

USER MANUAL

DSL-2640B

VERSION 2.0



Federal Communication Commission Interference Statement

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

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

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

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

IMPORTANT NOTE:

FCC Radiation Exposure Statement:

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

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

Table of Contents

<i>Before You Begin</i>	1	<i>Port Forwarding</i>	39
Package Contents	1	<i>Port Triggering</i>	41
System Requirements	1	<i>DMZ</i>	43
Features	2	<i>Parental Control</i>	43
HARDWARE OVERVIEW	3	Block Website	44
<i>Connections</i>	3	Block MAC Address	45
<i>LED Indicators</i>	4	<i>Filtering Options</i>	47
INSTALLATION	5	Inbound IP Filtering	47
Mounting the Device on the Wall	5	Outbound IP Filtering	49
Installation Notes	6	Bridge Filtering	51
<i>Information you will need from your ADSL service provider</i>	8	<i>Firewall Settings</i>	53
<i>Information you will need about DSL-2640B</i>	9	<i>DNS</i>	54
<i>Information you will need about your LAN or computer:</i>	9	<i>Dynamic DNS</i>	55
Device Installation	10	<i>Network Tools</i>	56
<i>Power on Router</i>	10	Port Mapping	57
<i>Factory Reset Button</i>	10	IGMP Snooping	60
<i>Network Connections</i>	11	Queue Configuration	60
INTRODUCTION TO WEB CONFIGURATION	12	Quality of Service	61
Preparation Before Login	12	UPnP	63
Logging In to the Modem	13	ADSL Settings	63
<i>First-Time Login</i>	13	SNMP	64
SETUP	15	TR-069	65
<i>Wizard</i>	15	Certificates	66
<i>Internet Setup</i>	24	<i>Routing</i>	66
<i>Wireless Settings</i>	26	Static Route	67
Wireless Basics	26	Default Gateway	68
Wireless Security	27	RIP	68
<i>Local Network</i>	30	<i>Schedules</i>	69
<i>Time and Date</i>	32	MAINTENANCE	70
<i>Logout</i>	32	<i>System</i>	70
Advanced Configuration	33	<i>Firmware Update</i>	71
<i>Advanced Wireless</i>	33	<i>Access Controls</i>	72
Advanced Settings	34	Account Password	73
MAC Filtering	35	Services	74
Security Settings	36	IP Address	75
		<i>Diagnostics</i>	76

<i>System Log</i>	77
Status	78
<i>Device Information</i>	79
<i>Wireless Clients</i>	80
<i>DHCP Clients</i>	81
<i>Logs</i>	81
<i>Statistics</i>	82
<i>Route information</i>	83
TROUBLESHOOTING	84
NETWORKING BASICS	85
Check Your IP Address	85
Statically Assign An IP Address	86
TECHNICAL SPECIFICATIONS	87

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

Package Contents

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



System Requirements

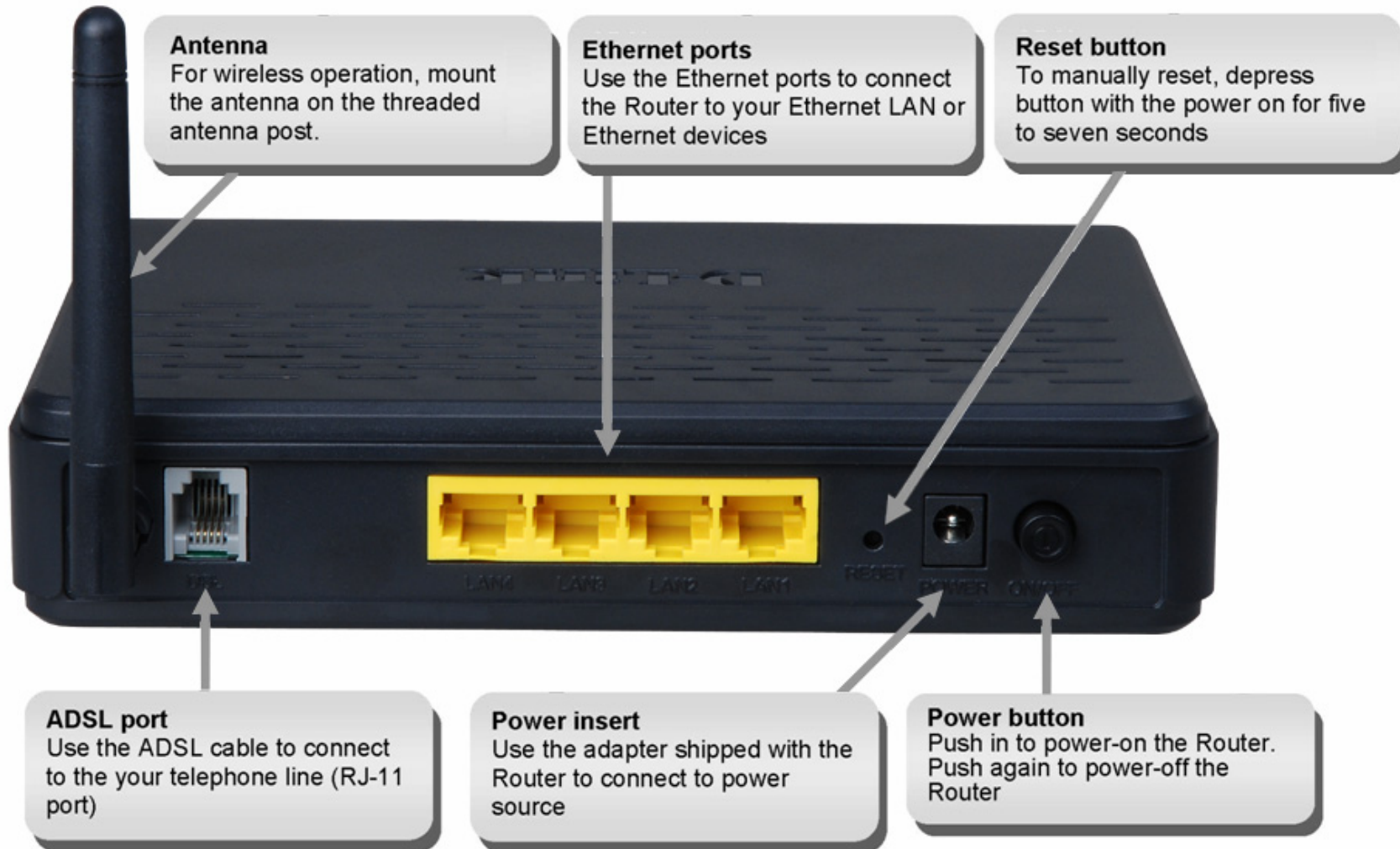
- ADSL Internet service
- Computer with:
 - 200 MHz Processor
 - 64MB Memory
 - CD-ROM Drive
 - Ethernet Adapter with TCP/IP Protocol Installed
 - Internet Explorer v6 or later, FireFox v1.5
 - Computer with Windows 2000, Windows XP, or Windows Vista

Features

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

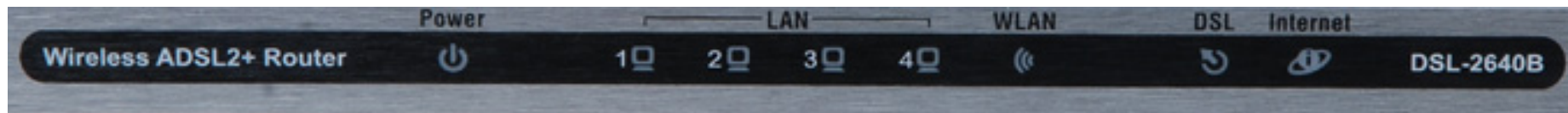
Hardware Overview

Connections



LED Indicators

Front Panel



Side Panel



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

Installation

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

Mounting the Device on the Wall

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

See the following figure:



Installation Notes

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

Low Pass Filters

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

Operating Systems

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

Web Browser

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

Ethernet Port (NIC Adapter)

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

Additional Software

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

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

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

Installation

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 192.168.1.1. This may be changed to suit any IP address scheme the user desires. This address will be the base IP address used for DHCP service on the LAN when DHCP is enabled.

LAN Subnet Mask for the DSL-2640B

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

Information you will need about your LAN or computer:

Ethernet NIC

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

DHCP Client status

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

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

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

Device Installation

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

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

Power on Router

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

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

Factory Reset Button

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

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

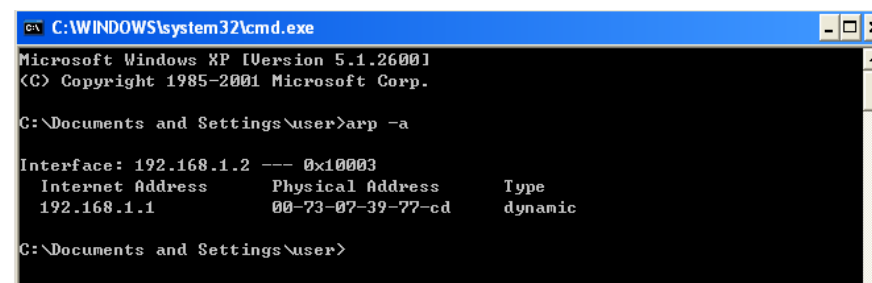
Introduction to Web Configuration

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 192.168.1.X (2~254), net mask as 255.255.255.0, gateway address as 192.168.1.1 (for customized version, configure them according to the actual version).
- Enter **arp -a** in the DOS window to check whether the PC can read the MAC address of the Modem.
- Ping the MAINTENANCE IP address (192.168.1.1 by default) of the Modem.
If the PC can read the MAC address of the Modem and can ping through the MAINTENANCE IP address of the Modem, that means the communication of the PC and the Modem is normal.

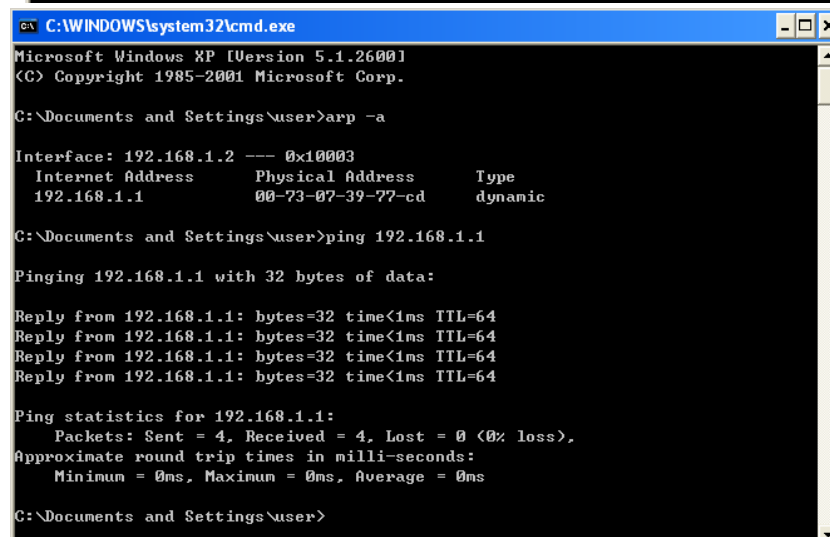


```
C:\WINDOWS\system32\cmd.exe
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

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

Interface: 192.168.1.2 --- 0x10003
Internet Address      Physical Address      Type
192.168.1.1          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: 192.168.1.2 --- 0x10003
Internet Address      Physical Address      Type
192.168.1.1          00-73-07-39-77-cd    dynamic

C:\Documents and Settings\user>ping 192.168.1.1

Pinging 192.168.1.1 with 32 bytes of data:

Reply from 192.168.1.1: bytes=32 time<1ms TTL=64
Reply from 192.168.1.1: bytes=32 time<1ms TTL=64
Reply from 192.168.1.1: bytes=32 time<1ms TTL=64
Reply from 192.168.1.1: bytes=32 time<1ms TTL=64

Ping statistics for 192.168.1.1:
    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.

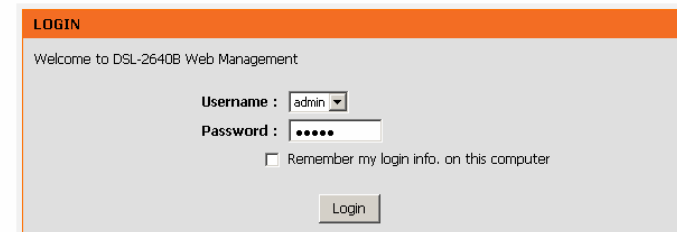
Logging In to the Modem

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.

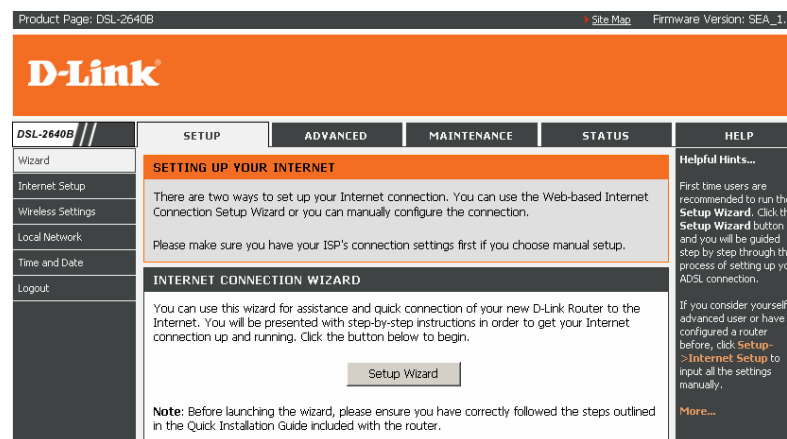
- Step 1** Open a Web browser on your computer.
- Step 2** Enter **http://192.168.1.1** (DSL router default IP address) in the address bar. The login page appears.
- Step 3** Enter a user name and the password. The default username and password of the super user are **admin** and **admin**. The username 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 **Login** to log in.



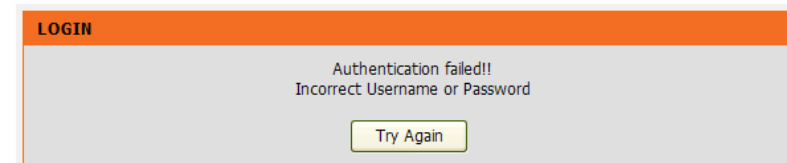
After logging in to the DSL router as a super user, you can query, configure, and modify all configurations, and diagnose the system.

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.

If you log in as the super user successfully, the page shown in the figure appears.



If the login information is incorrect, the page shown in the figure appears. Click **Try Again** to log in again.



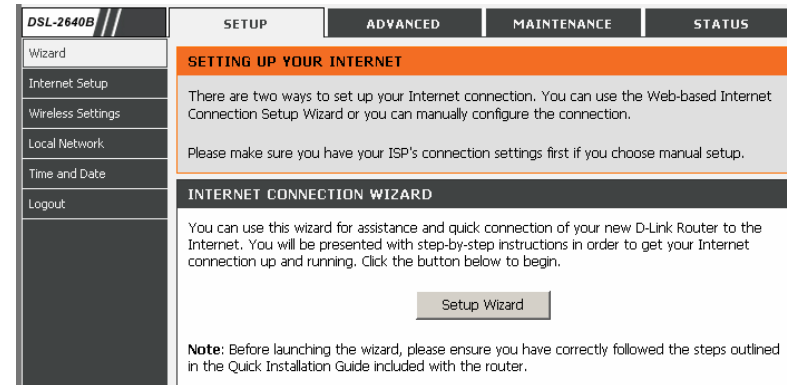
SETUP

Wizard

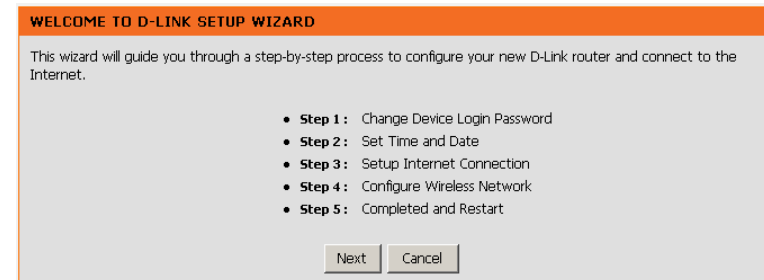
Wizard enables fast and accurate configuration of Internet connection and other important parameters. The following sections describe these various configuration parameters.

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 about the properties of your Internet connection is provided by your Internet service provider (ISP). For example, your ISP should inform you whether you are connected to the Internet using a static or dynamic IP address, or the protocol, such as PPPoA or PPPoE, that you use to communicate over the Internet.

Choose **Setup > Wizard**. The page shown in the figure appears.



Click **Setup Wizard**. The page shown in the figure appears.



Web Configuration

There are four steps to configure the device. Click **Next** to continue.

Change the password for logging in to the device.

The default password is **admin**. To secure your network, modify the password timely.

Note:

Confirm password must be the same as the new password.

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

STEP 1: CHANGE DEVICE LOGIN PASSWORD → 2 → 3 → 4 → 5

The factory default password of this router is admin. To help secure your network, D-Link recommends that you should choose a new password. If you do not wish to choose a new password now, just click "Skip" to continue. Click "Next" to proceed to next step.

Current Password :

New Password :

Confirm Password :

Set the time and date.

Configure the Internet connection.

Select the country and ISP. Set the VPI and VCI. If you fail to find the country and ISP from the drop-down lists, select **Others**.

1 → STEP 2: SET TIME AND DATE → 3 → 4 → 5

The Time Configuration option allows you to configure, update, and maintain the correct time on the internal system clock. From this section you can set the time zone that you are in and set the NTP (Network Time Protocol) Server. Daylight Saving can also be configured to automatically adjust the time when needed.

TIME SETTINGS

Automatically synchronize with Internet time servers

First NTP time server : ntp1.dlink.com

Second NTP time server : None

TIME CONFIGURATION

Current Router Time : Sat Jan 1 01:47:33 2000

Time Zone : (GMT-12:00) International Date Line West

Enable Daylight Saving

Daylight Saving Offset : -2:00

Daylight Saving Dates : Start Month Week Day Time
Jan 1st Sun 12 am

End Month Week Day Time
Jan 1st Sun 12 am

Back Next Cancel

1 → 2 → STEP 3: SETUP INTERNET CONNECTION → 4 → 5

Please select your Country and ISP (Internet Service Provider) from the list below. If your Country or ISP is not in the list, please select "Others".

Country : (Click to Select)

Internet Service Provider : (Click to Select)

Protocol : (Click to Select)

Connection Type : (Click to Select)

VPI : (Enter a number) (0-255)

VCI : (Enter a number) (32-65535)

Enable DSL Auto-scan

Back Next Cancel

If the **Protocol** is **PPPoE** or **PPPoA**, the page shown in either of the two figures appears.

1 → 2 → STEP 3: SETUP INTERNET CONNECTION → 4 → 5

Please select your Country and ISP (Internet Service Provider) from the list below. If your Country or ISP is not in the list, please select "Others".

Country :

Internet Service Provider :

Protocol :

Connection Type :

VPI : (0-255)

VCI : (32-65535)

Enable DSL Auto-scan

PPPoE

Please enter your Username and Password as provided by your ISP (Internet Service Provider). Please enter the information exactly as shown taking note of upper and lower cases. Click "Next" to continue.

Username :

Password :

Confirm Password :

Set the user name and password as provided by your ISP.

1 → 2 → **STEP 3: SETUP INTERNET CONNECTION** → 4 → 5

Please select your Country and ISP (Internet Service Provider) from the list below. If your Country or ISP is not in the list, please select "Others".

Country :

Internet Service Provider :

Protocol :

Connection Type :

VPI : (0-255)

VCI : (32-65535)

Enable DSL Auto-scan

PPPoA

Please enter your Username and Password as provided by your ISP (Internet Service Provider). Please enter the information exactly as shown taking note of upper and lower cases. Click "Next" to continue.

Username :

Password :

Confirm Password :

If the **Protocol** is **Static IP**, the page shown in the figure appears.
Enter the **IP Address**, **Subnet Mask**, **Default Gateway**, and **Primary DNS Server**.

1 → 2 → STEP 3: SETUP INTERNET CONNECTION → 4 → 5

Please select your Country and ISP (Internet Service Provider) from the list below. If your Country or ISP is not in the list, please select "Others".

Country : Others
Internet Service Provider : Others
Protocol : Static IP
Connection Type : (Click to Select)
VPI : (Enter a number) (0-255)
VCI : (Enter a number) (32-65535)

Enable DSL Auto-scan

STATIC IP

You have selected Static IP Internet connection. Please enter the appropriate information below as provided by your ISP.

The Auto PVC Scan feature will not work in all cases so please enter the VPI/VCI numbers if provided by the ISP.

Click Next to continue.

IP Address : 0.0.0.0
Subnet Mask : 0.0.0.0
Default Gateway : 0.0.0.0
Primary DNS Server : 192.168.1.1

Back Next Cancel

If the **Protocol** is **Dynamic IP** or **Bridge**, the page shown in the figure appears.

1 → 2 → STEP 3: SETUP INTERNET CONNECTION → 4 → 5

Please select your Country and ISP (Internet Service Provider) from the list below. If your Country or ISP is not in the list, please select "Others".

Country : Others
Internet Service Provider : Others
Protocol : Dynamic IP
Connection Type : (Click to Select)
VPI : (Enter a number) (0-255)
VCI : (Enter a number) (32-65535)

Enable DSL Auto-scan

Back Next Cancel

Web Configuration

After proper configuration, click **Next**.

1 → 2 → **STEP 3: SETUP INTERNET CONNECTION** → 4 → 5

Please select your Country and ISP (Internet Service Provider) from the list below. If your Country or ISP is not in the list, please select "Others".

Country :

Internet Service Provider :

Protocol :

Connection Type :

VPI : (0-255)

VCI : (32-65535)

Enable DSL Auto-scan

Configure the wireless network. Enter the information and click **Next**.

1 → 2 → 3 → **STEP 4: CONFIGURE WIRELESS NETWORK** → 5

Your wireless network is enabled by default. You can simply uncheck it to disable it and click "Next" to skip configuration of wireless network.

Enable Your Wireless Network

Your wireless network needs a name so it can be easily recognized by wireless clients. For security purposes, it is highly recommended to change the pre-configured network name.

Wireless Network Name (SSID) : (1~32 characters)

Select "Visible" to publish your wireless network and SSID can be found by wireless clients, or select "Invisible" to hide your wireless network so that users need to manually enter SSID in order to connect to your wireless network.

Visibility Status : Visible Invisible

In order to protect your network from hackers and unauthorized users, it is highly recommended you choose one of the following wireless network security settings.

None	Security Level		Best
<input type="radio"/> None	<input type="radio"/> WEP	<input checked="" type="radio"/> WPA-PSK	<input type="radio"/> WPA2-PSK

Security Mode: WPA-PSK
Select this option if your wireless adapters support WPA-PSK.

Now, please enter your wireless security key.

WPA Pre-Shared Key :
(8-63 characters, such as a~z, A~Z, or 0~9, i.e. **'%Fortress123&'**)

Note: You will need to enter the same key here into your wireless clients in order to enable proper wireless connection.

The page shown in the right figure appears. In this page, you can view the configuration information.

1 → 2 → 3 → 4 **STEP 5: COMPLETED AND RESTART**

Setup complete. Click "Back" to review or modify settings. Click "Restart" to apply current settings and reboot the DSL-2640B router.

If your Internet connection does not work after restart, you can try the Setup Wizard again with alternative settings or use Manual Setup instead if you have your Internet connection details as provided by your ISP.

SETUP SUMMARY

Below is a detailed summary of your settings. Please print this page out, or write the information on a piece of paper, so you can configure the correct settings on your wireless client adapters.

Time Settings :	Disabled
VPI / VCI :	0 / 32
Protocol :	PPPoE
Connection Type :	LLC
Username :	tinet
Password :	tinet
Wireless Network Name (SSID) :	Dlink
Visibility Status :	Visible
Encryption :	WPA-PSK/TKIP (also known as WPA Personal)
Pre-Shared Key :	%Fortress123&

Back Restart Cancel

When the settings are complete, click **Restart** to apply the settings and reboot the device.

Note:

In each step of the Wizard page, you can click **Back** to review or modify the previous settings. Click **Cancel** to exit the wizard page.

DSL ROUTER REBOOT

The DSL Router has been configured and is rebooting. Please wait...
If necessary, reconfigure your PC's IP address to match your new configuration after reboot finishes.

||||||| 9%

Internet Setup

Choose **SETUP** > **Internet Setup**. The page as shown in the figure appears:

INTERNET SETUP

Choose "Add", "Edit", or "Delete" to configure WAN interfaces.
Choose "Finish" to apply the changes and reboot the system.

WAN SETUP

VPI/VCI	VLAN Mux	Con. ID	Service Name	Protocol	IGMP	QoS	State	Status	Action
0/32	Off	1	wizard_pvc	PPPoE	Disabled	Disabled	Enabled	Link Down	Up

Add Edit Delete Finish

Web Configuration

In this page, you can configure the WAN interface of the device.

Click **Add** and the page as shown in the figure appears:

The table describes the parameters in this page.

Field	Description
ATM PVC CONFIGURATION	
VPI	Virtual Path Identifier (VPI) is the virtual path between two points in an ATM network. Its value range is from 0 to 255.
VCI	Virtual Channel Identifier (VCI) is the virtual channel between two points in an ATM network. Its value range is from 32 to 65535 (0 to 31 is reserved for local MAINTENANCE of ATM traffic).
Service Category	Select UBR with PCR , UBR without PCR , CBR , Non Realtime VBR , or Realtime VBR from the drop-down list.
Peak Cell Rate	Set the maximum transmission rate of the cell in ATM transmission.
Sustainable Cell Rate	Set the minimum transmission rate of the cell in ATM transmission.
Maximum Burst Size	Set the maximum burst size of the cell in ATM transmission.
CONNECTION TYPE	
Protocol	Select PPP over ATM (PPPoA) , PPP over Ethernet (PPPoE) , MAC Encryption Routing (MER) , IP over ATM , or Bridging from the drop-down list.
Encapsulation Mode	Select LLC or VCMUX from the drop-down list. Usually, you can select LLC .
BRIDGE SETTINGS	
Enable Bridge Service	Select or deselect the check box to enable or disable the WAN connection.
Service Name	The name to identify the WAN connection. You need not modify it.

INTERNET SETUP

This screen allows you to configure an ATM PVC identifier (VPI and VCI) and select a service category.

ATM PVC CONFIGURATION

VPI: (0-255)

VCI: (32-65535)

Service Category:

Peak Cell Rate: (cells/s)

Sustainable Cell Rate: (cells/s)

Maximum Burst Size: (cells)

Enable Quality Of Service:

CONNECTION TYPE

Protocol:

Encapsulation Mode:

Enable Multiple Protocols Over A Single PVC:

802.1Q VLAN ID: (0-4095)

BRIDGE SETTINGS

Enable Bridge Service:

Service Name:

Wireless Settings

This section describes the wireless LAN and some basic configuration. Wireless LANs 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 which bridge network traffic to wired LAN.

Choose **Setup > Wireless Settings**. The **Wireless Settings** page shown in the right figure appears.

SETUP ADVANCED MAINTENANCE STATUS

WIRELESS SETTINGS -- WIRELESS BASICS

Configure your wireless basic settings.

Wireless Basics

WIRELESS SETTINGS -- WIRELESS SECURITY

Configure your wireless security settings.

Wireless security

Wireless Basics

In the **Wireless Settings** page, click **Wireless Basics**. The page shown in the right figure appears. In this page, you can configure the parameters of wireless LAN clients that may connect to the device.

The wireless channel is from 1 to 11.

You can select the 802.11 mode from the drop-down list.

Mixed 802.11g and 802.11b ▼

802.11g only

Mixed 802.11g and 802.11b

802.11b only

WIRELESS BASICS

Use this section to configure the wireless settings for your D-Link router. Please note that changes made in this section will also need to be duplicated to your wireless clients and PC.

WIRELESS NETWORK SETTINGS

Enable Wireless

Wireless Network Name (SSID) :

Visibility Status : Visible Invisible

Country :

Wireless Channel : (Current: CH 1)

802.11 Mode :

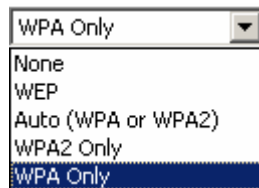
Please take note of your SSID as you will need to duplicate the same settings to your wireless devices and PC.

Apply Cancel

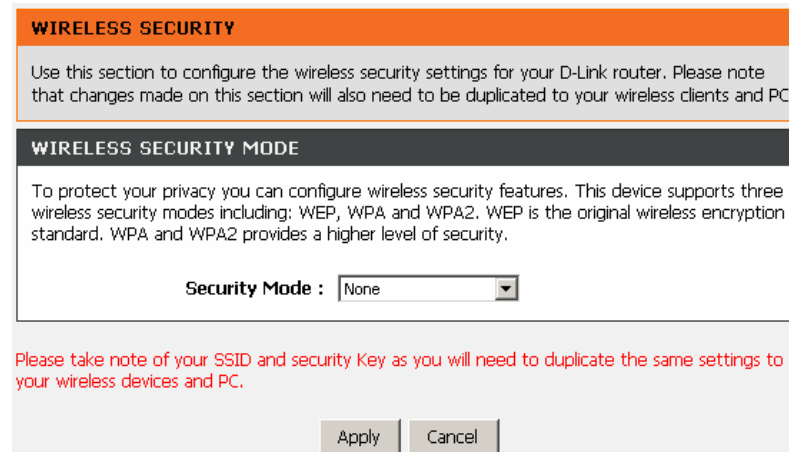
Wireless Security

In the **Wireless Settings** page, click **Wireless Security**. The page shown in the right figure appears. Wireless security is vital to your network to protect the wireless communication among wireless stations, access points and wired network.

You can select the security mode from the drop-down list.



A screenshot of a web browser's drop-down menu. The menu is open, showing several options: 'WPA Only' (selected), 'None', 'WEP', 'Auto (WPA or WPA2)', 'WPA2 Only', and 'WPA Only' (highlighted in blue at the bottom).



The screenshot shows the 'Wireless Security' configuration page. At the top, there is an orange header with the text 'WIRELESS SECURITY'. Below this is a grey box containing the instruction: 'Use this section to configure the wireless security settings for your D-Link router. Please note that changes made on this section will also need to be duplicated to your wireless clients and PC.' Below this is a dark grey header with the text 'WIRELESS SECURITY MODE'. Underneath is a white box with the text: 'To protect your privacy you can configure wireless security features. This device supports three wireless security modes including: WEP, WPA and WPA2. WEP is the original wireless encryption standard. WPA and WPA2 provides a higher level of security.' Below this text is a label 'Security Mode :' followed by a drop-down menu currently set to 'None'. At the bottom of the page, there is a red warning message: 'Please take note of your SSID and security Key as you will need to duplicate the same settings to your wireless devices and PC.' and two buttons labeled 'Apply' and 'Cancel'.

Web Configuration

If you select WEP as the security mode, the right page appears.

WIRELESS SECURITY MODE

To protect your privacy you can configure wireless security features. This device supports three wireless security modes including: WEP, WPA and WPA2. WEP is the original wireless encryption standard. WPA and WPA2 provides a higher level of security.

Security Mode :

WEP

If you choose the WEP security option this device will **ONLY** operate in **Legacy Wireless mode (802.11B/G)**.

WEP is the wireless encryption standard. To use it you must enter the same key(s) into the router and the wireless stations. For 64 bit keys you must enter 10 hex digits into each key box. For 128 bit keys you must enter 26 hex digits into each key box. A hex digit is either a number from 0 to 9 or a letter from A to F. For the most secure use of WEP set the authentication type to "Shared Key" when WEP is enabled.

You may also enter any text string into a WEP key box, in which case it will be converted into a hexadecimal key using the ASCII values of the characters. A maximum of 5 text characters can be entered for 64 bit keys, and a maximum of 13 characters for 128 bit keys.

WEP Key Length : (length applies to all keys)

WEP Key 1 :

WEP Key 2 :

WEP Key 3 :

WEP Key 4 :

Authentication :

Please take note of your SSID and security Key as you will need to duplicate the same settings to your wireless devices and PC.

Web Configuration

If you select the **Auto (WPA or WPA2)**, **WPA**, or **WPA2** as the security mode, the right page appears.

WIRELESS SECURITY MODE

To protect your privacy you can configure wireless security features. This device supports three wireless security modes including: WEP, WPA and WPA2. WEP is the original wireless encryption standard. WPA and WPA2 provides a higher level of security.

Security Mode :

WPA

Use **WPA or WPA2** mode to achieve a balance of strong security and best compatibility. This mode uses WPA for legacy clients while maintaining higher security with stations that are WPA2 capable. Also the strongest cipher that the client supports will be used. For best security, use **WPA2 Only** mode. This mode uses AES(CCMP) cipher and legacy stations are not allowed access with WPA security. For maximum compatibility, use **WPA Only**. This mode uses TKIP cipher. Some gaming and legacy devices work only in this mode.

To achieve better wireless performance use **WPA2 Only** security mode (or in other words AES cipher).

Auto(WPA or WPA2) uses TKIP+AES cipher .

WPA-PSK does not require an authentication server. The WPA option requires an external RADIUS server.

WPA Mode :

Group Key Update Interval : (seconds)

PRE-SHARED KEY

Pre-Shared Key :

Please take note of your SSID and security Key as you will need to duplicate the same settings to your wireless devices and PC.

Local Network

You can configure the LAN IP address according to the actual application. The preset IP address is 192.168.1.1. You can use the default settings and DHCP service to manage the IP settings for the private network. The IP address of the device is the base address used for DHCP. To use the device for DHCP on your LAN, the IP address pool used for DHCP must be compatible with the IP address of the device. The IP address available in the DHCP IP address pool changes automatically if you change the IP address of the device.

You can also enable the secondary LAN IP address. The two LAN IP addresses must be in different networks.

Choose **Setup > Local Network**. The **Local Network** page shown in the figure appears.

LOCAL NETWORK

This section allows you to configure the local network settings of your router. Please note that this section is optional and you should not need to change any of the settings here to get your network up and running.

ROUTER SETTINGS

Use this section to configure the local network settings of your router. The Router IP Address that is configured here is the IP Address that you use to access the Web-based management interface. If you change the IP Address here, you may need to adjust your PC's network settings to access the network again.

Router IP Address :

Subnet Mask :

Configure the second IP Address and Subnet Mask for LAN interface

IP Address :

Subnet Mask :

DHCP SERVER SETTINGS (OPTIONAL)

Use this section to configure the built-in DHCP Server to assign IP addresses to the computers on your network.

Enable DHCP Server

DHCP IP Address Range : to

DHCP Lease Time : (hours)

By default, **Enable DHCP Server** is selected for the Ethernet LAN interface of the device. DHCP service supplies IP settings to workstations configured to automatically obtain IP settings that are connected to the device through the Ethernet port. When the device is used for DHCP, it becomes the default gateway for DHCP client connected to it. If you change the IP address of the device, you must also change the range of IP addresses in the pool used for DHCP on the LAN. The IP address pool can contain up to 253 IP addresses.

Click **Apply** to save the settings.

DHCP SERVER SETTINGS (OPTIONAL)

Use this section to configure the built-in DHCP Server to assign IP addresses to the computers on your network.

Enable DHCP Server

DHCP IP Address Range : to

DHCP Lease Time : (hours)

In the **Local Network** page, you can assign IP addresses on the LAN to specific individual computers based on their MAC addresses.

DHCP RESERVATIONS LIST

Status	Computer Name	MAC Address	IP Address
<input type="button" value="Add"/> <input type="button" value="Edit"/> <input type="button" value="Delete"/>			

Click **Add** to add static DHCP (optional). The page shown in the figure appears.

Select **Enable** to reserve the IP address for the designated PC with the configured MAC address.

The **Computer Name** helps you to recognize the PC with the MAC address. For example, Father's Laptop.

Click **Copy Your PC's MAC Address** to obtain the MAC address from the PC you are using.

Click **Apply** to save the settings.

After the DHCP reservation is saved, the DHCP reservations list displays the configuration. If the DHCP reservations list table is not empty, you can select one or more items and click **Edit** or **Delete**.

ADD DHCP RESERVATION (OPTIONAL)

Enable :

Computer Name :

IP Address :

MAC Address :

The **NUMBER OF DYNAMIC DHCP CLIENTS** page shows the current DHCP clients (PC or Laptop) connected to the device and the detailed information of the connected computer(s).

NUMBER OF DYNAMIC DHCP CLIENTS : 0

Computer Name	MAC Address	IP Address	Expire Time
---------------	-------------	------------	-------------

Time and Date

Choose **Setup > Time and Date**. The page shown in the figure appears.

In the **Time and Date** page, you can configure, update, and maintain the correct time on the internal system clock. You can set the time zone that you are in and the network time protocol (NTP) server. You can also configure daylight saving to automatically adjust the time when needed.

Select **Automatically synchronize with Internet time servers**.

Select the specific time server and the time zone from the corresponding drop-down lists.

Select **Enable Daylight Saving** if necessary. Select the proper **Daylight Saving Offset** from the drop-down list and set the daylight saving dates.

Click **Apply** to save the settings.

TIME AND DATE

The Time Configuration option allows you to configure, update, and maintain the correct time on the internal system clock. From this section you can set the time zone that you are in and set the NTP (Network Time Protocol) Server. Daylight Saving can also be configured to automatically adjust the time when needed.

TIME SETTINGS

Automatically synchronize with Internet time servers

First NTP time server : ntp1.dlink.com

Second NTP time server : None

TIME CONFIGURATION

Current Router Time : Sat Jan 1 00:30:56 2000

Time Zone : (GMT-12:00) International Date Line West

Enable Daylight Saving

Daylight Saving Offset : -2:00

Daylight Saving Dates : Start Month Week Day Time
End Month Week Day Time

Start Jan 1st Sun 12 am

End Jan 1st Sun 12 am

Apply Cancel

Logout

Choose **Setup > Logout**. The page shown in the figure appears. In this page, you can log out of the configuration page.

LOGOUT

Logging out will close the browser.

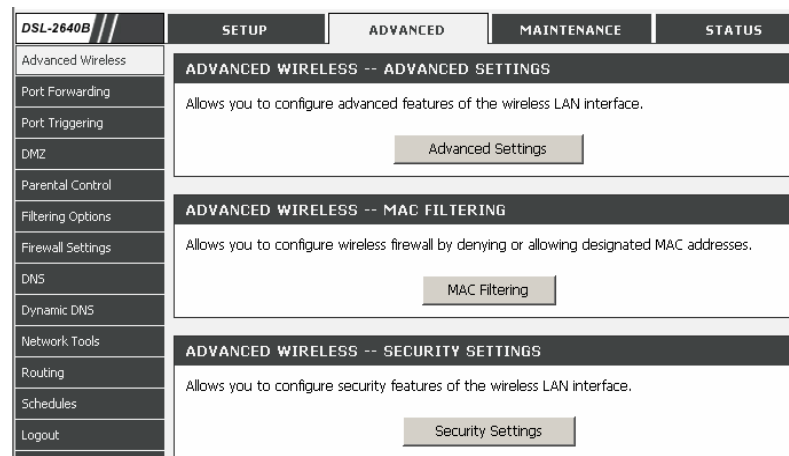
Logout

Advanced Configuration

This section contains advanced features used for network MAINTENANCE, security and administrative tools to manage the device. You can view the status and other information of the device, to examine the performance and troubleshoot.

Advanced Wireless

Choose **ADVANCED** > **Advanced Wireless**. The page shown in the right figure appears.



Advanced Settings

Select **Advance Settings**. The page shown in the following figure appears.
Click **Apply** to save the settings.

ADVANCED SETTINGS

These options are for users that wish to change the behaviour of their 802.11g wireless radio from the standard setting. D-Link does not recommend changing these settings from the factory default. Incorrect settings may impair the performance of your wireless radio. The default settings should provide the best wireless radio performance in most environments.

ADVANCED WIRELESS SETTINGS

Transmission Rate :	Auto	(20 ~ 65535)
Multicast Rate :	Auto	(20 ~ 65535)
Transmit Power :	100%	(20 ~ 65535)
Beacon Period :	100	(20 ~ 65535)
RTS Threshold :	2347	(0 ~ 2347)
Fragmentation Threshold :	2346	(256 ~ 2346)
DTIM Interval :	1	(1 ~ 255)
Preamble Type :	long	

SSID

Enable Wireless	<input checked="" type="checkbox"/>
Wireless Network Name (SSID) :	Dlink
Visibility Status :	<input checked="" type="radio"/> Visible <input type="radio"/> Invisible
User Isolation :	Off

Apply Cancel

MAC Filtering

Select **MAC Filtering**. The page shown in the right figure appears.

MAC FILTERING

Enter the MAC address and click "Apply" to add the MAC address to the wireless MAC address filters.

Wireless MAC Filtering Policy:

Enable Wireless MAC Filtering

Only **ALLOW** computers listed to access wireless network

Only **DENY** computers listed will be blocked to access wireless network

Apply Cancel

WIRELESS MAC FILTERING LIST

MAC Address	SSID
-------------	------

Add

Click **Add**. The page shown in the right figure appears.
Click **Apply** to save the settings.

MAC FILTERING

MAC Address :

SSID : Dlink ▾

Apply Cancel

Security Settings

Select **Security Settings**. The page shown in the right figure appears.

Select the SSID that you want to configure from the drop-down list.

Select the encryption type from the **Security Mode** drop-down list. You can select **None**, **WEP**, **AUTO (WPA or WPA2)**, **WPA Only**, or **WPA2 Only**.

SECURITY SETTINGS

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

WIRELESS SSID

Select SSID :

WIRELESS SECURITY MODE

To protect your privacy you can configure wireless security features. This device supports three wireless security modes including: WEP, WPA and WPA2. WEP is the original wireless encryption standard. WPA and WPA2 provides a higher level of security.

Security Mode :

WPA

Use **WPA or WPA2** mode to achieve a balance of strong security and best compatibility. This mode uses WPA for legacy clients while maintaining higher security with stations that are WPA2 capable. Also the strongest cipher that the client supports will be used. For best security, use **WPA2 Only** mode. This mode uses AES(CCMP) cipher and legacy stations are not allowed access with WPA security. For maximum compatibility, use **WPA Only**. This mode uses TKIP cipher. Some gaming and legacy devices work only in this mode.

To achieve better wireless performance use **WPA2 Only** security mode (or in other words AES cipher).

Auto(WPA or WPA2) uses TKIP+AES cipher .

WPA-PSK does not require an authentication server. The WPA option requires an external RADIUS server.

WPA Mode :

Group Key Update Interval : (seconds)

PRE-SHARED KEY

Pre-Shared Key :

Please take note of your SSID and security Key as you will need to duplicate the same settings to your wireless devices and PC.

If you select **WEP**, the page shown in the right figure appears.

WIRELESS SECURITY MODE

To protect your privacy you can configure wireless security features. This device supports three wireless security modes including: WEP, WPA and WPA2. WEP is the original wireless encryption standard. WPA and WPA2 provides a higher level of security.

Security Mode :

WEP

If you choose the WEP security option this device will **ONLY** operate in **Legacy Wireless mode (802.11B/G)**.

WEP is the wireless encryption standard. To use it you must enter the same key(s) into the router and the wireless stations. For 64 bit keys you must enter 10 hex digits into each key box. For 128 bit keys you must enter 26 hex digits into each key box. A hex digit is either a number from 0 to 9 or a letter from A to F. For the most secure use of WEP set the authentication type to "Shared Key" when WEP is enabled.

You may also enter any text string into a WEP key box, in which case it will be converted into a hexadecimal key using the ASCII values of the characters. A maximum of 5 text characters can be entered for 64 bit keys, and a maximum of 13 characters for 128 bit keys.

WEP Key Length : (length applies to all keys)

WEP Key 1 :

WEP Key 2 :

WEP Key 3 :

WEP Key 4 :

Authentication :

Please take note of your SSID and security Key as you will need to duplicate the same settings to your wireless devices and PC.

Web Configuration

If you select **AUTO (WPA or WPA2)**, **WPA Only**, or **WPA2 Only**, the page shown in the right figure appears.

Only the WPS button is effective in **WPA-PSK** mode.

Click **Apply** to save the settings.

WIRELESS SECURITY MODE

To protect your privacy you can configure wireless security features. This device supports three wireless security modes including: WEP, WPA and WPA2. WEP is the original wireless encryption standard. WPA and WPA2 provides a higher level of security.

Security Mode :

WPA

Use **WPA or WPA2** mode to achieve a balance of strong security and best compatibility. This mode uses WPA for legacy clients while maintaining higher security with stations that are WPA2 capable. Also the strongest cipher that the client supports will be used. For best security, use **WPA2 Only** mode. This mode uses AES(CCMP) cipher and legacy stations are not allowed access with WPA security. For maximum compatibility, use **WPA Only**. This mode uses TKIP cipher. Some gaming and legacy devices work only in this mode.

To achieve better wireless performance use **WPA2 Only** security mode (or in other words AES cipher).

Auto(WPA or WPA2) uses TKIP+AES cipher .

WPA-PSK does not require an authentication server. The WPA option requires an external RADIUS server.

WPA Mode :

Group Key Update Interval : (seconds)

PRE-SHARED KEY

Pre-Shared Key :

Please take note of your SSID and security Key as you will need to duplicate the same settings to your wireless devices and PC.

Port Forwarding

This function is used to open ports in your device and re-direct data through these ports to a single PC in your network (WAN-to-LAN traffic). It allows remote users to access services in your LAN, such as FTP for file transfers or SMTP, and POP3 for e-mail. The device receives remote requests for these services at your public IP address. It uses the specified TCP or UDP protocol and port, and redirects these requests to the server on your LAN with the specified LAN IP address. Note that the specified private IP address must be within the available IP address range of the subnet where the device is in.

Choose **ADVANCED > Port Forwarding**. The page as shown in the figure appears:

PORT FORWARDING

Port Forwarding allows you to direct incoming traffic from the WAN side (identified by protocol and external port) to the internal server with a 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 of 32 entries can be configured.

Select the service name, and enter the server IP address and click "Apply" to forward IP packets for this service to the specified server. **NOTE: The "Internal Port End" cannot be changed. It is the same as "External Port End" normally and will be the same as the "Internal Port Start" or "External Port End" if either one is modified.**

PORT FORWARDING SETUP

Server Name	External Port		Protocol	Internal Port		Server IP Address	Schedule Rule	Remote IP
	Start	End		Start	End			

Add

Click **Add** to add a virtual server. See the figure:

Select a service for a preset application or enter the name in the **Custom Server** field.

Enter an IP address in the **Server IP Address** field, to appoint the corresponding PC to receive forwarded packets.

The port table displays the ports that you want to open on the device. The **Protocol** indicates the type of protocol used by each port.

PORT FORWARDING SETUP

Remaining number of entries that can be configured: 32

Server Name :

Select a Service : (Click to Select)

Custom Server :

Schedule : Always [View Available Schedules](#)

Server IP Address : 192.168.1.

External Port Start	External Port End	Protocol	Internal Port Start	Internal Port End	Remote IP
<input type="text"/>	<input type="text"/>	TCP	<input type="text"/>	<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>	TCP	<input type="text"/>	<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>	TCP	<input type="text"/>	<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>	TCP	<input type="text"/>	<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>	TCP	<input type="text"/>	<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>	TCP	<input type="text"/>	<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>	TCP	<input type="text"/>	<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>	TCP	<input type="text"/>	<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>	TCP	<input type="text"/>	<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>	TCP	<input type="text"/>	<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>	TCP	<input type="text"/>	<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>	TCP	<input type="text"/>	<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>	TCP	<input type="text"/>	<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>	TCP	<input type="text"/>	<input type="text"/>	<input type="text"/>

Apply Cancel

Port Triggering

Some applications require that specific ports in the firewall of the device are open for the remote parties to access. Application rules dynamically open the firewall ports when an application on the LAN initiates a TCP/UDP connection to a remote party using the trigger ports. The device allows the remote party from the WAN side to establish new connections back to the application on the LAN side using the firewall ports. A maximum of 32 entries can be configured.

Choose **ADVANCED > Port Triggering**. The page shown in the right figure appears.

PORT TRIGGERING

Some applications require that specific ports in the Router's firewall be opened for access by the remote parties. Port Trigger dynamically opens up the "Open Ports" in the firewall when an application on the LAN initiates a TCP/UDP connection to a remote party using the "Triggering Ports". The Router allows the remote party from the WAN side to establish new connections back to the application on the LAN side using the "Open Ports".

Some applications such as games, video conferencing, remote access applications and others require that specific ports in the Router's firewall be opened for access by the applications. You can configure the port settings from this screen by selecting an existing application or creating your own (Custom application) and click "Apply" to add it.

A maximum of 32 entries can be configured.

PORT TRIGGERING

Application	Trigger		Open		Schedule Rule	
Name	Protocol	Port Range		Protocol	Port Range	
		Start	End		Start	End

Web Configuration

Click **Add**. The page shown in the following figure appears.

Select a name for the preset application, or enter a name in the **Custom application** field.

Enter the trigger port and select the **Trigger Protocol**.

Click **Apply** to save the settings.

PORT TRIGGERING

Remaining number of entries that can be configured :32

Application Name :

Select an application : (Click to Select) ▼

Custom application :

Schedule : Always ▼ [View Available Schedules](#)

Trigger Port Start	Trigger Port End	Trigger Protocol	Open Port Start	Open Port End	Open Protocol
<input type="text"/>	<input type="text"/>	TCP ▼	<input type="text"/>	<input type="text"/>	TCP ▼
<input type="text"/>	<input type="text"/>	TCP ▼	<input type="text"/>	<input type="text"/>	TCP ▼
<input type="text"/>	<input type="text"/>	TCP ▼	<input type="text"/>	<input type="text"/>	TCP ▼
<input type="text"/>	<input type="text"/>	TCP ▼	<input type="text"/>	<input type="text"/>	TCP ▼
<input type="text"/>	<input type="text"/>	TCP ▼	<input type="text"/>	<input type="text"/>	TCP ▼
<input type="text"/>	<input type="text"/>	TCP ▼	<input type="text"/>	<input type="text"/>	TCP ▼
<input type="text"/>	<input type="text"/>	TCP ▼	<input type="text"/>	<input type="text"/>	TCP ▼
<input type="text"/>	<input type="text"/>	TCP ▼	<input type="text"/>	<input type="text"/>	TCP ▼

Apply Cancel

DMZ

Since some applications are not compatible with NAT, the device supports the use of a DMZ IP address for a single host on the LAN. This IP address is not protected by NAT and it is visible to agents on the Internet with the correct type of software. Note that any client PC in the DMZ is exposed to various types of security risks. If you use the DMZ, take measures (such as client-based virus protection) to protect the remaining client PCs on your LAN from possible contamination through DMZ.

Choose **ADVANCED > DMZ**. The page shown in the right figure appears.

Click **Apply** to save the settings.

DMZ

The DSL Router will forward IP packets from the WAN that do not belong to any of the applications configured in the Port Forwarding table to the DMZ host computer.

Enter the computer's IP address and click "Apply" to activate the DMZ host.

Clear the IP address field and click "Apply" to deactivate the DMZ host.

DMZ HOST

DMZ Host IP Address :

Apply Cancel

Parental Control

Choose **ADVANCED > Parental Control**. The **Parent Control** page shown in the right figure appears.

PARENTAL CONTROL -- BLOCK WEBSITE

Uses URL (i.e. www.yahoo.com) to implement filtering.

Block Website

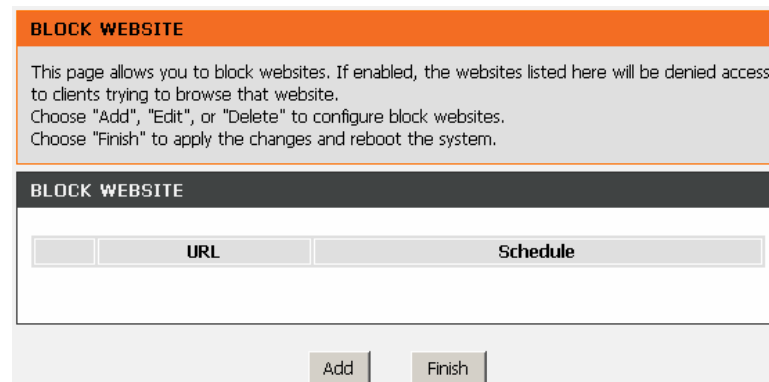
PARENTAL CONTROL -- BLOCK MAC ADDRESS

Uses MAC address to implement filtering.

Block MAC Address

Block Website

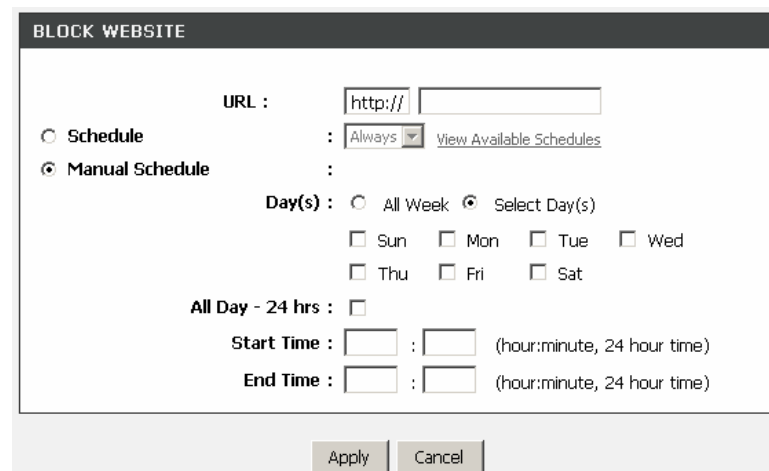
In the **Parent Control** page, click **Block Website**. The page shown in the right figure appears.



Click **Add**. The page shown in the right page appears.

Enter the website in the **URL** field. Select the **Schedule** from drop-down list, or select **Manual Schedule** and select the corresponding time and days.

Click **Apply** to add the website to the **BLOCK WEBSITE Table**.



Block MAC Address

In the **PARENT CONTROL** page, click **Block MAC Address**. The page as shown in the figure appears.

BLOCK MAC ADDRESS

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

This page adds a time of day restriction to a special LAN device connected to the router. The "Current PC's MAC Address" automatically displays the MAC address of the LAN device where the browser is running. To restrict another 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, open a command prompt window and type "ipconfig /all".

	Username	MAC	Schedule
--	----------	-----	----------

Add

Click **Add**. The page as shown in the following figure appears. The table describes the parameters in this page.

Field	Description
User Name	Enter the name that identifies your configuration. For example, <i>kids</i> .
Current PC's MAC Address	Enter the MAC address of the computer that connects to the device.
Other MAC Address	Enter the MAC address of another device that is included in MAC filtering.
Schedule	Select the time of MAC filter from the drop-down list. You can select always or never .
Manual Schedule	If you select this check box, you need to manually set the time of MAC filtering.

Enter the use name and MAC address. Select the corresponding time and days. Then, click **Apply** to add the MAC address to the **BLOCK MAC ADDRESS** table. The page as shown in the figure appears.

TIME OF DAY RESTRICTION

User Name :

Current PC's MAC Address :

Other MAC Address :

Schedule Rule : [View Available Schedules](#)

Manual Schedule :

Day(s) : All Week Select Day(s)

Sun Mon Tue Wed

Thu Fri Sat

All Day - 24 hrs :

Start Time : : (hour:minute, 24 hour time)

End Time : : (hour:minute, 24 hour time)

BLOCK MAC ADDRESS

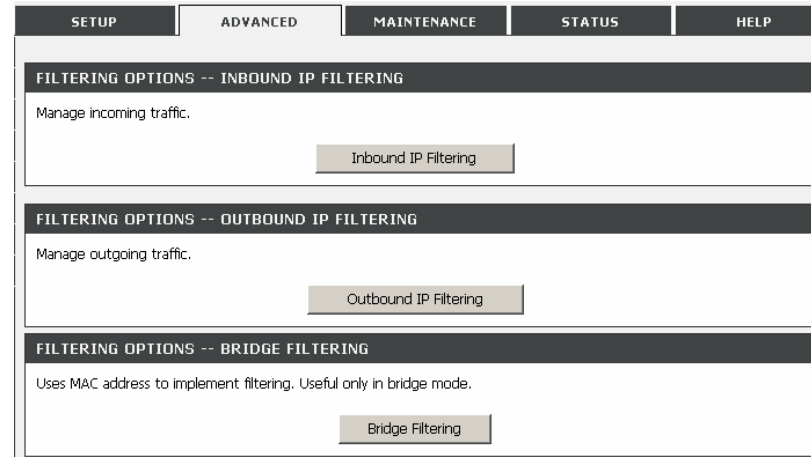
Time of Day Restrictions -- A maximum of 16 entries can be configured

This page adds a time of day restriction to a special LAN device connected to the router. The "Current PC's MAC Address" automatically displays the MAC address of the LAN device where the browser is running. To restrict another 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, open a command prompt window and type "ipconfig /all".

	Username	MAC	Schedule
<input type="checkbox"/>	eg	00:11:22:33:44:55	Always

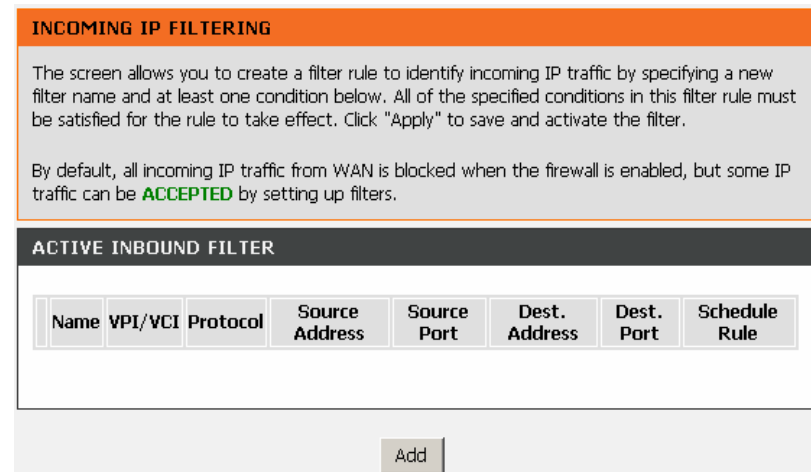
Filtering Options

Choose **ADVANCED > Filtering Options**. The **FILTERING OPTIONS** page as shown in the figure appears.




Inbound IP Filtering

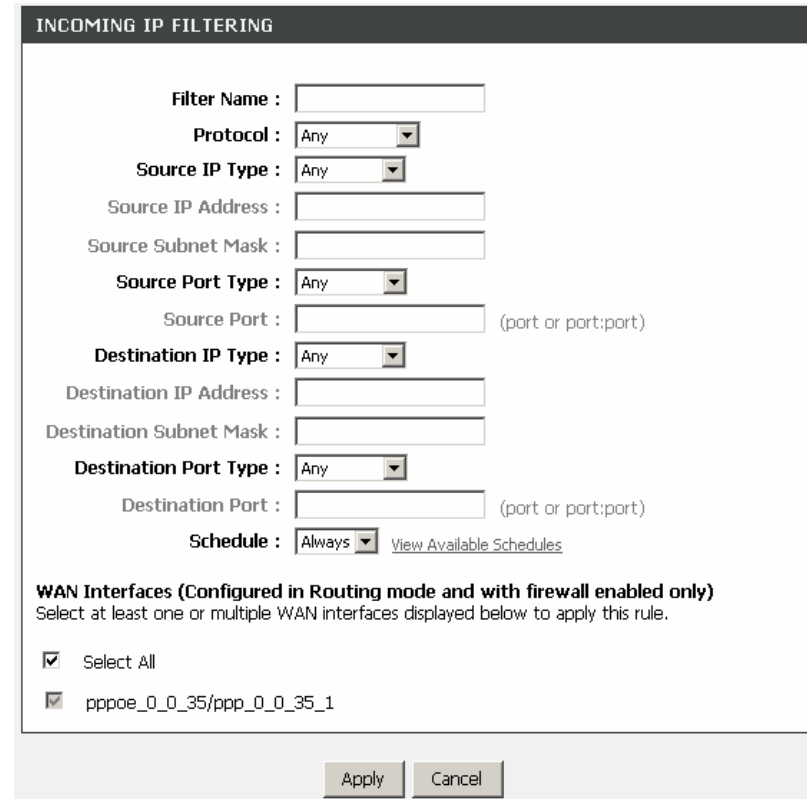
In the **FILTERING OPTIONS** page, click **Inbound IP Filtering**. The **INCOMING IP FILTERING** page as shown in the figure appears.



Click **Add** to add an inbound IP filter. The page as shown in the figure appears. Enter the **Filter Name** and specify at least one of the following criteria: protocol, source/destination IP address, subnet mask, and source/destination port. Then, click **Apply** to save the settings.

 **Note:**
The settings apply only when the firewall is enabled.

The **ACTIVE INBOUND FILTER** in the **INCOMING IP FILTERING** page displays detailed information of each created inbound IP filter. Click **Delete** to delete an IP filter. Note that the **Delete** button appears only when at least one IP filter exists.



INCOMING IP FILTERING

Filter Name :

Protocol : Any

Source IP Type : Any

Source IP Address :

Source Subnet Mask :

Source Port Type : Any

Source Port : (port or port:port)

Destination IP Type : Any

Destination IP Address :

Destination Subnet Mask :

Destination Port Type : Any

Destination Port : (port or port:port)

Schedule : Always [View Available Schedules](#)

WAN Interfaces (Configured in Routing mode and with firewall enabled only)
Select at least one or multiple WAN interfaces displayed below to apply this rule.

Select All

pppoe_0_0_35/ppp_0_0_35_1

Apply Cancel

Outbound IP Filtering

By default, all outgoing IP traffic from the LAN is allowed. The outbound filter allows you to create a filter rule to block outgoing IP traffic by specifying a filter name and at least one criterion.

In the **FILTERING OPTIONS** page, click **Outbound IP Filtering**. The **OUTGOING IP FILTERING** page as shown in the figure appears.

OUTGOING IP FILTERING

This screen allows you to create a filter rule to identify outgoing IP traffic by specifying a new filter name and at least one condition below. All of the specified conditions in this filter rule must be satisfied for the rule to take effect. Click "Apply" to save and activate the filter.

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.

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

ACTIVE OUTGOING IP FILTER

Name	Protocol	Source Address	Source Port	Dest. Address	Dest. Port	Schedule Rule
------	----------	----------------	-------------	---------------	------------	---------------

Add

Web Configuration

Click **Add** to add an outbound IP filter. The page as shown in the figure appears.

Enter the **Filter Name** and specify at least one of the following criteria: protocol, source/destination IP address, subnet mask, and source/destination port. Click **Apply** to save the settings.

The **ACTIVE OUTBOUND FILTER** in the **OUTGOING IP FILTERING** page displays detailed information OF each created outbound IP filter. Click **Delete** to delete an IP filter. Note that the **Delete** button appears only when at least one IP filter exists.

OUTGOING IP FILTERING

Filter Name :

Protocol : Any

Source IP Type : Any

Source IP Address :

Source Subnet Mask :

Source Port Type : Any

Source Port : (port or port:port)

Destination IP Type : Any

Destination IP Address :

Destination Subnet Mask :

Destination Port Type : Any

Destination Port : (port or port:port)

Schedule : Always [View Available Schedules](#)

Bridge Filtering

In the **FILTERING OPTIONS** page, click **Bridge Filtering**. The page as shown in the figure appears.

This page is used to configure bridge parameters. In this page, you can modify the settings or view the information of the bridge and its attached ports.

SETUP
ADVANCED
MAINTENANCE
STATUS

BRIDGE FILTERING

Bridge Filtering is only effective on ATM PVCs configured in Bridge mode. **ALLOW** means that all MAC layer frames will be **ALLOWED** except those matching with any of the specified rules in the following table. **DENY** means that all MAC layer frames will be **DENIED** except those matching with any of the specified rules in the following table.

Create a filter to identify the MAC layer frames by specifying at least one condition below. If multiple conditions are specified, all of them take effect. Click "Apply" to save and activate the filter.

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.

Bridge Filtering Global Policy:

ALLOW all packets but **DENY** those matching any of specific rules listed

DENY all packets but **ALLOW** those matching any of specific rules listed

Apply Cancel

BRIDGE FILTER SETUP

VPI/VCI	Protocol	Destination MAC	Source MAC	Frame Direction	Schedule Rule

Add

Web Configuration

Click **Add** to add a bridge filter. The page as shown in the figure appears.

The table describes the parameters in this page.

Field	Description
Protocol Type	Select the protocol type to be mapped from the drop-down list. You can select PPPoE , IPv4 , IPv6 , AppleTalk , IPX , NetBEUI , or IGMP .
Destination MAC Address	Enter the destination MAC address to be mapped.
Source MAC Address	Enter the source MAC address to be mapped.
Frame Direction	Select the frame direction to be mapped from the drop-down list. The device supports frame direction from LAN to WAN and that from WAN to LAN.
Schedule	Select the time that you want to apply the rule from the drop-down list. You can select always or never .
Wan interface	Select the WAN interface to be mapped from the drop-down list.

Click **Apply** to save the settings.

ADD BRIDGE FILTER

Protocol Type : (Click to Select) ▾

Destination MAC Address :

Source MAC Address :

Frame Direction : LAN<=>WAN ▾

Schedule : Always ▾ [View Available Schedules](#)

WAN Interfaces (Configured in Bridge mode only)

Select All

Apply Cancel

Firewall Settings

A denial-of-service (DoS) attack is characterized by an explicit attempt by attackers to prevent legitimate users of a service from using that service. Examples include the following

- The attackers attempt to flood a network, thereby preventing legitimate network traffic
- The attackers attempt to disrupt connections between two machines, thereby preventing access to a service
- The attackers attempt to prevent a particular individual from accessing a service
- The attackers attempt to disrupt service to a specific system or person.

Port scan protection is designed to block attempts to discover vulnerable ports or services that might be exploited in an attack from the WAN.

Choose **ADVANCED > Firewall Settings**. The page shown in the right figure appears.

Click **Apply** to save the settings.

FIREWALL SETTINGS

Click "Apply" button to make the changes effective after reboot the device.

FIREWALL CONFIGURATION

Enable Attack Prevent

Rate(pkt/sec)Burst(bit/sec)

TCP DoS :

Ping DoS :

Port Scan :

Prevent IP Spoofing :

Apply Cancel

DNS

Domain name system (DNS) is an Internet service that translates domain names into IP addresses. Because domain names are alphabetic, they are easier to remember. The Internet, however, is actually based on IP addresses. Each time you use a domain name, a DNS service must translate the name into the corresponding IP address. For example, the domain name www.example.com might be translated to 198.105.232.4.

The DNS system is, in fact, its own network. If one DNS server does not know how to translate a particular domain name, it asks another one, and so on, until the correct IP address is returned.

Choose **ADVANCED > DNS**. The page as shown in the figure appears.

The table describes the parameters in this page.

Field	Description
Obtain DNS server address automatically	If you select this radio button, the device automatically obtains IP address of the DNS server from the ISP. You need not manually enter the IP address of the server.
Use the following DNS server addresses	If you select this radio button, you need to manually enter the IP address of the server provided by the ISP.
Preferred DNS server	Enter the IP address of the primary DNS server.
Alternate DNS server	Enter the IP address of the secondary DNS server. If the primary DNS server fails to work, the device tries to connect the secondary DNS server.

Click **Apply** to save the settings.

Dynamic DNS

The device supports dynamic domain name service (DDNS). The dynamic DNS service allows a dynamic public IP address to be associated with a static host name in any of the many domains, and allows access to a specified host from various locations on the Internet. Click a hyperlinked URL in the form of hostname.dyndns.org and allow remote access to a host. Many ISPs assign public IP addresses using DHCP, so locating a specific host on the LAN using the standard DNS is difficult. For example, if you are running a public web server or VPN server on your LAN, DDNS ensures that the host can be located from the Internet even if the public IP address changes. DDNS requires that an account be set up with one of the supported DDNS service providers (DyndDNS.org or dlinkddns.com).

Choose **ADVANCED > Dynamic DNS**. The page shown in the right page appears.

DYNAMIC DNS

The Dynamic DNS feature allows you to host a server (Web, FTP, Game Server, etc...) using a domain name that you have purchased (www.whateveryournameis.com) with your dynamically assigned IP address. Most broadband Internet Service Providers assign dynamic (changing) IP addresses. Using a DDNS service provider, your friends can enter your host name to connect to your game server no matter what your IP address is.

[Sign up for D-Link's Free DDNS service at www.DLinkDDNS.com](http://www.DLinkDDNS.com)

Hostname	Username	Service	Interface
Add			

Click **Add** to add dynamic DNS. The page shown in the right figure appears.

- **DNS provider:** Select one of the DDNS registration organizations from the down-list drop.

- **Host Name:** Enter the host name that you registered with your DDNS service provider.
- **Username:** Enter the user name for your DDNS account.
- **Password:** Enter the password for your DDNS account.

Click **Apply** to save the settings.

ADD DYNAMIC DNS

DDNS provider : dlinkddns.com(Free)

Hostname :

Interface : wizard_pvc/ppp_0_0_32_1

Username :

Password :

Apply Cancel

Network Tools

Choose **ADVANCED > Network Tools**. The **NETWORK TOOLS** page as shown in the figure appears.

The screenshot displays a vertical list of network tool configuration sections. Each section has a dark header with the tool name, a brief description, and a button to access the configuration page.

- NETWORK TOOLS -- PORT MAPPING**
Port Mapping supports multiple port to PVC and bridging groups. Each group will perform as an independent network.
Port Mapping
- NETWORK TOOLS -- IGMP**
Transmission of identical content, such as multimedia, from a source to a number of recipients.
IGMP
- NETWORK TOOLS -- QUEUE CONFIG**
Allows you to add Classification Queue precedence for QoS.
Queue Config
- NETWORK TOOLS -- QUALITY OF SERVICE**
Allows you to manually configure different priority to different interfaces.
Quality of Service
- NETWORK TOOLS -- UPnP**
Allows you to enable or disable UPnP.
UPnP
- NETWORK TOOLS -- ADSL**
Allows you to configure advanced settings for ADSL.
ADSL Settings
- NETWORK TOOLS -- SNMP**
Allows you to configure SNMP (Simple Network Management Protocol).
SNMP
- NETWORK TOOLS -- TR-069**
Allows you to configure TR-069 protocol.
TR-069
- NETWORK TOOLS -- CERTIFICATES**
Allows you to manage certificates used with TR-069.
Certificates

Port Mapping

In the **NETWORK TOOLS** page, click **Port Mapping**. The page as shown in the figure appears.

PORT MAPPING

Port Mapping -- A maximum 16 entries can be configured

Port Mapping supports multiple port to PVC 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 "Delete" button will remove the grouping and add the ungrouped interfaces to the Default group.

Enable virtual ports on

PORT MAPPING SETUP

Group Name	Interfaces
Default	LAN(1-4), Wireless

In this page, you can bind the WAN interface and the LAN interface to the same group. When you setup the port mapping, you need to enable the virtual ports at first.

PORT MAPPING

Port Mapping -- A maximum 16 entries can be configured

Port Mapping supports multiple port to PVC 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 "Delete" button will remove the grouping and add the ungrouped interfaces to the Default group.

Enable virtual ports on

PORT MAPPING SETUP

Group Name	Interfaces
Default	LAN4, LAN3, LAN2, LAN1, Wireless

Click **Add** to add port mapping. The page as shown in the figure appears.

To create a mapping group, do as follows:

Step 1 Enter the group name.

Step 2 Select interfaces from the **Available Interfaces** list and click the **<-** arrow button to add them to the grouped interface list, in order to create the required mapping of the ports. The group name must be unique.

Step 3 Click **Apply** to save the settings.

ADD PORT MAPPING

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. Click "Apply" button to make the changes effective immediately.

PORT MAPPING CONFIGURATION

Group Name:

Grouped Interfaces **Available Interfaces**

 LAN4
LAN3
LAN2
LAN1
Wireless

->
<-

Apply Cancel

IGMP Snooping

In the **NETWORK TOOLS** page, click **IGMP**. The page as shown in the figure appears. When IGMP snooping is enabled, only hosts that belong to the group receive the multicast packets. If a host is deleted from the group, the host cannot receive the multicast packets any more. Click **Apply** to save the settings.

IGMP

Transmission of identical content, such as multimedia, from a source to a number of recipients.

IGMP SETUP

Enable IGMP Snooping

Queue Configuration

In the **NETWORK TOOLS** page, click **Queue Config**. The page as shown in the figure appears. Entries in this table are used to assign the precedence for each incoming packet based on physical LAN port, TCP or UDP port number, source or destination IP address, and subnet mask.

QUEUE CONFIG

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 effect.

QUEUE CONFIG LIST

Interface Name	Description	Precedence	Queue Key	Enable	Remove
wireless	WMM Voice Priority	1	1		
wireless	WMM Voice Priority	2	2		
wireless	WMM Video Priority	3	3		
wireless	WMM Video Priority	4	4		
wireless	WMM Best Effort	5	5		
wireless	WMM Background	6	6		
wireless	WMM Background	7	7		
wireless	WMM Best Effort	8	8		

Web Configuration

Click **Add**. The page as shown in the figure appears.
Click **Apply** to save the settings.

ADD QUEUE CONFIG

Queue Configuration: (Click to Select) ▾

Status: (Click to Select) ▾

Queue: (Click to Select) ▾

Queue Precedence: (Click to Select) ▾

Apply Cancel

Quality of Service

In the **NETWORK TOOLS** page, click **Quality of Service**. The page as shown in the figure appears.

QUALITY OF SERVICE

If you disable WMM function in Wireless Page, classification related to wireless will not take effect.
Choose "Add" or "Remove" to configure network traffic classes.

QUALITY OF SERVICE SETUP

MARK						
Class Name	DSCP Mark	Queue ID	802.1P Mark	Order	Enable/Disable	Details

Add

Click **Add** and the page as shown in the figure appears.
 The table describes the parameters in this page.

Field	Description
Traffic Class Name	Enter the name of the traffic class.
Assign Classification Queue	Specify the queue to which the packet belongs. You can set the queue in the classification configuration.
DSCP Mark	Attach the DSCP mark to the mapped packet.
Physical LAN Port	Select the physical port of the packet from the drop-down list.
Source MAC Address	Enter the source MAC address of the packet.
Source MAC Mask	Use mask 000000ffff to mask the MAC address. 00 indicates not mapped and ff indicates mapped.
Destination MAC Address	Enter the destination MAC address of the packet.
Destination MAC Mask	Use mask 000000ffff to mask the MAC address. 00 indicates not mapped and ff indicates mapped.
802.1p Priority	Select the 802.1p priority of the packet from the drop-down list. You can select Any or a value in the range of 0—7. Note that this function is not supported at the moment.

Click **Apply** to save the settings.

QUALITY OF SERVICE

The screen creates a traffic class rule to classify the upstream traffic, assign queue which defines the precedence and the interface and optionally overwrite the IP header DSCP byte. A rule consists of a class name and at least one condition below. All of the specified conditions in this classification rule must be satisfied for the rule to take effect. Click "Apply" to save and activate the rule.

Assign ATM Priority and/or DSCP Mark for the class
 If non-blank value is selected for "Assign Differentiated Services Code Point (DSCP) Mark", the corresponding DSCP byte in the IP header of the upstream packet is overwritten by the selected value.

NETWORK TRAFFIC CLASS RULE

Traffic Class Name :

Rule Order : Last

Rule Status :

Assign Classification Queue :

Assign Differentiated Services Code Point (DSCP) Mark : No Change

Mark 802.1p if 802.1q is enabled : No Change

SPECIFY TRAFFIC CLASSIFICATION RULES

Enter the following conditions either for IP level, SET-1, or for IEEE 802.1p, SET-2.

SET-1

Physical LAN Port : Any

Protocol : Any

Differentiated Services Code Point (DSCP) Check : Any

Source IP Type : Any

Source IP Address :

Source Subnet Mask :

Source Port Type : Any

UDP/TCP Source Port (port or port:port) :

Destination IP Type : Any

Destination IP Address :

Destination Subnet Mask :

Destination Port Type : Any

UDP/TCP Destination Port (port or port:port) :

Source MAC Address :

Source MAC Mask :

Destination MAC Address :

Destination MAC Mask :

SET-2

802.1p Priority : Any

UPnP

Choose **ADVANCED > Network Tools** and click **UPnP**. The page shown in the following figure appears.

In this page, you can configure universal plug and play (UPnP). The system acts as a daemon after you enable UPnP.

UPnP is used for popular audio visual software. It allows automatic discovery of your device in the network. If you are concerned about UPnP security, you can disable it. Block ICMP ping should be enabled so that the device does not respond to malicious Internet requests.

Click **Apply** to save the settings.

UPNP

Universal Plug and Play (UPnP) supports peer-to-peer Plug and Play functionality for network devices.

UPNP SETUP

Enable UPnP

Apply Cancel

ADSL Settings

In the **NETWORK TOOLS** page, click **ADSL**. The page as shown in the figure appears.

In this page, you can select the ADSL modulation. Normally, you are recommended to keep the factory defaults. The device negotiates the modulation mode with the DSLAM.

Click **Apply** to save the settings.

ADSL

This page allows you to configure the modem's ADSL modulation.

Select the modulation below.

ADSL SETTINGS

G.Dmt Enabled
 G.Lite Enabled
 T1.413 Enabled
 ADSL2 Enabled
 AnnexL Enabled
 ADSL2+ Enabled
 AnnexM Enabled

Capability

Bitswap Enable
 SRA Enable

Apply Cancel

SNMP

Choose **ADVANCED > Network Tools** and click **SNMP**. The page shown in the right figure appears. In this page, you can set SNMP parameters.

- **Read Community:** The network administrator must use this password to read the information of this device.
- **Set Community:** The network administrator must use this password to configure the information of this device.
- **Trap Manager IP:** The trap information is sent to this host.

Click **Apply** to save the settings.

The screenshot shows the SNMP configuration page. At the top, there is an orange header with the text "SNMP". Below this, a grey box contains the following text: "Simple Network Management Protocol (SNMP) allows a management application to retrieve statistics and status from the SNMP agent in this device." and "Select the desired values and click 'Apply' to configure the SNMP options." Below this is a dark grey header with the text "SNMP -- CONFIGURATION". The main content area contains a list of configuration options, each with a label and a text input field. The "Enable SNMP Agent" option is checked. The input fields contain the following values: "public" for Read Community, "private" for Set Community, "DSL-2640B" for System Name, "unknown" for System Location, "unknown" for System Contact, and "0.0.0.0" for Trap Manager IP. At the bottom right of the form, there are two buttons: "Apply" and "Cancel".

SNMP

Simple Network Management Protocol (SNMP) allows a management application to retrieve statistics and status from the SNMP agent in this device.

Select the desired values and click "Apply" to configure the SNMP options.

SNMP -- CONFIGURATION

Enable SNMP Agent

Read Community :

Set Community :

System Name :

System Location :

System Contact :

Trap Manager IP :

TR-069

In the **NETWORK TOOLS** page, click **TR-069**. The page as shown in the figure appears. In this page, you can configure the TR-069 CPE. The table describes the parameters in this page.

Field	Description
Inform	You can select Disabled or Enabled to disable or enable notification. <ul style="list-style-type: none"> ● Disabled indicates that the device does not automatically send requests to the TR069 server. ● Enabled indicates that the device automatically sends a request of connection to the TR069 server. The following function items are available only when Inform is set to Enabled.
Inform Interval	The interval of sending a request of connection to the TR069 server from the device.
ACS URL	The path of the TR069 server to which the device sends a request.
ACS User Name	The user name that the devices uses to log in to the TR069 server.
ACS Password	The password that the devices uses to log in to the TR069 server.
Connection Request Authentication	Select the check box to enable authentication of connection request. If you enable the function, you need to enter the user name and password for authentication.
Connection Request User Name	The user name that the TR069 server uses to access the TR069 progress of the device.
Connection Request Password	The password that the TR069 server uses to access the TR069 progress of the device.

Click **Apply** to save settings.

TR-069

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.

TR-069 CLIENT -- CONFIGURATION

Inform Disable Enable

Inform Interval:

ACS URL:

ACS User Name:

ACS Password:

Connection Request Authentication

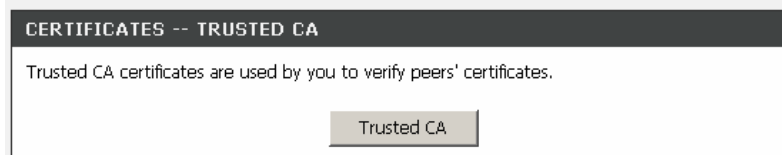
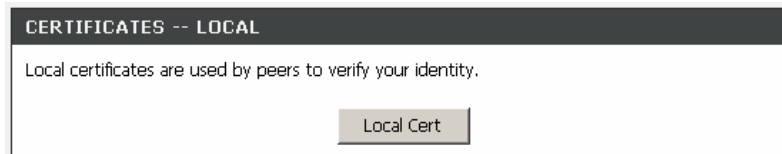
Connection Request User Name:

Connection Request Password:

Certificates

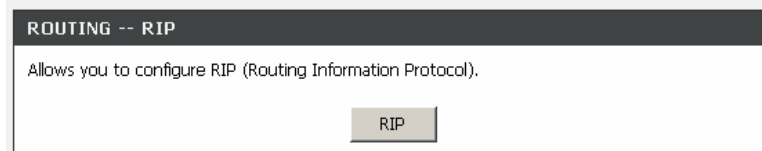
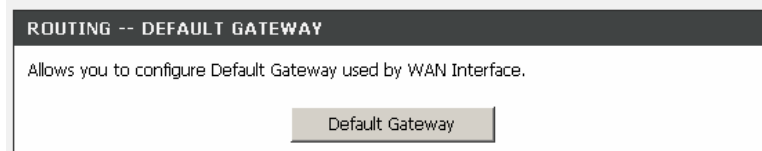
Choose **ADVANCED > Network Tools** and click **Certificates**. The **Certificates** page shown in the right figure appears.

In this page, you can set local certificate and trusted certificate.



Routing

Choose **ADVANCED > Routing**. The page as shown in the figure appears.



Static Route

Choose **ADVANCED > Routing** and click **Static Route**. The page as shown in the figure appears. This page displays the information of existing static routes.

Click **Add** and the page as shown in the figure appears.

The table describes the parameters in this page.

Field	Description
Destination Network Address	The destination IP address of the device.
Subnet Mask	The subnet mask of the destination IP address.
Use Gateway IP Address	The gateway IP address of the device.
Use Interface	Select the interface of the static routing used by the device from the drop-down list.

 **Note:**

You can enter the gateway IP address of the device in the **Use Gateway IP Address** field or set the **User Interface**, but cannot apply the two settings at the same time.

Click **Apply** to save the settings.

Default Gateway

Choose **ADVANCED > Routing** and click **Default Gateway**. The page as shown in the figure appears.

In this page, you can select **Enable Automatic Assigned Default Gateway**, or enter the information in the **Use Gateway IP Address** and **Use Interface** fields. Click **Apply** to save the settings.

DEFAULT GATEWAY

If Enable Automatic Assigned Default Gateway checkbox is selected, this router will accept the first received default gateway assignment from one of the PPPoA, PPPoE or MER/DHCP enabled PVC(s). If the checkbox is not selected, enter the static default gateway OR a WAN interface. Click "Apply" button to save it.

DEFAULT GATEWAY

Enable Automatic Assigned Default Gateway

Use Default Gateway IP Address :

Use Interface : wizard_pvc/ppp_0_0_32_1

RIP

Choose **ADVANCED > Routing** and click **RIP**. The page shown in the following figure appears. This page is used to select the interfaces on your device that use RIP and the version of the protocol used.

If you are using this device as a RIP-enabled device to communicate with others using the routing information protocol, enable RIP and click **Apply** to save the settings.

RIP

To activate RIP for the device, select the "Enabled" checkbox for Global RIP Mode. To configure an individual interface, select the desired RIP version and operation, followed by placing a check in the "Enabled" checkbox for the interface. Click the "Apply" button to save the configuration, and to start or stop RIP based on the Global RIP Mode selected.

ROUTING -- RIP

Enable Global RIP Mode

Interface	VPI/VCI	Version	Operation	Enabled
br0	(LAN)	2	Active	<input type="checkbox"/>
ppp_0_0_32_1	0/0/32	2	Passive	<input type="checkbox"/>

Schedules

Choose **ADVANCED** > **Schedules**. The page as shown in the figure appears.

Click **Add** to add a schedule rule. The page as shown in the figure appears.

The table describes the parameters in this page.

Field	Description
Name	Set the name of the schedule.
Day(s)	You can select one, more, or all of the seven days in a week.
All Day – 24 hrs	If you select the check box, the rule applies throughout the 24 hours of the day.
Start Time	Set the start time of the firewall.
End Time	Set the end time of the firewall.

Click **Apply** to save the settings.

MAINTENANCE

System

Choose **MAINTENANCE > System MAINTENANCE**. The **System** page as shown in the figure appears.

In this page, you can restart the device, back up the current settings to a file, update the backup file, and restore the factory default settings.

The table describes the buttons in this page.

Button	Description
Reboot	Restart the device.
Backup Settings	Specify the path to back up the current configuration in a configuration file on your computer. You can rename the configuration file.
UPDATE SETTINGS	Click Browse... to select the configuration file of device and click Update Settings to update the configuration of the device.
Restore Default Settings	Reset the device to default settings.



Caution:

Do not turn off your device or press the Reset button when the procedure is in progress.

DSL-2640B
SETUP
ADVANCED
MAINTENANCE
STATUS

SYSTEM -- REBOOT

Click the button below to reboot the router.

SYSTEM -- BACKUP SETTINGS

Back up DSL Router configurations. You may save your router configurations to a file on your PC.
Note: Please always save configuration file first before viewing it.

SYSTEM -- UPDATE SETTINGS

Update DSL Router settings. You may update your router settings using your saved files.

Settings File Name :

SYSTEM -- RESTORE DEFAULT SETTINGS

Restore DSL Router settings to the factory defaults.

Firmware Update

Choose **MAINTENANCE > Firmware Update**. The page as shown in the figure appears. In this page, you can upgrade the firmware of the device. To update the firmware, do as follows:

Step 1 Click **Browse...** to select the file.

Step 2 Click **Update Firmware** to update the configuration file.

The device loads the file and reboots automatically.



Caution:

Do not turn off your device or press the Reset button when the procedure is in progress.

FIRMWARE UPDATE

Step 1: Obtain an updated firmware 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 Firmware" button once to upload the new image file.

NOTE: The update process takes about 2 minutes to complete, and your DSL Router will reboot. Please DO NOT power off your router before the update is complete.

FIRMWARE UPDATE

Current Firmware Version : SEA_1.00
Current Firmware Date : Nov 10 2009

Firmware File Name :

Access Controls

Choose **MAINTENANCE** > **Access Controls**. The **ACCESS CONTROLS** page as shown in the figure appears.

This page contains **Account Password**, **Services**, and **IP Address**.

SETUP	ADVANCED	MAINTENANCE	STATUS	HELP
ACCESS CONTROLS -- ACCOUNT PASSWORD				
Manage DSL Router user accounts.				
<input type="button" value="Account Password"/>				
ACCESS CONTROLS -- SERVICES				
A Service Control List ("SCL") enables or disables services from being used.				
<input type="button" value="Services"/>				
ACCESS CONTROLS -- IP ADDRESS				
Permits access to local management services.				
<input type="button" value="IP Address"/>				

Account Password

In the **ACCESS CONTROLS** page, click **Account Password**. The page as shown in the figure appears.

In this page, you can change the password and set the time for automatic logout.

You are recommended to change the default password to ensure the security of your network. Ensure that you remember the new password or write it down and keep it in a safe location for future reference. If you forget the password, you need to reset the device to the factory default settings. In that case, all configuration settings of the device are lost.

The table describes the parameters in this page.

Field	Description
ACCOUNT PASSWORD	
Username	Select a user name from the drop-down list to access the device. You can select admin, support, or user .
Current Password	Enter the password of the user.
New Password	Enter the new password.
Confirm Password	Enter the new password again for confirmation.
WEB IDLE TIME OUT SETTINGS	
Web Idle Time Out	Set the time after which the system automatically exits the configuration page. Its value range is 5—30 minutes.

Click **Apply** to apply the settings.

ACCOUNT PASSWORD

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

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 firmware.

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

ADMINISTRATOR SETTINGS

Username :

Current Password :

New Password :

Confirm Password :

WEB IDLE TIME OUT SETTINGS

Web Idle Time Out : (5 ~ 30 minutes)

Services

In the **ACCESS CONTROLS** page, click **Services**. The page as shown in the figure appears.

In this page, you can enable or disable the services that are used by the remote host. For example, if telnet service is enabled at port 23, the remote host can access the device by telnet through port 23.

Select the MAINTENANCE services that you want to enable or disable at the LAN or WAN interface and click **Apply** to apply the settings.



Caution:

If you disable the HTTP service, you cannot access the configuration page of the device any more.

SERVICES

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

ACCESS CONTROL -- SERVICES

Service	LAN	WAN	WAN Port
FTP	<input checked="" type="checkbox"/> Enabled	<input type="checkbox"/> Enabled	<input type="text" value="21"/>
HTTP	<input checked="" type="checkbox"/> Enabled	<input type="checkbox"/> Enabled	<input type="text" value="80"/>
ICMP	<input checked="" type="checkbox"/> Enabled	<input type="checkbox"/> Enabled	
SNMP	<input checked="" type="checkbox"/> Enabled	<input type="checkbox"/> Enabled	<input type="text" value="161"/>
SSH	<input checked="" type="checkbox"/> Enabled	<input type="checkbox"/> Enabled	<input type="text" value="22"/>
TELNET	<input checked="" type="checkbox"/> Enabled	<input type="checkbox"/> Enabled	<input type="text" value="23"/>
TFTP	<input checked="" type="checkbox"/> Enabled	<input type="checkbox"/> Enabled	<input type="text" value="69"/>

IP Address

In the **ACCESS CONTROLS** page, click **IP Address**. The page as shown in the figure appears.

In this page, you can configure the IP address in the access control list (ACL). If ACL is enabled, only devices of the specified IP addresses can access the device.

Select **Enable Access Control Mode** to enable ACL.



Note:

If you enable ACL, ensure that the IP address of the host is in the ACL list.

Click **Add**. The page as shown in the figure appears.

Enter the IP address of the desired device in the **IP Address** field and click **Apply** to apply the settings.

SETUP ADVANCED MAINTENANCE STATUS

IP ADDRESS

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.

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

ACCESS CONTROL -- IP ADDRESSES

Enable Access Control Mode

IP Address

Add

IP ADDRESS

IP Address :

Apply Cancel

Diagnostics

Choose **MAINTENANCE > Diagnostic**. The page as shown in the figure appears.

In this page, you can test the connection status of the device. Click **Rerun Diagnostic Tests** to run diagnostics.

DSL-2640B	SETUP	ADVANCED	MAINTENANCE	STATUS
System	DIAGNOSTICS			
Firmware Update	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.			
Access Controls	WAN Connection : <input type="text" value="PPPoE/0/32/1"/> <input type="button" value="Rerun Diagnostic Tests"/>			
Diagnostics	TEST THE CONNECTION TO YOUR LOCAL NETWORK			
System Log	Test your Wireless Connection: PASS			
Logout	TEST THE CONNECTION TO YOUR DSL SERVICE PROVIDER			
	Test ADSL Synchronization: PASS			
	TEST THE CONNECTION TO YOUR INTERNET SERVICE PROVIDER			
	Ping default gateway: FAIL			
	Ping primary Domain Name Server: FAIL			

System Log

Choose **MAINTENANCE > System Log**. The **SYSTEM LOG** page as shown in the figure appears.

In this page, you can enable the log function. You can set **Mode** to **Local**, **Remote**, or **Both**. **Local** indicates to save the log in the local computer. **Remote** indicates to send the log to the remote log server. **Both** indicates to save the log in the local computer and the remote log server.

To log the events, do as follows:

Step 3 Select **Enable Log**.

Step 4 Select a mode from the drop-down list.

If you select **Remote** or **Both**, enter the IP address and port number of the server.

Step 5 Click **Apply** to apply the settings.

Step 6 Click **View System Log** to view the detail information of the system log.

SYSTEM LOG

If the log mode is enabled, the system will begin to log all the selected events. For the Log Level, all events above or equal to the selected level will be logged. For the Display Level, all logged events above or equal to the selected level will be displayed. If the selected mode is "Remote" or "Both", events will be sent to the specified IP address and UDP port of the remote syslog server. If the selected mode is "Local" or "Both", events will be recorded in the local memory.

Select the desired values and click "Apply" to configure the system log options.

Note: This will not work correctly if modem time is not properly set! Please set it in "Setup/Time and Date"

SYSTEM LOG -- CONFIGURATION

Enable Log

Log Level :

Display Level :

Mode :

Server IP Address :

Server UDP Port :

Status

In the **Status** page, you can view the system information and monitor the performance of the device.

Device Information

Choose **STATUS > Device Info**. The page as shown in the figure appears. The page displays the summary of the device status, including the system information, WAN connection information, and local network information.

DSL-2640B	SETUP	ADVANCED	MAINTENANCE	STATUS													
Device Info	DEVICE INFO																
Wireless Clients	This information reflects the current status of your DSL connection.																
DHCP Clients	SYSTEM INFO																
Logs	Model Name: DSL-2640B																
Statistics	Time and Date: Sat Jan 1 00:14:47 2000																
Route Info	Firmware Version: SEA_1.00																
Logout	INTERNET INFO																
	Internet Connection: <input type="text" value="ppp_0_0_32_1"/>																
	Internet Connection Status: Link Down																
	Default Gateway:																
	Preferred DNS Server: 192.168.1.1																
	Alternate DNS Server: 192.168.1.1																
	Connection Up Time: N/A																
	Downstream Line Rate (Kbps):																
	Upstream Line Rate (Kbps):																
	Enabled WAN Connections:																
	<table border="1"> <thead> <tr> <th>VPI/VCI</th> <th>Service Name</th> <th>Protocol</th> <th>IGMP</th> <th>QoS</th> <th>IP Address</th> </tr> </thead> <tbody> <tr> <td>0/32</td> <td>wizard_pvc</td> <td>PPPoE</td> <td>Disabled</td> <td>Disabled</td> <td></td> </tr> </tbody> </table>	VPI/VCI	Service Name	Protocol	IGMP	QoS	IP Address	0/32	wizard_pvc	PPPoE	Disabled	Disabled					
VPI/VCI	Service Name	Protocol	IGMP	QoS	IP Address												
0/32	wizard_pvc	PPPoE	Disabled	Disabled													
	WIRELESS INFO																
	MAC Address: 00:66:66:66:66:67																
	Status: Enabled																
	Network Name (SSID): Dlink																
	Visibility: Visible																
	Security Mode: WPA																
	LOCAL NETWORK INFO																
	MAC Address: 00:66:66:66:66:66																
	IP Address: 192.168.1.1																
	Subnet Mask: 255.255.255.0																
	DHCP Server: Enabled																

Wireless Clients

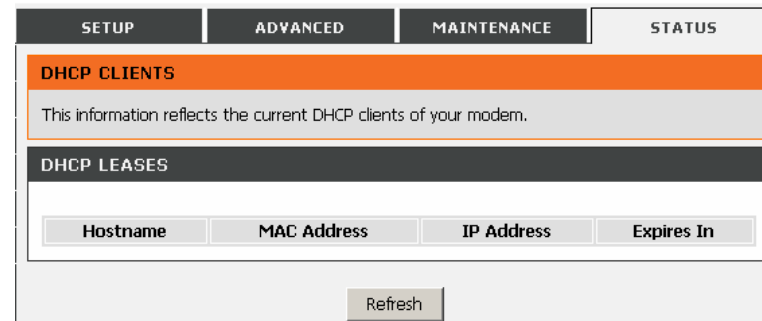
Choose **STATUS > Wireless Clients**. The page shown in the right page appears. The page displays authenticated wireless stations and their statuses.

The screenshot shows a web configuration interface with a top navigation bar containing four tabs: **SETUP**, **ADVANCED**, **MAINTENANCE**, and **STATUS**. The **STATUS** tab is selected. Below the navigation bar, there is a section titled **WIRELESS CLIENTS** with an orange header. Underneath this section, a message states: "This page shows authenticated wireless stations and their status." Below this message is another section titled **WIRELESS -- AUTHENTICATED STATIONS** with a dark grey header. This section contains a table with five columns: **MAC**, **Associated**, **Authorized**, **SSID**, and **Interface**. At the bottom right of the page, there is a **Refresh** button.

DHCP Clients

Choose **STATUS** > **DHCP Clients**. The page as shown in the figure appears.

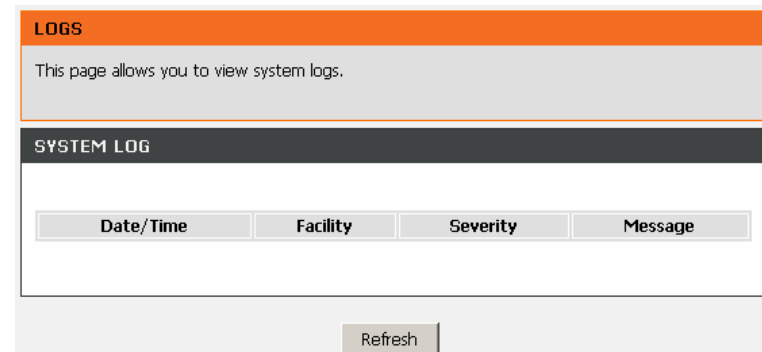
This page displays all client devices that obtain IP addresses from the device. You can view the host name, IP address, MAC address, and expiration time of the IP address.



Logs

Choose **STATUS** > **Logs**. The page as shown in the figure appears.

This page displays the system log. Click **Refresh** to refresh the system log shown in the box.



Statistics

Choose **STATUS > Statistics**. The page as shown in the figure appears.

This page displays the statistics information of the network and data transmission. The information helps technicians to identify whether the device is functioning properly. The information does not affect the functions of the device.

SETUP
ADVANCED
MAINTENANCE
STATUS

STATISTICS

This information reflects the current status of your DSL connection.

LOCAL NETWORK & WIRELESS

Interface	Received				Transmitted			
	Bytes	Pkts	Errs	Drops	Bytes	Pkts	Errs	Drops
Ethernet	195642	1811	0	0	1856180	2380	0	0
Wireless	0	0	0	0	0	0	2	0

INTERNET

Service	VPI/VCI	Protocol	Received				Transmitted			
			Bytes	Pkts	Errs	Drops	Bytes	Pkts	Errs	Drops
wizard_pvc	0/32	PPPoE	0	0	0	0	0	0	0	0

ADSL

Mode:		
Type:		
Line Coding:		
Status:	Link Down	
	Downstream	Upstream
SNR Margin (dB):		
Attenuation (dB):		
Output Power (dBm):		
Attainable Rate (Kbps):		
Rate (Kbps):		
HEC Errors:		
OCD Errors:		
LCD Errors:		
Total ES:		

ADSL BER Test
Reset Statistics

Route information

Choose **STATUS > Route Info**. The page as shown in the figure appears.
The table displays destination routes commonly accessed by the network.

SETUP	ADVANCED	MAINTENANCE	STATUS			
ROUTE INFO						
Flags: U - up, ! - reject, G - gateway, H - host, R - reinstate D - dynamic (redirect), M - modified (redirect).						
DEVICE INFO -- ROUTE						
Destination	Gateway	Subnet Mask	Flags	Metric	Service	Interface
192.168.1.0	0.0.0.0	255.255.255.0	U	0		br0

Troubleshooting

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

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

- Connect your PC to the Router using an Ethernet cable.
- Open a web browser and enter the address <http://192.168.1.1>.
- The default username is 'admin' and the default password is '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.

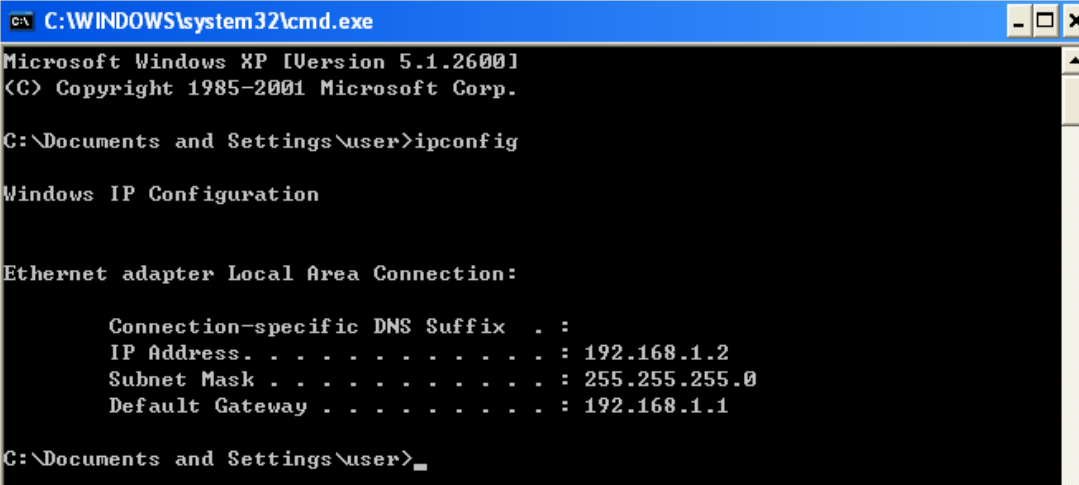
Click **Start > Run**. In the run box type “*cmd*” and click **OK**.

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.



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

C:\Documents and Settings\user>ipconfig

Windows IP Configuration

Ethernet adapter Local Area Connection:

    Connection-specific DNS Suffix  . :
    IP Address . . . . . : 192.168.1.2
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.1.1

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

Statically Assign An IP Address

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

Step 1

Windows® XP - Click **Start** > **Control Panel** > **Network Connections**.

Windows® 2000 - From the desktop, right-click **My Network Places** > **Properties**.

Step 2

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

Step 3

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

Step 4

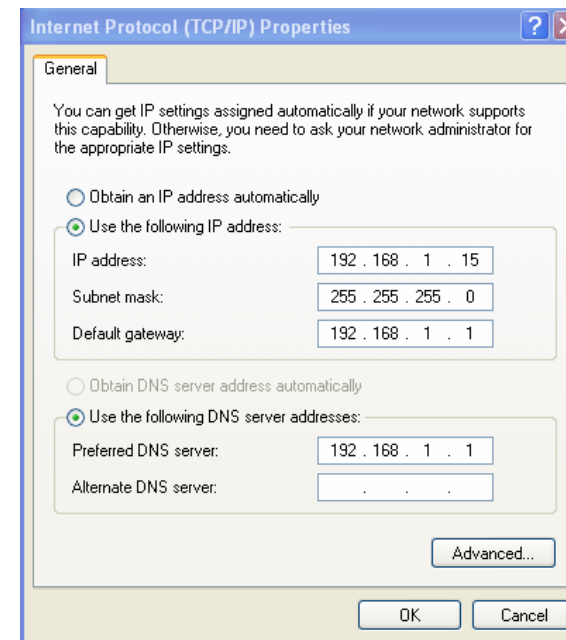
Click on the **Use the following IP address** and enter an IP address that is on the same subnet as your network or the LAN IP address on your router.

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

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

Step 5

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



Technical Specifications

ADSL Standards

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

ADSL2 Standards

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

ADSL2+ Standards

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

Protocols

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

DC Power

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

Data Transfer Rate

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

Wireless Transfer Rates

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

Media Interface

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

Default Settings

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