed right. If a test displays a fail status, click **Tests** at the bottom of this page to make sure the fail status is consistent. If the test continues to fail, click **Help** and follow the troubleshooting procedures.

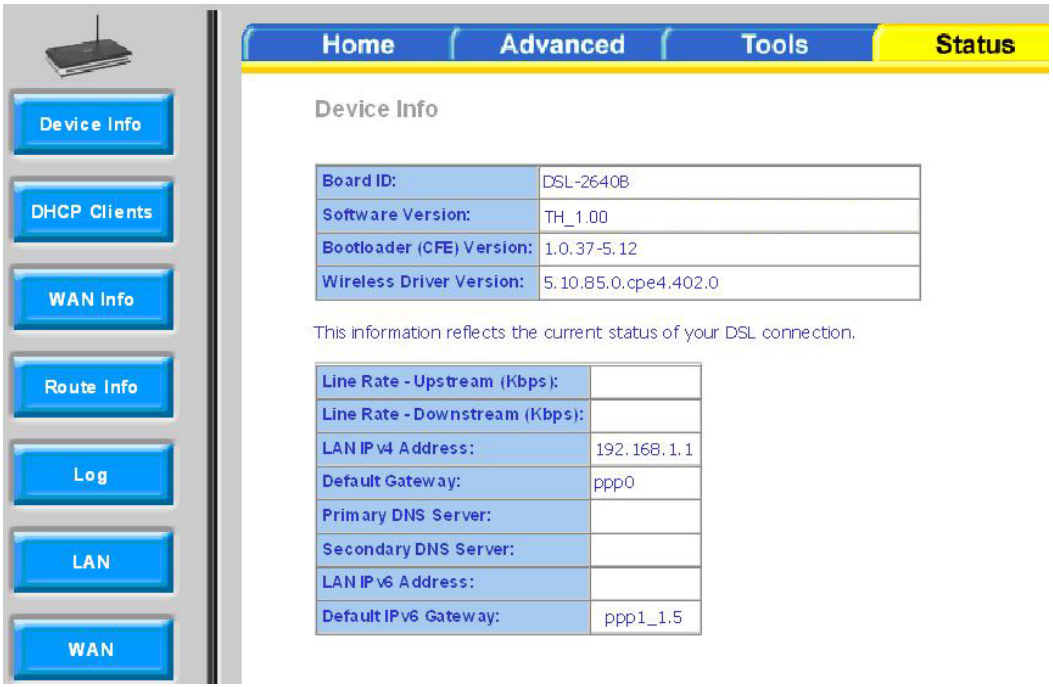


Status

Summary Information of the Router

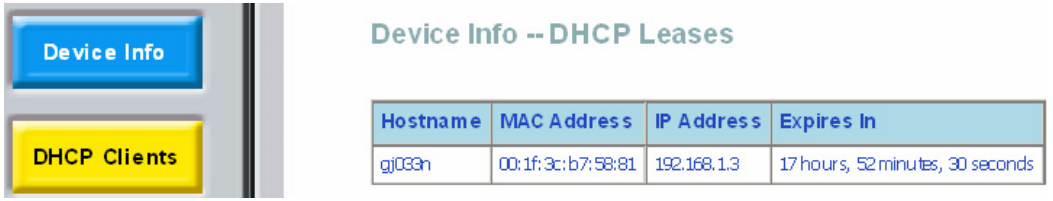
Choose **Status** > **Device Info**, the right page appears.

- **LAN IPv4 Address:** The management IPv4 address.
- **Default Gateway:** In the bridging mode there is no gateway. In other modes, it is the address of the uplink equipment, for example, PPPoE/PPPoA.
- **DNS Server:** In the PPPoE/PPPoA mode, it is obtained from the uplink equipment. In the bridging mode, there is no DNS Server address and you can manually enter the information.
- **LAN IPv6 Address:** The management IPv6 address.
- **Default IPv6 Gateway:** No gateway in a pure bridging mode; under other modes such as PPPoE/PPPoA, it is the address of the uplink equipment (support IPv6).



DHCP Client

Click **DHCP Clients** and the right page appears. You can query the IP address assignment for MAC address at the LAN side of the DSL router and obtain the IP Address from the DHCP server through Ethernet and wireless in the DSL router.



WAN Interface Information

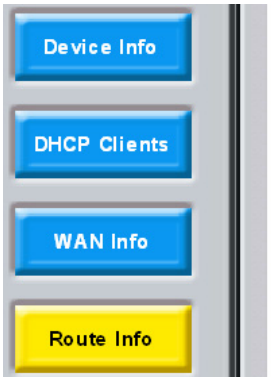
The **WAN Info** page displays the status and the connect or disconnect button, depending on the selected connection mode.

WAN Info

Interface	Description	Type	IPv6	MLD	Igmp	NAT	Firewall	Status	IPv4 Address
ppp0	pppoe_0_1_32	PPPoE	Disabled	Disabled	Disabled	Enabled	Disabled	Connecting	
ppp1_1.5	pppoe_0_0_35_1.5	PPPoE	Enabled	Disabled	Disabled	Disabled	Disabled	Connecting	

Route Table Information

Click **Route Info**, and if the system is in the default configuration, the right page appears.



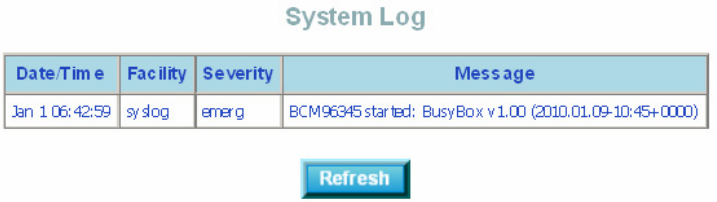
Device Info -- Route

Flags: U - up, ! - reject, G - gateway, H - host, R - reinstate
D - dynamic (redirect), M - modified (redirect).

Destination	Gateway	Subnet Mask	Flag	Metric	Service	Interface
192.168.1.0	0.0.0.0	255.255.255.0	U	0		br0

System Log

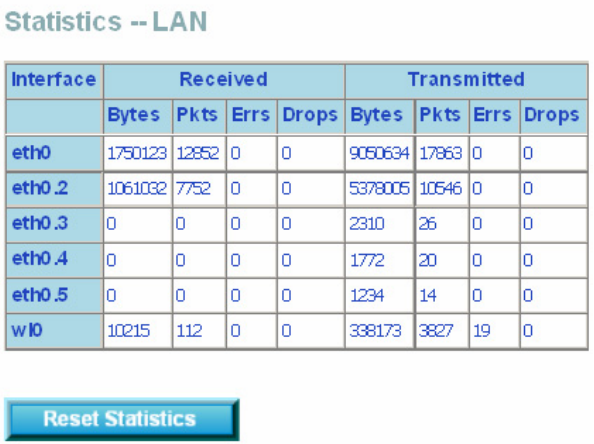
Click **Log**, the right page appears. In this page, you can view the information of system log.



Statistics of LAN

Click **LAN** and the right page appears. You can query information of packets recevied at the Ethernet, and wireless interfaces. Click **Reset Statistics** to restore the values to zero and recount them.

The LAN side interface includes Ethernet and wireless device.

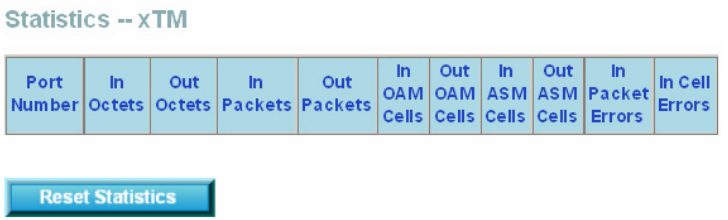


Statistics of WAN

Click **WAN** and the right page appears. You can query information of packets recevied by the WAN interfaces. Click **Reset Statistics** to restore the values to zero and recount them.

Statistics of ATM

Click **ATM** and the right page appears. In this page, you can query information of packets recevied by the ATM interfaces. Click **Reset Statistics** to restore the values to zero and recount them.



Statistics of ADSL

Click **ADSL** and right page appears.

Click **Reset Statistics** at the bottom to restore the values to zero and recount them.

Statistics -- xDSL

Mode:		
Type:		
Line Coding:		
Status:		Disabled
Link Power State:		L3
	Downstream	Upstream
SNR Margin (0.1 dB):		
Attenuation (0.1 dB):		
Output Power (0.1 dBm):		
Attainable Rate (Kbps):		
Rate (Kbps):		
Super Frames		
Super Frame Errors:		
RS Words:		
RS Correctable Errors::		
RS Uncorrectable Errors:		
HEC Errors:		
OCD Errors:		
LCD Errors:		
Total Cells:		
Data Cells:		
Bit Errors:		
Total ES:		
Total SES:		
Total UAS:		

xDSL BER Test Reset Statistics

Wireless Station Information

This page shows authenticated wireless stations and their status about Association and authentication.

Troubleshooting

This chapter provides solutions to problems that might occur during the installation and operation of the DSL-2640B. Read the following descriptions if you are having problems. (The examples below are illustrated in Windows® XP. If you have a different operating system, the screenshots on your computer will look similar to the following examples.)

1. How do I configure my DSL-2640B Router without the CD-ROM?

- Connect your PC to the Router using an Ethernet cable.
- Open a web browser and enter the address **http://192.168.1.1** .
- The default username is 'admin' and the default password is '**tot**'.
- If you have changed the password and cannot remember it, you will need to reset the Router to the factory default setting (see question 2), which will set the password back to 'tot'.

Note: Please refer to next section **Network Basics** to check your PC's IP configuration if you can't see the login window.

2. How do I reset my Router to the factory default settings?

- Ensure the Router is powered on.
- Press and hold the reset button on the back of the device for about one second.
- This process would take about 1~2 minutes to complete.

Note: Resetting the Router to the factory default settings will erase the current configuration settings. To reconfigure your settings, log in to the Router as outlined in question 1.

3. What can I do if my Router is not working correctly?

There are a few quick steps you can take to try and resolve any issues:

- Follow the directions in question 2 to reset the Router.
- Check that all the cables are firmly connected at both ends.
- Check the LEDs on the front of the Router. The Power indicator should be on, and the DSL and LAN indicators should be on as well.
- Please ensure that the settings in the Web-based configuration manager, e.g. ISP username and password etc., are the same as the settings provided by your ISP.

4. Why can't I get an Internet connection?

For ADSL subscribers, please contact your ISP to make sure the ADSL service has been enabled, and your ISP username and password are correct.

Networking Basics

Check Your IP Address

After you install your new D-Link adapter, by default, the TCP/IP settings should be set to obtain an IP address from a DHCP server (i.e. wireless router) automatically. To verify your IP address, please follow the steps below.

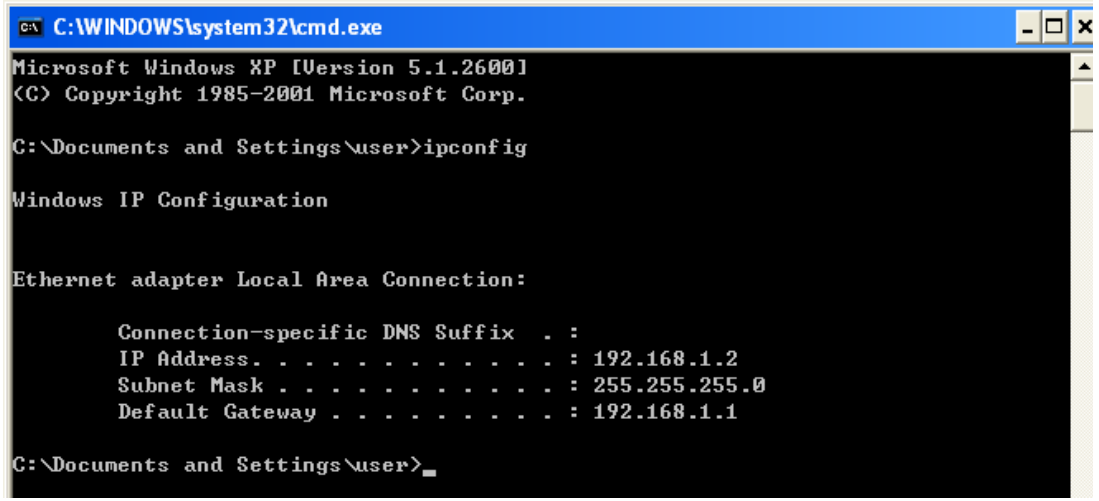
Click **Start** > **Run**. In the run box type "***cmd***" and click **OK**.

At the prompt, type "***ipconfig***" and press **Enter**.

This will display the IP address, subnet mask, and the default gateway of your adapter.

If the address is 0.0.0.0, check your adapter installation, security settings, and the settings on your router. Some firewall software programs may block a DHCP request on newly installed adapters.

If you are connecting to a wireless network at a hotspot (e.g. hotel, coffee shop, airport), please contact an employee or administrator to verify their wireless network settings.



Statically Assign An IP Address

If you are not using a DHCP capable gateway/router, or you need to assign a static IP address, please follow the steps below:

Step 1
Windows® XP - Click **Start** > **Control Panel** > **Network Connections**.
Windows® 2000 - From the desktop, right-click **My Network Places** > **Properties**.

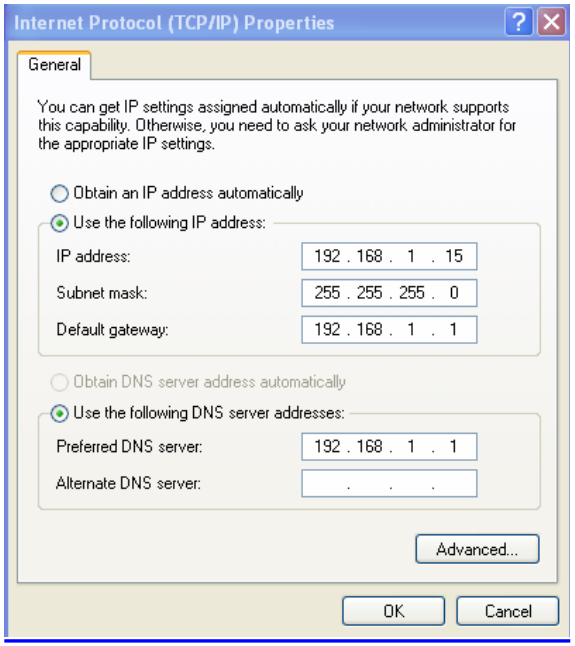
Step 2
Right-click the **Local Area Connection** that represents your D-Link network adapter and select **Properties**.

Step 3
Highlight **Internet Protocol (TCP/IP)** and click **Properties**.

Step 4
Click on the **Use the following IP address** and enter an IP address that is on the same subnet as your network or the LAN IP address on your router.
Example: If the router's LAN IP address is **192.168.1.1**, make your IP address 192.168.1.X where X is a number between 2 and 254. Make sure that the number you choose is not in use on the network. Set Default Gateway the same as the LAN IP address of your router (192.168.1.1).

Set Primary DNS the same as the LAN IP address of your router (192.168.1.1). The Secondary DNS is not needed or you may enter a DNS server from your ISP.

Step 5
Click on the **OK** twice to save your settings.



Technical Specifications

ADSL Standards

- Full-rate ANSI T1.413 Issue 2
- ITU G.992.1 (G.dmt)
- ITU G.992.2 (G.lite)
- ITU G.994.1 (G.hs)

ADSL2 Standards

- ITU G.992.3 (G.dmt.bis)

ADSL2+ Standards

- ITU G.992.5 (G.dmt.bisplus)

Protocols

- IEEE 802.1d Spanning Tree
- TCP/UDP
- ARP
- RARP
- ICMP
- RFC1058 RIP v1
- RFC1213 SNMP v1 & v2c
- RFC1334 PAP
- RFC1389 RIP v2
- RFC1577 Classical IP over ATM
- RFC1483/2684 Multiprotocol Encapsulation over ATM Adaptation Layer 5 (AAL5)
- RFC1661 Point to Point Protocol
- RFC1994 CHAP
- RFC2131 DHCP Client / DHCP Server
- RFC2364 PPP over ATM
- RFC2516 PPP over Ethernet

DC Power

- Input: 100V-240V, 0.6A, 50 Hz -60 Hz
- Output: 12V, 1A

Data Transfer Rate

- G.dmt full rate downstream: up to 8 Mbps / upstream: up to 1 Mbps
- G.lite: ADSL downstream up to 1.5 Mbps / upstream up to 512 Kbps
- G.dmt.bis full rate downstream: up to 12 Mbps / upstream: up to 1 Mbps
- ADSL2+ full rate downstream: up to 24 Mbps / upstream: up to 1 Mbps

Wireless Transfer Rates

- IEEE 802.11b: 11, 5.5, 2, and 1Mbps
- IEEE 802.11g: 6, 9, 12, 18, 24, 36, 48, 54 Mbps

Media Interface

- ADSL interface: RJ-11 connector for connection to 24/26 AWG twisted pair telephone line
- LAN interface: four RJ-45 ports for 10/100BASE-T Ethernet connection

Default Settings

IP Settings: **IP Address**: 192.168.1.1, **Netmask**: 255.255.255.0, **User Name:** admin, **Password:** tot
DHCP Server: Enabled