D-Link®

DSL-500

ADSL Router

User's Guide

Wichtige Sicherheitshinweise

1. Bitte lesen Sie sich diese Hinweise sorgfältig durch.
2. Heben Sie diese Anleitung für den spätern Gebrauch auf.
3. Vor jedem Reinigen ist das Gerät vom Stromnetz zu trennen. Vervenden Sie keine Flüssig- oder Aerosolreiniger. Am besten dient ein angefeuchtetes Tuch zur Reinigung.
4. Um eine Beschädigung des Gerätes zu vermeiden sollten Sie nur Zubehörteile verwenden, die vom Hersteller zugelassen sind.
5. Das Gerät is vor Feuchtigkeit zu schützen.
6. Bei der Aufstellung des Gerätes ist auf sichern Stand zu achten. Ein Kippen oder Fallen könnte Verletzungen hervorrufen. Verwenden Sie nur sichere Standorte und beachten Sie die Aufstellhinweise des Herstellers.
7. Die Belüftungsöffnungen dienen zur Luftzirkulation die das Gerät vor Überhitzung schützt. Sorgen Sie dafür, daß diese Öffnungen nicht abgedeckt werden.
8. Beachten Sie beim Anschluß an das Stromnetz die Anschlußwerte.
9. Die Netzanschlußsteckdose muß aus Gründen der elektrischen Sicherheit einen Schutzleiterkontakt haben.
10. Verlegen Sie die Netzanschlußleitung so, daß niemand darüber fallen kann. Es sollete auch nichts auf der Leitung abgestellt werden.
11. Alle Hinweise und Warnungen die sich am Geräten befinden sind zu beachten.
12. Wird das Gerät über einen längeren Zeitraum nicht benutzt, sollten Sie es vom Stromnetz trennen. Somit wird im Falle einer Überspannung eine Beschädigung vermieden.
13. Durch die Lüftungsöffnungen dürfen niemals Gegenstände oder Flüssigkeiten in das Gerät gelangen. Dies könnte einen Brand bzw. Elektrischen Schlag auslösen.
14. Öffnen Sie niemals das Gerät. Das Gerät darf aus Gründen der elektrischen Sicherheit nur von authorisiertem Servicepersonal geöffnet werden.
15. Wenn folgende Situationen auftreten ist das Gerät vom Stromnetz zu trennen und von einer qualifizierten Servicestelle zu überprüfen:
a – Netzkabel oder Netzstecker sint beschädigt.
b – Flüssigkeit ist in das Gerät eingedrungen.
c – Das Gerät war Feuchtigkeit ausgesetzt.
d – Wenn das Gerät nicht der Bedienungsanleitung ensprechend funktioniert oder Sie mit Hilfe dieser Anleitung keine Verbesserung erzielen.
e – Das Gerät ist gefallen und/oder das Gehäuse ist beschädigt.
f – Wenn das Gerät deutliche Anzeichen eines Defektes aufweist.
16. Bei Reparaturen dürfen nur Orginalersatzteile bzw. den Orginalteilen entsprechende Teile verwendet werden. Der Einsatz von ungeeigneten Ersatzteilen kann eine weitere Beschädigung hervorrufen.
17. Wenden Sie sich mit allen Fragen die Service und Repartur betreffen an Ihren Servicepartner. Somit stellen Sie die Betriebssicherheit des Gerätes sicher.
18. Zum Netzanschluß dieses Gerätes ist eine geprüfte Leitung zu verwenden, Für einen Nennstrom bis 6A und einem Gerätegewicht großer 3kg ist eine Leitung nicht leichter als H05VV-F, 3G, 0.75mm2 einzusetzen

Limited Warranty

Hardware:

D-LINK WARRANTS EACH OF ITS HARDWARE PRODUCTS TO BE FREE FROM DEFECTS IN WORKMANSHIP AND MATERIALS UNDER NORMAL USE AND SERVICE FOR A PERIOD COMMENCING ON THE DATE OF PURCHASE FROM D-LINK OR ITS AUTHORIZED RESELLER AND EXTENDING FOR THE LENGTH OF TIME STIPULATED BY THE AUTHORIZED RESELLER OR D-LINK BRANCH OFFICE NEAREST TO THE PLACE OF PURCHASE.

THIS WARRANTY APPLIES ON THE CONDITION THAT THE PRODUCT REGISTRATION CARD IS FILLED OUT AND RETURNED TO A D-LINK OFFICE WITHIN NINETY (90) DAYS OF PURCHASE. A LIST OF D-LINK OFFICES IS PROVIDED AT THE BACK OF THIS MANUAL, TOGETHER WITH A COPY OF THE REGISTRATION CARD.

IF THE PRODUCT PROVES DEFECTIVE WITHIN THE APPLICABLE WARRANTY PERIOD, D-LINK WILL PROVIDE REPAIR OR REPLACEMENT OF THE PRODUCT. D-LINK SHALL HAVE THE SOLE DISCRETION WHETHER TO REPAIR OR REPLACE, AND REPLACEMENT PRODUCT MAY BE NEW OR RECONDITIONED. REPLACEMENT PRODUCT SHALL BE OF EQUIVALENT OR BETTER SPECIFICATIONS, RELATIVE TO THE DEFECTIVE PRODUCT, BUT NEED NOT BE IDENTICAL. ANY PRODUCT OR PART REPAIRED BY D-LINK PURSUANT TO THIS WARRANTY SHALL HAVE A WARRANTY PERIOD OF NOT LESS THAN 90 DAYS, FROM DATE OF SUCH REPAIR, IRRESPECTIVE OF ANY EARLIER EXPIRATION OF ORIGINAL WARRANTY PERIOD. WHEN D-LINK PROVIDES REPLACEMENT, THEN THE DEFECTIVE PRODUCT BECOMES THE PROPERTY OF D-LINK.

WARRANTY SERVICE MAY BE OBTAINED BY CONTACTING A D-LINK OFFICE WITHIN THE APPLICABLE WARRANTY PERIOD, AND REQUESTING A RETURN MATERIAL AUTHORIZATION (RMA) NUMBER. IF A REGISTRATION CARD FOR THE PRODUCT IN QUESTION HAS NOT BEEN RETURNED TO D-LINK, THEN A PROOF OF PURCHASE (SUCH AS A COPY OF THE DATED PURCHASE INVOICE) MUST BE PROVIDED. IF PURCHASER'S CIRCUMSTANCES REQUIRE SPECIAL HANDLING OF WARRANTY CORRECTION, THEN AT THE TIME OF REQUESTING RMA NUMBER, PURCHASER MAY ALSO PROPOSE SPECIAL PROCEDURE AS MAY BE SUITABLE TO THE CASE.

AFTER AN RMA NUMBER IS ISSUED, THE DEFECTIVE PRODUCT MUST BE PACKAGED SECURELY IN THE ORIGINAL OR OTHER SUITABLE SHIPPING PACKAGE TO ENSURE THAT IT WILL NOT BE DAMAGED IN TRANSIT, AND THE RMA NUMBER MUST BE PROMINENTLY MARKED ON THE OUTSIDE OF THE PACKAGE. THE PACKAGE MUST BE MAILED OR OTHERWISE SHIPPED TO D-LINK WITH ALL COSTS OF MAILING/SHIPPING/INSURANCE PREPAID. D-LINK SHALL NEVER BE RESPONSIBLE FOR ANY SOFTWARE, FIRMWARE, INFORMATION, OR MEMORY DATA OF PURCHASER CONTAINED IN, STORED ON, OR INTEGRATED WITH ANY PRODUCT RETURNED TO D-LINK PURSUANT T O THIS WARRANTY.

ANY PACKAGE RETURNED TO DLINK WITHOUT AN RMA NUMBER WILL BE REJECTED AND SHIPPED BACK TO PURCHASER AT PURCHASER'S EXPENSE, AND D-LINK RESERVES THE RIGHT IN SUCH A CASE TO LEVY A REASONABLE HANDLING CHARGE IN ADDITION MAILING OR SHIPPING COSTS.

Software:

WARRANTY SERVICE FOR SOFTWARE PRODUCTS MAY BE OBTAINED BY CONTACTING A D-LINK OFFICE WITHIN THE APPLICABLE WARRANTY PERIOD. A LIST OF DLINK OFFICES IS PROVIDED AT THE BACK OF THIS MANUAL, TOGETHER WITH A COPY OF THE REGISTRATION CARD. IF A REGISTRATION CARD FOR THE PRODUCT IN QUESTION HAS NOT BEEN RETURNED TO A D-LINK OFFICE, THEN A PROOF OF PURCHASE (SUCH AS A COPY OF THE DATED PURCHASE INVOICE) MUST BE PROVIDED WHEN REQUESTING WARRANTY SERVICE. THE TERM "PURCHASE" IN THIS SOFTWARE WARRANTY REFERS TO THE PURCHASE TRANSACTION AND RESULTING LICENSE TO USE SUCH SOFTWARE.

D-LINK WARRANTS THAT ITS SOFTWARE PRODUCTS WILL PERFORM IN SUBSTANTIAL CONFORMANCE WITH THE APPLICABLE PRODUCT DOCUMENTATION PROVIDED BY D-LINK WITH SUCH SOFTWARE PRODUCT, FOR A PERIOD OF NINETY (90) DAYS FROM THE DATE OF PURCHASE FROM D-LINK OR ITS AUTHORIZED RESELLER. D-LINK WARRANTS THE MAGNETIC MEDIA, ON WHICH D-LINK PROVIDES ITS SOFTWARE PRODUCT, AGAINST FAILURE DURING THE SAME WARRANTY PERIOD. THIS WARRANTY APPLIES TO PURCHASED SOFTWARE, AND TO REPLACEMENT SOFTWARE PROVIDED BY D-LINK PURSUANT TO THIS WARRANTY, BUT SHALL NOT APPLY TO ANY UPDATE OR REPLACEMENT WHICH MAY BE PROVIDED FOR DOWNLOAD VIA THE INTERNET, OR TO ANY UPDATE WHICH MAY OTHERWISE BE PROVIDED FREE OF CHARGE.

D-LINK'S SOLE OBLIGATION UNDER THIS SOFTWARE WARRANTY SHALL BE TO REPLACE ANY DEFECTIVE SOFTWARE PRODUCT WITH PRODUCT WHICH SUBSTANTIALLY CONFORMS TO D-LINK'S APPLICABLE PRODUCT DOCUMENTATION. PURCHASER ASSUMES RESPONSIBILITY FOR THE SELECTION OF APPROPRIATE APPLICATION AND SYSTEM/PLATFORM SOFTWARE AND ASSOCIATED REFERENCE MATERIALS. D-LINK MAKES NO WARRANTY THAT ITS SOFTWARE PRODUCTS WILL WORK IN COMBINATION WITH ANY HARDWARE, OR ANY APPLICATION OR SYSTEM/PLATFORM SOFTWARE PRODUCT PROVIDED BY ANY THIRD PARTY, EXCEPTING ONLY SUCH PRODUCTS AS ARE EXPRESSLY REPRESENTED, IN D-LINK'S APPLICABLE PRODUCT DOCUMENTATION AS BEING COMPATIBLE. D-LINK'S OBLIGATION UNDER THIS WARRANTY SHALL BE A REASONABLE EFFORT TO PROVIDE COMPATIBILITY, BUT D-LINK SHALL HAVE NO OBLIGATION TO PROVIDE COMPATIBILITY WHEN THERE IS FAULT IN THE THIRD-PARTY HARDWARE OR SOFTWARE. D-LINK MAKES NO WARRANTY THAT OPERATION OF ITS SOFTWARE PRODUCTS WILL BE UNINTERRUPTED OR ABSOLUTELY ERROR-FREE, AND NO WARRANTY THAT ALL DEFECTS IN THE SOFTWARE PRODUCT, WITHIN OR WITHOUT THE SCOPE OF D-LINK'S APPLICABLE PRODUCT DOCUMENTATION, WILL BE CORRECTED.

D-Link Offices for Registration and Warranty Service

THE PRODUCT'S REGISTRATION CARD, PROVIDED AT THE BACK OF THIS MANUAL, MUST BE SENT TO A DLINK OFFICE. TO OBTAIN AN RMA NUMBER FOR WARRANTY SERVICE AS TO A HARDWARE PRODUCT, OR TO OBTAIN WARRANTY SERVICE AS TO A SOFTWARE PRODUCT, CONTACT THE D-LINK OFFICE NEAREST YOU. AN ADDRESS/TELEPHONE/FAX/E-MAIL/WEB SITE LIST OF D-LINK OFFICES IS PROVIDED IN THE BACK OF THIS MANUAL.

LIMITATION OF WARRANTIES

IF THE D-LINK PRODUCT DOES NOT OPERATE AS WARRANTED ABOVE, THE CUSTOMER'S SOLE REMEDY SHALL BE, AT D-LINK'S OPTION, REPAIR OR REPLACEMENT. THE FOREGOING WARRANTIES AND REMEDIES ARE EXCLUSIVE AND ARE IN LIEU OF ALL OTHER WARRANTIES, EXPRESSED OR IMPLIED, EITHER IN FACT OR BY OPERATION OF LAW, STATUTORY OR OTHERWISE, INCLUDING WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. D-LINK NEITHER ASSUMES NOR AUTHORIZES ANY OTHER PERSON TO ASSUME FOR IT ANY OTHER LIABILITY IN CONNECTION WITH THE SALE, INSTALLATION MAINTENANCE OR USE OF D-LINK'S PRODUCTS

D-LINK SHALL NOT BE LIABLE UNDER THIS WARRANTY IF ITS TESTING AND EXAMINATION DISCLOSE THAT THE ALLEGED DEFECT IN THE PRODUCT DOES NOT EXIST OR WAS CAUSED BY THE CUSTOMER'S OR ANY THIRD PERSON'S MISUSE, NEGLECT, IMPROPER INSTALLATION OR TESTING, UNAUTHORIZED ATTEMPTS TO REPAIR, OR ANY OTHER CAUSE BEYOND THE RANGE OF THE INTENDED USE, OR BY ACCIDENT, FIRE, LIGHTNING OR OTHER HAZARD.

LIMITATION OF LIABILITY

Trademarks

Copyright Statement

FCC Warning

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.

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 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 equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

-Reorient or relocate the receiving antenna.

-Increase the separation between the equipment and receiver.

-Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.

-Consult the dealer or an experienced radio/TV technician for help.

CE Mark Warning

This is a Class B product. In a domestic environment, this product may cause radio interference in which case the user may be required to take adequate measures.

TABLE OF CONTENTS

About This Guide

Thank you for choosing the DSL-500 ADSL Router. The DSL-500 will provide your private small office or home network with convenient Internet access and rapid download speeds while improving network efficiency and security. D-Link strives to provide cost effective broadband access devices that are easy to use and upgrade for small office and home networks.

If you would like to set up the device quickly in order to verify that the ADSL connection to the WAN (wide area network) is working properly, please read the Quick Installation Guide included in the DSL-500 package.

This user's guide provides instructions on how to install the DSL-500 ADSL Router and use it to connect several PCs on an Ethernet LAN (Local Area Network) to the Internet. For the sake of simplicity, this document uses the terms Router (first letter upper case) to refer specifically to the DSL-500 ADSL Router, and router (first letter lower case) to refer to all such devices including the DSL-500.

DSL services are provided by many different types of business entities such as telephone companies, Internet service providers (ISPs), DSL resellers and others. ADSL service is sometimes bundled together with some form of network service such as an ISP account. This guide uses the generic terms ADSL service provider or network service provider to refer to any or all businesses that provide ADSL service or Internet account services.

Furthermore it is assumed that the reader has some familiarity with Ethernet networks, networking devices, routing protocols and the TCP/IP suite of protocols.

Overview of the User's Guide

Chapter 1 Introduction to Router – Describes the Router and its key features. Provides an introduction to ADSL. Lists standards to which the Router complies. Contains a packing list.

Chapter 2 Prepare for Installation – Lists everything needed for the installation of the Router, including specific information needed for configuration. Provides space for recording all the necessary information.

Chapter 3 Hardware Installation – Discusses how to connect the Router to an Ethernet LAN.

Chapter 4 First Time Set Up – Provides information on how to configure the Router and establish the ADSL connection using the web-based manager.

Chapter 5 Web-based Management – Describes how to use the web-based manager and discusses the management options available.

Chapter 6 LAN Setup – Discusses different options for IP addressing on your LAN. Describes how to change the IP address of the LAN interface on the Router.

Chapter 7 Using the Console Manager- Describes how to use the console manager and lists the most commonly used commands, including how to change the password used to access the web-based manager.

Appendix A Technical Specifications – Lists the technical specifications of the Router, including standards compliance.

Appendix B IP Concepts – A discussion of IP address assignment and subnets for a private network.

Appendix C DSL-500 Firmware Upgrade Utility – Describes how to install and use the firmware upgrade utility used with the Router.

1

Introduction to the Router

This chapter describes the Router and it features and includes an introduction to ADSL technology. Diagrams are provided detailing the hardware and LED indicators. A list of package contents is presented at the end of the chapter.

Router Description and Operation

The DSL-500 ADSL Router is designed to provide a simple, cost-effective and secure ADSL Internet connection for your small- to medium-sized private network. The DSL-500 combines the benefits of high-speed ADSL connection technology and TCP/IP routing with a conventional Ethernet interface in one compact and convenient package. ADSL connection technology enables many interactive multi-media applications such as video conferencing and collaborative computing.

The Router is easy to install and use. The DSL-500 connects to an Ethernet LAN via a standard Ethernet 10BASE-T interface using RJ-45 connectors. The ADSL connection is made using ordinary twisted-pair telephone line with standard RJ-11 connectors. This arrangement means that several PCs can be networked and connected to the Internet using a single WAN interface and IP address.

The Router supports transparent bridging and can be used for IP packet routing over the Internet. Cost saving features of the Router such as NAT (Network Address Translator) and DHCP (Dynamic Host Configuration Protocol) improve administration efficiency and improve security. The advanced security enhancements, packet filtering and port redirection, can help protect your network from potentially devastating intrusions by malicious agents from outside your network.

ADSL Technology

Asymmetric Digital Subscriber Line (ADSL) is an access technology that utilizes ordinary copper telephone lines to enable broadband high-speed digital data transmission and interactive multimedia applications for business and residential customers. The use of existing copper telephone lines forgoes the need for upgrading lines or adding expensive new cable.

ADSL devices use digital coding techniques that greatly increase the potential capacity of phone lines without interfering with regular telephone services. For the ADSL user, this means much faster data communications and the potential for interactive video capabilities. ADSL devices make it possible to enjoy benefits such as high-speed Internet access, telecommuting (remote LAN access), collaborative computing, distance learning, movies on demand and multi-player video gaming, without experiencing any loss of quality or disruption of voice/fax telephone capabilities.

ADSL provides a dedicated service over a single telephone line operating at speeds of up to 8 Mbps downstream (to the user) and up to 640 Kbps upstream depending on local telephone line conditions. These conditions are ideal for many user applications. A secure point-to-point connection is established between the user and the central office of the local telephone service provider. The user is always connected thus eliminating dial-up time and simplifying connectivity issues.

Product Features

The DSL-500 ADSL Router utilizes the latest ADSL enhancements and router technologies to provide a robust Internet gateway suitable for most small to medium sized offices.

PPP (Point-to-Point Protocol) Security

The DSL-500 ADSL Router supports PAP (Password Authentication Protocol) and CHAP (Challenge Handshake Authentication Protocol) for PPP connections.

DHCP Support (Dynamic Host Configuration Protocol)

DHCP (Dynamic Host Configuration Protocol) automatically and dynamically assigns al 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-500 allows multiple users on the LAN to access the Internet concurrently through a single Internet account. This provides Internet access to everyone in the office for the price of a single user.

NAT improves network security in effect by hiding the private network behind one global and visible IP address. NAT address mapping can also be used to link two IP domains via a LAN-to-LAN connection.

TCP/IP (Transfer Control Protocol/Internet Protocol)

The DSL-500 supports TCP/IP protocol, the language used for the Internet. It is compatible with access servers manufactured by major vendors.

RIP-1/RIP-2

The DSL-500 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 a 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-500 supports *Bridged Ethernet over ATM* (RFC1483), *IP over ATM* (RFC1577) and *PPP over ATM* (RFC 2364). The Router can support up to eight Virtual Circuit Connections (VCCs).

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

Very high rates of data transfer are possible with the Router. Up to 8 Mbps downstream bit rate using the G.dmt.

Full Network Management

The DSL-500 incorporates SNMP (Simple Network Management Protocol) support for web-based management and text-based network management via an RS-232 or **Telnet** connection.

Telnet Connection

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

Easy Installation

The DSL-500 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.

Standards Compatibility and Compliance

The DSL-500 complies with or is compatible with the following standards as recognized by their respective agencies.

- ITU G.994.1 (G.Hs *Auto-handshake*) compliant

- ITU G.992.1 (G.dmt *Full-rate ADSL*) compliant

- ITU G.992.2 (G.lite *"Splitterless ADSL"*) compliant

- ITU-T Rec. I.361 compliant

- ITU-T Rec. I.610 compliant

- Compatible with all T1.413 issue 2 (full rate DMT over analog POTS), and CO DSLAM equipment

- RFC 1483 Multi-protocol over ATM "Bridged Ethernet" compliant

- RFC 2364 *PPP over ATM* compliant

- RFC 2516 *PPP over Ethernet* compliant

- RFC 1334 PPP Authentication Protocol compliant

- RFC 1994 Challenge Handshake Authentication Protocol compliant

- RFC 791 *Internet Protocol* compliant

- RFC 826 Address Resolution Protocol compliant

- RFC 950 Internet Control Message Protocol compliant

- RFC 1631 Net Address Translator compliant

- Supports RFC 2131 and RFC 2132 DHCP functions including: automatic assignment of IP address, use of subnet mask and default gateway and provision of DNS server address for all hosts

- IEEE 802.3 compliant

- IEEE 802.3u compliant

- IEEE 802.1d compliant

- Supports RIP v1 and RIP v2

- Supports Static Routing

- Supports ATM Forum UNI V3.1 PVC

- Minimum ATM cell forwarding rate: 640 Kbps

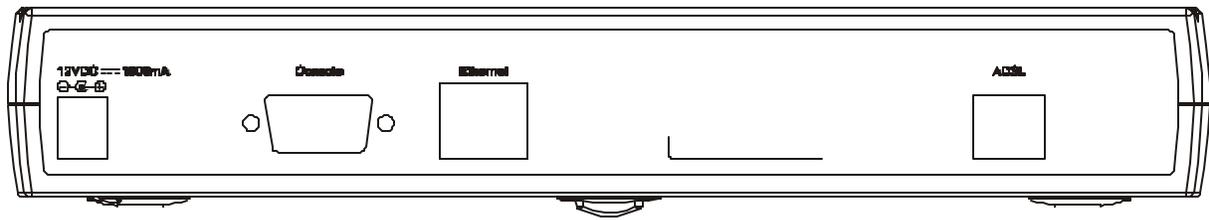- Supports up to eight simultaneous ATM virtual connections

Front Panel

Place the Router in a location that permits an easy view of the LED indicators shown in the front panel diagram below.
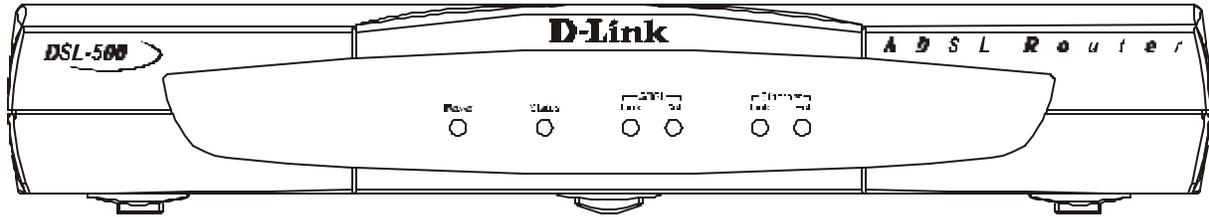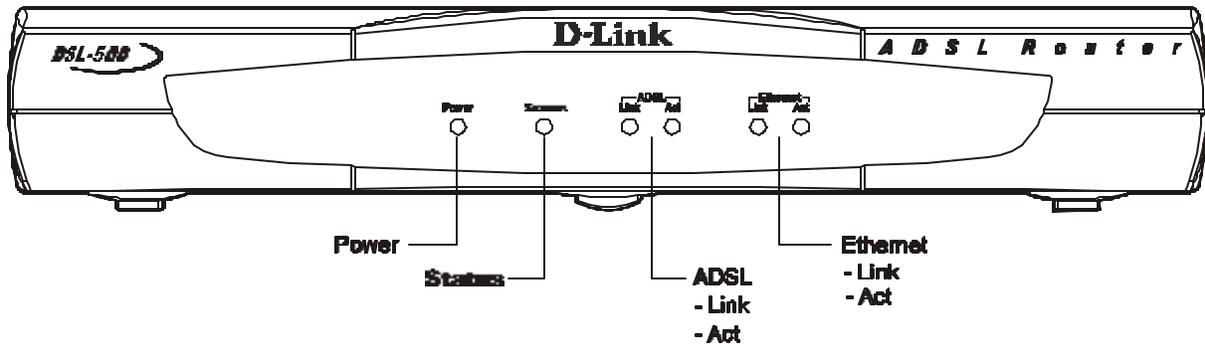
Front Panel

Rear Panel

The rear panel of the Router provides access to the AC power adapter cord connection as well as the port connections.

Rear Panel

LED Indicators

LED Indicators

The LED Indicators read as follows:

Power	Steady green light indicates the unit is powered on.
Status	Lights steady green during the ADSL negotiation phase. Once the connection status has been settled, the light will blink green.
ADSL: Link	Steady green light indicates a valid ADSL connection. This will light after the ADSL negotiation process has been settled.
ADSL: Act	Blinking green light indicates an active wan session.
Ethernet: Link	Steady green light indicates a valid Ethernet connection.
Ethernet: Act	Blinking green indicates an active Ethernet session.

2

Prepare for Installation

For the smoothest possible installation, assemble all the equipment and information needed to set up the Router and establish the initial ADSL connection before you begin. Everything needed for the installation is listed and discussed in this chapter.

Verify Package Contents

Open the box and carefully remove all items. In addition to this Installation Guide, make sure that you have:

RS 232

CD

5

DSL-500

3

1

ADSL Cable

Adapter

4

2

Manual

6
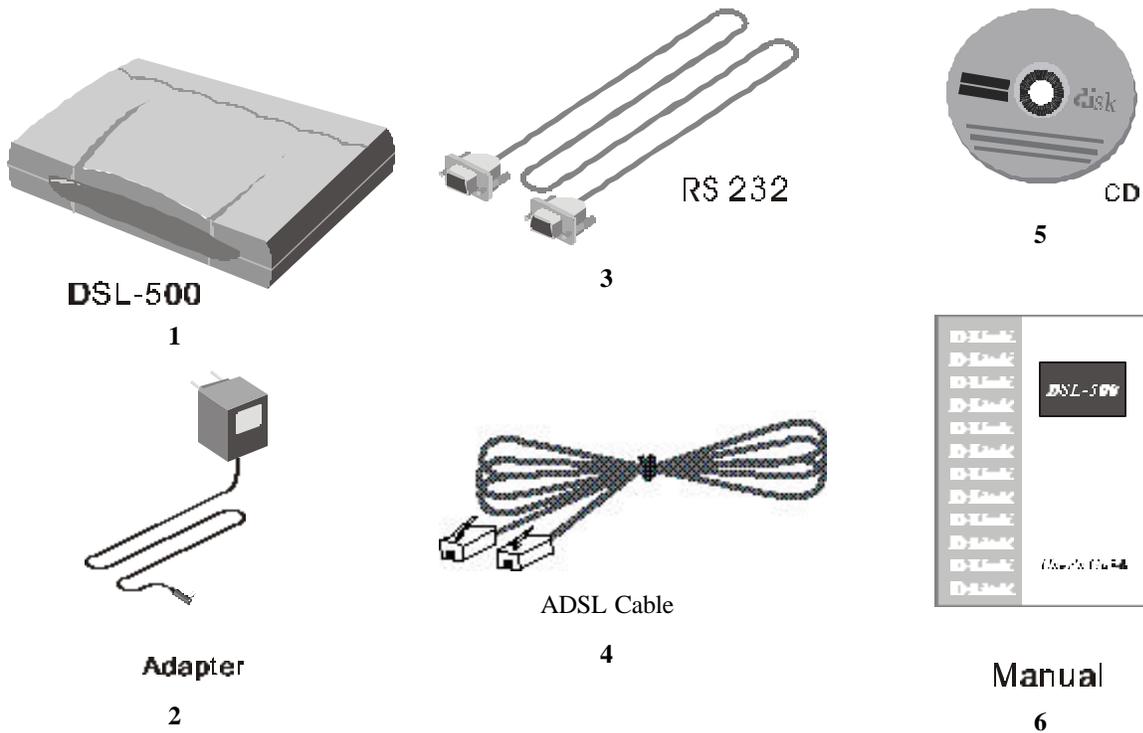
1. One DSL-500 ADSL Router

2. One AC power adapter suitable for your electric service

3. One RS-232 (DB-9 to DB-9) cable for console connection

4. One ADSL telephone cable with RJ-11 connectors for ADSL connection (standard telephone wire)

5. One DSL-500 tool kit on CD-ROM

6. One DSL-500 User's Guide

Microfilters and Splitters

Most ADSL clients will be required to install a simple device that prevents the ADSL line from interfering with regular telephone services. These devices are commonly referred to as microfilters or sometimes called (inaccurately) line splitters. They are easy to install and use standard telephone connectors and cable.

Some ADSL service providers will send a telecommunications technician to modify the telephone line, usually at the point where the telephone line enters the building. If a technician has divided or split your telephone line into two separate lines - one for regular telephone service and the other for ADSL – then you do not need to use any type of filter device. Follow the instructions given to you by your ADSL service provider about where and how you should connect the Modem to the ADSL line.

Microfilters

Unless you are instructed to use a "line splitter" (see below), it will be necessary to install a microfilter (low pass filter) device for each telephone or telephone device (answering machines, Faxes etc.) that share the line with the ADSL service. Microfilters are easy-to-install, in-line devices, which attach to the telephone cable between the telephone and wall jack. Microfilters that install behind the wall plate are also available. A typical in-line microfilter installation is shown in the diagram below.
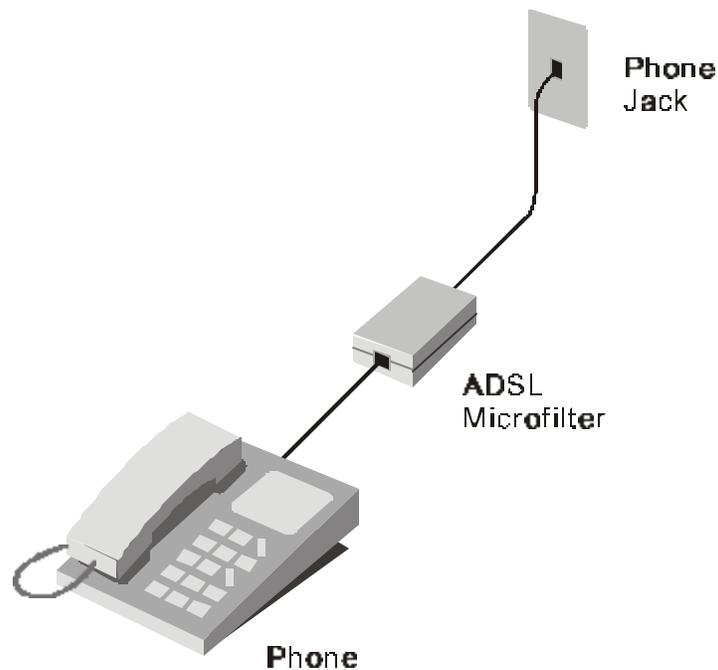
Microfilter Installation

Note: Do not install the microfilter between the Modem and the telephone jack. Microfilters are only intended for use with regular telephones, Fax machines and other regular telephone devices.
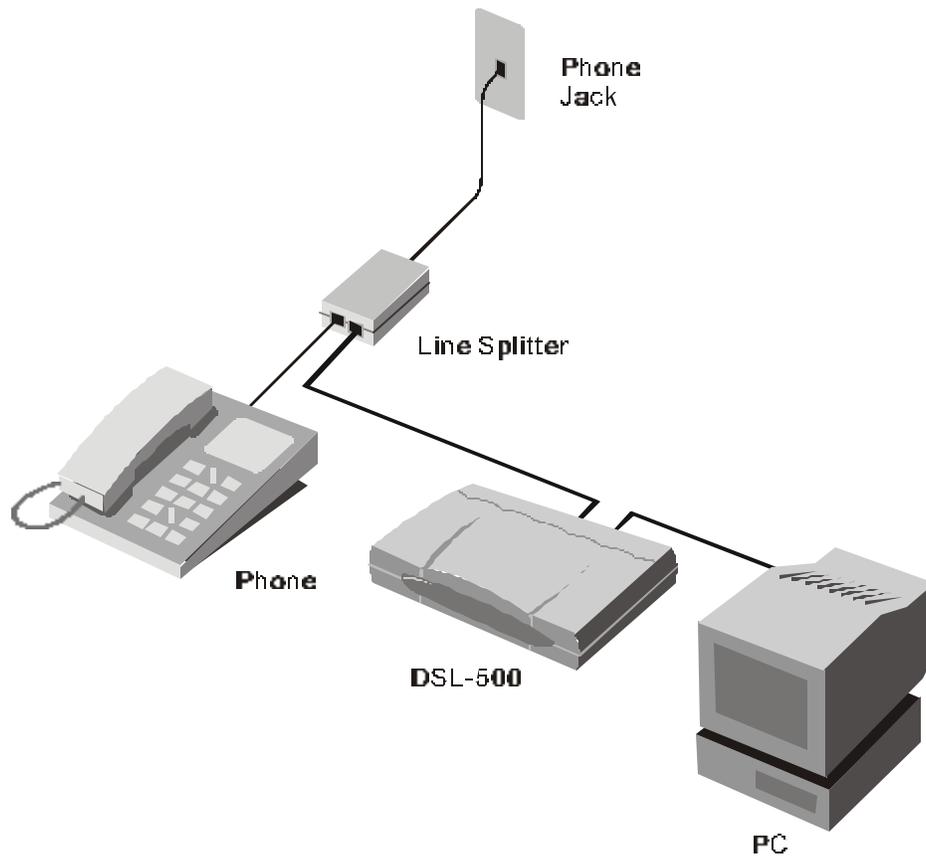

Line Splitter

If you are instructed to use a "line splitter", you must install the device between the Modem and the phone jack. Use standard telephone cable with standard RJ-11 connectors. The splitter has three RJ-11 ports used to connect to the wall jack, the Modem and if desired, a telephone or telephone device. The connection ports are typically labeled as follows:

Line - This port connects to the wall jack.

ADSL – This port connects to the Modem.

Phone – This port connects to a telephone or other telephone device.

The diagram below illustrates the proper use of the splitter.

Line Splitter Installation

Additional Requirements

You will need a PC (referred to in this guide as the Manager PC) to set up and use the Router. In addition, it will be necessary to configure the device using information provided by your ADSL service provider. This information is used to establish the parameters of the ADSL connection and identify the Router on the WAN. The requirements for the PCs on your LAN are summarized below.

PC Workstation Requirements

You can use the Router with PCs that meet the conditions discussed here.

Operating System

The web-based management software can be used on PCs running one of the following operating systems:

Microsoft® Windows 95	Windows 98 SE	Windows 2000
Windows 98	Windows Me	Windows NT 4.x

Web Browser

Any common web browser such as Microsoft Internet Explorer or Netscape Navigator can be used to configure the Router using the embedded web-based management software.

Ethernet Adapter (NIC)

All PCs using the Router for Internet access, including the Manager PC, must have an Ethernet NIC (Network Interface Card) installed. Each computer on the internal network must have TCP/IP Protocol enabled. If you have an existing Ethernet set up, the PCs should already meet this requirement.

If you are using the Router in the role of a simple bridge (RFC 1483), additional software may be needed for the computer or server connected to the Router (on the LAN side). You may be instructed by your service provider to configure the NIC card for DHCP or PPP connection. Your network service provider will give you more information.

Connection Method

It is necessary to know the connection method used for the ADSL connection. The connection method is also known as the ADSL Protocol, Encapsulation Protocol or Encapsulation Method. These protocols are defined by "RFCs" which are internationally recognized standards for networking protocols. You will be required to configure the Router to use the correct method. PPP connections require account information to be entered and stored in the device. Bridged Ethernet connections require that the IP settings be set manually.

The Router supports three connection methods:

♦ PPP over ATM (RFC 2364) used by default

♦ PPP over Ethernet (RFC 2516)

♦ IP over ATM (RFC 1577)

♦ Ethernet over ATM (RFC 1483)

PPP Connections (RFC 2516 & RFC 2364)

For PPPoA or PPPoE connections, a verification process is required before the network connection can be established. Use this section to record the information used for authentication.

Account Information (User Name and Password)

For PPP connections, a User Name and Password for the user account are needed to connect to the service provider's network.

ACCOUNT INFORMATION (PPP Connections Only)
User Name:
Password:

Bridged Ethernet Connections (RFC 1483)

Using this method, the DSL-500 acts as a transparent bridge, and is invisible to other devices on both the WAN and LAN side of the bridge. It is therefore necessary to provide some means of acquiring global IP settings for your account.

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, server or firewall hardware. The IP address can be assigned in a number of ways. Your network service provider will give you instructions about any additional connection software or NIC configuration that may be required.

IPoA Connections (RFC 1577)

IP over ATM connections may require global IP settings for the device. Your service provider will give you IP settings information if needed. Some IPoA connections function like peer-to-peer connections and therefore do not require IP settings on the WAN interface.

PVC Settings

Some subscribers may be instructed to change the VPI and VCI values for the device. These numbers define a unique route used on the ATM backbone of the WAN. If your service provider asks you to configure these values for your network connection, follow the instructions in the *Connection Profile* section of Chapter 5.

3

Hardware Installation

This chapter discusses the various connections you will need to make in order to use the Router.

When selecting the location for the Router, allow room to access the connections on the rear panel. You will want to place the Router so that you will be able to see the LED indicators on the front panel. Also allow some space above the Router for ventilation to avoid problems with overheating.

It may be convenient for you locate the Router near the PC you intend to use for initial configuration of the Router. For initial configuration of the device you may need convenient access to the RS-232 serial port on the rear panel. The RS-232 serial port is intended for use with text-based console management software for the initial configuration and for out-of-band management of the Router. Whether it is necessary to use an RS-232 console manager for first time set up depends on how you allocate IP addresses on your network. Read Chapter 4, *First Time Set Up* to help you decide how best to use the Router on your network.

Connect the Power

Insert the AC Power Adapter cord into the power receptacle located on the rear panel of the Router and plug the adapter into a nearby power source. You should see the Power LED indicator light up and remain lit.

Connect ADSL Line

Use the twisted-pair ADSL cable (standard telephone cable) included with the Router to connect it to your telephone line. Simply 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 wall jack. The ADSL connection is the WAN interface. It links the Router to the network service provider's backbone infrastructure. This is the Router's access point to the Internet.

The Router must undergo a negotiation process to establish the terms of the ADSL connection. During this negotiation the Status LED will light a steady green, after which it will blink. If the ADSL line is disconnected, it will repeat this process.

Connect Ethernet LAN to Router

The Router may be connected to any 10BASE-T Ethernet LAN. Connection to an Ethernet concentrating device such as a switch or hub should use standard twisted-pair cable with RJ-45 connectors. The RJ-45 port on the Router is a straight-through (MDI-X) connection. Follow standard Ethernet guidelines when deciding what type of cable to use to make this connection. Use a normal crossed cable when connecting the Router to a normal (MDI-X) port on a switch or hub. Use a straight-through cable when connecting it to an uplink (MDI-II) port on a hub or switch. When connecting the Router directly to a PC or server (MDI-II) use a straight-through cable. A valid connection will be indicated by a steady green Ethernet Link LED indicator.

The rules governing Ethernet cable lengths apply to the LAN to Router connection. Be sure that the cable connecting the Ethernet LAN to the Router does not exceed 100 meters.

The diagram below illustrates a typical Ethernet LAN to Router connection.
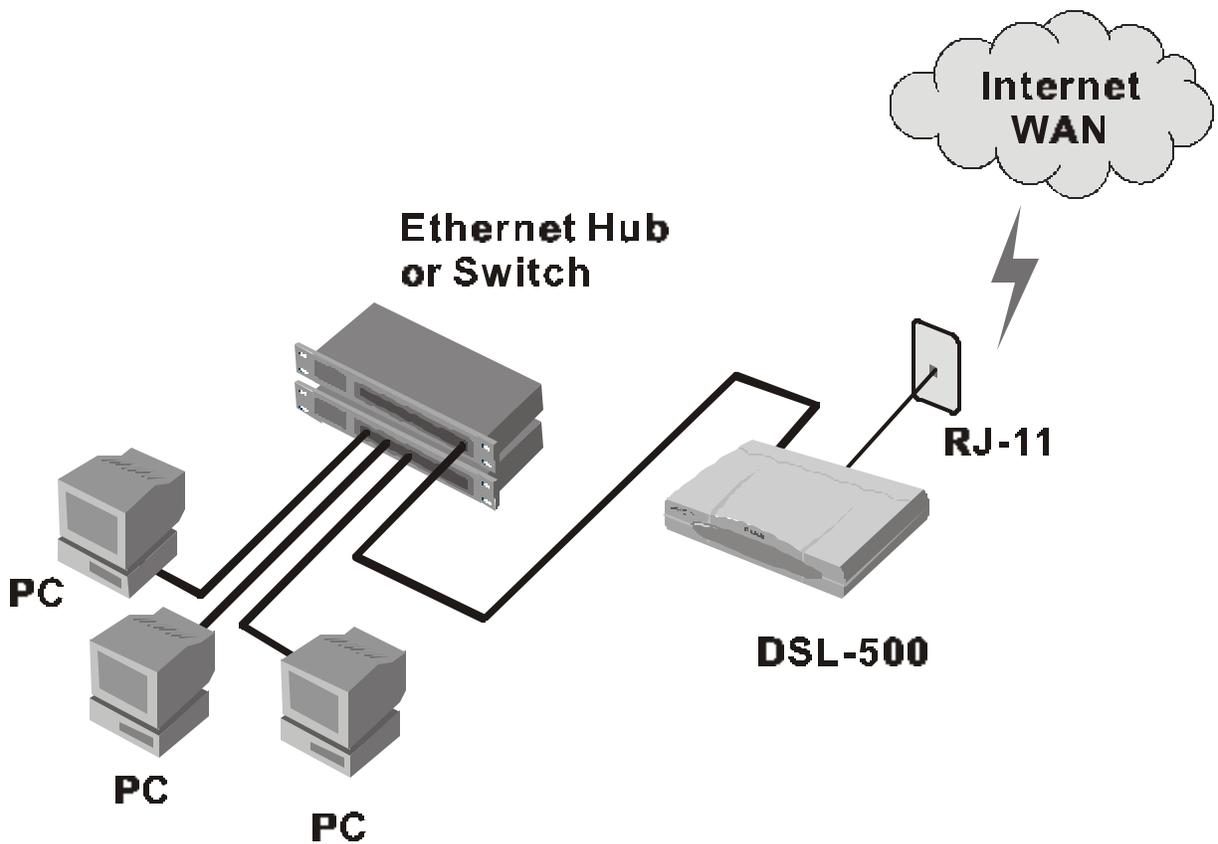
Connect Server or PC to Router

The Router may be connected directly to a server or PC using the RJ-45 Ethernet port. The diagram below illustrates a PC/Server to Router connection with the Router being employed as a firewall.

4
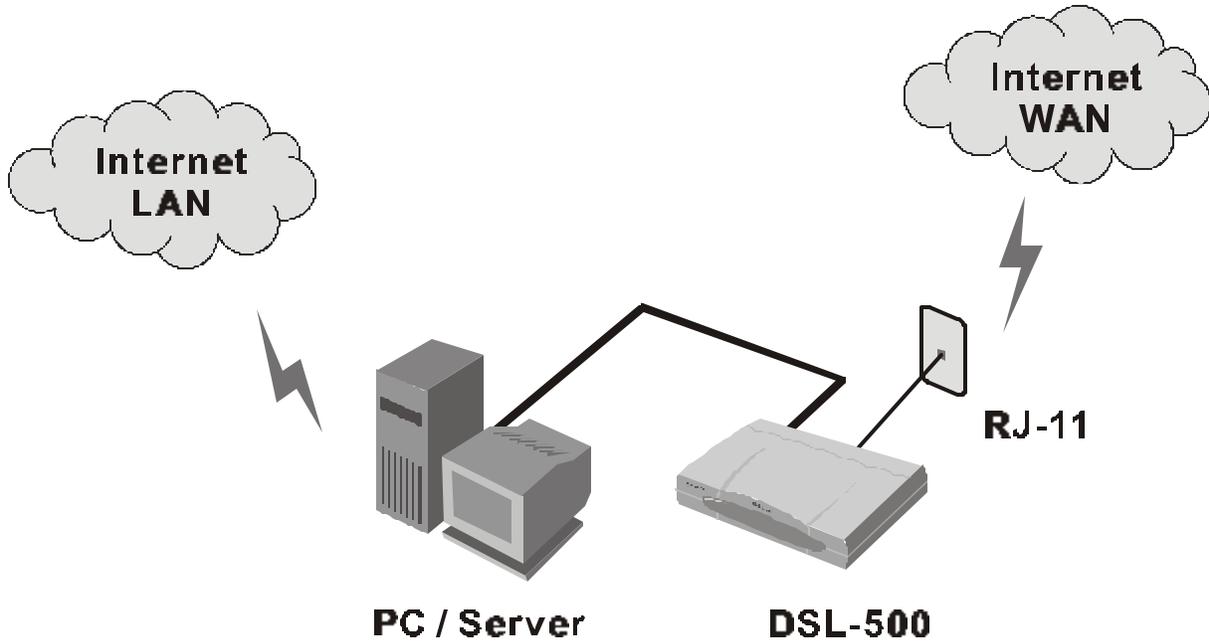
First Time Set Up

This chapter discusses the steps to first establish the WAN connection. The remaining features not directly concerned with establishing the initial connection are explained in Chapter 5, *Web-based Management*.

It will be convenient for most users to establish an initial ADSL connection for one PC equipped with an Ethernet NIC (Network Interface Card). It is recommended that you install and configure the Router using one non-networked computer. This allows you to verify that the ADSL service is functioning and that you are able to communicate with the device. Once the initial ADSL connection is established, you can proceed to build an Ethernet LAN around the device or incorporate it into an existing LAN. For convenience, the PC used to configure the Router is referred to as the manager PC.

IP Settings

To further simplify things it is recommended that you use the Router's web-based management software for initial configuration. To communicate with the Router, the manager PC must be connected to it via an Ethernet connection and have a web browser installed. Furthermore, the manager PC must reside within the same subnet as the Router. This can be done easily using the DHCP function of the Router. The Router will act as a DHCP server by default. You can configure the manager PC to obtain its IP settings from the Router by following the procedure in the next section, *Configure the Manager PC for DHCP*.

You should start by configuring the manager PC to obtain IP settings from the Router. Next disconnect the manager PC from the network and connect it directly to the Router with a straight-through Ethernet cable.

Bridged Connections (RFC 1483)

For connections using the DSL-500 as a simple bridge, it may be more convenient to change the LAN IP address of the device. Instructions for changing the device's LAN IP address read Chapter 6, *LAN Setup*, for more information.

Configure the Manager PC as a DHCP Client (Windows OS)

Use the following steps to configure the manager PC to be a DHCP client. These same steps must be performed for every host PC on your network if you use the DHCP function of the Router.

1. In Windows 95/98, click on the START button, go to Settings and choose Control Panel.
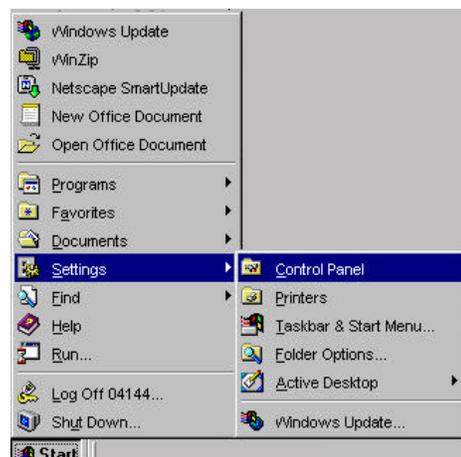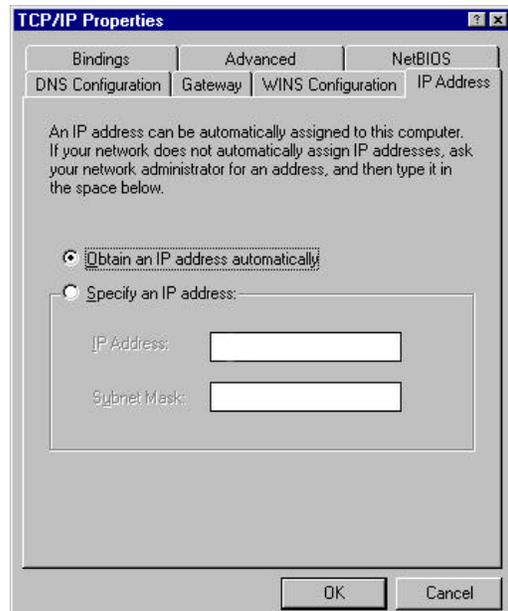
2. In the **Control Panel** window, double-click on the **Network** icon.
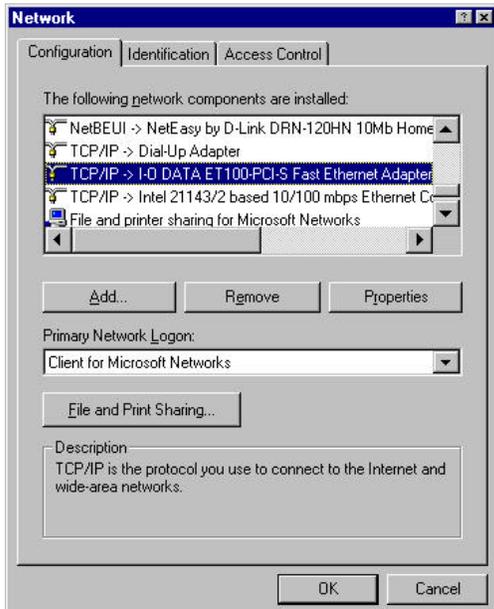
3. Under the Configuration tab, select the **TCP/IP** component and click **Properties**.

4. Choose the Obtain an IP address automatically option and click OK.

5. Restart the PC to let the new setting take effect.

Access the Web-based Manager

The Manager PC can now use a web browser to communicate with the Router.

Note: **Be sure that the Manager PC is not configured to use a proxy server in the Internet settings. In Windows Internet Explorer, you can check if a proxy server is enabled using the following procedure:**

1. In Windows, click on the START button, go to Settings and choose Control Panel.

2. In the Control Panel window, double-click on the Internet Options icon.

3. Click the Connections tab and click on the LAN Settings button.

4. Verify that the "Use proxy server" option is NOT checked. If it is checked, click in the checked box to deselect the option and click OK.

To use the web-based management software, launch a suitable web browser and direct it to the IP address of the Router. Type in **http://** followed by the default IP address, **192.168.0.1** in the address bar of the browser. The URL in the address bar should read: **http://192.168.0.1**.

In the page that opens, click on the **Login to web-based management module** button in the center.

A new window will appear and you will be prompted for a user name and password to access the web-based manager. Use the default user name **admin** and password **admin** for first time set up. You should change the web-based manager access user name and password once you have verified that a connection can be established. The user name and password allows any PC within the same subnet as the Router to access the web-based manger.

> **NOTE:** Do not confuse the user name and password used to access the web-based manager with the ADSL account user name and password needed for PPP connections to access the ADSL or network service provider's network.

Logging in will bring up the Router/Bridge Configuration window of the web-based management module. In this window, you will see the D-Link DSL-500 folder is open revealing its contents of three subfolders. These subfolders contain menu buttons you can click on to see various menu screens used to configure the device for connection to the WAN and other functions.
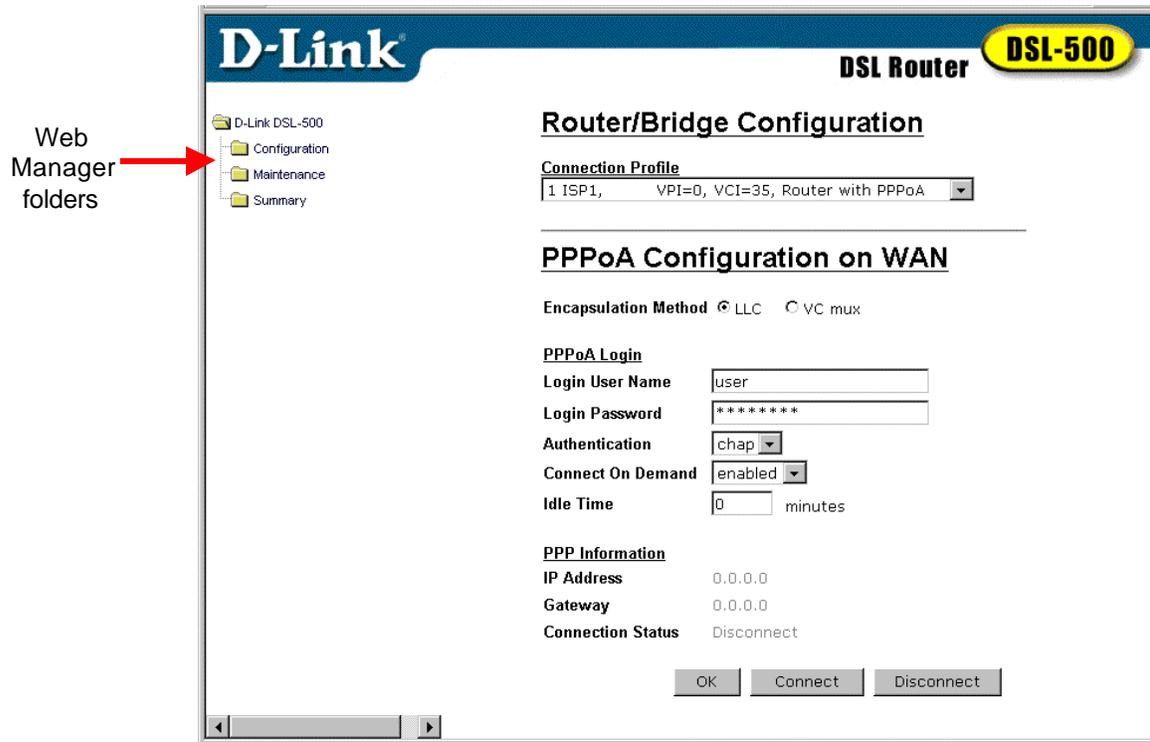
Web-based Manager Main Menu – First Time Log On

Configure the WAN Connection

Now that you have accessed the web-based manager, you can configure the device for the WAN connection. For PPPoE and PPPoA connections, you will need to provide a User Name and Password used by your ISP for authentication purposes. For "Bridged Ethernet" (RFC 1483) connections, a static IP address must be used. It is necessary to supply IP settings for the WAN connection and other information discussed in Chapter 2, *Prepare for Installation*.

All connection methods available to the Router are discussed in this chapter, beginning with PPPoA connections. PPPoA is the default method used by the Router.

If you are using a PPPoE, IPoA, or Bridged Ethernet (RFC 1483) connection, it is necessary to change the connection method. Please read *Changing the Connection Type* following the *PPPoA Connections* section for more information.

PPPoA Connections

The default connection method used by the Router is Point-to-Point-Protocol over ATM (PPPoA). In the PPPoA Configuration window, you must enter the user name and password for network account authentication and verification. When this information is entered, the changes must be saved and the Router restarted. In the **Bridge/Router Configuration** window, follow these steps to establish the WAN connection using PPPoA:

1. Under **PPPoA Login**, enter the **Login User Name** used for your network account. The user name and login password, are used to authenticate the identity of the ADSL client and provide access to the service provider's network. The user name and login password can be any combination of up to 64 characters.

2. Enter the Login Password.

3. Unless you are instructed to use a different **Authentication** method, leave the default **chap** protocol selected. The alternative method, **pap**, can be selected from the pull-down menu if required by the service provider.

4. Leave the **Connect on Demand** option as **enabled** in the pull-down menu. This will allow the Router to establish a WAN connection upon restarting.

5. Leave **Idle Time** set to the default value 0.

6. Click on the **OK** button on the bottom of the window. A new screen appears:

7. The **<u>Save changes and reboot system?</u>** message prompt offers two option:

    A. You can save the configuration changes and restart the device now by clicking OK; or,

    B. If you want to change the user name and password used to access the Web Manager, select the "Continue and do 'Save Changes' later" option and click OK, and go to the System Username and Password menu in the Maintenance folder.

Changing the Connection Profile

The default connection method used by the Router for the WAN connection is PPP over ATM. If you wish to use this method, it is not necessary to change this setting. However, if you will use a static IP address for a "Bridged Ethernet" (RFC 1483) connection, PPP over Ethernet or IPoA you must change the connection method.

There are two menus used to change the connection method or connection profile. The Bridge/Router Configuration menu, the first screen that appears when you log in, can be used to configure the device to use one of the three available methods. This procedure is described below. The connection profile can also be changed using the Connection Profile menu, this is described in its own section in Chapter 5.

To change the connection profile using the Bridge/Router Configuration menu, follow these steps:

1. In the **Bridge/Router Configuration** window, use the drop-down menu under **Connection Profile** to select an alternative connection method. The alternative connection options are **Bridge with RFC 1483**, **Router with PPPoE** and **Router with IPoA**. You will also see the VPI and VCI values listed here.

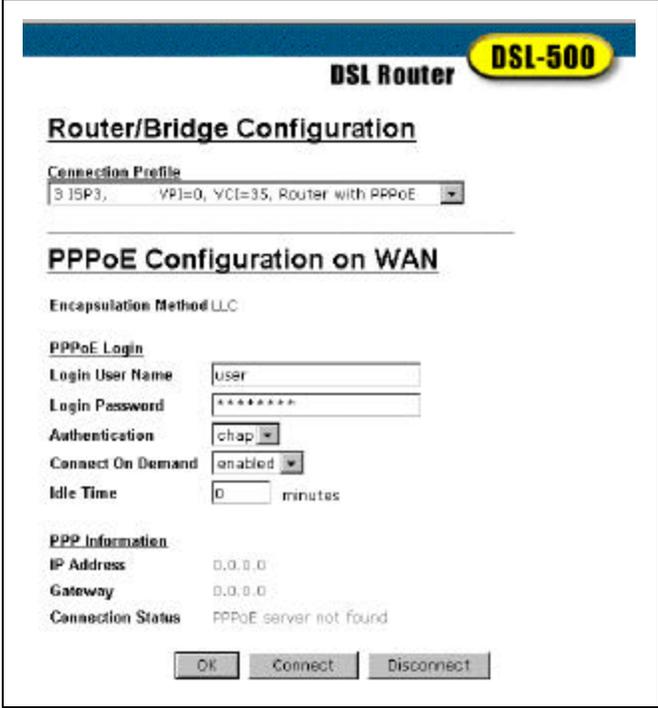2. Click on the **OK** button on the bottom of the window. A new screen will appear:
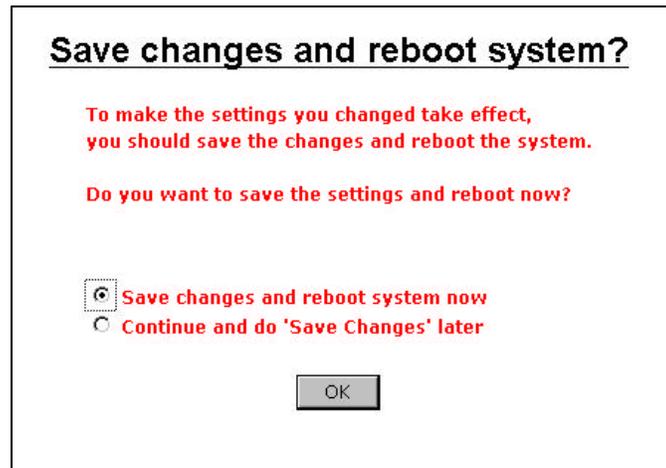
3. The **Save changes and reboot system?** message prompt offers two option:

    A. You can save the configuration changes and restart the device now by clicking OK; or,

    B. If you want to change the user name and password used to access the Web Manager, select the "Continue and do 'Save Changes' later" option and click **OK**, and go to the System Username and Password menu in the Maintenance folder.

PPP Connections

Although the connection methods differ significantly, from the viewpoint of the ADSL subscriber, there is little difference between the two variations of PPP connections. The information entered for PPPoE connections is the same as that used for PPPoA connections.
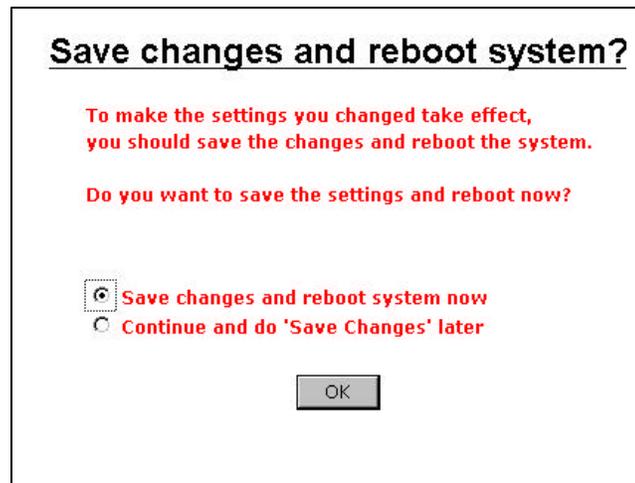
Once you have changed the connection method to PPPoE, saved the configuration change and restarted the device, you can proceed to enter authentication information used to connect to the WAN. Follow these steps:

Router/Bridge Configuration - PPPoE

1. Under **PPPoE Login**, enter the **Login User Name** used for your network account. The user name and login password, are used to authenticate the identity of the ADSL client and provide access to the service provider's network. The user name and login password can be any combination of up to 64 characters.

2. Enter the Login Password.

3. Unless you are instructed to use a different **Authentication** method, leave the default **chap** protocol selected. The alternative method, **pap**, can be selected from the pull-down menu if required by the service provider.

4. Leave the **Connect on Demand** option as **enabled** in the pull-down menu. This will allow the Router to establish a WAN connection upon restarting.

5. Leave **Idle Time** set to the default value 0.

6. Click on the **OK** button on the bottom of the window. A new screen appears:

7. The **Save changes and reboot system?** message prompt offers two option:

    A. You can save the configuration changes and restart the device now by clicking OK; or,

    B. If you want to change the user name and password used to access the Web Manager, select the "Continue and do 'Save Changes' later" option and click **OK**, and go to the System Username and Password menu in the Maintenance folder.

RFC 1483 Bridged Ethernet Connections

If you are using the "Bridged Ethernet" method for the WAN connection, the global IP settings must be configured in another device. When using this connection method, the device functions as a bridge, so it is does not perform any IP functions. The device will have a IP address on the LAN, but not on the WAN interface. After changing the connection profile to **Bridge with RFC 1483**, you will need to configure the PC or server connected to the DSL-500 so the WAN interface a way to obtain a global IP address. This can be accomplished in different ways according to the circumstances of your network and the nature of your ADSL subscriber account. Your network service provider will give you instructions or additional computer software as needed to handle global IP settings for your account.

IPoA Connections

IPoA connections may require that global IP settings be configured for the device manually or be configured to use DHCP to obtain these settings. If you are instructed to set the WAN IP address manually or use DHCP, read the *IPoA Configuration* section of Chapter 5. Otherwise, the connection will be established upon restarting the device.

Changing the User Name and Password

Before you configure the Router and connect to the WAN you should change the user name and password used to access the web-based manager. Open the Maintenance folder and click on the System Username and Password button to change the manager username and password.

User Name and Password Menu

8.   Type the current **User Name** in the entry field provided.

9.   Type in the current password in the **Old Password** entry field.

10. Type in the **New Password** in the entry field provided.

11. Type in the new password again in the **Confirm New Password** field.

12.   Click the **OK** button.

13. The **Save changes and reboot system?** message appears:

   A.   You can save the configuration changes and restart the device now by clicking OK; or,

   B.   If you want to change the user name and password used to access the Web Manager, select the "Continue and do 'Save Changes' later" option and click **OK**.

Connect to WAN

Once you have configured the Router, saved changes and restarted it, you can connect the manager PC to the Internet. The procedure is the same for PPPoE and PPPoA connections.

Connect with PPP (PPPoE and PPPoA)

If you have enabled the Connect on Demand feature, the Router will have established the WAN connection upon restarting.

If the Connect on Demand feature has been disabled, click the **Connect** button to initiate the PPP connection via the ADSL WAN interface. The "handshake" process will take a few seconds.

In the PPPoE or PPPoA Configuration widow, viewing the **Connection Status** *Connected*, under **PPPoE Information** or **PPPoA Information** will indicate a valid connection. A valid ADSL connection can also be confirmed by observing the LED indicators on the front panel of the device.

Disconnect PPP

For PPP connections. the WAN connection can be terminated at any time by clicking on the **Disconnect** button in the PPPoE or PPPoA Configuration window. It is recommended that you disconnect the ADSL connection and change the user name and password used to access the web-based manager. Then set up the rest of your network.

Connect with IPoA (RFC 1577)

IP over ATM connections may require global IP settings for the device. Your service provider will give you IP settings information if needed. Some IPoA connections function like peer-to-peer connections and therefore do not require IP settings on the WAN interface.

Connect with RFC 1483

Upon restarting the device, it will serve as a bridge, and therefore it will not have any IP (Layer 3) function on the WAN interface. Your network service provider will instruct you on what further steps are needed to establish the WAN connection. You may have to install software on your PC or you may be required to alter the IP settings of the NIC adapter on your PC.

You will notice that the configuration options have changed. Please read *Bridge with RFC 1483* in Chapter 5 for more information on bridge configuration.

5

Web-based Management

The DSL-500 offers a web-based (HTML) graphical user interface allowing users to manage the Router from anywhere on the LAN using a standard browser, software such as Netscape Navigator or Microsoft Internet Explorer. The web browser is used for direct communication with the Router using HTTP protocol.

Accessing the Web Manager

In order to access the web-based management interface it will be necessary to have both the manager's PC and the Router on the same IP subnet. If the manager PC is configured as a DHCP client, the Router will automatically assign IP settings. If you choose to disable the DHCP function, it will be necessary to either change the IP settings of the PC or change the IP address of the Router. See Chapter 6 for information about assigning IP addresses on the network and changing the IP address of the device using the console interface.

To use the web-based management software simply run the browser you have installed on your computer and point it to the IP address defined for the device. The first time you access the web-based manager you will need to type the default IP address, **192.168.0.1** in the address bar of the browser. The URL in the address bar should read: **http://192.168.0.1**. If you change the IP address you will use the new IP address to access the web-based manager.

In the page that opens, click on the **Login to web-based management module** button.

A new window will appear and you will be prompted for a user name and password. Use default user name **admin** and password **admin** for first time set up.


User Login

If you have forgotten your user name or password you can use the out-of-band console manager to access this information. For details on how to use the console manager to find the user name and password, see Chapter 7, *Using the Console Manager*.

> **Note:** Be sure that the Manager PC is not configured to use a proxy server in the Internet settings. In Windows Internet Explorer, you can check if a proxy server is enabled using the following procedure:

1. In Windows, click on the START button, go to Settings and choose Control Panel.

2. In the Control Panel window, double-click on the Internet Options icon.

3. Click the Connections tab and click on the LAN Settings button.

4. Verify that the "Use proxy server" option is NOT checked. If it is checked, click in the checked box to deselect the option and click OK.

Web Manager Interface

Once you have successfully logged on to the web manager, your browser will display the Bridge/Router Configuration menu. If you wish to change the connection method used by the device, please see *Changing the Connection Method* in the Chapter 4.
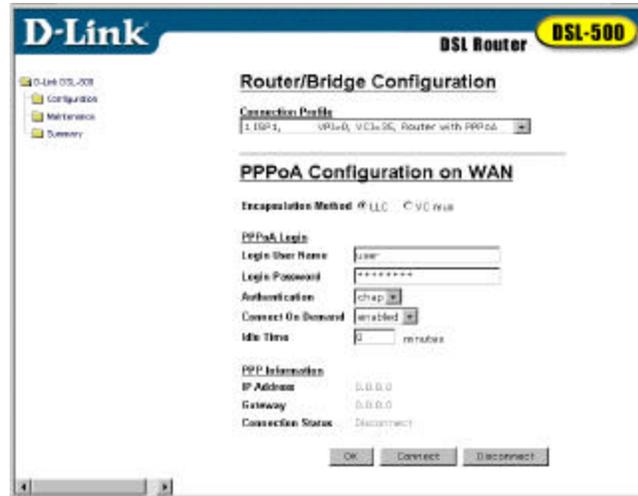
**Web Manager GUI – First Time Login**

Folders and Menus

The web manager interface is divided into two sections, the left side displays an open folder labeled D-Link DSL-500. The subfolders inside are labeled Configuration, Maintenance and Summary. The contents of these subfolders differs depending on the connection profile of the device. The figure to the right reveals the contents of the folders when the device is configured to serve as a router (Router with PPPoA or PPPoE connections). The next section, *Router with PPP Configuration*, instructs you on how to use the web manager for configuration of the DSL-500 functioning as a router. For device configuration of bridged (RFC 1483) connections, skip ahead to *Bridge with RFC 1483 Configuration*.
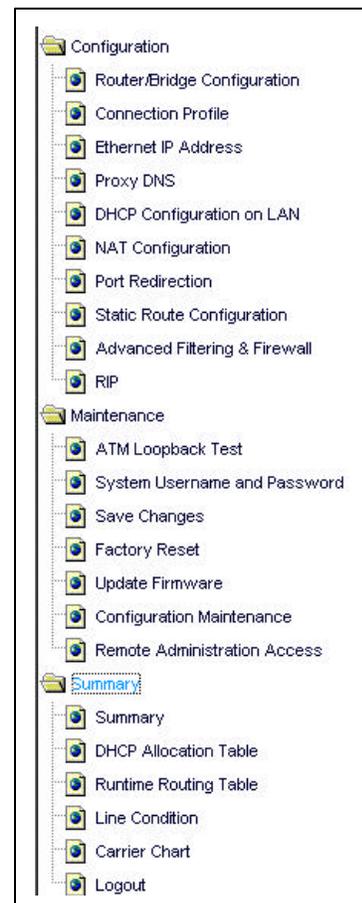
Router Configuration Menus

Changing the Connection Profile

Use the Connection Profile menu to add, change or delete connection profiles. This menu is used to change the VPI/VCI settings for the device.
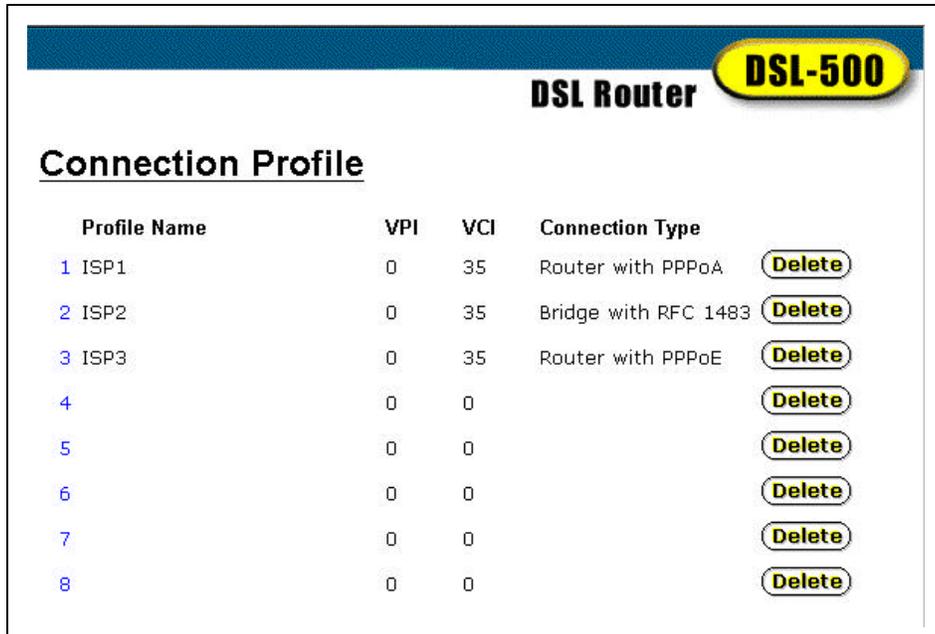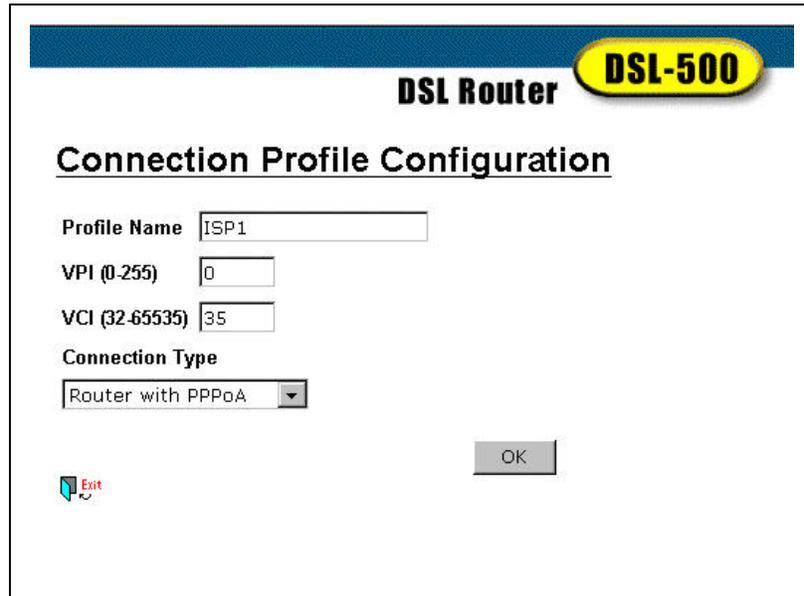

Connection Profile Screen

The Connection Profile screen contains a numbered list of existing profiles is as follows:

Profile Name	Connection profile name
VPI	Virtual Path Identifier
VCI	Virtual Channel Identifier
Connection Type	The functional role of the DSL-500 and connection protocol used

A profile may be deleted by clicking on the **Delete** button for that profile. To change an existing profile click on the number for that profile Connection Profile Configuration menu will appear. To add a new profile, click on an unused number to see the Connection Profile Configuration menu.

Connection Profile Configuration

Connection Profile Configuration

Use the Connection Profile Configuration menu to change the following parameters:

Profile Name   Type in a new name for this profile

VPI   Type in the new VPI setting (*0-255*)

VCI   Type in the new VCI setting (*32-65535*)

Connection Type   From the drop-down menu select *Router with PPPoA*, *Router with PPPoE*, *Router with IPoA*, or *Bridge with RFC 1483*

When all the changes have been made, click on the **OK** button. You will be prompted to save the changes and reboot the device.

To return to the Connection Profile Screen, click the Exit icon.

> **Note:** The VPI and VCI numbers are assigned by the network service provider. These values should not be changed unless you are instructed to do so. Incorrect VPI or VCI settings will not allow the device to connect to the WAN.
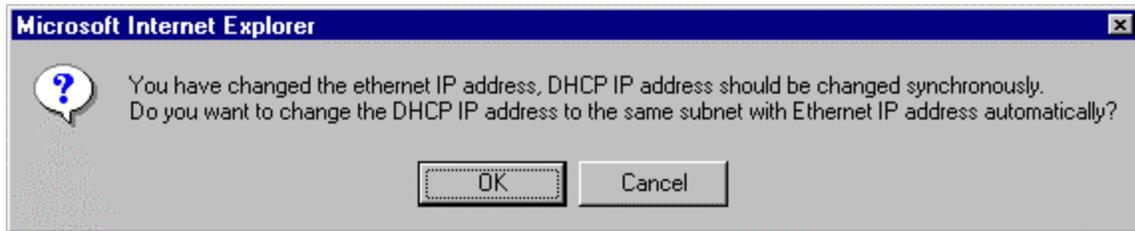
IP Address on LAN

Use this menu to change the LAN IP address of the Router.
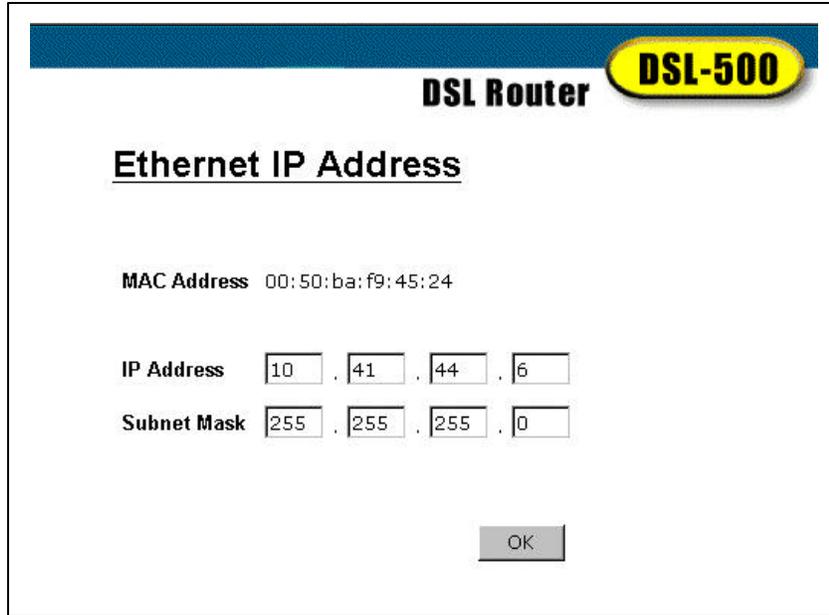
Ethernet IP Address Menu

The Ethernet IP Address displays the current LAN IP settings of the Router. To change the IP address, type in the new **IP Address** and **Subnet Mask** in the spaces provided and click on the **OK** button. If DHCP is enabled, a screen prompt will appear:

If you will continue to use the DHCP function, click the **OK** button.

You will be prompted again to restart the device. Restart now or continue to make changes and save the changes later.

Router Configuration

The DSL-500 serving as a router has a different role than it does when it is configured to be a bridge. This section discusses the different menus used for configuration when it serves as a router. The device is configured as a router when using a connection profile characterized by a PPPoE, PPPoA or IPoA connection.

PPP Configuration (PPPoE & PPPoA)

The first menu displayed is the Router/Bridge Configuration menu. You may access this window at any time by clicking on the first button in the Configuration folder.

Router with PPP Configuration Menu

The PPP Configuration menu presents the following user defined parameters:

Connection Profile	Drop-down menu used to change connection method.
Login User Name	Used for authentication by your network service provider.
Login Password	Used for authentication by your network service provider.
Authentication	Protocol used to confirm the identity of the subscriber.
	Choose chap (default) or pap form the drop-down menu.
Connect on Demand	Select enabled or disabled. When this function is enabled the router will connect any workstation on your LAN to the Internet upon request. If this function is disabled, it will be necessary to access this menu and hit the Connect button each time you want to establish a connection to the WAN or the Internet.
Idle Time	The default value = 0. This means that the Router is always connected and able to connect on demand. If your network account is billed according to the amount of time the Router is actually connected to the Internet, enter an appropriate Idle Time value (in seconds). This will disconnect the Router after the WAN connection has been idle for the amount of time specified.

When you finished making changes to the PPP configuration, click the **OK** button to save the changes. It will be necessary to restart the Router for the new configuration to go into effect.

PPPoE Information

This read-only field provides information regarding the status of the Router connection to the WAN. The global **IP Address** for the Router should be assigned automatically by the network service provider's PPP server. The **Connection Status** will read Disconnect until the Router has established the WAN connection.

Connect to WAN

If you have enabled the Connect on Demand feature, the Router will have established the WAN connection upon restarting.

If the Connect on Demand feature has been disabled, click the **Connect** button to initiate the PPP connection via the ADSL WAN interface. The "handshake" process will take a few seconds. To sever the WAN connection, click on the **Disconnect** button.

IPoA Configuration

The IP over ATM connection method uses a different method to connect to the WAN. Some IPoA connections operate in a way similar to peer-to-peer connections, and therefore do not require a global IP address for the WAN interface. Some networks using IPoA do require global IP settings. In this case the settings are assigned manually or by DHCP. The default configuration for IPoA is peer-to-peer connection, that is, global IP settings are not required.

Router with IPoA Configuration

For peer-to-peer network connections, check the **IP Unnumbered** box (checked by default) and click **OK**.

For DHCP service, check the **DHCP client** box and click **OK**.

To assign the global IP settings manually, type in the **IP Address**, **Subnet Mask** and **Default Gateway** IP settings given assigned by your network service provider, and click **OK**.

Clicking **OK** will bring up the Save and reboot system? prompt.

Proxy DNS Settings

You may use the Router to provide DNS services for work stations on your LAN. To configure on-board DNS, click on the Proxy DNS button.

Proxy DNS Menu

The Proxy DNS Menu presents the following user defined parameters:

Proxy DNS	Default = enabled. Choose *enabled* or *disabled* from the drop-down menu to enable or disable the proxy DNS function.
Get DNS IP automatically	Default = auto-detect. Click in the box to use (checked) or not use (unchecked) automatic DNS detection. Using automatic DNS detection not allow you to select a DNS server.
DNS Server IP	(DNS auto-detect must be disabled) Type in the IP address of the DNS server you want to use.

When you are finished making changes to the Router DNS settings click on the **OK** button. You must save the changes and restart the device for the settings to go into effect.

DHCP Configuration

Us e the DHCP Configuration on LAN menu to configure the Router to act as a DHCP server for the LAN.

DHCP Configuration Menu

Configure LAN DHCP services by defining the following parameters:

Start IP Address	Type in the base address for the IP pool of unassigned IP addresses.
End IP Address	Type in the last address of the contiguous IP address range to be used by the Router for DHCP function.
Netmask	Type in a subnet mask IP address.
Default Gateway	Type in the Default Gateway IP Address that will be assigned to and used by the DHCP clients.
Leased Time	This specifies the amount of time (in hours) a client can lease an IP address, from the dynamically allocated IP pool. A value of 4294967295 assigns permanent IP settings.
Primary DNS	Enter any Internet DNS server IP address available through the WAN connection or use the DNS settings supplied by your service provider.
Secondary DNS	Enter a backup DNS IP address or leave blank.
Primary WINS	Some LANs may require using WINS servers, enter the IP address of the WINS server or leave blank.
Secondary WINS	Enter a back-up WINS server IP address or leave blank.
Domain Name	Enter a domain name for the network group or leave blank.
State	Default = enabled. If you wish to disable the DHCP function, select *disabled* from the drop-down menu.

NAT Configuration

Network Address Translation (NAT) is a routing protocol that allows your network to become a *private* network that is isolated from, yet connected to the Internet. It does this by changing the IP address of packets from a *global* IP address usable on the Internet to a *local* IP address usable on your private network (but not on the Internet) and vice-versa. The Router allows up to 128 host IP addresses.

NAT has two major benefits. First, NAT allows many users to access the Internet using a single global IP address. This can greatly reduce the costs associated with Internet access and also helps alleviate the current shortage of Internet IP addresses. Secondly, the NAT process creates an added degree of security by hiding your private network behind one IP address. The NAT function will normally only allow incoming packets that are generated in response to a request from a host within the LAN.

If your network uses web servers, FTP servers or other proxies used for data requests from outside the private network, you can use NAT in conjunction with Port Redirection to allow appropriate use of your servers by outside users. See the section on Port Redirection for more information.

For the purposes of network administration, NAT is almost indispensable. Hosts and servers on the internal network can be moved easily. Using NAT together with DHCP can greatly reduce the workload of a network manager while allowing tremendous flexibility.

To view the NAT Configuration menu, click on the NAT Configuration button:

NAT Configuration Menu

The following parameters can be configured using the NAT Configuration menu:

|	
NAT Function	Default = enabled. Select *enabled* or *disabled* to enable or disable the NAT function.
DMZ State	Default = disabled. Select *enabled* or *disabled* to enable or disable the DMZ function.
DMZ IP Address	With the DMZ State enabled, type in the LAN IP address of a designated DMZ device. (see explanation below)

DMZ IP Address

NAT may conflict with certain interactive applications such as video conferencing or playing Internet video games. For these applications, a NAT bypass can be set up using a DMZ IP address. The DMZ IP address is a "visible" address and does not benefit from the full protection of the NAT function. Therefore it is advisable that other security precautions be enabled to protect the other computers and devices on the LAN. It may be wise to use isolate the device with the DMZ IP address from the rest of the LAN.

For example, if you want to use video conferencing and still use NAT, you can use the DMZ IP address function. In this case, you must have a PC or server through which video conferencing will take place. The IP address of this PC or server will then be the DMZ IP address. You can designate the server's IP address as the DMZ by typing in the IP address in the **DMZ IP Address** space provided and clicking the **OK** button.

Port Redirection
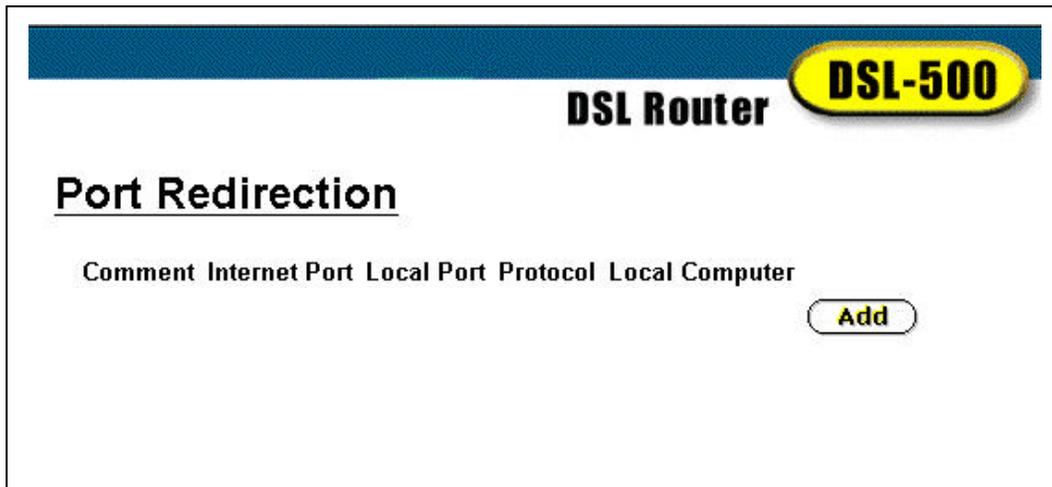
Port Redirection Add Menu

The Port Redirection feature of the Router is used in conjunction with NAT to improve security and efficiency. Port redirection can be used to direct potentially hazardous packets to a proxy server outside your firewall. For example, it is common practice to direct HTTP packets to a designated HTTP server in the DMZ. Other common applications might include directing incoming SMTP packets to an Email server for data scrutiny and improved network efficiency. Click the **Add** button in the Port Redirection window to access the Redirect Port - Add menu.

Port Redirection (continued)

Redirect Port – Add Menu

The Redirect Port window presents eight entry fields:

Comment	Assign an appropriate name to the new route.
Internet Port	Enter the designated TCP or UDP protocol port number or use a well-know port for the particular protocol packet you wish to redirect.
Well-known port	Select one of the well-known ports to redirect incoming packets through that port.
Local Port	Enter the port number used by the designated host on the LAN or use a well-known port.
Well-known port	Select one of the well-known ports to redirect incoming packets through that port on the local host.
Protocol	Choose the protocol either TCP or UDP from the drop-down menu.
Local Computer	Enter the IP address of the local designated host computer or device.

Click the **OK** button when the port redirection parameters have been entered. You can save and reboot the system now, or if you want to add more redirection sets, choose to save later and click the Exit icon to go back to the previous menu.

Static Route Configuration

Use Static Routing to specify a route used for data traffic within your LAN. This can be used to specify that all packets destined for a particular subnet use a predetermined gateway.

Static Route Configuration Table

Up to 18 static route configurations can be entered into the table. To eliminate an existing static route configuration, click the **Delete** button for that configuration.

The information listed for the static route configuration is as follows:

IP Address	IP address of the subnet or device where packets are routed.
Subnet Mask	Subnet mask that allows packets to be routed as intended.
Gateway	IP address of the gateway used for this static route.
Interface	LAN interface
Metric	Maximum number of hops allowed for the static route.
State	Route is enabled or disabled.
Name	Name of the subnet or static route used.

To modify and existing route configuration click on the number for that route to see the configuration menu. To define a new route, click on an unused static route configuration number to see the configuration menu.

Static Route Configuration – Modify/Add

Static Route Configuration Menu

To add or modify a static route, define the following parameters:

Name Provide a name for the static route or subnet (optional).

IP Address Type in the IP address of the subnet or device where packets are routed.

Subnet Mask Type in an appropriate subnet mask that allows the static route to function.

Gateway Type in the IP address of the gateway used for traffic destined for the specified subnet or device.

Metric Type in the maximum number of hops allowed for the static route.

State Enable of disable the route using the drop-down menu.

Click on **OK** to put the static route into the table. It will appear in the Static Route Table shown previously.

To clear the settings for this configuration, click the **Clear** button.

To return to the Static Route Table, click the Exit icon.

Advanced Filter & Firewall

One of the most important elements of any network security implementation is the firewall. Packet filtering is a basic firewall security measure and should be used on any network that is exposed to security risk. A packet filter system examines data packets and scrutinizes them in order to control network access. Filtering rules determine whether packets are passed through the Router from either side of the gateway. The rules are created and controlled by the network administrator and can be precisely defined. These rules are used to block access to the LAN from outside the network and/or to deny access to the WAN from within the network. The Router uses filtering rules to examine data packet headers for specific information. Packets passing through the Router that do not meet the criteria specified by the rule set are dropped.

In order to improve network security without severely limiting network efficiency, it is important to carefully plan the sets of access rules. Effective implementation of packet filtering requires detailed knowledge of network services and communication protocols. An overly complicated filtering scheme can adversely effect routing performance, while an inadequate set of rules may needlessly compromise security.

Packet filtering can be used in conjunction with NAT, port redirection and proxy servers to help provide basic firewall protection. However, these measures do not address many security issues and should be used as only one part of an overall network security strategy. It is important to remember that IP packet filtering examines only the packet header and is not concerned with application information. Therefore, packet filtering does not protect against higher-level security threats that may operate at the application or other level.

Filtering rules can be precisely defined based upon source and destination IP address, as well as port and protocol information. Up to four filter sets can be used; each set contains up to sixteen filtering rules subsets.
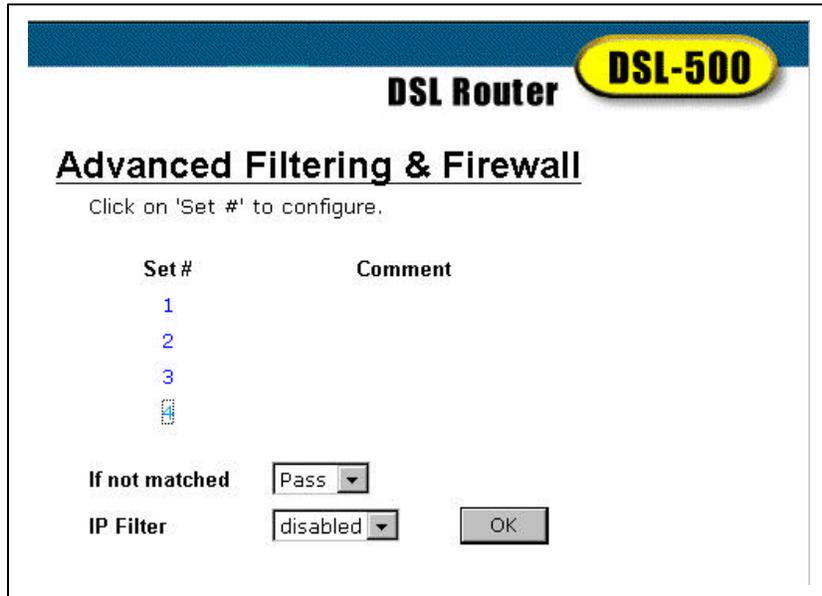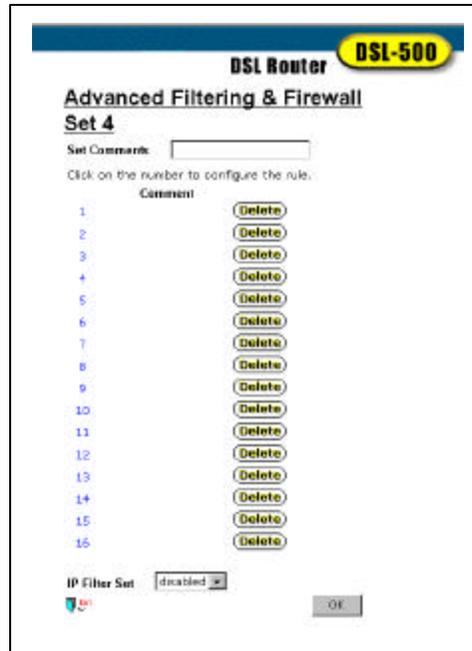

Filter & Firewall Menu 1

The first Filter & Firewall menu lists the four filtering sets, each followed by an identifying comment. Below the list are two drop-down menus. The filtering sets are sets of filtering rules defined in the menus shown below.

When you are finished defining the rules for each set, use the **If not matched** menu to select *Pass* or *Block* for all the sets listed. From the **IP Filter** menu, select *enabled* or *disabled* to enable or disable the listed filtering sets. When all the changes are made to the sets as you want them, click on the **OK** button. You can save the sets and reboot the system now or continue to make other changes.

Create or Modify Packet Filtering

To define new filtering rules or modify an existing one follow these steps:

1. In the first Advanced Filtering and Firewall window, click on the set number you wish to configure to proceed to the Set # window.

Filtering & Firewall – Set # Menu

2. In the Set # window, click on the rule number to define or modify that rule. The rule definition menu appears.

Filtering & Firewall - Define Rules Menu

For each rule in a set, you may define the following parameters:

Comment	Type in an appropriate identifying comment for the rule.
Pass or Block	Select *Pass* or *Block* to perform this action on packets as defined below.
Direction	Select *In* or *Out* to pass or block packets coming in or going out of the network.
Protocol	Select *IGMP*, *TCP*, *UDP* or *All* to pass or block packets of that protocol type.

IP Address Filter Rule

Source	Type in the source IP address and select the Subnet Mask to pass or block packets form that IP address.
Destination	Type in the destination IP address and select the Subnet Mask to pass or block packets destined to that IP address.

Port Filter Rule   UDP and TCP packets only. Select a range of ports to pass or block.

Use the following guide to define the port or port range (Start Port and End Port):

< : specifies the port numbers less than and equal to the Start Port number

> : specifies the port numbers greater than and equal to the Start Port number

= : sets the port number equal to the Start Port if there is no End Port specified; if an End Port number is specified, this defines a range of ports to filter. The range is defined as the port numbers between the Start Port and End Port, including the Start and End Port numbers.

≠ : the port number does <u>not</u> equal to the Start Port if there is no End Port specified; if an End Port number is specified, this defines a range of ports <u>not</u> to filter. The range is defined as the port numbers between the Start Port and End Port, including the Start and End Port numbers.

Filter Rule State   Select *enabled* or *disabled* to enable or disable the filter rule as defined in the menu.

When you have defined the rule, click on **OK**, the <u>Save changes and reboot system</u> prompt will appear. You can save and reboot now, or continue to define more filtering rules.

To clear the rules menu to show the default values, click the **Clear** button.

To return to the Set # menu, click the Exit icon. The comment you entered for new rule will appear next to the rule number.

RIP

To enable RIP or specify use of Version 1 or 2 access the RIP menu.
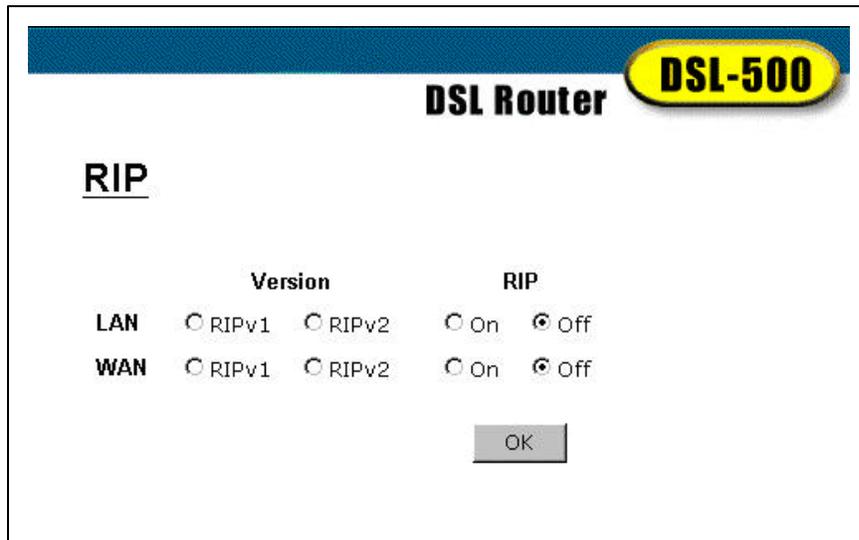
RIP Menu

Select to use RIPv1, RIPv2 or On (both versions) for the LAN and WAN interface. To disable both versions of RIP select Off. Click **OK** to bring up the Save changes and reboot system menu.

Bridge with RFC 1483 Configuration

Menu options for the DSL-500 are different when the connection profile specifies Bridge with RFC 1483 since it is acting in the capacity of a bridge rather than a router. You can see from the figure below that there are fewer menu options for device configuration. Most of the menus in the Configuration file are the same and are used in the same way they are used for Router with PPP configuration. Instructions for using the Connection Profile and Ethernet IP Address menus can be found in the previous section, *Router with PPP Configuration*.

The Layer 2 Filtering menu only appears when the device is in bridge mode.
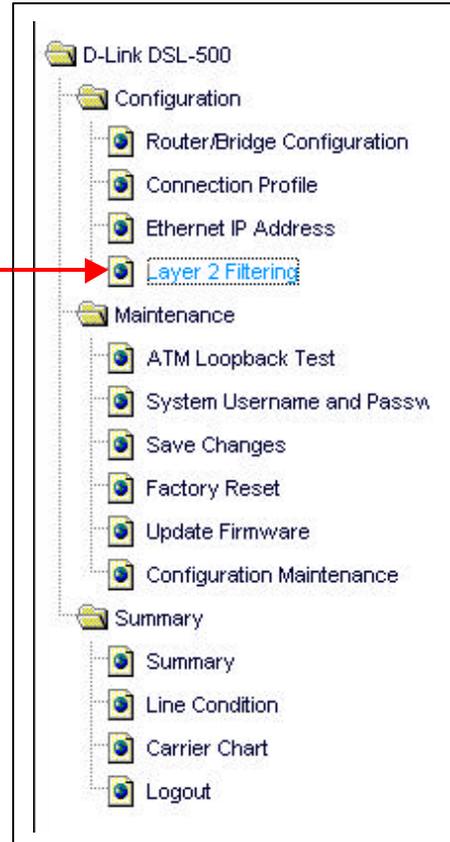
Bridge Configuration Menus

Change Encapsulation - Bridge Configuration

When the device connection profile defines the device as a Bridge with RFC 1483, the first window that appears after login is the Bridge/Router Configuration window. Use this menu to change the encapsulation method used for packets transported through the bridge.

Bridge Configuration Menu

To change the **Encapsulation Method**, click *LLC* or *VC mux* as specified by your service provider and click the **OK** button. You will see the <u>Save changes and reboot system?</u> menu. The default encapsulation setting is LLC.

This menu may also be used change the connection method in the **Connection Profile** drop-down menu.

Layer 2 Filtering (bridge mode only)

The Layer 2 filtering option is available in the bridge configuration folder, it is not an option when the device is configured as a router.

Layer 2 Filter Menu

By default, the bridge will pass all packets in either direction. You may specify that certain types of packets be dropped in order to free up bandwidth or improve security. To block a packet type, click in the box so that check mark does not appear in the box and click **OK**. You will see the Save changes and reboot system? menu.

Maintenance

The Maintenance folder contains the same menus for bridge and router configurations with the exception of the Remote Administration Access option, available only for router configurations.

ATM Loopback Test

ATM loopback tests are used to verify connectivity and path integrity along a specified ATM circuit. In the test, a cell is sent to an endpoint or to the end of the first segment of the ATM path. If the path is available and the connections are functioning, an test cell will be returned along the same ATM path and be detected by the device. This is very similar to a Ping test. The test can help to determine if connectivity problems originate from outside the LAN.

ATM Loopback Screen

To perform the test, define the following parameters:

VPI   Type in the VPI setting used for the network connection.

VCI   Type in the VCI setting used for the network connection.

F4/F5   Choose *F4* (Virtual Path) or *F5* (Virtual Connection) from the pull-down menu to define the flow type. An F4 flow test is used to verify that ATM network information (ATM cells) can be shared between network elements. This information is used within virtual paths to report an unavailable path or a virtual path that cannot be guaranteed. An F5 flow test is also used to verify that ATM network information can be shared between network elements. This information is used within virtual connections to report degraded virtual channel performance such as late arriving cells, lost cells, and cell insertion problems.

etoe/segment   Select the test type from the remaining pull-down menu. Choose *End-to-End* to test the entire path from the Router to the ATM connection endpoint. Choose *segment* to test the path from the Router to the end of the first ATM connection segment.

Status   A success or fail message appears here after the test is completed. If the reply cell is received within the standard-defined time, the Status will read *OK*. This indicates that the specified test path is functioning normally and all connections were successful. If the Status reads *Fail*, there is a fault in the segment or path tested.

When all the test parameters have been specified, click on the **Loop Test** button to initiate the test.

System Username and Password

Use this screen to change the username and password used to access the Web Manager. The Web Manager can be accessed remotely from outside the LAN when it is functioning in router mode using the Remote Administration Access menu (described in a later section).

User Name and Password Menu

1. Type the current **User Name** in the entry field provided.

2. Type in the current password in the **Old Password** entry field.

3. Type in the **New Password** in the entry field provided.

4. Type in the new password again in the **Confirm New Password** field.

5. Click the **OK** button. The <u>**Save changes and reboot system?**</u> message appears.

Save Changes

In order to save the configuration changes you have just made they must be saved to the Router's non-volatile RAM. In the Maintenance folder, click on the Save Changes button to access the menu below:
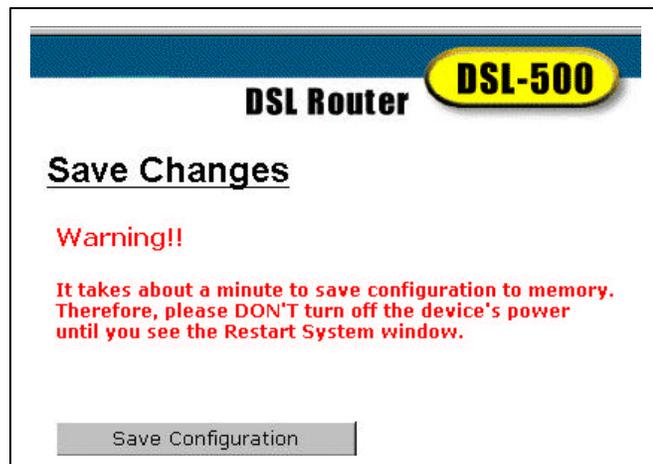
Save Changes Menu

1. Click the **Save Configuration** button. A pop-up message window will inform you that the Router must be restarted. Do not turn off the power to the Router while the settings are being saved.

2. When the **Restart System** window appears, click the **Restart** button.
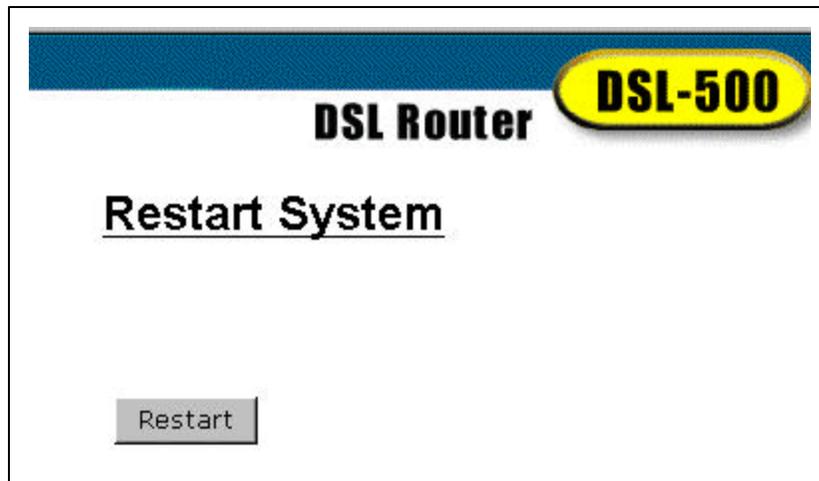
Restart System Window

Factory Reset

The DSL-500 can be reset to the default configuration for all settings using the Factory Reset option. This will also change the both the LAN and WAN IP address of the device, so these will need to be reconfigured accordingly.
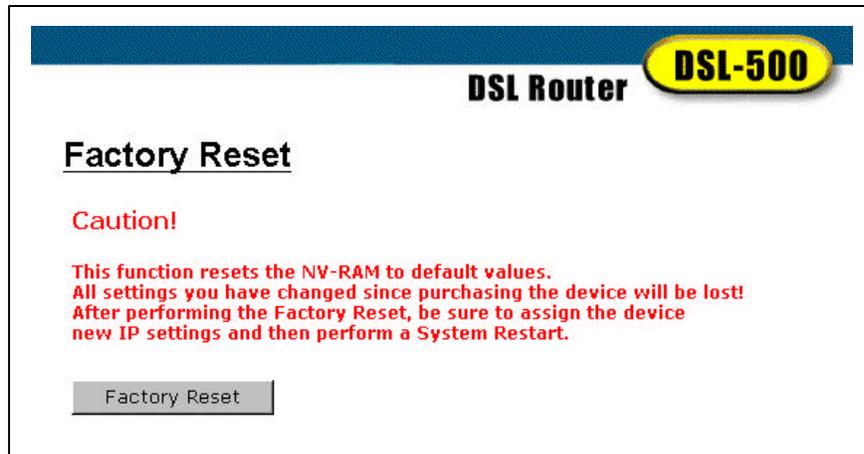
Factory Reset Screen

To perform a factory reset, click the **Factory Reset** button. Since the IP settings will return to their default, you will lose access to the Web Manager. To use the Web Manager interface, the LAN IP address will need to be reconfigured.

Update Firmware

Use the Update Firmware feature to load the latest firmware for the device. You can obtain the latest version of the DSL-500 firmware by logging onto the D-Link web site at www.dlink.com. Access the D-Link web site by clicking on the D-Link logo in the upper left corner of the browser window. Save the latest firmware version to a file on the Manager PC or accessible server.
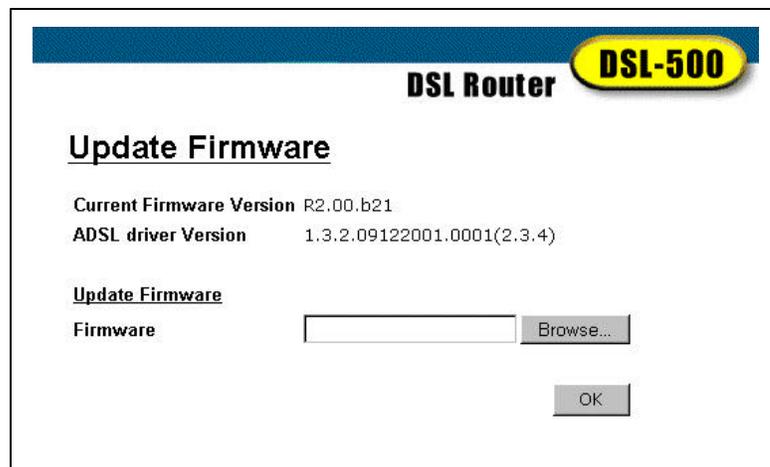
Update Firmware Screen

To upgrade firmware, type in the name and path of the file or click on the **Browse** button to search for the file. Click the **OK** button to begin copying the file. The file will load and restart automatically.

Configuration File Maintenance

Use the Configuration File Maintenance store current settings to a file on the Manager PC or to load previously saved configuration files on the device.

Configuration Maintenance Screen

To save the current settings to a configuration file on the PC, click on the lower **OK** button, after the *Backup configuration file* option. The file will be saved as dslmodem.cfg or you can specify another file name.

To load a saved configuration file form the PC, type in the full name and path in the Configuration File space or click on the **Browse** button to search for the file.

Remote Administration Access (Router mode only)

The Router can be administered using a PC located outside the LAN. Permission to allow remote management must first be allowed by enabled remote management.

Remote Administration Access

Enable remote access to the web manager by selecting *Yes* and clicking **OK**. The Save changes and reboot? Prompt will appear. Remote Administration is disabled by default.

Summary

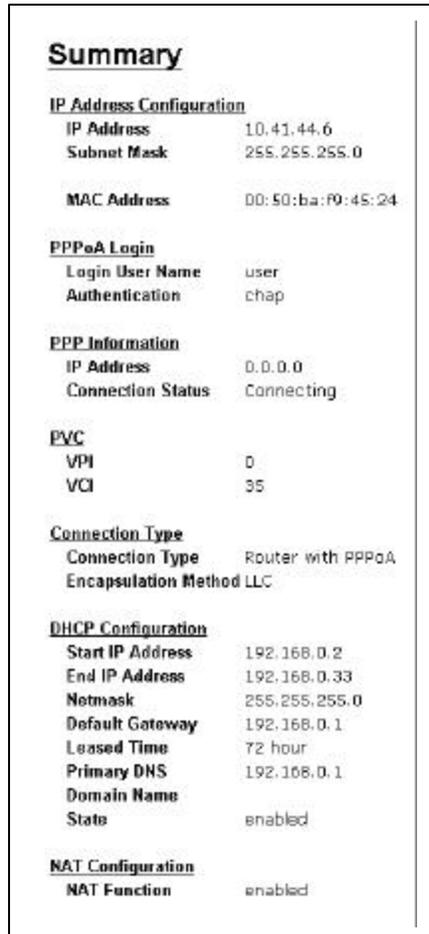The contents of the Summary folder differ depending on the mode of operation used by the device. In router mode, the folder offers two additional screens, a DHCP table and a runtime routing table. In addition, the Summary chart contains different information.

Summary

IP Address Configuration
IP Address   10.41.44.6
Subnet Mask   255.255.255.0

MAC Address   00:50:ba:f0:45:24

PPPoA Login
Login User Name   user
Authentication   chap

PPP Information
IP Address   0.0.0.0
Connection Status   Connecting

PVC
VPI   0
VCI   35

Connection Type
Connection Type   Router with PPPoA
Encapsulation Method LLC

DHCP Configuration
Start IP Address   192.168.0.2
End IP Address   192.168.0.33
Netmask   255.255.255.0
Default Gateway   192.168.0.1
Leased Time   72 hour
Primary DNS   192.168.0.1
Domain Name
State   enabled

NAT Configuration
NAT Function   enabled

Router Summary Screen

In router mode, the information presented in the Summary screen is as follows:

LAN IP Address Configuration

IP Address	LAN IP Address of the Router
Subnet Mask	Router Subnet Mask on the LAN
MAC Address	Router MAC Address

PPP Login

Login User Name	User name for PPP log in
Authentication	Authentication method used for PPP connection

PPP Information

IP Address	WAN IP Address used by the Router
Connection Status	Status of WAN connection

PVC Information

    VPI   Virtual Path Identifier

    VCI   Virtual Circuit Identifier

Connection

    Connection Type   PPPoA, PPPoE or IPoA

    Encapsulation Method   Packet encapsulation method used LLC or VC Mux

DHCP Information

    Start IP Address   Beginning IP address used for LAN DHCP scheme

    End IP Address   Ending IP address used for LAN DHCP scheme

    Netmask   Subnet Mask used on LAN

    Default Gateway   LAN default gateway IP address

    Leased Time   LAN IP address lease time

    Primary DNS   DNS server IP address

    Domain Name   Domain name used

    State   DHCP enable or disabled

NAT Configuration

    NAT Function   NAT enabled or disabled
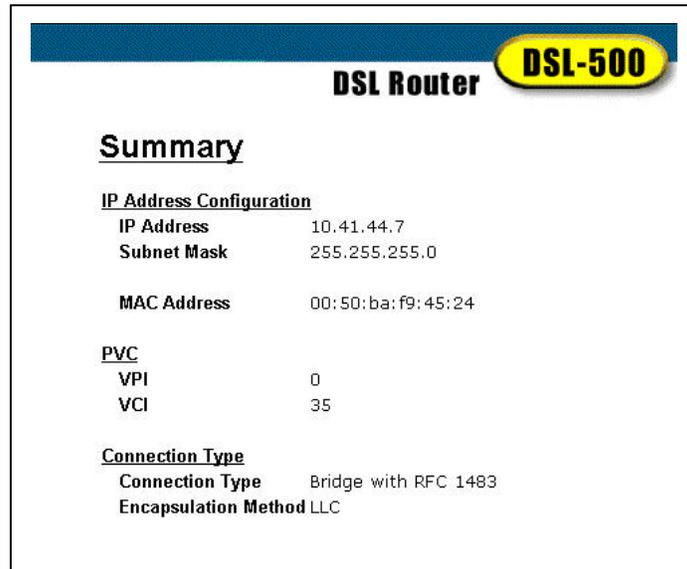
Bridge Summary Screen

In bridge mode, the device does not contain information associated with router functions in the Summary screen.

Line Condition

In the Line Condition window you can monitor the characteristics of the ADSL connection and confirm that it has been established.

Line Condition Screen

Line condition statistics listed here are as follows:

Protocol

Data Path	Current data path type Fast or Interleaved
Operation Mode	Modulation technique used for ADSL connection, G.DMT or G.lite

Rate

Downstream	Downstream data transfer rate in Kbps
Upstream Rate	Upstream data transfer rate in Kbps

SNR

SNR	Signal-to-noise ratio in dB

ATEN

ATEN Downstream	Downstream attenuation of signal in dB
ATEN Upstream	Upstream attenuation of signal in dB

Loop Distance

Loop Distance	Loop in K ft. range = 0 – 18 K ft.

Near End

Number of data transfer errors on the near end (ATU-R) listed according to the correction technique

- FEC Forward Error Correction

- CRC Cyclic Redundancy Control

- HEC Header Error Check

Far End

Number of data transfer errors on the far end (ATU-C) listed according to the correction technique

- FEC Forward Error Correction

- CRC Cyclic Redundancy Control

- HEC Header Error Check

Carrier Chart

The Carrier Chart illustrates the data rates distributed across the upstream and downstream frequency ranges.
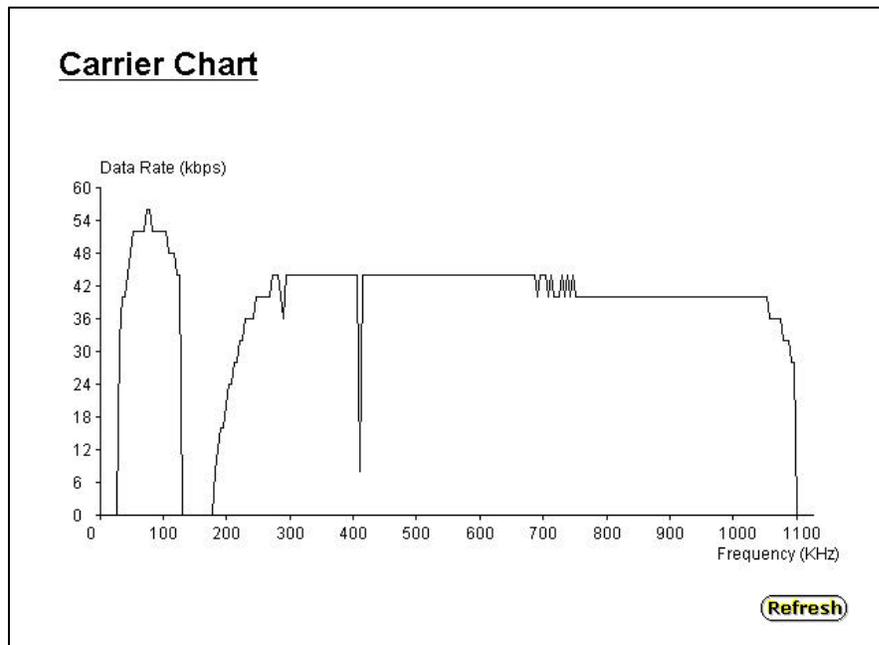
Carrier Chart

This chart can be used to gauge signal quality for the entire upstream (lower portion) and downstream (upper portion) range of discrete modular tones. The example above displays normal signal function for the full range of frequencies.

DHCP Allocation Table (Router mode only)

The DHCP Allocation Table provides a summary of current IP setting allocation for the network.
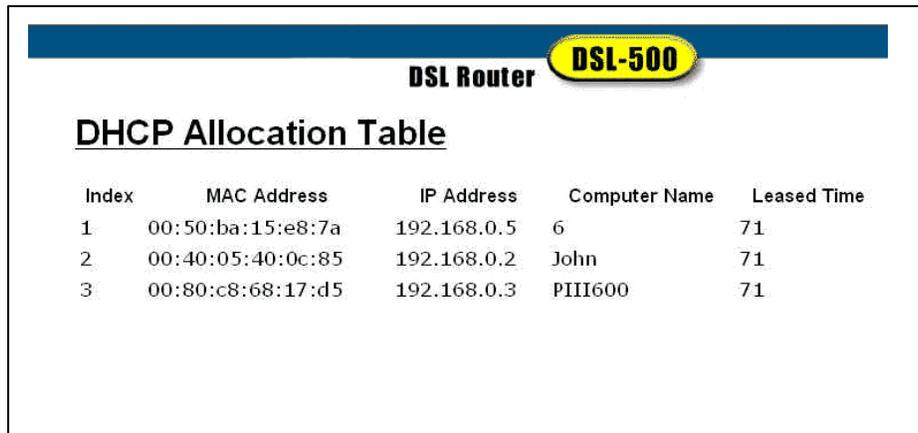
DHCP Allocation Table

Information listed in the DHCP Allocation Table includes the following:

Index	Index reference number for entry
MAC Address	MAC address of computer or networked device
IP Address	Assigned IP address of computer or networked device
Computer Name	Name of computer or networked device
Leased Time	Leased time of assigned IP address

Runtime Routing Table (Router mode only)

The Runtime Routing Table provides a summary of dynamic and static routing information for both the LAN and WAN interface.

Runtime Routing Table

Information listed in the Runtime Routing Table includes the following:

IP Address   IP address of network, subnet or device used for route

Subnet Mask   Subnet mask used for route

Gateway   IP address of gateway device used for route

Protocol   Route protocol or type, Direct or Static

Interface   Interface of network, subnet or device used for router, LAN or WAN

Metric   Number of hops used/allowed for route

Name   Name assigned to route

6

LAN Setup

The Router allows many possibilities for network layout. This gives the network administrator much flexibility to decide how best to use it. One of the most important decisions for the network administrator involves IP addressing on the LAN. The easiest choice in most cases is to let the Router take care of it for you using DHCP, which is done by default. This chapter discusses the various alternatives for IP address assignment using the Router.

Assigning Network IP Addresses

The IP address settings, which include the IP address, subnet mask and gateway IP address are the first and most important internal network settings that need to be configured. The Router is assigned a default LAN IP address and subnet mask. If you do not have a preexisting IP network and are setting one up now, using the factory default IP address settings can greatly ease the setup process. If you already have a preexisting IP network, you can adjust the IP settings for the Router to fit within your existing scheme.

Using the Default IP Address

The Router comes with a preset default IP address setting of 192.168.0.1 for the LAN port. There are two ways to use this default IP address, you can manually assign an IP address and subnet mask for each PC on the LAN or you can instruct the Router to automatically assign them using DHCP. The simplest method is to use DHCP. The DHCP function is active by default.

Manual IP Address Assignment

You can manually set the IP address, subnet mask and default gateway on each computer by performing the following steps for each PC on the network:

1. In Windows 95/98, click on the **START** button, go to **Settings** and choose **Control Panel**.

2. In the window that opens, double-click on the **Network** icon.

3. Under the Configuration tab, select the **TCP/IP** component and click *Properties*.

4. Choose the *Specify an IP address* option and edit the address settings accordingly. Consult the table below for IP settings on a Class C network.

Default Addressing Example			
Host	**IP Address**	**Subnet Mask**	**Gateway IP**
Router	192.168.0.1	255.255.255.0	
Computer #1	192.168.0.2	255.255.255.0	192.168.0.1
Computer #2	192.168.0.3	255.255.255.0	192.168.0.1
Computer #3	192.168.0.4	255.255.255.0	192.168.0.1

Please note that when using the default IP address as in the above example, the first three numbers in the IP address must always be the same with only the fourth number changing (for a Class C network). This is because the first three numbers define the network IP address (all machines must belong to the same IP network), while the last number denotes the host IP address (each computer must have a unique address to distinguish it on the network). Also note that the subnet mask is the same for all machines and the default gateway address is the LAN IP address of the Router.

It is a good idea to make a note of each device's IP address for reference during troubleshooting or when adding new stations or devices.

Using DHCP

The second way to use the default settings is to allow the Router to automatically assign IP addresses to your computers using DHCP. To do this, simply make sure your computers' IP addresses are set to 0.0.0.0 (under Windows, choose the option Obtain an IP address automatically in the TCP/IP network component described above). When the computers are restarted, their IP settings will automatically be assigned by the Router. The Router is set by default to use DHCP. See the discussion in Chapter 5 for information on how to use configure the Router for DHCP.

Changing the IP Address of the Router

If you choose to change the IP address of the Router you will need to access the device directly via the RS-232 connection using a terminal emulation interface (such as Microsoft HyperTerminal used in the sample screen captures). Your terminal parameters will need to be set to:

       C. VT-100/ANSI compatible

       D. Terminal keys enabled

       E. 9,600 baud

       F. 8 data bits

       G. No parity

       H. One stop bit

Connect a standard RS-232 (DB-9 to DB-9) cable to the Router's RS-232 port on the rear panel, connect the other end to a PC with a terminal emulation program already installed. Power on the Router and launch the emulation program. The terminal emulator will display system information while the unit undergoes self-testing. When `192.168.0.1>` appears on the screen the unit has completed its self-test. In this mode, the default IP address 192.168.0.1 and an angle bracket ("greater than") will appear each time the Enter key is depressed.
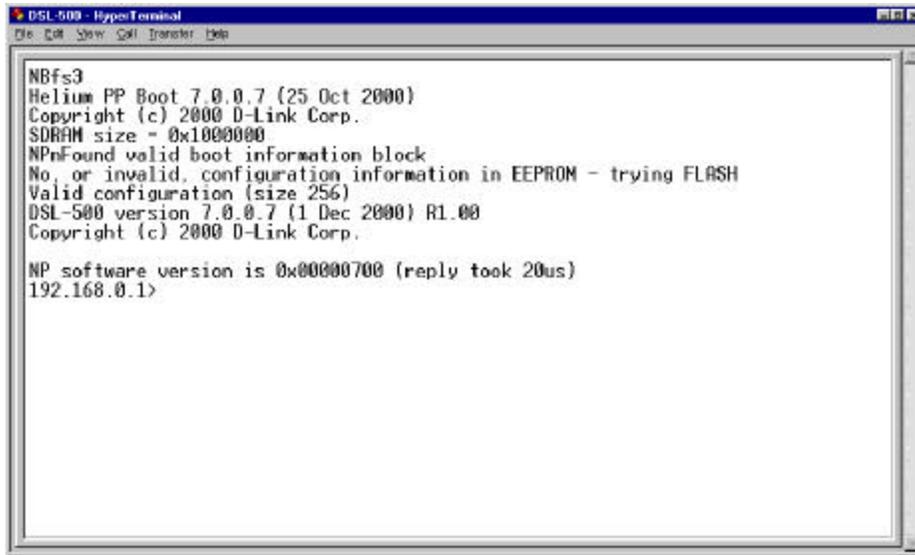
HyperTerminal Interface (Boot Up)

To change the IP address of the Router type **ip** after the command prompt and hit Enter. Be sure to type commands using all lower case letters as the console interface is case sensitive. A new command prompt **192.168.0.1 ip>** will appear indicating that the unit is now ready to accept ip commands.

Type the following command series after the ip prompt: **enable ethernet** followed by the **new IP address** to be assigned to the device as seen in the example below.
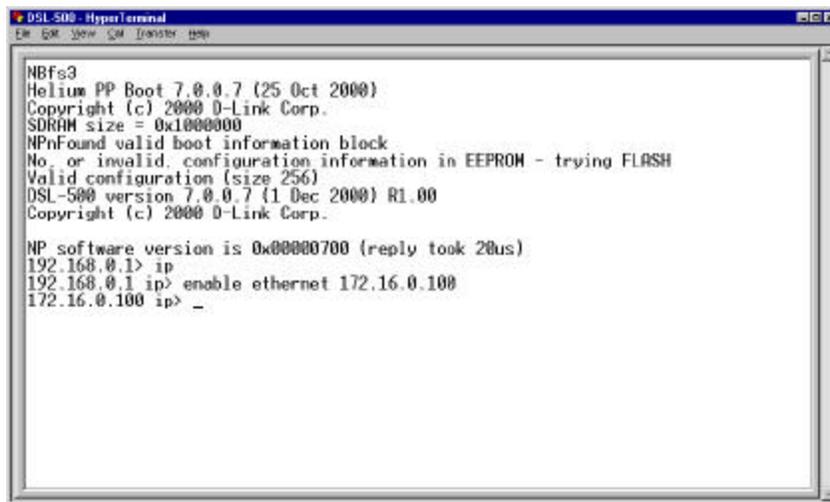
HyperTerminal Interface with new IP address

You must save the new IP address by typing the command series **config save** and pressing Enter. This will save the new IP address for the Router and store it in the device's flash memory. You may now disconnect the terminal emulator and access the device using the web-based management interface for configuration. For more thorough instructions on using the out-of-band console manager, see Chapter 7. FIND ALL REFS

A

Technical Specifications

GENERAL		
STANDARDS:	• ITU G.992.1 (G.dmt) • ITU G.992.2 (G.lite) • ITU G.994.1 (G.Hs) • ITU-T Rec. I.361 • ITU-T Rec. I.610 • IEEE 802.3 • IEEE 802.3u • IEEE 802.1d • RFC 791 (IP Routing) • RFC 792 (UDP) • RFC 826 (ARP) • RFC 1058 (RIP 1) • RFC 1389 (RIP 2) • RFC 1213 compliant • RFC 1483 (Bridged Ethernet) • RFC 1577 (IP over ATM)	• RFC 1661 (PPP) • RFC 1994 (CHAP) • RFC 1334 (PAP) • RFC 2364 (PPP over ATM) • RFC 1631 (NAT) • RFC 1877 (Automatic IP assignment) • RFC 2516 (PPP over Ethernet) • Supports RFC 2131 and RFC 2132 (DHCP) • Compatible with all T1.413 issue 2 (full rate DMT over analog POTS), and CO DSLAM equipment • Supports ATM Forum UNI V3.1 PVC
PROTOCOLS:	TCP/IP UDP RIP-1 RIP-2 IGMP	DHCP BOOTP ARP AAL5
DATA TRANSFER RATE:	G.dmt full rate: Downstream up to 8 Mbps Upstream up to 640 Kbps G.lite: Downstream up to 1.5 Mbps Upstream up to 512 Kbps	
MEDIA INTERFACE EXCHANGE:	RJ-11 port ADSL telephone line connection RJ-45 port for 10BASET Ethernet connection RS-232 (DB9 female) console port for local configuration	

Physical and Environmental	
DC inputs: Power Adapter:	Input: 120V AC 60Hz 24W Output: 12V DC 1.0 A
Power Consumption:	10 Watts (max)
Operating Temperature:	0° to 40° C (32° - 104° F)
Humidity:	5 to 95% (non-condensing)
Dimensions:	215 mm x 163 mm x 45 mm
Weight:	455 gm (1 lb.)
EMI:	CE Class B FCC Class B
Safety:	UL/CUL TUV
Reliability:	Mean Time Between Failure (MTBF) min. 4 years

B

IP Concepts

This appendix describes some basic IP concepts, the TCP/IP addressing scheme and show how to assign IP Addresses.

When setting up the Router, you must make sure it has a valid IP address. Even if you will not use the WAN port (ADSL port), you should, at the very least, make sure the Ethernet LAN port is assigned a valid IP address. This is required for telnet, in-band SNMP management, and related functions such as "trap" handling and TFTP firmware download.

IP Addresses

The Internet Protocol (IP) was designed for routing data between network sites all over the world, and was later adapted for routing data between networks within any site (often referred to as "subnetworks" or "subnets"). IP includes a system by which a unique number can be assigned to each of the millions of networks and each of the computers on those networks. Such a number is called an IP address.

To make IP addresses easy to understand, the originators of IP adopted a system of representation called "dotted decimal" or "dotted quad" notation. Below are examples of IP addresses written in this format:

<div align="center">

201.202.203.204   189.21.241.56   125.87.0.1

</div>

Each of the four values in an IP address is the ordinary decimal (base 10) representation of a value that a computer can handle using eight "bits" (binary digits — 1s and 0s). The dots are simply convenient visual separators.

Zeros are often used as placeholders in dotted decimal notation; 189.21.241.56 can therefore also appear as 189.021.241.056.

IP networks are divided into three classes on the basis of size. A full IP address contains a network portion and a "host" (device) portion. The network and host portions of the address are different lengths for different classes of networks, as shown in the table below.
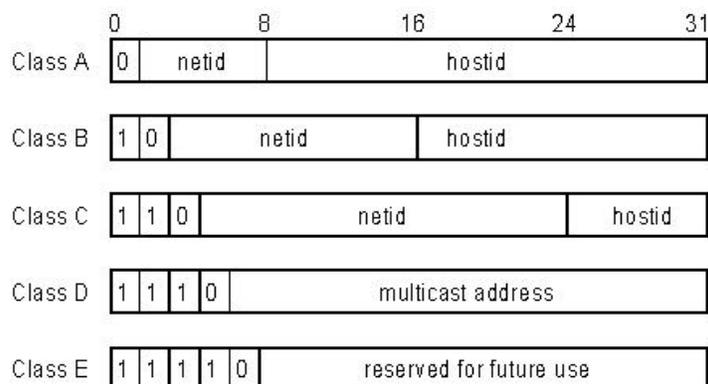
Networks attached to the Internet are assigned class types that determine the maximum number of possible hosts per network. The previous figure illustrates how the net and host portions of the IP address differ among the three classes. Class A is assigned to networks that have more than 65,535 hosts; Class B is for networks that have 256 to 65534 hosts; Class C is for networks with less than 256 hosts.

IP Network Classes			
Class	**Maximum Number of Networks in Class**	**Network Addresses (Host Portion in Parenthesis)**	**Maximum Number of Hosts per Network**
A	126	1(.0.0.0) to 126(.0.0.0)	16,777,214
B	16,382	128.1(.0.0) to 191.254(.0.0)	65,534
C	2,097,150	192.0.1(.0) to 223.255.254(.0)	254

Note: **All network addresses outside of these ranges (Class D and E) are either reserved or set aside for experimental networks or multicasting.**

When an IP address's host portion contains only zero(s), the address identifies a network and not a host. No physical device may be given such an address.

The network portion must start with a value from 1 to 126 or from 128 to 223. Any other value(s) in the network portion may be from 0 to 255, except that in class B the network addresses 128.0.0.0 and 191.255.0.0 are reserved, and in class C the network addresses 192.0.0.0 and 223.255.255.0 are reserved.

The value(s) in the host portion of a physical device's IP address can be in the range of 0 through 255 as long as this portion is not all-0 or all-255. Values outside the range of 0 to 255 can never appear in an IP address (0 to 255 is the full range of integer values that can be expressed with eight bits).

The network portion must be the same for all the IP devices on a discrete physical network (a single Ethernet LAN, for example, or a WAN link). The host portion must be different for each IP device — or, to be more precise, each IP-capable port or interface — connected directly to that network.

The network portion of an IP address will be referred to in this manual as a **network number**; the host portion will be referred to as a **host number**.

To connect to the Internet or to any private IP network that uses an Internet-assigned network number, you must obtain a registered IP network number from an Internet-authorized network information center. In many countries you must apply through a government agency, however they can usually be obtained from your Internet Service Provider (ISP).

If your organization's networks are, and will always remain, a closed system with no connection to the Internet or to any other IP network, you can choose your own network numbers as long as they conform to the above rules.

If your networks are isolated from the Internet, e.g. only between your two branch offices, you can assign any IP Addresses to hosts without problems. However, the Internet Assigned Numbers Authority (IANA) has reserved the following three blocks of IP Addresses specifically for private (stub) networks:

Class	Beginning Address	Ending Address
A	10.0.0.0	10.255.255.255
B	172.16.0.0	172.31.255.255
C	192.168.0.0	192.168.255.255

It is recommended that you choose private network IP Addresses from the above list. For more information on address assignment, refer to RFC 1597, *Address Allocation for Private Internets* and RFC 1466, *Guidelines for Management of IP Address Space*.

Subnet Mask

In the absence of subnetworks, standard TCP/IP addressing may be used by specifying subnet masks as shown below.

IP Class	Subnet Mask
Class A	255.0.0.0
Class B	255.255.0.0
Class C	255.255.255.0

Subnet mask settings other than those listed above add significance to the interpretation of bits in the IP address. The bits of the subnet mask correspond directly to the bits of the IP address. Any bit an a subnet mask that is to correspond to a net ID bit in the IP address must be set to 1.

C

DSL-500 Firmware Upgrade Utility

You can update system firmware using the DSL-500 Firmware Upgrade Utility. To upgrade the Router's firmware you must have installed this software on the PC you wish to use for this purpose. Install the utility by clicking the file titled **setup.exe** located on the Installation CD-ROM. It will be installed automatically. It is recommended that the PC be directly connected to the Router using a crossed cable, however you may upgrade it through the LAN from a remote host.

You also need to download the latest firmware version file from the D-Link web site to the PC on which you will use the Upgrade Utility. Instructions for downloading the firmware are located on the web site at www.dlink.com

To launch the DSL-500 Firmware Upgrade Utility, click on the icon. Allow a few moments for the software to discover the Router on the network. After the discovery phase the following window will appear. You will see all the DSL-500 Routers on your network. You can identify individual devices by either its IP address or its MAC address. Select the device you wish to upgrade by double clicking on it.
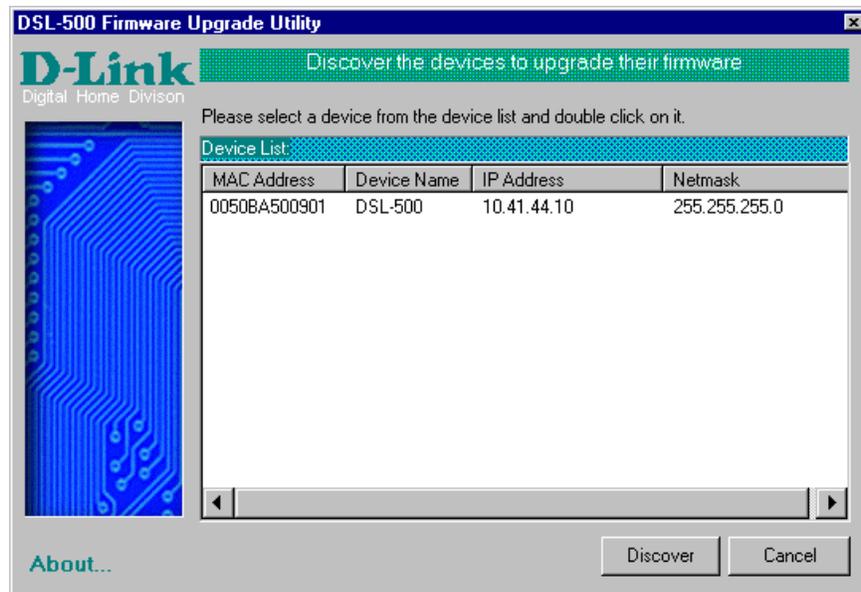
When you select a Router to upgrade you will be prompted for a password. The default password is **admin**. If you want to change the password, you can change it using the console manager interface as described in Chapter 6.
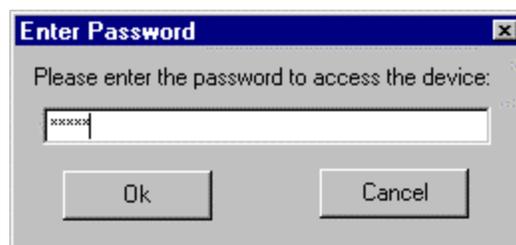

Enter the password and click OK.

In the new window you will see the MAC address of the Router and the IP address of the PC you are using. The PC and the Router must be on the same subnet for the upgrade to be completed. The upgrade utility will suggest a new IP address to be temporarily assigned to the device during the firmware upgrade procedure. Check the suggested IP address listed for the Router to be sure that it does not conflict with any existing IP addresses on your network. To change the temporary IP address of the Router, type in an available IP address in the space provided. You should change only the host portion of the address.

To upload the new firmware to the selected Router click the 'Upgrade' button. The utility will automatically load the new firmware. During the upgrade process it is important that you allow the entire file to load onto the device. Do not turn off the Router while the flash memory is being updated. A warning will appear during the upgrade reminding you not to power off the device.

When the new firmware has been successfully loaded a new window will inform you of the upgrade and tell you that the Router has been restarted. Click OK to proceed.
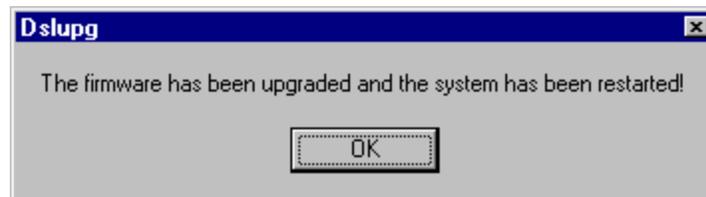
D-Link® Offices

AUSTRALIA	**D-LINK AUSTRALASIA** Unit 16, 390 Eastern Valley Way, Roseville, NSW 2069, Australia TEL: 61-2-9417-7100 FAX: 61-2-9417-1077 TOLL FREE: 1800-177-100 (Australia), 0800-900900 (New Zealand) URL: www.dlink.com.au E-MAIL: support@dlink.com.au, info@dlink.com.au
CANADA	**D-LINK CANADA** 2180 Winston Park Drive, Oakville, Ontario L6H 5W1 Canada TEL: 1-905-829-5033 FAX: 1-905-829-5223 BBS: 1-965-279-8732 FREE CALL: 1-800-354-6522 URL: www.dlink.ca FTP: ftp.dlinknet.com E-MAIL: techsup@dlink.ca
CHILE	**D-LINK SOUTH AMERICA** Isidora Goyenechea #2934 of.702, Las Condes, Santiago, Chile TEL: 56-2-232-3185 FAX: 56-2-2320923 URL: www.dlink.cl E-MAIL: ccasassu@dlink.cl, tsilva@dlink.cl
DENMARK	**D-LINK DENMARK** Naverland 2, DK-2600 Glostrup, Copenhagen, Denmark TEL:45-43-969040 FAX:45-43-424347 URL: www.dlink.dk E-MAIL: info@dlink.dk
EGYPT	**D-LINK MIDDLE EAST** 7 Assem Ebn Sabet Street, Heliopolis Cairo, Egypt TEL: 202-2456176 FAX: 202-2456192 URL: www.dlink-me.com E-MAIL: support@dlink-me.com, fateen@dlink-me.com
FRANCE	**D-LINK FRANCE** Le Florilege #2, Allee de la Fresnerie 78330 Fontenay Le Fleury France TEL: 33-1-30238688 FAX: 33-1-3023-8689 URL: www.dlink-france.fr E-MAIL: info@dlink-france.fr
GERMANY	**D-LINK CENTRAL EUROPE/D-LINK DEUSTSCHLAND GMBH** Schwalbacher Strasse 74, 65760 Eschborn Germany TEL: 49-(0) 6196-7799-0 FAX: 49-(0) 6196-7799-300 URL: www.dlink.de E-MAIL: mbischoff@dlink.de, mboerner@dlink.de
INDIA	**D-LINK INDIA** Plot No.5, Kurla-Bandra Complex Road, Off Cst Road, Santacruz (E), Bombay - 400 098 India TEL: 91-22-652-6696 FAX: 91-22-652-8914 URL: www.dlink-india.com E-MAIL: service@dlink.india.com

ITALY	**D-LINK ITALY**
	Via Nino Bonnet No. 6/b, 20154 Milano, Italy
	TEL: 39-02-2900-0676
	FAX: 39-02-2900-1723
	E-MAIL: info@dlink.it
	URL: www.dlink.it
JAPAN	**D-LINK JAPAN**
	10F, 8-8-15 Nishi-Gotanda, Shinagawa-ku, Tokyo 141 Japan
	TEL: 81-3-5434-9678
	FAX: 81-3-5434-9868
	URL: www.d-link.co.jp
	E-MAIL: kida@d-link.co.jp
RUSSIA	**D-LINK RUSSIA**
	Michurinski Prospekt 49, 117607 Moscow, Russia
	TEL: 7-095-737-3389, 7-095-737-3492 FAX: 7-095-737-3390
	E-MAIL: vl@dlink.ru
SINGAPORE	**D-LINK INTERNATIONAL**
	1 International Business Park, #03-12 The Synergy, Singapore 609917
	TEL: 65-774-6233 FAX: 65-774-6322
	URL: www.dlink-intl.com
	E-MAIL: info@dlink.com.sg
S. AFRICA	**D-LINK SOUTH AFRICA**
	Unit 2, Parkside 86 Oak Avenue
	Highveld Technopark Centurion, Gauteng, Republic of South Africa
	TEL: 27(0)126652165 FAX: 27(0)126652186
	CELL NO: 0826010806 (Bertus Moller)
	CELL NO: 0826060013 (Attie Pienaar)
	E-MAIL: bertus@d-link.co.za, attie@d-link.co.za
SWEDEN	**D-LINK SWEDEN**
	P.O. Box 15036, S-167 15 Bromma Sweden
	TEL: 46-(0)8564-61900
	FAX: 46-(0)8564-61901
	E-MAIL: info@dlink.se
	URL: www.dlink.se
TAIWAN	**D-LINK TAIWAN**
	2F, No. 119 Pao-Chung Road, Hsin-Tien, Taipei, Taiwan
	TEL: 886-2-2910-2626
	FAX: 886-2-2910-1515
	URL: www.dlinktw.com.tw
	E-MAIL: dssqa@tsc.dlinktw.com.tw
U.K.	**D-LINK EUROPE**
	D-Link (Europe) Ltd. 4th Floor Merit House,
	Edgware Road, Colindale, London NW95AB U.K.
	TEL: 44-20-8731-5555 FAX: 44-20-8731-5511
	URL: www.dlink.co.uk
	E-MAIL: info@dlink.co.uk
U.S.A	**D-LINK U.S.A.**
	53 Discovery Drive, Irvine, CA 92618 USA
	TEL: 1-949-788-0805 FAX: 1-949-753-7033
	INFO LINE: 1-800-326-1688
	BBS: 1-949-455-1779, 1-949-455-9616
	URL: www.dlink.com
	E-MAIL: tech@dlink.com, support@dlink.com

Registration Card

Print, type or use block letters.

Your name: Mr./Ms _____

Organization: _____Dept._____

Your title at organization:_____

Telephone:_____ Fax:_____

Organization's full address:_____

_____

Country:_____

Date of purchase (Month/Day/Year):_____

Product Model	Product Serial No.	* Product installed in type of computer (e.g., Compaq 486)	* Product installed in computer serial No.

(* Applies to adapters only)

Product was purchased from:

Reseller's name:_____

Telephone:_____ Fax:_____

Reseller's full address:_____

_____

Answers to the following questions help us to support your product:

1. Where and how will the product primarily be used?
   ☐Home ☐Office ☐Travel ☐Company Business ☐Home Business ☐Personal Use

2. How many employees work at installation site?
   ☐1 employee ☐2-9 ☐10-49 ☐50-99 ☐100-499 ☐500-999 ☐1000 or more

3. What network protocol(s) does your organization use ?
   ☐XNS/IPX ☐TCP/IP ☐DECnet ☐Others_____

4. What network operating system(s) does your organization use ?
   ☐D-Link LANsmart ☐Novell NetWare ☐NetWare Lite ☐SCO Unix/Xenix ☐PC NFS ☐3Com 3+Open
   ☐Banyan Vines ☐DECnet Pathwork ☐Windows NT ☐Windows NTAS ☐Windows '95
   ☐Others_____

5. What network management program does your organization use ?
   ☐D-View ☐HP OpenView/Windows ☐HP OpenView/Unix ☐SunNet Manager ☐Novell NMS
   ☐NetView 6000 ☐Others_____

6. What network medium/media does your organization use ?
   ☐Fiber-optics ☐Thick coax Ethernet ☐Thin coax Ethernet ☐10BASE-T UTP/STP
   ☐100BASE-TX ☐100BASE-T4 ☐100VGAnyLAN ☐Others_____

7. What applications are used on your network?
   ☐Desktop publishing ☐Spreadsheet ☐Word processing ☐CAD/CAM
   ☐Database management ☐Accounting ☐Others_____

8. What category best describes your company?
   ☐Aerospace ☐Engineering ☐Education ☐Finance ☐Hospital ☐Legal ☐Insurance/Real Estate ☐Manufacturing
   ☐Retail/Chainstore/Wholesale ☐Government ☐Transportation/Utilities/Communication ☐VAR
   ☐System house/company ☐Other_____

9. Would you recommend your D-Link product to a friend?
   ☐Yes ☐No ☐Don't know yet

10. Your comments on this product? _____
_____
_____
_____

TO:

_____

D-Link®