

FCC Information

This equipment complies with CFR 47, Part 15.19 of the FCC rules. Operation of the equipment is subject to the following 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.

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

NOTE: THE MANUFACTURER IS NOT RESPONSIBLE FOR ANY RADIO OR TV INTERFERENCE CAUSED BY UNAUTHORIZED MODIFICATIONS TO THIS EQUIPMENT. SUCH MODIFICATIONS COULD VOID THE USER'S AUTHORITY TO OPERATE THE EQUIPMENT.

Federal Communications Commission (FCC) Requirements, Part 15

This equipment has been tested and found to comply with the limits for a class B digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation.

This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

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

Regulatory information / Disclaimers

Installation and use of this Wireless LAN device must be in strict accordance with the instructions included in the user documentation provided with the product. Any changes or modifications (including the antennas) made to this device that are not expressly approved by the manufacturer may void the user's authority to operate the equipment. The manufacturer is not responsible for any radio or television interference caused by unauthorized modification of this device, or the substitution of the connecting cables and equipment other than manufacturer specified. It is the responsibility of the user to correct any interference caused by such unauthorized modification, substitution or attachment. Manufacturer and its authorized resellers or distributors will assume no liability for any damage or violation of government

CAUTION: To maintain compliance with FCC's RF exposure guidelines, this equipment should be installed and operated with minimum distance 20cm between the radiator and your body. Use on the supplied antenna. Unauthorized antenna, modification, or attachments could damage the transmitter and may violate FCC regulations.

MPE Statement (Safety Information)

Your device contains a low power transmitter. When device is transmitted it sends out Radio Frequency (RF) signal.

Safety Information

In order to maintain compliance with the FCC RF exposure guidelines, this equipment should be installed and operated with minimum distance 20cm between the radiator and your body. Use only with supplied antenna. Unauthorized antenna, modification, or attachments could damage the transmitter and may violate FCC regulations.

Table of Contents

<i>Before You Begin</i>	1	<i>Port Mapping</i>	47
Package Contents	1	IPSec	47
System Requirements	1	Certificate	47
Features	2	Wireless	47
HARDWARE OVERVIEW	3	Wireless LAN Basics	47
Connections	3	Wireless – Basic	47
LED Indicators	4	Wireless – Security	47
INSTALLATION	5	Wireless - MAC Filter	47
Installation Notes	5	Wireless – Bridge	47
<i>Information you will need from your ADSL service provider</i>	7	Wireless – Advanced	47
<i>Information you will need about DSL-2640B</i>	8	Wireless -- Authenticated Stations	47
<i>Information you will need about your LAN or computer:</i>	8	Diagnostics	47
Device Installation	9	Management	47
<i>Power on Router</i>	9	Settings	47
<i>Factory Reset Button</i>	9	System Log	47
<i>Network Connections</i>	10	TR-069 Client	47
INTRODUCTION TO WEB CONFIGURATION	11	Internet Time	47
Preparation Before Login	11	Access Control	47
Logging In to the Modem	12	Update Software	47
<i>First-Time Login</i>	12	Save/Reboot	47
Quick Setup	13	TROUBLESHOOTING	47
<i>WAN Interface Setup</i>	13	NETWORKING BASICS	47
<i>LAN Interface Setup</i>	22	Check Your IP Address	47
<i>Wireless Interface Setup</i>	23	Statically Assign An IP Address	47
<i>WAN Setup Summary</i>	23	TECHNICAL SPECIFICATIONS	47
<i>Quick Setup Completion</i>	24		
DSL Router Device Information	24		
<i>Summary of Device Information</i>	25		
<i>WAN Interface Information</i>	25		
<i>Statistics of LAN</i>	26		
<i>Statistics of WAN</i>	26		
<i>Statistics of ATM</i>	26		
<i>Statistics of ADSL</i>	27		
<i>Route Table Information</i>	28		
<i>ARP Table Information</i>	29		
Advanced Setup	29		
<i>WAN Configuration</i>	29		
<i>LAN Configuration</i>	31		
NAT	31		
Security	36		
Parental Control	40		
Quality of Service	41		
Routing	47		
DNS	47		
DSL	47		

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.

- = 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.

Package Contents



System Requirements

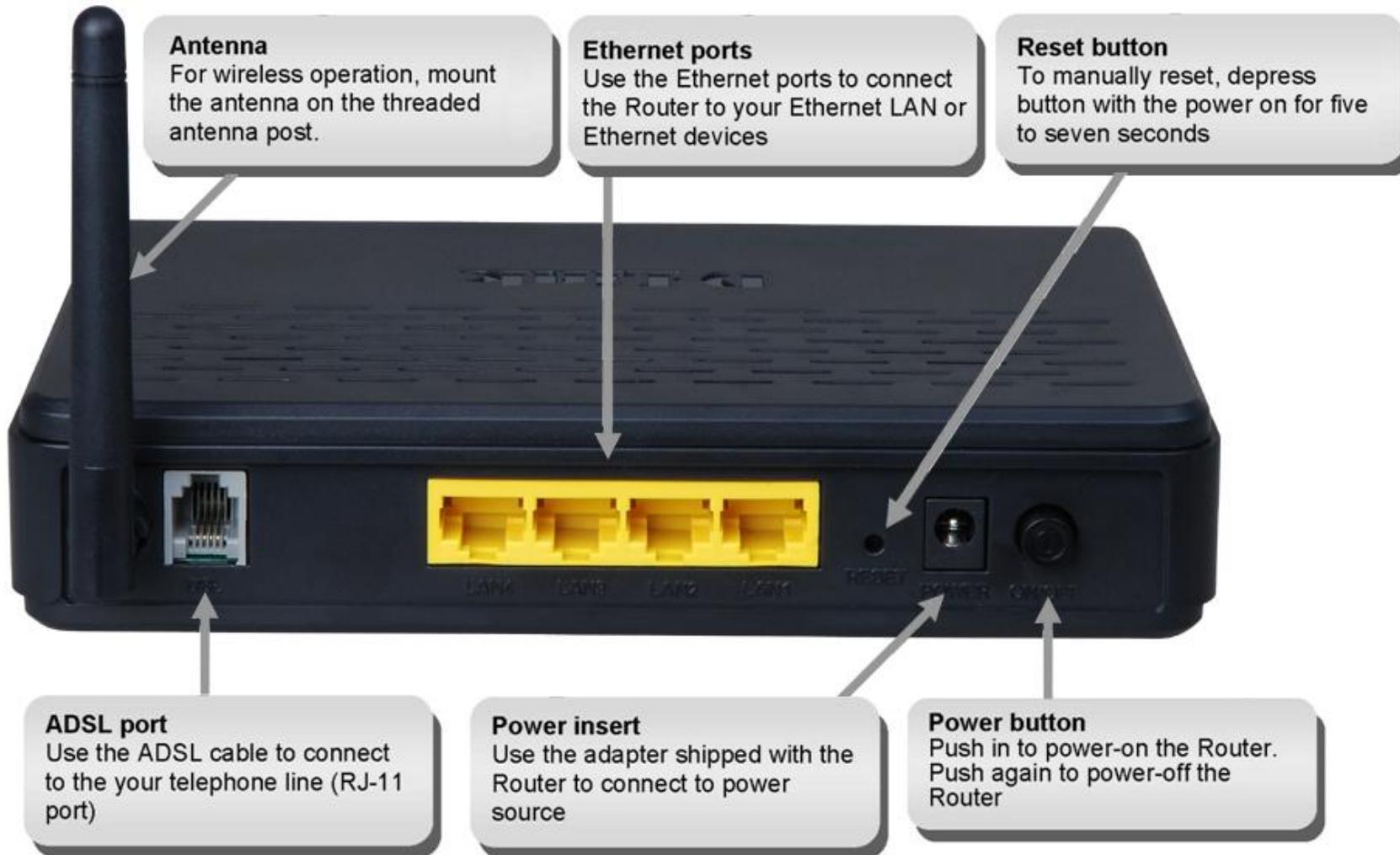
- ADSL Internet service
- Computer with:
 - 200 MHz Processor
 - 64MB Memory
 - CD-ROM Drive
 - Ethernet Adapter with TCP/IP Protocol Installed
 - Internet Explorer v6 or later, FireFox v1.5
 - Computer with Windows 2000, Windows XP, or Windows Vista

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.
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.

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

Installation

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 "**admin**." 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 10.1.1.1. 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 255.0.0.0. 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 10.1.1.5 to 10.1.1.254. 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 **10.1.1.1** and the subnet mask is **255.0.0.0**, the default management Username is “admin” and the default Password is “admin.”

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

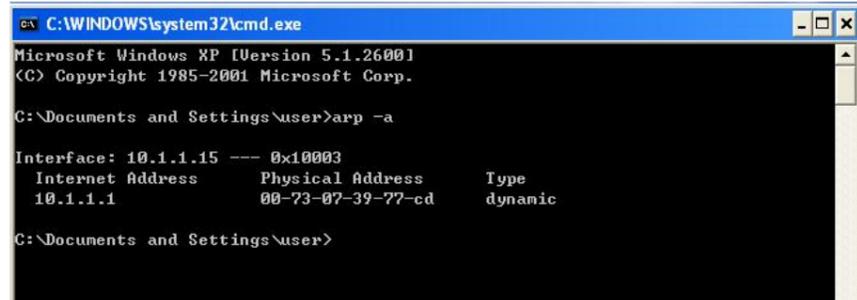
The first time you setup the Router. It is recommended that you configure the WAN connection using a single computer, to ensure that both the computer and the Router are not connected to the LAN. Once the WAN connection operates properly, you may continue to make changes to Router configuration, including 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 10.1.1.X (2~254), net mask as 255.0.0.0, gateway address as 10.1.1.1 (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 (10.1.1.1 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.

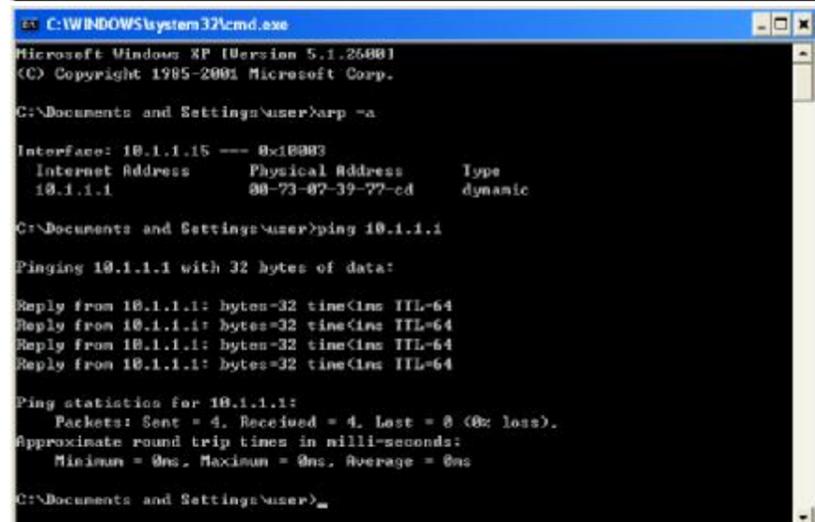


```
C:\WINDOWS\system32\cmd.exe
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\user>arp -a

Interface: 10.1.1.15 --- 0x10003
Internet Address      Physical Address      Type
10.1.1.1              00-73-07-39-77-cd    dynamic

C:\Documents and Settings\user>
```



```
C:\WINDOWS\system32\cmd.exe
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\user>arp -a

Interface: 10.1.1.15 --- 0x10003
Internet Address      Physical Address      Type
10.1.1.1              00-73-07-39-77-cd    dynamic

C:\Documents and Settings\user>ping 10.1.1.1

Pinging 10.1.1.1 with 32 bytes of data:

Reply from 10.1.1.1: bytes=32 time<ms TTL=64

Ping statistics for 10.1.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\Documents and Settings\user>
```

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://10.1.1.1> (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 of the super user are **admin** and **admin**. The username and password of the common user are **user** and **user**. 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.

Quick Setup

The **Quick Setup** page mainly includes the following three functions:

- = WAN interface setup
- = LAN interface setup
- = Wireless interface setup

Quick setup enables fast and accurate configuration of your Internet connection and other important parameters. The following sections describe these various configuration parameters. Whether you configure these parameters or use the default ones, click Next to enable your Internet connection.

When subscribing to a broadband service, you should be aware of the method by which you are connected to the Internet. Your physical WAN device can be Ethernet, DSL, or both. Technical information regarding the properties of your Internet connection should be provided by your Internet service provider (ISP). For example, your ISP should inform you whether you are connected to the Internet by using a static or dynamic IP address, or the protocols, such as PPPOA or PPPoE, which you use to communicate over the Internet.

WAN Interface Setup

During WAN interface setup, you can set up a PVC and its properties:

- = VPI
- = VCI
- = QoS
- = Internet connection type
- = Encapsulation type
- = IGMP service
- = NAT

Setting Up VPI/VCI and QoS

After logging in to the DSL router, if no PVC is configured previously and no default settings exist, the **Quick Setup** webpage appears, which contains some basic configuration that is needed by ATM PVC. The following introduction guides you through the necessary steps to configure your DSL Router.

Web Configuration

According to your ISP instructions, specify the following parameters:

- = VPI (Virtual Path Identifier)
Virtual path between two points in an ATM network. The valid value range is from 0 to 255.
- = VCI (Virtual Channel Identifier)
Virtual channel between two points in an ATM network. The valid value range is from 32 to 65535 (1 to 31 are reserved for known protocols).
- = Enable Quality Of Service
Enabling QoS for a PVC improves performance for selected classes of applications. However, since QoS also consumes system resources, the number of PVCs is reduced consequently. Use **Advanced Setup/Quality of Service** to assign priorities for the applications.

For example, PVC 0/35 is to be modified and the default values of QoS remain. In actual applications, you can modify them depending on your ISP instructions.

The screenshot shows the 'Quick Setup' page for a D-Link DSL Router. The left sidebar contains navigation links: Device Info, Quick Setup, Advanced Setup, Wireless, Diagnostics, and Management. The main content area is titled 'Quick Setup' and includes a sub-section 'ATM PVC Configuration'. It explains that VPI and VCI are needed for setting up the ATM PVC and provides input fields for VPI (set to 0) and VCI (set to 35). There is also a checkbox for 'Enable Quality Of Service' which is currently unchecked. A 'Next' button is located at the bottom right of the configuration area.

Selecting Internet Connection Type and Encapsulation Type

You can select your connection type from the following list. Each connect type corresponds to several encapsulation types:

- = PPP over ATM (PPPoA)
PPPoA Encapsulation Mode: VC/MUX, LLC/ENCAPSULATION
- = PPP over Ethernet (PPPoE)
PPPoE Encapsulation Mode: LLC/SNAP-BRIDGING, VC/MUX
- = MAC Encapsulation Routing (MER)
MER Encapsulation Mode: LLC/SNAP-BRIDGING, VC/MUX
- = IP over ATM (IPoA)
IPoA Encapsulation Mode: LLC/SNAP-ROUTING, VC/MUX
- = Bridging
Bridging Encapsulation Mode: LLC/SNAP-BRIDGING, VC/MUX

For example, change the connection type of PVC 0/35 to **Bridging**. Select **Bridging**, and set **Encapsulation Mode** to **LLC/SNAP-BRIDGING** (depending on the uplink equipment).

Connection Type

Select the type of network protocol for IP over Ethernet as WAN interface

- PPP over ATM (PPPoA)
- PPP over Ethernet (PPPoE)
- MAC Encapsulation Routing (MER)
- IP over ATM (IPoA)
- Bridging

Encapsulation Mode

LLC/SNAP-BRIDGING

Back Next

Internet Connection Type - PPP over ATM (PPPoA)

- Step 5** In the **PVC and its QoS configuration** page, configure a PVC and its QoS.
- Step 6** In the **Internet connection type and encapsulation type** page, set the **Connection Type** to **PPP over ATM (PPPoA)** and select the encapsulation mode.

Connection Type

Select the type of network protocol for IP over Ethernet as WAN interface

- PPP over ATM (PPPoA)
- PPP over Ethernet (PPPoE)
- MAC Encapsulation Routing (MER)
- IP over ATM (IPoA)
- Bridging

Encapsulation Mode

VC/MUX

Back Next

Web Configuration

Step 7 Click **Next** and the **PPP information configuration** page appears.

Your ISP should provide you with the following information:

- = PPP Username
- = PPP Password
- = Authentication Method

You can also select another service function as follows:

- = Dial on demand (with idle timeout timer)
- = PPP IP extension
- = Use static IP address
- = Retry PPP password on authentication error
- = Enable PPP debug mode

Step 8 Click **Next** and the **PPPoA IGMP and WAN function configuration** page appears.

To use IGMP service on pppoa pvc, select the **Enable IGMP Multicast** check box.

PPP Username and Password

PPP usually requires that you have a user name and password to establish your connection. In the boxes below, enter the user name and password that your ISP has provided to you.

PPP Username:
PPP Password:
Authentication Method:
MTU (1-1500):

- Enable Fullcone NAT
- Dial on demand (with idle timeout timer)
- PPP IP extension
- Use Static IP Address
- Retry PPP password on authentication error
- Enable PPP Debug Mode

Enable IGMP Multicast, and WAN Service

Enable IGMP Multicast
Enable WAN Service
Service Name

Internet Connection Type - PPP over Ethernet (PPPoE)

- Step 1** In the **PVC and its QoS configuration** page, configure a PVC and its QoS.
- Step 2** In the Internet connection type and encapsulation type page, set the **Connection Type** to **PPP over Ethernet (PPPoE)** and select the encapsulation mode.

Connection Type

Select the type of network protocol for IP over Ethernet as WAN interface

- PPP over ATM (PPPoA)
- PPP over Ethernet (PPPoE)
- MAC Encapsulation Routing (MER)
- IP over ATM (IPoA)
- Bridging

Encapsulation Mode

LLC/SNAP-BRIDGING ▾

Back Next

Web Configuration

Step 3 Click **Next** and the **PPP information configuration page** appears.

Your ISP should provide you with the following information:

- = PPP Username
- = PPP Password
- = Authentication Method

You can also select another service function as follows:

- = Dial on demand (with idle timeout timer)
- = PPP IP extension
- = Use Static IP Address
- = Retry PPP password on authentication error
- = Enable PPP Debug Mode

Step 4 Click **Next** and the **PPPoE IGMP and WAN function configuration page** appears.

To use IGMP service on pppoe pvc, select the **Enable IGMP Multicast** check box.

PPP Username and Password

PPP usually requires that you have a user name and password to establish your connection. In the boxes below, enter the user name and password that your ISP has provided to you.

PPP Username:
PPP Password:
PPPoE Service Name:
Authentication Method:
MTU (65535):

- Enable Firewall NAT
- Dial on demand (with idle timeout timer)
- PPP IP extension
- Use Static IP Address
- Retry PPP password on authentication error
- Enable PPP Debug Mode
- Enable PPPoE Frames between WAN and Local Ports (Default enabled)

Enable IGMP Multicast, and WAN Service

Enable IGMP Multicast
Enable WAN Service
Service Name

Web Configuration

- Step 4** Click **Next** and the **MER IGMP and WAN function configuration page** appears. To use IGMP service on MER pvc, select the **Enable IGMP Multicast** check box. In the MER mode, you can configure the following functions:
- = Enable NAT.
 - = Enable Fullcone NAT.
 - = Enable Firewall.

Enable NAT

Enable Fullcone NAT

Enable Firewall

Enable IGMP Multicast and WAN Service

WAN Service Mode: IPoA

Back Next

Internet Connection Type - IP over ATM (IPoA)

- Step 1** In the **PVC and its QoS configuration** page, configure a PVC and its QoS.
- Step 2** In the **Internet connection type and encapsulation type** page, set the **Connection Type** to **IP over ATM (IPoA)** and select the encapsulation mode.

Connection Type

Select the type of network protocol for IP over Ethernet as WAN interface

PPP over ATM (PPPoA)

PPP over Ethernet (PPPoE)

MAC Encapsulation Routing (MER)

IP over ATM (IPoA)

Bridging

Encapsulation Mode

LLC/SNAP-ROUTING

Back Next

- Step 3** Click **Next** and the **WAN IP configuration page** appears.
- You can select the service function as follows:
- = Use the following IP address (static wan ip)
 - = Use the following default gateway (static gateway ip)
 - = Use the following DNS server addresses (static DNS server ip)

- Step 4** Click **Next** and the **IPoA IGMP and WAN function configuration page** appears.
- To use IGMP service on ipoa pvc, select the **Enable IGMP Multicast** check box.
- In the MER mode, you can configure the following functions:
- = Enable NAT.
 - = Enable Fullcone NAT.
 - = Enable Firewall.

WAN IP Settings

Enter information provided to you by your ISP to configure the WAN IP settings.

Notice: DHCP is not supported in IPoA mode. Changing the default gateway or the DNS affects the whole system. Configuring them with static values will disable the automatic assignments from other WAN connection.

WAN IP Address:

WAN Subnet Mask:

Use the following default gateway:

Use IP Address:

Use WAN Interface:

Use the following DNS server addresses:

Primary DNS server:

Secondary DNS server:

Network Address Translation Settings

Network Address Translation (NAT) allows you to share one Wide Area Network (WAN) Local Area Network (LAN).

Enable NAT

Enable Fullcone NAT

Enable Firewall

Enable IGMP Multicast, and WAN Service

Enable IGMP Multicast

Enable WAN Service

Service Name:

Internet Connection Type – Bridging

- Step 1** In the **PVC and its QoS configuration** page, configure a PVC and its QoS.

Web Configuration

Step 2 In the **Internet connection type and encapsulation type** page, set the **Connection Type** to **Bridging** and select the encapsulation mode.

Connection Type

Select the type of network protocol and encapsulation mode over the ATM PVC that your ISP has instructed by 802.1q VLAN tagging is only available for PPPoE, NBR and Bridging.

PPP over ATM (PPPoA)

PPP over Ethernet (PPPoE)

MAC Encapsulation Routing (MER)

IP over ATM (IPoA)

Bridging

Encapsulation Mode

LLC/SNAP-BRIDGING

Back Next

Step 3 Click **Next** and the **Bridging service configuration** page appears.

Unselect the check box below to disable this WAN service

Enable Bridge Service:

Service Name:

Back Next

LAN Interface Setup

The **LAN interface setup** page is shown on the right.

Device Setup

Configure the DSL Router IP Address and Subnet Mask for your Local Area Network (LAN).

IP Address:

Subnet Mask:

Back Next

Wireless Interface Setup

Enable Wireless: Select or deselect the check box to enable or disable wireless connection.
SSID: It is the network name shared among all points in a wireless network. The SSID must be identical for all points in the wireless network. It is case-sensitive and must not exceed 32 characters (use any character on the keyboard).

Wireless -- Setup

Enable Wireless

Enter the wireless network name (also known as SSID).

SSID:

[Back](#)

[Next](#)

WAN Setup Summary

In WAN setup summary, you can view the following properties of the added PVC:

- = VPI/VCI
- = Connection Type:
- = Service Name:
- = Service Category:
- = IP Address:
- = Service State:
- = NAT
- = Firewall
- = IGMP
- = QoS

WAN Setup - Summary

Make sure that the settings below match the settings provided by your ISP.

PORT / VPI / VCI:	0 / 0 / 35
Connection Type:	Bridge
Service Name:	br_0_0_35
Service Category:	UHR
IP Address:	Not Applicable
Service State:	Enabled
NAT:	Enabled
Firewall:	Enabled
IGMP Multicast:	Not Applicable
Quality Of Service:	Enabled

Click "Save/Reboot" to save these settings and reboot router. Click "Back" to make any modifications.

NOTE: The configuration process takes about 1 minute to complete and your DSL Router will reboot.

[Back](#)

[Save/Reboot](#)

Web Configuration

To make any modifications, click **Back**. Click **Save/Reboot**, and the following page appears.

Note: You need to reboot to activate this WAN page and further configure services in this interface, and it takes about two minutes to reboot.

DSL Router Reboot

The DSL Router has been configured and is rebooting.

Close the DSL Router Configuration window and wait for 2 minutes before reopening your web browser. If necessary, reconfigure your PC's IP address to match your new configuration.

Quick Setup Completion

After the previous setup, you can immediately start using your gateway to:

- = Share a broadband connection among multiple users (HTTP, FTP, Telnet, NetMeeting) and between all of the computers connected to your home network.
- = Build a home network by connecting additional PCs and network devices to the gateway.
- = Control network parameters, including DHCP, DNS, and WAN settings.
- = View network status, traffic statistics, system log, and more.
- = Allow access from the Internet to games and other services provided by computers in the home network.
- = Prohibit computers in the home network from accessing selected services on the Internet.
- = Block access to specific Internet websites from your home network.

If your gateway is equipped with multiple LAN ports, you can connect additional devices directly to the gateway. Otherwise, connect a hub or switch to the LAN port, to which you can connect additional devices. In both cases, configure newly connected devices to automatically obtain IP address as previously described.

DSL Router Device Information

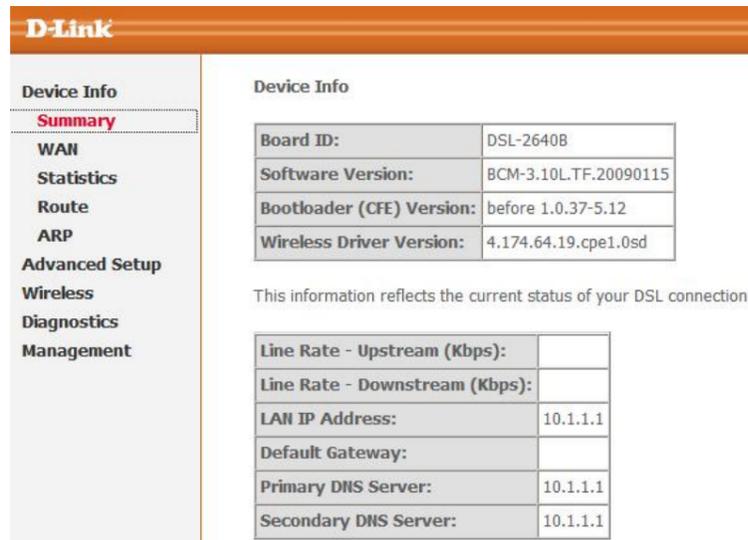
Click **Device Info** and you can view the following information.

- = Summary
- = WAN
- = Statistics
- = Route
- = ARP
- = DHCP

Summary of Device Information

Click **Summary** and the **Device Info** page appears.

- = **LAN IP Address:** the management IP 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.



D-Link

Device Info

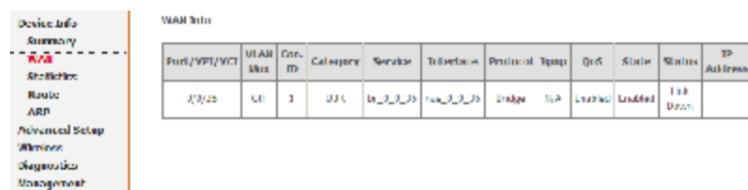
Board ID:	DSL-2640B
Software Version:	BCM-3.10L.TF.20090115
Bootloader (CFE) Version:	before 1.0.37-5.12
Wireless Driver Version:	4.174.64.19.cpe1.0sd

This information reflects the current status of your DSL connection.

Line Rate - Upstream (Kbps):	
Line Rate - Downstream (Kbps):	
LAN IP Address:	10.1.1.1
Default Gateway:	
Primary DNS Server:	10.1.1.1
Secondary DNS Server:	10.1.1.1

WAN Interface Information

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



Device Info

Summary

WAN

Statistics

Route

ARP

Advanced Setup

Wireless

Diagnostics

Management

WAN Info

Port/VPI/VCI	WAN Interface	Conn. ID	Category	Service	Trunking	Protocol	Temp.	QoS	Status	Status	IP Address
0/32	UI	1	JJL	DSL-2640B	DSL-2640B	Bridge	10	10240	Enabled	10	Down

Statistics of LAN

Choose **Statistics > LAN** and the following page appears. You can query information of packets received at the Ethernet and wireless interfaces. Click **Reset Statistics** to restore the values to zero and recount them.

Device Info

- Summary
- WAN
- Statistics
- LAN
- WAN
- ATM
- ADSL
- Route
- ARP

Statistics -- LAN

Interface	Received				Transmitted			
	Bytes	Pkts	Errs	Drops	Bytes	Pkts	Errs	Drops
Ethernet	287549	2349	0	0	780510	2077	0	0
Wireless	1368	4	0	0	104923	650	0	0

Statistics of WAN

Click **Statistics > WAN** and the following page appears. You can query information of packets received at the WAN interfaces. Click **Reset Statistics** to restore the values to zero and recount them.

Device Info

- Summary
- WAN
- Statistics
- LAN
- WAN
- ATM
- ADSL

Statistics -- WAN

Service	VPI/VCI	Protocol	Interface	Received				Transmitted					
				Bytes	Pkts	Errs	Drops	Bytes	Pkts	Errs	Drops		
br	0/35	0/0/35	Bridge	0	0	0	0	0	0	0	0	0	0

Statistics of ATM

Click **Statistics > ATM** and the following page appears. You can query information of packets received at the ATM interfaces. Click **Reset** to restore the values to zero and recount them.

Device Info

- Summary
- WAN
- Statistics
- LAN
- WAN
- ATM
- ADSL

ATM Interface Statistics

In Octets	Out Octets	In Errors	In Unknown	In Frame Errors	In Port VPI VCI Errors	In Port Inside Errors	In P11 Errors	In Idle Cells	In Cell Type Errors	In OAM RM CRC Errors	In GTC Errors
0	0	0	0	0	0	0	0	0	0	0	0

ATM5 Interface Statistics

In Octets	Out Octets	In Discard Pkts	Out Discard Pkts	In Errors	Out Errors	In Discards	Out Discards
0	0	0	0	0	0	0	0

ATM5 VCC Statistics

VPI/VCI	CRC Errors	SAR Timeouts	Overized SDUs	Short Packet Errors	Length Errors
0/35	0	0	0	0	0

Statistics of ADSL

Click **Statistics > ADSL**. If the DSL line is activated, the window shows on the left appears.
Click **Reset Statistics** at the bottom to restore the values to zero and recount them.

Device Info

- Summary
- WAN
- Statistics
- LAN
- WAN
- ATM
- ADSL**
- Route
- ARP
- Advanced Setup
- Wireless
- Diagnostics
- Management

Statistics -- ADSL

Mode:		
Line Coding:		
Status:	Link Down	
Link Power State:	LO	
	Downstream	Upstream
SNR Margin (dB):		
Attenuation (dB):		
Output Power (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:		

Web Configuration
ADSL BER Test

Click **ADSL BER Test** to perform a bit error rate (BER) test on the DSL line. The test page is as follows.

The **Tested Time (sec)** can be 1, 5, 10, 20, 60, 120, 180, 240, 300, or 360. Select a time and click **Start**. The following pages appear.

Note: If the BER reaches e-5, you cannot access the Internet.

ADSL BER Test - Start

The ADSL Bit Error Rate (BER) test determines the quality of the ADSL connection. The test is done by transferring idle calls containing a known pattern and comparing the received data with this known pattern to check for any errors.

Select the test duration below and click "Start".

Tested Time (sec):

ADSL BER Test - Result

The ADSL BER test completed successfully.

Test Time (sec):	20
Total Transferred Bits:	0x0000000000000000
Total Error Bits:	0x0000000000000000
Error Ratio:	Not Applicable

Route Table Information

Click **Route**, and if the system is in the default configuration, the following page appears. If the configuration of modem is as PPPoE/PPPoA dial-up, the page shows different.

Device Info

Summary

WAN

Statistics

Route

ARP

Advanced Setup

Wireless

Diagnostics

Management

Device Info -- Route

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

Destination	Gateway	Subnet Mask	Flag	Metric	Service	Interface
10.0.0.0	0.0.0.0	255.0.0.0	U	0		br0

ARP Table Information

Click **ARP** and the following page appears. You can query the MAC and IP address information of the equipment attached to the modem.

Device Info

Summary

WAN

Statistics

Route

ARP

Device Info -- ARP

IP address	Flags	HW Address	Device
10.1.1.15	Complete	00:1D:0F:19:91:C1	br0

Advanced Setup

This chapter include the more advanced features used for network management and security as well as administrative tools to manage the Router, view status and other information used to examine performance and for troubleshooting.

WAN Configuration

Choose **Advanced Setup > WAN**, and the following page appears, so you can modify and configure the WAN interface.

Note: After a PVC is deleted or modified, the system must be rebooted. Otherwise, the modification does not take effect.

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

Click **Save/Reboot** to save the modification, and reboot the modem to make the modification effective.

Device Info

Advanced Setup

WAN

LAN

Security

Quality of Service

Routing

VPN

DSL

Port Mapping

Trunk

Configuration

View Area Network (WAN) Setup

Click Add, Edit, or Remove to configure WAN interface.
Click Save/Reboot to apply the changes and reboot the system.

Port/Vlan/Vo	VLAN No.	Conn. ID	Category	Service	Interface	Protocol	Jump	QoS	Status	Remove	Edit
1/1/15	15	1	LAN	LAN	eth0/eth1	Static	NA	Priority	Enable	<input type="checkbox"/>	<input type="button" value="Edit"/>

Web Configuration

Click **Add**, and the following page appears. In this page, you can modify VPI/VCI, service categories, and QoS.

- = **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).
- = **Service Category**: UBR Without PCR/UBR With PCR/CBR/Non Realtime VBR/Realtime VBR.
- = **Enable Quality Of Service**: Enable or disable QoS.

After proper modifications, click **Next** and the following page appears. This window allows you to select the appropriate connection type. The choices include PPP over ATM (PPPoA), PPP over Ethernet (PPPoE), MAC Encapsulation Routing (MER), IP over ATM (IPoA), and Bridging (default).

This window also allows you to use the drop-down menu to select the desired Encapsulation Mode. Click the **Next** button to continue. For further information about each of the five connection types available on the Router, please go to the **Quick Setup** section earlier in this manual as all of the windows are identical.

ATM PVC Configuration
This screen allows you to configure an ATM PVC Identifier (PORT and VPI and VCI) and select a service category. Otherwise choose an existing Interface by selecting the checkbox to enable it.

VPI: [0-255]
VCI: [32-65535]

VMAN-Mux: Enable Multiple Protocols Over a Single PVC

Service Category: **UBR without PCR**

Enable Quality of Service

Enabling packet level QoS for a PVC improves performance for selected classes of applications. QoS cannot be set for CBR and Realtime VBR. QoS consumes system resources; therefore the number of PVCs will be reduced. Use **Advanced Setup/Quality of Service** to assign priorities for the applications.

Enable Quality of Service

Connection Type

Click the type of network protocol that you want to use over the ATM PVC. If you do not know the type available for PPPoE, MER and Bridging.

- PPP over ATM (PPPoA)
- PPP over Ethernet (PPPoE)
- MAC Encapsulation Routing (MER)
- IP over ATM (IPoA)
- Bridging

Encapsulation Mode

LLC/EXAF-ORIGGING

LAN Configuration

In this interface, you can modify and configure IP Address and DHCP Server.

If the mode is router, the interface shows as follows. In the Bridging mode, the interface shows different.

NAT

Note: You need to enable the NAT service when you configure the WAN connection at first, the **NAT** item appears in the **Advanced Setup** directory. In the pure bridging mode, there is not the NAT service.

Overview

Setting up the NAT Function

- = The DSL router is equipped with the network address translation (NAT) function. With address mapping, several users in the local network can access the Internet via one or more public IP addresses. All the local IP addresses are assigned to the public IP address of the router by default.
- = One of the characteristics of NAT is that data from the Internet is not allowed into the local network unless it is explicitly requested by one of the PCs in the network. Most Internet applications can run behind the NAT firewall without any problems. For example, if you request Internet pages or send and receive e-mails, the request for data from the Internet comes from a PC in the local network, and so the router allows the data to pass through. The router opens one specific port for the

Web Configuration

application. A port in this context is an internal PC address, via which the data is exchanged between the Internet and a client on a PC in the local network. Communicating via a port is subject to the rules of a particular protocol (TCP or UDP).

- = If an external application tries to send a call to a PC in the local network, the router blocks it. There is no open port via which the data could enter the local network. Some applications, such as games on the Internet, require several links (that is, several ports), so that players can communicate with each other. In addition, these applications must also be permitted to send requests from other users on the Internet to users in the local network. These applications cannot run if NAT is activated.
- = Using port forwarding (the forwarding of requests to particular ports), the router is forced to send requests from the Internet for a certain service, for example, a game, to the appropriate port(s) on the PC on which the game is running. Port triggering is a special variant of port forwarding. Unlike port forwarding, the DSL router forwards the data from the port block to the PC which has previously sent data to the Internet via a certain port (trigger port). This means that approval for the data transfer is not tied to one specific PC in the network, but rather to the port numbers of the required Internet service. Where configuration is concerned, you must define a so-called trigger port for the application and also the protocol (TCP or UDP) that this port uses. You then assign the public ports that are to be opened for the application to this trigger port. The router checks all outgoing data for the port number and protocol. If it identifies a match of port and protocol for a defined trigger port, then it opens the assigned public ports and notes the IP address of the PC that sent the data. If data comes back from the Internet via one of these public ports, the router allows it to pass through and directs it to the appropriate PC. A trigger event always comes from a PC within the local network. If a trigger port is addressed from outside, the router simply ignores it.

Note:

- = An application that is configured for port triggering can only be run by one user in the local network at a time.
- = After public ports are opened, they can be used by unauthorized persons to gain access to a PC in the local network.
- = When the DSL router is supplied, the NAT function is activated. For example, all IP addresses of PCs in the local network are converted to the public IP address of the router when accessing the Internet. You can use NAT settings to configure the DSL router to carry out the following tasks.
- = For functions described as follows, IP addresses of the PCs must remain unchanged. If the IP addresses of the PCs are assigned via the DHCP server of the DSL router, you must disable DHCP server as the settings in the local network menu entry for the lease time or assign static IP addresses for the PCs.

You can enable or disable the NAT function. By default, the NAT function is enabled.

NAT-Virtual Server Setup

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.

Web Configuration

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.

To accomplish this, do as follows:

Step 1 Define a port forwarding rule for the HTTP service, with the PC IP or host name.

Step 2 Specify 8080 in the **Forward to Port** field.

All incoming HTTP traffic is forwarded to the PC running the Web server on port 8080. When setting a port forwarding service, ensure that the port is not used by another application, which may stop functioning. A common example is when using SIP signaling in Voice over IP, the port used by the gateway VoIP application (5060) is the same port, on which port forwarding is set for LAN SIP agents.

Note: Some applications, such as FTP, TFTP, PPTP and H323, require the support of special specific application level gateway (ALG) modules in order to work inside the home network. Data packets associated with these applications contain information that allows them to be routed correctly. An ALG is needed to handle these packets and ensure that they reach their intended destinations. DSL router is equipped with a robust list of ALG modules in order to enable maximum functionality in the home network. The ALG is automatically assigned based on the destination port.

Virtual servers are configured for this purpose.

Adding Port Forwarding

Step 1 To set up virtual servers for a service, select **Advanced Setup > NAT > Virtual Servers**, and click **Add**.

NAT -- Virtual Servers Setup

Virtual server allows you to direct incoming traffic from WAN side (identified by protocol and external port) to the internal server with private IP address on the LAN side. The internal port is required only if the external port needs to be converted to a different port number used by the server on the LAN side. A maximum 32 entries can be configured.

Add Remove

Server Name	External Port Start	External Port End	Protocol	Internal Port Start	Internal Port End	Server IP Address	Remote Host	Remarks
-------------	---------------------	-------------------	----------	---------------------	-------------------	-------------------	-------------	---------

Web Configuration

- Step 2** Select a service or enter a custom server.
- Step 3** Set **Server IP Address**.
- Step 4** 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.
- Step 5** Set **External Port Start** and **External Port End**.
- Step 6** Select **Protocol**.
- Step 7** Set **Internal Port Start** and **Internal Port End**.
- Step 8** Enter **Remote IP**.
- Step 9** Click **Save/apply** to apply the settings.

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

Select the protocol for the service you are providing from the **Protocol** drop-down list.

Under **External Port**, enter the port number of the service you are providing. In the **Internal Port** field, enter the internal port number, to which service requests are to be forwarded. In the **Local IP Address** field, enter the IP address of the PC that provides the service.

Virtual Server

Select the service name and enter the server IP address and click **Save/apply** to forward IP packets to the server. If the service name is the "Internal Port" field must be changed. If the service is "External Port" already and will be the same as the "Internal Port Start" or "External Port Start" if either one is nullified. Remaining number of entries that can be configured: 32

Service Name:

Select a Service:

Internal IP Address:

External Port Start:

External Port Start	External Port End	Protocol	Internal Port Start	Internal Port End	Remote IP
		HTTP			
		TCP			
		UDP			
		TCP			
		UDP			
		TCP			
		UDP			
		TCP			
		UDP			
		TCP			
		UDP			
		TCP			
		UDP			
		TCP			
		UDP			

Example

The Web server is configured to react to requests on port 8080. However, the requests from websites enter the Web server via port 80 (standard value). If you add the PC to the forwarding table and define port 80 as the public port and port 8080 as an internal port, all requests from the Internet are diverted to the service with port 80 on the Web server of the PC you have defined with port 8080.

Deleting Port Forwarding

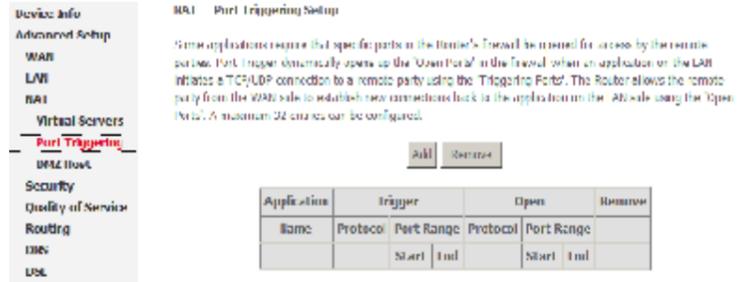
- Step 1** Select the **Remove** check box.
- Step 2** Click **Remove** to apply the settings.

Port Triggering

If you configure port triggering for a certain application, you need to determine a so-called trigger port and the protocol (TCP or UDP) that this port uses. You then assign the public ports that are to be opened for the application to this trigger port. You can select known Internet services or manually assign ports or port blocks.

Adding Port Triggering

Step 1 To set up port triggering for a service, select **Advanced Settings > NAT > Port Triggering**, and click **Add**.

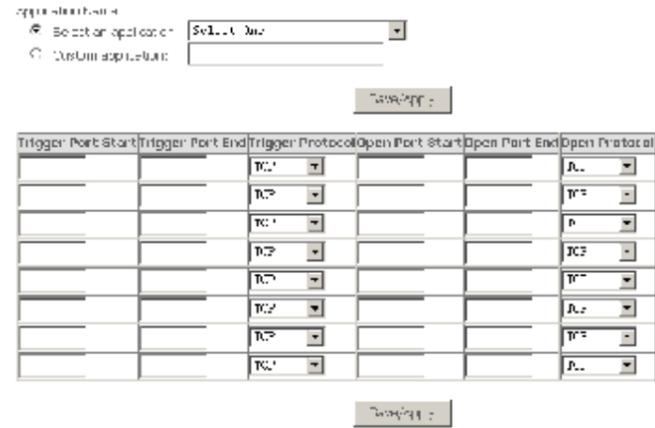


Step 2 Select the required application from the **Select an application** drop-down list, or manually enter the information in the **Custom application** field.

- = **Trigger Port Start and Trigger Port End**: enter the port that is to be monitored for outgoing data traffic.
- = **Trigger Protocol**: select the protocol that is to be monitored for outgoing data traffic.
- = **Open Protocol**: select the protocol that is to be allowed for incoming data traffic
- = **Open Port Start and Open Port End**: enter the port that is to be opened for incoming traffic.

Step 3 Click **Save/Apply** to apply the settings.

Router's firewall will be opened for access by the applications. You can confer to the port settings from this screen by selecting an application. Total number of entries: you can't (Custom Application) > List: Save/Apply: Break: Remaining number of entries that can be configured: 32



Removing Port Triggering

Step 1 Select the **Remove** check box.

Step 2 Click **Save/Apply** to apply 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.

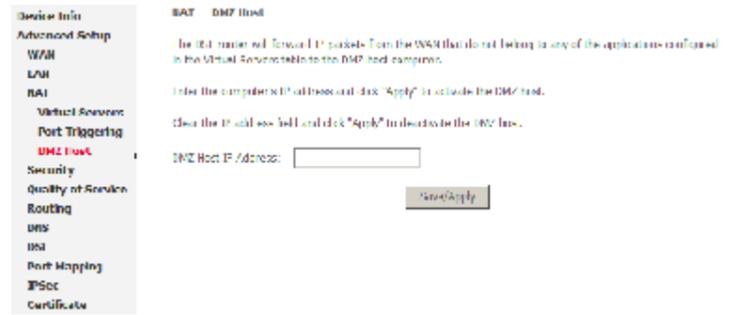
Web Configuration

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

- Step 1** To set up a PC as a DMZ host, select **Advanced Setup > NAT > DMZ host**.
- Step 2** Enter the local IP address of the PC that is to be enabled as an exposed host.
- Step 3** Click **Save/Apply** to apply the settings.



Remove DMZ host

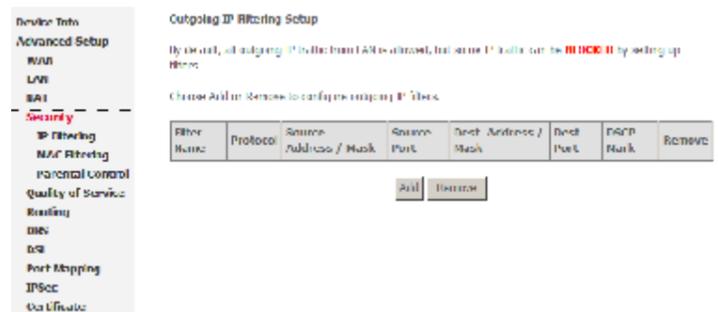
- Step 1** Clear the DMZ Host Address.
- Step 2** Click **Save/Apply** to apply the settings.

Security

Click **Security > IP Filtering** and the following interface 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.

Note: If the modem is configured to bridge mode only, IP filtering is disabled and the IP filtering interface does not appear.

If the modem does not configure a PVC of Bridge mode, MAC filtering is disabled and the MAC Filtering interface does not appear.



Outgoing IP Filtering Setup

Click **Security > IP Filtering > Outgoing** and the following page appears.

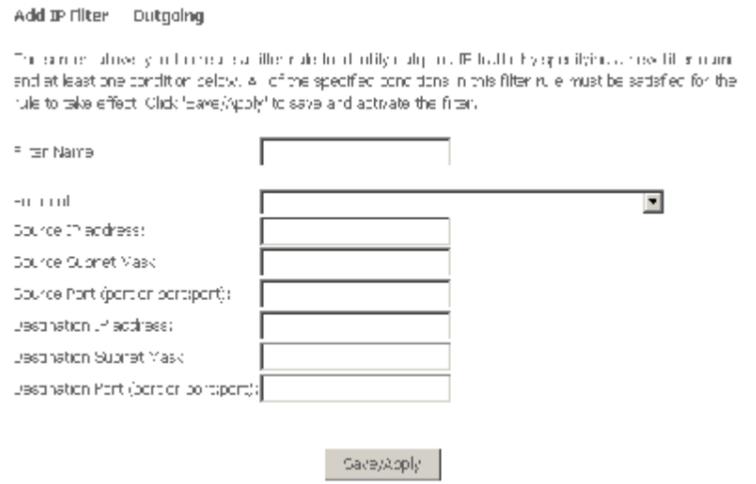
By default, all outgoing IP traffic from LAN is allowed, but some IP traffic can be blocked by setting up filters.



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.

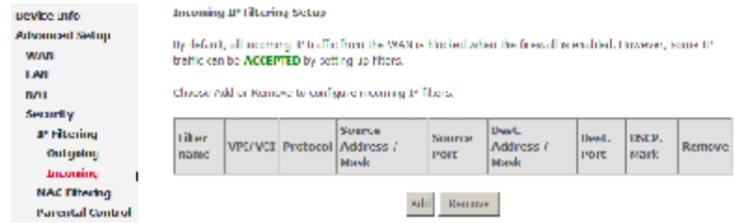
Click **Save/Apply** to save and activate the filter.



Incoming IP Filtering Setup

Click **Security > IP Filtering > Incoming** and the following 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.



Web Configuration

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

Read the warning information. Click **Yes** to change the MAC filtering global policy from **Forwarded** to **Blocked**. Click **No** to cancel.

For example, to forbid the PC whose MAC address is 00:13:20:9E:0F:10 through PPPoE dial-up, begin with the following page.

Click **Add** to configure the interface as follows.

Click **Save/Apply** and the following page appears.

Change MAC Filtering Global Policy

WARNING: Changing from one global policy to another will cause all defined rules to be REMOVED AUTOMATICALLY! You will need to create new rules for the new policy.

Are you sure you want to change MAC Filtering Global Policy from **FORWARDED** to **BLOCKED**?

Add MAC Filter

Create a filter to identify the MAC Layer frames by specifying global and interface rules. If multiple conditions are specified, all of them take effect. Click 'Apply' to save and activate the filter.

Protocol Type:

Destination MAC Address:

Source MAC Address:

Frame Direction:

WAN Interfaces (Configured in Bridge mode only)

- Serial
- br 0 0 05mas 0 0 05

MAC Filtering Setup

MAC Filtering Global Policy: **FORWARDED**

MAC Filtering is not effective on a DSL Port configured in Bridge mode. **FORWARDED** means that all MAC Layer frames will be **FORWARDED** unless they are matching with any of the specific rules in the following table. **BLOCKED** means that all MAC Layer frames will be **BLOCKED** except those matching with any of the specific rules in the following table.

Choose Add or Remove to configure MAC filtering rules

VPI/VCI	Protocol	Destination MAC	Source MAC	Frame Direction	Remove
ALL	PPPoE		00:13:20:9E:0F:10	LAN to WAN	<input type="checkbox"/>

Parental Control

Click **Security>Parental Control** and the following page appears.

Click **Add** and the following 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.

Time of Day Restrictions -- A maximum 16 entries can be configured.

Username	MAC	Mon	Tue	Wed	Thu	Fri	Sat	Sun	Start	Stop	Remove
<input type="button" value="Add"/> <input type="button" value="Remove"/>											

Time of Day Restriction

This page allows 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 the 'Other MAC Address' button and enter the MAC address of the other LAN device. To find out the MAC address of a Windows based PC, go to command prompt and type 'ipconfig /all'

User Name:

Browser's MAC Address:

 Other MAC Address:

(Hexadecimal only)

Days of the Week	Mon	Tue	Wed	Thu	Fri	Sat	Sun
Link to select	<input type="checkbox"/>						

Start Blocking Time (hh:mm)

End Blocking Time (hh:mm)

URL Filter

Choose **Advanced Setup > Parental Control > Url Filter**, and the **Url Filter** page appears. In this page, there are two URL list types – **Exclude** and **Include**. If select Exclude, LAN devices could not access Url addresses in the list. And so if select Include, LAN devices just could access Url addresses in the list. Otherwises, one of list types should be selected.

URL Filter -- A maximum 100 entries can be configured.

URL List Type: Exclude Include

Address	Port	Remove
<input type="button" value="Add"/> <input type="button" value="Remove"/> <input type="button" value="Save/Reboot"/>		

Web Configuration

After proper selection, click **Add**. In this page, enter the URL address and port number then click **Save/Apply** to add the entry to the URL filter. If don't enter port number, default 80 will be applied.

Parental Control -- URL Filter Add

Enter the URL address and port number then click "Save/Apply" to add the entry to the URL filter.

URL Address:

Port Number:

(Default 80 will be applied if leave blank.)

Save/Apply

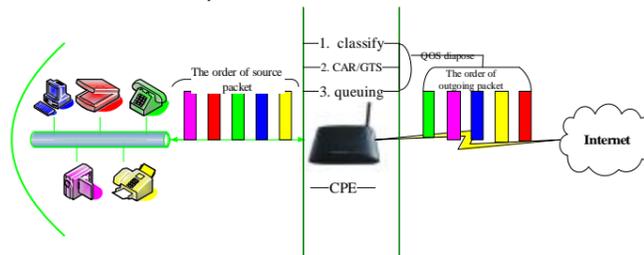
Quality of Service

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.

Click **Quality of Service** and the following page appears. Under **Quality of Service**, there are two network share modes: **Queue Config** and **QoS Classification**.

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.



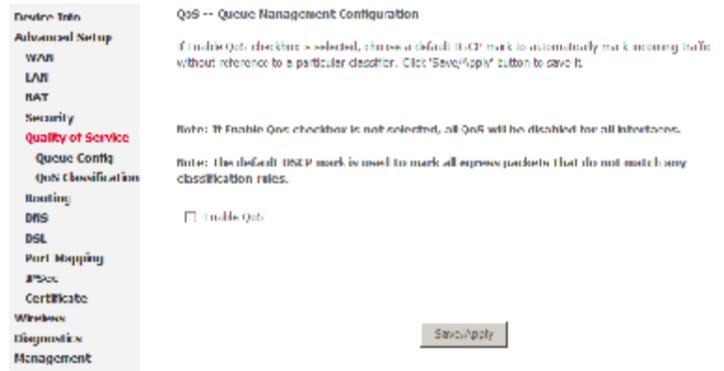
Enabling QoS

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.

Select **Advanced Setup > Quality of Service** and the following page appears.

Select **Enable QoS** to enable QoS and set the default DSCP mark.

Click **Save/Apply** to activate QoS.



QoS-Queue Configuration

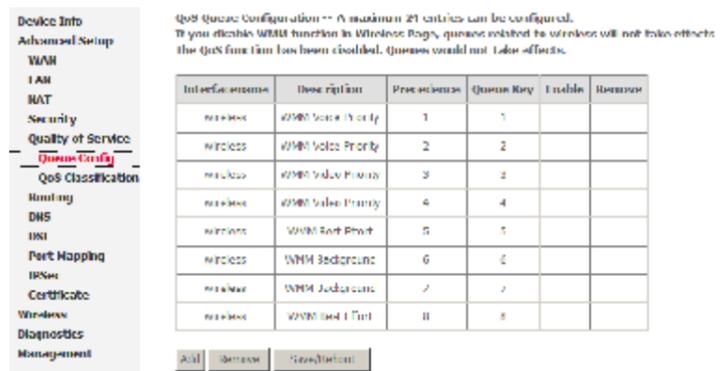
The queuing in packet QoS becomes effective only when packet is forwarded to QoS-enabled PVC. Packet forwarding is determined by IP routing or bridging, not under control of the packet QoS.

Click **Queue Config**, and the following page appears. In this page, you can configure QoS queue. A maximum of 24 entries can be configured.

QoS Queue Configuration 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.

For example, add a QoS queue entry and allocate it to a specific network interface (PVC 0/0/35). Set integer values for queue precedence to 1.

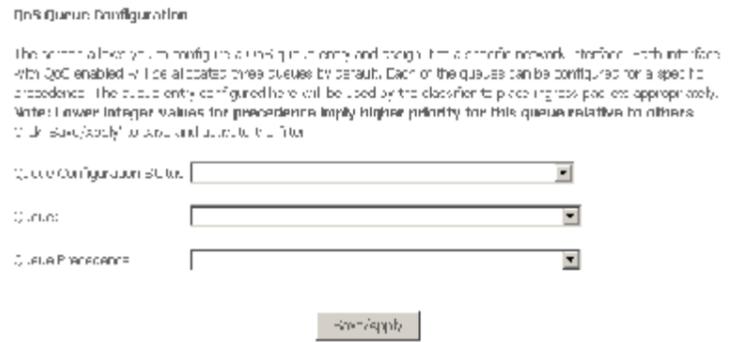


Web Configuration

Step 1 Click **Add**, and the following page appears.

- = **Policy Select:** you can select Strict Priority Policy or WRR Policy.
- = **Queue Configuration Status:** set to enable or disable a QoS queue.
- = **Queue:** select a specific network interface. When you have already selected a network interface, the specific network interface selected automatically allocates to the queue.
- = **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.

Step 2 Add a QoS queue entry and assign it to a specific network interface (PVC 0/0/35), and set integer values for queue precedence to 1. See the following figure:



Web Configuration

Step 3 After proper modifications, click **Save/Apply** and the following page appears. This configuration takes effective at once.

To delete a certain queue, disable it, select it, and then click **Remove**.

After the queue is configured, you can create several traffic class rules to classify the upstream traffic.

QoS Queue Configuration - A maximum 24 entries can be configured. If you disable WMM function in Wireless Page, queues related to wireless will not take effects

Interface Name	Description	Precedence	Queue Key	Enable	Remove
wireless	WMM Voice Priority	1	1	<input type="checkbox"/>	<input type="checkbox"/>
wireless	WMM Video Priority	2	2	<input type="checkbox"/>	<input type="checkbox"/>
wireless	WMM Video Priority	3	3	<input type="checkbox"/>	<input type="checkbox"/>
wireless	WMM Video Priority	4	4	<input type="checkbox"/>	<input type="checkbox"/>
wireless	WMM Best Effort	5	5	<input type="checkbox"/>	<input type="checkbox"/>
wireless	WMM Background	6	6	<input type="checkbox"/>	<input type="checkbox"/>
wireless	WMM Background	7	7	<input type="checkbox"/>	<input type="checkbox"/>
wireless	WMM Best Effort	8	8	<input type="checkbox"/>	<input type="checkbox"/>
eth0/usb		1	1	<input checked="" type="checkbox"/>	<input type="checkbox"/>

WRR (Weighted Round Robin): this is another QoS method. If you want to set WRR, you must disable the **Strict-Priority Queue (PQ)**. The WRR is mutex to PQ. Only one QoS method can exist at the same time. Select WRR in **QoS Queue Configuration** page. The following interface appears.

For example, add a QoS queue entry and allocate it to a specific network interface (PVC 0/2/35). Set queue precedence to 2 and weight value to 30%.

QoS Queue Configuration

The WRR method is mainly for using in every and large enterprise network. Before setting for the WRR, you should disable the Strict-Priority Queue (PQ). The WRR is mutex to PQ. Only one QoS method can exist at the same time. Select WRR in QoS Queue Configuration page. The following interface appears.

Interface:

Queue Name:

Queue Precedence:

Weight:

Web Configuration

After proper modifications, click **Save/Apply** and the following page appears.

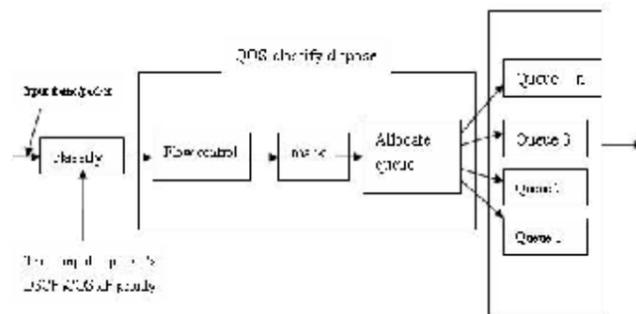
QoS Queue Configuration - A maximum 24 entries can be configured.
 If you disable WMM function in Wireless Page, queues related to wireless will not take effects

Interface name	Description	Precedence	Queue Key	Disable	Remove
> wlan	WMM Voice Priority	1	1	<input type="checkbox"/>	<input type="checkbox"/>
> wlan	WMM Video Priority	2	2	<input type="checkbox"/>	<input type="checkbox"/>
> wlan	WMM Video Priority	3	3	<input type="checkbox"/>	<input type="checkbox"/>
> wlan	WMM Video Priority	4	4	<input type="checkbox"/>	<input type="checkbox"/>
> wlan	WMM Best Effort	5	5	<input type="checkbox"/>	<input type="checkbox"/>
> wlan	WMM Best Effort	6	6	<input type="checkbox"/>	<input type="checkbox"/>
> wlan	WMM Best Effort	7	7	<input type="checkbox"/>	<input type="checkbox"/>
> wlan	WMM Best Effort	8	8	<input type="checkbox"/>	<input type="checkbox"/>
PVC 0,0/25	WRR 0%	1	9	<input checked="" type="checkbox"/>	<input type="checkbox"/>
PVC 0,0/25	WRR 30%	2	--	<input checked="" type="checkbox"/>	<input type="checkbox"/>

The weighted round robin (WRR) queue schedule divides each port into several output queues. Queues are scheduled in turn to ensure that each queue obtains a certain service time. WRR configures a weighted value (w3, w2, w1 and w0) for each queue. The weighted value represents the proportion of the obtained resources. For example, the weighted value of WRR queue schedule algorithm of a 100M port is configured as 50, 30, 10 and 10 (corresponding to w3, w2, w1 and w0), so that the queue with minimum priority obtains a bandwidth of at least 10Mbps, which avoids the disadvantage that a message in queue with low priority during PQ schedule may not obtain service for a long time. WRR queue still has another advantage. Although the schedule of these queues are conducted in turn, each queue is not assigned with a fixed service time slice-if a certain queue is null, it is immediately changed to the next queue. In this way, the bandwidth resources can be fully utilized.

QoS-QoS Classification

Some applications require specific bandwidth to ensure its data be forwarded in time. QoS classification can create traffic class rule to classify the upstream traffic. Assign queue which defines the precedence and the interface and optionally overwrite the IP header DSCP byte. After QoS classification, QoS divides capacity between different applications and provides undelayed, continuous data transfer where data packet with higher priority is given preference. The follow figure shows QoS classification.



QoS-DSCP Setting

In order to understand what is differentiated services code point (DSCP), you should be familiar with the differentiated services model (Diffserv). Diffserv is a class of service (CoS) model that enhances best-effort Internet services via differentiating traffic by users, service requirements and other criteria. Packets are specifically marked, allowing network nodes to provide different levels of service, via priority queuing or bandwidth allocation, or by choosing dedicated routes for specific traffic flows.

As displayed in following diagram, the IPv4 packet has a TOS field. Diffserv defines TOS field in IP packet headers referred to as DSCP. Hosts or routes that pass traffic to a Diffserv-enabled network typically mark each transmitted packet with an appropriate DSCP. The DSCP markings are used by Diffserv network routers to appropriately classify packets and to apply particular queue handing or scheduling behavior.

Layer 3 IPv4 packet

Version/length	TOS (1 word)	length	ID	Offset/mark	TTL	protocol	Checksum	IP-SA	IP-DA	data
----------------	--------------	--------	----	-------------	-----	----------	----------	-------	-------	------

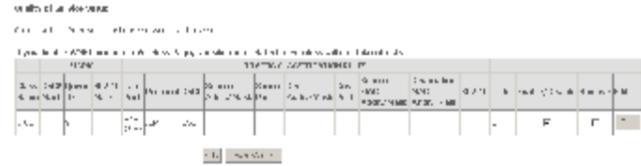
TOS field-IP priority (TOS front 3 bit) or DSCP (front 6 bit)

7	6	5	4	3	2	1	0
IP priority			Undefined				
DSCP				Flow control			

For example, mark each transmitted ICMP packet which passes traffic to 0-35class with an appropriate DSCP (CS1).

After proper modifications, click **Save/Apply** and the following page appears.

Click **Save/Apply**. This configuration takes effective at once.



QoS-802.1p Setting

The IEEE 802.1p priority marking method is a standard for prioritizing network traffic at the data link/Mac sub-layer. 802.1p traffic is simply classified and sent to the destination, with no bandwidth reservations established.

The following diagram shows the structure of 802.1Q Frame. The 802.1Q header includes a 3-bit prioritization field, which allows packets to be grouped into eight levels of priority (0-7), where level 7 is the highest one. In addition, DSL maps these eight levels to priority queues, where queue 1 has the highest priority.

Layer 2 802.Q frame

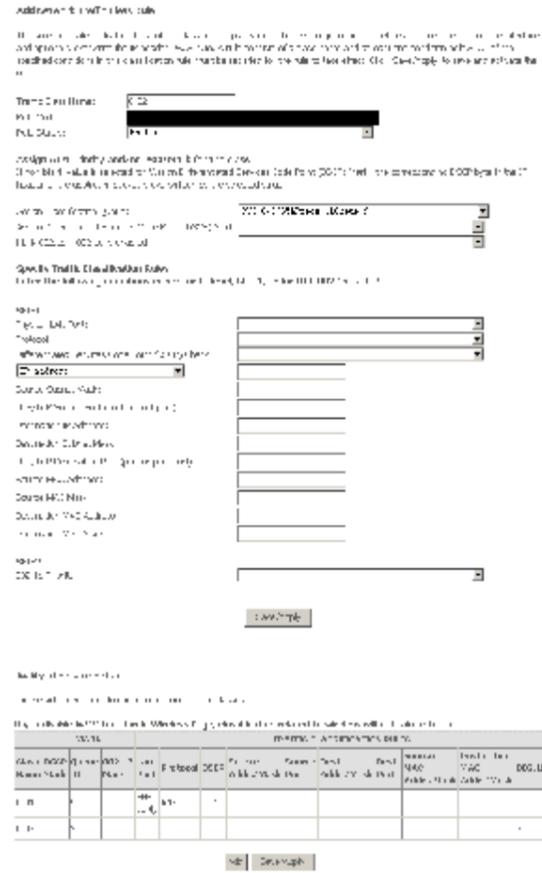
Preamble	SFD	DA	SA	mark (4 word)	Len/Etype (2 word)	DATA	FCS
----------	-----	----	----	------------------	-----------------------	------	-----

Mark

TPID(0x8100)	Priority(3bit)	CFI (1bit)	VLAN (12bit)	ID
--------------	----------------	------------	-----------------	----

Web Configuration

For example: mark the frame of 802.1p that queued to Queue 9 on value 2.



After proper modifications, click **Save/Apply** to show the following interface.

Routing

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



Routing - 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 **Save/Apply**.

Note: If the Automatic Assigned Default Gateway check box is changed from deselected to selected, you need to reboot the router to obtain the automatic assigned default gateway.



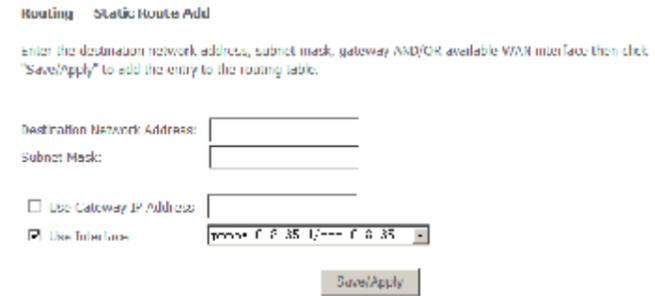
Routing - Static Route

In this interface, you can modify the static route settings.

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.
- = **Subnetmask:** 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** and the following page appears. Enter the destination network address, subnet mask, gateway AND/OR available WAN interface, then click **Save/Apply** to add the entry to the routing table.



DNS

DNS Server

In this interface, you can modify the DNS server settings.



Web Configuration

If select **Enable Automatic Assigned DNS**, this router accepts the first received DNS assignment from one of the PPPoA, PPPoE or MER/DHCP enabled PVC(s) during the connection establishment.

If the checkbox is not selected, enter the primary and optional secondary DNS server IP addresses. The interface is as follows.

Click **Save** to save the new configuration.

Note: You must reboot the router to make the new configuration effective.

DNS Server Configuration

If you select **Enable Automatic Assigned DNS** checkbox as enable, this router will accept the first received DNS assignment from one of the PPPoA, PPPoE or MER/DHCP enabled PVC(s) during the connection establishment. If the checkbox is not selected, enter the primary and optional secondary DNS server IP addresses. Click **Save** button to save the new configuration. You must reboot the router to make the new configuration effective.

Enable Automatic Assigned DNS

Primary DNS server:

Secondary DNS server:

Save

Dynamic DNS

In this interface, you can modify the Dynamic DNS settings.

The Dynamic DNS service allows you to alias a dynamic IP address to a static hostname in any of the many domains, allowing your DSL router to be more easily accessed from various locations on the Internet.

- Device Info
- Advanced Setup
 - WAN
 - LAN
 - RAI
 - Security
 - Quality of Service
 - Routing
 - DNS
 - DNS Server
 - Dynamic DNS**
 - DSL
 - Port Mapping
 - IPSec
 - Certificate

Dynamic DNS

The Dynamic DNS service allows you to alias a dynamic IP address to a static hostname in any of the many domains, allowing your DSL router to be more easily accessed from various locations on the Internet.

Click **Add to Domains** to configure Dynamic DNS.

Domains | **Domains** | **Services** | **Interface** | **Domains**

Add | **Remove**

Web Configuration

Click **Add** to add dynamic DDNS.

Add dynamic DDNS

This page allows you to add a Dynamic DNS address from DynDNS.org or TZO.

D-DNS provider	<input type="text" value="DynDNS.org"/>
Hostname	<input type="text"/>
Interface	<input type="text" value="pppoe_0_0_35_1/ppp_0_0_35_1"/>

DynDNS Settings

Username	<input type="text"/>
Password	<input type="text"/>

DSL

In this interface, you can modify the DSL settings.

Select one you need. But the default setting can check G.dmt/ G.lite/ T1.413/ ADSL2/AnnexI/ ADSL2+/ Inner pair/ Bitswap. The modem can negotiate the modulation mode with the DSLAM.

<ul style="list-style-type: none"> Device Info Advanced Setup WAN LAN NAT Security Quality of Service Routing DNS DSL Port Mapping IPSec Certificate Wireless Diagnostics Management 	<p>DSL Settings</p> <p>Select the modulation below.</p> <ul style="list-style-type: none"> <input checked="" type="checkbox"/> G.Dmt Enabled <input checked="" type="checkbox"/> G.lite Enabled <input checked="" type="checkbox"/> T1.413 Enabled <input checked="" type="checkbox"/> ADSL2 Enabled <input checked="" type="checkbox"/> AnnexL Enabled <input checked="" type="checkbox"/> ADSL2+ Enabled <input type="checkbox"/> AnnexM Enabled <p>Select the phone line pair below.</p> <ul style="list-style-type: none"> <input checked="" type="radio"/> Inner pair <input type="radio"/> Outer pair <p>Capability</p> <ul style="list-style-type: none"> <input checked="" type="checkbox"/> Bitswap Enable <input type="checkbox"/> HRA Enable
---	---

Port Mapping

Port Mapping supports multiple ports to PVC and bridging groups. Each group performs as an independent network. To support this feature, you must create mapping groups with appropriate LAN and WAN interfaces using the **Add** button. The **Remove** button removes the grouping and adds the ungrouped interfaces to the Default group. Only the default group has the IP interface.

In **Port Mapping** page, select the **Enable virtual ports** check box and create three virtual interfaces within the Linux system. Each virtual interface represents a physical Ethernet port within the external Ethernet Switch. The page displays four Ethernet ports: ENET1, ENET2, ENET3, and ENET4. ENET1, ENET2, and ENET3 represent Ethernet port ID 0, 1 and 2 within the Ethernet Switch respectively. ENET4 represents the Ethernet MAC/PHY MDI port.

If you deselect the **Enable virtual ports** check box, the modem fails to recognize individual Ethernet ports within the Ethernet switch. The page displays two Ethernet ports, ENET(1-3) and ENET4. The ENET(1-3) represents the Ethernet MAC MII port. The ENET4 represents the BCM634x Ethernet MAC/PHY MDI port.

Creating a Mapping Group

Choose **Advanced Setup > Port Mapping**, and the following page appears.

Port Mapping -- A maximum 16 entries can be configured

Port Mapping supports multiple ports to P/C and bridging groups. Each group will perform as an independent network. To support this feature, you must create mapping groups with appropriate LAN and WAN interfaces using the Add button. The Remove button will remove the grouping and add the ungrouped interfaces to the Default group. Only the default group has IP interface.

Enable virtual ports on:

Group Name	Enable/Disable	Remove	Edit	Interfaces	Enable/Disable
Default	<input checked="" type="checkbox"/>			ENET(1-4)	<input checked="" type="checkbox"/>
				Wireless	<input checked="" type="checkbox"/>
				RAS_0_0_35	<input checked="" type="checkbox"/>

Web Configuration

Click **Add**, and the following page appears.

- = **Group Name:** Enter a unique group name.
- = **Grouped Interfaces:** The port belongs to this group.
- = **Available Interfaces:** It shows the available Ethernet port which you can select.
- = **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 vendor ID of default DHCP client of Windows 2000/XP is MSFT 5.0).

Enter the Group name and select interfaces from the available interface list and add it to the grouped interface list using the arrow buttons to create the required mapping of the ports. The group name must be unique.

If you like to automatically add LAN clients to a PVC in the new group, add the DHCP vendor ID string. By configuring a DHCP vendor ID string, DHCP clients with the specified vendor ID (DHCP option 60) refuse IP addresses from the local DHCP server.

Note: These clients may obtain public IP addresses.

Click **Save/Apply** to apply the changes immediately.

Note: The selected interfaces are removed from their existing groups and added to the new group.

Port Mapping Configuration

To create a new mapping group:

1. Enter the Group name and select interfaces from the available interface list and add it to the grouped interface list using the arrow buttons to create the required mapping of the ports. The group name must be unique.
2. If you like to automatically add LAN clients to a PVC in the new group add the DHCP vendor ID string. By configuring a DHCP vendor ID string, DHCP client request with the specified vendor ID (DHCP option 60) will be denied an IP address from the local DHCP server.
Note: that these clients may obtain public IP addresses.
3. Click **Save/Apply** button to make the changes effective immediately.

Note: that the selected interfaces will be removed from their existing groups and added to the new group.

IMPORTANT! If a vendor ID is configured for a specific client device, please **REBOOT** the client device attached to the modem to allow it to obtain an appropriate IP address.

Group Name:

Grouped Interfaces	Available Interfaces
<div style="border: 1px solid black; height: 50px; width: 100%;"></div>	ETHER (1-4) nsl_u_u_t Wireless

Automatically Add Clients With the following DHCP Vendor IDs:

IPSec

Click **IPSec**, and the following page appears.

Click **Add New Connection** to add a new IPSec connection.

You can click **Show Advance Settings** to view some advance parameters and modify them to match the other side of this connection.

Click **Save/Apply** to save this connection, then you can check the checkbox of enable column to enable this IPSec connection. And the communication is established.

Device Info

Advanced Setup

WAN

LAN

RAI

Security

Quality of Service

Routing

DMZ

DSL

Port Mapping

IPSec

Certificate

Wireless

Diagnostics

Management

IPSec: Tunnel Mode Connections

Add, edit or remove IPSec tunnel mode connections from this page.

	Enable	Connection Name	Remote Gateway	Local Addresses	Remote Addresses
	<input type="checkbox"/>				

[Add New Connection](#)

IPSec Settings

IPSec Connection Name

Remote IPSec Gateway Address

Tunnel access from local IP addresses

IP Address for VPN

IP Subnetmask

Tunnel access from remote IP addresses

IP Address for VPN

IP Subnetmask

Key Exchange Method

Authentication Method

Pre-Shared Key

Perfect Forward Secrecy

Advanced IKE Settings

Certificate

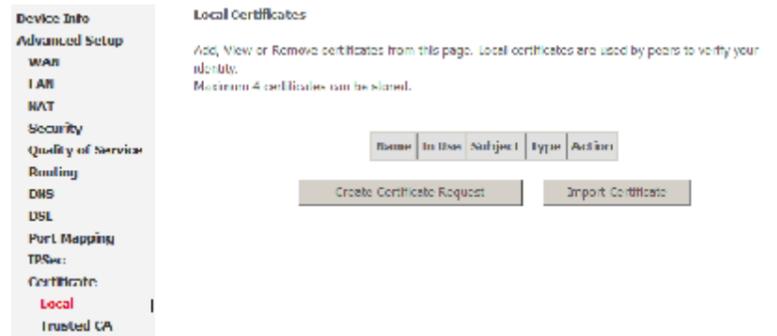
Local Certificates

Click **Certificate > Local** and the following page appears.

Local certificates are used by peers to verify your identity. It can store maximum 4 certificates.

Click **Create Certificate Request** and the following page appears.

To generate a certificate signing request, you need to include Common Name, Organization Name, State/Province Name, and the 2-letter Country Code for the certificate.



Create new certificate request

To generate a certificate signing request you need to include Common Name, Organization Name, State/Province Name, and the 2-letter Country Code for the certificate.

Certificate Name:

Common Name:

Organization Name:

State/Province Name:

Country/Region Name:

Web Configuration

If click **Import Certificate**, the following page appears. Then you can enter certificate name, paste certificate content and private key.

Import Certificate

Enter certificate name, paste certificate content and private key.

Certificate Name:

Certificate:

```
-----BEGIN CERTIFICATE-----  
[Certificate Content]  
-----END CERTIFICATE-----
```

Private Key:

```
-----BEGIN PRIVATE KEY-----  
[Private Key Content]  
-----END PRIVATE KEY-----
```

Trusted CA Certificates

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

Device Info

- Advanced Setup
- WAN
- LAN
- NAT
- Security
- Quality of Service
- Routing
- DNS
- DSL
- Port Mapping
- IPSec
- Certificate
- Local
- Trusted CA**

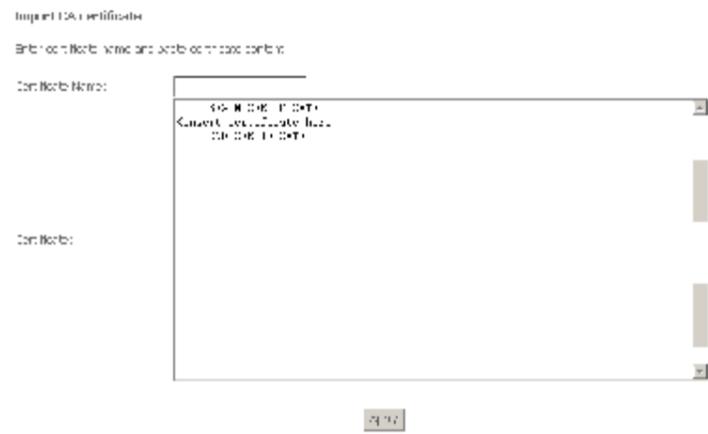
Trusted CA (Certificate Authority) Certificates

All, valid or expired certificates from this page. CA certificates are used by you to verify peers' certificates. Maximum 4 certificates can be stored.

Name	Subject	Type	Action
------	---------	------	--------

Web Configuration

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



Wireless

This section introduces the wireless LAN and some basic configurations. Wireless LAN can be as simple as two computers with wireless LAN cards communicating in a peer-to-peer network or as complex as a number of computers with wireless LAN cards communicating through access points (AP) that bridge network traffic to the wired LAN.

The Modem Wi-Fi® certified IEEE 802.11g compliant wireless access point allows multiple computers to connect wirelessly to your local network over the Modem Wireless LAN environment. The Modem is backward compatible with IEEE 802.11b, which means 802.11b and 802.11g devices can coexist in the same wireless network. The Wireless Distribution System (WDS) on your Modem allows you to extend the range of your wireless network. To be able to use WDS, you will need to introduce an additional WDS-enabled access point into your wireless network. To be able to connect the computers, make sure that a wireless client adapter (WLAN client) is installed on each computer you want to connect via the WLAN.

Wireless LAN Basics

Some basic understanding of 802.11b/g wireless technology and terminology is useful when you are setting up the Router or any wireless access point. If you are not familiar with wireless networks please take a few minutes to learn the basics.

Wireless client requirements

All wireless client adapters compliant to 802.11g and/or 802.11b can communicate with the Modem (W) LAN environment. However, be aware that only 802.11g compliant wireless clients are able to gain full profit of the 54 Mb/s (Max) bandwidth delivered by the Modem. It is highly recommended to use only wireless client adapters that are Wi-Fi™ certified to ensure smooth interoperability with the Modem's WLAN.

Radio Transmission

Wireless LAN or WLAN devices use electromagnetic waves within a broad, unlicensed range of the radio spectrum to transmit and receive radio signals. When a wireless access point is present, it becomes a base station for the WLAN nodes in its broadcast range. WLAN nodes transmit digital data using FM (frequency modulation) radio

Web Configuration

signals. WLAN devices generate a carrier wave and modulate this signal using various techniques. Digital data is superimposed onto the carrier signal. This radio signal carries data to WLAN devices within range of the transmitting device. The antennae of WLAN devices listen for and receive the signal. The signal is demodulated and the transmitted data extracted. The transmission method used by the access point is called Direct Sequence Spread Spectrum (DSSS) and operates in a range of the radio spectrum between 2.4GHz and 2.5GHz for transmission. See the expert technical specifications for more details on wireless operation.

Antennas

Direct the external antenna to allow optimization of the wireless link. If for example the antenna is erect, wireless links in the horizontal plane are favored. Please note that the antenna characteristics are influenced by the environment, that is, by reflections of the radio signal against walls or ceilings. It is advisable to use the received signal strength as indicated by the wireless client manager to optimize the antenna position for the link to a given client. Concrete walls weaken the radio signal and thus affect the connection.

Range

Range should not be a problem in most homes or small offices. If you experience low or no signal strength in some areas, consider positioning the Router in a location between the WLAN devices that maintains a roughly equal straight-line distance to all devices that need to access the Router through the wireless interface. Adding more 802.11g access points to rooms where the signal is weak can improve signal strength. Read the section about placement of the Router titled Location in the next chapter, Hardware Installation, for more information.

SSID

Wireless networks use an SSID (Service Set Identifier) to allow wireless devices to roam within the range of the network. Wireless devices that wish to communicate with each other must use the same SSID. Several access points can be set up using the same SSID so that wireless stations can move from one location to another without losing connection to the wireless network. The Modem operates in Infrastructure mode. It controls network access on the wireless interface in its broadcast area. It will allow access to the wireless network to devices using the correct SSID after a negotiation process takes place. By default the Modem broadcasts its SSID so that any wireless station in range can learn the SSID and ask permission to associate with it. Many wireless adapters are able to survey or scan the wireless environment for access points. An access point in Infrastructure mode allows wireless devices to survey that network and select an access point with which to associate. You may disable SSID broadcasting the wireless menu of web management.

Radio channels

The 802.11g standard allows several WLAN networks using different radio channels to be co-located. The Modem supports multiple radio channels and is able to select the best radio channel at each startup. You can choose to set the channels automatically or manually.

The different channels overlap. To avoid interference with another access point, make sure that the separation (in terms of frequency) is as high as possible. It is recommended to keep at least 3 channels between 2 different access points.

The Modem supports all channels allowed for wireless networking. However, depending on local regulations, the number of channels actually allowed to be used may be additionally restricted, as shown in the table below.

Regulatory Domain	Allowed Radio Channels
USA / Canada	1 to 11

Wireless Security

Various security options are available on the Modem including open or WEP, 802.1x, WPA, WPA-PSK, WPA2 and WPA2-PSK. Authentication may use an open system or a shared key. For details on these methods and how to use them, please read the wireless LAN configuration information in Section 3.5.3 (Wireless Security Configuration).

About 802.11g Wireless

802.11b is an IEEE standard, operating at 2,4 GHz at a speed of up to 11 Mb/s. 802.11g, a newer IEEE standard also operating at 2,4 GHz, gives you up to 54 Mb/s speed, more security and better performance.

Today's 11-megabits-per-second 802.11b wireless networks are fine for broadband Internet access (which typically tops out at about 1 mbps) but rather slow for large internal file transfers or streaming video. However, 54-mbps, corporate-oriented 802.11a is expensive and because its radio uses the 5-GHz band and 802.11b uses the 2.4 GHz band, upgrading to an 802.11a network means either scrapping 802.11b gear or buying even-pricier hardware that can support both standards.

But 802.11g promises the same speed as 802.11a and the ability to coexist with 802.11b equipment on one network, since it too uses the 2.4-GHz band. 802.11g is an extension to 802.11b, the basis of many wireless LANs in existence today. 802.11g will broaden 802.11b's data rates to 54 Mbps within the 2.4 GHz band using OFDM (orthogonal frequency division multiplexing) technology. Because of backward compatibility, an 802.11b radio card will interface directly with an 802.11g access point (and vice versa) at 11 Mbps or lower depending on range. You should be able to upgrade the newer 802.11b access points to be 802.11g compliant via relatively easy firmware upgrades.

Similar to 802.11b, 802.11g operates in the 2.4GHz band, and the transmitted signal uses approximately 30MHz, which is one third of the band. This limits the number of non-overlapping 802.11g access points to three, which is the same as 802.11b.

Note: *Maximum wireless signal rate based on IEEE Standard 802.11g specifications is 54 Mbps. But actual data throughput varies depending on network conditions and environmental factors, including volume of network traffic, building materials and construction, and network overhead will cause lower actual data throughput rate.*

Access Point and Wireless Fidel

The Wi-Fi certification ensures that your Modem will interoperate with any Wi-Fi certified 802.11g and 802.11b compliant wireless device.

The Modem Wireless LAN Access Point (AP) behaves as a networking hub allowing to wirelessly interconnect several devices to the local (W) LAN and to provide access to the Internet.

Wireless – Basic

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.

Web Configuration

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. Otherwise, the Hide Access Point SSID, Country, Enable Wireless Guest Network, and Guest SSID box will not be displayed.
- = **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.
- = **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.
- = **Guest SSID:** The SSID (Service Set Identification) is the unique name shared among all devices in a guest wireless network. The SSID must be identical for all devices in the guest wireless network.

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

The screenshot shows the 'Wireless -- Basic' configuration page. On the left is a navigation menu with options: Device Info, Advanced Setup, Wireless (highlighted), Basic, Security, MAC filter, Wireless Bridge, Advanced, Station Info, Diagnostics, and Management. The main content area has a heading 'Wireless -- Basic' and a descriptive paragraph: '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. Click "Apply" to configure the basic wireless options.' Below this are several settings: 'Enable Wireless' (checked), 'Hide Access Point' (unchecked), 'Clients Isolation' (unchecked), and 'Disable WMM Advantise' (unchecked). There are input fields for SSID (containing 'Dlink1000'), BSSID (containing '00:73:07:39:77:CC'), Country (a dropdown menu set to 'CHINA'), and Max Clients (a text box containing '128'). A 'Save/Apply' button is at the bottom right.

Wireless – Security

This page allows you can configure security features of the wireless LAN interface. You can sets 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.

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). 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.

Web Configuration

Following is a description of the different options.

- = Select SSID: Select the wireless LAN of SSID to configure security features.
- = No Encryption: Please refer to below for details of configuration
- = Network Authentication: Select the authentication mode for the selected wireless LAN of SSID to be open.
- = WEP Encryption: Disable WEP Encryption.

The data is not encrypted when it is transferred from the device to the client station. This is the default option.

Click **Save/Apply** to save the wireless security options and make the modification effect.

64-bit WEP

- = Network Authentication: Select the authentication mode for the selected wireless LAN of SSID to be open or shared.
- = WEP Encryption: Enable WEP Encryption.
- = Encryption Strength: click the desired Data Security level to be 64-bit.
- = Current Network Key: Select one of network key that you set on the Key boxes as default one.
- = Network Key 1 to 4: Enter 5 ASCII characters or 10 hexadecimal digits for 64-bit encryption keys to fill out WEP keys box. The system allows you to type in 4 kinds of the WEP key.

Click **Save/Apply** to save the wireless security options and make the modification effect.

128-bit WEP

- = Network Authentication: Select the authentication mode for the selected wireless LAN of SSID to be open or shared.
- = WEP Encryption: Enable WEP Encryption.
- = Encryption Strength: Click the desired Data Security level to be 128-bit.
- = Current Network Key: Select one of network key that you set on the Key boxes as default one.
- = Network Key 1 to 4: Enter 13 ASCII characters or 26 hexadecimal digits for 128-bit encryption keys to fill out WEP keys box. The system allows you to type in 4 kinds of the WEP key.

Click **Save/Apply** to save the wireless security options and make the modification effect.

Network authentication: Shared

WEP Encryption: Enabled

Encryption Strength: 128-bit

Current Network Key: 1

Network Key 1

Network Key 2

Network Key 3

Network Key 4

Enter 13 ASCII characters or 26 hexadecimal digits for 128-bit encryption keys.
Enter 13 ASCII characters or 26 hexadecimal digits for 128-bit encryption keys.

Save/Apply

802.1x Authentication

- = Network Authentication: Select the authentication mode for the selected wireless LAN of SSID to be 802.1x.
- = Radius Server IP Address: Enter the IP Address of the authentication server.
- = Radius Port: Enter the port number of the authentication server. The default port number is 1812.
- = Radius Key: Enter the same key as the Radius server's.
- = WEP Encryption: Enable WEP Encryption. This is default
- = Encryption Strength: click the desired Data Security level to be 64-bit or 128-bit.
- = Current Network Key: Select one of network key that you set on the Key boxes as default one.
- = Network Key 1 to 4: Enter 5 ASCII characters or 10 hexadecimal digits for 64-bit encryption keys or enter 13 ASCII characters or 26 hexadecimal digits for 128-bit encryption keys to fill out WEP keys box. The system allows you to type in 4 kinds of the WEP key.

Click **Save/Apply** to save the wireless security options and make the modification effect.

Network authentication: 802.1x

Radius Server IP Address: 0.0.0.0

Radius Port: 1812

Radius Key: 1

WEP Encryption: Enabled

Encryption Strength: 128-bit

Current Network Key: 1

Network Key 1

Network Key 2

Network Key 3

Network Key 4

Enter 5 ASCII characters or 10 hexadecimal digits for 64-bit encryption keys.
Enter 13 ASCII characters or 26 hexadecimal digits for 128-bit encryption keys.

Save/Apply

WPA Authentication

- = Network Authentication: Select the authentication mode for the selected wireless LAN of SSID to be WPA.
- = WPA Group Rekey Interval: Specifies the timer the WPA key must change. If the value set 0, no need to change. The change is done automatically between the server and the client.
- = Radius Server IP Adress: Enter the IP Address of the authentication server.
- = Radius Port: Enter the port number of the authentication server. The default port number is 1812.
- = Radius Key: Enter the same key as the Radius server's.
- = WPA Encryption: Select TKIP, AES or TKIP + AES. The TKIP is default. The TKIP + AES encryption mode means AP auto adjust to use TKIP or AES according to wireless clients.

Click **Save/Apply** to save the wireless security options and make the modification effect.

WPA2 Authentication

- = Network Authentication: Select the authentication mode for the selected wireless LAN of SSID to be WPA2.
- = WPA2 Preauthentication: Select Enable or Disable.
- = Network Re-auth Interval: Specifies the timer of re-authentication between the server and the client.
- = WPA Group Rekey Interval: Specifies the timer the WPA key must change. If the value set 0, no need to change. The change is done automatically between the server and the client.
- = RADIUS Server IP Adress: Enter the IP Address of the authentication server.
- = RADIUS Port: Enter the port number of the authentication server. The default port number is 1812.
- = RADIUS Key: Enter the same key as the Radius server's.
- = WPA Encryption: Select TKIP, AES or TKIP + AES. The AES is default. The TKIP + AES encryption mode means AP auto adjust to use TKIP or AES according to wireless clients.

Click **Save/Apply** to save the wireless security options and make the modification effect.

Mixed WPA2/WPA Authentication

This authentication mode means AP auto adjust to use WPA2 or WPA according to wireless clients.

- = Network Authentication: Select the authentication mode for the selected wireless LAN of SSID to be Mixed WPA2/WPA.
- = WPA2 Preauthentication: Select Enable or Disable.
- = Network Re-auth Interval: Specifies the timer of re-authentication between the server and the client.
- = WPA Group Rekey Interval: Specifies the timer the WPA key must change. If the value set 0, no need to change. The change is done automatically between the server and the client.
- = Radius Server IP Address: Enter the IP Address of the authentication server.
- = Radius Port: Enter the port number of the authentication server. The default port number is 1812.
- = Radius Key: Enter the same key as the Radius server's.
- = WPA Encryption: Select TKIP, AES or TKIP + AES. The AES is default. The TKIP + AES encryption mode means AP auto adjust to use TKIP or AES according to wireless clients.

Click **Save/Apply** to save the wireless security options and make the modification effect.

WPA-PSK Authentication

- = Network Authentication: Select the authentication mode for the selected wireless LAN of SSID to be Mixed WPA-PSK.
- = WPA Pre-Shared Key: Enter the pre-shared key for WPA. Client stations must use the same key in order to connect with this device. Check the table below for instructions when entering the key.

Format	Minimum characters	Maximum Characters
ASCII	8	63
Hexadecimal	8	64

- = WPA Group Rekey Interval: Specifies the timer the WPA key must change. If the value set 0, no need to change. The change is done automatically between the server and the client.
- = WPA Encryption: Select TKIP, AES or TKIP + AES. The TKIP is default. The TKIP + AES encryption mode means AP auto adjust to use TKIP or AES according to wireless clients.

Click **Save/Apply** to save the wireless security options and make the modification effect.

WPA2-PSK Authentication

- = Network Authentication: Select the authentication mode for the selected wireless LAN of SSID to be Mixed WPA2-PSK.
- = WPA Pre-Shared Key: Enter the pre-shared key for WPA. Client stations must use the same key in order to connect with this device. Check the table below for instructions when entering the key.

Format	Minimum characters	Maximum Characters
ASCII	8	63
Hexadecimal	8	64

- = WPA Group Rekey Interval: Specifies the timer the WPA key must change. If the value set 0, no need to change. The change is done automatically between the server and the client.
- = WPA Encryption: Select TKIP, AES or TKIP + AES. The AES is default. The TKIP + AES encryption mode means AP auto adjust to use TKIP or AES according to wireless clients.

Click **Save/Apply** to save the wireless security options and make the modification effect.

Network Authentication:

WPA Pre-Shared Key: [Click here to copy](#)

WPA Group Rekey Interval:

WPA Encryption:

WPA Authentication:

Mixed WPA2/WPA-PSK Authentication

This authentication mode means AP auto adjust to use WPA2-PSK or WPA-PSK according to wireless clients.

- = Network Authentication: Select the authentication mode for the selected wireless LAN of SSID to be Mixed WPA2/WPA-PSK.
- = WPA Pre-Shared Key: Enter the pre-shared key for WPA. Client stations must use the same key in order to connect with this device. Check the table below for instructions when entering the key.

Format	Minimum characters	Maximum Characters
ASCII	8	63
Hexadecimal	8	64

- = WPA Group Rekey Interval: Specifies the timer the WPA key must change. If the value set 0, no need to change. The change is done automatically between the server and the client.
- = WPA Encryption: Select TKIP, AES or TKIP + AES. The AES is default. The TKIP + AES encryption mode means AP auto adjust to use TKIP or AES according to wireless clients.

Network Authentication:

WPA Pre-Shared Key: [Click here to copy](#)

WPA Group Rekey Interval:

WPA Encryption:

WPA Authentication:

Web Configuration

AES encryption mode means AP auto adjust to use TKIP or AES according to wireless clients.

Click **Save/Apply** to save the wireless security options and make the modification effect.

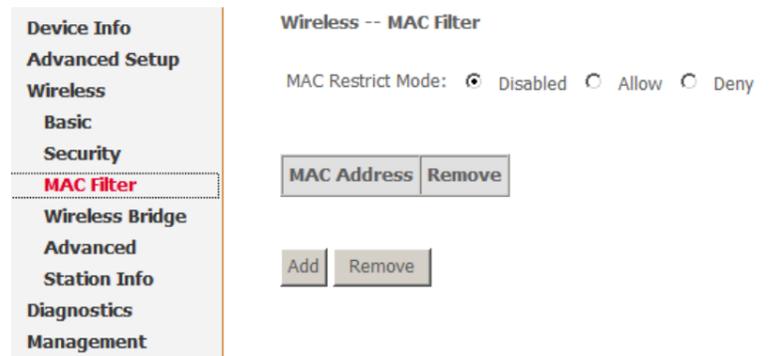
Wireless - MAC Filter

The web 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**.



Wireless – Bridge

This page allows you to configure wireless bridge features of the wireless LAN interface.

The Wireless Distribution System (WDS) allows you to extend the range of your wireless network by introducing one or more WDS-enabled devices into your wireless network. You can only establish WDS links with WDS-enabled devices.

Web Configuration

- = **AP Mode:** Select Access Point's functionality to be Access Point or pure Wireless Bridge. You can select Wireless Bridge (also known as Wireless Distribution System) to disable access point functionality. Selecting Access Point enables access point functionality and Wireless bridge functionality will still be available and wireless stations will be able to associate to the AP.
- = **Bridge Restrict:** Select **Disabled** in Bridge Restrict which disables wireless bridge restriction. Any wireless bridge will be granted access. Selecting **Enabled** or **Enabled (Scan)** enables wireless bridge restriction. Only those bridges selected in Remote Bridges are granted access.

You can manually enter Remote Bridges MAC Address to the list. You can also do it automatically in the following steps:

Step 1 In the Bridge Restrict list, click Enabled (Scan).

Step 2 Click Refresh to update the remote bridges.

The router waits for a few seconds to update. And then lists the results in the Accessible Access Points table.

Step 3 Check on the box in the left column of the list for selecting the Access Point to which you want to establish a WDS connection.

Step 4 Click **Save/Apply**.

You must configure all Bridges Access Point with:

- = The same encryption and authentication mode as Open, Shared, WEP, WPA-PSK or WPA2-PSK.
- = The same fixed channel.

Click **Save/Apply** to configure the wireless bridge options and make the modification effect.

The screenshot shows the 'Wireless -- Bridge' configuration page. On the left is a navigation menu with options: Device Info, Advanced Setup, Wireless, Basic, Security, MAC Filter, **Wireless Bridge** (highlighted), Advanced, Station Info, Diagnostics, and Management. The main content area has a title 'Wireless -- Bridge' and a paragraph explaining the page's purpose: 'This page allows you to configure wireless bridge features of the wireless LAN interface. You can select Wireless Bridge (also known as Wireless Distribution System) to disable access point functionality. Selecting Access Point enables access point functionality. Wireless bridge functionality will still be available and wireless stations will be able to associate to the AP. Select Disabled in Bridge Restrict which disables wireless bridge restriction. Any wireless bridge will be granted access. Selecting Enabled or Enabled(Scan) enables wireless bridge restriction. Only those bridges selected in Remote Bridges will be granted access. Click "Refresh" to update the remote bridges. Wait for few seconds to update. Click "Save/Apply" to configure the wireless bridge options.'

Below the text are three configuration fields:

- AP Mode: A dropdown menu with 'Fi ii' selected.
- Bridge Restrict: A dropdown menu with 'Disabled' selected.
- Remote Bridges MAC Address: Two empty text input boxes.

At the bottom of the configuration area are two buttons: 'Refresh' and 'Save/Apply'.

Wireless – Advanced

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.

- = **Band:** Select 802.11b/g using wireless frequency band range. The radio frequency remains at 2.437 GHz.
- = **Channel:** Fill in the appropriate channel to correspond with your network settings. 11 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

Web Configuration

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.
- = **XPress™ Technology:** Select Enable or Disable. This is a special accelerating technology for IEEE802.11g. The default 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 **Save/Apply** to configure the advanced wireless options and make the changes take effect.

Wireless -- Authenticated Stations

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

MAC	Associated	Authorized	SSID	Interface
00:1C:26:89:5F:6D	Yes		Broadcom	wl0

Refresh

Diagnostics

Click **Diagnostics** to show the interface.

Your modem is capable of testing your DSL connection. The individual tests are listed below. If a test displays a fail status, click **Rerun Diagnostic 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.

The screenshot shows the 'Diagnostics' page for a D-Link DSL-2640B. On the left is a navigation menu with 'Diagnostics' highlighted. The main content area is titled 'br_0_0_35 Diagnostics' and contains the following text: 'Your modem is capable of testing your DSL connection. The individual tests are listed below. If a test displays a fail status, click "Rerun Diagnostic 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.'

Under the heading 'Test the connection to your local network', there are two test results:

Test your EME(1-4) Connection:	PASS	Help
Test your Wireless Connection:	PASS	Help

Under the heading 'Test the connection to your DSL service provider', there are three test results:

Test ADSL Synchronization:	FAIL	Help
Test ATM OAM F5 segment ping:	FAIL	Help
Test ATM OAM F5 end-to-end ping:	FAIL	Help

At the bottom of the page, there are two buttons: 'Rerun Diagnostic Tests' and 'Test With OAM P4'.

Management

Settings

Settings Backup

Click **Settings > Backup** to back up the DSL router configuration.

The screenshot shows the 'Settings - Backup' page. On the left is a navigation menu with 'Backup' highlighted. The main content area is titled 'Settings - Backup' and contains the text: 'Backup DSL router configurations. You may save your router configurations as a file on your PC.'

At the bottom of the page, there is a single button labeled 'Backup Settings'.

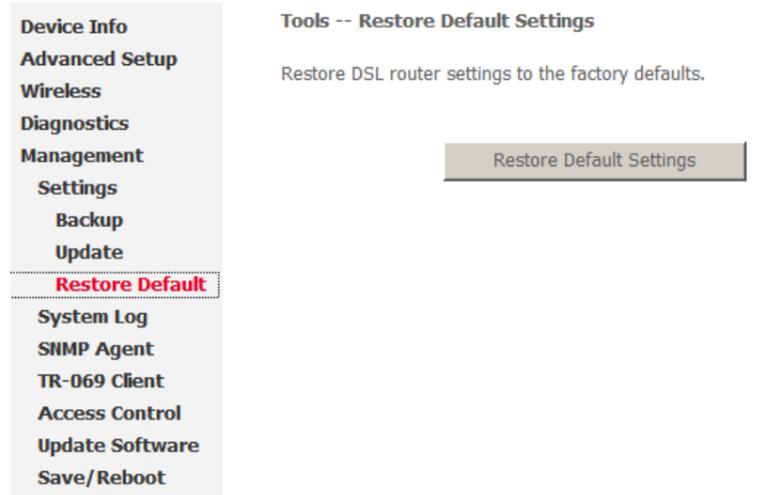
Web Configuration
Settings Update

Click **Browse** and select the correct update configure settings file. Then, click **Update Settings** to update the modem settings.



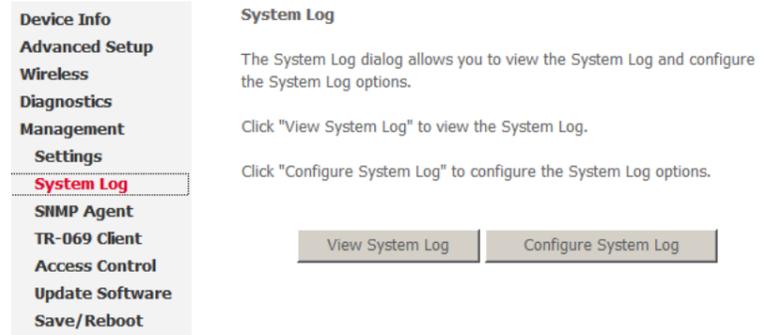
Settings Restore Default

Click **Restore Default Settings** to restore DSL router settings to the factory defaults.



System Log

Click **System Log** to show the following interface. 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.



TR-069 Client

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

The screenshot shows a web configuration page for the TR-069 Client. On the left is a vertical navigation menu with the following items: Device Info, Advanced Setup, Wireless, Diagnostics, Management, Settings (highlighted), System Log, SNMP Agent, TR-069 Client, Access Control, Update Software, and Save/Reboot. The main content area is titled "TR-069 client - Configuration". It contains the following text and controls:

- WAN Management Protocol (TR-069) allows a Auto-Configuration Server (ACS) to perform auto-configuration, provision, collection, and diagnostics to this device.
- Select the desired values and click "Apply" to configure the TR-069 client options.
- TR69c Status: Disable Enable
- Inform : Disable Enable
- Inform Interval:
- ACS URL:
- ACS User Name:
- ACS Password:
- Display SOAP messages on serial console: Disable Enable
- Connection Request Authentication
- Connection Request User Name:
- Connection Request Password:
- Buttons: Save/Apply, GetRPCMethods

Internet Time

Note: When the PVC is PPPoE connection, the **Internet Time** appears in the Management directory.

Click **Internet Time** to show the following page. In this page, the modem can synchronize with Internet time servers.

The screenshot shows a web configuration page for Internet Time. On the left is a vertical navigation menu with the following items: Device Info, Advanced Setup, Wireless, Diagnostics, Management, Settings, System Log, SNMP Agent, TR-069 Client, Internet Time (highlighted), Access Control, Update Software, and Save/Reboot. The main content area is titled "Time settings". It contains the following text and controls:

- This page allows you to the modem's time configuration.
- Automatically synchronize with Internet time servers
- Button: Save/Apply

Web Configuration

After enable **Automatically synchronize with Internet time servers**, the interface show below. Enter proper configurations and click **Save/Apply**.

Time settings

This page allows you to the modem's time configuration.

Automatically synchronize with Internet time servers

First NTP time server:

Second NTP time server:

Time zone offset:

Access Control

Access Control – Services

Click **Access Control > Services** to show the following interface. In the interface, you can enable or disable HTTP, ICMP, SSH, TELNET and TFTP 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.

Device Info
Advanced Setup
Wireless
Diagnostics
Management
Settings
System Log
SNMP Agent
TR-069 Client
Access Control
Services
IP Addresses
Passwords
Update Software
Save/Reboot

Access Control -- Services

A Service Control List ("SCL") enables or disables services from being used.

Services	LAN
FTP	<input checked="" type="checkbox"/> Enable
HTTP	<input checked="" type="checkbox"/> Enable
ICMP	Enable
SNMP	<input checked="" type="checkbox"/> Enable
SSH	<input checked="" type="checkbox"/> Enable
TELNET	<input checked="" type="checkbox"/> Enable
TFTP	<input checked="" type="checkbox"/> Enable

Access Control -- IP Addresses

Click **Access Control > IP Addresses** to show the following interface.

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 **Save/Apply**.

The screenshot shows a web configuration page. On the left is a vertical navigation menu with items: Device Info, Advanced Setup, Wireless, Diagnostics, Management, Settings, System Log, SNMP Agent, TR-069 Client, Access Control, Services, IP Addresses (highlighted with a red dashed box), Passwords, Update Software, and Save/Reboot. The main content area is titled 'Access Control -- IP Address' and contains a descriptive paragraph: 'The IP Address Access Control mode, 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 will not validate IP addresses for incoming packets. The services are the system applications listed in the Service Control List.' Below this text are two radio buttons for 'Access Control Mode': 'Disable' (selected) and 'Enable'. At the bottom of the main area are two buttons: 'IP Address' and 'Remove'.

Access Control

Enter the IP address of the management station permitted to access the local management services, and click 'Save/Apply.'

IP Address:

Access Control – Passwords

Click **Access Control > Passwords** to show the following interface. In the interface, you can modify the accounts passwords.

Access Control - Passwords

Access to your DSL router is controlled through three user accounts: admin, support, and user.

The user name "admin" has unrestricted access to change and view configuration of your DSL Router.

The user name "support" is used to allow an ISP technician to access your DSL Router for maintenance and to run diagnostics.

The user name "user" can access the DSL Router, view configuration settings and statistics, as well as, update the router's software.

Use the fields below to enter up to 16 characters and click "Apply" to change or create passwords. Note: Password cannot contain a space.

Username:

Old Password:

New Password:

Confirm Password:

Update Software

Click **Update Firmware** to show the following interface. In this interface, you can update the modem firmware. Click **Browse** to find the right version file and click **Update Firmware** 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 modem to the factory defaults and configure it again.

Tools - Update Software

Step 1: Obtain an updated software image file from your ISP.

Step 2: Enter the path to the image file location in the box below or click the "Browse" button to locate the image file.

Step 3: Click the "Update Software" button once you upload the new image file.

NOTE: The update process takes about 2 minutes to complete, and your DSL Router will reboot.

Software File Name:

Save/Reboot

Click **Save/Reboot** to show the following interface. Click **Save/Reboot** to save and reboot the router.

- Device Info
- Advanced Setup
- Wireless
- Diagnostics
- Management
- Settings
- System Log
- SNMP Agent
- TR-069 Client
- Access Control
- Update Software
- Save/Reboot**

Click the button below to save and reboot the router.

Save/Reboot

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://10.1.1.1> .
- = The default username is 'admin' and the default password is 'admin'.
- = 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 'admin'.

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.

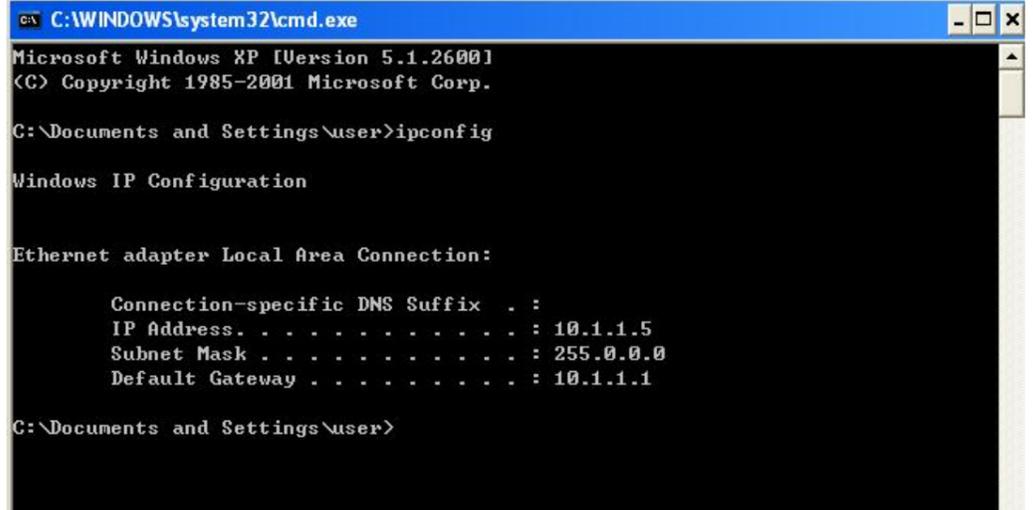
Click **Start > Run**. In the run box type "**cmd**" and click **OK**.

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.

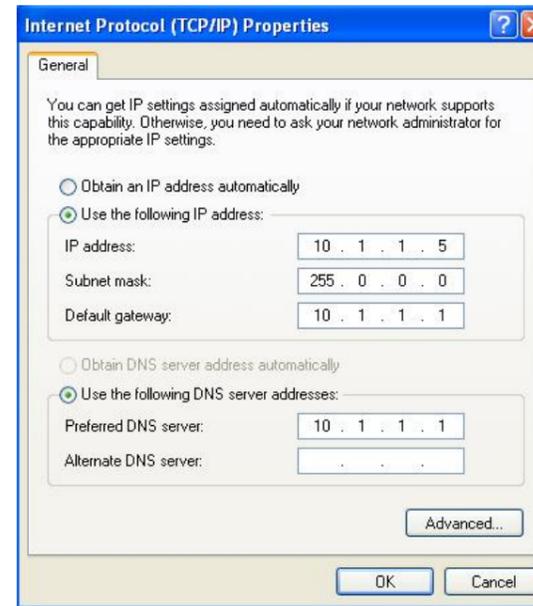
Example: If the router's LAN IP address is **10.1.1.1**, make your IP address 10.1.1.X where X is a number between 2 and 254.

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 (10.1.1.1).

Set Primary DNS the same as the LAN IP address of your router (10.1.1.1). 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:** 10.1.1.1, **Netmask:** 255.0.0.0, **User Name:** admin, **Password:** admin
DHCP Server: Enabled