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 TO THIS WARRANTY.

ANY PACKAGE RETURNED TO D-LINK 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 D-LINK 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 D-LINK 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

IN NO EVENT WILL D-LINK BE LIABLE FOR ANY DAMAGES, INCLUDING LOSS OF DATA, LOSS OF PROFITS, COST OF COVER OR OTHER INCIDENTAL, CONSEQUENTIAL OR INDIRECT DAMAGES ARISING OUT THE INSTALLATION, MAINTENANCE, USE, PERFORMANCE, FAILURE OR INTERRUPTION OF A D- LINK PRODUCT, HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY. THIS LIMITATION WILL APPLY EVEN IF D-LINK HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.
IF YOU PURCHASED A D-LINK PRODUCT IN THE UNITED STATES, SOME STATES DO NOT ALLOW THE LIMITATION OR EXCLUSION OF LIABILITY FOR INCIDENTAL OR CONSEQUENTIAL DAMAGES, SO THE ABOVE LIMITATION MAY NOT APPLY TO YOU.

Trademarks

Copyright ©2000 D-Link Corporation.
Contents subject to change without prior notice.
D-Link is a registered trademark of D-Link Corporation/D-Link Systems, Inc.

All other trademarks belong to their respective proprietors.

Copyright Statement

No part of this publication may be reproduced in any form or by any means or used to make any derivative such as translation, transformation, or adaptation without permission from D-Link Corporation/D-Link Systems Inc., as stipulated by the United States Copyright Act of 1976

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

Preface

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

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 Compatability 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
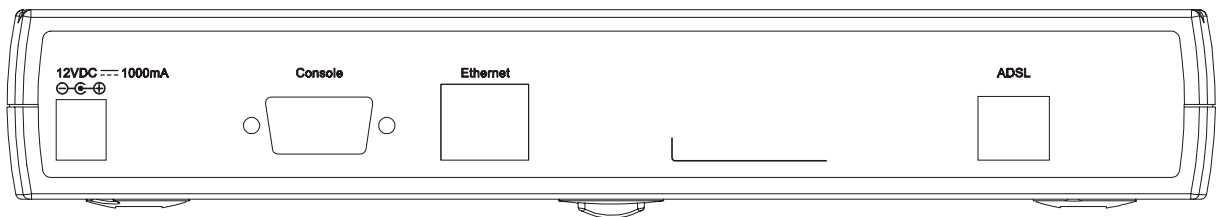- Supports up to eight simultaneous ATM virtual connections

Front Panel

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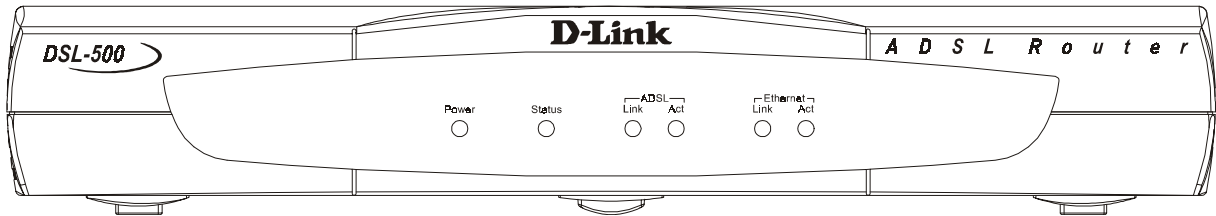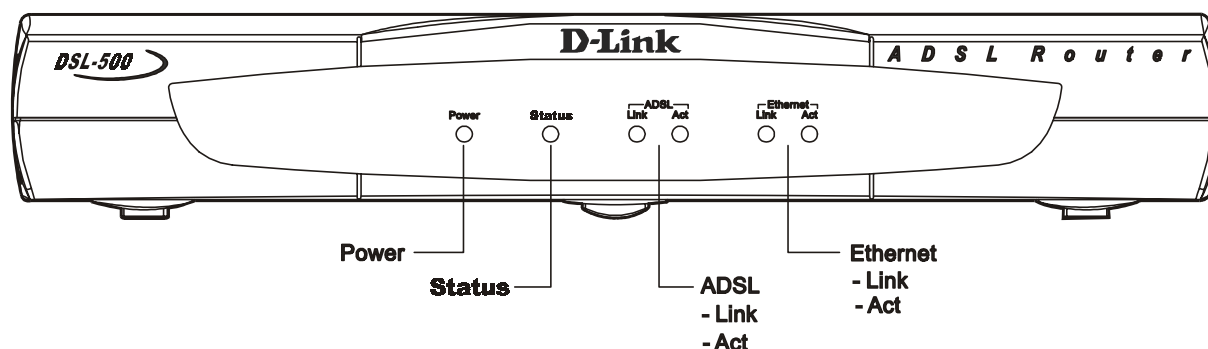
Front Panel

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.

Verify Package Contents

Open the box and carefully remove all items. In addition to this Installation Guide, make sure that you have:
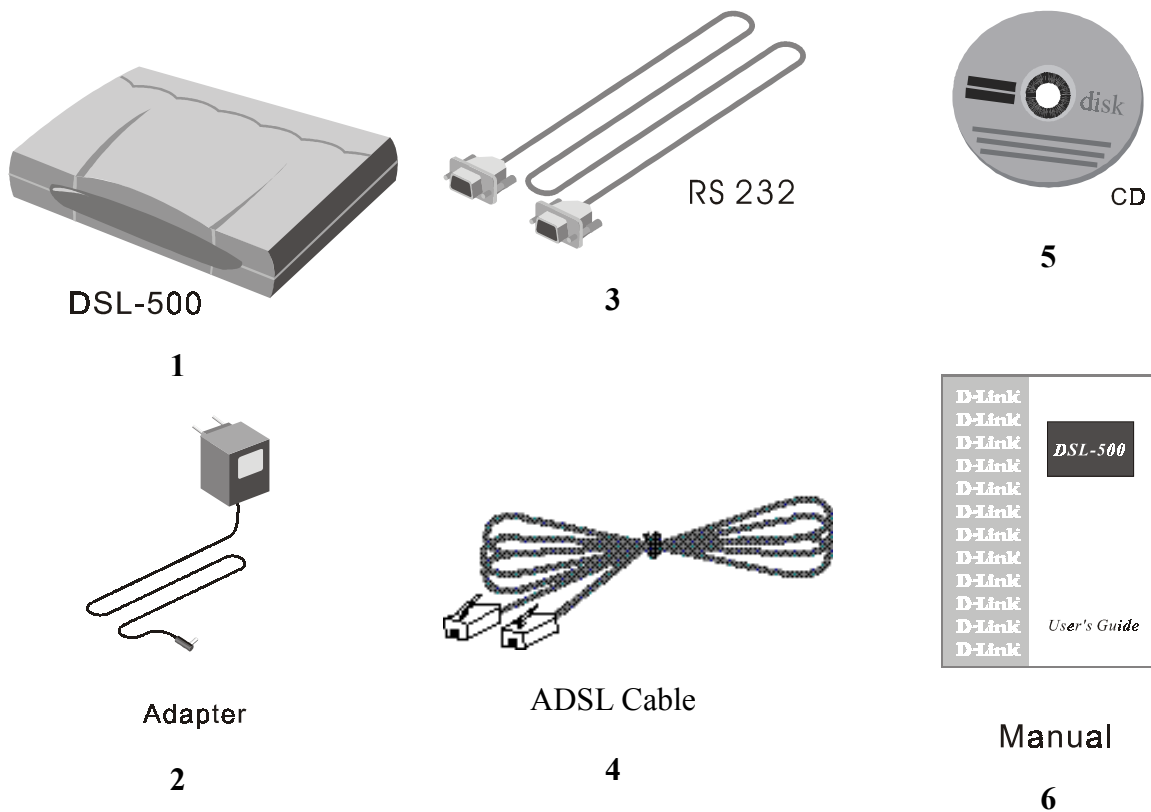
1. One DSL-500 ADSL Router

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

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.
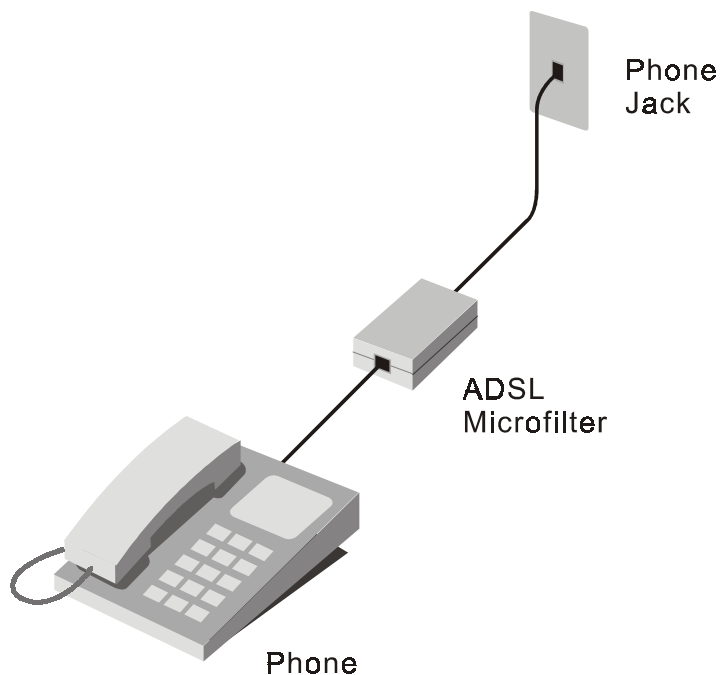
Microfilters and Splitters

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 phone 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.
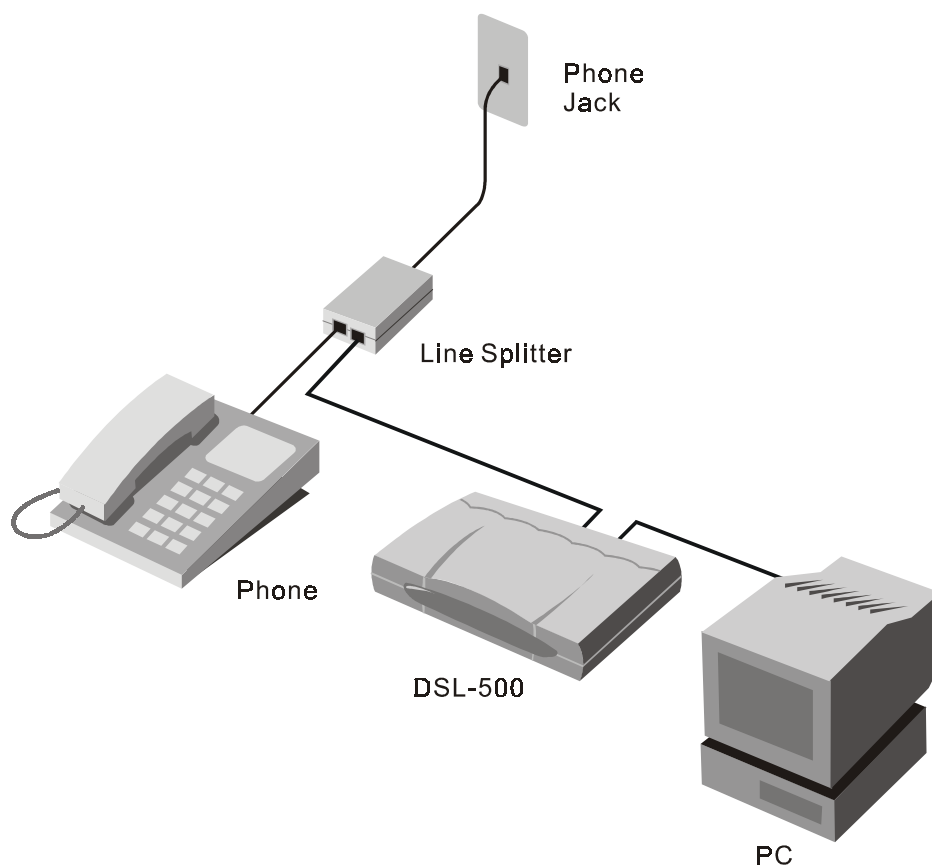
Line Splitter Installation

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

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.

ADSL SETTINGS

Each ADSL client on a DSL network has a unique integer pair used by the DSL network managers to provide dedicated bandwidth on the ATM network backbone. This pair of numbers is sometimes called the VPI/VCI pair.

The **Virtual Path Identifier** (VPI) and a **Virtual Channel Identifier** (VCI) must be entered during the configuration process.

ADSL SETTINGS	
VPI value:	**VCI value:**

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 Ethernet (RFC 2516) used by default

♦ PPP over ATM (RFC 2364)

♦ Ethernet over ATM (RFC 1483)

CONNECTION METHOD	
Protocol:	RFC 2516 Point-to-Point Protocol over Ethernet
	RFC 1483 Multi-protocol Encapsulation over ATM
	RFC 2364 Point-to-Point Protocol over ATM

PPP CONNECTIONS (RFC 2516 & RFC 2364)

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)

For Bridged Ethernet connections it will be necessary to give the Router a global IP address and default gateway.

Global IP Address

If the connection method used is Ethernet over ATM (RFC 1483), a unique global IP address will be needed for the Router. The assigned global IP address must be entered **only if** the connection method used is Ethernet over ATM (RFC 1483). When using the default connection method, PPP over Ethernet (RFC 2516), a global IP address will be assigned automatically during the connection process.

Default Gateway IP Address

Some network service providers require that a default gateway router be used by the Router to connect to their network backbone. If this is the case, the IP address of the default gateway (router) must be entered during the configuration of the device.

BRIDGED ETHERNET CONNECTIONS
Global IP Address: _____ : _____ : _____ : _____
Default Gateway IP Address: _____ : _____ : _____ : _____

DNS SETTINGS

Your DSL service provider should give you DNS settings. These settings should include the IP address of the DNS server as well as its domain name. You must enter these in the DHCP Configuration menu.

DNS SETTINGS
DNS Domain Name:
DNS Server IP Address:

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.
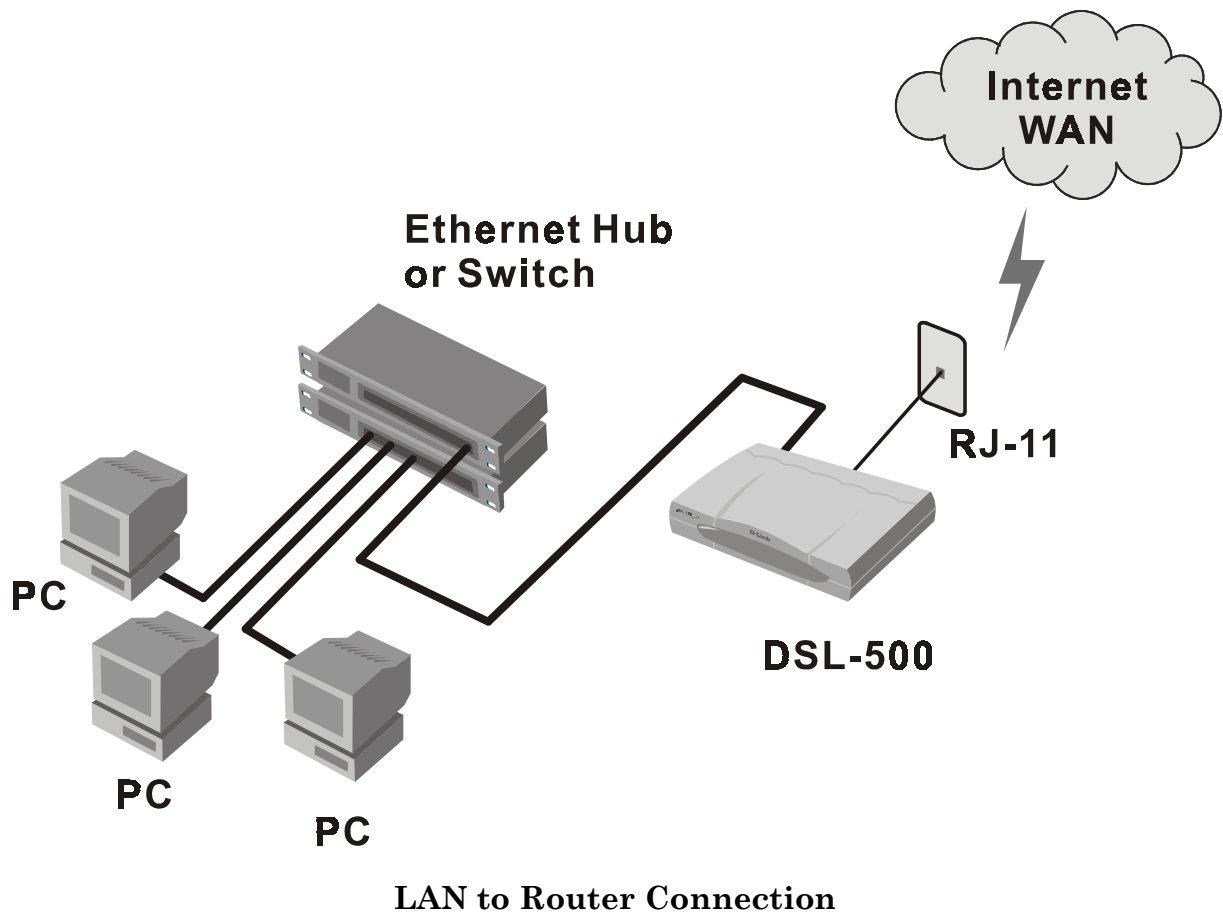
Connect Ethernet LAN to Router

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.

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.

PC/Server to Router Connection
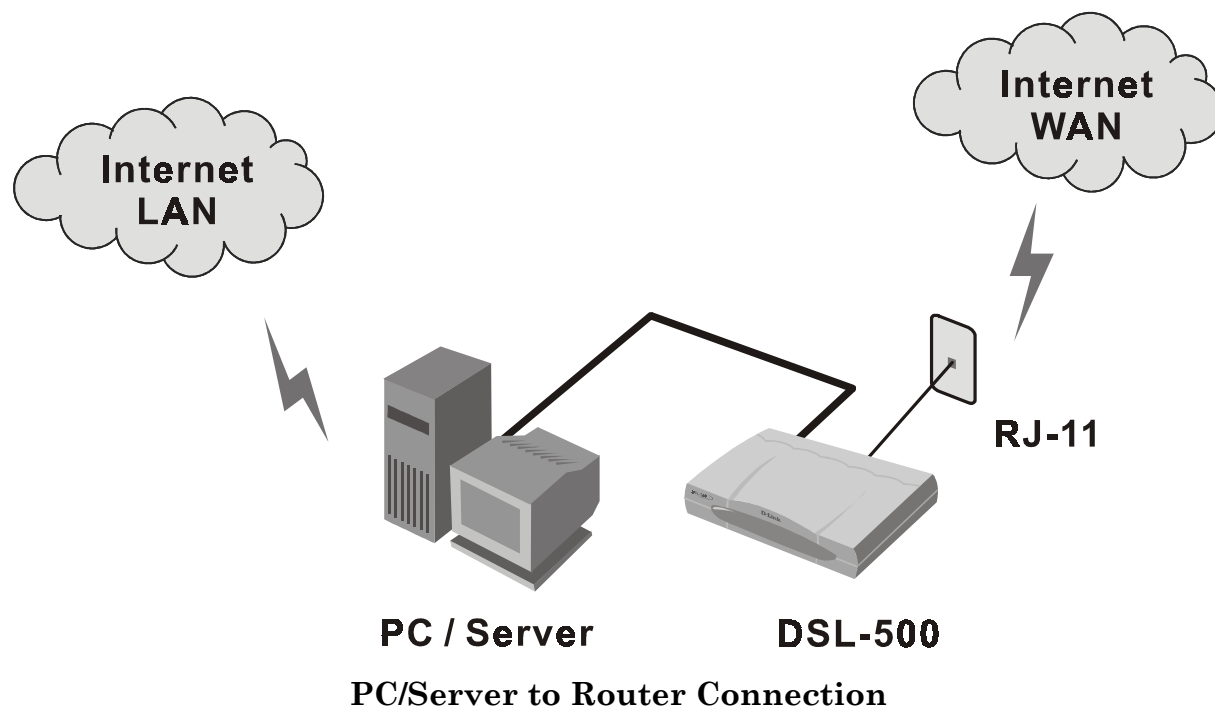
4

First Time Set Up

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 henceforth referred to as the manager PC.

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.

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.

If you do not wish to change the existing IP settings of the manager PC, you can change the IP address of the Router. For instructions for changing the Router's IP address read Chapter 6, *LAN Setup*, for more information.

Configure the Manager PC for DHCP

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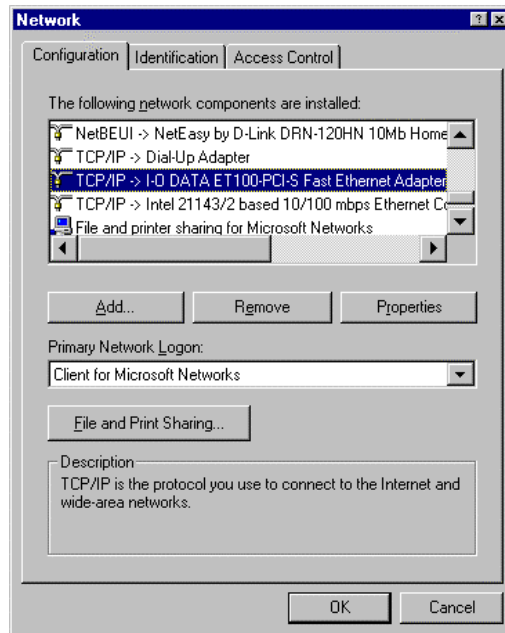
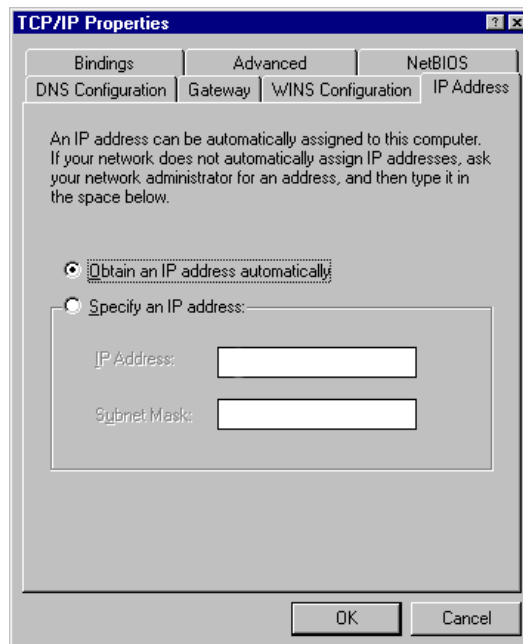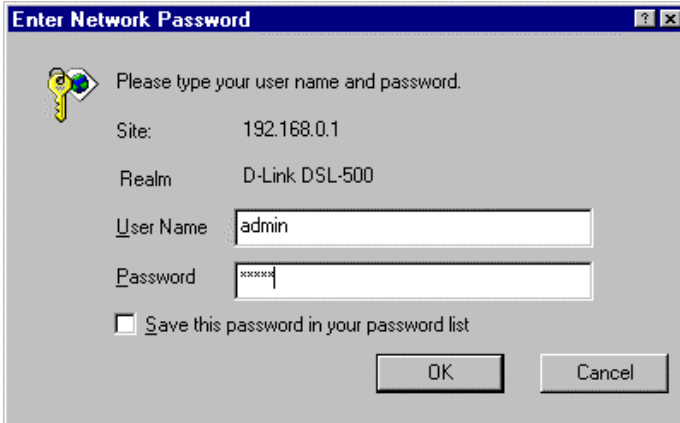7. In Windows 95/98, click on the **START** button, go to **Settings** and choose **Control Panel**.
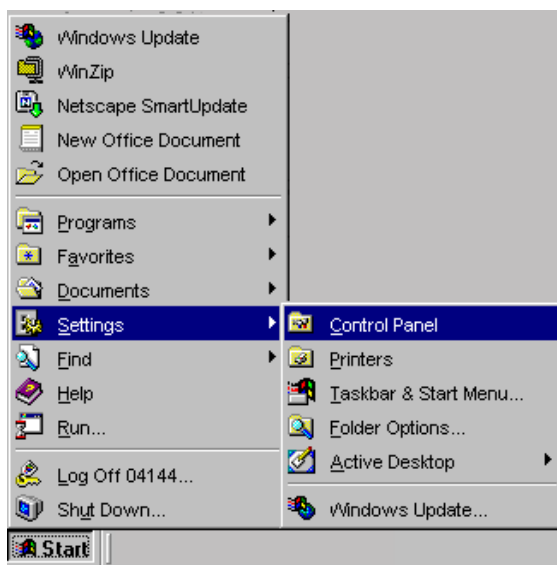
8. In the **Control Panel** window, double-click on the **Network** icon.
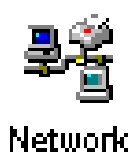
9. Under the Configuration tab, select the **TCP/IP** component and click **Properties**.

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

11. 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. Be sure that the Manager PC is not configured to use a proxy server for Internet access.

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:

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 main page of the web-based management module. Click the DSL-500 folder in the main window. This folder will open revealing the management menu options. These menus are used to configure the Router for connection to the WAN and other router functions. 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*.
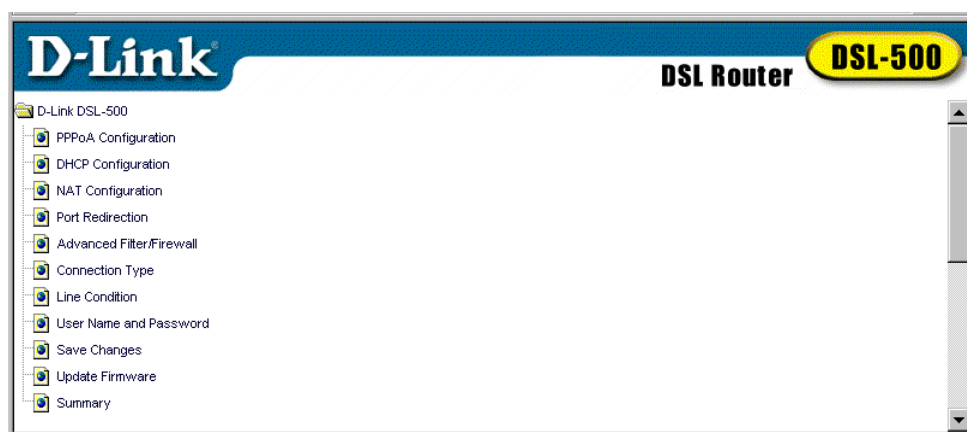
Web-based Manager Main Menu

Configure the WAN Connection

Now that you have accessed the web-based manager, you must configure the Router for the ADSL connection (VPI/VCI pair) and provide other information to establish the WAN connection. The other information provided depends on the type of WAN connection you have. For PPPoE and PPPoA connections, you will need to provide a User Name and Password used 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 PPPoE connections. PPPoE is the most commonly used protocol to provide ADSL connection and is the default method used by the Router. For a more detailed discussion of the various menu items in the connection configuration windows, see Chapter 5, *Web-based Management*.

If you are using either a PPPoA or Bridged Ethernet (RFC 1483) connection it will be necessary to change the connection method. Please read the section Changing the Connection Type following the PPPoE Configuration section for more information.

PPPoE Connections

The default connection method used by the Router is Point-to-Point-Protocol over Ethernet (PPPoE) as defined in RFC 2516. In the PPPoE Configuration window (shown below) you must to enter the VPI and VCI values, as well as 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. Follow these steps to establish the PPP and ADSL network connection:

1. Click on the PPPoE Configuration button in the main menu to bring up the window displayed below:

PPPoE Configuration

2. Under **PPPoE Login**, enter the **Login User Name** used for the ADSL 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.

3. Enter the **Login Password**.

4. 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 network service provider.

5. Change the **Connect on Demand** option to **enabled** in the pull-down menu.

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

7. Under **PVC**, enter the **VPI** and **VCI** values for the Router.

8. Proceed to the Change User Name and Password and Save Changes sections in this chapter.

Changing the Connection Type

The default connection method used by the Router for the WAN connection is PPP over Ethernet. If you wish to use this method you do not need to change this setting. However if you plan to use a static IP address for a "Bridged Ethernet" (RFC 1483) connection, or PPP over ATM (RFC 2364) you must select those protocols in this window.
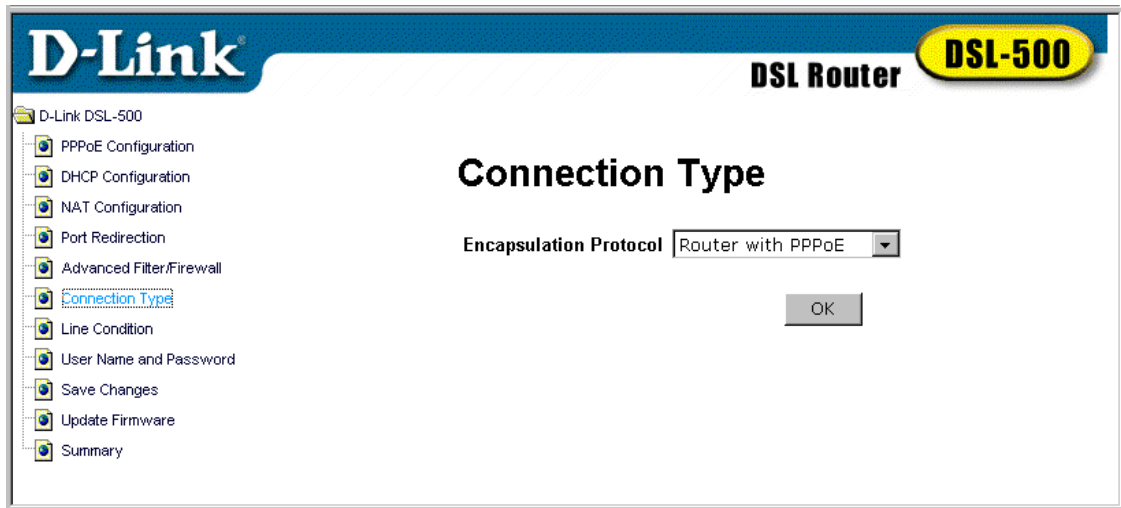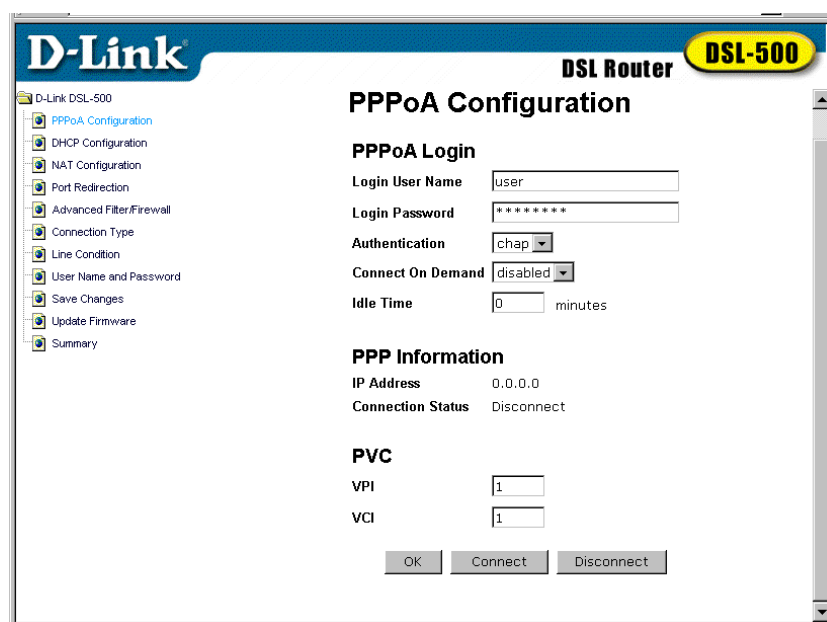

Connection Type Window (PPPoE)

To change the connection method, select either **Router with RFC 1483** or **Router with PPPoA** from the pull down menu in the **Encapsulation Protocol** field and click the **OK** button. It will then be necessary to save the change and restart the Router. Read the Save Changes section later in this chapter.

Once the Router has been restarted it is ready to be configured according to the connection method selected.

PPPoA Connections

Although the protocols differ significantly, from the viewpoint of the ADSL client, there is little difference between the two variations of PPP connections. The values that must be entered for PPPoA connections are the same as those you would enter for PPPoE connections. To configure the Router using for a PPPoA connection, follow the instructions below.

1. After you have changed the Connection Type to PPPoA, click on the PPPoA Configuration button in the main menu to bring up the window displayed below:

PPPoA Configuration

2. 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.

3. Enter the **Login Password**.

4. 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.

5. Change the **Connect on Demand** option to **enabled** in the pull-down menu.

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

7. Under **PVC**, enter the **VPI** and **VCI** values for the Router.

8. Proceed to the Changing the User Name and Password and Saving Changes sections in this chapter.

RFC 1483 Bridged Ethernet Connections

To configure the Router for RFC 1483 connections it is necessary to provide a static global IP address and subnet mask for the WAN interface. In addition, you may need to define the DNS settings as well. Ask your network service provider about DNS configuration settings. You can enter the DNS settings in the DHCP Configuration menu. DHCP Configuration is discussed in Chapter 5, *Web-based Management*.

After you have changed the Connection Type to RFC 1483, click on the Static IP Address Configuration button to bring up the window below:

Static IP Address Configuration Window

In the Static IP Address Configuration window you will need to enter the global **IP Address** and **Subnet Mask** used to identify the Router on the Internet. Some static IP address connections will also require use of a default gateway. If you are given a **Default Gateway** IP address by the network service provider enter that here as well.
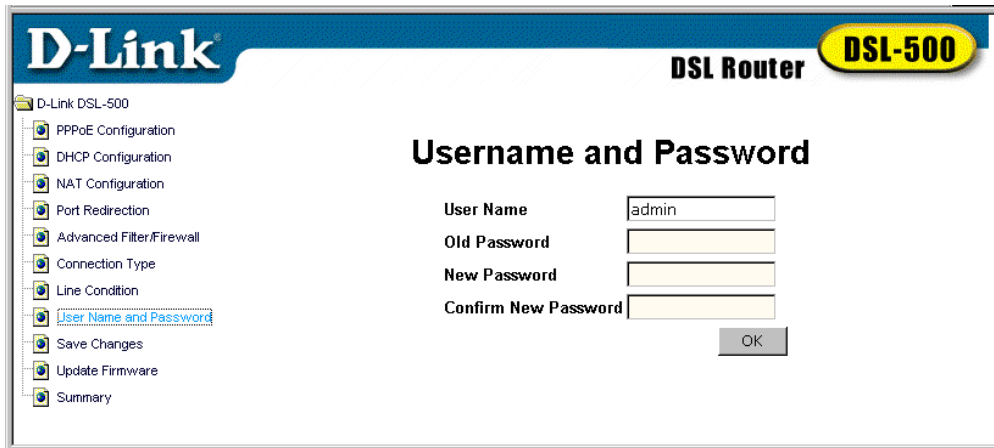
In the **PVC** field, enter the **VPI** and **VCI** values used for the ADSL connection.

Check all of the entries in this window to be certain that they are correct and click the **OK** button. Once all the values have been set you must save the changes and restart the Router.

After the Router has been configured and restarted you can access the Internet by simply launching the web browser of the manager PC. When your LAN is set up, any workstation properly connected to the Router will have Internet access using a web browser.

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. Click on the User Name and Password button in the main menu.
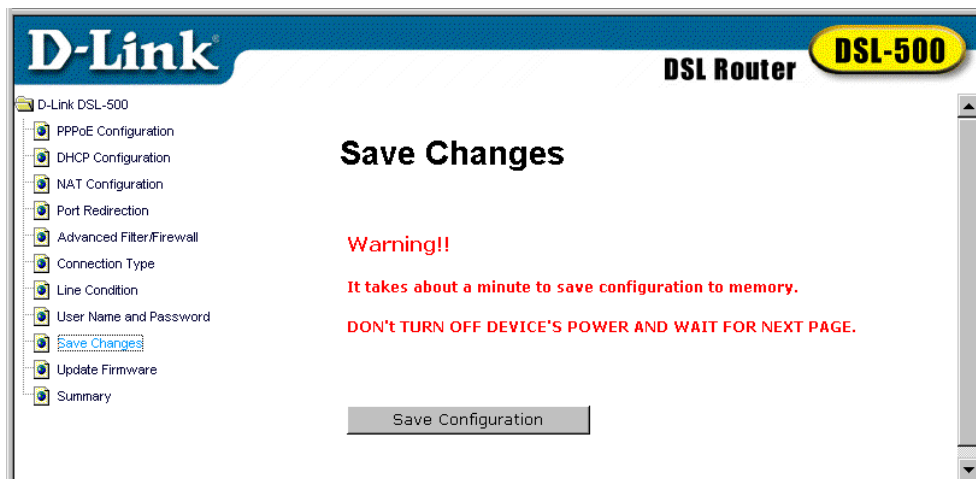

User Name and Password Window

Type the new **User Name** and **Old Password** in their respective fields. Type the **New Password** and confirm it in the **Confirm New Password** field and click the **OK** button.

Saving Changes

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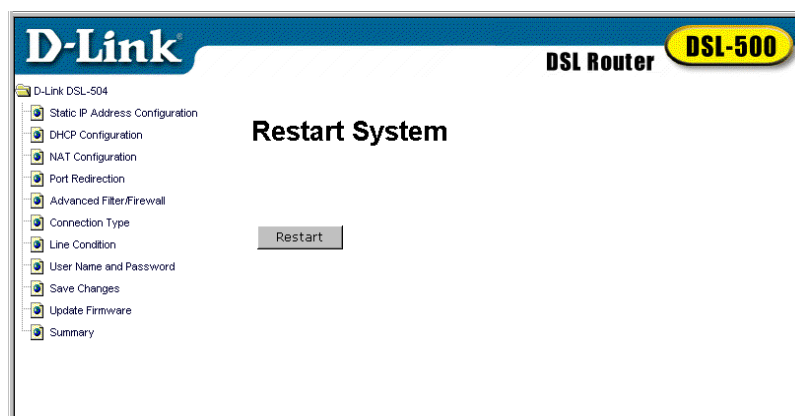

Save Changes Window

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.

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

<div align="center">**Restart System Window**</div>

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.

Connect with RFC 1483

Bridged Ethernet connections are established upon restarting the Router. Internet access is simply a matter of launching a web browser on the manager PC.

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.

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 network 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. Your browser window may not appear exactly with the screen captures (pictures) in this guide.

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**.

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.

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:

Login 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.
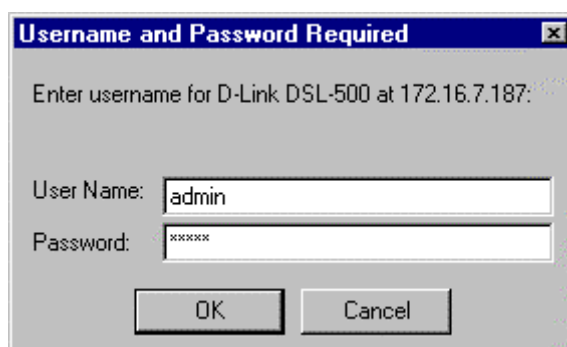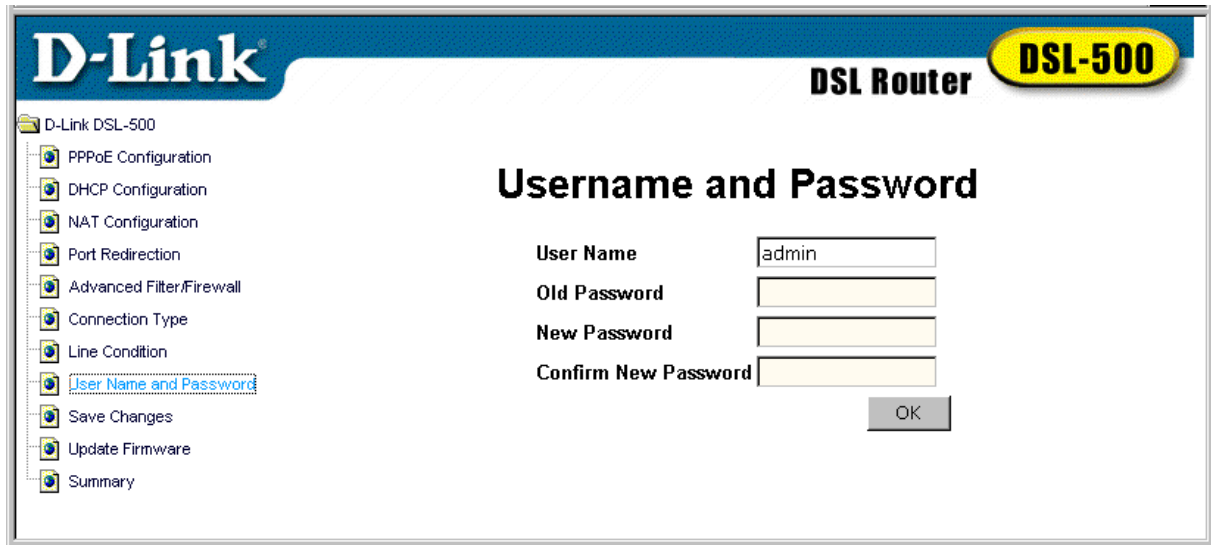

User Login

Logging in will bring up the main page of the web-based management module. Click the D-Link DSL-500 folder located below the D-Link logo in the upper left-hand corner. This folder will open revealing the management menu options. These options include **PPPoE Configuration**, **DHCP Configuration**, **NAT Configuration**, **Port Redirection**, **Advanced Filter/Firewall**, **Connection Type**, **Line Condition**, **Save Changes**, **Update Firmware** and **Summary**. The various management options are explained in the following sections. To access any of the option menus click on the appropriate button in the main menu window.

IMPORTANT: For any changes to the Router's configuration to take effect, you must save the new settings to non-volatile ram by going to the Save Changes menu, and initiating the saving procedure. It will then be necessary to restart the Router. See the section entitled Save Changes.

Change User Name and Password

Before you configure the Router and connect to the WAN you should change the user name and password you just used to access the web-based manager. You can change these by clicking on the User Name and Password button in the main menu.

User Name and Password Window

Use this window to change the **User Name** and **Password** used to access the web-based manager. Type the new **User Name** and **Old Password** in their respective fields. Type the **New Password** and confirm it in the **Confirm New Password** field and click the **OK** button.

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*.

Connection Configuration

To establish the WAN connection, the Router must be configured to suit the requirements of the ADSL connection protocol. This section discusses how to configure the Router for the various connection types. Most ADSL clients will use the default method PPPoE, discussed below. If you are using an ADSL service that employs an alternative connection method, namely, PPP over ATM (RFC 2364) or "Bridged Ethernet" Multiprotocol Encapsulation over IP (RFC 1483), please skip ahead to the section on Connection Method.

PPPoE Configuration

The default connection method used by the Router is PPPoE as defined by RFC 2516. Use the PPPoE Configuration window to set the VPI and VCI values and enter your network account name and password. This window is also used to terminate the WAN (PPP) connection.

To bring up the PPPoE Configuration window, click on the PPPoE Configuration menu button and the following screen will appear:

PPPoE Configuration Window

PVC

Use this field to assign the **VPI** and **VCI** values for the Router. These numbers are given to you by your DSL service provider and must be entered in order to establish the ADSL connection.

PPPoE Login

Use this field to assign a **Login User Name** and **Password** used for authentication by your network service provider. Type in the user name and password in their respective fields. You can use any combination of up to 64 characters (no spaces) in both fields.

The **Authentication** protocol used to confirm the identity of the user can be chosen from the pull-down menu. The available protocols are **chap** (by default) and **pap**.

The **Connect on Demand** pull-down menu toggles either *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. Most users will probably want to enable this feature.

If your network account is not billed according to the amount of time connected, the **Idle Time** field should be left at 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.

PPPoE Information

This field provides information regarding the status of the Router's 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.

In the PPPoE or PPPoA Configuration widow, viewing the **Connection Status** *Connected*, under **PPPoE 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.

Connection Type
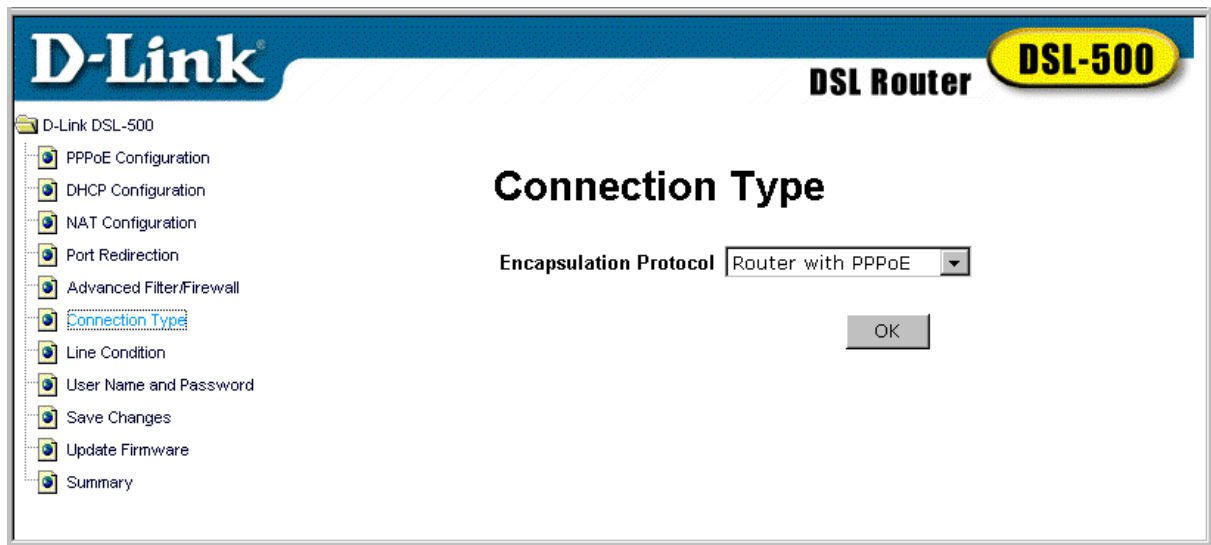
Connection Type Window (PPPoE)

The default connection method used by the Router for the WAN connection is PPP over Ethernet. If you wish to use this method you do not need to change this setting. However if you are using a static IP address (also called "Bridged Ethernet" encapsulation as defined by RFC 1483), or PPP over ATM (RFC 2364) you can select them here.

To change the connection method, select either **Router with RFC 1483** or **Router with PPPoA** from the pull down menu in the **Encapsulation Protocol** field and click OK. If you are changing the connection type to Router with RFC 1483, read the next section. If you are changing it to Router with PPPoA, read the PPPoA Configuration section.

Static IP Address Configuration (for RFC 1483)

Static IP Address Configuration Window

In the Static IP Address configuration window enter the static **IP Address** and subnet mask assigned by your network service provider for your WAN interface. The Static IP Address is a globally unique IP address used to identify the Router on the Internet. If you are given a **Default Gateway** IP address enter that here as well. The default gateway is another Router used to provide Internet access for many network clients.

You must enter the **VPI** and **VCI** values for the ADSL service here. Check the values for all of the entries in this window to be certain that they are correct and click the **OK** button.

PPPoA Configuration

PPPoA Configuration

PVC

Use this field to assign the **VPI** and **VCI** values for the Router. These numbers are given to you by your DSL service provider and must be entered in order to establish the ADSL connection.

PPPoA Login

Use this field to assign a **Login User Name** and **Password** used for authentication by your network service provider. Type in the user name and password in their respective fields. You can use any combination of up to 64 characters (no spaces) in both fields.

The **Authentication** protocol used to confirm the identity of the user can be chosen from the pull-down menu. The available protocols are **chap** (by default) and **pap**.

The **Connect on Demand** pull-down menu toggles either **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. Most users will probably want to enable this feature.

If your network account is not billed according to the amount of time connected, the **Idle Time** field should be left at 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.

PPP Information

This field provides information regarding the status of the Router's 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.

In the PPPoE or PPPoA Configuration widow, viewing the **Connection Status** *Connected,* under **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.

Line Condition
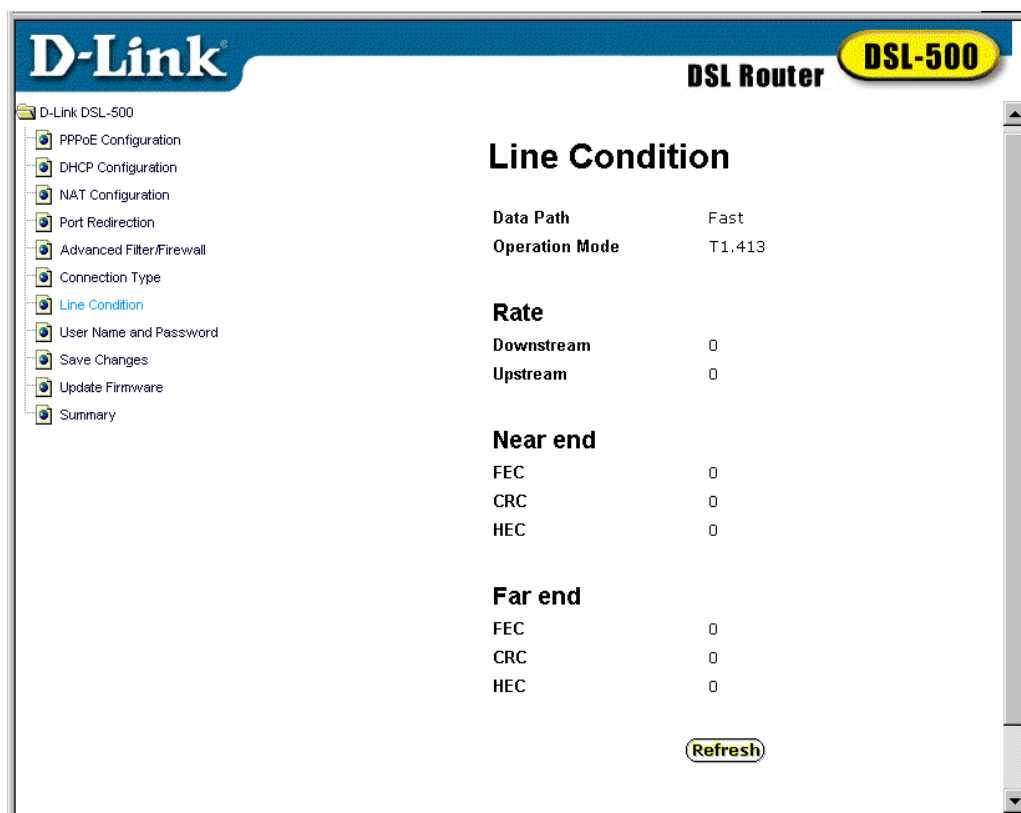
Line Condition

In the Line Condition window you can monitor the characteristics of the ADSL connection and confirm that it has been established. From here you can observe various performance statistics of each end of the connection, including:

Data Path: Displays the current data path type, *Fast* or *Interleaved*.

Operation Mode: Describes the of modulation technique used to make the ADSL connection. This will be either Discrete Multi-tone modulation (DMT) defined by the *G.dmt* standard or the variation of DMT described by the *G.lite* standard.

Downstream Rate: Lists the downstream data transfer rate in Kbps.

Upstream Rate: Lists the upstream data transfer rate in Kbps.

Near End (ADSL Router connection a.k.a. ATU-R): Lists the number of data transfer errors on the Router end of the ADSL connection. These errors are listed according to the technique used to correct them. The techniques used are **Forward Error Correction (FEC)**, **Cyclic Redundancy Control (CRC)** and **Header Error Check (HEC)**.

Far End (DSLAM): Lists the number of data transfer errors on the DSLAM end of the ADSL connection. These errors are listed according to the technique used to correct them. The techniques used are **Forward Error Correction (FEC)**, **Cyclic Redundancy Check (CRC)** and **Header Error Control (HEC)**.

Router Functions

The DHCP and NAT functions of the Router allows the network manager to more easily manage IP addresses and subnets, and enhance network security by presenting only one global IP address to the Internet. This section discusses how to use these conventional routing functions.

DHCP

The Dynamic Host Configuration Protocol (DHCP) allows the Router to assign IP addresses to all properly configured hosts on the network. Dynamic IP assignment alleviates the need for the network administrator to maintain and monitor IP address assignments and simplifies IP use because IP address are automatically assigned when a station powers-on. Click on the DHCP Configuration button to see the DHCP menu.

> **IMPORTANT**: If you use DHCP to set your local IP addresses, the IP settings of all stations on the network must be either manually configured to 0.0.0.0 or, select the "Obtain an IP address automatically" option under the TCP/IP Properties tab in the Network menu. See the Configure the Manager PC section at the beginning of Chapter 4 for more explicit instructions.

DHCP Configuration Window

In the DHCP Configuration window you define the following:

Start IP Address

This is the base (starting) address for the IP pool of unassigned IP addresses.

End IP Address

This is the last address of the contiguous IP address range to be used by the Router for DHCP function.

Netmask

This mask informs the client, how the destination IP address is to be divided into network, subnet, and host parts. The netmask has ones in the bit positions in the 32-bit address which are to be used for the network and subnet parts, and zeros for the host part.

Default Gateway

This specifies the Gateway IP Address that will be assigned to and used by the DHCP clients.

Leased Time

This specifies the amount of time (in seconds) a client can lease an IP address, from the dynamically allocated IP pool. A value of 4294967295 means the lease is permanent.

DNS Server IP

Domain Name Service (DNS) servers are used on the Internet to match the Uniform Resource Locator (URL) for a website to its Internet IP address. For example, the URL: www.cnn.com, is a pseudonym for the IP address: 207.25.71.25. DNS entries allow users to access resources using URLs instead of IP addresses.

You may enter any Internet DNS server IP address available through the WAN connection. This address should be provided by your network service provider. (Note that without a DNS server IP, internet sites will only be available using IP addresses and will not be available using URLs.)

State

This toggles *Disable* and *Enable* for DHCP function.

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.
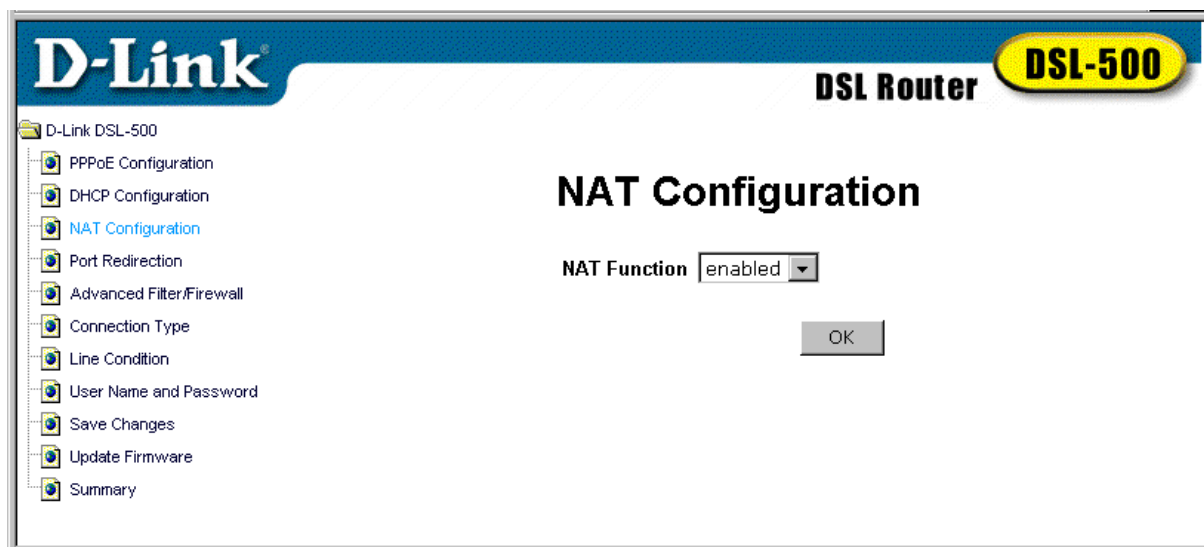
NAT Configuration Window

The NAT function is enabled by default on the Router. If you want to disable NAT, open the NAT Configuration window, select *disabled* in the **NAT Function** pull-down menu. Click the **OK** button to implement your choice. There are security risks associated with disabling NAT, so it is important that you have other network protection mechanisms in place before you do this.

Security Features

Network security is an unfortunate necessity for any network connected to the Internet. Protection of sensitive information and proprietary assets on your private network should be designed into the network infrastructure from the beginning. If you are not already, it is recommended that you become familiar with network security issues and the strategies available to help reduce risks from outside as well as from within your LAN. The Router provides features that can enhance your network security and should be used in concert with other security provisions, such as virus scanning software for all workstations, the use of proxy servers and stateful inspection methods.
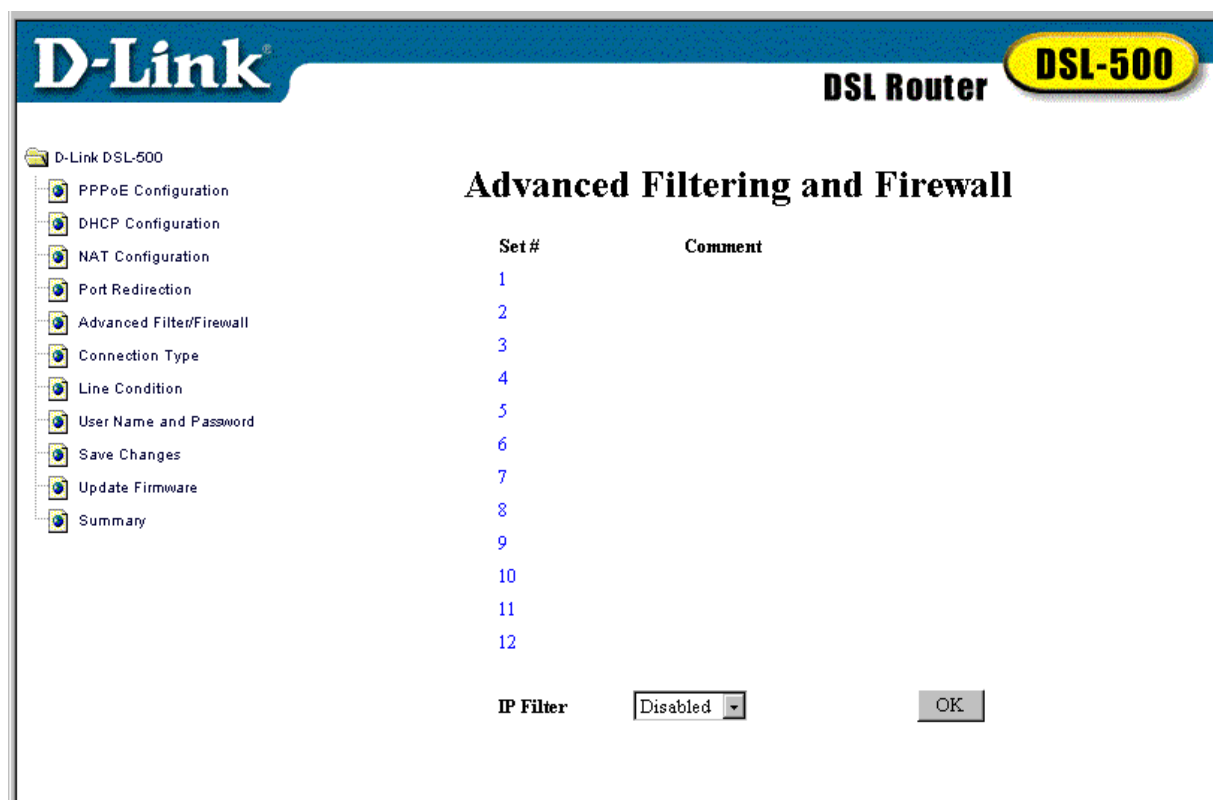
Advanced Filtering and Firewall

One of the most important elements of any network security implementation is the firewall. Packet filtering is a basic firewall security measure that should be used on any network that is exposed to security risk. A packet filter system examines data packets and scrutinizes them for the purpose of controlling network access. Filtering rules determine whether or not to allow access 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 network from the outside, or 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 twelve filter sets can be used; each set contains up to seven filtering rules subsets.

Advanced Filtering and Firewall (Screen #1)

To define the filter rule sets, click on the Advanced Filtering and Firewall button to bring up the first window. Choose E*nable* in the **IP Filter** pull-down menu and click the **OK** button to enable IP filtering. Then click on the set number you wish to configure to proceed to the next window.
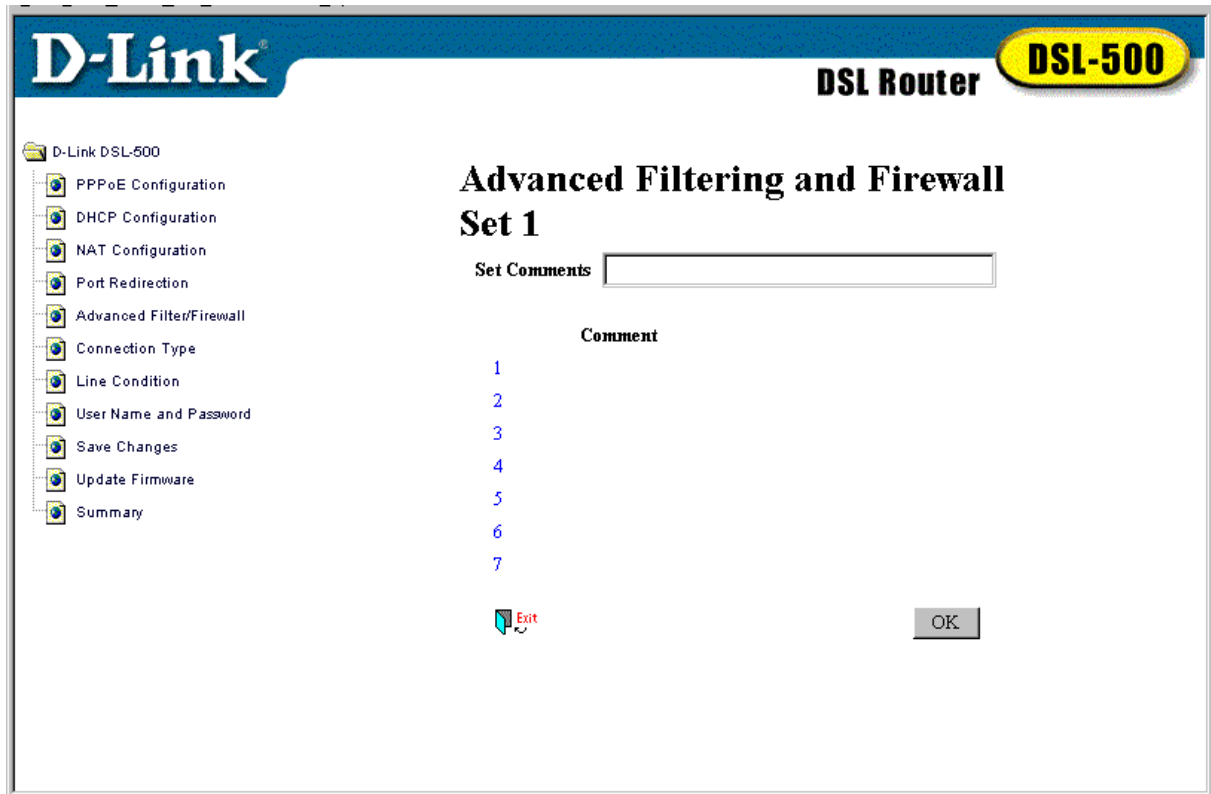
Advanced Filtering and Firewall (Screen #2)

In the second Advanced Filtering window you can supply a comment or name of up to 15 characters for the set in the **Set Comments** field. Click the **OK** button to save the comments, then click on the number of the subset you want to configure to proceed to the next window.

Advanced Filtering and Firewall (Screen #3)

In the third Advanced Filtering window you will define the rule applied for the chosen subset. Again you can supply a name for the subset in the **Comment** field and click the box on the right to **enable the Filter Rule**.

In the **Pass or Block** field select the action to be performed on the IP packets, the default is *Pass Immediately*. All blocked packets will be dropped.

In the **Direction** field choose either *In* or *Out* from the pull down menu. You can block IP packets from coming into the network, by selecting *In*, blocking packets from a specific IP address for example. Or you can block packets from a specific IP address or subnet from leaving the LAN by selecting *Out*, for example, to block Internet access for a specific host.

The **Protocol** field allows you to block packets based on the protocol used. You may choose to block ICMP, TCP or UDP transmissions from the pull-down menu.

You must next specify the **Source** and **Destination IP Addresses** as well as their **Subnet Mask**. This will block the packets from or destined to any specified IP address from passing through the Router.

Finally you can specify individual protocol ports or an entire range of protocol ports to be blocked for the **Source** or **Destination**. Type the **Start Port** number

57

in either the Source or Destination row. If there is no port specified in the Start Port column, the filter rule will be ignored. Use the **<**, **>**, **=** or **≠** in the pull down menu to specify the port or range of ports to be filtered. Use the following guide to define the port or port range:

< : 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.

Port Redirection
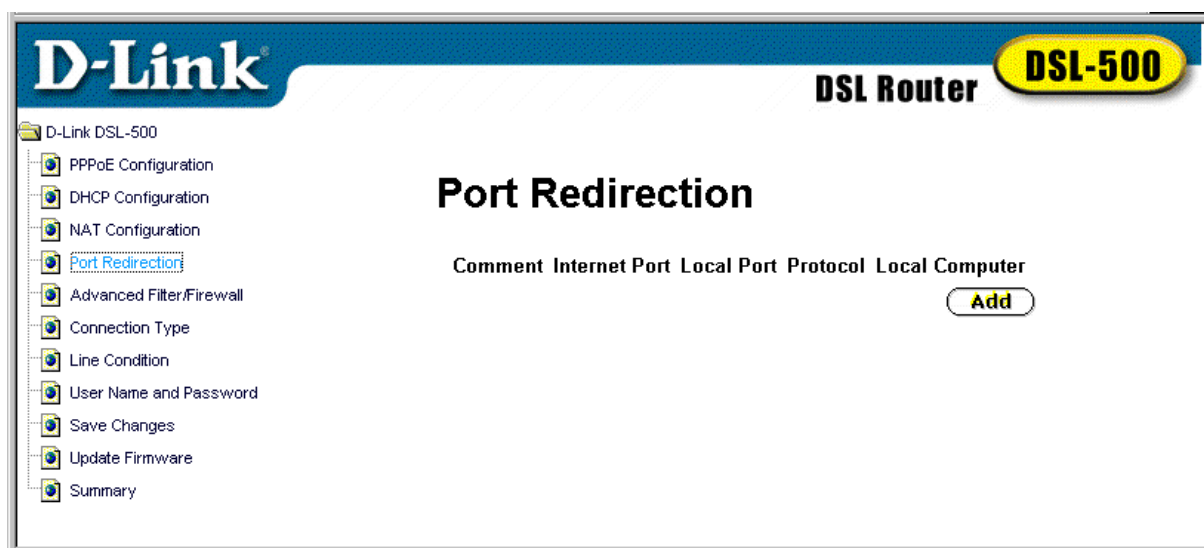
Port Redirection Window

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 menu.

Redirect Port Window

The Redirect Port window presents five entry fields. The first field, **Comment** can be used to assign an appropriate name to the new route, for our example we will use the name *HTTP Server*. In the **Internet Port** field enter the designated TCP or UDP protocol port number for the particular protocol packet you wish to redirect. In our example an incoming HTTP packets use port 80. The local port is the port used by the designated host on the LAN. In this case an HTTP server, conventionally port 8080 is used for this purpose. Choose the protocol either TCP or UDP from the pull-down **Protocol** menu, HTTP is defined within TCP. In the **Local Computer** field supply the IP address of the local designated host computer or device. Using our example you would enter the IP address of the HTTP server.

Router Utility Functions

Once the Router configurations have been set, it is necessary to save the new settings to memory. You may also upgrade the Router to use the latest firmware. The procedures for saving settings and upgrading firmware are discussed here.

Save Changes

In order to save the configuration changes that have been made to the Router you must save them to the Router's non-volatile RAM. You can change any or all of the configurable settings in one session before you initiate the saving procedure. If you experience a power loss or reboot the Router before saving, all changes will have to be reset.
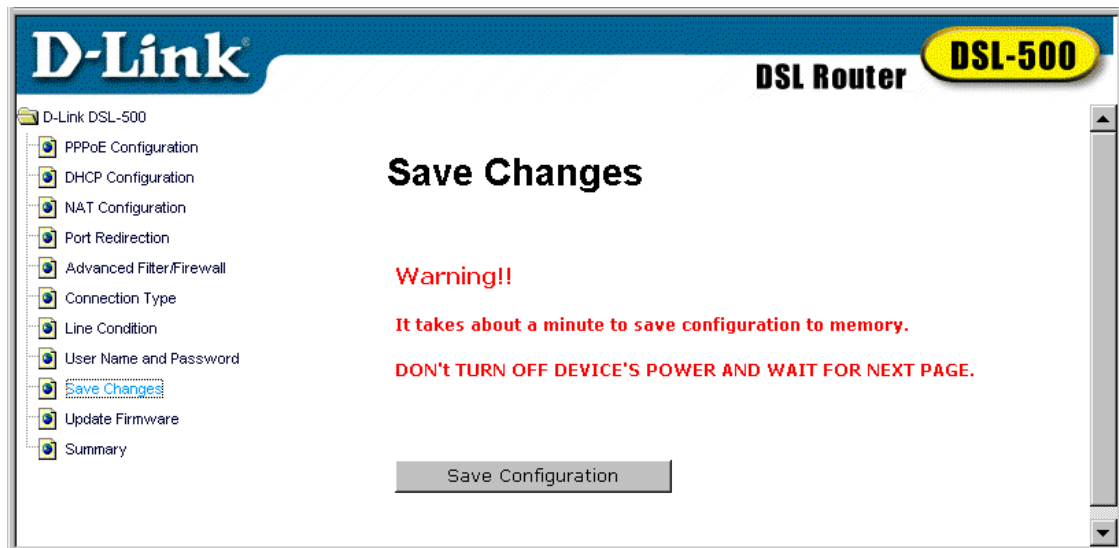
Save Changes Window

When you are ready to save the settings, click the **Save Configuration** button. A pop-up message window informs you that the Router must be restarted. Do not turn off the power to the Router while the settings are being saved.

When the **Restart System** window appears, click the **Restart** button.
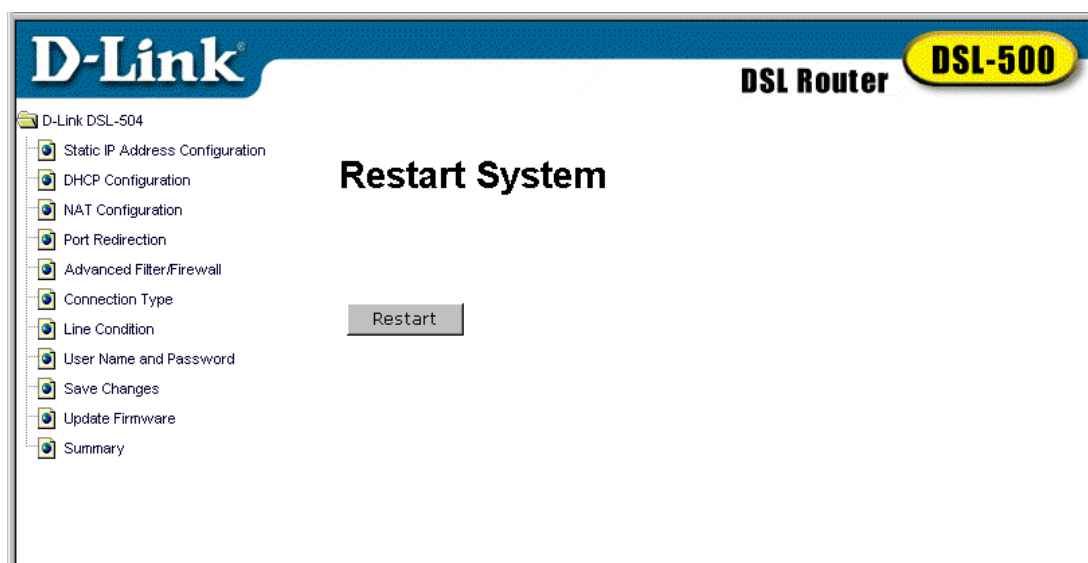
After restarting the Router, the *Login to web-based management module* page will again appear.

Update Firmware

In order to keep pace with changes in ADSL standards and technology the DSL-500 allows you to easily update the embedded firmware. You may obtain the latest version of the DSL-500 firmware by logging onto the D-Link web site at www.dlink.com. If you are connected to the Internet, you can access the D-Link web site by clicking on the blue URL in the Update Firmware window.
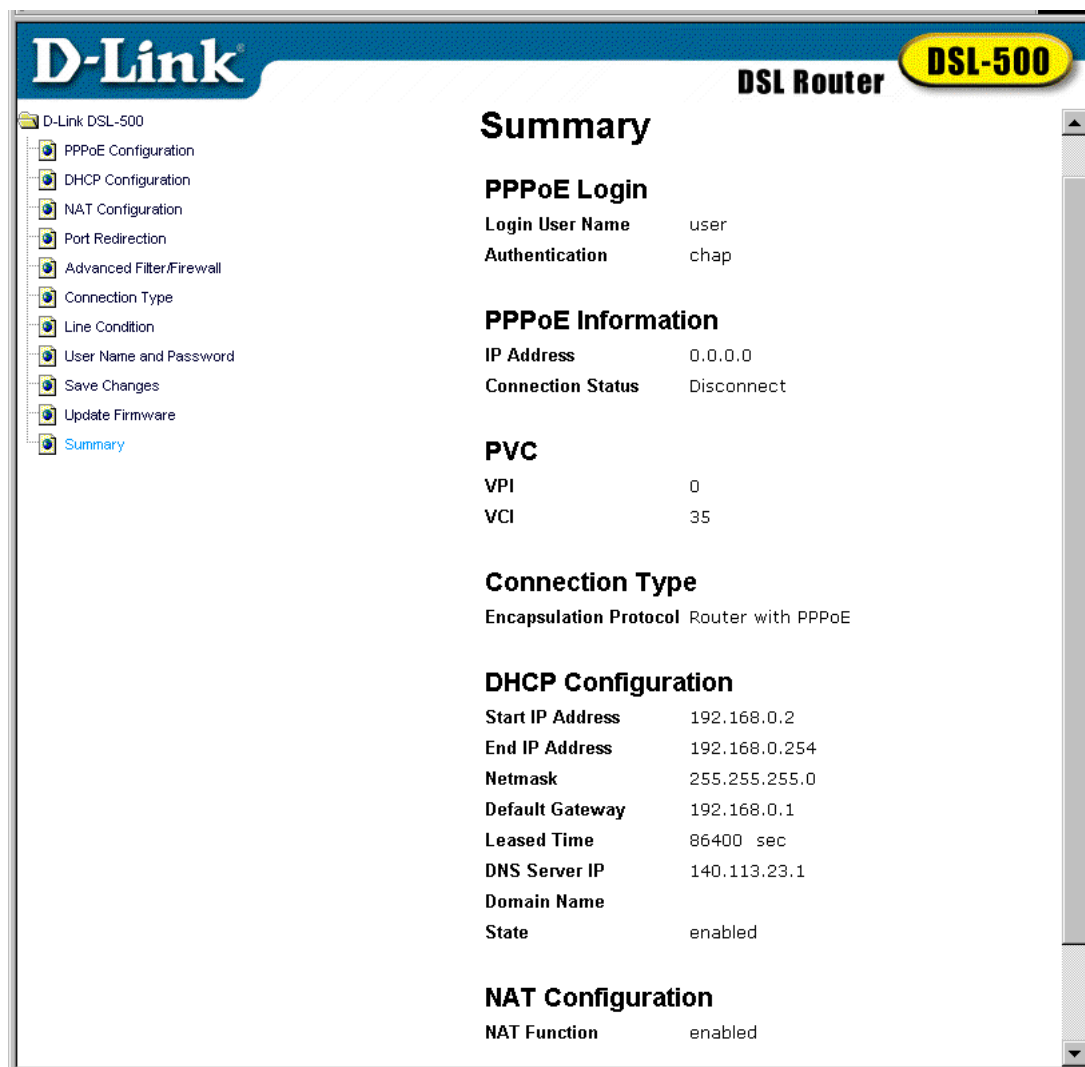
Update Firmware Window

The Update Firmware window lists the version of the firmware the Router is currently using. If you would like to update, follow the instructions given on the D-Link web site firmware update page to download the new firmware. You can then use the DSL-500 Firmware Upgrade Utility included with the Router to transfer the new firmware to the Router. For instructions on using the Upgrade Utility software please read Appendix C.

The Installation CD-ROM included with the Router contains an installation file for the DSL-500 Firmware Upgrade Utility. You should install this on the computer you will use to make the occasional upgrades. Click on the setup.exe file and the utility will be automatically installed.

Summary Statistics

Click on the Summary button for a concise presentation of various Router statistics.

Summary

This page provides summary statistics of the various features of the Router. The list includes: **PPPoE Login**, **PPPoE Information** (when using PPPoE connection method), **PVC**, **Connection Method**, **DHCP Configuration** and **NAT Configuration**.

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
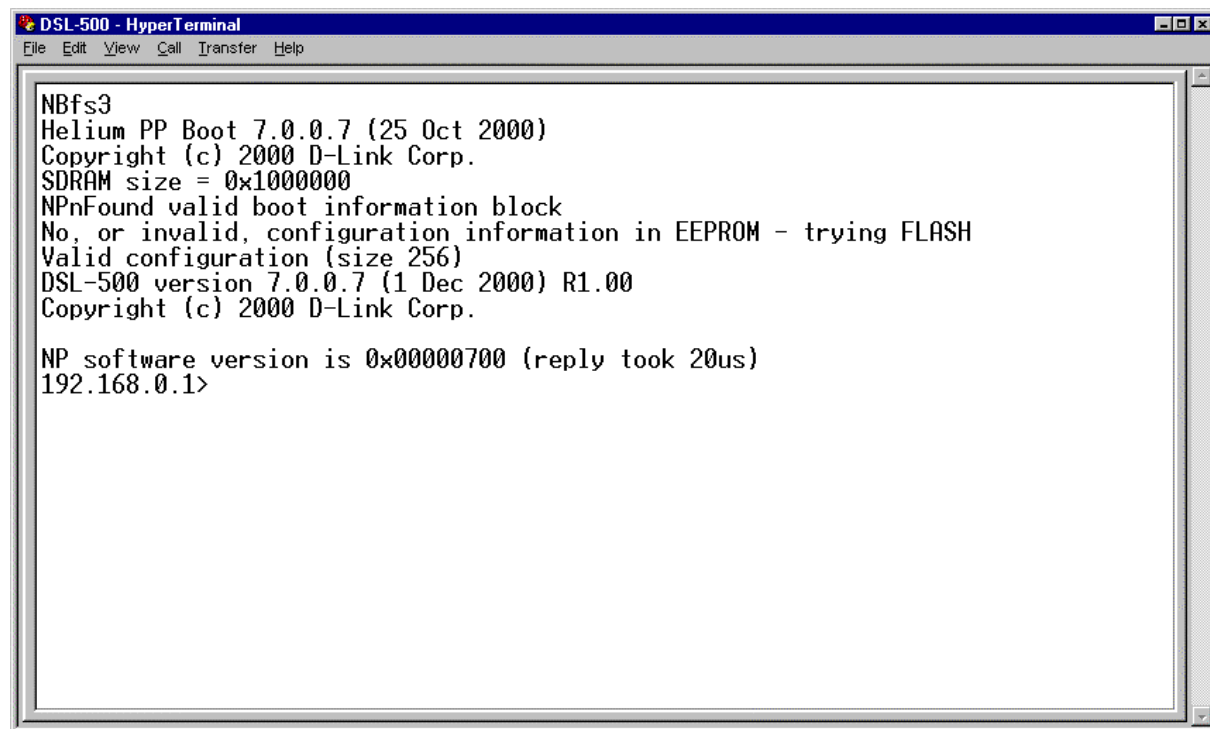
The second way to use the default settings is to allow the Router to automatically assign IP addresses to your computers using DHCP. To do this, simply make sure your computers' IP addresses are set to 0.0.0.0 (under Windows, choose the option Obtain an IP address automatically in the TCP/IP network 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:

VT-100/ANSI compatible
Terminal keys enabled
9,600 baud
8 data bits
No parity
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.
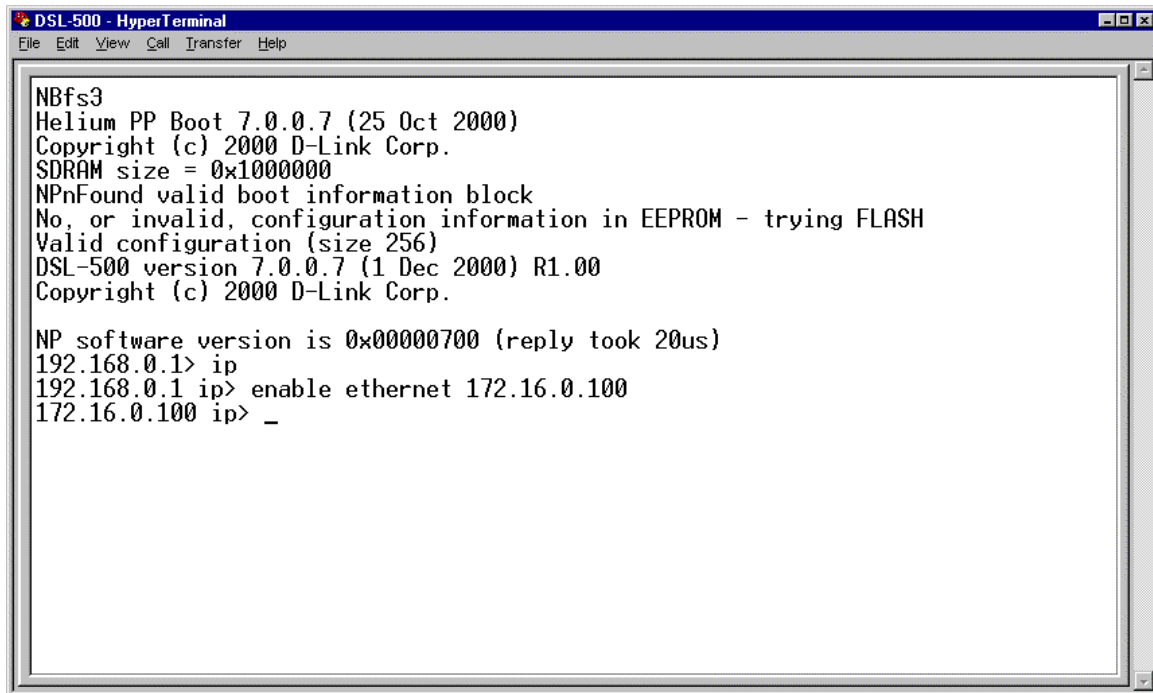
```
NBfs3
Helium PP Boot 7.0.0.7 (25 Oct 2000)
Copyright (c) 2000 D-Link Corp.
SDRAM size = 0x1000000
NPnFound valid boot information block
No, or invalid, configuration information in EEPROM - trying FLASH
Valid configuration (size 256)
DSL-500 version 7.0.0.7 (1 Dec 2000) R1.00
Copyright (c) 2000 D-Link Corp.

NP software version is 0x00000700 (reply took 20us)
192.168.0.1> ip
192.168.0.1 ip> enable ethernet 172.16.0.100
172.16.0.100 ip> _
```

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.

7

Using the Console Manager

Settings for the Router can be configured via the RS-232 console port connection using terminal emulation software such as Microsoft HyperTerminal included with Microsoft's operating systems. This chapter lists and describes a few of the most essential command sets that might be used by the typical user. This chapter is not intended to be a complete list of the commands available.

General Use

To use a terminal emulation interface with the device, the terminal parameters will need to be set to:

VT-100/ANSI compatible
Terminal keys enabled
9,600 baud
8 data bits
No parity
One stop bit

With the correct parameters set and the RS-232 connection established you should be able to use the keyboard to communicate with the device. If the Router is powered on when the terminal interface appears, depress the Enter key to bring up the initial prompt. This will be the IP address of the device. For information about changing the IP address, please read the section in Chapter 6.

If at any time you want to view a list of commands available in the particular mode you are currently operating, type **help** and press Enter. This will bring up a list of the commands available in the current mode. For example, type help after the initial IP address prompt and you will see a menu similar to this:

`ap`	`atm`	`bridge`	`buffer`	`bun`
`chips`	`config`	`dhcpclient`	`dhcpserver`	`diap`
`edd`	`ethernet`	`event`	`flashfs`	`ip`
`ip_filter`	`isfs`	`itex`	`led`	`nat`
`oamloop`	`portcli`	`ppp`	`r1483`	`reflect`
`restart`	`snmp`	`tftp`	`uptime`	`version`
`webserver`				

To see a list of available commands and command syntax along with brief explanation of the command, type **help all** and depress Enter. Remember that the console interface commands are case sensitive.

Typing any of the commands listed above and depressing Enter will put the console interface into that command mode. For example, form the IP address prompt type **ip** and depress Enter. This will put the interface into "**ip**" where it can now accept ip mode commands. While in ip mode or any other command mode you may again type help or help all to list the commands available in that mode. You will see the command appear after the IP address and before the "greater than" sign. If you type **help** in ip mode you would see a menu such as this:

?	**arp**	**config**	**device**
disable	**enable**	**help**	**ipatm**
nat	**norelay**	**ping**	**relay**
rip	**route**	**routes**	**snmp**
stats	**subnet**	**version**	

If you at any time wish to return to the original undefined command prompt (the first IP address prompt), type **home** and depress Enter and you will again see the IP address prompt.

The commands **restart**, **uptime** and **version** are not command modes. The restart command will restart (reboot) the Router. Remember that any changes made to the configuration must be saved before the Router is restarted or the changes will be lost. The uptime and version commands simply list the uptime (amount of time the Router has been continuously operating) and the software version of the unit.

Saving Changes

To save changes made to the Router configuration type **config save** and press Enter, the current settings will be saved to nonvolatile RAM.

Finding the Password

If you forget the user name and password that allows you to access the web-based manager you can retrieve this information using the console terminal interface. To do this type **flashfs cat initweb** and you will see the user name and password listed.

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	

General	
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:

> 201.202.203.204   189.21.241.56   125.87.0.1

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.
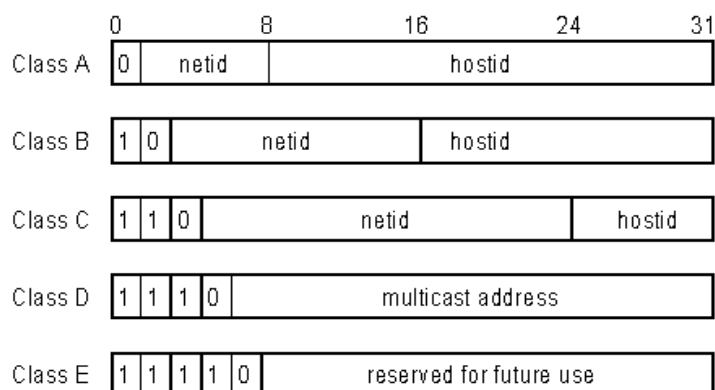
Networks attached to the Internet are assigned class types that determine the maximum number of possible hosts per network. The previous figure illustrates how the net and host portions of the IP address differ among the three classes. Class A is assigned to networks that have more than 65,535 hosts; 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.
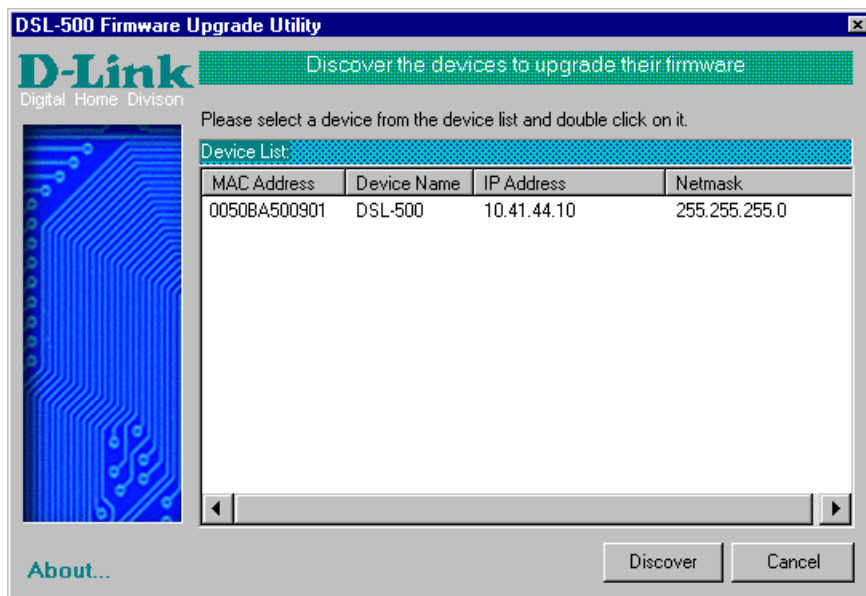
When you select a Router to upgrade you will be prompted for a password. The default password is **admin**. If you want to change the password, you can change it using the console manager interface as described in Chapter 6.
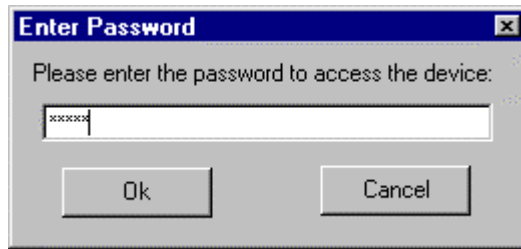
Enter the password and click OK.

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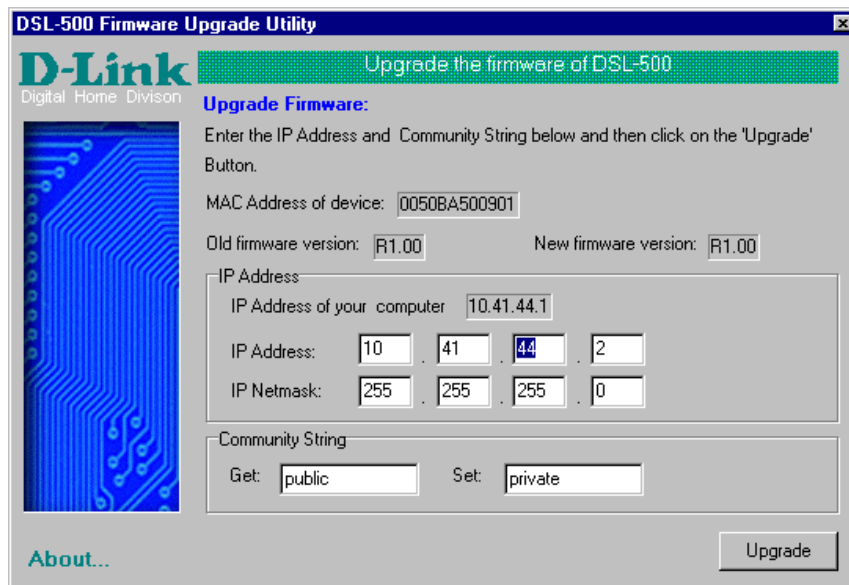
To upload the new firmware to the selected Router click the 'Upgrade' button. The utility will automatically load the new firmware. During the upgrade process it is important that you allow the entire file to load onto the device. Do not turn off the Router while the flash memory is being updated. A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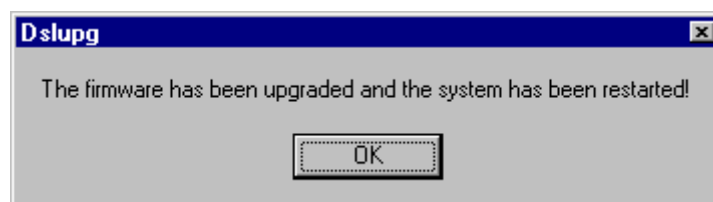
D-Link Offices

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®