D-Link®

DSL-1501G

SHDSL 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

About This Guide

Thank you for choosing the DSL-1501G Wireless SHDSL Router. The DSL-1500G delivers affordable T1 equivalent Internet access characterized by very high rate upload and downloads data transmission speeds. The standardized SHDSL technology implemented in the Router is ideally suited for VPN applications, video teleconferencing, IP telephony applications, public web servers and interactive gaming over the Internet. This reliable high-capacity Router can serve as the primary gateway device for busy corporate networks, improving network efficiency and enhanced security.

If you would like to set up the device quickly in order to verify that the SHDSL connection to the WAN (wide area network) is working properly, please read the Quick Installation Guide included in the DSL-1501G package.

Some basic information about Ethernet LAN, networking devices, gateway routers and the TCP/IP suite of protocols is provided in the text of this guide. If you would like to learn more about home or small office networking D-Link has tutorials available at:

> http://www.dlink.com/learnbasic/ and http://www.dlink.com/learnbasic/homenetwork/.

Guide Overview

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

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

Configuring the Router for the First Time – Provides information on how to configure the Router and establish the WAN connection using the web-based manager.

Web-based Configuration – Describes how to use the web-based manager to change Router settings and configure additional virtual connections (PVCs).

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

Before You Start

Please read and make sure you understand all the prerequisites for proper installation of your new Router. Have all the necessary information and equipment on hand before beginning the installation.

Installation Overview

The procedure to install the Router can be described in general terms in the following steps:

1. Gather information and equipment needed to install the device. Before you begin the actual installation make sure you have all the necessary information and equipment. A packing list is included at the end of this section. Check the contents of the package to be certain that everything listed on the packing list is included. The information you will need includes the account name or number and the password used to gain access to your service provider's network, and ultimately to the Internet. In addition, some users may be given information used to configure the Router so it can establish a connection to the service provider's network and the Internet.

2. Install the hardware, that is, connect the Ethernet and telephone cables to the device to establish the necessary network links to your computer and to the service provider's network and connect the power adapter to power-on the Router.

3. Check the IP settings on your computer and change them if necessary so the computer can access the web-based software built into the Router. Without the correct IP settings your computer will not be able to communicate with the ddevice or access the software used to configure the Router. Without compatible IP settings on your computer, you will not be able to use a web browser to access the Internet.

4. Use the web-based management software to configure the device to suit the requirements of your SHDSL account as instructed by your service provider. Some users may not need to change any of the device settings that establish and maintain the network connection. It may only be necessary to supply the user name or number and the password used for your account. Other users may not be required to change anything in the Router but they may need to install software on a computer used to access the Internet. Follow the instructions of your service provider to find out what is required for your account.

Requirements for Installation

In order to use SHDSL you must have SHDSL service set up by your service provider. SHDSL operates on a separate physical line from normal voice telephone service therefore you must have a line dedicated for SHDSL in addition to your regular telephone line.

To install and use the Router you need a computer equipped with an Ethernet port (such as an Ethernet NIC) and a web browser. To establish the WAN connection to your ISP's network, it will be necessary for most users to make some changes to the WAN configuration of the Router. This change may only be to supply a user name and password for your ISP account (see below).

Operating System

The Router uses an HTML-based web interface for setup and management. The web configuration manager may be accessed using any operating system capable of running web browser software.

Web Browser

Any common web browser can be used to configure the Router using the web configuration management software. The program is designed to work best with more recently released browsers such as Microsoft Internet Explorer® version 5.0, Netscape Navigator® version 4.7, or later versions. The web browser must have JavaScript enabled. JavaScript is enabled by default on many browsers. Make sure JavaScript has not been disabled by other software (such as virus protection or web user security packages) that may be running on your computer.

Ethernet Port (NIC Adapter)

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

Account Information (User Name and Password)

Most users will need to supply a user name and password used to access the service provider's network (and ultimately, the Internet). This information is stored either in the Router's memory or on your computer depending on the type of SHDSL connection profile (encapsulation method) you have.

ISP ACCOUNT INFORMATION
User Name:
Password:

Packing List

Open the shipping carton and carefully remove all items. Make sure that you have the items listed here.

1. One DSL-1501G SHDSL Ethernet Router

2. One CD-ROM containing the User's Guide

3. One twisted-pair telephone cable used for SHDSL connection

4. One straight-through Ethernet cable

5. One AC power adapter suitable for your electric service

1

Introduction

This chapter describes the Router and its features and includes a brief introduction to SHDSL. Front and rear panel diagrams are used to illustrate the LED indicators and cable connections.

Router Description and Operation

The DSL-1501G SHDSL Router is designed as a gateway for busy networks. It provides upload and download speeds of up to 4.6 Mbps. High speed symmetrical data transmission is ideally suited to business networks using VPN and remote LAN-to-LAN applications, video teleconferencing, web servers, IP telephony and Internet gaming.

The Router is easy to install and use. The DSL-1501G connects to an Ethernet LAN via a standard Ethernet 10BASE-T interface using RJ-45 connectors. The SHDSL connection is made using ordinary twisted-pair telephone line with standard RJ-11 connectors. Enhanced 4-wire SHDSL service requires a special installation. (Ask your service provider about the availability of 4-wire SHDSL service).

Enterprise-grade features on the DSL-1501G provide security, efficiency and reliability for demanding business networks. The Router supports transparent bridging or it 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 efficiency and 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.

About SHDSL

Symmetric High-Speed Digital Subscriber Line technology is the first international DSL standard developed from the ground up. It represents a very significant improvement over the interim SDSL standard, delivering higher bit rates over longer distances. SHDSL allows telecommunications companies to deliver T1-level data network services at fraction of the cost. The standard has been developed by the International Telecommunications Union (ITU) in Geneva Switzerland with cooperation and input from a consortium of telecommunications and computer technology industry leaders.

It is important to note that SHDSL does not support analog splitting technologies and therefore cannot coexist with regular voice telephone service or ISDN installations. Unlike Asymmetric Digital Subscriber Line (ADSL) technology, SHDSL requires a separate dedicated physical line (standard twisted-pair copper telephone wire). Plain Old Telephone Services (POTS) cannot share the same line with SHDSL, although IP phones can be used over SHDSL. The standard also allows for extended reach double twisted-pair (4-wire) implementations that can double the bandwidth to up to 4.6 Mbps upstream and downstream.

Product Features

The DSL-1501G SHDSL Router utilizes the latest DSL enhancements and router technologies to provide a robust Internet gateway suitable for most small to medium sized networks.

VPN Support

The DSL-1501G SHDSL supports VPN Pass Through for L2TP, PPTP and IP Sec.

Firewall Protection

Tailored firewall security features include packet filtering for protocol and IP address and port redirection.

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 and medium office networks, the DSL-1501G allows multiple users on the LAN to access the Internet concurrently through a single IP address. This provides Internet access to every workstation using a single Internet account.

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 for remote LAN implementations.

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, you can 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).

Multiple Encapsulation Support

The DSL-1501G supports *Bridged Ethernet over ATM* (RFC2684), *IP over ATM* (RFC1577) and *PPP over ATM* (RFC 2364).

Precise ATM Traffic Shaping

Traffic shaping is a method of controlling the flow rate of ATM data cells. This function helps to establish the Quality of Service for ATM data transfer.

High Performance

Very high symmetric data transfer rates of up to 4.6 Mbps Upstream/Downstream over standard single twisted-pair telephone cable.

Full Network Management

The DSL-1501G incorporates SNMP (Simple Network Management Protocol) support for web-based management and text-based network management via an RS-232 or Telnet connection. Enable Telnet for remote text-based management access to the Router. Management through the WAN port can be enabled for access from outside the LAN.

Easy Installation

The DSL-1501G uses a web-based graphical user interface program for convenient management access and easy set up. Any common web browser software can be used to manage the Router

Standards Compatibility and Compliance

The DSL-1501G complies with or is compatible with the following standards as recognized by their respective agencies.

- ITU G.991.2 SHDSL compliant

- 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

- Supports RIP v1 and RIP v2

- Supports Static Routing

- Minimum ATM cell forwarding rate: 320 Kbps

Front Panel LED Display

Place the Router in a location that permits an easy view of the LED indicators on the front panel.

The LED indicators on the front panel include the Power, Status, SHDSL Link/Activity, and WLAN indicators. Each Ethernet LAN port displays a pair of indicators for monitoring connection speed (10M/100M), link status and activity (Link/Act).

Power	Steady green light indicates the unit is powered on.
Status	Lights steady green during power on self-test. Once the connection status has been settled, the light will blink green. A steady light or no light indicates system failure. Reboot the device if the Status light shines steady green.
DSL	Steady green light indicates a valid DSL connection. This will light after the DSL negotiation process has been settled. Blinking green light indicates activity on the WAN interface.
Ethernet	Steady green indicates a 100Mbps Fast Ethernet connection. For 10Mbps Ethernet connection it is dark. Blinking green light indicates activity on the LAN interface.

Rear Panel Cable Connections

Connect the AC power adapter cord and network cables on the rear panel. The power switch and reset button are also located on the back of the device.

2
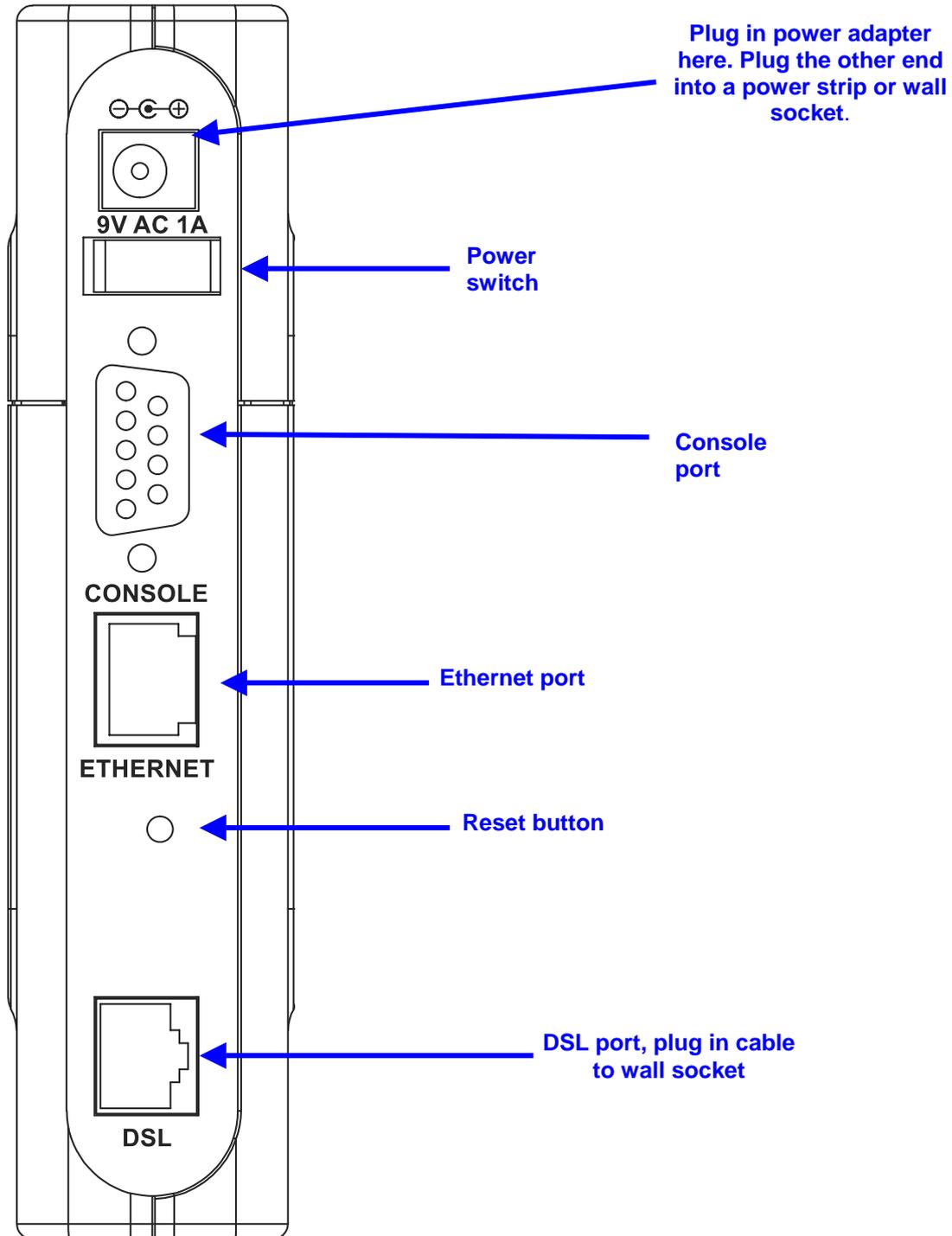
Hardware Installation

Follow the instructions here to connect the Router and power it on. Instructions for performing a factory reset are provided at the end of this section.

Select Location

Place the Router in a location where the LED indicators can be easily viewed. Keep the device away from any significant heat source and allow space on the sides and especially above for ventilation. As with any electrical device, place the device in a suitable and safe location.

Connect SHDSL Line

Use the DSL cable included with the Router to connect it to the telephone socket dedicated for your SHDSL service. Plug one end of the cable into the DSL port (RJ-11 receptacle) on the rear panel of the Router and insert the other end into the dedicated SHDSL socket. The SHDSL connection represents the WAN interface. It is the physical link to the ISP's network backbone and ultimately to the Internet.

Connect Router to Ethernet

The Router connects directly to Ethernet workstation or to an Ethernet LAN. The RJ-45 port on the Router is a crossed port (MDI-X) and can be connected to an Ethernet adapter with a straight-through (MDI-II) port using normal straight-through Ethernet cable. Use crossed cable when connecting the Router to a crossed port (MDI-X) on a switch or hub. Use straight-through cable when connecting it to an uplink (MDI-II) port on a hub or switch. A valid connection is indicated if the Ethernet Link LED indicator on the front panel shines steady green. Be sure to use Category 5 or better Ethernet cable.

The rules governing Ethernet cable lengths apply to the four Ethernet ports. Be sure that the cable connecting the Router to other Ethernet devices does not exceed 100 meters.

Power On Router

To power on the Router:

1. Insert the AC Power Adapter cord into the power receptacle located on the rear panel of the Router and plug the adapter into a suitable nearby power source.
2. Turn on the power with the power switch located on the rear panel.
3. You should see the Power LED indicator light up and remain lit. The Status LED should light solid green and begin to blink after a few seconds.
4. If you have the Router connected to your network you can look at the Ethernet Link/Act LED indicators to make sure they have valid connections. The Router will attempt to establish the SHDSL connection, if the SHDSL line is connected and the connection is properly configured this should light up after several seconds.

Factory Reset Button

The Router may be reset to the original factory default settings by depressing the reset button for a few seconds while the device is powered on. Use a ballpoint or paperclip to push down the reset button. Remember that this will wipe out any settings stored in flash memory including IP settings. The factory default IP address of the Router is 192.168.0.1 and the subnet mask is 255.255.255.0.

3

Configuring the Router for the First Time

The first time you set up the Router it is recommended that you configure the WAN connection using a single computer making sure that both the computer and the Router are not connected to the LAN. Once the WAN connection is functioning properly you may continue to change settings to suit your preferences. This chapter is only concerned with establishing the WAN connection. The following chapter, Web-based Management Guide, describes the various menus used to configure and monitor the Router including how to change IP settings and DHCP server setup.

Wan Configuration Summary

1. **Connect to the Router** To configure the WAN connection used by the Router it is first necessary to communicate with the Router through its management interface, which is HTML-based and can be accessed using a web browser. To access the management software your computer must be able to "see" the Router. Your computer can see the Router if it is in the same "neighborhood" or subnet as the Router. This is accomplished by making sure your computer has IP settings that place it in the same subnet as the Router. The easiest way to make sure your computer has the correct IP settings is to configure it to use the DHCP server in the Router. The next section describes how to change the IP configuration for a computer running a Windows operating system to be a DHCP client.

2. **Configure the WAN Connection** Once you are able to access the configuration software you can proceed to change the settings required to establish the SHDSL connection and connect to the service provider's network. There are different methods used to establish the connection to the service provider's network and ultimately to the Internet. You should know what Encapsulation and connection type you are required to use for your SHDSL service. It is also possible that you must change the PVC settings used for the SHDSL connection. Your service provider should provide all the information you need to configure the WAN connection.

Configuring IP Settings on Your Computer

In order to configure your system to receive IP settings from the Router it must first have the TCP/IP protocol installed. If you have an Ethernet port on your computer, it probably already has TCP/IP protocol installed. If you are using Windows XP the TCP/IP is enabled by default for standard installations. Below is an illustrated example of how to configure a Windows XP system to automatically obtain IP settings from the Router. Following this example is a step-by-step description of the procedures used on the other Windows operating systems to first check if the TCP/IP protocol has been installed, if it is not instruction are provided for installing it. Once the protocol has been installed you can configure the system to receive IP settings from the Router.

For computers running non-Windows operating systems, follow the instructions for your OS that configure the system to receive an IP address from the Router, that is, configure the system to be a DHCP client.

NOTE: If you are using this Router to provide Internet access for more than one computer, you can use these instructions later to change the IP settings for the other computers. However you cannot use the same IP address since every computer must have its own IP address that is unique on the local network.

Configure DHCP for Windows 95/98/Me

Use the following steps to configure the administrator's computer to be a DHCP client for computers running Windows 95, 98 or Me.

1. In Windows 95/98, click on the **Start** button, go to **Settings** and choose **Control Panel**.
2. In the Control Panel window, **double-click** on the **Network** icon.
3. Under the Configuration tab, select the **TCP/IP** component for your Ethernet connection and click **Properties**.
4. Check to see if the "**Obtain an IP address**" automatically has already been selected, if not, select the Obtain an IP address automatically by clicking the blank circle to the left of the option and click **OK**. If this option is already selected, renew the IP settings by following the instructions on the next page.
5. **Restart** the computer to let the new setting take effect.

Configure DHCP for Windows 2000/XP

Use the following steps to configure the administrator's computer to be a DHCP client for computers running Windows 2000.

1. Go to Start/Settings/Network and Dial-up Connections:
2. Right-click the Ethernet connection for which you want to install and enable TCP/IP, and then click Properties.
3. Click "Obtain an IP address automatically" and then click OK. If this option is already selected, you may run a renew IP settings commend in Windows. See the next page for details.

DHCP Configuration for Windows NT

Use the following steps to configure the administrator's computer to be a DHCP client for computers running Windows NT.

1. From the Start menu, select **Settings**, choose **Control Panel**.
2. Double-click on the **Network** control panel.
3. Click on the **Protocol** tab.
4. Select **TCP/IP** and click **Properties**.
5. Select "**Obtain an IP address from a DHCP Service**". If this option is already selected, you may run a renew IP settings commend in Windows. See the next page for details
6. Click **OK** for the TCP/IP Properties window.
7. Click **OK** for the Network window.
8. **Restart** your computer.

Renew IP Settings in Windows for DHCP Client

If your computer is already configured for DHCP (Obtain IP settings automatically), the IP settings can be renewed without restarting. Follow the procedures below for your Windows OS.

Windows 95/98/Me

1. For Windows 95/98/Me click on the **Start** button, go to the **Run** and click once to see the command dialog box.
2. Type in **winipcfg** and click **OK**. A new screen appears listing information about your network IP settings.
3. In the new screen, click on the **Renew All** button.
4. Click **OK**. The IP settings should now be updated so you can use the web manager.

Windows 2000/NT/XP

1. For Windows 2000/NT/XP bring up the **Command Prompt** screen.
2. Type in **ipconfig** and click **OK**. A new screen appears listing information about your network IP settings.
3. In the new screen, click on the **Renew All** button.
4. Click **OK**. The IP settings should now be updated so you can use the web manager.

Accessing the Configuration Manager

Now that your computer's IP settings allow it to communicate with the Router, you can access the configuration software.

NOTE: Be sure that the web browser on your computer 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.

Alternatively you can access this Internet Options menu using the Tools pull down menu in Internet Explorer.

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** button.
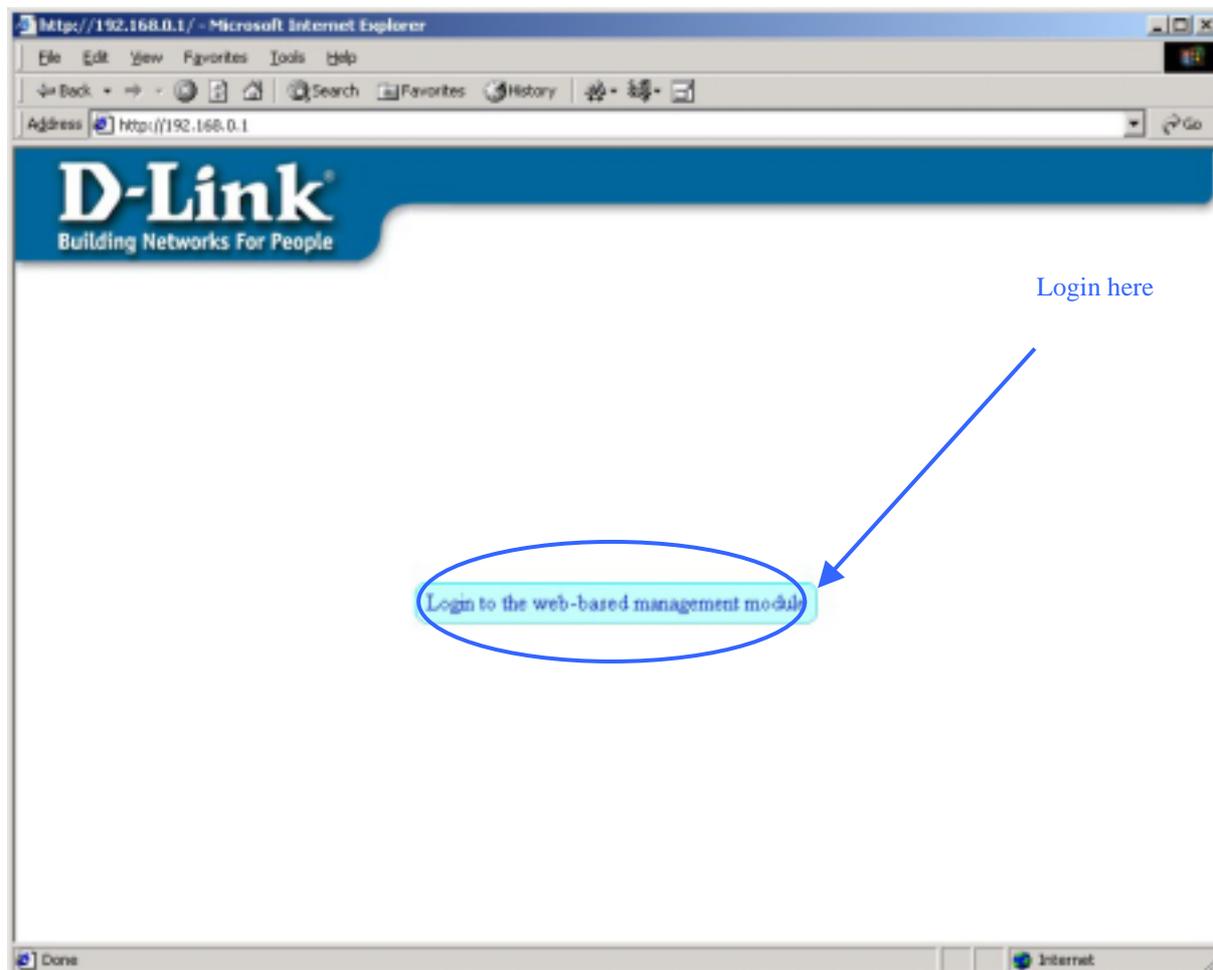
Login Page

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 setup. 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.

Enter User Name and Password

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

4

Web-based Management Guide

The DSL-1501G uses an HTML-based graphical user interface (GUI) allowing users to manage the Router from anywhere on the LAN using a standard browser, software such as Netscape Navigator or Microsoft Internet Explorer. The web browser is used for direct communication with the Router using HTTP protocol.

Accessing the Web Manager

In order to use the web-based management software it will be necessary to use a computer that occupies the same subnet as the Router. The simplest way to do this for many users will be to use DHCP server that is enabled by default on the Router. Chapter 3 provides instructions on how to configure a system running Windows operating systems to be DHCP client. You may also manually assign IP settings for the computer so that it resides on the same subnet as the Router. The Router has a default IP address of 192.168.0.1 and a subnet mask of 255.255.255.0. If you specify IP settings, use an IP address in the range 192.168.0.2 – 192.168.0.254 with a subnet mask of 255.255.255.0. Once you have accessed the configuration software you can configure the Router's IP settings and DHCP server configuration to suit your preferences.

To use the web-based management software run the browser you have installed on your computer and direct it to the Router's HTML interface using its LAN IP address. If this is the first time you are accessing the web-based manager you must type its 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** button.

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

Web Manager Layout

The web manager GUI (Graphic User Interface) displays two fields that can be scrolled with your mouse to view areas of the field that may be hidden from view. The field located on the left side of the GUI contains three folders that can be opened with a double left click of the mouse. Open the Configuration folder, the Maintenance folder and the Summary folder and you will see that each contains a number of labeled link buttons. You can click the button or the hyperlinked title of these buttons to view the menu associated with it. These are the menus you will use to configure, manage and monitor the Router.

Web Manager GUI

Web Manager Folders and Menus

Router Configuration

All the settings that define Router operations on both the LAN and WAN can be configured with the menus located in the **Configuration** folder. These menus are described in the first part of this chapter presented in the same order that they appear in your browser.

The **Maintenance** folder and **Summary** folder contain menus useful for system upkeep and analysis. These menus are described later in this chapter.

Multiple PVC

The Multiple PVC menu entry fields will change depending upon the index you select − using the **Select index to set** drop-down menu − or the encapsulation method you select − using the **Encapsulation** drop-down menu. Fields that will allow you to enter the appropriate information for the connection method selected.

Multiple PVC menu is used to configure the WAN connection. The WAN connection must have the correct connection Index including accurate VPI and VCI values. For PPPoA and PPPoE connections you must also supply user account information (User Name and Password) to access the service provider's network. *This is NOT the same as the System User Name and Password used to access the web manager of the Router*. See the table below for a complete description of the various configurable parameters in the Router/Bridge Configuration menu. Auto-refresh may be disabled to prevent the PPP Information from displaying updates.

Multiple PVC

The parameters available to be configured in the Router/Bridge Configuration menu change according to the Connection Profile configured.

NOTICE: If you must change the Connection Profile, change it to the desired setting and click the **OK** button without making any other changes. Save the changes and reboot the device. Upon restarting continue to configure any remaining settings that need to be changed in the Router/Bridge Configuration Menu. It will again be necessary to save settings and restart the Router to establish the WAN connection.

All connections must configure:	
Select Index to set	Use this drop-down menu to select the connection Index. If your DSL connection uses different VPI/VCI values, a new connection index must be created. As new connection indexes are created, they will be listed at the top of the **Multiple PVC** page.
Encapsulation Method	Select LLC or VC Mux as instructed by your service provider.
PPPoA and PPPoE connection profiles must configure:	
Login User Name	Type in the account user name used for authentication by your network service provider.
Login Password	Type in the account password used for authentication by your network service provider.
Confirm Password	Type the same password to confirm it.
Authentication	Choose the security protocol used to confirm the identity of the subscriber. Choose chap (default) or pap from the drop-down menu.
Connect on Demand	Select enabled or disabled. When this function is enabled the router will connect to any workstation on your LAN to the Internet upon request. If this function is disabled, it will be necessary to access this menu and hit the Connect button each time you want to establish a connection to the WAN or the Internet.
Idle Time	A value of 0 means that the PPP connection will remain connected. 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. The default value = 0.
IPoA connection profiles must configure:	
IP Unnumbered	This is enabled by default and therefore no IP settings need to be entered for the account. If this is disabled, (global) IP settings must be configured for the WAN interface.
IP Address	If IP Unnumbered is disabled, type in the WAN IP address for the account.
Subnet Mask	If IP Unnumbered is disabled, type in the subnet mask for the WAN interface.

Connect / Disconnect Buttons

If you have enabled the Connect on Demand feature, the Router will begin to negotiate the WAN connection upon restarting. If the Connect on Demand feature has been disabled, click the **Connect** button to initiate the connection via the WAN interface. The process will take a few seconds. To end the WAN connection, click on the **Disconnect** button.

Bridge Configuration

The DSL-1500 supports RFC 1483 sometimes called Bridged Ethernet. In bridge mode operation the device does not have the same capabilities as it does when operating in router mode. Packet forwarding for a bridge is limited to Layer 2, i.e. MAC address information only. A bridge operation may be appropriate when it is necessary to bridge the WAN and LAN interface in order to support non-IP based protocols. Bridge mode may also be best suited for LAN-to-LAN operations.

Bridge LLC mode – Multiple PVC menu

If you change the Multiple PVC page to Bridge LLC or VC mux, the user changeable parameters will change on the Multiple PVC page to allow you to enter the information appropriate to the connection method.

IPoA Configuration

IPoA connections are configured by first selecting **IPoA LLC** or **IPoA VC mux** from the **Encapsulation** drop-down menu. The Multiple PVC page will then change the user-entry fields to reflect the information you must enter to configure an IPoA connection.

IPoA LLC mode – Multiple PVC menu

The **IP Unnumbered** option is disabled by default. If you have not been given specific IP settings to configure for the device using IPoA, leave this option disabled.

If the IP Unnumbered option is not enabled the IP settings must be specified, use the IP settings information provided by your ISP. Type in the WAN interface **IP Address** and **Subnet Mask** for the account.

Configuring LAN IP Settings

Use this menu to change the LAN IP address of the Router. You can also find the MAC address for the Router listed here.

Ethernet IP Address Menu

The Ethernet IP Address displays the current LAN IP settings of the Router. To change the IP address, type in the new LAN **IP Address** in the space provided and select a **Subnet Mask** from the drop-down menu. Click on the **OK** button. If DHCP is enabled, a screen prompt will appear:
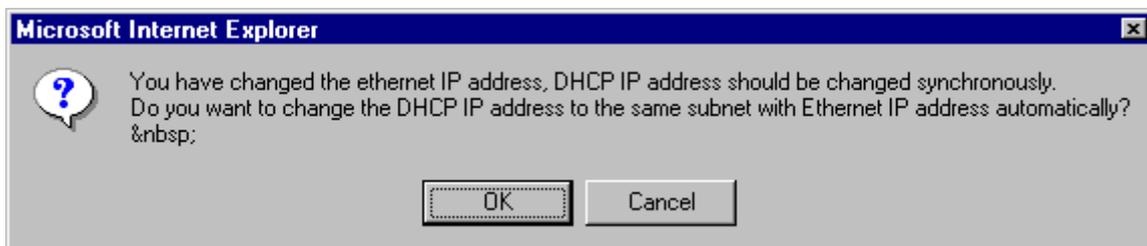
If you will continue to use the DHCP function, click the **OK** button. Otherwise you will need to manually configure the DHCP server addresses to reflect the change.

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

Proxy DNS Settings

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

Proxy DNS Menu

The Proxy DNS Menu presents the following user defined parameters:

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

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

DHCP Configuration

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

DHCP Configuration Menu

Configure LAN DHCP services by defining the following parameters:

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

NAT Configuration

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

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

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

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

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

NAT Configuration Menu

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

NAT Function	Default = enabled. Select *enabled* or *disabled* to enable or disable the NAT function.
DMZ State	Default = disabled. Select *enabled* or *disabled* to enable or disable the DMZ function.
DMZ IP Address	With the DMZ State enabled, type in the LAN IP address of a designated DMZ device (see explanation below).
Interface	For users with multiple PVC accounts, you can configure NAT for each profile. NAT is enabled by default for any additional profiles.

DMZ IP Address

NAT may conflict with certain interactive applications such as video conferencing or playing Internet video games. For these applications, a NAT bypass can be set up using a DMZ IP address. The DMZ IP address is a "visible" address and does not benefit from the full protection of the NAT function. Therefore it is advisable that

other security precautions be enabled to protect the other computers and devices on the LAN. It may be wise to isolate the device with the DMZ IP address from the rest of the LAN.

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

For the system that uses the DMZ IP address, you may want to manually assign an IP address to it and adjust your DHCP server addresses so that the DMZ IP address is not included in the DHCP server range. This way you avoid possible IP address problems if you reboot the DMZ system.

Multiple NAT Configuration

The Multiple NAT function will allow the user to configure NAT from more than one ISP designated IP address. This function is useful for users who have a limited number of IP addresses for a great amount of computers. If you only have one designated IP address given to you by your ISP, assure that this function is disabled, which is the default setting.

The top half of the screen displays the current status and settings implemented for the Multiple NAT mode, including the Index, State, Item Name, LAN configurations, WAN configurations and the DMZ status. The bottom half of the screen is where the user can configure Multiple NATs.

To view the Multiple NAT configuration menu, click on the Multiple NAT button:

Multiple NAT Configuration Menu

Multiple NAT State	Default = disabled. Select *enabled* if you wish to configure multiple NATs. Select *disabled* if there is only one designated IP address assigned to you by you ISP. Click **Apply** to change the state and save the changes to the router's memory. The system must be rebooted for these changes to take affect.	
Select index to set	Default = not selected. Upon initial configuration, this field will have no entries because they need to be set by the user. After setting an index (item name) you may click on the buttons adjacent to this field to modify or delete an index. The Clear button will clear all of the settings in the fields directly below.	
LAN	Start IP	Specify the IP address of the router used for allocation of IP addresses to computers on you Local Area Network.
	Range	Specify a range of numbers between 2 and 254 that you would like the router to automatically allot to the computers on your network. This range will represent the ending numbers of the Start IP address. (x, where x is 192.168.0.x)
WAN	Start IP	Specify the IP address given to you by your ISP.
	Range	Specify a range of numbers between 2 and 254 which denote the range of IP addresses given to you by your ISP.
DMZ	Default = disabled. Select *enabled* or *disabled* to enable or disable the DMZ function within the specified Nat index.	

NAT ALGs

NAT ALGs, or Application Layer Gateway is a function that helps applications running behind NAT to function correctly, and quickly without great involvement from the user. Certain protocols, such as IPsec and PPTP, have difficulty operating in conjunction with NAT. With NAT ALGs enabled, the router can forward those packets without subjecting them to NAT address mapping. Checking the corresponding boxes next to the protocols listed below will allow applications using these protocols to function correctly and quickly within the assigned LAN by allowing those packets to pass, by default. Unchecking the corresponding box will block the packet type from routing Protocols supported by this application are *H.323*, *IPsec*, *PPTP*, *ICQ* and *SIP*. *H323*, *IPsec*, *PPTP* and *ICQ* are checked, by default. Click **OK** to set checked protocols.
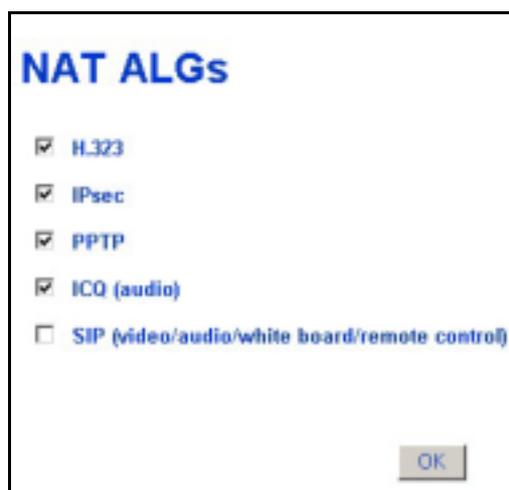
NAT ALGs Configuration Menu

IP Masquerade Timer

The IP Masquerade Timer is used to control how frequently the IP Masquerade table is updated. The IP Masquerade table is used to map the internal LAN IP addresses to the external WAN global IP address used for your account. If you are familiar with Ethernet switching, you can think of the IP Masquerade Timer as being similar to a MAC address table timeout in a switch.

IP Masquerade Timer

To change the IP Masquerade for the default settings, select the time for TCP or UDP packets from their respective drop-down menus and click the *OK* button.

Port Redirection
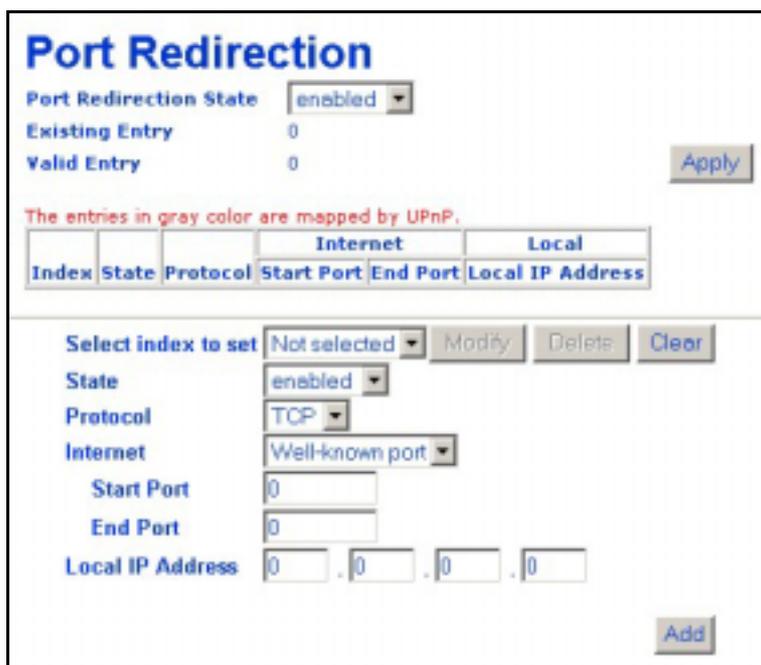
Port Redirection Menu

The Port Redirection feature of the Router is used in conjunction with NAT or IP Masquerading to improve security and efficiency. Port redirection can be used to direct potentially hazardous packets to a proxy server outside your firewall. For example, you can configure the Router 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.

Port Redirection can be used to redirect TCP or UDP packets to a specified port and a specified IP address on your local network. You can define a set of instructions for a specific incoming port or for a range of incoming ports. Each instruction set or rule is indexed and can be modified or deleted later as needed.

The user changeable variables available for Port Redirection are listed in the table below.

Port redirection is universally enabled or disabled for the Router with the **Port Redirection State** drop-down menu. The **Existing Entry** number tells you how many sets currently are configured. The **Valid Entry** number tells you the number of sets that are active.

Select index to set	When adding a new set, choose the *Not selected* option from the drop-down menu first. This will automatically add the next available index number to the new rule. If you are deleting or modifying an existing rule, select it and click the appropriate button to the right.
State	Select *Enabled* to put the set into effect when it is applied. To save a set you do not want to use now for later use without deleting it you can choose *Disabled*.
Protocol	Select the designated TCP or UDP protocol port number or use a well-know port for the particular protocol packet you wish to redirect.
Internet	Select one of the well-known ports to redirect incoming packets through that port.
Start Port	For a range of ports, this will be the first port in the range. For a single port enter the port number.
End Port	For a range of ports, this will be the last port in the range. For a single port just enter the same port number entered in Start Port.
Local IP Address	Enter the IP address of the local designated host computer or device.

If you wish to delete or modify an existing rule, select the index number and click the action button for **Delete** or **Modify**. Clicking on the **Clear** button will set the variables to the blank or default setting.

Each new set that is added will appear in the entry table at the top of the web page. When you have configure all the redirection sets you want to produce, click on the **Apply** button. You can save and reboot the system now, or continue to configure the Router.

Static Route Configuration

Use Static Routing to specify a route used for data traffic within your Ethernet LAN or to route data on the WAN. This is used to specify that all packets destined for a particular network or subnet use a predetermined gateway. The **Existing Entry** number tells you how many routes are currently configured. The **Valid Entry** number tells you the number of routes that are enabled.

Static Route Configuration Table

The following variables must be defined for static route configuration is as follows:

Select index to set	When adding a new route, choose the *Not selected* option from the drop-down menu first. This will automatically assign the next available index number to the new route. If you are deleting or modifying an existing route, select it and click the appropriate button to the right.
Item Name	Name of the subnet or static route used.
State	Select *Enabled* to start using the static route when it is applied. To save a route you do not want to use now for later use without deleting it you can choose *Disabled*.
IP Address	IP address of the subnet or device where packets are routed.
Subnet Mask	Subnet mask that allows packets to be routed as intended.
Gateway	IP address of the gateway used for this static route.
Interface	Choose Ethernet or select a WAN interface. If you have a single PVC and have not modified the name of the WAN interface, it appears here as ISP1 (the default name for the WAN interface).
Metric	Maximum number of hops allowed for the static route.

To delete or modify an existing route, select the index number and click the action button for *Delete* or *Modify*. Clicking on the *Clear* button will set the variables to the blank or default setting.

Each new route that is added will appear in the entry table at the top of the web page. When you have configured all the routes you want to use, click on the *Apply* button. You can save and reboot the system now, or continue to configure the Router.

Advanced Filter & Firewall

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

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

Filtering rules can be precisely defined based upon source and destination IP address, as well as port and protocol information.

Filter & Firewall Main Menu

The **Existing Entry** number tells you how many routes are currently configured. The **Valid Entry** number tells you the number of routes that are enabled. Filtering can be universally enabled or disabled with the drop-down **IP Filter State** drop-down menu.

Define these variables for each filter rule:

Select index to set	When adding a new rule, choose the *Not selected* option from the drop-down menu first. This will automatically assign the next available index number to the new rule. If you are deleting or modifying an existing rule, select it and click the appropriate button to the right.

Item Name	Name filtering rule defined here.
State	Select *Enabled* to start using the static route when it is applied. To save a route you do not want to use now for later use without deleting it you can choose *Disabled*.
Pass or Block	Choose *Block* to drop packets as defined by the rule. The default *Pass* will route data without restriction as a normal packet.
Interface	Choose Ethernet or select a WAN interface. If you have a single PVC and have not modified the name of the WAN interface, it appears here as ISP1 (the default name for the WAN interface).
Protocol	Select *ICMP*, *TCP*, *UDP* or *All* to pass or block packets of that protocol type.
Source	Type in the source IP address and select the Subnet Mask to pass or block packets form that IP address.
< 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.	
Start Port	For a range of ports, this will be the first port in the range. For a single port enter the port number.
End Port	For a range of ports, this will be the last port in the range. For a single port just enter the same port number entered in Start Port.
Destination	Type in the destination IP address and select the Subnet Mask to pass or block packets destined to that IP address.

To delete or modify an existing rule, select the index number and click the action button for **Delete** or **Modify**. Clicking on the **Clear** button will set the variables to the blank or default setting.

Each new rule that is added will appear in the entry table at the top of the web page. When you have configured all the rules you want to use, click on the **Apply** button. You can save and reboot the system now, or continue to configure the Router.

RIP

Use the RIP menu to enable RIP version 1, version 2 or both for any interface. You can further specify whether to enable RIP packets to be sent or accepted. RIP is disabled by default on all interfaces (sending and accepting RIP packets).

RIP Menu

Select the Interface to configure for RIP and then select to RIP version 1 (*V1*), version 2 (*V2*) or *Both* for RIP packets sent from the Router (**Send**) or accepted by the Router (**Accept**). When you have configured RIP settings, click on the *Apply* button. You can save and reboot the system now, or continue to configure the Router.

Date & Time Settings

The Router can use Network Time Protocol (NTP) to set system time and date accurately using a public or private NTP server. The function may be disabled if highly accurate time recording is not a priority.

Date & Time Configuration

If you wish to use NTP to set system time and date following these steps:

1. Make sure *NTP enabled* is displayed in the **NTP State** drop-down menu.

2. Type in an NTP server IP address that can be used by the Router. Keep in mind that many NTP servers require permission before they may be used.

3. Select the **Time Zone** where the Router is located or the time zone you want to use for system time. Time zones are displayed as GMT (Greenwich Mean Time) plus or minus hours incremented by whole hours.

4. Click the *Set Time* button to set the time with the chosen NTP server. This will send a request to update system time and date. NTP update packets are sent periodically to ensure precision.

If you prefer to use to use the timer located in the computer you are using to configure the Router:

1. Select *Set time with local PC time* in the **NTP State** drop-down menu.

2. Click the *Set Time* button to set the time with your computer.

UPnP

Universal Plug and Play (UPnP) is a feature that facilitates networking for a variety of devices and systems. UPnP allows enabled systems to be networked more easily. This feature is enabled by default. You can disable it in the UPnP Configuration menu by selecting *disabled* and clicking the *OK* button.

UPnP Configuration

System Maintenance

The Mainatenance folder in the web mananger contains links to menus used for sytem maintenance functions including firmware upgarde and username/password configuration.

ATM Loopback Test

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

ATM Loopback Screen

To perform the test, define the following parameters:

VPI	Type in the VPI setting used for the network connection.
VCI	Type in the VCI setting used for the network connection.
F4/F5	Choose *F4* (Virtual Path) or *F5* (Virtual Connection) from the pull-down menu to define the flow type. An F4 flow test is used to verify that ATM network information (ATM cells) can be shared between network elements. This information is used within virtual paths to report an unavailable path or a virtual path that cannot be guaranteed. An F5 flow test is also used to verify that ATM network information can be shared between network elements. This information is used within virtual connections to report degraded virtual channel performance such as late arriving cells, lost cells, and cell insertion problems.
etoe/segment	Select the test type from the remaining pull-down menu. Choose *End-to-End* to test the entire path from the Router to the ATM connection endpoint. Choose *segment* to test the path from the Router to the end of the first ATM connection segment.
Status	A success or fail message appears here after the test is completed. If the reply cell is received within the standard-defined time, the Status will read *OK*. This indicates that the specified test path is functioning normally and all connections were successful. If the Status reads *Fail*, there is a fault in the segment or path tested.

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

System Username and Password

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

System User Name and Password Menu

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

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

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

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

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

Save Changes

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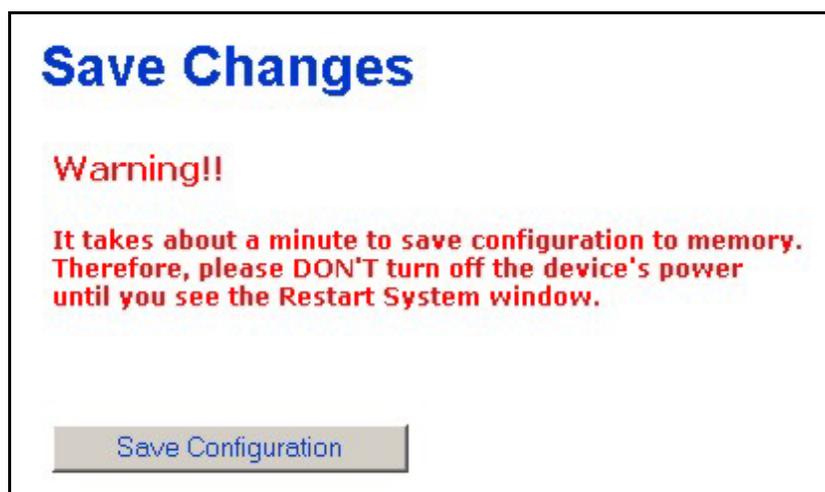
Save Changes Menu

Factory Reset

The DSL-1501G can be reset to the default configuration for all settings using the Factory Reset option. This will also change the both the LAN and WAN IP address of the device, so these will need to be reconfigured accordingly.
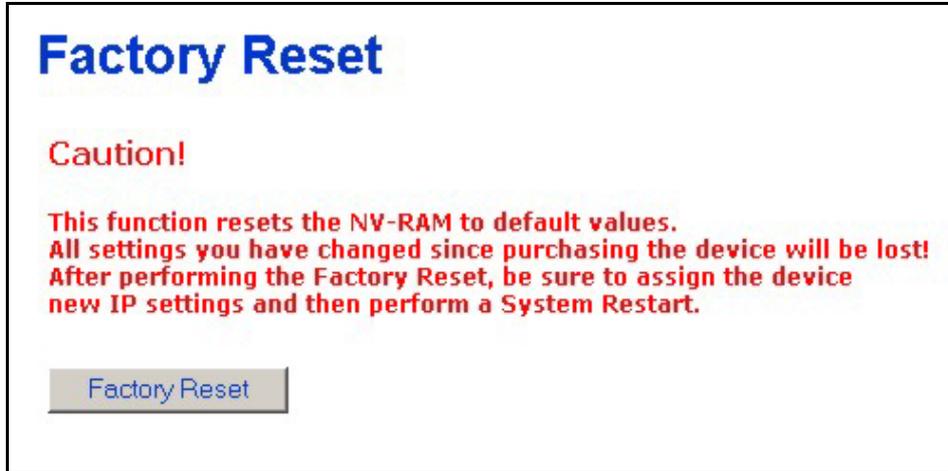
Factory Reset Screen

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

Update Firmware

Use the Update Firmware feature to load the latest firmware for the device. You can obtain the latest version of the DSL-1501G firmware by logging onto the D-Link web site at www.dlink.com. Access the D-Link web site by clicking on the D-Link logo in the upper left corner of the browser window. Save the latest firmware version to a file on your computer or an accessible TFTP server.

Update Firmware Screen

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

Configuration File Maintenance

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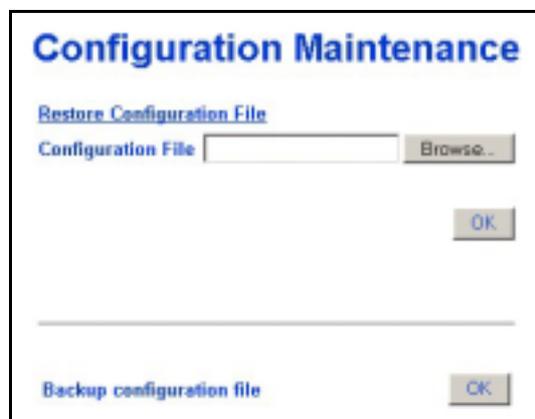
Configuration Maintenance Screen

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

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

Remote Administration Access

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

Remote Administration Access

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

SHDSL Line Setting

If your SHDSL connection is disconnected or the connection is faulty, you can try to reconnect using the SHDSL Line Setting menu. The SHDSL/Link LED Indicator will light green if you have a viable SHDSL link. You can

also look at the Summary statistics and Line Condition windows to diagnose problems with the SHDSL connection.

To reestablish the SHDSL connection, click the **Retrain** button. The Router will initiate a new attempt to negotiate and establish the SHDSL connection. If this fails, check to make sure you are using the correct PVC (VPI/VCI) settings and restart the Router. If problems persist, call your ISP or SHDSL service provider. Inability to initiate or maintain the SHDSL link may indicate a problem at the other end (DSLAM) of the SHDSL connection.

Line Retrain

Connection Status	*disconnected* indicates an SHDSL connection failure
	idle indicates a valid connection that is currently not active
	active indicates a valid connection that currently is transmitting packets

Summary

Use the summary windows to monitor Router performance and troubleshoot the device.

System Summary

The main summary page displays key information about the WAN connection and various Router functions.

System Summary

See the Summary description on the following page.

IP Address Configuration	**IP Address**	Router LAN IP Address
	Subnet Mask	Subnet Mask on LAN
	MAC Address	Fixed Hardware ID of Router
PPP Login Information	**Login User Name**	User name used for PPP login
	Authentication	Method used for PPP authentication
WAN (PPP) Information	**IP Address**	WAN IP address used for account
	Connection Status	WAN connection status
PVC	**VPI**	Virtual Path Identifier
	VCI	Virtual Circuit Identifier
Connection Type	Mode	WAN Connection Protocol
	Encapsulation Method	Packet encapsulation method
Proxy DNS		Status of proxy DNS function
Get DNS IP automatically		Status of auto-detect DNS, *enabled* indicates the Router will get DNS information from the WAN (usually from the ISP server) if *disabled*, a DNS server IP address must be manually entered
DNS Server IP		IP address of DNS server being used, if there is no DNS server detected IP address will be 0.0.0.0
DHCP Configuration		DHCP server status
UPnP State		UPnP status
NAT Configuration		NAT status
DMZ State		DMZ status
IP Filter State		Filtering status
Date/Time		NTP status (*enabled* indicates Router is using NTP server)
Event Log		Event log status
Remote Administration Access		Remote administration status

DHCP Allocation Table

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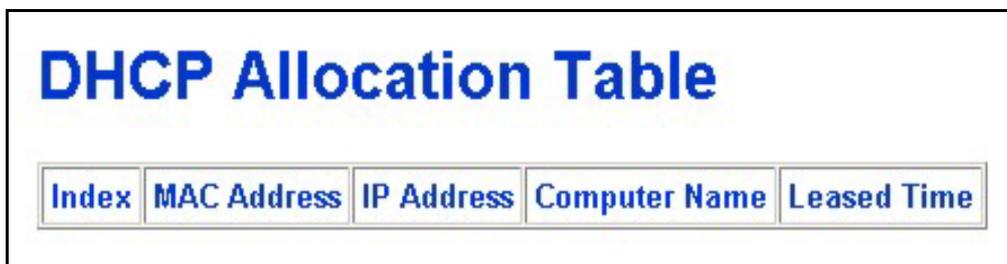
DHCP Allocation Table

Information listed in the DHCP Allocation Table includes the following:

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

Port Redirection Summary

The Port Redirection summary window is a lets you see how port redirection is currently configured for the Router.

Port Redirection Summary

Runtime Routing Table

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

Runtime Routing Table

Information listed in the Runtime Routing Table includes the following:

IP Address	IP address of network, subnet or device used for route
Subnet Mask	Subnet mask used for route
Gateway	IP address of gateway device used for route
Protocol	Route protocol or type, Direct or Static
Interface	Interface of network, subnet or device used for router, LAN or WAN
Metric	Number of hops used/allowed for route
Name	Name assigned to route

Filter and Firewall Summary

The Filter and Firewall summary window is a convenient way to view that status of filtering setup for the Router.

Filtering & Firewall Summary

Line Condition

Use the Line Condition summary window for troubleshooting problems with the SHDSL connection.

Line Condition

Protocol	SHDSL State	*Disconnected* - SHDSL connection failure
		Idle - valid connection currently not active
		Active - valid connection that currently transmitting packets
	Data Path	Current data path type Fast or Interleaved
	Operation Mode	Modulation technique used for SHDSL connection, G.DMT or G.lite
Link Status	SHDSL Link Speed	Downstream/Upstream data transfer rate in Kbps
	SNR	Downstream/Upstream Signal-to-Noise Ratio in dB
	ATTEN	Downstream/Upstream attenuation of signal in dB
Line Error	FEC (SHDSL)	Downstream/Upstream FEC Forward Error Correction
	CRC (SHDSL)	Downstream/Upstream CRC Cyclic Redundancy Control
	HEC (ATM)	Downstream/Upstream HEC Header Error Check
Frame Counter	Number of data packets received and transmitted	
Loop Distance		Loop in K ft.

Use the *Clear* button to start a fresh session. Check the **Auto-Refresh** box to automatically refresh the screen.

A

Technical Specifications

GENERAL	
LINE RATE	1 pair rate: Downstream/ Upstream up to 2.3 Mbps
	2 pair rate: Downstream/ Upstream up to 4.6 Mbps
MEDIA INTERFACE EXCHANGE	One RJ-11 port SHDSL connection - 1 pair (pins 2 and 3) 2 pair (4 wire)
	One RJ-45 10/100 Mbps MDI-X Fast Ethernet
	One RS-232/DB-9/DCE port for console connection
MANAGEMENT	HTML-based web manager
	Telnet
	TFTP services
	SNMP v.1/v.2c (MIB II)
	SNTP support
	UPnP
	Diagnostics (DSL line condition, tests for: data transmission, PPP, ISP connection, DNS server)

PHYSICAL AND ENVIRONMENTAL	
Power	Input: 100 ~ 240V AC 60Hz
	Output: 9V AC 1A
	Consumption: 5.06 Watts (max)
	Dying Gasp support
Temperature	Operating: 0° to 40° C (32° - 104° F)
	Storage: -20° to 70° C (-4° - 158° F)
Humidity	5 to 95% (non-condensing)
Dimensions	180 mm x 141 mm x 30 mm
Weight	350 grams
EMI	FCC Class B, CE Class B
Safety	CSA International

FACTORY RESET	
Reset Button	Hold button for three seconds to reset all configuration settings to factory default
Factory Default Settings	Device LAN IP Address: 192.168.0.1
	Device LAN Subnet Mask: 255.255.255.0
	System User Name: admin
	System Password: admin
	DHCP server: enabled
	NAT: enabled
	Web Manager: enabled

STANDARDS AND PROTOCOLS	
ATM/DSL	ITU G.991.2 (G.SHDSL) Annex A, B
	ITU-T Rec. I.361
	AAL5
	ATM Forum UNI3.1/4.0
	Supports F4/F5 Loopback test
	ATM Traffic Shaping (UBR, CBR, VBR-rt, VBR-nrt)
ENCAPSULATION	RFC 2684 (Bridged/Routed Ethernet over ATM)
	RFC 1577 (IP over ATM)
	RFC 2364 (PPP over ATM)
	RFC 2516 (PPP over Ethernet)
ETHERNET	IEEE 802.3
	IEEE 802.3u
	Supports dynamic MAC address learning
IPv4	TCP/UDP
	RIP-1/RIP-2
	ICMP
	DHCP server/client
	ARP
	RARP
	IP Routing
	IP Static Routing
	IGMP proxy support
	DNS
	NAT/NAT ALGs (H.323, IP Sec, PPTP, ICQ/audio, SIP/video/audio/white board/remote control)
	PAP
	CHAP
	VPN pass through IP Sec/PPTP
	Supports filtering for: ICMP, TCP, UDP

D-Link Offices

Australia	**D-Link Australasia** 1 Giffnock Avenue, North Ryde, NSW 2113, Sydney, Australia TEL: 61-2-8899-1800 FAX: 61-2-8899-1868 TOLL FREE (Australia): 1800-177100 TOLL FREE (New Zealand): 0800-900900 URL: www.dlink.com.au E-MAIL: support@dlink.com.au & info@dlink.com.au Level 1, 434 St. Kilda Road, Melbourne, Victoria 3004 Australia TEL: 61-3-9281-3232 FAX: 61-3-9281-3229 MOBILE: 0412-660-064
Canada	**D-Link Canada** 2180 Winston Park Drive, Oakville, Ontario, L6H 5W1 Canada TEL: 1-905-829-5033 FAX: 1-905-829-5095 BBS: 1-965-279-8732 TOLL FREE: 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 Fono, 2323185, Santiago, Chile, S. A. TEL: 56-2-232-3185 FAX: 56-2-232-0923 URL: www.dlink.cl E-MAIL: ccasassu@dlink.cl & tsilva@dlink.cl
China	**D-Link China** 15th Floor, Science & Technology Tower, No.11, Baishiqiao Road, Haidan District, 100081 Beijing, China TEL: 86-10-68467106 FAX: 86-10-68467110 URL: www.dlink.com.cn E-MAIL: liweii@digitalchina.com.cn
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: 20-2-635-6176 FAX: 20-2-635-6192 URL: www.dlink-me.com E-MAIL: support@dlink-me.com & fateen@dlink-me.com
Finland	**D-Link Finland** Pakkalankuja 7A, FIN– 0150 VANTAA, Finland TEL: 358-9-2707-5080 FAX: 358-9-2702-5081 URL: www.dlink-fi.com
France	**D-Link France** Le Florilege, No. 2, Allea de la Fresnerie, 78330 Fontenay Le Fleury, France TEL: 33-1-3023-8688 FAX: 33-1-3023-8689 URL: www.dlink-france.fr E-MAIL: info@dlink-france.fr
Germany	**D-Link Central Europe/D-Link Deutschland GmbH** Schwalbacher Strasse 74, D-65760 Eschborn, Germany TEL: 49-6196-77990 FAX: 49-6196-7799300 URL: www.dlink.de BBS: 49-(0) 6192-971199 (analog) BBS: 49-(0) 6192-971198 (ISDN) INFO: 00800-7250-0000 (toll free) HELP: 00800-7250-4000 (toll free) REPAIR: 00800-7250-8000 E-MAIL: info@dlink.de
India	**D-Link India** Plot No.5, Bandra-Kurla Complex Rd., Off Cst Rd., Santacruz (East), Mumbai, 400 098 India TEL: 91-022-652-6696/6578/6623 FAX: 91-022-652-8914/8476 URL: www.dlink-india.com, www.dlink.co.in & tushars@dlink-india.com E-MAIL: service@dlink.india.com
Italy	**D-Link Mediterraneo Srl/D-Link Italia** Via Nino Bonnet n. 6/B, 20154, Milano, Italy TEL: 39-02-2900-0676 FAX: 39-02-2900-1723 URL: www.dlink.it E-MAIL: info@dlink.it
Japan	**D-Link Japan** 10F, 8-8-15 Nishigotahda, Shinagawa, 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

Netherlands	**D-Link Benelux** Fellenoord 1305611 ZB, Eindhoven, the Netherlands TEL: 31-40-2668713 FAX: 31-40-2668666 URL: www.d-link-benelux.nl
Norway	**D-Link Norway** Waldemar Thranesgate 77, 0175 Oslo, Norway TEL: 47-22-991890 FAX: 47-22-207039 URL: www.dlink.no
Russia	**D-Link Russia** Michurinski Prospekt 49, 117607 Moscow, Russia TEL: 7-095-737-3389 & 7-095-737-3492 FAX: 7-095-737-3390 URL: www.dlink.ru 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 E-MAIL: info@dlink.com.sg URL: www.dlink-intl.com
South Africa	**D-Link South Africa** Unit 2, Parkside, 86 Oak Avenue, Highveld Technopark, Centurion, Gauteng, South Africa TEL: 27 (0) 12-665-2165 FAX: 27 (0) 12-665-2186 URL: www.d-link.co.za E-MAIL: attie@d-link.co.za
Spain	**D-Link Iberia** C/Sabino De Arana, 56 Bajos, 08028 Barcelona, Spain TEL: 34 93 4090770 FAX: 34 93 4910795 URL: www.dlinkiberia.es E-MAIL: info@dlinkiberia.es
Sweden	**D-Link Sweden** P. O. Box 15036, S-167 15 Bromma, Sweden TEL: 46-(0) 8-564-61900 FAX: 46-(0) 8-564-61901 E-MAIL: info@dlink.se URL: www.dlink.se
Taiwan	**D-Link Taiwan** 2F, No. 233-2 Pao-chiao Rd, Hsin-tien, Taipei, Taiwan TEL: 886-2-2916-1600 FAX: 886-2-2914-6299 URL: www.dlink.com.tw E-MAIL: dssqa@tsc.dlinktw.com.tw
Turkey	**D-Link Middle East** Deniz Bilgisayar, Buyukdere Cad. Naci Kasim Sk., No. 5 Mecidiyekoy, Istanbul, Turkey TEL: 90-212-213-3400 FAX: 90-212-213-3420 E-MAIL: smorovati@dlink-me.com
U.A.E.	**D-Link Middle East** CHS Aptec (Dubai), P.O. Box 33550 Dubai U.A.E. TEL: 971-4-366-885 FAX: 971-4-355-941 E-MAIL: Wxavier@dlink-me.com
U.K.	**D-Link Europe** 4th Floor, Merit House, Edgware Road, Colindale, London NW9 5AB United Kingdom TEL: 44 (0) 20-8731-5555 FAX: 44 (0) 20-8731-5511 BBS: 44 (0) 181-235-5511 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 BBS: 1-949-455-1779 & 1-949-455-9616 INFO: 1-800-326-1688 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®