D-Link®

DSL-504G
ADSL Router
User's Guide

(February 2003)

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 User's Guide

This user's guide provides instructions on how to install the DSL-504G ADSL Router and use it to connect a computer or Ethernet LAN (Local Area Network) to the Internet.

If you are using a computer with a functioning Ethernet port, you can use the Quick Installation Guide to quickly establish your ADSL connection and access the Internet.

Some basic information about Ethernet, 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 ADSL. 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.

Appendix B - Low Pass Filters – Illustrated examples of how to install low pass filters.

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 is described in general terms in the steps below:

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. Check the contents of the package to be certain that everything listed on the packing list is included. A packing list is included at the end of this section. 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. Some users may be given additional information by their service provider used to configure the Router so it can establish the connection.

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 used 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 management 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(s), 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 ADSL 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

To install and use the Router you need a computer equipped with an Ethernet port (such as an Ethernet NIC adapter card) and a web browser. You may also need to use information given to you by your service provider. This information is stored in the Router's memory and used to establish the network connection and confirm your identity. The information may be only your user name (or number) and password, or it may be information used to define your connection profile. The connection profile is used to instruct the Router how to communicate with the computers and other routers that are used to control access to the service provider's network and ultimately to the Internet. The connection profile is a logical construct that establishes a definite path used for communication and defines the rules or protocols used to initiate and maintain the communication path.

Low Pass Filters

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

Operating System

The DSL-504G 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, pop-up ad killer 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. Normally, an Ethernet port will be TCP/IP enabled, this means that it is able to communicate with other computers on an IP network (such as the Internet). Make sure your computer has the TCP/IP protocol installed. If you have accessed the Internet with the computer before, it already has this installed.

Additional Software

It may be necessary to install software on your computer that enables it to access the Internet. Additional software must be installed if you are using what is called a "bridged" connection. For a bridged connection, the information needed to make and maintain the Internet connection is stored on your computer, not in the Router. This type of connection is similar to the arrangement used for analog dial-up Routers, but the connection speed is much faster. Various terms are to describe a bridged ADSL connection including the term "1483 Bridged IP" used in this guide. RFC 1484 is a technical standard used to define a bridged connection.

If your ADSL service is delivered through a PPP (Point to Point Protocol) connection, the information needed to establish and maintain the Internet connection is stored in the Router. In this case, it is not necessary to install software on your computer.

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 connection profile you use.

ACCOUNT INFORMATION
User Name:
Password:

About Bridged Ethernet Connections (RFC 1483)

Using this method, the DSL-504G acts as a transparent bridge, and is invisible to other devices on both the WAN (wide area network) and LAN (local area network) side of the bridge. It is "invisible" in the sense that it does not have an IP address associated with it. Every device connected to the WAN must have an IP address to be "seen" on the IP network. Devices that connect to the Internet have a "global" IP address that is unique and is used to identify the device so that it can send and receive data.

All connections to the Internet require a global IP address. It is therefore necessary to provide some means of acquiring global IP settings for your account. For bridged connections, the global IP settings must reside in a TCP/IP enabled device on the LAN side of the bridge, such as a computer, a server or a firewall device. The IP address can be assigned in a number of ways. Your network service provider will give you instructions about any additional connection software or NIC configuration that may be required.

About IPoA Connections (RFC 1577)

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

Packing List

Open the shipping carton and carefully remove all items. In addition to this User's Guide, ascertain that you have:

1. One DSL-504G ADSL Ethernet Router

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

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

4. One straight-through Ethernet cable

5. One AC power adapter suitable for your electric service

1

Introduction

This section provides a brief description of the Router, its associated technologies and a list of Router features.

What is ADSL?

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. For ADSL services, expensive new cabling or line conditioning is not necessary.

ADSL greatly increases the signal carrying capacity of copper telephone lines without interfering with regular telephone services. For the ADSL user, this means faster downloads and more reliable connectivity. ADSL devices make high-speed Internet access possible 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 and up to 640 Kbps upstream, depending on local telephone line conditions. A secure point-to-point connection is established between the user and the central office of the service provider.

D-Link ADSL devices incorporate the recommendations of the ADSL Forum regarding framing, data format, and upper layer protocols.

Router Description and Operation

The DSL-504G 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-504G 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-504G 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 allows several computers to be networked and connected to the Internet using a single WAN interface and IP address.

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 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.

Router Features

The DSL-504G ADSL Ethernet Router utilizes the latest ADSL enhancements to provide a reliable Internet portal suitable for most small to medium sized offices. DSL-504G advantages include:
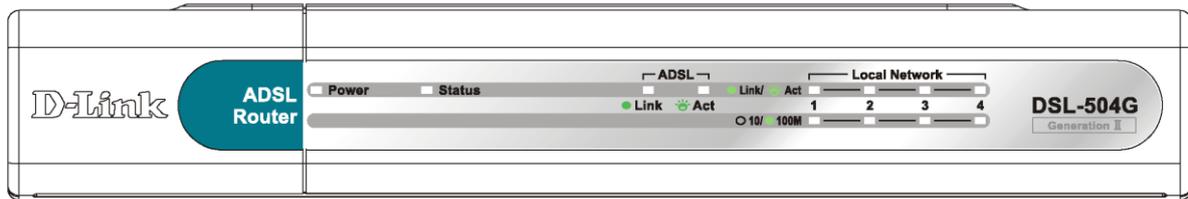
- **PPP (Point-to-Point Protocol) Security** The DSL-504G ADSL Router supports PAP (Password Authentication Protocol) and CHAP (Challenge Handshake Authentication Protocol) for PPP connections.

- **DHCP Support** 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-504G 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-504G 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-504G 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-504G supports *Bridged Ethernet over ATM* (RFC1483), *IP over ATM* (RFC1577) and *PPP over ATM* (RFC 2364).

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

- **G.hs (Auto-handshake)** This allows the Router to automatically choose either the G.lite or G.dmt ADSL connection standards.

- **High Performance** 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-504G 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-504G 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.

- **Multiple PVC Capability** The DSL-504G supports up to eight virtual channels operating simultaneously.

Front Panel Display and LED Indicators

Place the Router in a location that allows a view of the LED indicators on the front panel. LED indicators are especially useful for basic troubleshooting.
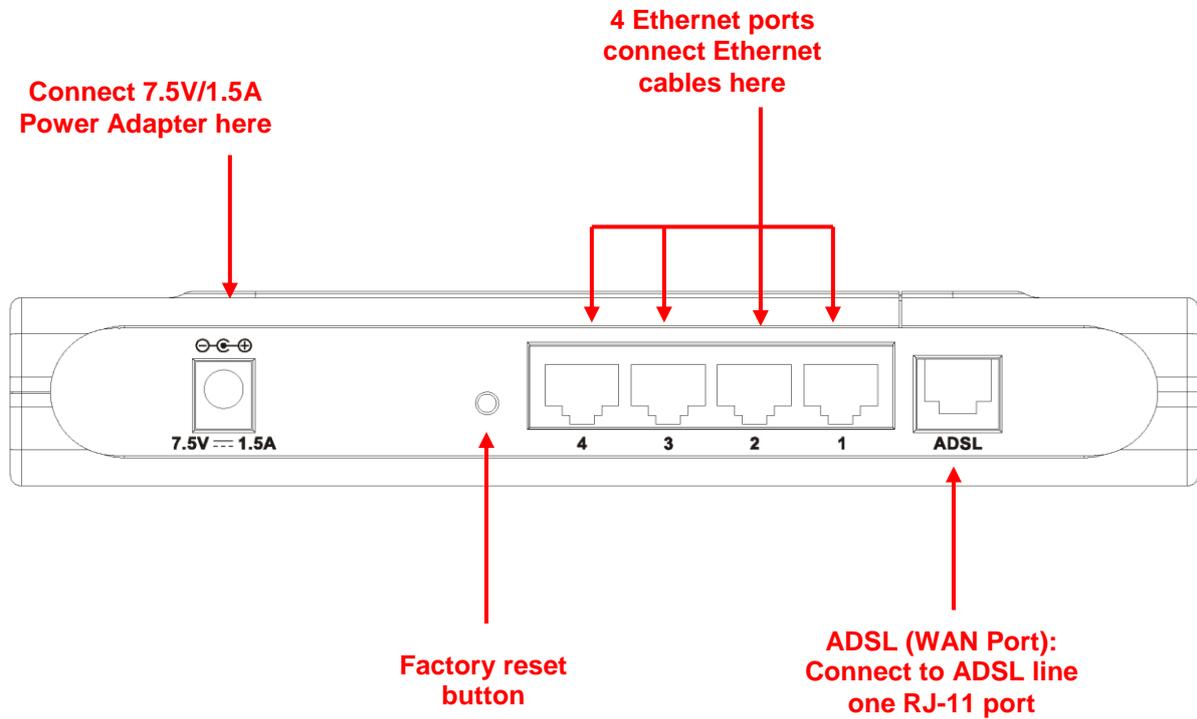

Front Panel Display

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 indicating normal function. A non-blinking or dark indicator after a successful negotiation indicates a problem. Try rebooting the Router if this occurs.
ADSL: Link/ Act	This will light after the ADSL negotiation process has been settled. Steady green light indicates a valid ADSL connection.
Ethernet: 10M/100M	These are per port indicators. Steady green indicates a 100 Mbps Fast Ethernet connection. It is dark for a 10 Mbps Ethernet connection.
Ethernet: Link/ Act	These are per port indicators. Green light indicates a valid Ethernet connection. Blinking green light indicates an active Ethernet session.

Rear Panel Cable Connections

All cable connections to the Router are made at the rear panel. Read the next chapter for a complete description of how to connect the Router.

4 Ethernet ports connect Ethernet cables here

Connect 7.5V/1.5A Power Adapter here

Factory reset button

ADSL (WAN Port): Connect to ADSL line one RJ-11 port

2

Hardware Installation

When selecting the location for the Router, be sure to allow room to access the connections on the rear panel. It is recommended that the Router be placed so the LED indicators can be seen easily for troubleshooting. Allow some space above the Router for ventilation and make sure it is not close to heat sources or appliances that produce a lot of heat to avoid problems from overheating. As with any electrical device, use common sense when choosing a location for the Router.

Connect ADSL Line

Use the ADSL cable included with the Router to connect it to a telephone wall socket. Plug one end of the cable into the ADSL port (RJ-11 receptacle) on the rear panel of the Router and insert the other end into the RJ-11 wall socket. If you are using a low pass filter device, follow the instructions included with the device or given to you by your service provider. The ADSL connection represents the WAN interface. It is the physical link to the ISP's network backbone and ultimately to the Internet.

After the Router is powered on it will undergo a negotiation process to establish 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 or the Router restarted, it will repeat this process. If you are required to change the PVC settings (VPI/VCI values), these will need to be changed before the Router can complete a connection to the ISP's network.

Connect Router to the Ethernet

The Router connects directly to Ethernet workstation or to an Ethernet LAN. The RJ-45 ports on the Router are crossed ports (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(s) on the front panel shine steady green.

The rules governing Ethernet cable lengths apply to the four Ethernet ports. Use standard Category 5 or better twisted-pair Ethernet cable with RJ-45 connectors. Be sure that the cable connecting the Router to other Ethernet devices does not exceed 100 meters. If the LED indicators do not indicate a valid Ethernet connection check each end of the cable to make sure it is securely inserted.

Computer to Router Connection

You can connect the Router directly to a 10/100BASE-TX Ethernet adapter card (NIC) installed on a computer or an embedded Ethernet port on a notebook computer or PC using the Ethernet cable provided. The Ethernet cable that comes with the Router is a straight-through cable. This type of cable is appropriate for connecting to a straight-through (MDI-II) port. MDI-II ports are commonly used for Ethernet adapters on desktop and notebook computers. Check the LED indicators to see if the link has been established.

Switch to Router Connection

If the switch has an available uplink port (MDI-II) you may connect the Router to the uplink port with a straight-through cable. If the switch has an uplink port and you wish to reserve this for another device, connect to any on the other MDI-X ports (1x, 2x, etc.) with a crossed cable. The easies way to see if the Ethernet connection is valid is to look at the LED indicators when the device is connected and powered on.

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 ADSL connection, if the ADSL 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 three times 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 10.1.1.1 and the subnet mask is 255.0.0.0.

3

Configuring the Router for the First Time

The first time you setup 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 change settings to suit your network. This chapter is only concerned with settings up 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 your are able to access the configuration software you can proceed to change the settings required to establish the ADSL 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 ADSL service. It is also possible that you must change the PVC settings used for the ADSL 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 Windows XP for DHCP

Use the following steps to configure a computer running Windows XP to be a DHCP client.
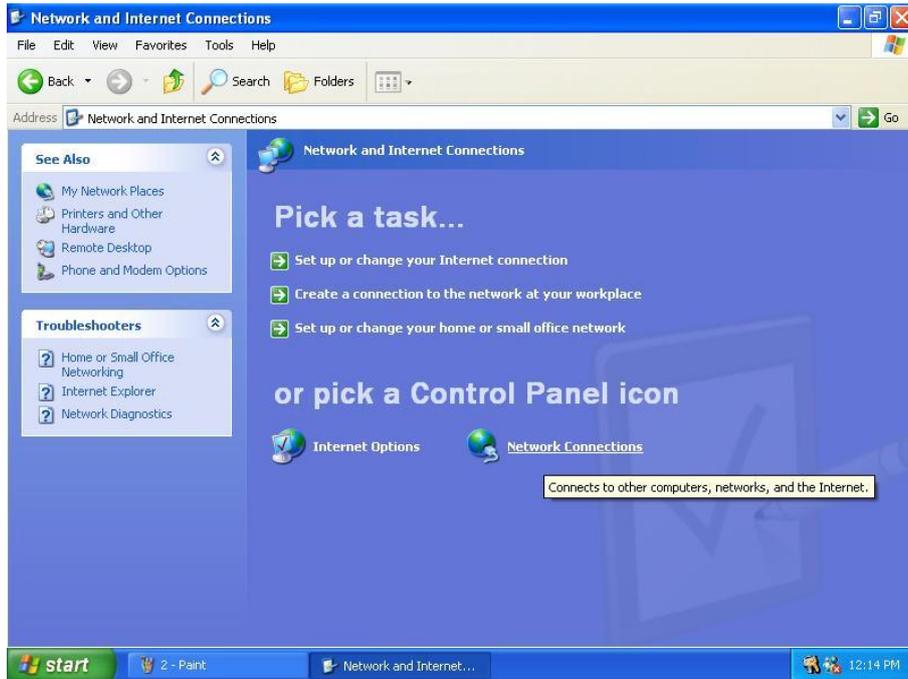
1. From the **Start** menu on your desktop, go to click on **Control Panel**.

2. In the Control Panel folder, click on **Network and Internet Connections**.
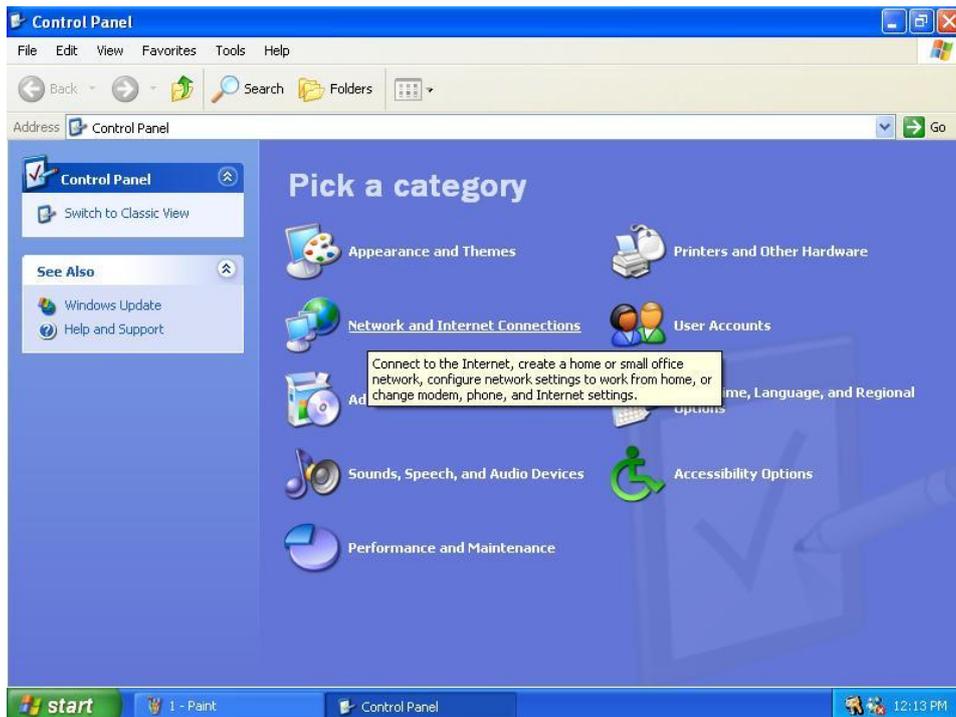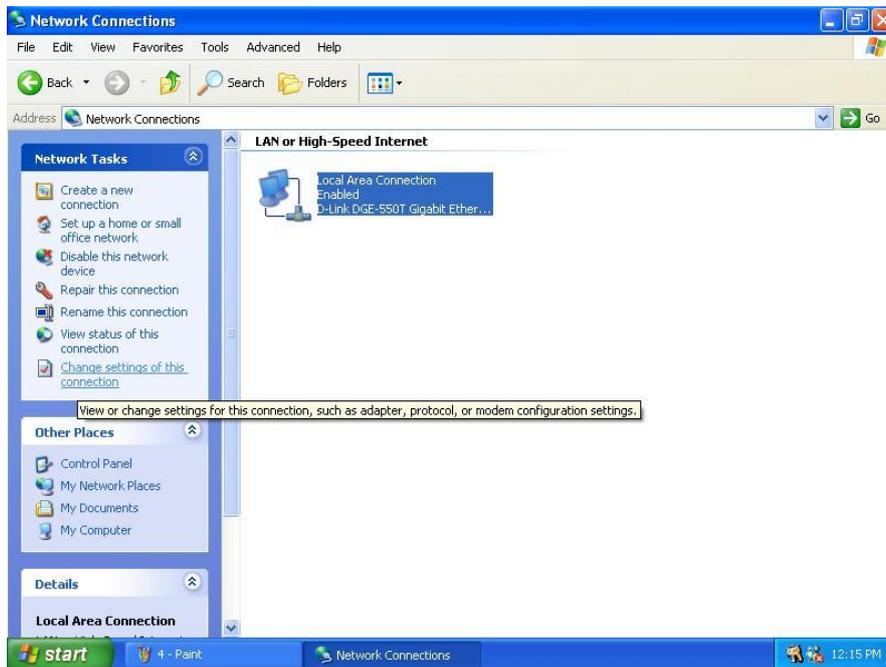
3. In the Network and Internet Connections folder, click on **Network Connections**.

4. In the Network Connections folder, highlight the **Local Area Connection** icon by clicking on it once. A new option is revealed under Network Tabs in the left side panel.
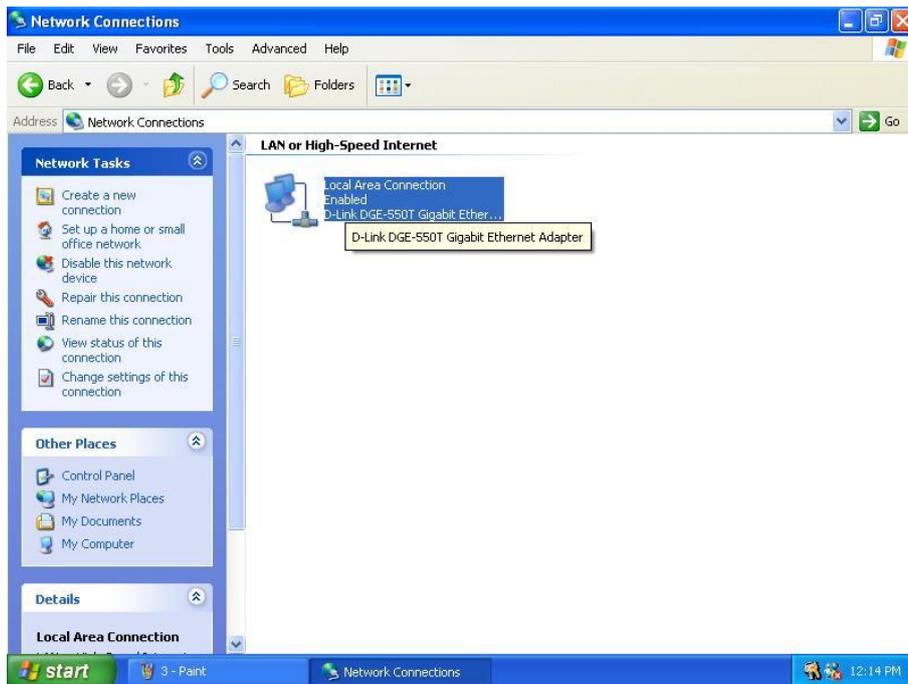
5. Click on **Change settings of the connection** under Network Tabs.

6. In the *General* Tab of the **Local Area Connection Properties** menu, highlight **Internet Protocol (TCP/IP)** under "This connection uses the following items:" by clicking on it once. Click on the **Properties** button.
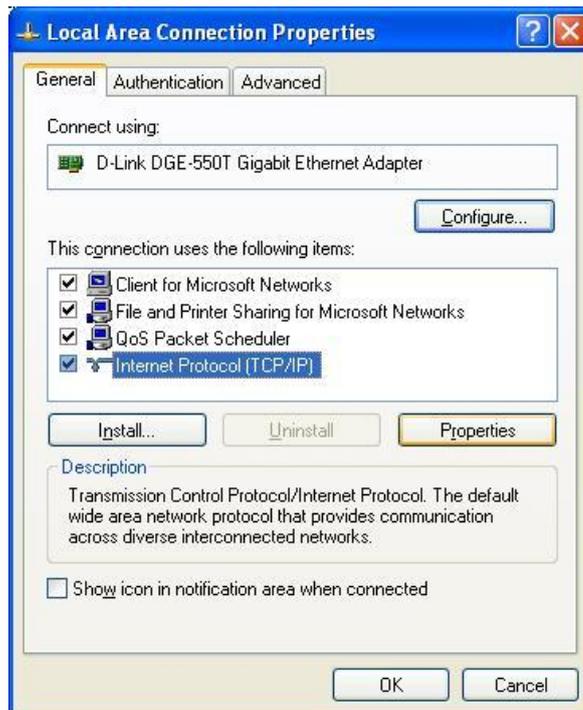
7. Select "Obtain an IP address automatically" by clicking once in the circle. Click the **OK** button.
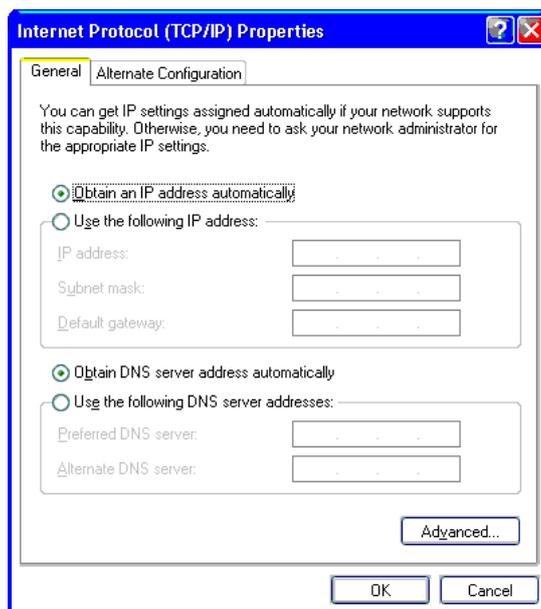
Your computer is now ready to use the Router's DHCP server.

Windows 2000

First, check for the IP protocol and, if necessary, install it:

1. In the Windows task bar, click the Start button, point to **Settings**, and then click **Control Panel**.
2. Double-click the Network and Dial-up Connections icon.
3. In the Network and Dial-up Connections window, right-click the Local Area Connection icon, and then select **Properties**.
4. The Local Area Connection Properties dialog box displays with a list of currently installed network components. If the list includes Internet Protocol (TCP/IP), then the protocol has already been enabled, skip ahead to *Configure Windows 2000 for DHCP*.
5. If Internet Protocol (TCP/IP) does not display as an installed component, click **Install**.
6. In the Select Network Component Type dialog box, select **Protocol**, and then click **Add**.
7. Select **Internet Protocol (TCP/IP)** in the Network Protocols list, and then click **OK**.
8. You may be prompted to install files from your Windows 2000 installation CD or other media. Follow the instructions to install the files.
9. If prompted, click **OK** to restart your computer with the new settings.

Configure Windows 2000 for DHCP

1. In the Control Panel, double-click the Network and Dial-up Connections icon.
2. In Network and Dial-up Connections window, right-click the Local Area Connection icon, and then select **Properties**.
3. In the Local Area Connection Properties dialog box, select **Internet Protocol** (**TCP/IP**), and then click **Properties**.
4. In the Internet Protocol (TCP/IP) Properties dialog box, click the button labeled **Obtain an IP address automatically**.
5. Double-click **OK** to confirm and save your changes, and then close the Control Panel.

Your computer is now ready to use the Router's DHCP server.

Windows ME

First, check for the IP protocol and, if necessary, install it:

1. In the Windows task bar, click the Start button, point to **Settings**, and then click **Control Panel**.
2. Double-click the Network and Dial-up Connections icon.
3. In the Network and Dial-up Connections window, right-click the Network icon, and then select **Properties**.
4. The Network Properties dialog box displays with a list of currently installed network components. If the list includes Internet Protocol (TCP/IP), then the protocol has already been enabled. Skip ahead to *Configure Windows ME for DHCP*.
5. If Internet Protocol (TCP/IP) does not display as an installed component, click **Add**.
6. In the Select Network Component Type dialog box, select **Protocol**, and then click **Add**.
7. Select **Microsoft** in the Manufacturers box.
8. Select **Internet Protocol (TCP/IP)** in the Network Protocols list, and then click **OK**.
9. You may be prompted to install files from your Windows Me installation CD or other media. Follow the instructions to install the files.
10. If prompted, click **OK** to restart your computer with the new settings.

Configure Windows ME for DHCP

1. In the Control Panel, double-click the Network and Dial-up Connections icon.
2. In Network and Dial-up Connections window, right-click the Network icon, and then select **Properties**.
3. In the Network Properties dialog box, select **TCP/IP**, and then click **Properties**.
4. In the TCP/IP Settings dialog box, click the **Obtain and IP address automatically** option.
5. Double-click **OK** twice to confirm and save your changes, and then close the Control Panel.

Your computer is now ready to use the Router's DHCP server.

Windows 95, 98

First, check for the IP protocol and, if necessary, install it:

1. In the Windows task bar, click the Start button, point to **Settings**, and then click **Control Panel**. Double-click the Network icon.
2. The Network dialog box displays with a list of currently installed network components. If the list includes TCP/IP, and then the protocol has already been enabled, skip to *Configure IP Information Windows 95, 98*.
3. If TCP/IP does not display as an installed component, click **Add**. The Select Network Component Type dialog box displays.
4. Select **Protocol**, and then click **Add**. The Select Network Protocol dialog box displays.
5. Click on **Microsoft** in the Manufacturers list box, and then click **TCP/IP** in the Network Protocols list box.
6. Click **OK** to return to the Network dialog box, and then click **OK** again. You may be prompted to install files from your Windows 95/98 installation CD. Follow the instructions to install the files.
7. Click **OK** to restart the PC and complete the TCP/IP installation.

Configure Windows 95, 98 for DHCP

1. Open the Control Panel window, and then click the Network icon.
2. Select the network component labeled TCP/IP, and then click **Properties**.
3. If you have multiple TCP/IP listings, select the listing associated with your network card or adapter.
4. In the TCP/IP Properties dialog box, click the IP Address tab.
5. Click the **Obtain an IP address automatically** option.
6. Double-click **OK** to confirm and save your changes. You will be prompted to restart Windows.
7. Click **Yes**.

When it has restarted your computer is ready to use the Router's DHCP server.

Windows NT 4.0 workstations:

First, check for the IP protocol and, if necessary, install it:

1. In the Windows NT task bar, click the Start button, point to **Settings**, and then click **Control Panel**.
2. In the Control Panel window, double click the Network icon.
3. In the Network dialog box, click the Protocols tab.
4. The Protocols tab displays a list of currently installed network protocols. If the list includes TCP/IP, then the protocol has already been enabled. Skip to "Configure IP Information"
5. If TCP/IP does not display as an installed component, click **Add**.
6. In the Select Network Protocol dialog box, select **TCP/IP**, and then click **OK**. You may be prompted to install files from your Windows NT installation CD or other media. Follow the instructions to install the files.
7. After all files are installed, a window displays to inform you that a TCP/IP service called DHCP can be set up to dynamically assign IP information.
8. Click **Yes** to continue, and then click **OK** if prompted to restart your computer.

Configure Windows NT 4.0 for DHCP

1. Open the Control Panel window, and then double-click the Network icon.
2. In the Network dialog box, click the Protocols tab.
3. In the Protocols tab, select **TCP/IP**, and then click **Properties**.
4. In the Microsoft TCP/IP Properties dialog box, click the **Obtain an IP address automatically** option.
5. Click **OK** twice to confirm and save your changes, and then close the Control Panel.

Your computer is now ready to use the Router's DHCP server.

Access the Web Configuration Manager

Once the computer has IP settings that allow it to access the web-based configuration software, you can change the settings to enable the Router to connect to the Internet.

If the browser software on the computer you are using is configured to use a proxy server for Internet access, it is necessary to first disable the proxy connection.

Check for Proxy service in Windows Internet Explorer:

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 your web browser software and use the LAN IP address of the Router to access the management software. The default LAN IP address of the Router is used in the Address bar of your web browser window. Type in **http://** followed by the default IP address, **10.1.1.1** in the address bar of the browser. The URL in the address bar should read: **http://10.1.1.1**

A new window appears prompting you for a user name and password needed to gain access the web configuration manager.


Use the default user name: **admin** and password: **admin** for first time set up. You can change the password once you have established the ADSL connection. The user name and password allows any computer on the same subnet as the Router to access the web configuration manger. This password can also be used to Telnet to the device through the Ethernet or the Internet interfaces. To change this password, see the next chapter.

	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.
Note	

The first web page you will see when you successfully login is the System View page. This page can be used later, once you have a connection established. For now however, the information contained here is not useful. The menu you need to establish the ADSL connection is the Quick Configuration menu. This menu is located in the Home folder located on the left hand side of your browser window. Open this folder by clicking on it twice.
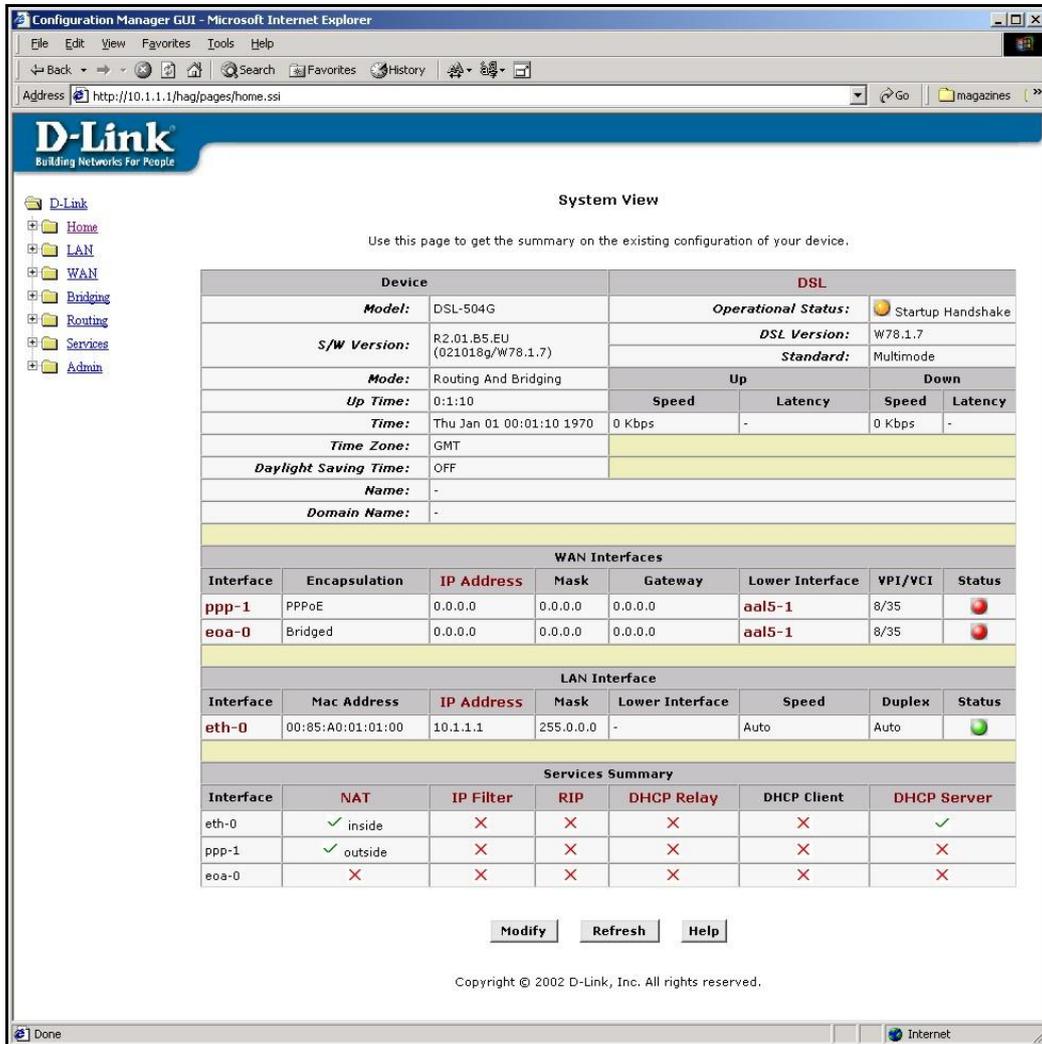

Web-based Manager Main Menu – First Time Log On

In the Home folder you will see two hyperlinks, Home and Quick Configuration. You need to access the Quick Configuration menu; double-click on the hyperlink for this menu. Once you have accessed the menu you can change the Router's configuration settings as instructed by your ISP. You will then need to save or "Submit" the settings to the flash memory of the Router. Finally you will use another menu to commit the new settings so these settings can be used by the Router, and restart the device. This last step is done in the Commit & Reboot menu. If you have been given special connection software to install on your computer, you can install it while the Router is rebooting.

# Configure WAN Connection (ADSL Service Connection)

Click on the Quick Configuration hyperlink to access the configuration settings you need to establish the ADSL connection.
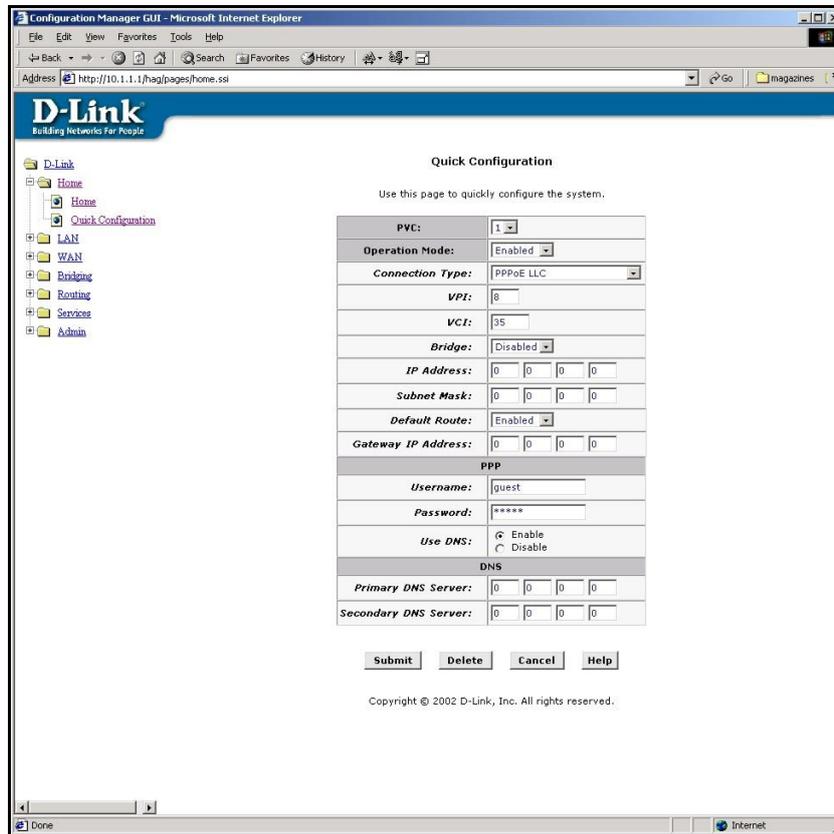
Quick Configuration Window

When setting up the Router for the first time, use the Quick Configuration window and follow the steps below to change settings as instructed by your ISP. Some of the settings can be left at their default value depending on the requirements of the connection. Details about the settings listed here can be found in the next chapter.

1. **PVC:** Leave this set at the default value 0 the first time the Router is set up. For more information on this option see Multiple PVC Operation.

2. **Operation Mode:** This also should be left at the default setting *Enabled*. This enables the PVC used for the initial connection.

3. *Connection Type:* Change connection method and packet encapsulation technique as instructed by your ISP. The available connection types are *PPPoA VC-Mux, PPPoA LLC, PPPoE VC-Mux, PPPoE LLC, 1483 Routed IP VC-Mux, 1483 Routed IP LLC, 1483 Routed IP LLC(1577), 1483 Bridged IP VC-Mux, 1483 Bridged IP LLC* from the pull-down menu. Default Connection Type = *PPPoE LLC*.

4. *VPI:* If instructed to change this, type in the VPI value for the initial connection (using PVC 0). Default = *8*.
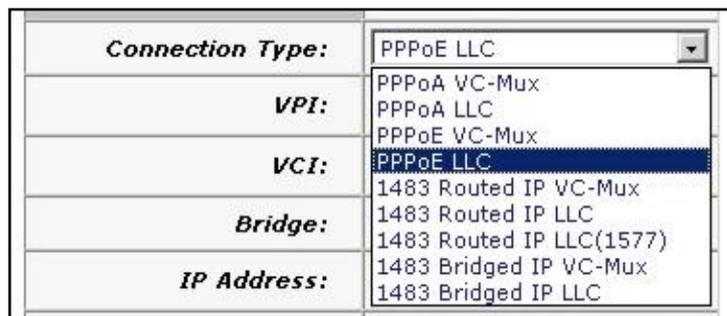
5. *VCI:* If instructed to change this, type in the VCI value for the initial connection (using PVC 0). Default = *35*.

6. *Bridge:* This may be left t the default setting *Disabled*. Some users may opt to enable this now by selecting *Enabled* from the drop-down menu.

7. *IP Address:* & *Subnet Mask:* Some users may be required to configure the IP settings for the WAN connection. If you are using IPoA or a Bridged IP connection, you may be instructed by your ISP to enter your global IP settings. If you are told to enter an IP Address and Subnet Mask, enter them here.

8. **DNS** Some users will be required to enter an IP address used for DNS services. If you are given a DNS server IP address enter that here along with a secondary or back-up DNS server IP address if you were given one.

9. For PPP connections (PPPoE or PPPoA), you must supply a **User Name** and **Password** used to verify the identity of your account.

10. If you entered a DNS server IP address (Step 9) leave this set to *Enable*. If you are not using DNS, select the *Disable* option.

11. When you have defined the Quick Configuration settings, click the **Submit** button to save the settings in temporary memory. These settings and all other configuration changes made to the Router must be Committed (to non-volatile memory) and the Router must be rebooted for the changes to go into effect. The Router will negotiate the ADSL connection automatically upon rebooting. Continue to the Commit & Reboot procedure.

Commit & Reboot

Commit and Reboot Menu

To save current configuration settings as they have been submitted click the Commit button. A message informs you when the settings have been successfully committed to memory. You must now reboot the device to put the

settings into effect. Make sure *Reboot* is selected in the **Reboot Mode:** pull-down menu and click **Reboot** .

After the Router has rebooted it will begin to negotiate the ADSL connection for your account. This will normally take a few seconds. When the ADSL connection has been successfully established, the ADSL Link LED indicator will light steady green. If the ADSL Link indicator does not light after a minute or so access the web configuration manager an double check the settings.

4

Web Configuration Management Guide

This chapter describes how to use the embedded web-based management software to configure the Router for additional PVC connection profiles, to change the LAN IP settings, to change the global WAN IP address and to perform other management functions.

Manager Interface Layout

The management software used for the Router initially presents the Home menu pictured below when you first log in. On the left side you see four folders, the hyperlinked Home folder contains the Quick Configuration menu. The LAN folder contains hyperlinked menus used for assigning LAN IP settings to the Router and IP services performed by the Router. The Bridging and Routing folders contain two of the same hyperlinked menus, the ATM VCC page and the EoA page. These are used to configure settings that allow the Router to operate on the service provider's network. If you are using the Router for multiple virtual connections, these menus are also used to configure these additional virtual connections (PVCs).
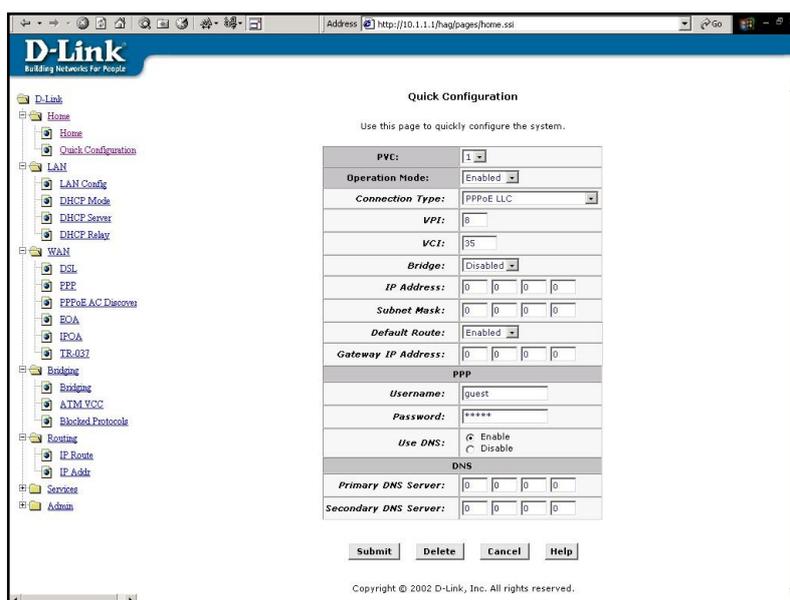
Router Web-based Quick Configuration Manager GUI

Commonly Used Buttons

The following buttons and icons are used throughout the web management application.

Submit	Stores in *temporary* system memory any changes you have made on the current page.
Refresh	Redisplays the current page with updated statistics or settings.
Clear	On pages that display accumulated statistics, this button resets the statistics to their initial values.
Help	Launches the online help for the current topic in a separate browser window. Help is available from the main topic pages.
(✏) pencil icon	The pencil icon links to another menu used to modify settings.
(🗑) trash icon	The trash can icon is used to delete a set of configuration values or parameters.
(🔍) view details icon	The view details icon allows you to view details about the configuration settings.

Quick Configuration

The Quick Configuration displays the settings you are most likely to need to change when you first set up the Router. These settings are explained briefly below:

ATM Interface	Select the ATM interface you want to use (use atm-0 for a single ATM interface). Your system may be configured with more than one ATM interface if you are using different types of services with your ISP. See ATM VC Configuration.
Operation Mode	This setting enables or disables the device's Internet and routing functions. When set to "No", the device cannot be used to provide Internet connectivity for your network.
Connection Type	This setting determines the type of data link used to communicate with your ISP. See ATM VC Configuration.
VPI and VCI	These settings determine the unique data path your modem uses to communicate with your ISP. See ATM VC Configuration.
Bridge	This setting enables or disables bridging between the device and your ISP. Your ISPs may also refer to this using "RFC 1483" or "Ethernet over ATM". See Bridging.
IP Address and Subnet Mask	If your ISP has assigned a public IP address to your LAN, enter the address and the associated subnet mask in the boxes provided. Check with your ISP to get this information. You may have to use the public IP address for your computer. In this case you do not enter the IP address here but configure these settings for your computer.
Default Route	When enabled, this setting specifies that the IP address specified above will be used as the default route for your LAN. Whenever, one of your LAN computers attempts to access the Internet, the data will be sent via the WAN interface.
Gateway IP Address	Specify the IP address that identifies the ISP server through which your Internet connection will be routed.
Username and Password	Enter the username and password you use to log in to your ISP. (Note: this is not the same as the user name and password you used to log in to Web Configuration Manager.)
Use DNS	Click *Enable* to turn on the DNS forwarding service, which forwards to your LAN PCs the Domain Name System server addresses that your PPP connection learns from your ISP. This option can only be used when the Router is configured to act as a DHCP server for your PCs. If you click *Disable*, you must configure DNS addresses manually on each PC or in the fields below.
Primary/Secondary DNS	Enter the Primary and Secondary DNS server addresses provided by your ISP.

Click the Submit button to save the settings in temporary memory. When you are done making changes to the configuration settings, open the **Commit & Reboot** menu and click the Commit button to save your changes to permanent memory.

You can click the Delete button to remove all existing Quick Configuration settings and return to the default values.

Home Page - System View

The System View read-only table on the Home Page displays a summary of various system settings and functions as described in the table below. Red colored text headings in this display are hyperlinked to a relavent menu.

Time information that appears in the System View menu can be changed in the Time & Date menu located in the Services folder.

Home Page – System View Display

Device	Displays the basic information about the device hardware and software versions, the system uptime, and the operating mode.
DSL	Displays the operational status and performance statistics for the DSL line.
WAN Interface	Displays the names and settings for the device WAN interfaces that communicate with your ISP via DSL, such as a PPP, EOA, or IPoA interface. Multiple software-defined interfaces may be configured to use the DSL connection. Click on the interface names to view the configuration menus for these interfaces. Each interface should display a lower interface name such as aal-5. Click on the lower interface name to view or change the ATM VC settings that this interface uses.
LAN Interface	Displays the software names and various settings for the device interfaces that communicate directly with your network. These typically include at least one Ethernet interface named *eth-0*. You can click on the interface names to display the LAN Configuration page.
Services Summary	Displays the following services that Router performs to help you manage your network: • NAT • IP Filter • RIP • DHCP status including DHCP Relay, DHCP Server or DHSCP Client.

Change LAN IP Settings

The LAN IP address identifies the LAN port (eth-0) as a node on your network; that is, its LAN IP address must be in the same subnet as the computers on your LAN.

You can change the default LAN IP address and Net Mask to suit the IP address arrangement you want to set up for your LAN. Click the LAN hyperlink view the LAN Configuration menu.

LAN Configuration

To change the Router Ethernet IP address, click the Refresh button and type in the new settings as described below.

System Mode	Read-only, lists the current mode of operation for the device.
Get LAN IP Address	Choose the source the Router uses to obtain its own IP settings for operation on the Ethernet LAN. By default the Router's IP settings are set to Manual.
	You may select External DHCP to use a DHCP server from outside the LAN. An external DHCP server will send DHCP settings through the WAN port. The external DHCP server may be part of the ISP's network.
	The remaining alternative, Internal DHCP Server is used to obtain IP settings from a DHCP server within the Ethernet LAN. The IP settings will sent through the LAN port.
LAN IP Address	The IP address your computers use to identify the device's LAN port.
	Note that the public IP address assigned to you by your ISP is not your LAN IP address. The public IP address identifies the WAN (ADSL) port on your Router to the Internet.
	Type in the IP address for the Ethernet LAN interface.
	Default = 10.1.1.1
LAN Network Mask	The LAN Network mask identifies which parts of the LAN IP Address refer to your network as a whole and which parts refer specifically to nodes on the network.
	Type in the Subnet Mask for the Ethernet LAN IP interface.
	Default = 255.0.0.0

Click the Submit button to save the settings in temporary memory. If you are changing the IP address you will need to login again to access the web manager. If you are getting IP settings from DHCP, the new IP settings will be applied after you submit, commit and reboot. You must Commit & Reboot the device to save your changes to permanent memory.

DHCP Service Modes

DHCP services can be employed in one of three different ways; it can provide DHCP services, it can receive DHCP services or it can relay DHCP service. By default the device is configured to act as a DHCP server on the Ethernet LAN. In this case it will supply IP settings to hosts that are configured to receive IP settings from a DHCP server.

The device may also be configured to relay IP settings from your ISP's DHCP server. In this case, you will want to configure the client hosts on your LAN to automatically obtain IP settings.

Finally the Router can perform no DHCP function at all. In this case, it will need to be either manually assigned IP settings or receive them from a DHCP server on your LAN or from the ISP (see previous section).

DHCP Mode Configuration

Choose one the options below from the **DHCP Mode:** drop-down menu.

DHCP Server	This is the default mode for the Router. In this mode it provides DHCP services to properly configured hosts on the Ethernet LAN.
DHCP Relay	In this mode the Router is an intermediary device or relay agent between a DHCP server owned by the ISP and host systems on your LAN.
None	In this mode the device does deliver or relay any DHCP services. If you choose this option and are operating in Router mode you will need to supply IP settings to the device manually (see previous section).

Click the Submit button to save the settings in temporary memory. When you are done making changes to the configuration settings, open the **Commit & Reboot** menu and click the Commit button to save your changes to permanent memory.

DHCP Server Configuration

The DSL-504G is configured by default to assign IP addresses for TCP/IP enabled devices your local Ethernet network. These devices must first be setup to receive this information from a DHCP server. A device that receives IP settings from a DHCP server is referred to as a DHCP client. The previous chapter describes how to configure IP settings on computers running a Windows operating system.

The DHCP Server Configuration menu displays the DHCP server pool or pools of IP addresses that have been configured for use.

Use this page if you are using the device as a DHCP server. This page lists the IP address pools available to computers on your LAN. The device distributes numbers in the pool to devices on your network as they request Internet access.

Start IP Address	End IP Address	Domain Name	Gateway Address	Status	Action(s)
10.1.1.3	10.1.1.34	-	0.0.0.0	Enabled	✎ 🗑 🔍

Add   Address Table   Refresh   Help

DHCP Server Configuration

When the Router functions as a DHCP server for your private LAN it uses a "pool" or group of IP addresses which are assigned to the DHCP clients on the LAN. By default, the Router uses a DHCP pool of 31 IP addresses in a range that are commonly used for private IP networks. These IP addresses are not in any way related to the global IP address that may be assigned to your DSL account since they are operating on a private network.

To delete an IP address pool, click the trashcan icon, then submit and commit your changes.

To view details on an IP address pool, click the magnifying glass icon. A page displays with all the same information that you entered when you added the pool.

To create a new pool of IP addresses used by the Router (DHCP server), click the Add button. A new window appears containing the following menu:

DHCP Server Pool Configuration

 Enter values for the Start IP Address, End IP Address, and Net Mask fields, which are required, and any others as needed:

Start/End IP Addresses	Specify the lowest and highest addresses in the pool, up to a maximum range of 254 addresses.
Mac Address:	(optional): Use this field only if you want to assign a specific IP address to a specific computer (that is, you are creating an exception to the dynamic assignment of addresses). The IP address you specify will be assigned to the computer that corresponds to this MAC address. (A MAC address is a manufacturer-assigned hardware ID that is unique for each device on a network.) If you type a MAC address here, you must have specified the same IP address in both the Start IP Address and End IP Address fields.
Net Mask:	Specifies which portion of each IP addresses in this range refers to the network and which portion refers to the host (computer). You can use the net mask to distinguish which pool of addresses should be distributed to a particular subset of computers on your LAN (call a *subnet*).
Domain Name:	(optional): A name that refers to the subnet that includes the addresses in this pool.
Gateway Address:	The address of the default gateway for computers that receive IP addresses from this pool. If no value is specified, then the appropriate LAN (eth-0) port address on the Router will be distributed to each computer as its gateway address, depending on how each is connected.
DNS/SDNS:	The IP address of the *Domain Name System* server to be used by computers that receive IP addresses from this pool. The DNS translates common Internet names that you type into your web browser into their equivalent numeric IP addresses. Typically, this server is located with your ISP.
WINS/SWINS:	(optional): The IP addresses of devices that perform various services for computers that receive IP addresses from this pool (such as WINS server which handles various network functions for Windows computers). Your ISP may provide some additional services using servers on their network. In this case the ISP will give you additional IP addresses to enter here.

Click the Submit button to save the DHCP pool. The new pool will be listed in the DHCP Server Configuration window.

> **Note**
>
> *To configure a computer running a Windows operating system to obtain IP settings from the Router (i.e. to be a DHCP client), read Configuring IP Settings on Your Computer in the previous chapter.*

Changing DHCP Address Pools

To modify an IP address pool click the pencil icon to display the DHCP Server Pool - Modify page. You can change the domain name associated with an IP address pool or enable/disable the pool. By default, a pool is enabled when you create it.

When you are done making modifications, and then click the Submit button. Use the **Commit & Reboot** menu to save your changes to permanent memory.

Excluding IP Addresses from a Pool

If you have IP addresses that are designated for fixed use with specific devices, or for some other reason you do not want to make them available to your network, you can exclude them from the pool.

On the DHCP Server Configuration Page, click the pencil con in the row corresponding to the pool you want to modify. On the DHCP Server Pool - Modify page, type each address to be excluded in the Excluded IP Field and click the Add button. When you are done specifying excluded addresses, click the Submit button, and then use the commit feature to save your changes to permanent memory.

Viewing Current IP Address Assignments

When the Router functions as a DHCP server for your LAN, it keeps a record of any addresses it has leased to your computers. To view a table of all current IP address assignments, display the DHCP Server Configuration page, and then click the Address Table button.

DHCP Server Address Table

IP Address	Netmask	Mac Address	Pool Start	Address Type	Time Remaining
10.1.1.5	255.0.0.0	00:07:0E:B3:8D:B2	10.1.1.3	Dynamic	2597657 Second(s)
10.1.1.6	255.0.0.0	00:40:05:BF:7B:DD	10.1.1.3	Dynamic	0 Second(s)
10.1.1.10	255.0.0.0	3A:E1:17:32:04:C0	10.1.1.3	Dynamic	6051 Second(s)
10.1.1.11	255.0.0.0	00:05:3C:06:A3:CB	10.1.1.3	Dynamic	2587307 Second(s)
10.1.1.12	255.0.0.0	00:80:45:11:51:F9	10.1.1.3	Dynamic	0 Second(s)
10.1.1.24	255.0.0.0	00:05:5D:76:5E:2C	10.1.1.3	Dynamic	0 Second(s)
10.1.1.25	255.0.0.0	76:5E:2C:32:04:C0	10.1.1.3	Dynamic	0 Second(s)
10.1.1.26	255.0.0.0	08:00:46:23:F3:2D	10.1.1.3	Dynamic	0 Second(s)
10.1.1.27	255.0.0.0	00:05:5D:F9:26:E5	10.1.1.3	Dynamic	0 Second(s)
10.1.1.28	255.0.0.0	00:50:BA:6B:34:76	10.1.1.3	Dynamic	0 Second(s)
10.1.1.29	255.0.0.0	00:02:A5:D1:00:36	10.1.1.3	Dynamic	1312 Second(s)
10.1.1.30	255.0.0.0	0C:43:CF:32:04:0A	10.1.1.3	Dynamic	0 Second(s)
10.1.1.31	255.0.0.0	00:40:05:C1:2C:68	10.1.1.3	Dynamic	0 Second(s)
10.1.1.32	255.0.0.0	00:E0:18:0E:CE:E0	10.1.1.3	Dynamic	0 Second(s)
10.1.1.33	255.0.0.0	C1:0B:44:32:04:C0	10.1.1.3	Dynamic	2395 Second(s)
10.1.1.34	255.0.0.0	00:50:BA:DA:02:51	10.1.1.3	Dynamic	931 Second(s)

Close   Refresh   Help

DHCP Server Address Table

The DHCP Server Address Table lists any IP addresses that are currently leased to LAN devices. For each leased address, the table lists the following information:

IP Address	The address that has been leased from the pool.
Netmask	The network mask associated with the leased address. This identifies the network ID and host ID portions of the address.
Mac Address	The hardware ID for the device to which the number has been assigned.
Pool Start	The lower boundary of the address pool (provided to identify the pool from which the leased number came).
Address Type	Static or Dynamic. *Static* indicates that the IP number has been assigned permanently to the specific hardware device. *Dynamic* indicates that the number has been leased temporarily for a specified length of time.
Time Remaining	The amount of time left for the device to use the assigned address. The default lease time is 30 days (315360000 seconds).

Configure DHCP Relay

The Router can be used to relay DHCP service to computers on your Ethernet LAN. This service is offered by some ISPs. To do this the Router must be configured to act as a DHCP relay agent (see DHCP Mode Configuration) and the computers on your network must be configured to be DHCP clients. The specific settings for the Router functioning in DHCP Relay Mode are configured in the DHCP Relay Configuration menu.

DHCP Relay Configuration

To configure the DHCP Relay settings:

1. Type the IP address of the ISP's DHCP server in the **DHCP Server Address** fields. If you do not have this number, it is not essential to enter it here. Requests for IP information from your LAN will be passed to the default gateway, which should route the request appropriately.

2. Select your WAN interface (ppp-0, eoa-0, or ipoa-0) from the drop-down list and click the Add button. Contact your ISP if you are unsure which type of WAN interface you use.

3. Click the Submit button. A page displays to confirm your changes, and then the program returns to the DHCP Relay Configuration page.

4. Click **DHCP Mode** in the task bar, then follow the instructions to enable DHCP relay.

WAN Configuration Options

If you are using the Router with two or more virtual connections (VC) one way to configure the additional connections is by using the WAN folder menus. You can use the ATM VC configuration menu to first create the additional VC. You may then need to create or modify a WAN interface using the PPP or IPoA configuration menus.

DSL Settings

You can view configuration parameters and performance statistics for the Router's DSL line by clicking the **DSL Status** hyperlink located in the WAN folder.

DSL Status Table

DSL Status

The DSL Status page displays current information on the DSL line performance. The page refreshes according to the setting in the Refresh drop-down list, which you can configure.

In the DSL Status table, the Operational Status setting displays a red, orange, or green ball to indicate that the DSL line is idle, starting up, or up-and-running, respectively. You can click the Loop Stop button to end the DSL connection. To restart the connection, you can click the Loop Start button that replaces the Stop button.

The statistics displayed in the DSL Status table are useful for troubleshooting connection problems. The data displayed here and in the sub-menus are read-only data.

- **DSL Parameters** From the DSL Status Page, you can click the DSL Parameters (DSL Param) button to display data about the configuration of the DSL line.

- **DSL Statistics** From the DSL Status page, you can click the Stats button to display DSL line performance statistics.

PPP Configuration

PPP is configured as a group of software settings associated with the ADSL port. Although the device has only one physical ADSL port, the Router can be defined with more than one group of PPP settings. Each group of settings is called a PPP interface and is given a name, such as *ppp-0*, *ppp-1*, etc.

Note	*If you are using AC Server Discovery to set up PPPoE service, do this first and then return to the PPP Configuration menu to continue setting up the PPP connection.*

The Router also supports a feature that automatically detects PPP service for connections using PPPoE. This auto-discovery feature is called **AC Server Discovery**. If your service provider supports automatic discovery for PPPoE service, read the next section for instruction on how to set up AC Server Discovery BEFORE using the PPP Configuration menu.

PPP Configuration

You can configure the following settings on the PPP Configuration page:

Inactivity TimeOut(mins): - The time in minutes that must elapse before a PPP connection times-out due to inactivity.

Ignore WAN to LAN traffic while monitoring activity: - When enabled, data traffic traveling in the incoming direction -- from the WAN port to the LAN port -- will not count as activity on the WAN port; i.e., it will not prevent the connection from being terminated if it has been otherwise inactive for the specified time.

To configure a new PPP interface click the Add button. A new menu appears.

PPP Interface - Add

The PPP Configuration table displays the following fields:

PPP Interface	The PPP interface you are configuring.
VC	The Virtual Circuit over which this PPP data is sent. The VC identifies the physical path the data takes to reach your ISP.
Interface Sec Type	The type of Firewall protections that are in effect on the interface. A *public* interface connects to the Internet (PPP interfaces are typically public). Packets received on a public interface are subject to the most restrictive set of firewall protections defined in the software. A *private* interface connects to your LAN, such as the Ethernet interface. Packets received on a private interface are subject to a less restrictive set of protections, because they originate within the network. The term *DMZ* (de-militarized zone), in Internet networking terms, refers to computers that are available for both public and in-network accesses (such as a company's public Web server).
Protocol	The type of PPP protocol used. Your ISP may use PPP-over-Ethernet (PPoE) or PPP-over-ATM (PPoA).
Service Name	This feature is available with PPoE interfaces but not with PPoA interfaces. The name of the ISP service you are using with this PPP connection. ISPs may offer different types of services (for example, for online gaming or business communications), each requiring a different login and other connection properties.
Use DHCP	When set to *Enable*, the device will acquire additional IP information from the ISP's DHCP server. The PPP connection itself acquires the device's IP address, mask, DNS address, and default gateway address.
Use DNS	When set to *Enable*, the DNS address learned through the PPP connection will be distributed to clients of the device's DHCP server. This option is useful only when the Router is configured to act as a DHCP Server for your LAN. When set to *Disable*, LAN hosts will use the DNS address(es) pre-configured in the DHCP pool.
Default Route	This indicates whether the Router should use the IP address assigned to this connection as its default route. It is Enabled by default and can be Disabled by selecting the appropriate option.
Security Protocol	Protocol used to confirm the identity of the subscriber.
Login Name	The name you use to log in to your ISP each time this PPP connection is established.
Login Password	The password you use to log in to your ISP each time this PPP connection is established.

When all PPP settings have been configured as desired, click the Submit button to save the settings temporarily. Continue to the Commit & Reboot menu and click the Commit button to save the setting to non-volatile memory.

AC Server Discovery

The AC Server Discovery feature can be used to automatically find available PPPoE servers and list them for user selection. Use this only if your service provider supports the feature and instructs you to use it. AC Server Discovery is not the same as the auto-configuration feature known as TR-037 described later in this guide.

AC Server Discovery

To initiate the server discovery click the Discovery button. It will take a few seconds for the Router to request and receive information from the available PPP servers on the network. A list of available PPPoE servers will appear listing the servers by AC Name and Service Name.

AC Server List

Select a server from the list and click the Submit button. A message should appear informing you that the connection to the AC server was successful and the web manager will return to the AC Server Discovery menu. If the connection fails, try it again. Successive failures to connect may indicate a problem with the server.

Return to the PPP Configuration menu and continue setting up the PPP connection. When all settings have been configured for PPP click the Submit button and continue to the Commit & Reboot menu. In the Commit & Reboot menu and click the Commit button to save the setting to non-volatile memory.

EOA Configuration

Ethernet-over-ATM (EOA) is a commonly used protocol for data transfer between Ethernet LANs and wide area networks that use the ATM protocol. Telecommunications industry networks often use the ATM in the within the their primary infrastructure or backbone. Network service providers that sell DSL services often use the EOA protocol for data transfer with their customers' DSL Routers.

EOA is implemented to create a bridged connection between a DSL Router and the ISP. In a bridged connection, data is shared between the ISP's network and their customer's as if the networks were on the same physical LAN. Bridged connections do not use the IP protocol. EOA can also be configured to provide a routed connection with the ISP, which uses the IP protocol to exchange data.

This section describes how to configure an Ethernet-over-ATM interface on the Router, if one is needed to communicate with your ISP.

Before creating an EOA interface or modifying the default settings, contact your ISP to determine which type of protocol they use.

⚠️ **IMPORTANT**	*Your ISP may use a protocol other than EOA for communication with the Router, such as the point-to-point protocol (PPP). One type of PPP, named PPP over Ethernet (PPPoE), actually works "on top" of the EOA protocol. The other type, PPP over ATM (PPPoA), does not. However, if your ISP uses either type of PPP, you **do not** need to separately create an EOA interface. If your service provider has given you PPP software for installation on your computer, follow the instructions given to you by your ISP and do not change the EOA settings.*

To view your current EOA configuration, log into the Configuration Manager, click the EoA button in the WAN folder, the EOA Configuration page appears:
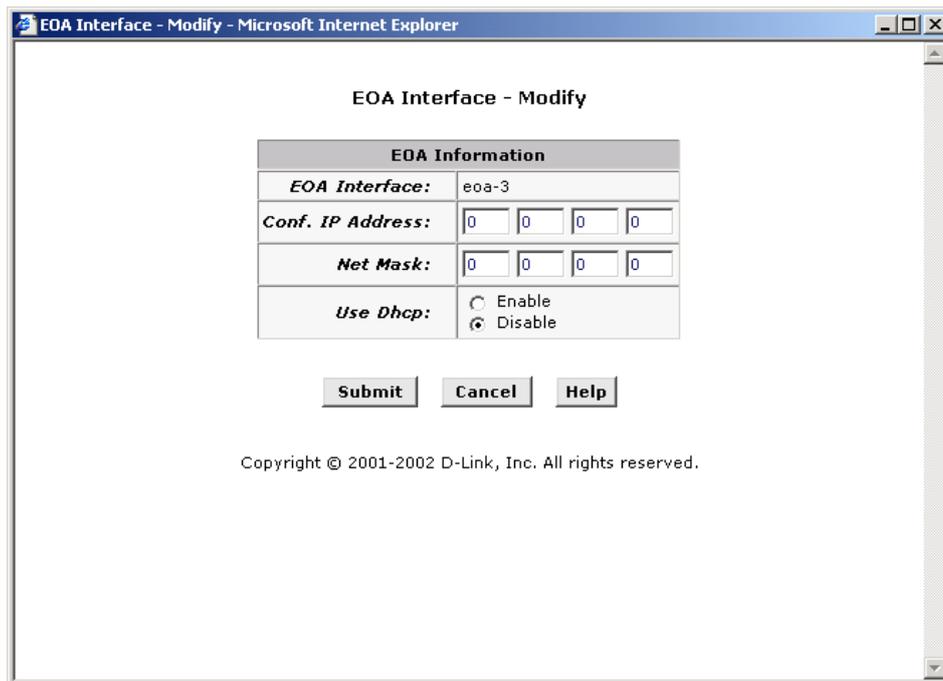

EOA Configuration

To define EOA settings for a new virtual connection, click the Add button.

EOA Interface – Modify

To Add or Modify AAL5 Parameters define the following:

EOA Interface	This is used (by the Router) to identify the EOA interface. If you are adding a new EOA interface, choose the EOA set you want to define from the pull-down menu (Add menu only).
Conf. IP Address:	The IP address assigned to the interface. If the interface will be used as a simple bridge to your ISP, then you do not need to specify IP information. If you enable DHCP for this interface, then the Configured IP address will serve only as a request to the DHCP server. The actual address that is assigned by the ISP may differ if this address is not available. Some ISPs use static IP settings that are manually assigned to each account. If your service provider instructs you to configure a Static IP Address, type in the global IP Address for this EOA interface.
Net Mask:	If you are assigned a Static IP Address and Net Mask, type in the Net Mask for this EOA interface.
Use DHCP:	When checked, this setting instructs the device to accept IP information assigned dynamically by your ISP's DHCP server. If the interface will be used for bridging with your ISP, leave this checkbox unselected. Select Enable or Disable for DHCP service.

Click the Submit button to save the settings in temporary memory. When you are done making changes to the configuration settings, open the **Commit & Reboot** menu and click the Commit button to save your changes to permanent memory.

IpoA Configuration

An IPoA interface can be used to exchange IP packets over the ATM network, without using an underlying Ethernet over ATM (EOA) connection. Typically, this type of interface is used only in product development environments, to eliminate unneeded variables when testing IP layer processing.

The IPoA table contains a row for each EOA interface currently defined on the device. The table may initially contain no entries.

IP over ATM (IPoA) Configuration

This Page is used to View, Add and Delete IPoA Interfaces.

| Interface	Interface Sec Type	RFC 1577	Lower Interface	Peer IP Address	Confg IP Address	Netmask	Gateway Address	Status	Action
No IPoA Interface!									

Add   Map   Refresh   Help

IPoA Configuration

The IPoA Configuration table displays the following fields:

IPoA Interface	The IPoA interface you are configuring.
Conf. IP Address	The IP address you want to assign to the interface.
Interface Sec Type	The type of Firewall protections that are in effect on the interface. A *public* interface connects to the Internet (PPP interfaces are typically public). Packets received on a public interface are subject to the most restrictive set of firewall protections defined in the software. A *private* interface connects to your LAN, such as the Ethernet interface. Packets received on a private interface are subject to a less restrictive set of protections, because they originate within the network. The term *DMZ* (de-militarized zone), in Internet networking terms, refers to computers that are available for both public and in-network accesses (such as a company's public Web server).
Netmask	The netmask you want to assign to the interface.
RFC 1577	Specifies whether the IPoA protocol to be used complies with the IEFT specification named "RFC 1577 - Classical IP and ARP over ATM" (contact your ISP if unsure).
Lower Interface	IPoA interfaces are defined in software, and then associated with lower-level software and hardware structures (at the lowest level, they are associated with a physical port - the WAN port). This field should reflect an interface name defined in the next lower level of software over which the IPoA interface will operate. This will be an ATM VC interface, such as aal5-0, as described in Configuring the ATM VC.
Peer IP Address	The IP address of the remote computer you will be connecting to via the WAN interface.
Default Route	This indicates whether the Router should use the IP address assigned to this connection as its default route. It is Enabled by default and can be Disabled by selecting the appropriate option.
Gateway IP Address	The external IP address that the Router communicates with via the IPoA interface to gain access to the Internet. This is typically an ISP server.

To configure a new IPoA interface click the Add button. A new menu appears. The Add and Modify menus for IPoA configuration require the same information.

Enter information needed for the IPoA connection follwing the steps below.
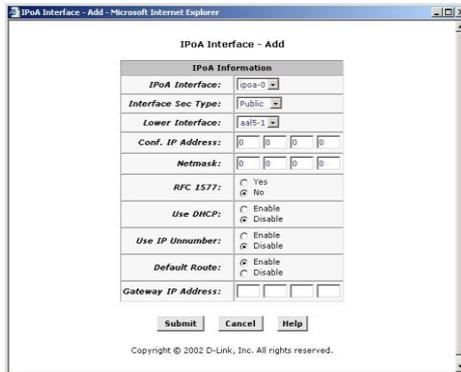
Add IPoA Interface

Follow these instructions to add an IPoA interface:

1. Select the next available interface name from the IPoA Interface drop-down list.

2. From the Interface Sec Type drop-down list, select the level of firewall security for the interface: Public, Private, or DMZ.

3. Select the Lower Interface: as instructed aal5-0, aal5-1 etc. from the pull-down menu.

4. In the Configured IP Address and Net Mask boxes, type the address and mask that you want to assign to the IPoA interface.

5. In the RFC 1577 Click the Yes radio button if the interface complies with the IETF specification RFC 1577.

6. If your IPoA interface is using DHCP enable this in the Use DHCP: menu.

7. If your IPoA interface is an IP Unnumbered IPoA interface, enable this with the Use IP Unnumbered: option. This will automatically remove the Use DHCP: option.

8. Click the Submit button. A confirmation page will display to confirm your changes.

9. Click the Close to return to the IPoA page and view the new interface in the table.

10. Display the Admin tab, and click **Commit & Reboot** in the task bar.

11. Click the Commit button to save your changes to permanent memory.

Configure TR-037

Some ISPs support an auto-configuration technical specification known as TR-037. This is intended to greatly simplify establishing and maintaining the WAN connection for DSL devices. Ask your ISP details on using TR-037 Auto-Configuration. This is disabled by default on the Router.
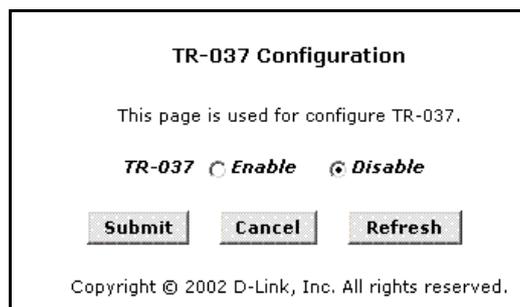
Enable/Disable TR-037 Auto-Configuration

Bridge Configuration

The Router can be configured to act as a bridging device between your LAN and your ISP. Bridges are devices that enable two or more networks to communicate as if they are two segments of the same physical LAN. This section describes how to configure the Router to operate as a bridge.

⚠️ **IMPORTANT**	*Before changing the bridge configuration, check with your ISP to determine the type of connection used to exchange data with their client's DSL Routers (such as Ethernet bridging).*

A bridge is a device used to connect two or more networks. A bridge device is able to learn the unique manufacturer-assigned hardware identifier (MAC Address) of each computer or device on either or both networks to which it is connected. It learns that some of the MAC addresses represent computers attached via one of the device's interfaces and other MACs represent computers connected via other interfaces. For example, the MAC addresses of your home computers are learned through (or associated with) the Ethernet port, and the MACs of your ISP's computers are attached via the WAN (DSL) port. It stores the MAC addresses and the interface associated with each MAC in its *bridge forwarding table*.

When the bridge receives a data packet, it compares its destination MAC to the entries in the bridge forwarding table. When the packet's destination MAC address matches one of the entries, it forwards the packet through the interface that connects to the corresponding network. The bridge does not send the data directly to the receiving computer, but broadcasts it to the receiving network, making it available to any node on that network. On the receiving network, the packet is delivered in a form recognized by the network protocol (Ethernet for the LAN side of the Router) and delivered to its destination.

When the bridge does not recognize a packet's destination MAC address, it broadcasts the packet through all of its interfaces – to both networks.

You may need to use the device as a bridge if:

- Your ISP uses protocols that require bridging with your LAN. The device can be configured to appear as a bridge when communicating with your ISP, while continuing to provide router functionality for your LAN.
- Your LAN may include computers that communicate using "layer-3" protocols other than the Internet Protocol. These include IPX® and AppleTalk®. In this case, the device can be configured to act as a bridge for packets that use these protocols while continuing to serve as a router for IP data.

To add or change bridge configuration settings, log into the Configuration Manager and click on the Bridging button in the Bridging folder.

Bridge Configuration Menu

To define Bridge settings for an existing virtual connection, click the Add button for the interface you wish to configure. When you choose to add a new set or modify an existing set, a new menu appears (see below). To delete an existing setting, click the trashcan (🗑) for that set.

Click the Submit button to save the settings in temporary memory. When you are done making changes to the configuration settings, open the **Commit & Reboot** menu and click the Commit button to save your changes to permanent memory.

> *If you enable bridging on an interface that has already been assigned an IP address, then it is considered IP-enabled and will route (rather than bridge) IP packets received on the interface. The interface will bridge non-IP data it receives, however.*
>
> **Note**
>
> *You can determine whether the Ethernet (eth-0 interface has been assigned an IP address by displaying the IP Address Table (display the **Routing** tab, then click **IP Addr**). These interfaces will display in the table only if they have been assigned IP addresses.*
>
> *You can check whether the eoa-0 interface has been assigned an IP address by displaying the EOA configuration table (display the **WAN** tab, and then click **EOA**). If the Config IP Address field is empty and the Use DHCP field contains the word Disable, then no IP address has been assigned.*

ATM VCC Configuration

When computers access the Internet using the Router, data is exchanged with your network service provider or ISP through a complex network of telephone switches, Internet routers, servers, and other specialized hardware. These various devices communicate using a common language, or protocol, called *Asynchronous Transfer Mode* (ATM). On the Wide Area Network (WAN) that connects you to your ISP, the ATM protocol performs functions like those that the Ethernet protocol performs on your LAN.

This section describes how to configure the ATM *virtual channel connection* (VCC). The VCC properties define the path the Router uses to communicate with your ISP over the ATM network.

To view your current configuration, log into the Configuration Manager, and then click the ATM VCC button in the Bridging folder. The ATM VCC Configuration page displays, as shown below:

ATM VCC Configuration Menu

Additional Virtual Connections

In order to use more than one PVC setting, it will be necessary to define one or two set of parameters for each virtual connection. First use the ATM VC Configuration menu to define new AAL5 settings. All additional PVCs must be added using the ATM VC menu. For connections that do not use PPPoE or PPPoA, it will also be necessary to use the EOA Configuration menu to establish Ethernet over ATM settings for the PVC adding in the ATM VC menu.

To define AAL5 settings for a new virtual connection, click the Add button. To modify an existing AAL5 setting, click the pencil icon (✏) for that set. When you choose to add a new set or modify an existing set, a new menu appears (see below). To delete an existing AAL5 setting, click the trashcan (🗑) for that set.
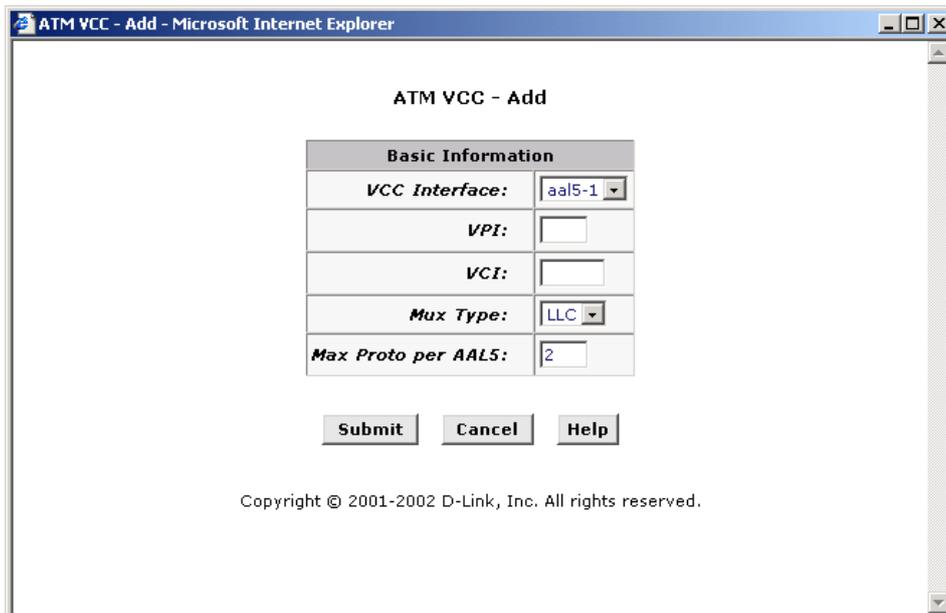
ATM VCC – Add (or Modify) Parameters

To Add or Modify AAL5 Parameters define the following:

VCC Interface	The name of the lower-level interface on which this VC operates. The low-level interface names are pre-configured in the software and identify the type of traffic that can be supported, such as data or voice. Internet data services typically use an AAL5-type interface.
	If you are adding a new VCC Interface, choose the AAL5 set you want to define from the pull-down menu (Add menu only).
VPI	This setting (together with the VCI and Mux Type) identifies a unique ATM data path for communication between the Router and service provider.
	If you are adding a new VCC Interface or changing the existing VPI value, type in the new VPI value.
VCI	If you are adding a new VCC Interface or changing the existing VCI value, type in the new VCI value.
Mux Type	Select VC-Mux or LLC from pull-down menu.
MAX Proto per AAL5	This setting indicates the number of higher-level interfaces that the VC can support (the higher level interfaces can be PPP, EoA, or IPoA interfaces). The Router supports up to eight however you must make arrangements your service provider for this additional service.

Click the Submit button to save the settings in temporary memory. When you are done making changes to the configuration settings, open the **Commit & Reboot** menu and click the Commit button to save your changes to permanent memory

Blocked Protocols

The Router is capable of sending and receiving information in a variety of protocol formats. The Blocked Protocols feature enables you to prevent the Router from passing any data that uses a particular protocol. Unlike the IP Filter feature, you cannot specify additional criteria for blocked protocols, such as particular users or destinations. However, when you are certain that a particular protocol is not needed or wanted on your network, this feature provides a convenient way to discard such data before it is passed.

Blocked Protocols

The following list describes each of the listed protocols.

- **PPPoE:** Point to Point Protocol over Ethernet. Many DSL modems use PPoE to establish and maintain a connection with a service provider. PPoE provides a means of logging in to the ISPs servers so that they can authenticate you as a customer and provide you access to the Internet. Check with your ISP before blocking this protocol.

- **IP Multicast:** IP Multicast is an extension to the IP protocol. It enables individual packets to be sent to multiple hosts on the Internet, and is often used for handling e-mail mailing lists and teleconferencing/videoconferencing.

- **RARP:** Reverse Address Resolution Protocol. This IP protocol provides a way for computers to determine their own IP addresses when they only know their hardware address (i.e., MAC addresses). Certain types of computers, such as diskless workstations, must use RARP to determine their IP address before communicating with other network devices.

- **AppleTalk®:** A networking protocol used in for Apple Macintosh® networks.

- **NetBEUI:** NetBIOS Enhanced User Interface. On many LAN operating systems, the NetBEUI protocol provides the method by which computers identify themselves to and communicate with each other.

- **IPX:** Internetwork Packet Exchange. A networking protocol used on Novell Netware ®-based LANs.

- **BPDU:** Bridge Protocol Data Unit. BPDUs are data messages that are exchanged across the switches between LANs that are connected by a bridge. BPDU packets contain information on ports, addresses, priorities and costs, and are exchanged across bridges to detect and eliminate loops in a network.

- **ARP:** Address Resolution Protocol. Computers on a LAN use ARP to learn the hardware addresses (i.e., MAC addresses) of other computers when they know only their IP addresses.

- **IPV6 Multicast:** IP Multicasting under IP Protocol version 6. See *IP Multicast* above.

- **802.1.Q:** This IEEE specification defines a protocol for virtual LANs on Ethernet networks. A virtual LAN is a group of PCs that function as a local area network, even though the PCs may not be physically connected. They are commonly used to facilitate administration of large networks.

To block a protocol, click the appropriate check box, and click the Submit button to save the settings in temporary memory. When you are done making changes to the configuration settings, open the **Commit & Reboot** menu and click the Commit button to save your changes to permanent memory.

Routing Configuration

Links to the IP Route and IP Address tables are found within the Routing folder. The remaining links are duplicate links to menus that have been previously described.

IP Route

IP Routes are used to define gateways and hops used to route data traffic. Most users will not need to use this feature as the previously configured default gateway and LAN IP settings on your host computers should be sufficient.

You may need to define routes if your LAN includes two or more networks or subnets, if you connect to two or more ISP services, or if you connect to a remote corporate LAN. Use the IP Route Table to Add new IP routes. The new IP routes are in effect additional rules used by the Router for routing data. See the next section, Adding IP Routes for instructions.

IP Route Table

Information displayed in the IP Route Table is summarized below:

Destination	Specifies the IP address of the destination computer. The destination can specified as the IP address of a specific computer or an entire network. It can also be specified as all zeros to indicate that this route should be used for all destinations for which no other route is defined (this is the route that creates the default gateway).
Netmask	Indicates which parts of the destination address refer to the network and which parts refer to a computer on the network. The default gateway uses a netmask of 0.0.0.0.
Next Hop	Specifies the *next* IP address to send data to when its final destination is that shown in the destination column.
IF Name	Displays the name of the interface through which to data is forwarded to the specified next hop.
Route Type	Displays whether the route is direct or indirect. In a direct route, the source and destination computers are on the same network, and the router attempts to directly deliver the data to the computer. In an indirect route, the source and destination computers are on different networks, and the router forwards data to a device on another network for further handling.
Route Origin	Displays how the route was defined. *Dynamic* indicates that the route was predefined on the system by your ISP or the manufacturer. Routes you create are labeled *Local*. Other routes can be created automatically, or defined remotely through various network management protocols (LCL or ICMP).

Adding IP Routes

To add an IP route to the device's routing table, follow these steps:

1. Click the Add button to display the IP Route – Add menu.
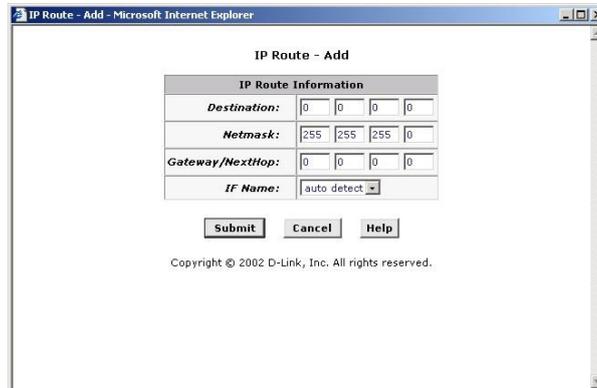
Add IP Route

2. Type in the destination, network mask, and gateway or next hop for this route.

    To create a route that defines the device's default gateway, enter 0.0.0.0 in both the Destination and Net Mask fields. Enter your ISP's IP address in the Gateway/NextHop field.

3. It may be necessary under certain circumstances to force the interface choice for the IP route. This can be done using the IF Name: pull-down menu. Select an existing or previously created interface to force the IP route through that interface.

4. Click the Submit button. A page will display to confirm your changes.

5. Click the Close button to return to the IP Route table page. The new route should display in the table.

6. Display the Admin tab, and click **Commit & Reboot** in the task bar.

7. Click Commit button to save your changes to permanent memory.

IP Address

The IP Address Table lists the IP addresses, network masks ("Net Mask"), and interface names ("IF Name") for each of its IP-enabled interfaces.

IP Address Table

The listed IP addresses include:

The IP address of the device's Ethernet LAN port (*eth-0).*

The IP address of the WAN interface (*ppp-0, eoa-0*, or *ipoa-0* depending on the connection protocol). This is the address that your ISP and other external devices use to identify your network. Your ISP may assign the same address each time, or it may change each time you reconnect.

The "loopback" IP address, named *lo-0*, of 127.0.0.1. This is a special address that enables the device to keep any data addressed directly to it, rather than route the data through the WAN or LAN ports.

If your device has additional interfaces, the IP addresses of these will also display.

NAT

Network Address Translation is a method for disguising the private IP addresses you use on your LAN as the public IP address you use on the Internet. You define NAT rules that specify exactly how and when to translate between public and private IP addresses.

NAT is enabled by default. You can enable or disable NAT by selecting the *Enable* or *Disable* option in the configuration menu and submitting the settings.

NAT Configuration

To view the NAT Rule setting menu or the NAT Translations entries, select the option from the **NAT Options:** drop-down menu. To configure NAT Rules, select the *NAT Rule Entry* option and click the Add button. A new window is displayed:

Add NAT Rule

From the **Rule Flavor** drop-down list, select *Basic, Filter, NAPT, BIMAP, RDR* or *PASS*. The page redisplays with only the fields that are appropriate for the chosen NAT flavor.

Enter information appropriate to the NAT flavor. The information in the various menus is summarized in the table below.

Rule ID	The Rule ID determines the order in which rules are invoked (the lowest numbered rule is invoked first, and so on). In some cases, two or more rules may be defined to act on the same set of IP addresses. Be sure to assign the Rule ID so that the higher priority rules are invoked before lower-priority rules. It is recommended that you select rule IDs as multiples of 5 or 10 so that, in the future, you can insert a rule between two existing rules. Once a data packet matches a rule, the data is acted upon according to that rule and is not subjected to higher-numbered rules.
IF Name	Typically, NAT rules are used for communication between your LAN and the Internet. Because the device uses the WAN interface (which may be named *ppp-0*, *eoa-0*, or *ipoa-0*) to connect your LAN to your ISP, it is the usual IF Name selection.
Protocol	This selection specifies which type of Internet communication will be subject to this translation rule. You can select ALL if the rule applies to all data. Or, select TCP, UDP, ICMP, or a number from 1-255 that represents the IANA-specified protocol number.
Local Address From	Type the starting IP of the range of private address you want to be translated. You can specify that data from all LAN addresses should be translated by typing 0 (zero) in each From field and 255 in each To field. Or, type the same address in both fields if the rule only applies to one LAN computer.
Local Address To	Type the ending IP of the range of private address you want to be translated.
Global Address From	Type the public IP address assigned to you by your ISP.
Global Address To	If you have multiple WAN interfaces, in both the Global Address From and Global Address To fields, type the IP address of the interface to which this rule applies. This rule will not be enforced for data that arrives on other PPP interfaces. If you have multiple WAN interfaces and want the rule to be enforced on a range of them, type the starting and ending IP addresses of the range. You can specify a single value by entering that value in both the From and To fields.
Destination Address (or addresses)*	Specify a range of destination addresses if you want this rule to apply only to outbound traffic to addresses in that range. If you enter only the network ID portion of the destination address, then the rule will apply to outbound traffic to all computers on network. You can specify a single value by entering that value in both the From and To fields.
Destination Port (or ports)*	In the Destination Port From and Destination Port To fields, enter the port ID (or a range) that you expect to see on incoming packets destined for the LAN computer for which this rule is being created. Incoming traffic that meets this criteria will be redirected to the Local Port number you specify in the next field. For example, if you grant public access to a Web server on your LAN, you would expect that incoming packets destined for that computer would contain the well-known web server port number, 80. This setting serves as a filter; data packets not containing this port number would not be granted access to you local computer.
Local Port	If the LAN computer that you are making publicly available is configured to use a non-standard port number for the type of traffic it receives, type the non-standard port number in the Local Port field. This option translates the standard port number in packets destined for your LAN computer to the non-standard number you specify. For example, if your Web server uses (non-standard) port 2000, but you expect incoming data packets to refer to (standard) port 80, you would enter 2000 here and 80 in the Destination Port fields. The headers of incoming packets destined for port 80 will be modified to refer to port 2000. The packet can then be routed appropriately to the web server.

∗ Specify both a destination address (or range) and a destination port (or range) if you want this translation rule to apply to accesses to the specified server type at the specified IP address or network.

RIP

RIP is an Internet protocol you can set up to share routing table information with other routing devices on your LAN, at your ISP's location, or on remote networks connected to your network via the ADSL line.

RIP Configuration

Most small home or office networks do not need to use RIP; they have only one router and one path to an ISP. In these cases, there is no need to share routes, because all routes from the network go to the same ISP gateway.

You may want to configure RIP if any of the following circumstances apply to your network:

- Your home network setup includes an additional router or RIP-enabled PC. The DSL-500G and your second router will need to communicate via RIP to share their routing tables.

- Your network connects via the ADSL line to a remote network, such as a corporate network. In order for the networks at the two sites to share the routes used internally within each LAN, they should *both* be configured with RIP.

- Your ISP requests that you run RIP for communication with devices on their network.

To change RIP configuration:

1. If necessary, change the Age and Update Time. These are global settings for all interfaces that use RIP.

   Age is the amount of time in seconds that the device's RIP table will retain each route that it learns from adjacent computers.

   Update Time specifies how frequently the Router will send out its routing table its neighbors.

2. In the **IF Name** column, select the name of the interface on which you want to enable RIP.

   For communication with RIP-enabled devices on your LAN, select eth-0 or the name of the appropriate virtual Ethernet interface.

   For communication with your ISP or a remote LAN, select the corresponding ppp, eoa, or other WAN interface.

3. Select a metric value for the interface.

4. RIP uses a "hop count" as a way to determine the best path to a given destination in the network. The hop count is the sum of the metric values assigned to each port through which data is passed before reaching the destination. Among several alternative routes, the one with the lowest hop count is considered the fastest path.

For example, if you assign this port a metric of 1, then RIP will add 1 to the hop count when calculating a route that passes through this port. If you know that communication via this interface is slower than through other interfaces on your network, you can assign it a higher metric value than the others. You can select any integer from 1 to 15.

5.   Select a Send Mode and a Receive Mode.

The Send Mode setting indicates the RIP version this interface will use when it sends its route information to other devices.

The Receive Mode setting indicates the RIP version(s) in which information must be passed to the Router in order for it to be accepted into its routing table.

RIP version 1 is the original RIP protocol. Select RIP1 if you have devices that communicate with this interface that understand RIP version 1 only.

RIP version 2 is the preferred selection because it supports "classless" IP addresses (which are used to create subnets) and other features. Select RIP2 if all other routing devices on your LAN support this version of the protocol.

6.   Click the Add button. The new RIP entry will display in the table.

7.   Click the **Enable** radio button to enable the RIP feature.

8.   Click the Submit button to save the settings in temporary memory. When you are done making changes to the configuration settings, open the **Commit & Reboot** menu and click the Commit button to save your changes to permanent memory.

Firewall

The Firewall enables you to protect the system against denial of service (DoS) attacks and other types of malicious accesses to your LAN. You can also specify how to monitor attempted attacks, and who should be automatically notified.

Firewall Configuration

Follow these instructions to configure global firewall settings:

Configure any of the following settings that display in the Firewall Global Information table:

- **Black List Status:** If you want the device to maintain and use a black list, click *Enable*. Click *Disable* if you do not want to maintain a list.
- **Black List Period(min)**: Specifies the number of minutes that a computer's IP address will remain on the black list (i.e., all traffic originating from that computer will be blocked from passing through any interface on the Router). For more information, see Managing the Black List below.
- **Attack Protection**: Click the *Enable* radio button to use the built-in firewall protections that prevent the following common types of attacks:

  IP Spoofing: Sending packets over the WAN interface using an internal LAN IP address as the source address.

  Tear Drop: Sending packets that contain overlapping fragments.

  Smurf and Fraggle: Sending packets that use the WAN or LAN IP broadcast address as the source address.

  Land Attack: Sending packets that use the same address as the source and destination address.

  Ping of Death: Illegal IP packet length.

- **DoS Protection**: Click the Enable radio button to use the following denial of service protections:

  SYN DoS

  ICMP DoS

  Per-host DoS protection

- **Max Half open TCP Connection**: Sets the percentage of concurrent IP sessions that can be in the half-open state. In ordinary TCP communication, packets are in the half-open state only briefly as a connection is being initiated; the state changes to active when packets are being exchanged, or closed when the exchange is complete. TCP connections in the half-open state can use up the available IP sessions. If the percentage is exceeded, then the half-open sessions will be closed and replaced with new sessions as they are initiated.

- **Max ICMP Connection**: Sets the percentage of concurrent IP sessions that can be used for ICMP messages. If the percentage is exceeded, then older ICMP IP sessions will be replaced by new sessions as the are initiated.

- **Max Single Host Connection**: Sets the percentage of concurrent IP session that can originate from a single computer. This percentage should take into account the number of hosts on the LAN.

- **Log Destination**: Specifies how attempted violations of the firewall settings will be tracked. Records of such events can be sent via Ethernet to be handled by a system utility Ethernet to (*Trace*) or can e-mailed to specified administrators.

- **E-mail ID of Admin 1/2/3**: Specifies the e-mail addresses of the administrators who should receive notices of any attempted firewall violations. Type the addresses in standard internet e-mail address format. The e-mail message will contain the time of the violation, the source address of the computer responsible for the violation, the destination IP address, the protocol being used, the source and destination ports, and the number violations occurring the the previous 30 minutes. If the ICMP protocol were being used, then instead of the source and destination ports, the e-mail will report the ICMP code and type.

Click the Submit button to save the settings in temporary memory. When you are done making changes to the configuration settings, open the **Commit & Reboot** menu and click the Commit button to save your changes to permanent memory.

Managing the Black List

If data packets are received that violate the firewall settings or any of the IP Filter rules, then the source IP address of the offending packets can be blocked from such accesses for a specified period of time. You can enable or disable use of the black list using the settings described above. The source computer remains on the black list for the period of time that you specify.

To view the list of currently blacklisted computers, click the Black List button at the bottom of the Firewall Configuration page. The table displays the following information for each entry:

- **Host IP Address**: The IP address of the computer that sent the packet(s) that caused the violation

- **Reason**: A short description of the type of violation. If the packet violated an IP Filter rule, the custom text from the Log Tag field will display.

- **IPF Rule ID**: If the packet violated an IP Filter rule, this field will display the ID assigned to the rule.

The IP filter feature enables you to create rules that control the forwarding of incoming and outgoing data between your LAN and the Internet and within your LAN. This topic explains how to create IP filter rules.

IP Filter

The IP Filter Configuration page displays global settings that you can modify, and the IP Filter rule table, which shows all currently established rules.

IP Filter Configuration

The IP Filter Configuration page enables you to configure the following IP filter global settings.

- **Security Level:** This setting determines which IP Filter rules take effect, based on the security level specified in each rule. For example, when *High* is selected, only those rules that are assigned a security value of *High* will be in effect. The same is true for the *Medium* and *Low* settings. When *None* is selected, IP Filtering is disabled.

- **Private/Public/DMZ Default Action:** This setting specifies a default action to be taken (Accept or Deny) on private, public, or DMZ-type device interfaces when they receive packets that *do not* match any of the filtering rules. You can specify a different default action for each interface type. (You specify an interface's type when you create the interface; see the PPP configuration page, for example.)

  - A *public* interface typically connects to the Internet. PPP, EoA, and IPoA interfaces are typically public. Packets received on a public interface are subject to the most restrictive set of firewall protections defined in the software. Typically, the global setting for public interfaces is *Deny*, so that all accesses to your LAN initiated from external computers are denied (discarded at the public interface), except for those allowed by a specific IP Filter rule.

  - A *private* interface connects to your LAN, such as the Ethernet interface. Packets received on a private interface are subject to a less restrictive set of protections, because they originate within the network. Typically, the global setting for private interfaces is *Accept*, so that LAN computers have access to the Routers' Internet connection.

The term *DMZ* (de-militarized zone), in Internet networking terms, refers to computers that are available for both public and in-network accesses (such as a company's public Web server). Packets received on a DMZ interface -- whether from a LAN or external source -- are subject to a set of protections that is in between public and private

interfaces in terms of restrictiveness. The global setting for DMZ-type interfaces may be set to *Deny* so that all attempts to access these servers are denied by default; the administrator may then configure IP Filter rules to allow accesses of certain types.

Adding an IP Filter Rule

To create an IP filter rule, you set various criteria that must be met in order for the rule to be invoked. Use these instructions to add a new IP filter rule:

1. On the main IP Filter page, click the Add button to display the IP Filter Rule - Add page.

IP Filter Rule - Add

2. Enter or select data for each field that applies to your rule. The following table describes the fields:

▪ **Rule ID**: Each rule must be assigned a sequential ID number. Rules are processed from lowest to highest on each data packet, until a match is found. It is recommended that you assign rule IDs in multiples of 5 or 10 (e.g., 10, 20, 30) so that you leave enough room between them for inserting a new rule if necessary.

▪ **Action**: Specifies what the rule will do to a packet when the packet matches the rule criteria. The action can be *Accept* (forward to destination) or *Deny* (discard the packet).

▪ **Direction**: Specifies whether the rule should apply to data packets that are incoming or outgoing on the selected interface. *Incoming* refers to packets coming in to the LAN on the interface, and *Outgoing* refers to packets going out from the LAN. You can use rules that specify the incoming direction to restrict external computers from accessing your LAN.

▪ **Interface**: The interface on the device on which the rule will take effect.

▪ **In Interface**: The interface from which packets must have been forwarded to the interface specified in the previous selection. This option is valid only on rules defined for the outgoing direction.

▪ **Log Option**: When *Enabled* is selected, a log entry will be created on the system each time this rule is invoked. The log entry will include the time of the violation, the source address of the computer responsible for the violation, the destination IP address, the protocol being used, the source and

destination ports, and the number violations occuring the the previous x minutes. (Logging may be helpful when troubleshooting.) This information can also be e-mailed to administrators.

▪ **Security Level:** The security level that must be enabled globally for this rule to take affect. A rule will be active only if its security level is the same as the globally configured setting (shown on the main IP Filter page). For example, if the rule is set to *Medium* and the global firewall level is set to *Medium*, then the rule will be active; but if the global firewall level is set to *High* or *Low*, then the rule will be inactive.

▪ **Black List Status**: Specifies whether or not a violation of this rule will result in the offending computer's IP address being added to the Black List, which blocks the Router from forwarding packets from that source for a specified period of time.

▪ **Log Tag:** A description of up to 16 characters to be recorded in the log in the event that a packet violates this rule. Be sure to set the Log Option to *Enable* if you configure a Log Tag.

▪ **Start/End Time:** The time range during which this rule is to be in effect, specified in military units.

▪ **Src IP Address**: IP address criteria for the source computer(s) from which the packet originates. In the drop-down list, you can configure the rule to be invoked on packets containing:

- **any**: any source IP address.
- **lt**: any source IP address that is numerically less than the specified address.
- **lteq**: any source IP address that is numerically less than or equal to the specified address.
- **gt**: any source IP address that is numerically greater than the specified address.
- **eq**: any source IP address that is numerically equal to the specified address.
- **neq**: any source IP address that is not equal to the specified address.
- **range**: any source IP address that is within the specified range, inclusive.
- **out of range**: any source IP address that is outside the specified range.
- **self**: the IP address of the Router interface on which this rule takes effect.

▪ **Dest IP Address**: IP address rule criteria for the destination computer(s) (i.e., the IP address of the computer to which the packet is being sent). In addition to the options described for the Src IP Address field, the following option is available:

- **bcast**: specifies that the rule will be invoked for any packets sent to the broadcast address for the receiving interface. (The broadcast address is used to send packets to all hosts on the LAN or subnet connected to the specified interface.) When you select this option, you do not need to specify the address, so the address fields are dimmed.

▪ **Protocol**: IP protocol criteria that must be met for rule to be invoked. You can specify that packets must contain the selected protocol (*eq*), that they must not contain the specified protocol (*neq*), or that the rule can be invoked regardless of the protocol (*any*). TCP, UDP, and ICMP are commonly used IP protocols; others can be identified by number, from 0-255, as defined by the Internet Assigned Numbers Authority (IANA).

▪ **Store State**: If this option is enabled, then *stateful filtering* is performed and the rule is also applied in the other direction on the given interface during an IP session.

▪ **Source Port**: Port number criteria for the computer(s) from which the packet originates. This field will be dimmed (unavailable for entry) unless you have selected TCP or UDP as the protocol. See the description of Src IP Address for the selection options.

▪ **Dest Port**: Port number criteria for the destination computer(s) (i.e., the port number of the type of computer to which the packet is being sent). This field will be dimmed (unavailable for entry) unless you have selected TCP or UDP as the protocol. See the description of Src IP Address for the selection options.

▪ **TCP Flag**: Specifies whether the rule should apply only to TCP packets that contain the synchronous (*SYN*) flag, only to those that contain the non-synchronous (*NOT-SYN*) flag, or to all TCP packets. This field will be dimmed (unavailable for entry) unless you selected TCP as the protocol.

▪ **ICMP Type**: Specifies whether the value in the type field in ICMP packet headers will be used as a criteria. The code value can be any decimal value from 0-255. You can specify that the value must equal (*eq*) or not equal (*neq*) the specified value, or you can select *any* to enable the rule to be invoked

on all ICMP packets. This field will be dimmed (unavailable for entry) unless you specify ICMP as the protocol.

- **ICMP Code**: Specifies whether the value in the code field in ICMP packet headers will be used as a criteria. The code value can be any decimal value from 0-255. You can specify that the value must equal (*eq*) or not equal (*neq*) the specified value, or you can select *any* to enable the rule to be invoked on all ICMP packets. This field will be dimmed (unavailable for entry) unless you specify ICMP as the protocol.

- **IP Frag Pkt:** Determines how the rule applies to IP packets that contain fragments. You can choose from the following options:
  - **Yes**: The rule will be applied only to packets that contain fragments.
  - **No**: The rule will be applied only to packets that do not contain fragments.
  - **Ignore**: (Default) The rule will be applied to packets whether or not they contain fragments, assuming that they match the other criteria.

- **IP Option Pkt:** Determines whether the rule should apply to IP packets that have options specified in their packet headers.
  - **Yes:** The rule will be applied only to packets that contain header options.
  - **No:** The rule will be applied only to packets that do not contain header options.
  - **Ignore:** (Default) The rule will be applied to packets whether or not they contain header options, assuming that they match the other criteria.

- **Packet Size:** Specifies that the IP Filter rule will take affect only on packets whose size in bytes matches this criteria. (*lt* = less than, *gt* = greater than, *lteq* = less than or equal to, etc.)

- **TOD Rule Status:** The Time of Day Rule Status determines how the Start Time/End Time settings are used.
  - **Enable:** (Default) The rule is in effect for the specified time period.
  - **Disable:** The rule is not in effect for the specified time period, but is effective at all other times.

3. When you are done selecting criteria, ensure that the Enable radio button is selected at the top of the page, and then click the Submit button at the bottom of the page.

   After a confirmation page displays, the IP Filter - Configuration page will redisplay with the new rule showing in the table.

   If the security level of the rule matches the globally configured setting, a green ball in the Status column for that rule, indicating that the rule is now in effect. A red ball will display when the rule is disabled or if its security level is different than the globally configured level.

7. Ensure that the Security Level and Private/Public/DMZ Default Action settings on the IP Filter Configuration page are configured as needed, then click the Submit button. A page displays to confirm your changes.

8. Click the Submit button to save the settings in temporary memory. When you are done making changes to the configuration settings, open the **Commit & Reboot** menu and click the Commit button to save your changes to permanent memory.

DNS

Multiple DNS addresses are useful to provide alternatives when one of the servers is down or is encountering heavy traffic. ISPs typically provide primary and secondary DNS addresses, and may provide additional addresses.

Domain Name Service (DNS) Configuration

This page is used for adding and deleting DNS server ip addresses. User can also enable/disable DNS relay from this page.

◉ *Enable*   ○ *Disable*

DNS Server IP Address	Action
No DNS Entries!	
0 0 0 0	Add

Submit   Cancel   Refresh   Help

DNS Configuration

Your LAN PCs learn these DNS addresses in one of the following ways:

- **Statically:** If your ISP provides you with their DNS server addresses, you can assign the addresses to each PC by modifying the PCs' IP properties.

- **Dynamically from a DHCP pool:** You can configure the DHCP Server feature on the Router and create an address pool that specify the DNS addresses to be distributed to the PCs.

In either case, you can specify the actual addresses of the ISP's DNS servers (on the PC or in the DHCP pool), or you can specify the address of the LAN port on the Router (e.g., 10.1.1.1). When you specify the LAN port IP address, the device performs DNS relay.

Configuring DNS Relay

When you specify the device's LAN port IP address as the DNS address, then the Router automatically performs **DNS relay**; i.e., because the device itself is not a DNS server, it forwards domain name lookup requests that it receives from LAN computers to a DNS server at the ISP. It then relays the DNS server's response to the PC. When performing DNS relay, the device must maintain the IP addresses of the DNS servers it contacts. It can learn these addresses in either or both of the following ways:

- **Learned through PPP:** If the device uses a PPP connection to the ISP, the primary and secondary DNS addresses can be learned via the PPP protocol. To use this method, the "Use DNS" checkbox must be selected in the PPP interface properties. (You cannot change this property by modifying an existing PPP interface; you must delete the interface and recreate it with the new setting.) Using this option provides the advantage that you will not need to reconfigure the PCs or the Router if the ISP changes their DNS addresses.

- **Configured on the Router:** You can use the device's DNS feature to specify the ISP's DNS addresses. If the device also uses a PPP interface with the "Use DNS" property enabled, then these configured addresses will be used in addition to the two addresses learned through PPP. If "Use DNS" is not enabled, or if a protocol other than PPP is used (such as EoA), then these configured addresses will be used as the primary and secondary DNS addresses.

Follow these steps to configure DNS relay:

1. Configure the LAN PCs to use the Router's LAN IP address as their DNS server address -- by assigning the LAN IP address statically to each PC, or by inputting the LAN IP address or the address 0.0.0.0 as the DNS address in a DHCP server pool.

2. If using a PPP connection to the ISP, configure it to "Use DNS" so that the DNS server addresses it learns are used for DNS relay.

   --OR--

   If not using a PPP connection (or if you want to specify DNS addresses in addition to those learned through PPP), configure the DNS addresses on the Router as follows:

   a. Click the Services tab, and then click **DNS** in the task bar. The DNS Configuration page displays.
   b. Type the IP address of the DNS server in an empty row and click the Add button. You can enter only two addresses.

   c. Click the **Enable** radio button, and then click the Submit button.

3. Click the Submit button to save the settings in temporary memory. When you are done making changes to the configuration settings, open the **Commit & Reboot** menu and click the Commit button to save your changes to permanent memory.

PPPoE Pass Through

The PPPoE Pass Through feature can be enabled to allow individual computers to gain access to PPPoE servers used for authentication by the ISP. Normally, when the device is functioning as a Router, the authentication process is handled by the Router on behalf of the computers on the LAN. Using PPPoE Pass Through enables individual computers on the LAN to establish separate PPPoE connections to servers outside the LAN.

Enable/Disable PPPoE PassThrough

Time & Date

The Router provides a number of options to maintain current date and time. This information is used to calculate and report various performance data. The Time & Date menu is divided into two fields. Use the upper portion to set the time using the computer you are now using to access the web manager. Use the lower portion to configure time information using Simple Network Time Protocol (SNTP).

Note	*Changing the device date and time does not affect the date and time on your PCs.*

Time & Date Configuration

To change the device date and time using your computer as the reference:

1. Leave the **Sync. with** option to select PC.

2. Find the appropriate **Time Zone:** from the drop-down list.

3. Click Submit button. You should see the time and date information change immediately so it is synchronized to your computers time. Continue to the Commit & Reboot menu. Click the Commit button to save your changes to permanent memory.

To use SNTP you will need to gain permission to use an SNTP server. Some companies maintain servers on their private network for this purpose. It is also possible to use a public SNTP service via the Internet. To set up SNTP service:

1. Select the SNTP option in the **Sync. with** field in the upper portion of the Time & Date menu.

2. Click the Add button in the lower, SNTP Server Configuration portion of the menu. A new window, the SNTP Server – Add menu appears.

3. Use the SNTP Server – Add menu to select an SNTP server by either an IP address or a domain name.

4. Choose the **Type:** of method used to find the SNTP server, if you are using an IP address select SNTP Address (default) and type in the IP address of the SNTP server below in the **Server Address:** space. If you are using the **Domain Name:** of the SNTP server, type in the domain name in the space provided.

5. Additional SNTP servers can be used in a standby capacity by repeating the Add SNTP Server process. All entries will appear listed in the lower portion of the Time & Date menu.

SNTP Server – Add menu

After adding the SNTP server or servers they appear listed under SNTP Server Configuration as shown below. The first server listed acts as the active server. If this connection fails or if for any reason SNTP information is interrupted from the active server, the system will switch to the backup server. To delete any listed server just click the trash can symbol under Actions for the server you want to delete.

SNTP Server Configuration list

Changing the Manager Password

The first time you log into the Web Configuration Manager, use the default user ID and password (*admin* and *admin*). The system allows only one user ID and password. Only the password can be changed. Access the User Configuration menu in the Admin folder.

User Configuration

This page displays user information. Use this page to add/delete users and change your password. Your new password can be up to 64 characters and is case-sensitive.

User ID	Privilege	Action(s)
admin	Root	🖉

Add   Refresh   Help

Change User Password

To change user name and password used for management privileges, log into the Configuration Manager, click on the Add button and change these settings in a new window:

User Config - Add

New User Information

User ID:	
Privilege:	○ Root ⊙ User
Password:	
Confirm Password:	

Submit   Cancel   Help

Add User

User ID:	This lists the current User ID (user name).
New Password:	Type in the new password.
Confirm New:	Type in the new password a second time for confirmation.

Click the Submit button to save the settings in temporary memory. When you are done making changes to the configuration settings, open the **Commit & Reboot** menu and click the Commit button to save your changes to permanent memory.

Commit & Reboot

Whenever you use the Web Configuration Manager to change system settings, the changes are initially placed in temporary storage (called random access memory or RAM). Your changes are made effective when you submit them, but will be lost if the device is reset or turned off.

To save your changes for future use, you can use the commit function. This function saves your changes from RAM to permanent storage (called flash memory).

Note	*When you Submit changes, they are activated immediately, but they are only saved until the device is reset or turned off. You must Commit the changes to saves them permanently.*

Use the Commit & Reboot menu to commit changes to permanent storage.

After you have submitted all the configuration changes you want to make for this session, click on the Commit & Reboot button in the Admin folder to view the Commit & Reboot page.

Commit and Reboot

To save current configuration settings as they have been submitted click **Commit**. (Disregard the selection in the Reboot Mode drop-down list; it does not affect the commit process.)

The changes are now saved to permanent storage (flash memory).

Reboot the Router

To reboot the device using the Configuration Manger, display the Commit & Reboot page, select the appropriate reboot mode from the drop-down menu, and then click **Reboot**.

⚠ IMPORTANT	*Do not reboot the device using the Reset button on the back panel of the Router to activate new changes. This button resets the device settings to the manufacturer's default values. Any custom settings will be lost.*

Reboot Options

Select the reboot option from the pull-down menu. The options are a described here:

Reboot	A simple reboot. This will put into effect any configuration changes that have been successfully committed to flash memory.
Reboot From Last Configuration	This will reboot the device using the current settings in permanent memory, including any changes you just committed.
Reboot From Default Configuration	This reboots the device to default settings provided by your ISP or the manufacturer. Choosing this option erases any custom settings.

Image Upgrade

Use the Image Upgrade menu to update firmware from a file on your system.

Image Upgrade

This page is used to upload a new image to the system.

Current Firmware Version:	R2.01.B5.EU(021018g/W78.1.7)
Upgrade File:	[ ] Browse...

Upload   Help

Image (Firmware) Upgrade

Upgrade File:	Type in the full path and file name of the firmware file to be uploaded. Alternatively you may click the Browse button to search for the file on your system.

When the filenames have been entered, click the Upload button to commence loading the firmware file. If the upload is successful, a message informs you that is was successfully loaded and asks you to reboot the device. Go to the Reboot menu and perform and simple reboot. If the firmware does not load, an error message informs you to try the upload again. Check the filenames and attempt to upload again. If the file still will not load, reboot the device and try again.

Diagnostics

The diagnostics feature executes a series of test of your system software and hardware connections. Use this feature when working with your ISP to troubleshoot problems.

Diagnostics Window

Select the Virtual Circuit and click the Submit button. A message will appear informing you if the loop test succeeded or failed.
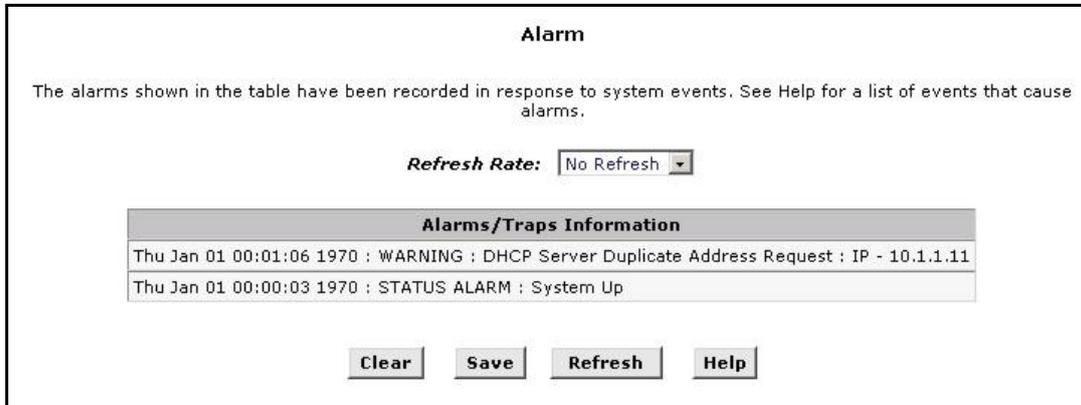
The diagnostics utility will run a series of test to check whether the device's connections are up and working. This takes only a few seconds. The program reports whether the test passed or failed. A test may be skipped if the program determines that no suitable interface is configured on which to run the test.

Alarms

The Configuration Manager can be used to view alarms that occur in the system. Alarms, also called traps, are caused by a variety of system events, including connection attempts, resets, and configuration changes.

Although you will not typically need to view this information, it may be helpful in working with your ISP to troubleshoot problems you encounter with the device. (Despite their name, not all alarms indicate problems in the functioning of the system.)

To display the Alarm page, log into the Configuration Manager, click the Alarm button in the Admin folder.

Alarm

The alarms shown in the table have been recorded in response to system events. See Help for a list of events that cause alarms.

Refresh Rate: No Refresh

Alarms/Traps Information
Thu Jan 01 00:01:06 1970 : WARNING : DHCP Server Duplicate Address Request : IP - 10.1.1.11
Thu Jan 01 00:00:03 1970 : STATUS ALARM : System Up

Clear   Save   Refresh   Help

Alarm/Trap Information Page

Listed under Alarm/Trap Information are the time and date of each recorded alarm event, the type of alarm, and a brief statement indicating its cause.

To remove all entries from the list, click the Clear button. New entries will begin accumulating and will display when you click the Refresh button.

To view or save the Alarm/Trap log, click on the Save button. Clicking on the Save button brings up a dialog box asking if you want to open the or save it to your computer. Clicking Open will open the file named SystemLog.txt. If you opt to save the file a new dialog box asks where on your computer you want to save the file. You can browse to select a location and save the file for later reference.

File Download

You are downloading the file:

SystemLog.txt from 10.1.1.1

Would you like to open the file or save it to your computer?

Open   Save   Cancel   More Info

☑ Always ask before opening this type of file
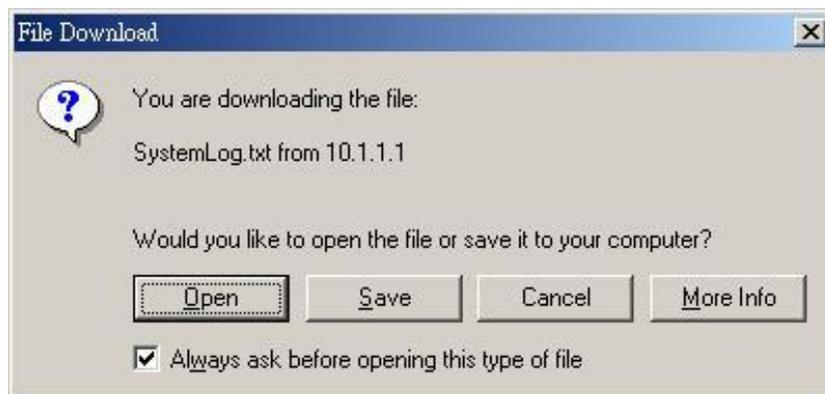
Port Settings

The Router allows some standard (logical) port settings to be changed. Under some circumstances it is desirable to redirect incoming data packets to a specialized server such as a Web server.

Change Port Settings

To redirect incoming HTTP, Telnet or FTP packets to a non-standard port, type in the new value in the space provided and click on the Submit button.

Remote Access.

The Router can be managed from outside the LAN (i.e. though the WAN port) by enabling Remote Administrator Access.

Choose to either *Enable* or *Disable* Remote Administration of the Router and click on the Submit button.

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 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	DHCP BOOTP ARP AAL5
DATA TRANSFER RATE:	G.dmt full rate: Downstream up to 8 Mbps Upstream up to 640 Kbps G.lite: Downstream up to 1.5 Mbps Upstream up to 512 Kbps	
MEDIA INTERFACE EXCHANGE:	RJ-11 port ADSL telephone line connection RJ-45 port for 10/100BASE-TX Ethernet connection RS-232 (DB9 female) console port for local configuration	

| Physical and Environmental	
DC inputs: **Power Adapter:**	Input: 120V AC 60Hz Output: 7.5V DC 1.5A
Power Consumption:	7.5 Watts (max)
Operating Temperature:	0° to 40° C (32° - 104° F)
Storage Temperature:	-20° to 70° C (-4° - 158° F)
Humidity:	5 to 95% (non-condensing)
Dimensions:	190 mm x 116.8 mm x 30.9 mm
Weight:	300 gm
EMI:	CE Class B FCC Class B
Safety:	CSA International Mark

B

Low Pass Filters

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 low pass filters and are variously referred to as in-line filters, micro-filters, line splitters or split line filters. They are easy to install and use standard telephone connectors and cable.

For some ADSL clients, a telecommunications technician will be sent to the client's premises to modify the telephone line, usually at the point where the telephone line enters the building. If a technician has divided or split your telephone line into two separate lines - one for regular telephone service and the other for ADSL – then you do not need to use any type of filter device. Follow the instructions given to you by your ADSL service provider, ISP or telephone company about where and how you should connect the Router to the ADSL line.

In-Line Filters

Two common styles of low pass filters are shown in this section, the first is an in-line filter and is illustrated below. In-line filters are easy-to-install, in-line devices, which attach to the telephone cable between the telephone and wall jack.
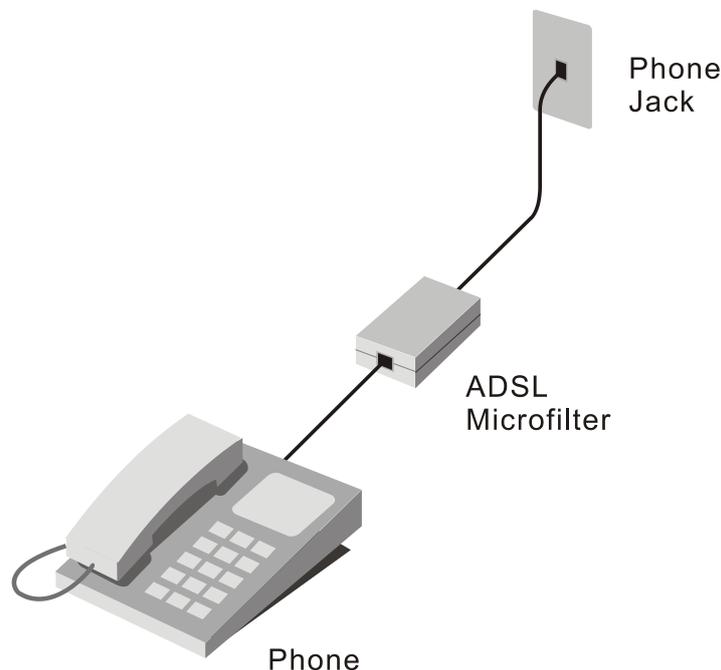
In-line Filter Installation

Note	*Do not install an in-line filter between the Router and the telephone jack. In-line filters are only intended for use with regular telephones, Fax machines and other regular telephone devices.*

Split Line Filter

If you are instructed to use a split line style filter you must install the device between the Router 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 Router 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 Router.

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

The diagram below illustrates the proper use of the split line style filter.
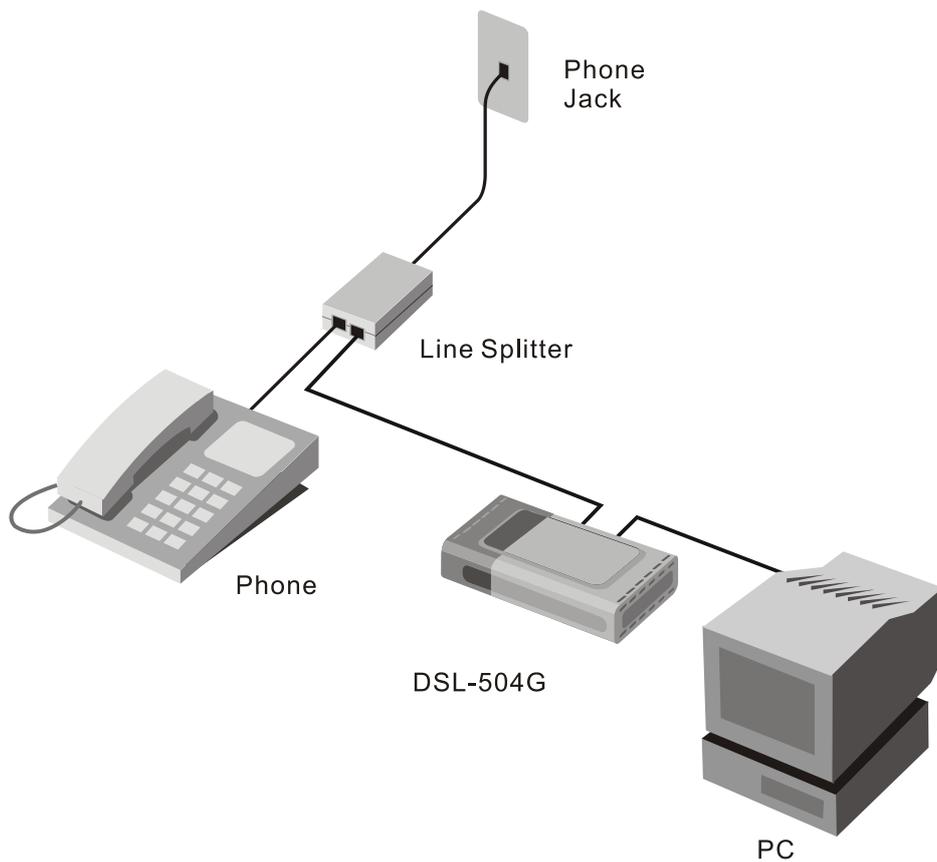
Split Line Filter Installation

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 (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 Goyeechea 2934 of 702, Las Condes, 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** 2F, Sigma Building, 49 Zhichun Road, Haidan District, 100080 Beijing, China TEL: 86-10-88097777 FAX: 86-10-88096789 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** Thlli-ja Pakkahuone Katajanokanlaituri 5, FIN– 00160 Helsinki TEL: 358-9-622-91660 FAX: 358-9-622-91661 URL: www.dlink-fi.com
France	**D-Link France** Le Florilege #2, Allee 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, Kurla-Bandra Complex Rd., Off Cst Rd., 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 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 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
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 Thranesgt. 77, 0175 Oslo, Norway
	TEL: 47-22-991890 FAX: 47-22-207039
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**
	102 – 106 Witchhazel Avenue, Einstein Park 2, Block B, Highveld Technopark,
	Centurion, 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. 119 Pao-Chung Rd, 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
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®