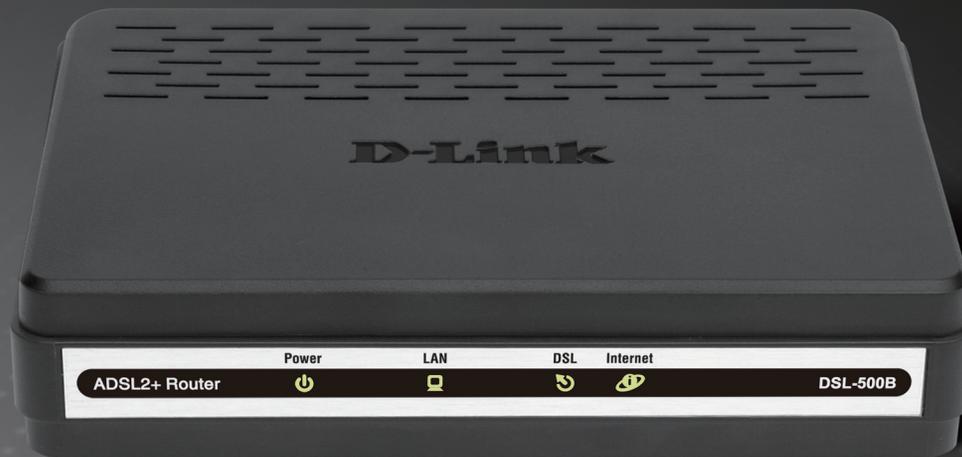


USER MANUAL

DSL-500B

VERSION 1.0



Preface

D-Link reserves the right to revise this publication and to make changes in the content hereof without obligation to notify any person or organization of such revisions or changes.

Manual Revisions

Revision	Date	Description
1.0	April 24, 2009	DSL-500B Revision A1 with firmware version 1.00

Trademarks

D-Link and the D-Link logo are trademarks or registered trademarks of D-Link Corporation or its subsidiaries in the United States or other countries. All other company or product names mentioned herein are trademarks or registered trademarks of their respective companies.

Copyright © 2009 by D-Link Systems, Inc.

All rights reserved. This publication may not be reproduced, in whole or in part, without prior expressed written permission from D-Link Systems, Inc.

Federal Communication Commission Interference Statement

Federal Communication Commission Interference Statement

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

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

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

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

IMPORTANT NOTE:

FCC Radiation Exposure Statement:

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

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

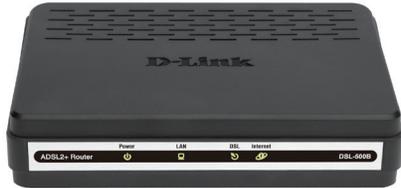
IEEE 802.11b or 802.11g operation of this product in the U.S.A. is firmware-limited to channels 1 through 11.

Table of Contents

Product Overview	6	Summary of Device Information	39
Package Contents	6	WAN Interface Information	40
System Requirements	7	Statistics - LAN	40
Features	8	Statistics - WAN	40
Hardware Overview	10	Statistics - ATM.....	40
Rear Panel (Connections)	10	Statistics - ADSL.....	41
Front Panel (LED Indicators)	11	Route Table Information	42
Installation	12	ARP Table Information	42
Overview.....	12	Advanced Setup	43
Installation Notes	12	WAN Configuration	43
Information Required from ADSL Service		LAN Configuration	45
Provider	14	NAT.....	46
Information You Will Need About the DSL-		Security.....	55
500B	16	Quality of Service.....	60
Information You Will Need About Your LAN or		Routing	69
Computer	17	DNS	71
Device Installation.....	18	DSL.....	72
Power on.....	18	Diagnostics	73
Factory Reset	19	Management.....	73
Network Connections.....	20	Settings.....	73
Web Configuration	21	System Log	74
Introduction to Web Configuration	21	System Agent	75
Quick Setup	22	TR-069 Client.....	76
DSL Router Device Information.....	39	Internet Time.....	76
		Access Control.....	77
		Update Software	78
		Save/Reboot.....	78

Appendix A - Troubleshooting	79
Troubleshooting	79
Appendix B - Networking Basics	82
Check Your IP Address	82
Statically Assign An IP Address.....	83
Appendix C - Technical Specifications	84
Technical Specifications	84

Package Contents



**DSL-500B
ADSL Router**



Power Adapter



CD-ROM with User Manual



**Twisted-Pair Cable
(for ADSL)**



**Straight-Through CAT5
Ethernet Cable**

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

If any of the above items are missing, please contact your reseller.

System Requirements

ADSL Internet Service

Computer With:

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

D-LINK Click'n Connect Utility

Features

PPP (Point-to-Point Protocol) Security

The DSL-500B ADSL Router supports **PAP** (Password Authentication Protocol), **CHAP** (Challenge Handshake Authentication Protocol), and **MS-CHAP** for Point-to-Point Protocol connections.

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-500B allows multiple users on 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-500B supports TCP/IP protocol, the standard language used for Internet access. It is compatible with access servers manufactured by major vendors.

RIP-1/RIP-2 (Routing Information Protocol)

The DSL-500B 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.

ATM (Asynchronous Transfer Mode)

The DSL-500B supports Bridged Ethernet over ATM (RFC1483), IP over ATM (RFC1577), and PPP over ATM (RFC 2364).

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.

G.hs (Auto-handshake)

This allows the Router to automatically choose either the G.lite or G.dmt ADSL connection standards.

High Performance

The Router provides up to 8 Mbps downstream bit rate using the G.dmt standard.

Full Network Management

The DSL-500B incorporates SNMP (Simple Network Management Protocol) support for web-based management and text-based network management.

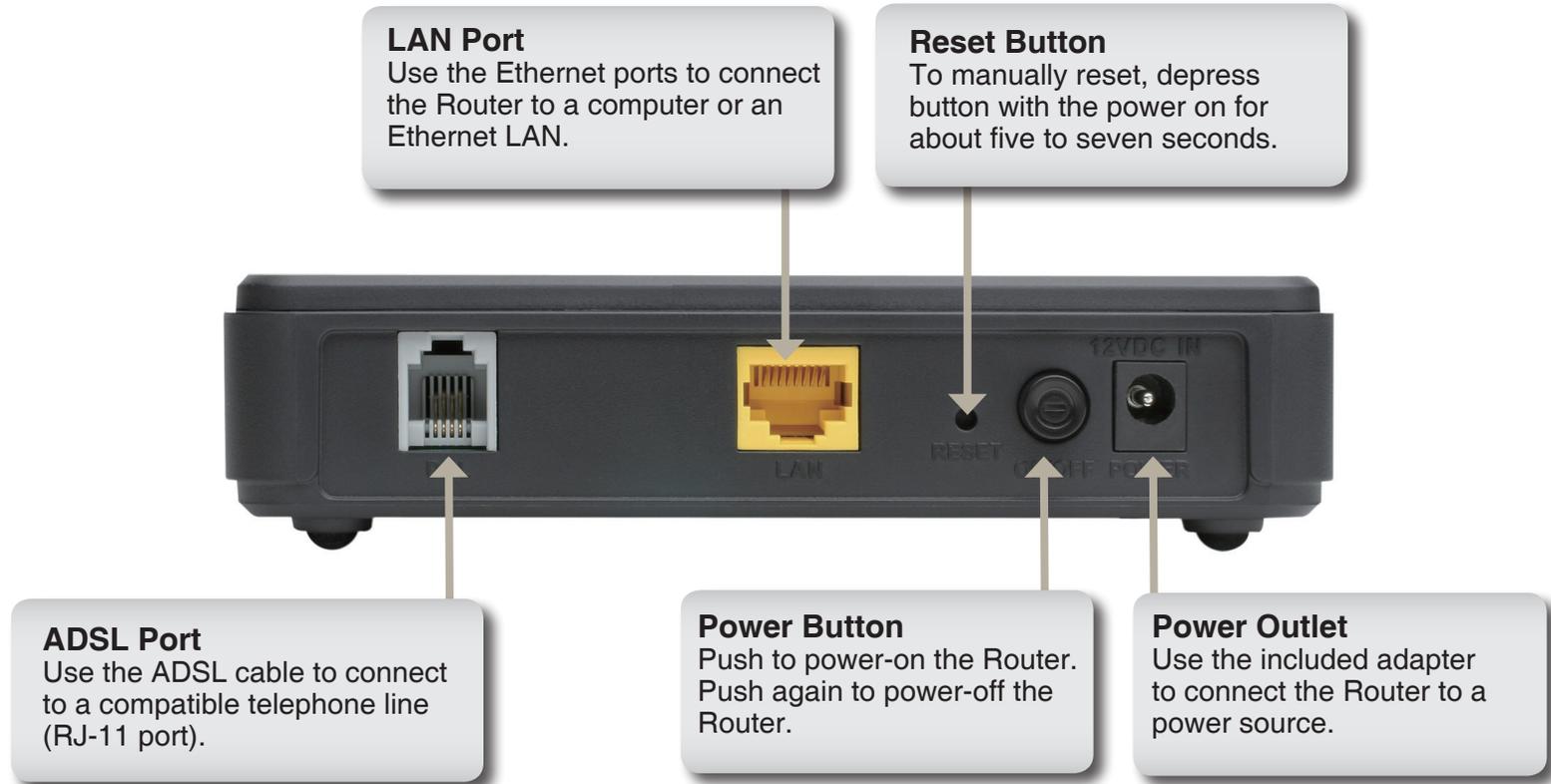
Telnet Connection

Telnet enables a network manager to access the Router's management software remotely.

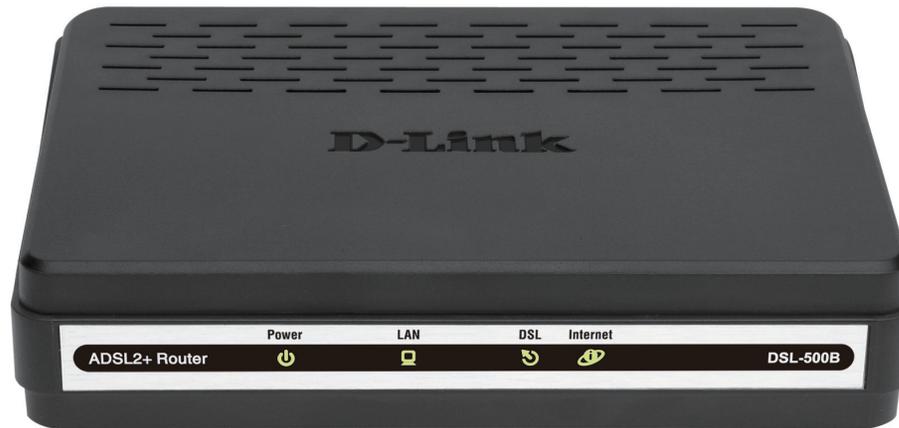
Easy Installation

The DSL-500B 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.

Rear Panel (Connections)



Front Panel (LED Indicators)



LED	Color	Status	Description
Power	Green	Off	Power not supplied.
		On	Power is supplied.
	Red	On	During power on self-test, or software update
LAN	Green	Off	No LAN link.
		Blink	Data is being transmitted through the LAN interface.
		On	LAN link is established and active.
DSL	Green	Off	DSL line is disconnected.
		Blink	DSL line is initializing.
		On	DSL line is connected.
Internet	Green	Off	The device is running under Bridge mode, a DSL connection is not present, or the power is off.
		Blink	DSL traffic is flowing.
		On	The device is connected, and has an IP.
	Red	On	The device attempted to connect, but failed.

Overview

This section will walk you through the installation process. Placement of the 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 ADSL Router in a location where it can be easily connected to Ethernet devices, the telephone line as well as to a power source.

Installation Notes

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.

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-500B uses an HTML-based web interface for setup and management. The web configuration manager may be accessed using any operating system capable of running web browser software, including Windows 98 SE, Windows ME, Windows 2000, Windows XP, and Windows Vista.

Web Browser

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

Ethernet Port (NIC Adapter)

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

Additional Software

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

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

All connections to the Internet require a unique global IP address. For bridged connections, the global IP settings must reside in a TCP/IP enabled device on the LAN side of the bridge, such as a PC, a server, a gateway device such as a router or similar firewall hardware. The IP address can be assigned in a number of ways. Your network service provider will give you instructions about any additional connection software or network configuration that may be required.

Information Required from 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 configuration (Connection Type settings listed in parenthesis):

- PPPoE/PPoA (PPPoE LLC, 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 the DSL-500B

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**. This name cannot be changed.

Password

This is the **Password** you will be prompted to enter when you access the Router's management interface. The default **Password** is **admin**. For security purposes, ensure to change this password.

LAN IP Addresses for the DSL-500B

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 **192.168.254.254**. 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-500B

This is the subnet mask used by the DSL-500B, 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 Network Interface Card (NIC)

If your computer has an Ethernet NIC, you can connect the DSL-500B to this Ethernet port using an Ethernet cable. You can also use the Ethernet port on the DSL-500B to connect to other computer or Ethernet device.

DHCP Client Status

Your DSL-500B ADSL Router is configured to be a DHCP server, by default. 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-500B will assign are from **192.168.254.1** to **192.168.254.253**. Your computer (or computers) needs to be configured to obtain an IP address automatically (that is, they must 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-500B ADSL Router.

Device Installation

The DSL-500B maintains two separate interfaces: ADSL (WAN) and an Ethernet (LAN). Place the Router in a location where it can be easily connected to Ethernet devices, the telephone line, and 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 of the device, should you ever need to view them for troubleshooting.

Power On

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

1. Connect the power adapter to the **Power** receptacle (12V DC, 1A) on the rear panel of the Router and plug the other end of the power adapter to a wall outlet or power strip.
2. Push the **On/Off** button on the rear panel of the Router to turn the power on.
3. The **Power** LED on the front panel will turn 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 Router will attempt to establish the ADSL connection, if the ADSL line is connected and the Router is properly configured, the ADSL LED will light up after several seconds. If this is your first time installing the device, some settings may need to be changed before the ADSL Router can establish a connection.

Factory Reset

The Router may be reset to the original factory default settings through the following actions.

1. Press and hold the reset button while the device is powered off using a paper clip or similar object.
2. Turn on the power and the router will restart. Observe the **Power** LED to verify.
3. Wait for 5~8 seconds and then release the reset button.
4. The device settings will be restored to the factory default IP address **192.168.254.254** and the subnet mask is **255.255.255.0**. The default username and password is **admin** and **admin**.

Note: A factory reset will erase the current configuration settings and reset them to the default settings.

After restarting your DSL-500B ADSL Router, log in to the router's web-based 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 crossover 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 crossover 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.

Connect Hub or Switch to Router

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 of the other MDI-X ports (1x, 2x, etc.) with a crossover cable.

Connect Computer to Router

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

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.

Web-based Configuration Utility

Step 1

Open a web browser such as Internet Explorer on your computer.

Step 2

Type **192.168.254.254** (DSL router default IP address) in the address bar. The login page will appear.

Step 3

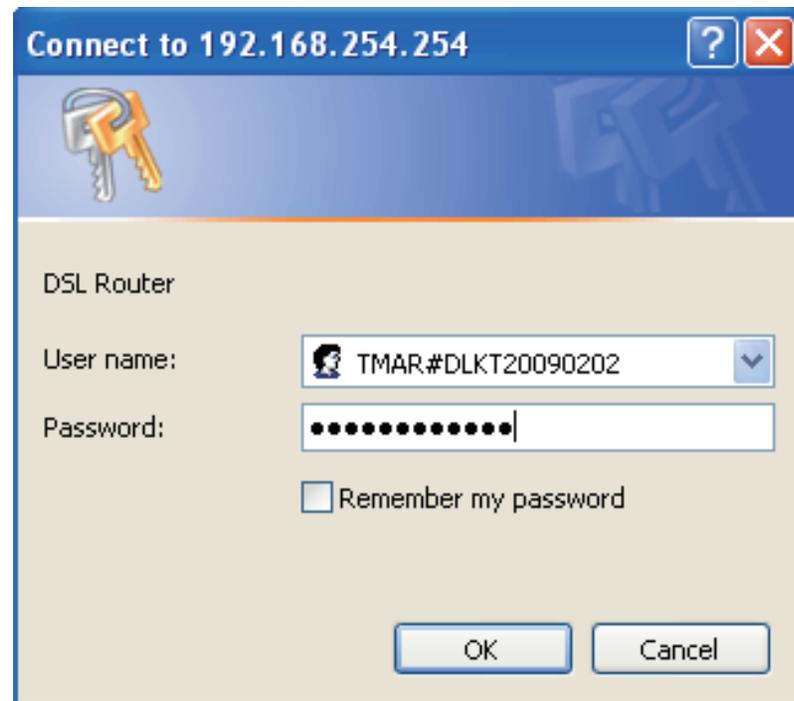
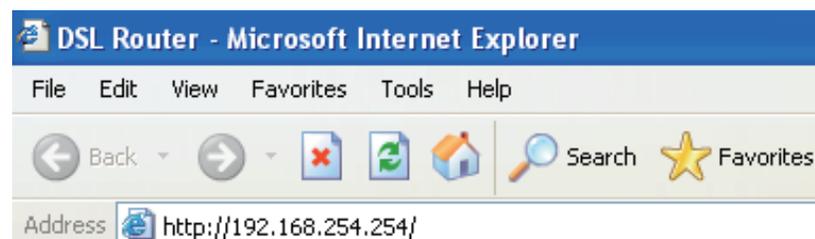
Enter a user name and the password. The default username and password of the super user are **admin** and **admin**. If you get a **Page Cannot be Displayed** error, please refer to the **Troubleshooting** section for information.

Note: It is recommended to change these default values after logging in to the DSL router for the first time.

Step 4

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

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



Quick Setup

This chapter describes the various menus used to configure and monitor the Router, including how to change IP settings and DHCP server setup.

Note: 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. For example, your ISP should inform you whether you are connected to the Internet by using a static or dynamic IP address, or the protocols, such as PPPOA or PPPoE, which you use to communicate over the Internet.

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

Setting Up VPI/VCI and QoS

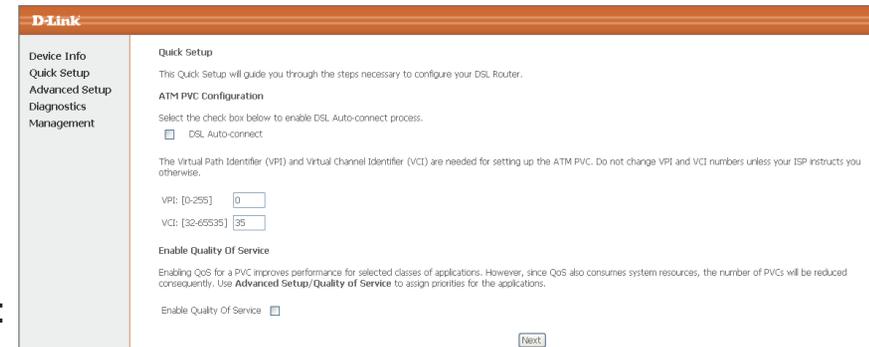
After logging in to the DSL router, if no PVC is configured previously and no default settings exist, the **Quick Setup** webpage will appear. This contains some basic configuration that is needed by ATM PVC. The following introduction guides you through the necessary steps to configure your DSL Router.

Based on your ISP's instructions, specify the following parameters:

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

Check the **DSL Auto-connect** box and then click **Next**.

If the ADSL connection is down, uncheck the **DSL Auto-connect** and then click **Next** to manually assign the VPI and VCI values.



The screenshot shows the D-Link Quick Setup interface. On the left is a navigation menu with options: Device Info, Quick Setup, Advanced Setup, Diagnostics, and Management. The main content area is titled 'Quick Setup' and includes instructions for configuring the DSL router. It features a section for 'ATM PVC Configuration' with a checkbox for 'DSL Auto-connect' (checked), and input fields for 'VPI: [0-255]' (set to 0) and 'VCI: [32-65535]' (set to 35). Below this is a section for 'Enable Quality Of Service' with a checkbox (unchecked) and a 'Next' button at the bottom right.

Selecting the Connection Type and Encapsulation Mode

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

PPP over ATM (PPPoA)

PPPoA Encapsulation Mode: VC/MUX, LLC/ENCAPSULATION

PPP over Ethernet (PPPoE)

PPPoE Encapsulation Mode: LLC/SNAP-BRIDGING, VC/MUX

MAC Encapsulation Routing (MER)

MER Encapsulation Mode: LLC/SNAP-BRIDGING, VC/MUX

IP over ATM (IPoA)

IPoA Encapsulation Mode: LLC/SNAP-ROUTING, VC/MUX

Bridging

Bridging Encapsulation Mode: LLC/SNAP-BRIDGING, VC/MUX

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

Connection Type

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

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

Encapsulation Mode

LLC/SNAP-BRIDGING ▼

Back Next

PPP over ATM (PPPoA)

Step 1

In the PVC and its QoS configuration page, configure a PVC and its QoS.

Step 2

In the Internet connection type and encapsulation mode page, set the **Connection Type** to **PPP over ATM (PPPoA)** and select the desired **Encapsulation Mode** from the drop-down box and click **Next** to continue.

Step 3

The **PPP Username and Password** page will appear. Update the following fields and click **Next** to continue.

Your ISP should provide you with the following information:

- PPP Username
- PPP Password
- Authentication Method

You can also select another service function as follows:

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

Connection Type

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

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

Encapsulation Mode

VC/MUX

Back Next

PPP Username and Password

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

PPP Username:
 PPP Password:
 Authentication Method:

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

Back Next

Step 4

To use IGMP service on PPPoA PVC, check the **Enable IGMP Multicast** and the **Enable WAN Service** box and enter a **Service Name**.

Note: Do not modify the default MTU value setting unless your ISP advises you to change it.

Click **Next** to continue.

Enable IGMP Multicast, and WAN Service

Enable IGMP Multicast

Enable WAN Service

Service Name

PPPoE Link Setting

MTU

[Back](#) [Next](#)

Step 5

Enter the **IP Address** and **Subnet Mask** for the LAN interface. In addition, you can either enable or disable the DHCP server.

To enable the DHCP server, enter a start and end IP address, and the Subnet Mask of the Router. You may also choose to change the default value of the lease time.

Click **Next** to continue.

Device Setup

Configure the DSL Router IP Address and Subnet Mask for LAN interface.

IP Address:

Subnet Mask:

Disable DHCP Server

Enable DHCP Server

Start IP Address:

End IP Address:

Subnet Mask:

Leased Time (hour):

Configure the second IP Address and Subnet Mask for LAN interface

[Back](#) [Next](#)

PPPoA Summary

This summary window allows you to confirm your PPPoA settings.

Click **Save/Reboot** to save your new PPP over ATM settings and restart the Router.

WAN Setup - Summary

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

PORT / VPI / VCI:	0 / 0 / 35
Connection Type:	PPPoA
Service Name:	pppoa_0_0_35_1
Service Category:	UBR
IP Address:	Automatically Assigned
Service State:	Enabled
NAT:	Enabled
Firewall:	Enabled
IGMP Multicast:	Disabled
Quality Of Service:	Disabled

Click "Save/Reboot" to save these settings and reboot router. Click "Back" to make any modifications.
NOTE: The configuration process takes about 1 minute to complete and your DSL Router will reboot.

[Back](#) [Save/Reboot](#)

PPP over Ethernet (PPPoE)

Step 1

In the PVC and its QoS configuration page, configure a PVC and its QoS.

Step 2

In the Internet connection type and encapsulation type page, set the **Connection Type** to **PPP over Ethernet (PPPoE)** and select the **Encapsulation Mode** from the drop-down box and click **Next** to continue.

Step 3

The **PPP Username and Password** page will appear. Update the following fields and click **Next** to continue.

Your ISP should provide you with the following information:

- PPP Username
- PPP Password
- Authentication Method

You can also select another service function as follows:

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

Connection Type

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

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

Encapsulation Mode

LLC/SNAP-BRIDGING ▼

Back Next

PPP Username and Password

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

PPP Username:
 PPP Password:
 PPPoE Service Name:
 Authentication Method:
 MTU[1-65535]:

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

Back Next

Step 4

To use IGMP service on PPPoE pvc, check the **Enable IGMP Multicast** and the **Enable WAN Service** box and enter a **Service Name**.

Note: Do not modify the default MTU value setting unless your ISP advises you to change it.

Click **Next** to continue.

Enable IGMP Multicast, and WAN Service

Enable IGMP Multicast

Enable WAN Service

Service Name

PPPoE Link Setting

MTU

[Back](#) [Next](#)

Step 5

Enter the **IP Address** and **Subnet Mask** for the LAN interface. In addition, you can either enable or disable the DHCP server.

To enable the DHCP server, enter a start and end IP address, and the Subnet Mask of the Router. You may also choose to change the default value of the lease time.

Click **Next** to continue.

Device Setup

Configure the DSL Router IP Address and Subnet Mask for LAN interface.

IP Address:

Subnet Mask:

Disable DHCP Server

Enable DHCP Server

Start IP Address:

End IP Address:

Subnet Mask:

Leased Time (hour):

Configure the second IP Address and Subnet Mask for LAN interface

[Back](#) [Next](#)

PPPoE Summary

This summary window allows you to confirm your PPPoE settings.

Click **Save/Reboot** to save your new PPPoE settings and restart the Router.

WAN Setup - Summary

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

PORT / VPI / VCI:	0 / 0 / 35
Connection Type:	PPPoE
Service Name:	pppoe_0_0_35_1
Service Category:	UBR
IP Address:	Automatically Assigned
Service State:	Enabled
NAT:	Enabled
Firewall:	Enabled
IGMP Multicast:	Disabled
Quality Of Service:	Disabled

Click "Save/Reboot" to save these settings and reboot router. Click "Back" to make any modifications.
NOTE: The configuration process takes about 1 minute to complete and your DSL Router will reboot.

[Back](#) [Save/Reboot](#)

MAC Encapsulation Routing (MER)

Step 1

In the PVC and its QoS configuration page, configure a PVC and its QoS.

Step 2

In the Internet connection type and encapsulation type page, set the **Connection Type** to **MAC Encapsulation Routing (MER)** and select the **Encapsulation Mode** from the drop-down box and click **Next** to continue.

Step 3

The WAN IP configuration page will appear. Select the service function as follows:

- Obtain an IP address automatically (use DHCP to obtain WAN IP)
- Use the following IP address (use static WAN IP)
- Obtain default gateway automatically (use DHCP to obtain gateway IP)
- Use the following default gateway (use static gateway IP)
- Obtain DNS server addresses automatically (use DHCP to obtain DNS server IP)
- Use the following DNS server addresses (use static DNS server IP)

Click **Next** to continue.

Connection Type

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

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

Encapsulation Mode

LLC/SNAP-BRIDGING ▾

Back Next

WAN IP Settings

Enter information provided to you by your ISP to configure the WAN IP settings.
 Notice: DHCP can be enabled for PVC in MER mode or IP over Ethernet as WAN interface if "Obtain an IP address automatically" is chosen. Changing the default gateway or the DNS effects the whole system. Configuring them with static values will disable the automatic assignment from DHCP or other WAN connection.
 If you configure static default gateway over this PVC in MER mode, you must enter the IP address of the remote gateway in the "Use IP address". The "Use WAN interface" is optional.

- Obtain an IP address automatically
- Use the following IP address:
 WAN IP Address:
 WAN Subnet Mask:
- Obtain default gateway automatically
- Use the following default gateway:
 Use IP Address:
 Use WAN Interface: mer_0_0_35/ ▾
- Obtain DNS server addresses automatically
- Use the following DNS server addresses:
 Primary DNS server:
 Secondary DNS server:

Back Next

Step 4

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

In the MER mode, you can configure the following functions:

- Enable NAT
- Enable Firewall

Click **Next** to continue.

Step 5

Enter the **IP Address** and **Subnet Mask** for the LAN interface. In addition, you can either enable or disable the DHCP server.

To enable the DHCP server, enter a start and end IP address, and the Subnet Mask. You may also choose to change the default value of the lease time. Click **Next** to continue.

Network Address Translation Settings

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

Enable NAT

Enable Firewall

Enable IGMP Multicast, and WAN Service

Enable IGMP Multicast

Enable WAN Service

Service Name:

[Back](#) [Next](#)

Device Setup

Configure the DSL Router IP Address and Subnet Mask for LAN interface.

IP Address:

Subnet Mask:

Disable DHCP Server

Enable DHCP Server

Start IP Address:

End IP Address:

Subnet Mask:

Leased Time (hour):

Configure the second IP Address and Subnet Mask for LAN interface

[Back](#) [Next](#)

MER Summary

This summary window allows you to confirm your MER settings.

Click **Save/Reboot** to save your new MER settings and restart the Router.

WAN Setup - Summary

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

PORT / VPI / VCI:	0 / 0 / 35
Connection Type:	MER
Service Name:	mer_0_0_35
Service Category:	UBR
IP Address:	Automatically Assigned
Service State:	Enabled
NAT:	Enabled
Firewall:	Enabled
IGMP Multicast:	Disabled
Quality Of Service:	Disabled

Click "Save/Reboot" to save these settings and reboot router. Click "Back" to make any modifications.
NOTE: The configuration process takes about 1 minute to complete and your DSL Router will reboot.

[Back](#) [Save/Reboot](#)

IP over ATM (IPoA)

Step 1

In the PVC and its QoS configuration page, configure a PVC and its QoS.

Step 2

In the Internet connection type and encapsulation type page, set the **Connection Type** to IP over ATM (IPoA) and select the **Encapsulation Mode** from the drop-down box.

Click **Next** to continue.

Step 3

The **WAN IP configuration** page will appear.

You can select the following service functions:

- Use the following IP address (Static WAN IP)
- Use the following default gateway (Static gateway IP)
- Use the following DNS server addresses (Static DNS server IP)

Connection Type

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

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

Encapsulation Mode

LLC/SNAP-ROUTING ▾

Back Next

WAN IP Settings

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

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

WAN IP Address:
 WAN Subnet Mask:

Use the following default gateway:
 Use IP Address:
 Use WAN Interface:

Use the following DNS server addresses:
 Primary DNS server:
 Secondary DNS server:

Back Next

Step 4

Click **Next** and the IPoA IGMP and WAN function configuration page will appear.

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

In the IPoA mode, you can configure the following functions:

- Enable NAT
- Enable Firewall

Click **Next** to continue.

Step 5

Enter the **IP Address** and **Subnet Mask** for the LAN interface. In addition, you can either enable or disable the DHCP server.

To enable the DHCP server, enter a start and end IP address, and the Subnet Mask. You may also choose to change the default value of the lease time.

Click **Next** to continue.

Network Address Translation Settings

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

Enable NAT

Enable Firewall

Enable IGMP Multicast, and WAN Service

Enable IGMP Multicast

Enable WAN Service

Service Name:

[Back](#) [Next](#)

Device Setup

Configure the DSL Router IP Address and Subnet Mask for LAN interface.

IP Address:

Subnet Mask:

Disable DHCP Server

Enable DHCP Server

Start IP Address:

End IP Address:

Subnet Mask:

Leased Time (hour):

Configure the second IP Address and Subnet Mask for LAN interface

[Back](#) [Next](#)

IPoA Summary

This summary window allows you to confirm your IPoA settings.

Click **Save/Reboot** to save your new IPoA settings and restart the Router.

WAN Setup - Summary

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

PORT / VPI / VCI:	0 / 0 / 35
Connection Type:	IPoA
Service Name:	ipoa_0_0_35
Service Category:	UBR
IP Address:	10.1.1.15
Service State:	Enabled
NAT:	Enabled
Firewall:	Enabled
IGMP Multicast:	Disabled
Quality Of Service:	Disabled

Click "Save/Reboot" to save these settings and reboot router. Click "Back" to make any modifications.
NOTE: The configuration process takes about 1 minute to complete and your DSL Router will reboot.

[Back](#)

[Save/Reboot](#)

Bridging

Step 1

In the PVC and its QoS configuration page, configure a PVC and its QoS.

Step 2

In the Internet connection type and encapsulation type page, set the **Connection Type** to **Bridging** and select the **Encapsulation Mode**. Click **Next** to continue.

Step 3

The Bridging service configuration page will appear. Select the **Enable Bridge Service** check box and then enter the **Service Name**.

Click **Next** to continue.

Step 4

Enter the Router's **IP Address** and **Subnet Mask** for your LAN, and then click **Next** to continue.

Connection Type

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

PPP over ATM (PPPoA)

PPP over Ethernet (PPPoE)

MAC Encapsulation Routing (MER)

IP over ATM (PoA)

Bridging

Encapsulation Mode

LLC/SNAP-BRIDGING

Back Next

Unselect the check box below to disable this WAN service

Enable Bridge Service:

Service Name:

Back Next

Device Setup

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

IP Address:

Subnet Mask:

Back Next

Bridging Summary

This summary window allows you to confirm your Bridge settings.

Click **Save/Reboot** to save your new **Bridging** settings and restart the Router.

WAN Setup - Summary

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

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

Click "Save/Reboot" to save these settings and reboot router. Click "Back" to make any modifications.
NOTE: The configuration process takes about 1 minute to complete and your DSL Router will reboot.

[Back](#) [Save/Reboot](#)

DSL Router Device Information

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

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

Summary of Device Information

Select **Summary** and the **Device Info** page will appear. This displays the current status of your DSL connection, including the software version, LAN IP address, and DNS server address.

- **LAN IP Address:** This is the management IP address.
- **Default Gateway:** In the bridging mode there is no gateway address. In other modes, it is the address of the uplink equipment, for example, PPPoE/PPPoA.
- **DNS Servers:** In the PPPoE and PPPoA mode, the Primary and Secondary DNS Server addresses are obtained from the uplink equipment. In the Bridging mode, there are no DNS Server address and you can manually enter the information.

D-Link

Device Info

Board ID:	DSL-500B
Software Version:	BCM-1.1.TM-20090217
Bootloader (CFE) Version:	1.0.37-10.3

This information reflects the current status of your DSL connection.

Line Rate - Upstream (Kbps):	
Line Rate - Downstream (Kbps):	
LAN IP Address:	192.168.254.254
MAC Address:	02-10-18-63-32-00
Default Gateway:	
Primary DNS Server:	192.168.254.254
Secondary DNS Server:	192.168.254.254

WAN Interface Information

Select **Device Info > WAN**. The **WAN Info** page will appear. It displays the current status of your WAN connection, depending on the selected connection type.

WAN Info

Port/VPI/VCI	Con. ID	Category	Service	Interface	Protocol	Igmp	QoS	State	Status	IP Address
0/0/35	1	UBR	br_0_0_35	nas_0_0_35	Bridge	N/A	Enabled	Enabled	ADSL Link Down	
0/8/35	1	UBR	pppoe_0_8_35_1	ppp_0_8_35_1	PPPoE	Disabled	Enabled	Enabled	ADSL Link Down	

Statistics - LAN

Select **Device Info > Statistics > LAN**. The **Statistics-LAN** page will appear. This page displays the Router's LAN statistics.

Click **Reset Statistics** to refresh these statistics.

Statistics -- LAN

Interface	Received				Transmitted			
	Bytes	Pkts	Errs	Drops	Bytes	Pkts	Errs	Drops
Ethernet	126285	999	0	0	297923	737	0	0

Reset Statistics

Statistics - WAN

Select **Device Info > Statistics > WAN**. The **Statistics-WAN** page will appear. This page displays the Router's WAN statistics.

Click **Reset Statistics** to refresh these statistics.

Statistics -- WAN

Service	VPI/VCI	Protocol	Interface	Received				Transmitted					
				Bytes	Pkts	Errs	Drops	Bytes	Pkts	Errs	Drops		
br_0_0_35	0/0/35	Bridge	nas_0_0_35	0	0	0	0	0	0	0	0	0	344
pppoe_0_8_35_1	0/8/35	PPPoE	ppp_0_8_35_1	0	0	0	0	0	0	0	0	0	0

Reset Statistics

Statistics - ATM

Select **Device Info > Statistics > ATM**. The **Statistics-ATM** page will appear. This page displays the Router's ATM statistics.

Click **Reset Statistics** to refresh these statistics.

ATM Interface Statistics

In Octets	Out Octets	In Errors	In Unknown	In Hec Errors	In Invalid Vpi Vci Errors	In Port Not Enable Errors	In PFI Errors	In Idle Cells	In Circuit Type Errors	In OAM RM CRC Errors	In GFC Errors
0	0	0	0	0	0	0	0	0	0	0	0

AAL5 Interface Statistics

In Octets	Out Octets	In Ucast Pkts	Out Ucast Pkts	In Errors	Out Errors	In Discards	Out Discards
0	0	0	0	0	0	0	0

AAL5 VCC Statistics

VPI/VCI	CRC Errors	SAR Timeouts	Overized SDUs	Short Packet Errors	Length Errors
0/35	0	0	0	0	0
8/35	0	0	0	0	0

Reset Statistics

Statistics - ADSL

Select **Device Info > Statistics > ADSL**. The **Statistics - ADSL** page will appear. This page displays the Router's ADSL statistics. Click **Reset Statistics** to refresh these statistics.

Click **ADSL BER Test** to access the ADSL Bit Error Rate Test window.

ADSL BER Test

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

Click **ADSL BER Test** to perform a bit error rate (BER) test on the DSL line.

The tested time (in seconds) can be 1, 5, 10, 20, 60, 120, 180, 240, 300, or 360. Select a time and click **Start**.

The following pages will appear.

Statistics -- ADSL

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

ADSL BER Test - Start

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

Select the test duration below and click "Start".

Tested Time (sec):

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

ADSL BER Test - Result

The ADSL BER test completed successfully.

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

Close

Route Table Information

Select **Device Info > Route**. The **Device-Route** page will appear if the system is in the default configuration.

Device Info -- Route

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

Destination	Gateway	Subnet Mask	Flag	Metric	Service	Interface
192.168.254.0	0.0.0.0	255.255.255.0	U	0		br0

ARP Table Information

Select **Device Info > ARP**. This page displays information on the Address Resolution Protocol (ARP).

Device Info -- ARP

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

DHCP Information

Select **Device Info > DHCP**. This page displays the DHCP lease information.

Device Info -- DHCP Leases

Hostname	MAC Address	IP Address	Expires In
----------	-------------	------------	------------

Advanced Setup

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

WAN Configuration

Select **Advanced Setup > WAN**. This page allows you to modify and configure the WAN interface.

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

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

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

If you are setting up the WAN interface for the first time, click **Add** and the **ATM PVC Configuration** page will appear.

D-Link

Device Info
Advanced Setup
 WAN
 LAN
 NAT
 Security
 Quality of Service
 Routing
 DNS
 DSL
 Diagnostics
 Management

Wide Area Network (WAN) Setup

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

Port/Vpi/Vci	Con. ID	Category	Service	Interface	Protocol	Icmp	QoS	State	Remove	Edit
0/0/35	1	UBR	br_0_0_35	nas_0_0_35	Bridge	N/A	Enabled	Enabled	<input type="checkbox"/>	Edit
0/8/35	1	UBR	pppoe_0_8_35_1	ppp_0_8_35_1	PPPoE	Disabled	Enabled	Enabled	<input type="checkbox"/>	Edit

Add Remove Save/Reboot

In this page, you can modify VPI/VCI, service categories, and QoS.

VPI: Virtual path between two points in an ATM network. Its valid value range is from 0 to 255.

VCI: Virtual channel between two points in an ATM network. Its valid value range is from 32 to 65535 (1 to 31 are reserved for known protocols).

Service Category: UBR Without PCR/UBR With PCR/CBR/Non Realtime VBR/Realtime VBR.

Enable Quality Of Service: Enable or disable QoS.

After the modifications, click **Next** and the **Connection Type** page will appear.

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

Select the desired **Encapsulation Mode** from the drop-down box and then click **Next** to continue.

Refer to the **Quick Setup** section for more information on the five connection types available in the Router.

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

VPI: [0-255]

VCI: [32-65535]

Service Category:

Connection Type

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

PPP over ATM (PPPoA)

PPP over Ethernet (PPPoE)

MAC Encapsulation Routing (MER)

IP over ATM (IPoA)

Bridging

Encapsulation Mode

LAN Configuration

Select **Advanced Setup > LAN** and the **Local Area Network (LAN) Setup** page will appear. Here you can modify and configure the IP Address, DHCP Server and enable IGMP Snooping.

Note: The most convenient way to manage your network is to use the default settings along with the DHCP services. In order to use the Router for DHCP settings, the IP address used for DHCP must be compatible with the IP address of the Router. The IP addresses available in the DHCP IP address pool will change automatically if you change the IP address of the Router.

When you are finished, click either **Save** to save the LAN configuration or **Save/Reboot** to save the data and reboot the Router.

Local Area Network (LAN) Setup

Configure the DSL Router IP Address and Subnet Mask for LAN interface. Save button only saves the LAN configuration data. Save/Reboot button saves the LAN configuration data and reboots the router to make the new configuration effective.

IP Address:
Subnet Mask:

- Enable IGMP Snooping
 Standard Mode
 Blocking Mode

Disable DHCP Server
 Enable DHCP Server
Start IP Address:
End IP Address:
Subnet Mask:
Leased Time (hour):

Reserve IP Address

Choose "Edit Reserved IP Address List" to configure Reserved IP Address List.
NOTE1: You can max reserve 10 ip address and special mac.
NOTE2: When you added a new reserve ip. You must reboot system to active it.

[Edit Reserved IP Address List](#)

- Configure the second IP Address and Subnet Mask for LAN interface

NAT

Note: You must enable the NAT service when you configure the WAN connection at first. The NAT item will then appear in the **Advanced Setup** directory. In the pure bridging mode, there is no NAT service.

Overview - Setting up the NAT Function

The DSL router is equipped with the Network Address Translation (NAT) function. With address mapping, several users in the local network can access the Internet via one or more public IP addresses. All the local IP addresses are assigned to the public IP address of the router by default.

One of the characteristics of NAT is that data from the Internet is not allowed into the local network unless it is explicitly requested by one of the PCs in the network. Most Internet applications can run behind the NAT firewall without any problems. For example, if you request Internet pages or send and receive e-mails, the request for data from the Internet comes from a PC in the local network, and so the router allows the data to pass through. The router opens one specific port for the application. A port in this context is an internal PC address, via which the data is exchanged between the Internet and a client on a PC in the local network. Communicating via a port is subject to the rules of a particular protocol (TCP or UDP).

If an external application tries to send a call to a PC in the local network, the router blocks it. There is no open port via which the data could enter the local network. Some applications, such as games on the Internet, require several links (that is, several ports), so that players can communicate with each other. In addition, these applications must also be permitted to send requests from other users on the Internet to users in the local network. These applications cannot run if NAT is activated.

Using port forwarding (the forwarding of requests to particular ports), the router is forced to send requests from the Internet for a certain service, for example, a game, to the appropriate port(s) on the PC on which the game is running. Port triggering is a special variant of port forwarding. Unlike port forwarding, the DSL router forwards the data from the port block to the PC which has previously sent data to the Internet via a certain port (trigger port). This means that approval for the data transfer is not tied to one specific PC in the network, but rather to the port numbers of the required Internet service.

Where configuration is concerned, you must define a so-called trigger port for the application and also the protocol (TCP or UDP) that this port uses. You then assign the public ports that are to be opened for the application to this trigger port. The router checks all outgoing data for the port number and protocol. If it identifies a match of port and protocol for a defined trigger port, then it opens the assigned public ports and notes the IP address of the PC that sent the data. If data comes back from the Internet via one of these public ports, the router allows it to pass through and directs it to the appropriate PC. A trigger event always comes from a PC within the local network. If a trigger port is addressed from outside, the router simply ignores it.

Note:

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

NAT - Virtual Server Setup

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

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

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

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

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

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

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

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

To accomplish this, do as follows:

Step 1

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

Step 2

Specify 8080 in the Forward to Port field.

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

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

Virtual servers are configured for this purpose.

Step 9

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

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

Select the protocol for the service you are providing from the Protocol drop-down list. Under External Port, enter the port number of the service you are providing. In the Internal Port field, enter the internal port number, to which service requests are to be forwarded. In the Local IP Address field, enter the IP address of the PC that provides the service.

Example

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

Deleting Port Forwarding

Step 1

Select the **Remove** check box.

Step 2

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

Port Triggering

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

Adding Port Triggering

Step 1

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

Step 2

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

Step 3

Trigger Port Start and Trigger Port End: Enter the port that is to be monitored for outgoing data traffic.

Trigger Protocol: Select the protocol that is to be monitored for outgoing data traffic.

Open Protocol: Select the protocol that is to be allowed for incoming data traffic.

Open Port Start and Open Port End: Enter the port that is to be opened for incoming traffic.

Step 4

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

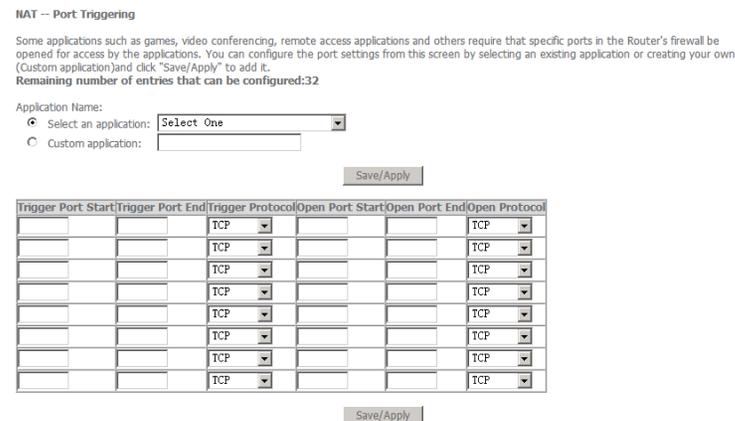
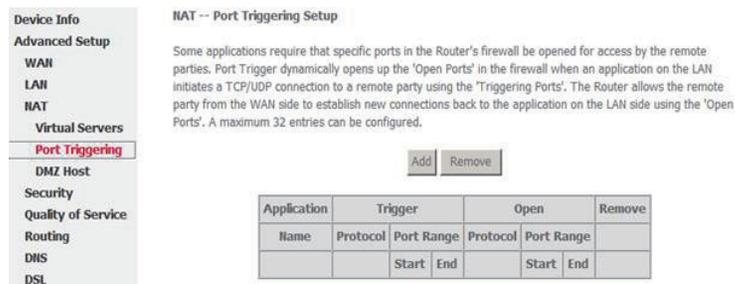
Removing Port Triggering

Step 1

Select the **Remove** check box.

Step 2

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



DMZ Host

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

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

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

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

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

Adding a DMZ Host

Step 1

To set up a PC as a DMZ host, select **Advanced Setup > NAT > DMZ Host**.

Step 2

Enter the local IP address of the PC that is to be enabled as an exposed host.

Step 3

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

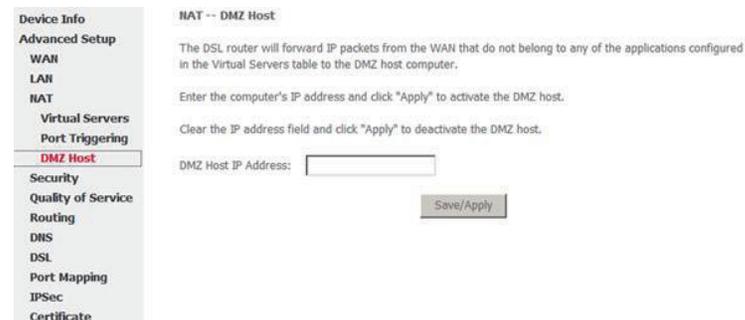
Remove DMZ host

Step 1

Clear the DMZ Host Address.

Step 2

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



Security

Select **Advanced Setup > Security > IP Filtering**. The **Outgoing IP Filtering Setup** page will appear.

By default, the firewall is enabled. The firewall is used to block data transmissions between the Internet and your PC. It serves as a security gate and permits only authorized traffic to be sent to the LAN.

Outgoing IP Filtering Setup

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

Choose Add or Remove to configure outgoing IP filters.

Filter Name	Protocol	Source Address / Mask	Source Port	Dest. Address / Mask	Dest. Port	DSCP. Mark	Remove
							<input type="button" value="Add"/> <input type="button" value="Remove"/>

Click **Add** to create an IP Filter Rule.

Outgoing IP Filtering Setup

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

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

Add IP Filter -- Outgoing

The 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 'Save/Apply' to save and activate the filter.

Filter Name:

Protocol:

Source IP address:

Source Subnet Mask:

Source Port (port or port:port):

Destination IP address:

Destination Subnet Mask:

Destination Port (port or port:port):

DSCP Mark:

Incoming IP Filtering Setup

Select **Security > IP Filtering > Incoming**. The **Incoming IP Filtering Setup** page will appear.

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

Click **Add** and the **Add IP Filter- Incoming** page will appear. In this page, you can create a filter rule to identify incoming IP traffic by specifying a new filter name and at least one condition. All specified conditions in this filter rule must comply with the rule.

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

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

Incoming IP Filtering Setup

By default, all incoming IP traffic from the WAN is blocked when the firewall is enabled. However, some IP traffic can be **ACCEPTED** by setting up filters.

Choose Add or Remove to configure incoming IP filters.

Filter Name	VPI/VCI	Protocol	Source Address / Mask	Source Port	Dest. Address / Mask	Dest. Port	DSCP. Mark	Remove
								<input type="button" value="Add"/> <input type="button" value="Remove"/>

Add IP Filter -- Incoming

The screen allows you to create a filter rule to identify incoming 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 'Save/Apply' to save and activate the filter.

Filter Name:

Protocol:

Source IP address:

Source Subnet Mask:

Source Port (port or port:port):

Destination IP address:

Destination Subnet Mask:

Destination Port (port or port:port):

DSCP Mark:

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_8_35_1/ppp_0_8_35_1

MAC Filtering Setup

Select **Security > MAC Filtering**, and the **MAC filtering Setup** page will appear.

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

Click **Change Policy** to change the MAC Filtering Global Policy from **FORWARDED** to **BLOCKED**.

Click **YES** to change the MAC filtering global policy from **FORWARDED** to **BLOCKED**. Click **NO** to cancel.

Change MAC Filtering Global Policy

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

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

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

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

Click **Save/Apply** and the MAC Filtering Setup page will appear.

Add MAC Filter

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.

Protocol Type:

Destination MAC Address:

Source MAC Address:

Frame Direction:

WAN Interfaces (Configured in Bridge mode only)

- Select All
- br_0_8_35/has_0_8_35

Save/Apply

MAC Filtering Setup

MAC Filtering Global Policy: **FORWARDED**

Change Policy

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

Choose Add or Remove to configure MAC filtering rules.

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

Add Remove

Parental Control

Click **Security > Parental Control**. The **Time of Day Restrictions** page will appear.

Click **Add** to configure the **Time of Day Restriction**.

In this page, you can add time of day restriction to a special LAN device connected to the Router. The **Browser's MAC Address** automatically displays the MAC address of the LAN device where the browser is running. To restrict another LAN device, click **Other MAC Address** and enter the MAC address of the another LAN device.

Also select the day and the start and end blocking time for the restriction.

URL Filter

Select **Advanced Setup > Parental Control** and then click **URL Filter**.

There are two types of URL list, **Exclude** and **Include**. If you selected **Exclude**, LAN devices will not be able to access the URL addresses in the list. And if you select **Include**, LAN devices will be able to access the URL addresses in the list. You must select one of these options to Add the URL address and then enter the **URL Address** and **Port Number**. The default port number is 80.

Click **Save/Apply** to add the URL filter.

Device Info

Advanced Setup

- WAN
- LAN
- NAT
- Security
- IP Filtering
- MAC Filtering
- Parental Control**
- URL Filter

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

Username	MAC	Mon	Tue	Wed	Thu	Fri	Sat	Sun	Start	Stop	Remove

Time of Day Restriction

This page adds time of day restriction to a special LAN device connected to the Router. The 'Browser's MAC Address' automatically displays the MAC address of the LAN device where the browser is running. To restrict other LAN device, click the "Other MAC Address" button and enter the MAC address of the other LAN device. To find out the MAC address of a Windows based PC, go to command window and type "ipconfig /all".

User Name:

Browser's MAC Address

Other MAC Address
(xx:xx:xx:xx:xx:xx)

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

Start Blocking Time (hh:mm)

End Blocking Time (hh:mm)

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

URL List Type: Exclude Include

Address	Port	Remove

Parental Control -- URL Filter Add

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

URL Address:

Port Number: (Default 80 will be applied if leave blank.)

Quality of Service

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

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

Enabling QoS

Select **Advanced Setup > Quality of Service**. In this page, you can perform QoS queue management configuration. By default, the system enables QoS and sets a default DSCP mark to automatically mark incoming traffic without reference to particular classifier.

QoS -- Queue Management Configuration

If Enable QoS checkbox is selected, choose a default DSCP mark to automatically mark incoming traffic without reference to a particular classifier. Click 'Save/Apply' button to save it.

Note: If Enable QoS checkbox is not selected, all QoS will be disabled for all interfaces.

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

Enable QoS

Select Default DSCP Mark:

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

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

QoS Queue Configuration

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

Select **Advanced Setup > Queue Config**. In this page, you can configure QoS queue. A maximum of 24 entries can be configured.

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

Note: Lower integer values for precedence imply higher priority for this queue relative to others. For example, add a QoS queue entry and allocate it to a specific network interface (PVC 0/0/35). Set integer values for queue precedence to 1.

Click **Add** to configure a QoS Queue configuration entry.

QoS Queue Configuration -- A maximum 16 entries can be configured. The QoS function has been disabled. Queues would not take effects.

Interfacename	Description	Precedence	Queue Key	Enable	Remove
<div style="display: flex; justify-content: space-between;">AddRemoveSave/Reboot</div>					

Step 1

This page allows you to configure a QoS queue entry and then assign it a specific network interface.

Queue Configuration Status: Set to enable or disable a QoS queue.

Queue: Select a specific network interface. When you have already selected a network interface, the specific network interface selected automatically allocates to the queue.

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

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

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

QoS Queue Configuration

The screen allows you to configure a QoS queue entry and assign it to a specific network interface. Each interface with QoS enabled will be allocated three queues by default. Each of the queues can be configured for a specific precedence. The queue entry configured here will be used by the classifier to place ingress packets appropriately. **Note: Lower integer values for precedence imply higher priority for this queue relative to others**
Click 'Save/Apply' to save and activate the filter.

Queue Configuration Status:

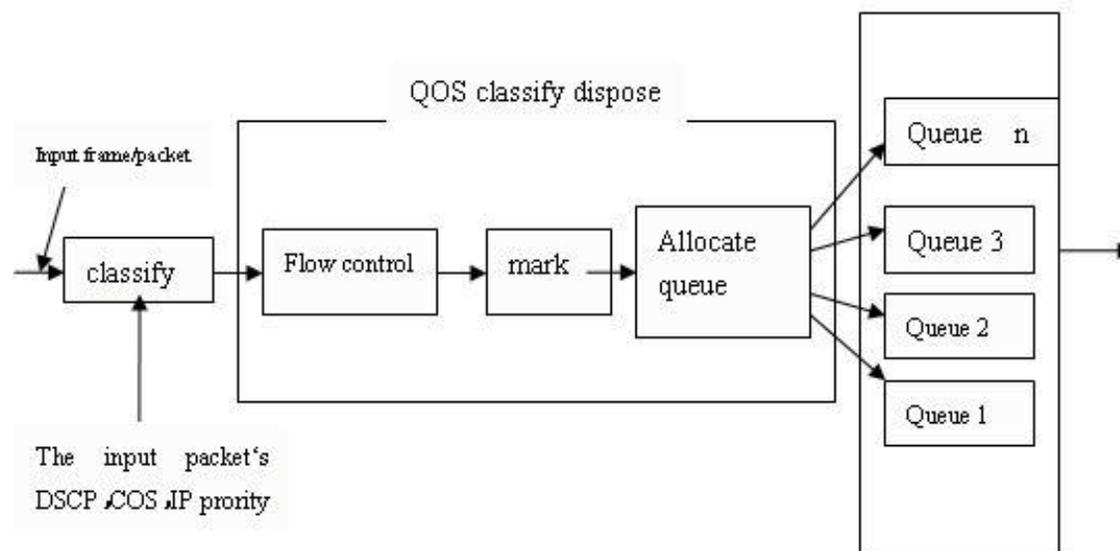
Queue:

Queue Precedence:

Save/Apply

QoS Classification

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



Select **Advanced Setup > QoS Classification**. In this page, you can configure network traffic classes.

Click **Add** to create a traffic class rule to classify the upstream traffic.

Traffic Class Name: Enter a name of the class.

Rule Order: Select order for queue.

Rule Status: Enable or disable this traffic class rule.

Assign Classification Queue: Select a classification queue.

Assign Differentiated Service Code Point (DSCP) Mark: Select a mark service that modifies the original packet IP header if all rules defined within the classification class are matched. (CS-Mark IP Precedence, AF-Assured Forwarding, EF-Expedited Forwarding)

Mark 802.1p if 802.1q is Enabled: Select an 802.1p priority number that serves as the 802.1p value.

There are two sets of classification rules. **Set-1** is based on different fields within TCP/UDP/IP layer plus physical LAN port; **Set-2** is based on IEEE 802.1p priority field.

Quality of Service Setup

Choose Add or Remove to configure network traffic classes.

MARK				TRAFFIC CLASSIFICATION RULES													
Class Name	DSCP Mark	Queue ID	802.1P Mark	Lan Port	Protocol	DSCP	Source Addr./Mask	Source Port	Dest. Addr./Mask	Dest. Port	Source MAC Addr./Mask	Destination MAC Addr./Mask	802.1P	Order	Enable/Disable	Remove	Edit
<input type="button" value="Add"/> <input type="button" value="Save/Apply"/>																	

Add Network Traffic Class Rule

The screen creates a traffic class rule to classify the upstream traffic, assign queue which defines the precedence and the interface and optionally overwrites 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 'Save/Apply' to save and activate the rule.

Traffic Class Name:

Rule Order: ▼

Rule Status: ▼

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.

Assign Classification Queue: ▼

Assign Differentiated Services Code Point (DSCP) Mark: ▼

Mark 802.1p if 802.1q is enabled on WAN: ▼

Specify Traffic Classification Rules

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

SET-1

Protocol: ▼

Differentiated Services Code Point (DSCP) Check: ▼

Source Subnet Mask:

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

Destination IP Address:

Destination Subnet Mask:

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: ▼

Set-1 rules contain the following:

Physical LAN Port: Select one among USB port, Ethernet ports and wireless port.

Protocol: Select one among TCP/UDP TCP UDP or ICMP protocols.

Source IP Address

Source subnet mask

UPD/TCP Source Port

Destination IP Address

Destination Subnet Mask

UPD/TCP destination port or a range of ports

Source Mac Address

Source Mac Mask

Destination Mac Address

Destination Mac Mask

Set-2 rules contain the following:

802.1p Priority: the 802.1p header includes a 3-bit prioritization field, which allows packets to be grouped into eight levels of priority (0-7), where level 7 is the highest one.

Click **Save/Apply** to save and activate this rule.

Add Network Traffic Class Rule

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 'Save/Apply' to save and activate the rule.

Traffic Class Name:
Rule Order:
Rule Status:

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.

Assign Classification Queue:
Assign Differentiated Services Code Point (DSCP) Mark:
Mark 802.1p if 802.1q is enabled on WAN:

Specify Traffic Classification Rules

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

SET-1
Protocol:
Differentiated Services Code Point (DSCP) Check:
IP Address:
Source Subnet Mask:
UDP/TCP Source Port (port or port:port):
Destination IP Address:
Destination Subnet Mask:
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:

QoS-DSCP Setting

In order to understand what is differentiated services code point (DSCP), you should be familiar with the differentiated services model (Diffserv).

Diffserv is a class of service (CoS) model that enhances best-effort Internet services via differentiating traffic by users, service requirements and other criteria. Packets are specifically marked, allowing network nodes to provide different levels of service via priority queuing or bandwidth allocation, or by choosing dedicated routes for specific traffic flows.

As displayed in following diagram, the IPV4 packet has a TOS field. Diffserv defines TOS field in IP packet headers referred to as DSCP. Hosts or routes that pass traffic to a Diffserv-enabled network typically mark each transmitted packet with an appropriate DSCP. The DSCP markings are used by Diffserv network routers to appropriately classify packets and to apply particular queue handing or scheduling behavior.

Layer 3 IPV4 Packet

Version/ Length	TOS (1 Word)	Length	ID	Offset/ Mark	TTL	Protocol	Checksum	IP-SA	IP-DA	Data
--------------------	-----------------	--------	----	-----------------	-----	----------	----------	-------	-------	------

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

7	6	5	4	3	2	1	0
IP Priority			Undefined				
DSCP						Flow Control	

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

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

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

Traffic Class Name:

Rule Order:

Rule Status:

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.

Assign Classification Queue:

Assign Differentiated Services Code Point (DSCP) Mark:

Mark 802.1p if 802.1q is enabled:

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:

Protocol:

Differentiated Services Code Point (DSCP) Check:

IP Address:

Source Subnet Mask:

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

Destination IP Address:

Quality of Service Setup
 Choose Add or Remove to configure network traffic classes.

If you disable WMM function in Wireless Page, classification related to wireless will not take effects

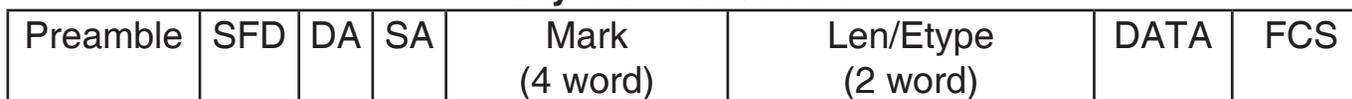
MARK		TRAFFIC CLASSIFICATION RULES															
Class Name	DSCP Mark	Queue ID	802.1p Mark	Lan Port	Protocol	DSCP	Source Addr./Mask	Source Port	Dest. Addr./Mask	Dest. Port	Source MAC Addr./Mask	Destination MAC Addr./Mask	802.1p	Order	Enable/Disable	Remove	Edit
9-81		9		ENET (1-4)	ICMP	CS1								1	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="button" value="Edit"/>

QoS-802.1p Setting

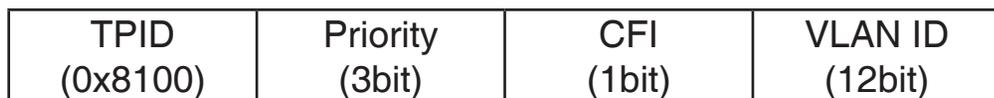
The IEEE 802.1p priority marking method is a standard for prioritizing network traffic at the data link/Mac sub-layer. 802.1p traffic is simply classified and sent to the destination, with no bandwidth reservations established.

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

Layer 2 802.Q Frame



Mark



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

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

Add Network Traffic Class Rule

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 'Save/Apply' to save and activate the rule.

Traffic Class Name:

Rule Order:

Rule Status:

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.

Assign Classification Queue:

Assign Differentiated Services Code Point (DSCP) Mark:

Mark 802.1p if 802.1q is enabled:

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:

Protocol:

Differentiated Services Code Point (DSCP) Check:

Source Subnet Mask:

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

Destination IP Address:

Destination Subnet Mask:

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:

Routing

Select **Advanced Setup > Routing**. The **Routing - Default Gateway** page will appear.

Routing - Default Gateway

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

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

Routing -- 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 AND/OR a WAN interface. Click 'Save/Apply' button to save it.

NOTE: If changing the Automatic Assigned Default Gateway from unselected to selected, You must reboot the router to get the automatic assigned default gateway.

Enable Automatic Assigned Default Gateway

Save/Apply

Routing - Static Route

On this page you can modify the static route settings. You can query the preset static routes, delete an existing static route, or add a new static route. By default, the system has no static route information.

Click **Add** and the following page will appear. Enter the destination network address, subnet mask, gateway AND/OR available WAN interface, then click **Save/Apply** to add the entry to the routing table.

Destination: The IP address to which packets are transmitted.

Subnet Mask: The subnet mask of the destination IP address.

Gateway: The gateway that the packets pass by during transmission.

Interface: The interface that the packets pass through on the modem.

Routing -- Static Route (A maximum 32 entries can be configured)

Destination	Subnet Mask	Gateway	Interface	Remove
<input type="button" value="Add"/> <input type="button" value="Remove"/>				

Routing -- Static Route Add

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

Destination Network Address:

Subnet Mask:

Use Gateway IP Address

Use Interface

DNS

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

DNS Server

Select **Advanced Setup > DNS**. The **DNS Server Configuration** page will appear.

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

If the checkbox is not selected, enter the primary and secondary DNS server IP addresses.

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

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

DNS Server Configuration

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

Enable Automatic Assigned DNS

Save

DNS Server Configuration

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

Enable Automatic Assigned DNS

Primary DNS server:

Secondary DNS server:

Save

DSL

Select **Advanced Setup > DSL**. The **DSL Settings** page will appear.

The available settings include G.Dmt/ G.lite/ T1.413/ ADSL2/ AnnexL/ ADSL2+/ AnnexM / Inner pair / Outer pair / Bitswap / SRA. The Router can negotiate the modulation mode with the DSLAM.

Click **Advanced Settings** to select the DSL test mode.

In the **DSL Advanced Settings** page select the desired DSL test mode and then click **Apply**.

Click **Tone Selection** to modify the upstream and downstream tones.

Select the appropriate upstream and downstream tones for your ADSL connection and then click **Apply**.

DSL Settings

Select the modulation below.

- G.Dmt Enabled
- G.lite Enabled
- T1.413 Enabled
- ADSL2 Enabled
- AnnexL Enabled
- ADSL2+ Enabled
- AnnexM Enabled

Select the phone line pair below.

- Inner pair
- Outer pair

Capability

- Bitswap Enable
- SRA Enable

Save/Apply Advanced Settings

DSL Advanced Settings

Select the test mode below.

- Normal
- Reverb
- Medley
- No retrain
- L3

Apply Tone Selection

ADSL Tone Settings

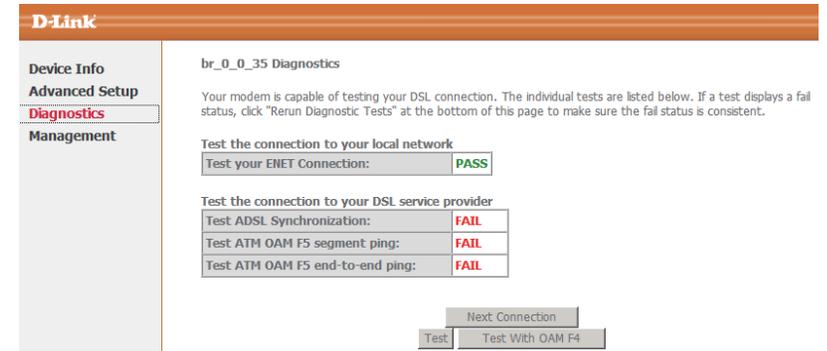
Upstream Tones																															
<input checked="" type="checkbox"/> 0	<input checked="" type="checkbox"/> 1	<input checked="" type="checkbox"/> 2	<input checked="" type="checkbox"/> 3	<input checked="" type="checkbox"/> 4	<input checked="" type="checkbox"/> 5	<input checked="" type="checkbox"/> 6	<input checked="" type="checkbox"/> 7	<input checked="" type="checkbox"/> 8	<input checked="" type="checkbox"/> 9	<input checked="" type="checkbox"/> 10	<input checked="" type="checkbox"/> 11	<input checked="" type="checkbox"/> 12	<input checked="" type="checkbox"/> 13	<input checked="" type="checkbox"/> 14	<input checked="" type="checkbox"/> 15	<input checked="" type="checkbox"/> 16	<input checked="" type="checkbox"/> 17	<input checked="" type="checkbox"/> 18	<input checked="" type="checkbox"/> 19	<input checked="" type="checkbox"/> 20	<input checked="" type="checkbox"/> 21	<input checked="" type="checkbox"/> 22	<input checked="" type="checkbox"/> 23	<input checked="" type="checkbox"/> 24	<input checked="" type="checkbox"/> 25	<input checked="" type="checkbox"/> 26	<input checked="" type="checkbox"/> 27	<input checked="" type="checkbox"/> 28	<input checked="" type="checkbox"/> 29	<input checked="" type="checkbox"/> 30	<input checked="" type="checkbox"/> 31
Downstream Tones																															
<input checked="" type="checkbox"/> 32	<input checked="" type="checkbox"/> 33	<input checked="" type="checkbox"/> 34	<input checked="" type="checkbox"/> 35	<input checked="" type="checkbox"/> 36	<input checked="" type="checkbox"/> 37	<input checked="" type="checkbox"/> 38	<input checked="" type="checkbox"/> 39	<input checked="" type="checkbox"/> 40	<input checked="" type="checkbox"/> 41	<input checked="" type="checkbox"/> 42	<input checked="" type="checkbox"/> 43	<input checked="" type="checkbox"/> 44	<input checked="" type="checkbox"/> 45	<input checked="" type="checkbox"/> 46	<input checked="" type="checkbox"/> 47	<input checked="" type="checkbox"/> 48	<input checked="" type="checkbox"/> 49	<input checked="" type="checkbox"/> 50	<input checked="" type="checkbox"/> 51	<input checked="" type="checkbox"/> 52	<input checked="" type="checkbox"/> 53	<input checked="" type="checkbox"/> 54	<input checked="" type="checkbox"/> 55	<input checked="" type="checkbox"/> 56	<input checked="" type="checkbox"/> 57	<input checked="" type="checkbox"/> 58	<input checked="" type="checkbox"/> 59	<input checked="" type="checkbox"/> 60	<input checked="" type="checkbox"/> 61	<input checked="" type="checkbox"/> 62	<input checked="" type="checkbox"/> 63
<input checked="" type="checkbox"/> 64	<input checked="" type="checkbox"/> 65	<input checked="" type="checkbox"/> 66	<input checked="" type="checkbox"/> 67	<input checked="" type="checkbox"/> 68	<input checked="" type="checkbox"/> 69	<input checked="" type="checkbox"/> 70	<input checked="" type="checkbox"/> 71	<input checked="" type="checkbox"/> 72	<input checked="" type="checkbox"/> 73	<input checked="" type="checkbox"/> 74	<input checked="" type="checkbox"/> 75	<input checked="" type="checkbox"/> 76	<input checked="" type="checkbox"/> 77	<input checked="" type="checkbox"/> 78	<input checked="" type="checkbox"/> 79	<input checked="" type="checkbox"/> 80	<input checked="" type="checkbox"/> 81	<input checked="" type="checkbox"/> 82	<input checked="" type="checkbox"/> 83	<input checked="" type="checkbox"/> 84	<input checked="" type="checkbox"/> 85	<input checked="" type="checkbox"/> 86	<input checked="" type="checkbox"/> 87	<input checked="" type="checkbox"/> 88	<input checked="" type="checkbox"/> 89	<input checked="" type="checkbox"/> 90	<input checked="" type="checkbox"/> 91	<input checked="" type="checkbox"/> 92	<input checked="" type="checkbox"/> 93	<input checked="" type="checkbox"/> 94	<input checked="" type="checkbox"/> 95
<input checked="" type="checkbox"/> 96	<input checked="" type="checkbox"/> 97	<input checked="" type="checkbox"/> 98	<input checked="" type="checkbox"/> 99	<input checked="" type="checkbox"/> 100	<input checked="" type="checkbox"/> 101	<input checked="" type="checkbox"/> 102	<input checked="" type="checkbox"/> 103	<input checked="" type="checkbox"/> 104	<input checked="" type="checkbox"/> 105	<input checked="" type="checkbox"/> 106	<input checked="" type="checkbox"/> 107	<input checked="" type="checkbox"/> 108	<input checked="" type="checkbox"/> 109	<input checked="" type="checkbox"/> 110	<input checked="" type="checkbox"/> 111	<input checked="" type="checkbox"/> 112	<input checked="" type="checkbox"/> 113	<input checked="" type="checkbox"/> 114	<input checked="" type="checkbox"/> 115	<input checked="" type="checkbox"/> 116	<input checked="" type="checkbox"/> 117	<input checked="" type="checkbox"/> 118	<input checked="" type="checkbox"/> 119	<input checked="" type="checkbox"/> 120	<input checked="" type="checkbox"/> 121	<input checked="" type="checkbox"/> 122	<input checked="" type="checkbox"/> 123	<input checked="" type="checkbox"/> 124	<input checked="" type="checkbox"/> 125	<input checked="" type="checkbox"/> 126	<input checked="" type="checkbox"/> 127
<input checked="" type="checkbox"/> 128	<input checked="" type="checkbox"/> 129	<input checked="" type="checkbox"/> 130	<input checked="" type="checkbox"/> 131	<input checked="" type="checkbox"/> 132	<input checked="" type="checkbox"/> 133	<input checked="" type="checkbox"/> 134	<input checked="" type="checkbox"/> 135	<input checked="" type="checkbox"/> 136	<input checked="" type="checkbox"/> 137	<input checked="" type="checkbox"/> 138	<input checked="" type="checkbox"/> 139	<input checked="" type="checkbox"/> 140	<input checked="" type="checkbox"/> 141	<input checked="" type="checkbox"/> 142	<input checked="" type="checkbox"/> 143	<input checked="" type="checkbox"/> 144	<input checked="" type="checkbox"/> 145	<input checked="" type="checkbox"/> 146	<input checked="" type="checkbox"/> 147	<input checked="" type="checkbox"/> 148	<input checked="" type="checkbox"/> 149	<input checked="" type="checkbox"/> 150	<input checked="" type="checkbox"/> 151	<input checked="" type="checkbox"/> 152	<input checked="" type="checkbox"/> 153	<input checked="" type="checkbox"/> 154	<input checked="" type="checkbox"/> 155	<input checked="" type="checkbox"/> 156	<input checked="" type="checkbox"/> 157	<input checked="" type="checkbox"/> 158	<input checked="" type="checkbox"/> 159
<input checked="" type="checkbox"/> 160	<input checked="" type="checkbox"/> 161	<input checked="" type="checkbox"/> 162	<input checked="" type="checkbox"/> 163	<input checked="" type="checkbox"/> 164	<input checked="" type="checkbox"/> 165	<input checked="" type="checkbox"/> 166	<input checked="" type="checkbox"/> 167	<input checked="" type="checkbox"/> 168	<input checked="" type="checkbox"/> 169	<input checked="" type="checkbox"/> 170	<input checked="" type="checkbox"/> 171	<input checked="" type="checkbox"/> 172	<input checked="" type="checkbox"/> 173	<input checked="" type="checkbox"/> 174	<input checked="" type="checkbox"/> 175	<input checked="" type="checkbox"/> 176	<input checked="" type="checkbox"/> 177	<input checked="" type="checkbox"/> 178	<input checked="" type="checkbox"/> 179	<input checked="" type="checkbox"/> 180	<input checked="" type="checkbox"/> 181	<input checked="" type="checkbox"/> 182	<input checked="" type="checkbox"/> 183	<input checked="" type="checkbox"/> 184	<input checked="" type="checkbox"/> 185	<input checked="" type="checkbox"/> 186	<input checked="" type="checkbox"/> 187	<input checked="" type="checkbox"/> 188	<input checked="" type="checkbox"/> 189	<input checked="" type="checkbox"/> 190	<input checked="" type="checkbox"/> 191
<input checked="" type="checkbox"/> 192	<input checked="" type="checkbox"/> 193	<input checked="" type="checkbox"/> 194	<input checked="" type="checkbox"/> 195	<input checked="" type="checkbox"/> 196	<input checked="" type="checkbox"/> 197	<input checked="" type="checkbox"/> 198	<input checked="" type="checkbox"/> 199	<input checked="" type="checkbox"/> 200	<input checked="" type="checkbox"/> 201	<input checked="" type="checkbox"/> 202	<input checked="" type="checkbox"/> 203	<input checked="" type="checkbox"/> 204	<input checked="" type="checkbox"/> 205	<input checked="" type="checkbox"/> 206	<input checked="" type="checkbox"/> 207	<input checked="" type="checkbox"/> 208	<input checked="" type="checkbox"/> 209	<input checked="" type="checkbox"/> 210	<input checked="" type="checkbox"/> 211	<input checked="" type="checkbox"/> 212	<input checked="" type="checkbox"/> 213	<input checked="" type="checkbox"/> 214	<input checked="" type="checkbox"/> 215	<input checked="" type="checkbox"/> 216	<input checked="" type="checkbox"/> 217	<input checked="" type="checkbox"/> 218	<input checked="" type="checkbox"/> 219	<input checked="" type="checkbox"/> 220	<input checked="" type="checkbox"/> 221	<input checked="" type="checkbox"/> 222	<input checked="" type="checkbox"/> 223
<input checked="" type="checkbox"/> 224	<input checked="" type="checkbox"/> 225	<input checked="" type="checkbox"/> 226	<input checked="" type="checkbox"/> 227	<input checked="" type="checkbox"/> 228	<input checked="" type="checkbox"/> 229	<input checked="" type="checkbox"/> 230	<input checked="" type="checkbox"/> 231	<input checked="" type="checkbox"/> 232	<input checked="" type="checkbox"/> 233	<input checked="" type="checkbox"/> 234	<input checked="" type="checkbox"/> 235	<input checked="" type="checkbox"/> 236	<input checked="" type="checkbox"/> 237	<input checked="" type="checkbox"/> 238	<input checked="" type="checkbox"/> 239	<input checked="" type="checkbox"/> 240	<input checked="" type="checkbox"/> 241	<input checked="" type="checkbox"/> 242	<input checked="" type="checkbox"/> 243	<input checked="" type="checkbox"/> 244	<input checked="" type="checkbox"/> 245	<input checked="" type="checkbox"/> 246	<input checked="" type="checkbox"/> 247	<input checked="" type="checkbox"/> 248	<input checked="" type="checkbox"/> 249	<input checked="" type="checkbox"/> 250	<input checked="" type="checkbox"/> 251	<input checked="" type="checkbox"/> 252	<input checked="" type="checkbox"/> 253	<input checked="" type="checkbox"/> 254	<input checked="" type="checkbox"/> 255

Check All Clear All Apply Close

Diagnostics

Click **Diagnostics** to show the interface.

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



Management

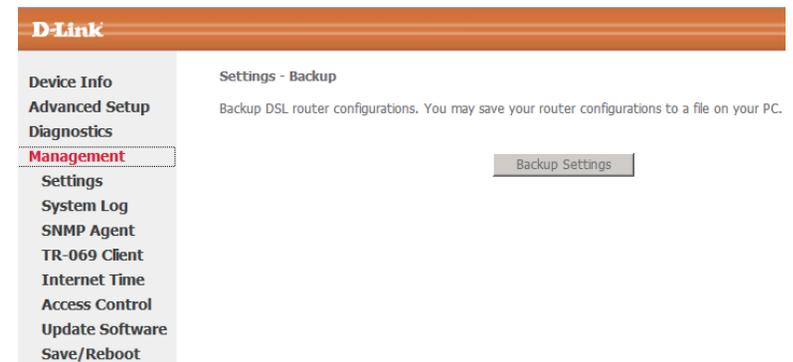
The Management features an array of options designed to help you get the most out of your Router.

Settings

Settings Backup

Select **Management > Settings > Backup**. This page allows you to back up your DSL Router configuration.

Click **Backup Settings** to save your Router configuration to a file on your computer.



System Log

Select **Management > System Log**. The **System Log page** will appear. The system log interface allows you to view the system log and configure the system log options.

Click **Configure System Log** and the **System Log - Configuration** page will appear.

Here, you can enable or disable the system log and select the **Log Level**, **Display Level** and **Mode**. Click **Save/Apply** to save your changes.

Both the log level and display level have eight choices. The default log level is **Debugging** and the default display level is **Error**. The mode options are **Local**, **Remote**, and **Both**. The default option is **Local**.

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

System Log

The System Log dialog allows you to view the System Log and configure the System Log options.

Click "View System Log" to view the System Log.

Click "Configure System Log" to configure the System Log options.

View System Log

Configure System Log

System Log -- Configuration

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 'Save/Apply' to configure the system log options.

Log: Disable Enable

Log Level:

Display Level:

Mode:

Save/Apply

After configuring the System Log options, click **View System Log** to query the system logs. In this example, the **View System Log** displays the default values.

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

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

System Log -- Configuration

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 'Save/Apply' to configure the system log options.

Log: Disable Enable

Log Level:

Display Level:

Mode:

Save/Apply

System Log

Date/Time	Facility	Severity	Message
Jan 1 01:09:56	syslog	emerg	BCM96345 started: BusyBox v1.00 (2009.01.16-13:07+0000)
Jan 1 01:09:57	user	crit	kernel: eth0 Link UP.

Refresh

Close

System Agent

Select **Management > SNMP Agent**. The **SNMP - Configuration** page will appear.

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

Click **Save/Apply** to save your changes.

SNMP - Configuration

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 Agent: Disable Enable

Read Community:

Set Community:

System Name:

System Location:

System Contact:

Trap Manager IP:

Save/Apply

TR-069 Client

Select **Management > TR-069 Client**.

The **TR-069 client - Configuration** page will appear.

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

TR-069 client - Configuration

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

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

TR69c Status:	<input type="radio"/> Disable <input checked="" type="radio"/> Enable
Inform :	<input checked="" type="radio"/> Disable <input type="radio"/> Enable
Inform Interval:	<input type="text" value="300"/>
ACS URL:	<input type="text"/>
ACS User Name:	<input type="text" value="admin"/>
ACS Password:	<input type="password" value="*****"/>
Display SOAP messages on serial console	<input checked="" type="radio"/> Disable <input type="radio"/> Enable
<input checked="" type="checkbox"/> Connection Request Authentication	
Connection Request User Name:	<input type="text" value="admin"/>
Connection Request Password:	<input type="password" value="*****"/>
<input type="button" value="Save/Apply"/> <input type="button" value="GetRPCMethods"/>	

Internet Time

Select **Management > Internet Time** and the **Time Settings** page will appear.

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

This window allows you to set the Router's time configuration.

Click **Save/Apply** to save your changes.

Time settings

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

Automatically synchronize with Internet time servers

Access Control

Access Control – Services

Select **Management > Access Control > Services**. In this interface, you can enable or disable HTTP, ICMP, SSH, TELNET and TFTP services. And the LAN and WAN side can have different configuration.

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

Access Control - IP Address

Select **Management > Access Control > IP Address**. The **Access Control - IP Address** page will appear.

If you enable **Access Control Mode**, the Router permits access to local management services from IP addresses contained in the Access Control List.

If you disable **Access Control Mode**, the system does not validate IP addresses for incoming packets. The services are the system applications listed in the **Service Control List**.

Click **Add** and the Access Control page will appear. Enter the IP address of the management station permitted to access the local management services, and click **Save/Apply**.

Access Control -- Services

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

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

Save/Apply

Access Control -- 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

Access Control Mode: Disable Enable

IP Address Remove

Add Remove

Access Control

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

IP Address:

Save/Apply

Access Control - Passwords

Select **Access Control > Passwords** to change the password of the Router.

Access Control -- Passwords

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

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

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

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

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

Username:

Old Password:

New Password:

Confirm Password:

Save/Apply

Update Software

Select **Management > Update Firmware**. In this page, you can update the Router's firmware.

Click **Browse** to find the file and click **Update Firmware** to update.

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

After updating the software, it is suggested to restore the Router to factory defaults and configure it again.

Tools -- Update Software

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

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

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

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

Software File Name:

Update Software

Save/Reboot

Select **Management > Save/Reboot**.

Click **Save/Reboot** to save your settings and reboot the router.

Click the button below to save and reboot the router.

Save/Reboot

Troubleshooting

This chapter provides solutions to problems that might occur during the installation and operation of the DSL-500B. (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-500B Router without the CD-ROM?

- Connect your PC to the Router using an Ethernet cable.
- Open a web browser and type **http://192.168.254.254**.
- 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). This default password is **admin**.

Note: If you cannot see the login window, please refer to the next section - **Network Basics** to check your PC's IP configuration.

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

- Ensure that the Router is powered on.
- Press and hold the reset button on the back of the device for few seconds.
- 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?

Here are a few steps that you can follow to resolve the issue:

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

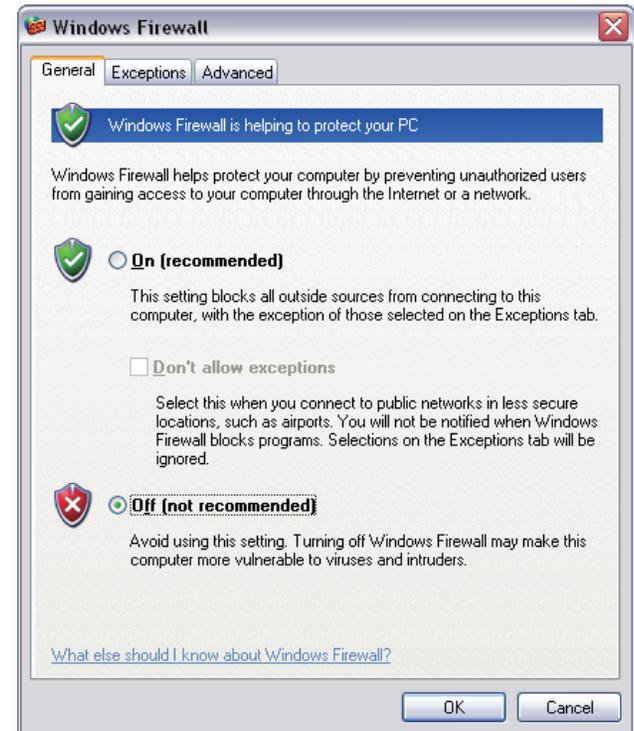
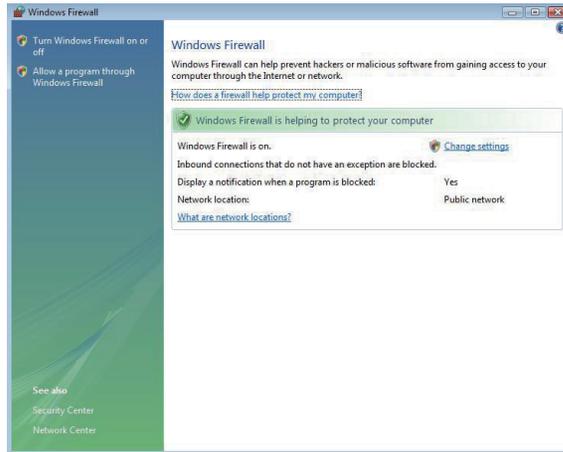
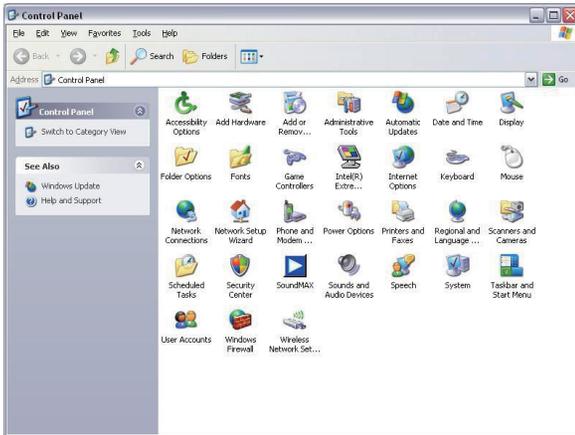
4. Why can't I connect to the Internet?

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

4. What can I do if my router can't be detected by the installation CD?

- Ensure the Router is powered on.
- Check if all the cables are firmly connected at both ends and all the LEDs are working correctly.
- Ensure that only one network interface card on your PC is activated.
- Disable Windows Firewall.
- In Windows XP, go to **Start > Control Panel** and then double-click **Security Center**.
- Disable the Windows Firewall setting and click **OK**.

Note: There might be a potential security issue if you disable the Firewall setting on your PC. Please remember to turn it back on once you have finished the installation procedure and successfully installed your router.



Networking Basics

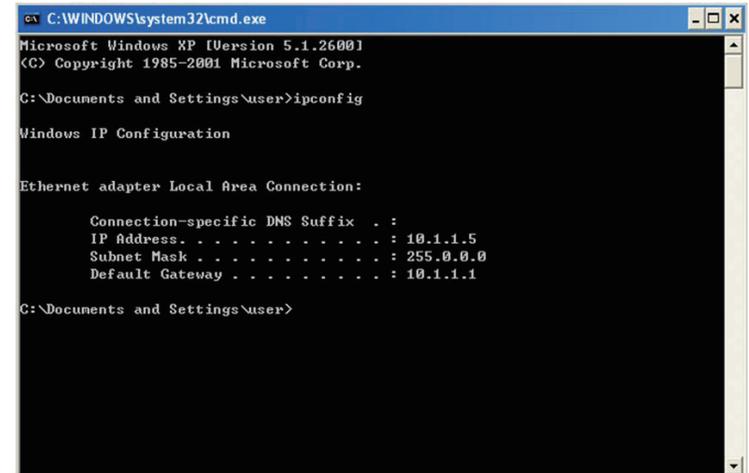
Check Your IP Address

After you install your new D-Link adapter, the TCP/IP settings, by default should be set to **Obtain an IP address from a DHCP server 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.



```
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. . . . . : 10.1.1.5
    Subnet Mask . . . . . : 255.0.0.0
    Default Gateway . . . . . : 10.1.1.1

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

Statically Assign An IP Address

If you are not using a DHCP capable gateway/router, or if 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

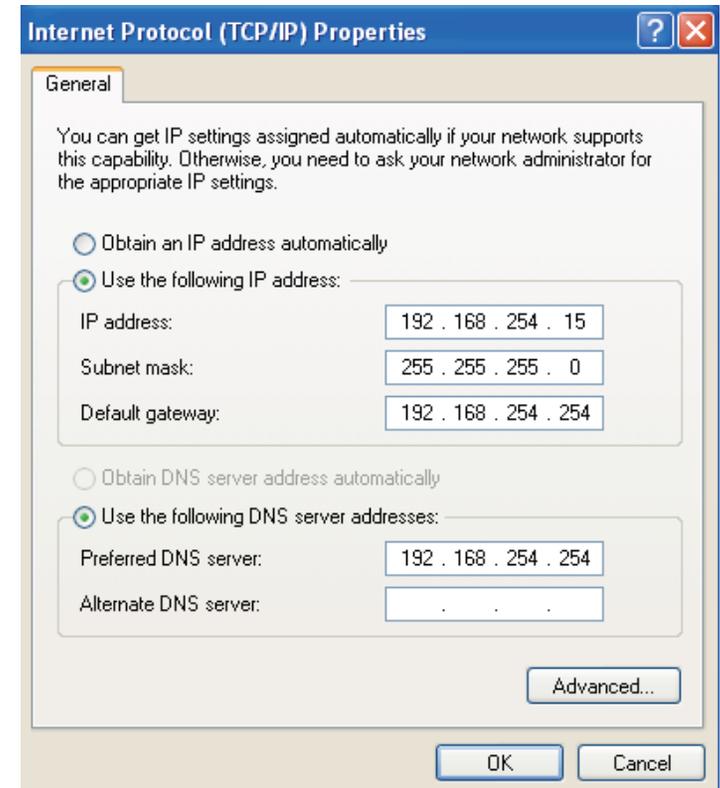
Right-click on **Local Area Connection** that represents your D-Link network adapter and select **Properties**.

Step 3

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

Step 4

Click on **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 192.168.254.254, make your IP address 192.168.254.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 (192.168.254.254).

Set Primary DNS address the same as the LAN IP address of your router (192.168.254.254). The Secondary DNS is not needed or you may enter a DNS server from your ISP.

Step 5

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

Technical Specifications

ADSL Standards

- ANSI T1.413 Issue 2
- ITU G.992.1 (G.dmt) Annex A
- ITU G.992.2 (G.lite) Annex A
- ITU G.994.1 (G.hs)
- ITU G.992.5 Annex A

ADSL2 Standards

- ITU G.992.3 (G.dmt.bis) Annex A
- ITU G.992.4 (G.lite.bis) Annex A

ADSL2+ Standards

- ITU G.992.5 (ADSL2+)

Data Transfer Rate

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

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

Media Interface

- ADSL interface: RJ-11 connector for connection to 24/26 AWG
- LAN interface: RJ-45 port for 10/100BASE-T Ethernet connection