

# **D-Link<sup>®</sup>**

***DSL-504***  
***ADSL Router***  
***User's Guide***

---

---

(September 2002)

---

---

## **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. Verwenden 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 ist 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 sollte 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 autorisiertem 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 sind beschädigt.
  - b – Flüssigkeit ist in das Gerät eingedrungen.
  - c – Das Gerät war Feuchtigkeit ausgesetzt.
  - d – Wenn das Gerät nicht der Bedienungsanleitung entsprechend 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 Originalersatzteile bzw. den Originalteilen entsprechende Teile verwendet werden. Der Einsatz von ungeeigneten Ersatzteilen kann eine weitere Beschädigung hervorrufen.
17. Wenden Sie sich mit allen Fragen die Service und Reparatur 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 größer 3kg ist eine Leitung nicht leichter als H05VV-F, 3G, 0.75mm<sup>2</sup> 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, NEGLIGENCE, 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

---

<b>ABOUT THIS USER'S GUIDE .....</b>	<b>VII</b>
Guide Overview .....	vii
Before You Start .....	vii
Requirements .....	vii
Web Browser.....	viii
Ethernet Port (NIC Adapter) .....	viii
About Bridged Ethernet Connections (RFC 1483) .....	viii
About IPoA Connections (RFC 1577) .....	ix
Additional PVC Settings .....	ix
<b>Packing List .....</b>	<b>ix</b>
<b>INTRODUCTION .....</b>	<b>1</b>
What is ADSL? .....	1
<b>Router Description and Operation .....</b>	<b>1</b>
<b>Router Features.....</b>	<b>2</b>
Front Panel Display and LED Indicators .....	3
Rear Panel Cable Connections .....	4
<b>HARDWARE INSTALLATION .....</b>	<b>5</b>
Connect ADSL Line.....	5
Connect Router to the Ethernet .....	5
Computer to Router Connection .....	5
Switch to Router Connection .....	5
Power On Router.....	6
<b>CONFIGURING THE ROUTER FOR THE FIRST TIME .....</b>	<b>7</b>
Configuring IP Settings on Your Computer.....	7
<b>Access the Configuration Manager .....</b>	<b>14</b>
Configure the Router.....	15
<b>WEB-BASED MANAGEMENT .....</b>	<b>17</b>
Accessing the Web Manager.....	17
Folders and Menus .....	18
<b>Router Configuration .....</b>	<b>18</b>
Configuring the WAN Connection .....	19
Additional Virtual Connections (PVCs) .....	21
Configuring LAN IP Settings.....	23
Layer 2 Filtering.....	24
Proxy DNS Settings .....	25
DHCP Configuration.....	26
NAT Configuration .....	27
IP Masquerade Pass Through.....	28
Port Redirection .....	30
Static Route Configuration.....	32
Advanced Filter & Firewall .....	33

RIP .....	35
Date & Time Settings.....	36
UPnP .....	37
<b>System Maintenance .....</b>	<b>38</b>
System Username and Password.....	39
Save Changes .....	39
Factory Reset.....	40
Update Firmware.....	40
ADSL Line Setting.....	42
<b>Summary.....</b>	<b>43</b>
System Summary .....	43
<b>TECHNICAL SPECIFICATIONS.....</b>	<b>49</b>
<b>LAN IP SETUP .....</b>	<b>51</b>
<b>Assigning Network IP Addresses.....</b>	<b>51</b>
Using the Default IP Address.....	51
Manual IP Address Assignment.....	51
Using DHCP .....	52
Changing the IP Address of the Router.....	52
<b>IP CONCEPTS .....</b>	<b>53</b>
<b>IP Addresses .....</b>	<b>53</b>
<b>Subnet Mask.....</b>	<b>55</b>
<b>DSL-504 FIRMWARE UPGRADE UTILITY .....</b>	<b>56</b>
<b>MICROFILTERS AND SPLITTERS .....</b>	<b>58</b>
Microfilters .....	58
Line Splitter .....	59

---

## About This User's Guide

This user's guide provides instructions on how to install the DSL-504 ADSL Router and use it to connect a computer or Ethernet LAN 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.

### 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 use 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 can be described in general terms in the following steps:

1. Gather information and equipment needed to install the device. Before you begin the actual installation make sure you have all the necessary information and equipment.
2. Install the hardware, that is, connect the cables (Ethernet and telephone) to the device and connect the power adapter.
3. Check the IP settings on your computer and change them if necessary so the computer can access the web-based software built into the Router.
4. Use the web-based management software to configure the device to suit the requirements of your ADSL account.

## Requirements

To install and use the Router you need a computer equipped with an Ethernet port (such as an Ethernet NIC) and a web browser. You may also need to use information given to you by your ISP. This information is stored in the Router's memory and used to establish the WAN connection and confirm your identity. Read the next page for more details about these requirements.

### 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-504 uses an HTML-based web interface for setup and management. The web configuration manager may be accessed using any operating system capable of running web browser software.

## Web Browser

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

## Ethernet Port (NIC Adapter)

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

## Additional Software

It may be necessary to install software on your computer that enables the computer to access the Internet. Additional software must be installed if you are using 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 used to describe a bridged ADSL connection including the term “RFC 1483 Bridge” which is used in this guide.

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 ADSL connection you have.

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

## About Bridged Ethernet Connections (RFC 1483)

Using this method, the DSL-504 acts as a transparent bridge, and is invisible to other devices on both the WAN and LAN side of the bridge. It is therefore necessary to provide some means of acquiring global IP settings for your account.

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



## **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.

## **Additional PVC Settings**

If you are using multiple virtual connections it will be necessary to provide additional VPI and VCI values for the device. These numbers define a unique route used on the ATM backbone of the WAN. Chapter 4 contains instruction on how to set up additional PVCs for accounts using more than one virtual connection.

## ***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-504 ADSL Ethernet Router
2. One 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





## 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, it is not necessary expensive new cabling or condition the line in any way.

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 it possible to enjoy benefits such as high-speed Internet access 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-504 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-504 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-504 connects to an Ethernet LAN via a standard Ethernet 10BASE-T interface using RJ-45 connectors. The ADSL connection is made using ordinary twisted-pair telephone line with standard RJ-11 connectors. This arrangement means that several computers can be networked and connected to the Internet using a single WAN interface and IP address.

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

## Router Features

The DSL-504 ADSL Ethernet Router utilizes the latest ADSL enhancements to provide a reliable Internet portal suitable for most small to medium sized offices. DSL-504 advantages include:

- **PPP (Point-to-Point Protocol) Security** The DSL-504 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 all LAN IP settings to each host on your network. This eliminates the need to reconfigure every host whenever changes in network topology occur.
- **Network Address Translation (NAT)** For small office environments, the DSL-504 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-504 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-504 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-504 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-504 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-504 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 Support** Up to eight PVCs can be assigned for use by the Router. This can be useful to ADSL clients who wish to dedicate a PVC for a specific application, LAN or server.

## 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.

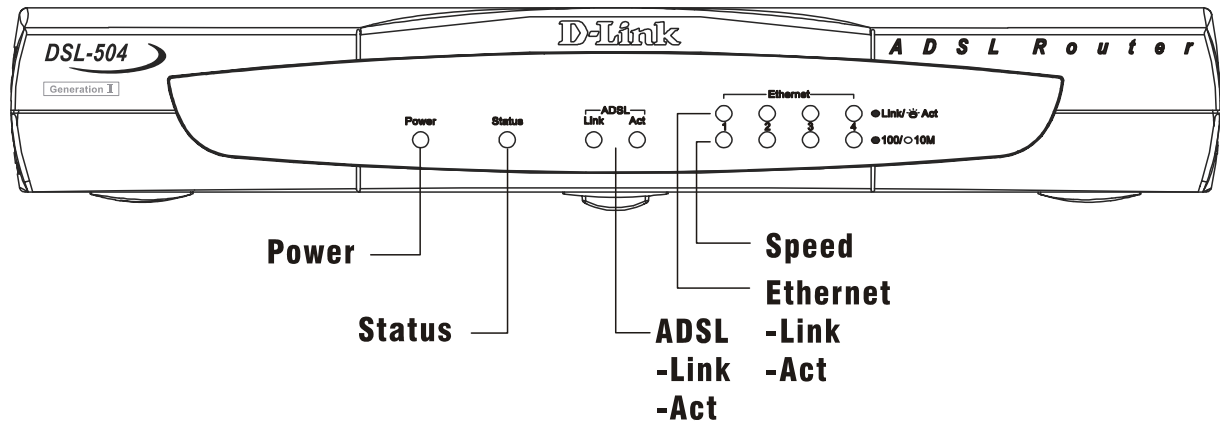


Figure 2 - 1. Front Panel Display

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.

**ADSL: Link** Steady green light indicates a valid ADSL connection. This will light after the ADSL negotiation process has been settled.

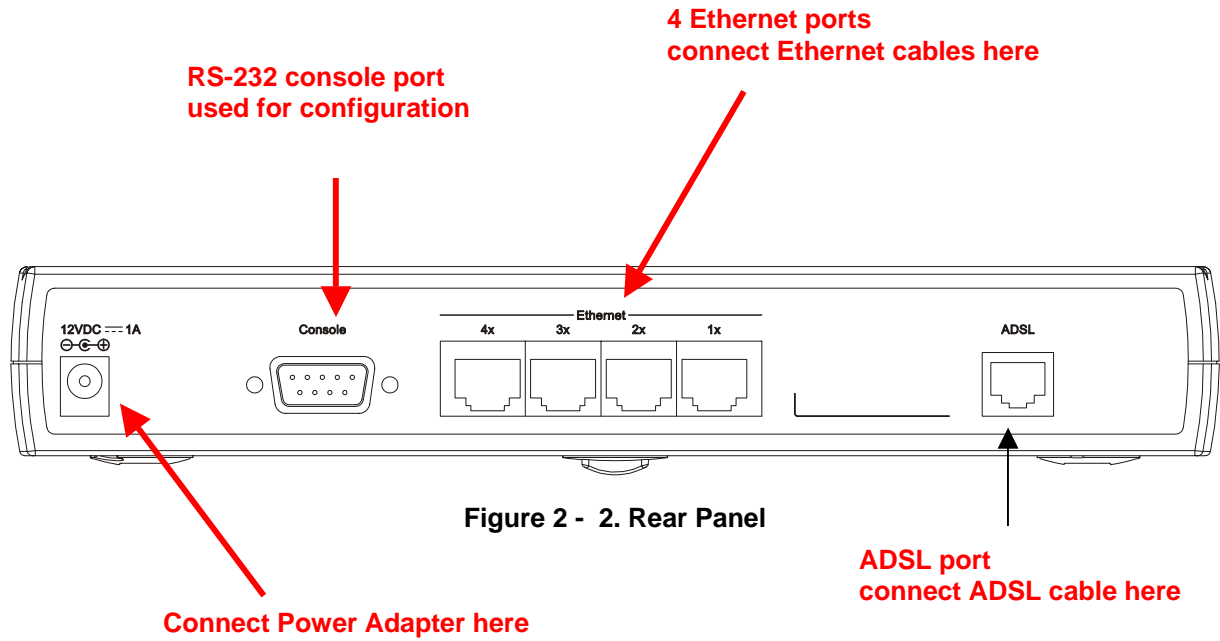
**ADSL: Act** Blinking green light indicates an active WAN session.

**Ethernet: Link** Steady green light indicates a valid Ethernet connection.

**Ethernet: Act** Blinking green indicates an active Ethernet session.

## Rear Panel Cable Connections

All cable connections to the Router are made at the rear panel.



## Hardware Installation

When selecting the location for the Router, be sure to allow room to access the connections on the rear panel. You will want to place the Router so that you will be able to see the LED indicators on the front panel. 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 twisted-pair ADSL cable (standard telephone cable) included with the Router to connect it to your telephone line. Plug one end of the cable into the ADSL port (RJ-11 receptacle) on the rear panel of the Router and insert the other end into the wall jack. The ADSL connection is the physical connection for the Router's WAN interface. It links the Router to the network service provider's backbone infrastructure. This is the Router's link 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 may be connected to any 10/100BASE-TX Ethernet LAN. Any connection to an Ethernet concentrating device such as a switch or hub must operate at a speed of 10/100 Mbps only. When connecting the Router to any Ethernet device that is capable of operating at speeds higher than 10Mbps, be sure that the device has auto-negotiation (NWay) enabled for the connecting port.

Use standard Category 5 or better twisted-pair Ethernet cable with RJ-45 connectors. The RJ-45 ports on the Router are crossed (MDI-X) ports.

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

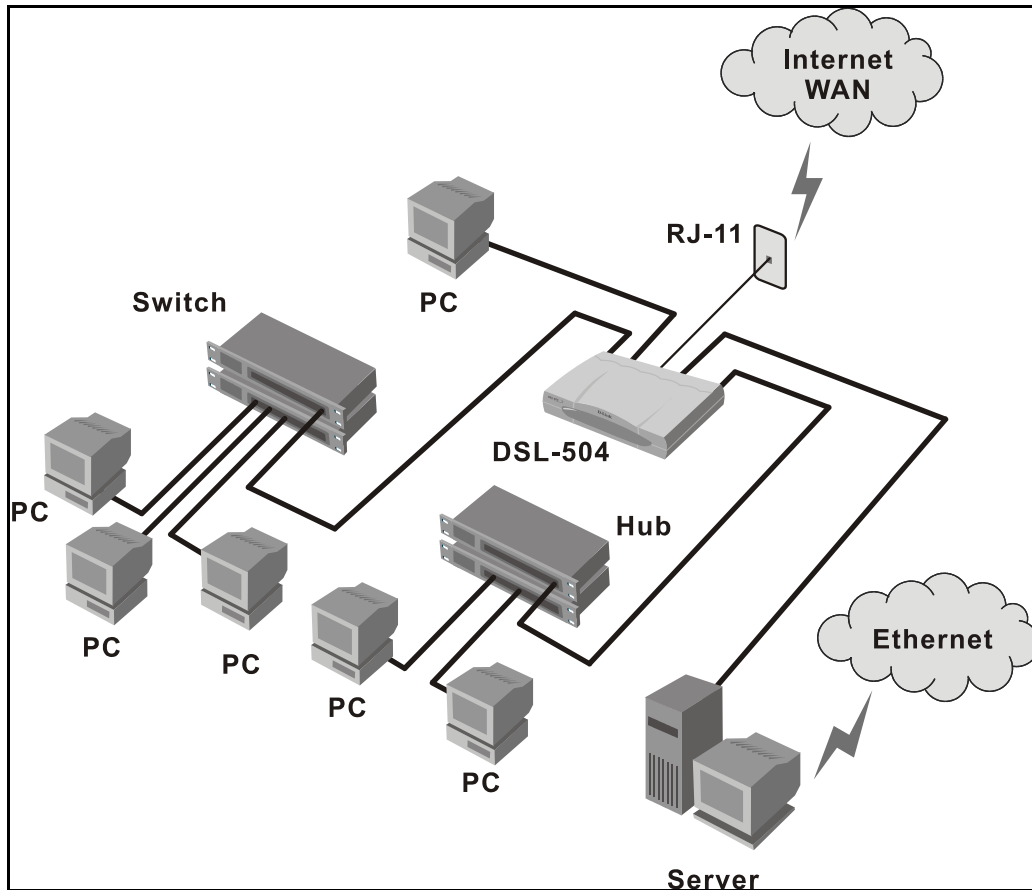
### Computer to Router Connection

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 come with the Router is known as a straight-through cable. This type of cable is appropriate for connecting to a crossed (MDI-X) port, the kind of port used on common Ethernet adapters for PCs and notebook computers.

### 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 easiest way to see if the Ethernet connection is valid is to look at the LED indicators when the device is connected and powered on.

The DSL-504 can provide a secure gateway to the Internet for small and medium sized Ethernet LANs.



**Sample Ethernet LAN with the DSL-504 Gateway**

## **Power On Router**

To power on the device:

1. Insert the AC Power Adapter cord into the power receptacle located on the rear panel (see Figure 2 - 2. Rear Panel) of the Router and plug the adapter into a nearby power source.
2. 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.
3. 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 (see Chapter 4) this should light up after several seconds.



## 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 to make changes to Router configuration including IP settings and DHCP setup. This chapter is concerned with using your computer to configure the WAN connection. The following chapter 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.

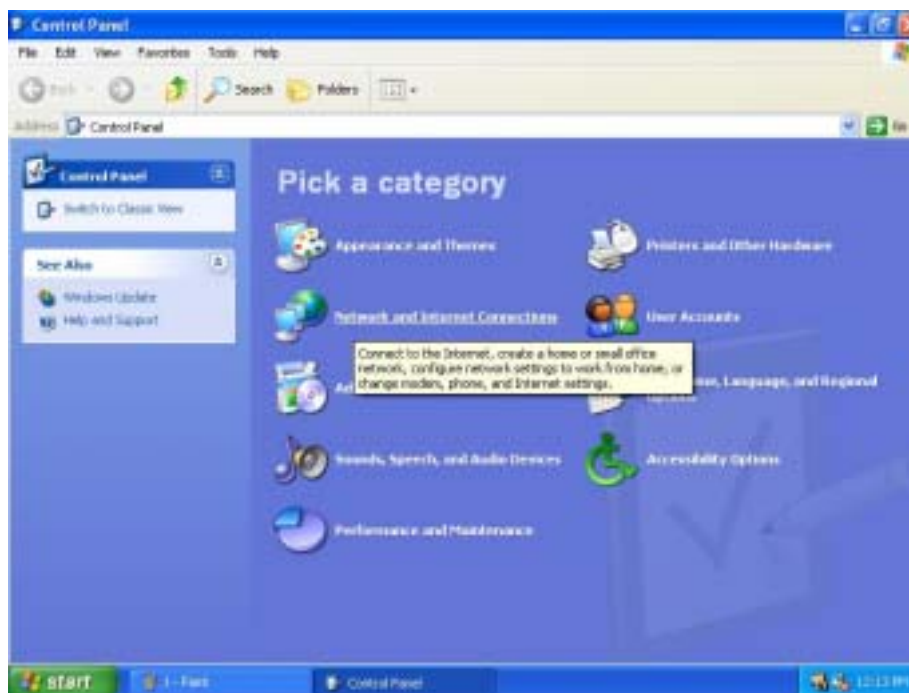
## Configure Windows XP for DHCP

Use the following steps to configure a computer running Windows XP to be a DHCP client.

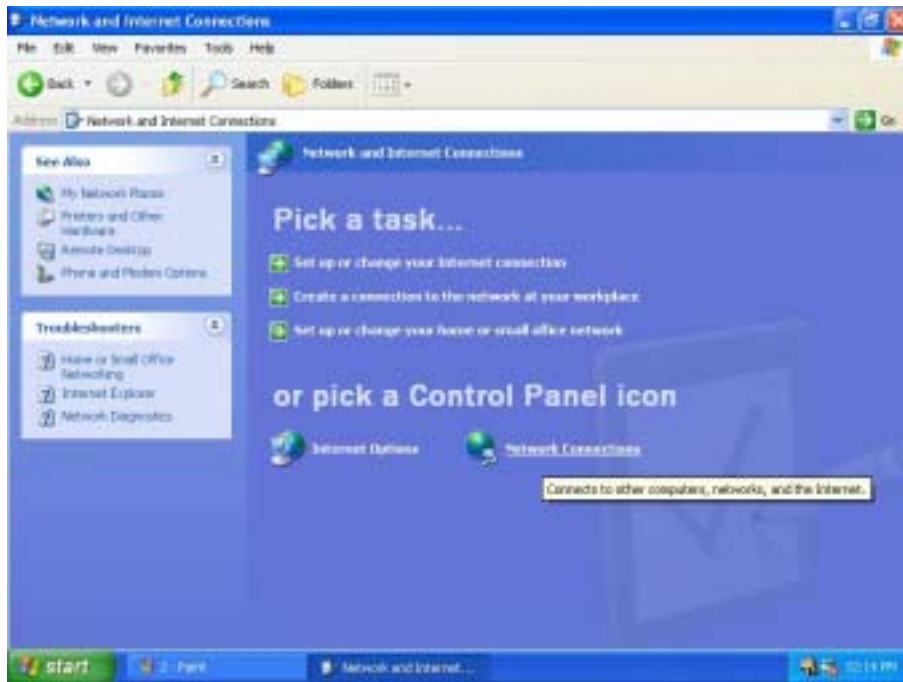
1. From the **Start** menu on your desktop, go to click on **Control Panel**.



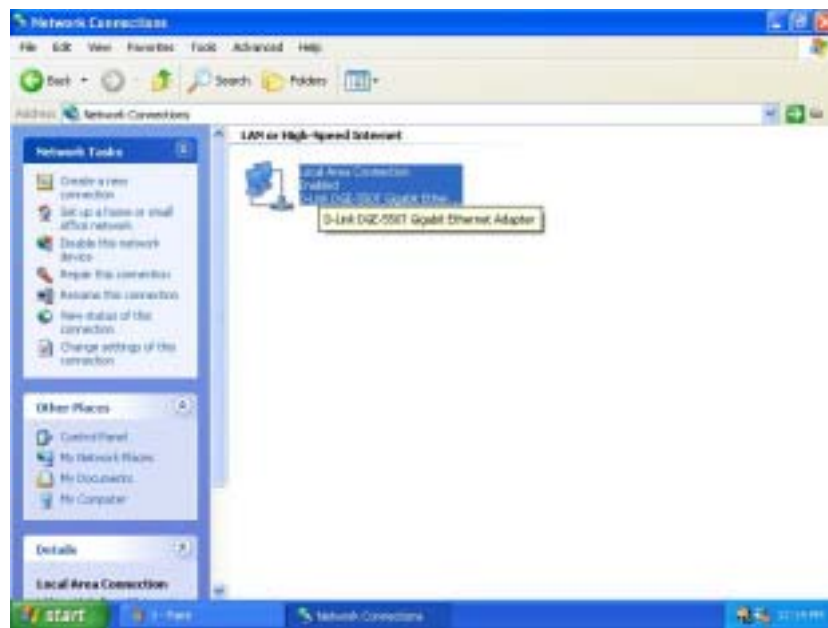
2. In the Control Panel folder, click on **Network and Internet Connections**.



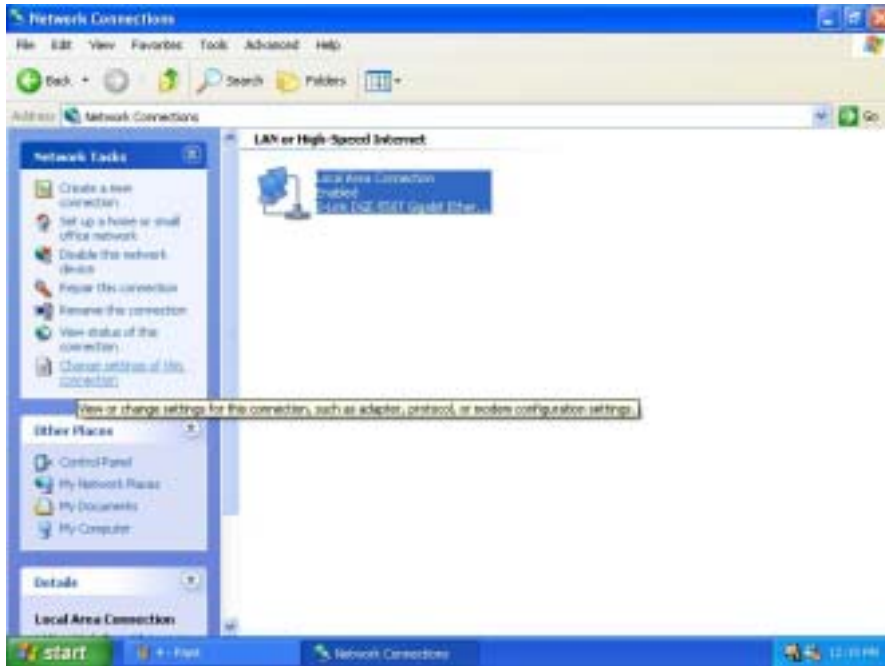
3. In the Network and Internet Connections folder, click on **Network Connections**.



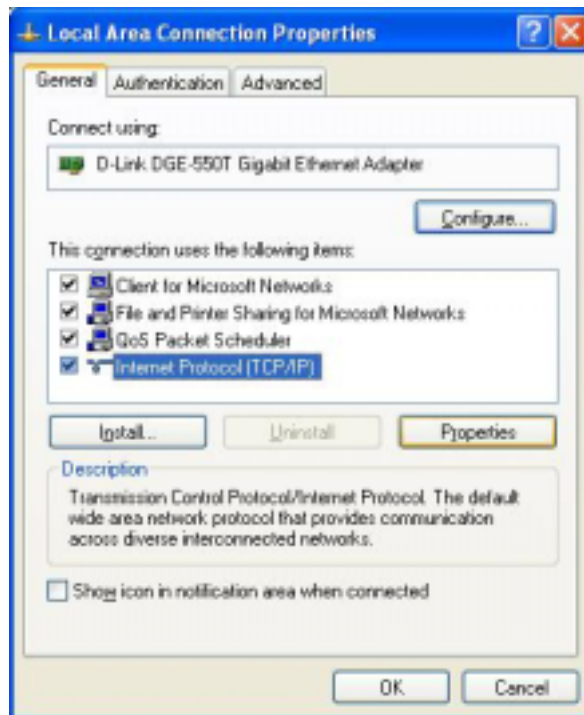
4. In the Network Connections folder, highlight the **Local Area Connection** icon by clicking on it once. A new option is revealed under Network Tabs in the left side panel.



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.

## Access the Configuration Manager

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

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

1. In Windows, click on the START button, go to Settings and choose Control Panel.
2. In the Control Panel window, double-click on the Internet Options icon.
3. Click the Connections tab and click on the LAN Settings button.
4. Verify that the "Use proxy server" option is NOT checked. If it is checked, click in the checked box to deselect the option and click OK.

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

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

In the page that opens, click on the **Login** button.

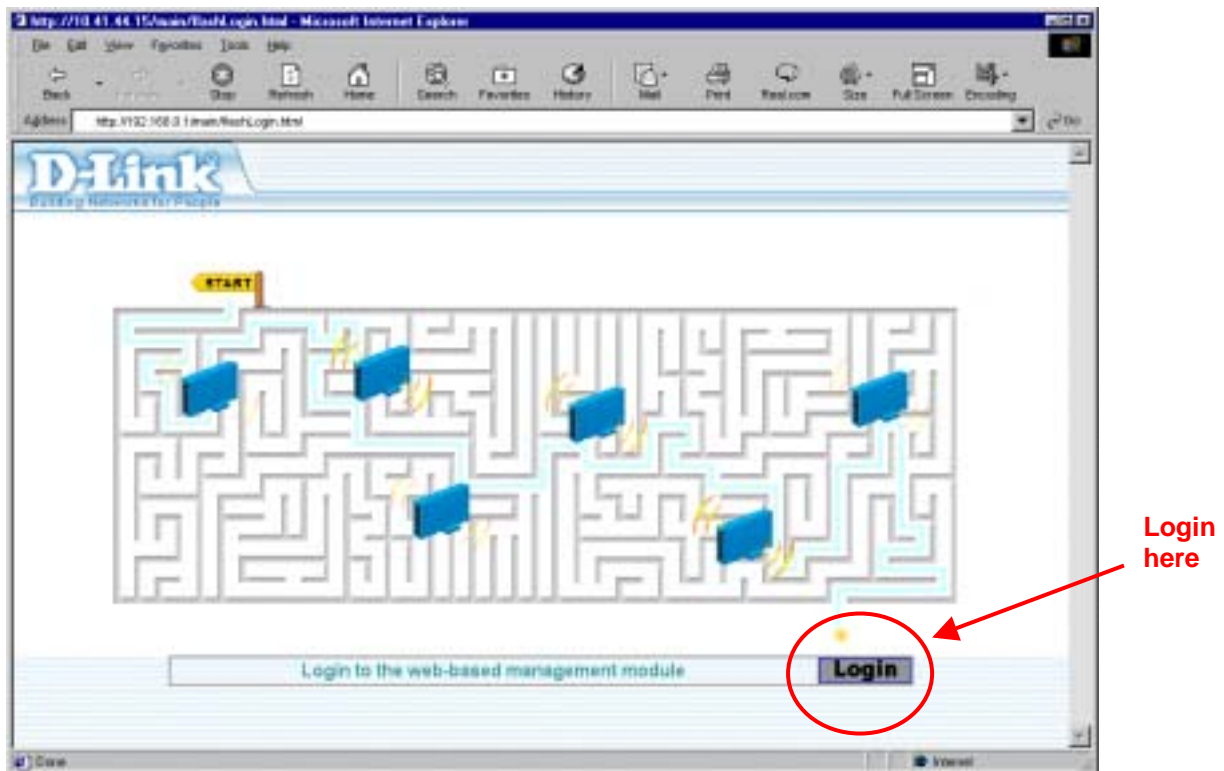


Figure 4 - 1. Login Page

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





Figure 4 - 2. Login to Router

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

## Configure the Router

The first page that appears after you successfully login displays the menu you need to configure the Router so it can connect to the Internet. The Multiple PVC menu is used to configure the Router's WAN connection and also used to add other virtual connections (PVCs). Our purpose now is to merely establish the primary connection. The remainder of this chapter describes what is how to establish this WAN connection. For a complete description of the user changeable variables in the Multiple PVC menu see Table 5 - 1. WAN Connection Configuration in the next chapter.



Figure 4 - 3. Configuring the WAN Connection (First Time Setup)

When the Router is used to provide Internet access it actually must first access your service provider's network, that is, it must communicate with computers and other routers owned by your service provider. These computers and routers then provide access to the Internet. The Router must be configured to communicate with the systems that give it access to the larger network. There are different methods or protocols used to make this communication possible, and both ends of the communication must agree on what method to use and how to set up the connection. This is what you will configure the Router to do, to agree with the service provider's equipment and negotiate the terms of the connection using a language or protocol that both sides understand.

Sometimes it is also necessary to configure settings that control the actual ADSL connection. The ADSL connection is what actually carries the data from one point to the other. So in addition to telling the Router what method it must use, you may also be asked change the PVC (Permanent Virtual Channel) settings. These settings are defined by two number the VPI (Virtual Path Indicator) and the VCI (Virtual Channel Indicator).

All the information you need to make the changes needed for a functioning WAN connection should have been provided to you by your ISP or network service provider.

To configure the WAN connection, open the Multiple PVC menu and perform the steps listed below. Some of the settings do not need to be changed when you first set up the device but can be changed later if you choose.

- 1 Leave **Select Index to set** at 1.
- 2 Type in an **Item Name** in the space provided. Or just use the default name ISP1.
- 3 Do not change the **VPI** or **VCI** values unless you are required to do so. If these settings are incorrect, the ADSL connection will not function. Many users will be able to use the default settings. If you are told to change these, type in the values given to you by your service provider.
- 4 Select the **Encapsulation** method used for your connection. The options available are *PPPoA VC mux*, *PPPoA LLC*, *PPPoE LLC*, *IPoA VC mux*, *IPoA LLC*, *Bridge VC mux* or *Bridge LLC*. The default Encapsulation is PPPoA LLC. If you select an IPoA or Bridge Encapsulation, the user changeable variables displayed in the browser will change. These different variables are described in step 5.1 – 5.3.
- 5 The remaining settings that must be configured are different for the different Encapsulations.
  - 5.1 If you have selected a PPPoE or PPPoA Encapsulation you must supply a **User Name** and **Password** used to verify the identity of your account. Type in the User Name and Password used for your PPP connection. Also select the **Authentication** method used, *pap* or *chap*, choose *Enabled* for **Connect On Demand** and leave the **Idle Time** setting at 0.
  - 5.2 If you have selected a IPoA Encapsulation, you must choose whether to enable or disable the **IP Unnumbered** option. The option is enabled by default. If you are instructed to leave this enabled, go to step 6. If you are told to disable the IP Unnumbered option, you must supply the global IP settings used for your account. In this case type in the **IP Address** and select the **Subnet Mask** from the drop down menu and go to step 6.
  - 5.3 If you have selected a Bridge Encapsulation, there are no more change needed to establish the WAN connection for the Router. However, you will probably have to install some sort of connection software on your computer. Go to step 6 and finalize the Router configuration, then install any additional software. Follow the instructions given to you by your ISP or network service provider.
- 6 Click the **Add** button when you have entered all the information. The web browser will briefly go blank. After a few seconds the PVC profile listed in the Existing Entry Table at the top of the web page will show the changes you just configured.
- 7 Click the **Apply** button located to the right of the Existing Entry Table. After a few second you will be prompted to save the changes and restart or continue to make other changes to the Router's configuration. Leave the Save and Restart option selected and click the **OK** button. The Router will save the WAN configuration settings and restart. After restarting it will begin to negotiate the connection. You can login to the web manager again and you should see the Router's **Connection Status** at the bottom of the web page. When this indicates the Router is *Connected* you can access the Internet or continue to configure the Router.

## Web-based Management

The DSL-504 offers a web-based (HTML) graphical user interface allowing users to manage the Router from anywhere on the LAN using a standard browser. A web browser is used to communicate directly with the Router and make changes to the configuration or monitor status.

### Accessing the Web Manager

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

To use the web-based management software run the browser you have installed on your computer and direct it to the Router's HTML interface using its LAN IP address. If this is the first time you are accessing the web-based manager you must type its default IP address, **192.168.0.1** in the address bar of the browser. The URL in the address bar should read: **http://192.168.0.1**. If you change the IP address you will use the new IP address to access the web-based manager.

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

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

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

1. In Windows, click on the START button, go to Settings and choose Control Panel.
2. In the Control Panel window, double-click on the Internet Options icon.
3. Click the Connections tab and click on the LAN Settings button.
4. Verify that the "Use proxy server" option is NOT checked. If it is checked, click in the checked box to deselect the option and click OK.

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

If this is the first time you are accessing the configuration manager and you simply want to establish a connection to the Internet, you may want to read the section titled Configure the Router in the previous chapter.

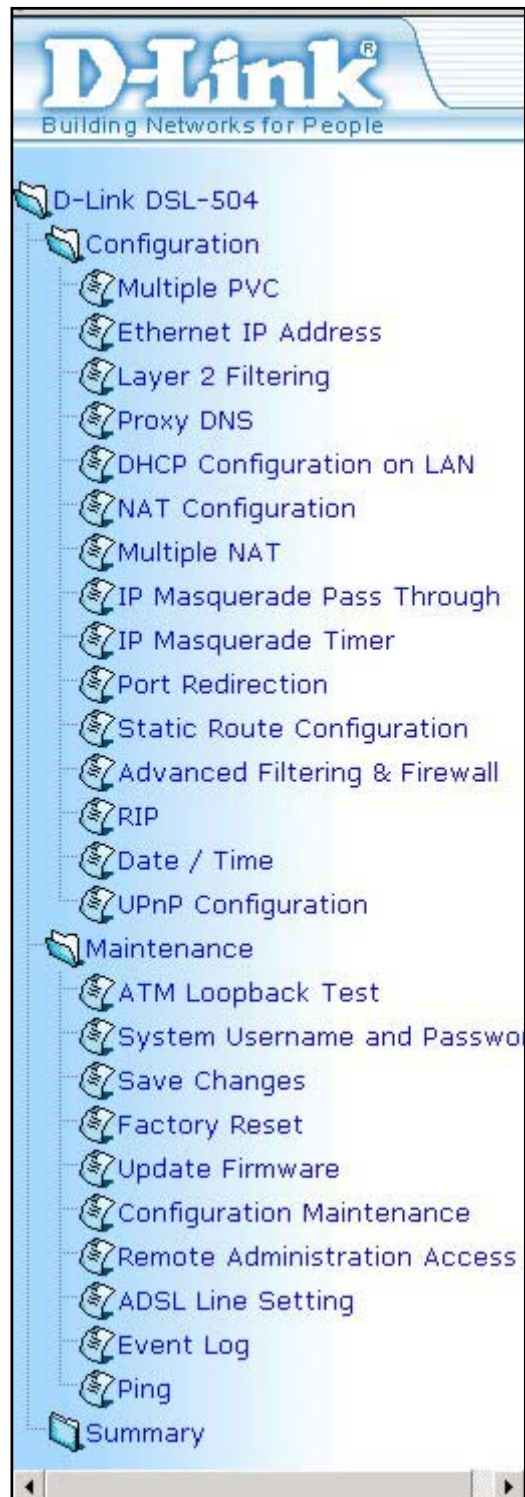
## Folders and Menus

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

## Router Configuration

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

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



## Configuring the WAN Connection

Use the Multiple PVC menu to configure the WAN interface for PVC settings and other settings used to configure the ADSL connection and the connection to the service provider's network. Use this menu to add, change or delete PVC connection profiles if you have a multiple PVC account. The following section, Additional Virtual Connections (PVCs), describes how to set up additional PVC connection profiles.



Figure 4 - 1. WAN Configuration

The Router may be configured to use common Encapsulation and connection methods commonly used for ADSL service. The information that is needed for the different method varies according to connection type. Therefore the menu will change to offer different settings depending on whether the connection is a PPP, IPoA or Bridged connection type.

To configure a single PVC profile, select the **Encapsulation** setting first. This may change the user configurable variables that are offered. The default Encapsulation used for the Index 1 profile is PPPoA LLC. Table 5 - 1. WAN Connection Configuration on the next page lists the configuration settings for the different Encapsulation types.

In the Multiple PVC configuration menu configure the WAN interface settings described in the table below.

<b>All connections must configure:</b>	
<b>Select index to set</b>	Choose the index number you wish to modify or delete.
<b>Item Name</b>	Type in a new name for this profile.
<b>VPI</b>	Type in the new VPI setting (0-255)
<b>VCI</b>	Type in the new VCI setting (32-65535)
<b>Encapsulation</b>	From the drop-down menu select <i>PPPoE LLC</i> , <i>PPPoA LLC</i> , <i>PPPoA VC mux</i> , <i>IPoA LLC</i> , <i>IPoA VC mux</i> , <i>Bridge LLC</i> , or <i>Bridge VC mux</i> . Default for Index 1 = PPPoA LLC.
<b>PPP Connections must configure:</b>	
<b>Login User Name</b>	Used for authentication by your network service provider.
<b>Login Password</b>	Used for authentication by your network service provider
<b>Confirm Password</b>	Type the same password to confirm it.
<b>Authentication</b>	Protocol used to confirm the identity of the subscriber. Choose chap (default) or pap from the drop-down menu.
<b>Connect on Demand</b>	Select enabled or disabled. When this function is enabled the router will connect any workstation on your LAN to the Internet upon request. If this function is disabled, it will be necessary to access this menu and hit the Connect button each time you want to establish a connection to the WAN or the Internet.
<b>Idle Time</b>	A value of 0 means that the PPP connection will remain connected. If your network account is billed according to the amount of time the Router is actually connected to the Internet, enter an appropriate Idle Time value (in seconds). This will disconnect the Router after the WAN connection has been idle for the amount of time specified. The default value = 0.
<b>IPoA Connections must configure:</b>	
<b>IP Unnumbered</b>	This is enabled by default and therefore no IP settings need to be entered for the account. If this is disabled, (global) IP settings must be configured for the WAN interface.
<b>IP Address</b>	If IP Unnumbered is disabled, type in the WAN IP address for the account.
<b>Subnet Mask</b>	If IP Unnumbered is disabled, type in the subnet mask for the WAN interface.

**Table 5 - 1. WAN Connection Configuration**

### **Connect / Disconnect**

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

## Additional Virtual Connections (PVCs)

The Router can use up to eight simultaneous PVC connections. These additional connections occupy the same bandwidth used for ADSL service. Additional PVC connections can be added to establish a private connection to remote offices or maintain a server accessible through the WAN port. Provision for additional PVC profiles must be done through the telephone company or telecommunications services company. The remote user must have suitable ADSL equipment for a successful connection.

Use the Multiple PVC menu to add, delete or modify additional PVCs as described below.

### Multiple PVC

Existing Entry    6 Apply

Index	Item Name	Interface	VPI	VCI	Encapsulation
1	ISP1	ppp_device	0	35	PPPoE LLC
2	remote 1	ppp_device2	2	32	PPPoE LLC
3	remote 2	ppp_device3	1	32	PPPoE LLC
4	Irvine	ppp_device4	1	33	PPPoE LLC
5	web server	bridge5	1	34	Bridge LLC
6	fireline	ppp_device6	2	34	PPPoE LLC

**Select index to set**    6 ▼    Modify    Delete    Clear

**Item Name**   

**VPI**   

**VCI**   

**Encapsulation**    PPPoE LLC ▼

**Login User Name**   

**Login Password**   

**Confirm Password**   

**Authentication**    pap ▼

**Connect On Demand**    enabled ▼

**Idle Time**

**PPP Information**

**IP Address**    0.0.0.0

**Gateway**    0.0.0.0

**Connection Status**    Physical line error

Add
Connect
Disconnect

**Figure 4 - 2. Multiple PVC Menu**

In order to use additional PVCs each profile must have a unique (to the Router) Item Name and a unique VCI/VCI combination. You may use any available Encapsulation or connection type. Follow the instructions on the next page to set up multiple PVCs.

**To add a PVC:**

1. Type in an **Item Name**. This name may not be used for any other PVC profiles on the Router.
2. Type in a new **VPI** and **VCI** value. This combination may not be used for another PVC profile on the Router.
3. Select the **Encapsulation** method used for the new PVC.
4. For PPP connections (PPPoE or PPPoA), you must supply a new **User Name** and **Profile**. You may use the same user name/password combination for more than one PVC unless you are specifically told not to do this by your service provider. It is recommended however that a different combination be used whenever it is practical. Also for PPP connections, select the **Authentication, Connect On Demand** and **Idle Time** settings (see Table 5 - 1. WAN Connection Configuration).
5. For IPoA connections, supply account IP settings if IP Unnumbered is disabled (see Table 5 - 1. WAN Connection Configuration)
6. Click the **Add** button when you have entered all the information. The web browser will briefly go blank. After a few seconds the new PVC profile appears listed in the Existing Entry Table at the top of the web page.
7. When all the new PVCs you wish to create have been entered, click the **Apply** button located to the right of the Existing Entry Table. After a few second you will be prompted to save the changes and restart or continue to make other changes to the Router's configuration.

**To modify an existing PVC:**

1. Select the index number of the PVC profile you want to change with the Select index to set drop-down menu.
2. Change the settings as desired making sure not to duplicate an existing Item Name or VPI/VCI setting.
3. Click the **Modify** button. The modified PVC profile will appear with the new settings in the Existing Entry Table.
4. Click the **Apply** button to put the change into effect. After a few second you will be prompted to save the changes and restart or continue to make other changes to the Router's configuration.

**To delete an exiting PVC:**

1. Select the index number of the PVC profile you want to delete with the Select index to set drop-down menu.
2. Click the **Delete** button. The PVC profile will disappear from the Existing Entry Table.
3. Click the **Apply** button to put the change into effect. After a few second you will be prompted to save the changes and restart or continue to make other changes to the Router's configuration.



## Configuring LAN IP Settings

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

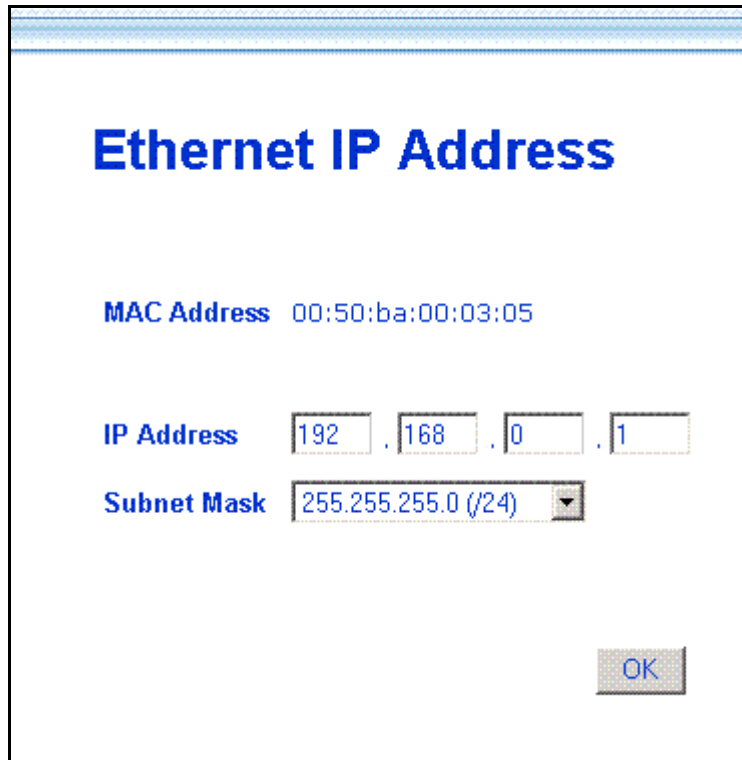
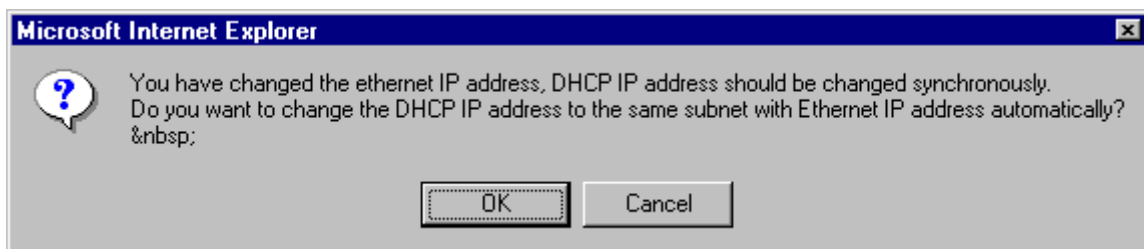


Figure 4 - 3. Ethernet IP Address Menu

The Ethernet IP Address displays the current LAN IP settings of the Router. To change the IP address, type in the new LAN **IP Address** in the space provided and select a **Subnet Mask** from the drop-down menu. Click on the **OK** button. If DHCP is enabled, a screen prompt will appear:



If you will continue to use the DHCP function, click the **OK** button. Otherwise you will need to manually configure the DHCP server addresses to reflect the change.

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

## Layer 2 Filtering

The Layer 2 Filter function of the Router can be configured to drop a number of packets types as they are encountered on either interface. This is especially useful is the Router is configured to operate as a simple bridge.

The packet types that can be filtered are the following:

- **ARP**
- **PPPoE**
- **IP Multicast**
- **IPv6 Multicast**
- **IP Broadcast** (blocked by default)
- **RARP** (blocked by default)
- **IPX**
- **NetBEUI**
- **Appletalk**
- **IEEE 802.1Q packets** (blocked by default)
- **Bridge Management Information**

A check mark in the box indicates the packet type will be passed. Any packet types that are not checked will be dropped by the Router. Select the packet type you want to allow to pass and click the **OK** button.



Figure 4 - 4. Layer 2 Filtering

## Proxy DNS Settings

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

The screenshot shows a web-based configuration interface for Proxy DNS. The title is "Proxy DNS". Below the title, there are three settings:

- Proxy DNS:** A dropdown menu currently showing "enabled".
- Get DNS IP automatically:** A checkbox that is checked.
- DNS Server IP:** Four input boxes, each containing a "0", separated by dots, representing an IP address.

An "OK" button is located at the bottom right of the form.

Figure 4 - 5. Proxy DNS Menu

The Proxy DNS Menu presents the following user defined parameters:

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

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

## DHCP Configuration

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

The screenshot shows the 'DHCP Configuration on LAN' web interface. It contains the following fields and values:

- Start IP Address: 192 . 168 . 0 . 2
- End IP Address: 192 . 168 . 0 . 33
- Netmask: 255.0.0.0 (/8)
- Default Gateway: 192 . 168 . 0 . 1
- Leased Time: 72 hour
- Primary DNS: 192 . 168 . 0 . 1
- Secondary DNS: 0 . 0 . 0 . 0
- Primary WINS: 0 . 0 . 0 . 0
- Secondary WINS: 0 . 0 . 0 . 0
- Domain Name: (empty)
- State: enabled

An 'OK' button is located at the bottom right of the form.

Figure 4 - 6. DHCP Configuration Menu

Configure LAN DHCP services by defining the following parameters:

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

## NAT Configuration

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

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

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

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

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

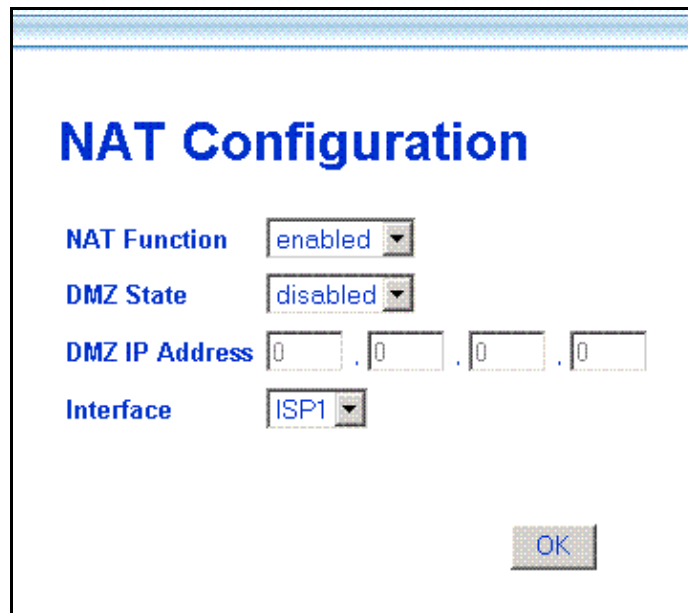


Figure 4 - 7. NAT Configuration Menu

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

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

## DMZ IP Address

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

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

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

## IP Masquerade Pass Through

Since certain protocols have difficulty operating in conjunction with NAT, the Router can forward these packets without subjecting them to NAT address mapping. In particular, IPsec (a special network security protocol) and PPTP (a tunneling protocol used for virtual private networks) are not compatible with NAT. For this reason, the Router is configured to allow them to pass by default. You may disable this using the IP Masquerade Pass Through menu. To block in effect either packet type while NAT is running you must deselect the type here and click the **OK** button.

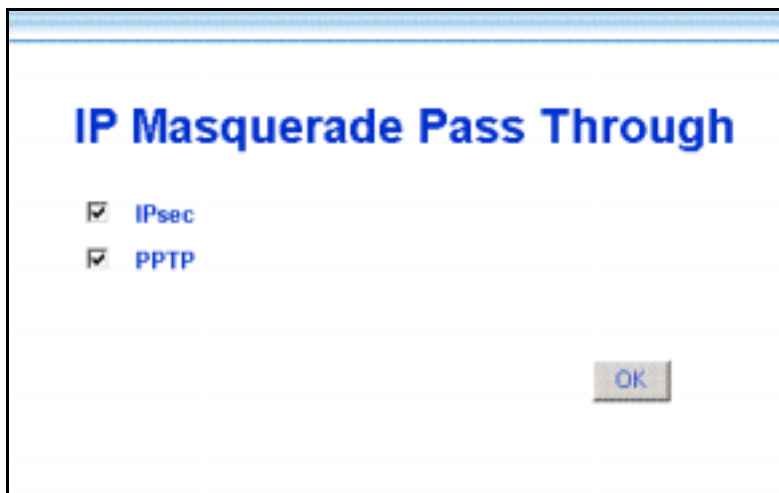


Figure 4 - 8. IP Masquerade Pass Through

## IP Masquerade Timer

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

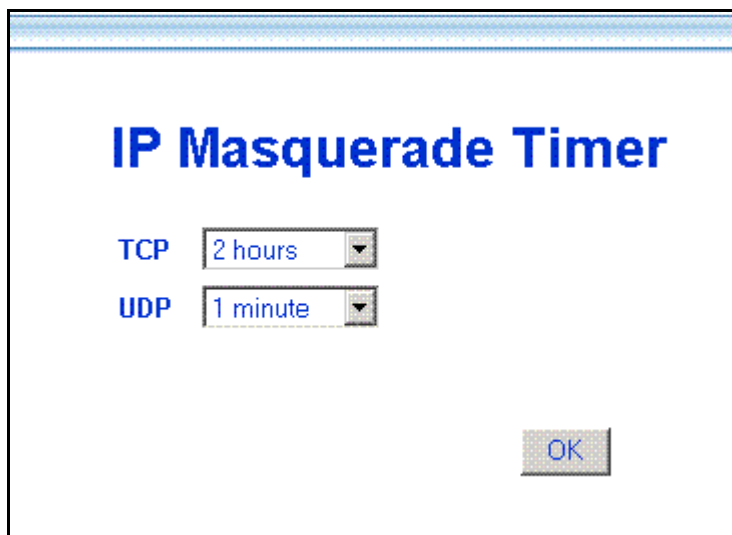


Figure 4 - 9. IP Masquerade Timer

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

## Port Redirection

### Port Redirection

Port Redirection State

Existing Entry 2

Valid Entry 2

The entries in gray color are mapped by UPnP.

Index	State	Protocol	Internet		Local
			Start Port	End Port	Local IP Address
1	enabled	TCP	23	23	192.168.0.2
2	enabled	TCP	80	80	192.168.0.3

---

Select index to set

State

Protocol

Internet

Start Port

End Port

Local IP Address  .  .  .

**Figure 4 - 10. Port Redirection Menu**

The Port Redirection feature of the Router is used in conjunction with NAT or IP Masquerading to improve security and efficiency. Port redirection can be used to direct potentially hazardous packets to a proxy server outside your firewall. For example, you can configure the Router to direct HTTP packets to a designated HTTP server in the DMZ. Other common applications might include directing incoming SMTP packets to an Email server for data scrutiny and improved network efficiency.

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

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



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

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

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

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

## Static Route Configuration

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

**Static Route Configuration**  
 Existing Entry: 2  
 Valid Entry: 2  
 [Apply]

Index	State	Item Name	IP Address/Subnet Mask	Gateway	Interface	Metric
1	enabled	San Diego	172.156.12.8/8	172.156.25.2	ISP1	0
2	enabled	Chicago	172.184.12.88/32	172.224.75.42	ISP1	0

Select index to set: 2 [Modify] [Delete] [Clear]

Item Name: Chicago  
 State: enabled  
 IP Address: 172 . 184 . 12 . 88  
 Subnet Mask: 255.255.255.255 (/32)  
 Gateway: 172 . 224 . 75 . 42  
 Interface: ISP1  
 Interface:   
 Metric: 0  
 [Add]

Figure 4 - 11. Static Route Configuration Table

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

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

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

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

## Advanced Filter & Firewall

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

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

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

Figure 4 - 12. Filter & Firewall Main Menu

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

Define these variables for each filter rule:

<b>Select index to set</b>	When adding a new rule, choose the <i>Not selected</i> option from the drop-down menu first. This will automatically assign the next available index number to the new rule. If you are deleting or modifying an existing rule, select it and click the appropriate button to the right.
<b>Item Name</b>	Name filtering rule defined here.
<b>State</b>	Select <i>Enabled</i> to start using the static route when it is applied. To save a route you do not want to use now for later use without deleting it you can choose <i>Disabled</i> .
<b>Pass or Block</b>	Choose <i>Block</i> to drop packets as defined by the rule. The default <i>Pass</i> will route data without restriction as a normal packet.
<b>Interface</b>	Choose Ethernet or select a WAN interface. If you have a single PVC and have not modified the name of the WAN interface, it appears here as ISP1 (the default name for the WAN interface).
<b>Protocol</b>	Select <i>ICMP</i> , <i>TCP</i> , <i>UDP</i> or <i>All</i> to pass or block packets of that protocol type.
<b>Source</b>	Type in the source IP address and select the Subnet Mask to pass or block packets form that IP address.
<p>&lt; specifies the port numbers less than and equal to the Start Port number</p> <p>&gt; specifies the port numbers greater than and equal to the Start Port number</p> <p>= sets the port number equal to the Start Port if there is no End Port specified; if an End Port number is specified, this defines a range of ports to filter. The range is defined as the port numbers between the Start Port and End Port, including the Start and End Port numbers.</p>	
<b>Start Port</b>	For a range of ports, this will be the first port in the range. For a single port enter the port number.
<b>End Port</b>	For a range of ports, this will be the last port in the range. For a single port just enter the same port number entered in Start Port.
<b>Destination</b>	Type in the destination IP address and select the Subnet Mask to pass or block packets destined to that IP address.

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

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

## RIP

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

Index	Interface	Send	Accept
1	ethernet	None	None
2	ISP1	None	None

Interface: ethernet

Send: None

Accept: None

Figure 4 - 13. RIP Menu

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

## Date & Time Settings

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

**Date / Time**

NTP State: Set device time with local PC time

NTP Server IP: 133 . 100 . 0 . 29

Timezone: GMT+09:00

---

**System time of the modem**

Date: 08 / 31 / 2002

Time: 15 : 16 : 37

Set Time

**Figure 4 - 14. Date & Time Configuration**

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

1. Make sure *NTP enabled* is displayed in the **NTP State** drop-down menu.
2. Type in an NTP server IP address that can be used by the Router. Keep in mind that many NTP servers require permission before they may be used.
3. Select the **Time Zone** where the Router is located or the time zone you want to use for system time. Time zones are displayed as GMT (Greenwich Mean Time) plus or minus hours incremented by whole hours.
4. Click the **Set Time** button to set the time with the chosen NTP server. This will send a request to update system time and date. NTP update packets are sent periodically to ensure precision.

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

1. Select *Set time with local PC time* in the **NTP State** drop-down menu.
2. Click the **Set Time** button to set the time with your computer.

## UPnP

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

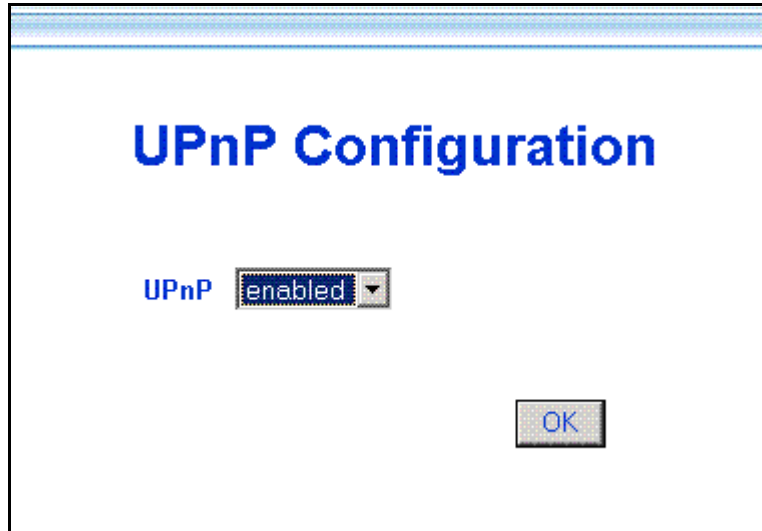


Figure 4 - 15. UPnP Configuration

## System Maintenance

The Maintenance folder in the web manager contains links to menus used for system maintenance functions including firmware upgrade and username/password configuration.

### ATM Loopback Test

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

Figure 4 - 16. ATM Loopback Screen

To perform the test, define the following parameters:

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

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



## System Username and Password

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



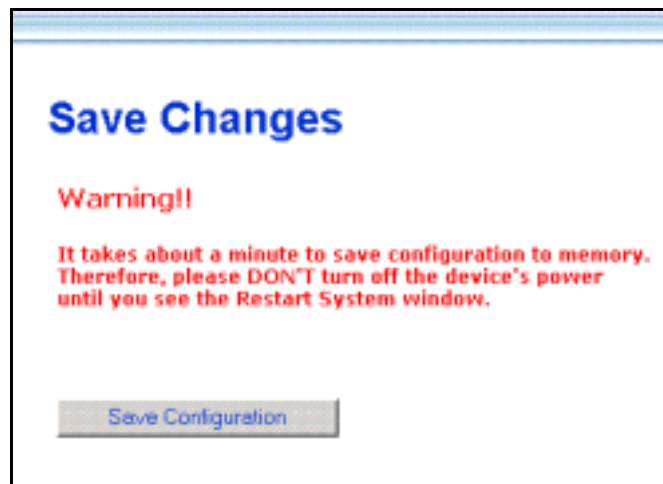
The screenshot shows a web interface titled "System Username and Password". It features four text input fields stacked vertically. The first field, labeled "User Name", contains the text "admin". The other three fields, labeled "Old Password", "New Password", and "Confirm New Password", are empty. At the bottom right of the form is a button labeled "OK".

Figure 4 - 17. System User Name and Password Menu

- 1 Type the current **User Name** in the entry field provided.
- 2 Type in the current password in the **Old Password** entry field.
- 3 Type in the **New Password** in the entry field provided.
- 4 Type in the new password again in the **Confirm New Password** field.
- 5 Click the **OK** button. The *Save changes and reboot system?* message appears.

## Save Changes

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



The screenshot shows a warning dialog box titled "Save Changes". The text inside reads: "Warning!! It takes about a minute to save configuration to memory. Therefore, please DON'T turn off the device's power until you see the Restart System window." At the bottom of the dialog is a button labeled "Save Configuration".

Figure 4 - 18. Save Changes Menu

## Factory Reset

The DSL-504 can be reset to the default configuration for all settings using the Factory Reset option. This will also change the both the LAN and WAN IP address of the device, so these will need to be reconfigured accordingly.

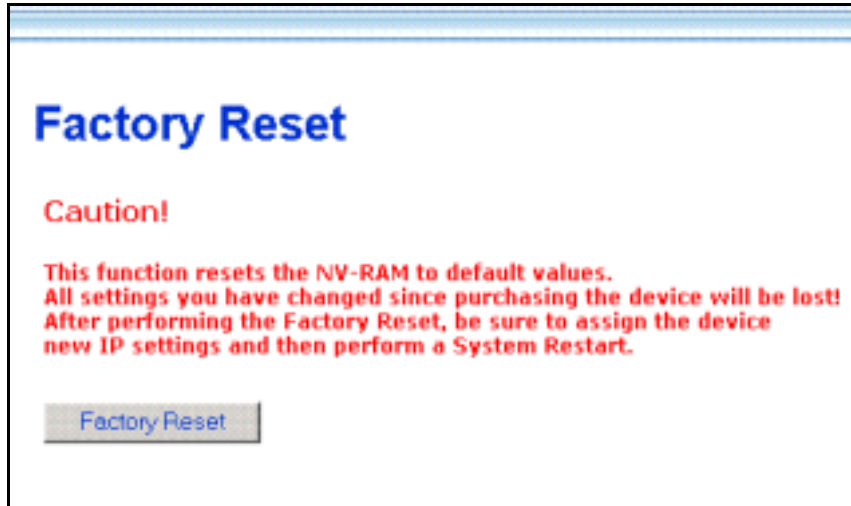


Figure 4 - 19. Factory Reset Screen

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

## Update Firmware

Use the Update Firmware feature to load the latest firmware for the device. You can obtain the latest version of the DSL-504 firmware by logging onto the D-Link web site at [www.dlink.com](http://www.dlink.com). Access the D-Link web site by clicking on the D-Link logo in the upper left corner of the browser window. Save the latest firmware version to a file on your computer or an accessible TFTP server.



Figure 4 - 20. Update Firmware Screen

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

## Configuration File Maintenance

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

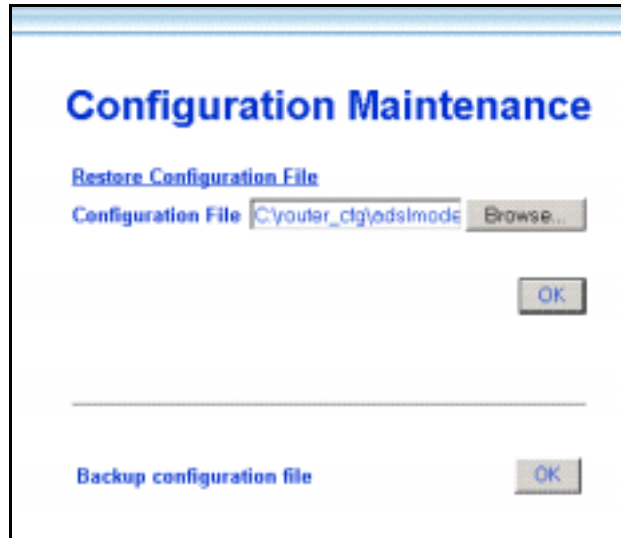


Figure 4 - 21. Configuration Maintenance Screen

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

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

## Remote Administration Access

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

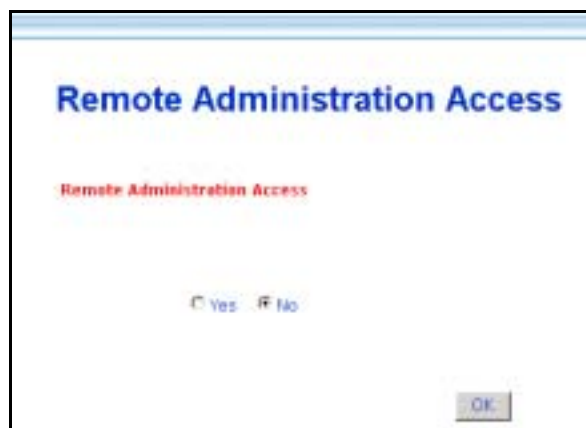


Figure 4 - 22. Remote Administration Access

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

## ADSL Line Setting

If your ADSL connection is disconnected or the connection is faulty, you can try to reconnect using the ADSL Line Setting menu. The ADSL/Link LED Indicator will light green if you have a viable ADSL link. You can also look at the Summary statistics and Line Condition windows to diagnose problems with the ADSL connection.

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

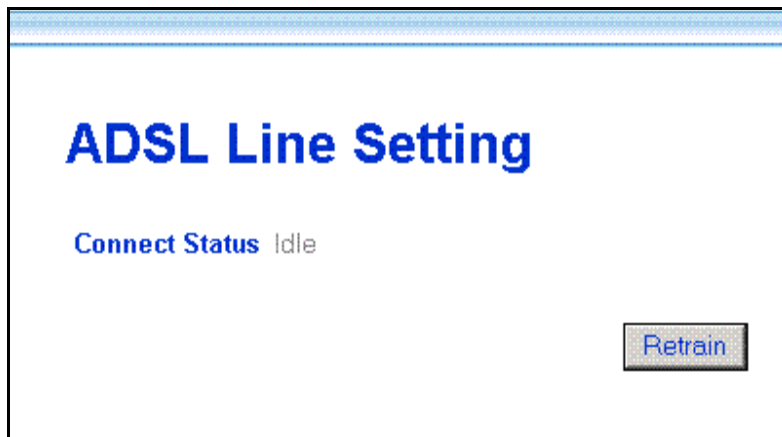


Figure 4 - 23. ADSL Line Retrain

<b>Connection Status</b>	<i>disconnected</i> indicates an ADSL connection failure <i>idle</i> indicates a valid connection that is currently not active <i>active</i> indicates a valid connection that currently is transmitting packets
--------------------------	--

## Summary

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

### System Summary

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

Summary					
<b>Multiple PVC</b>					
Index	Item Name	Interface	VPI	VCI	Encapsulation
1	ISP1	ppp_device	0	35	PPPoA LLC
<b>IP Address Configuration</b>		<b>IP Address</b>	192.168.0.1		
		<b>Subnet Mask</b>	255.255.255.0		
		<b>MAC Address</b>	00:50:ba:00:03:05		
<b>Proxy DNS</b>			enabled		
		<b>Get DNS IP automatically</b>	enabled		
		<b>DNS Server IP</b>	0.0.0.0		
<b>DHCP Configuration</b>			enabled		
<b>UPnP State</b>			enabled		
<b>NAT Configuration</b>			enabled		
<b>DMZ State</b>			disabled		
<b>IP Filter State</b>			disabled		
<b>Date / Time</b>			disabled		
<b>Event Log</b>			enabled		
<b>Remote Administration Access</b>			disabled		

Figure 4 - 24. System Summary

See the Summary description on the following page.

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

## DHCP Allocation Table

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

The screenshot shows a window titled "DHCP Allocation Table" with a table header containing the following columns: Index, MAC Address, IP Address, Computer Name, and Leased Time.

Index	MAC Address	IP Address	Computer Name	Leased Time
-------	-------------	------------	---------------	-------------

Figure 4 - 25. DHCP Allocation Table

Information listed in the DHCP Allocation Table includes the following:

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

## Port Redirection Summary

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

The screenshot shows a window titled "Port Redirection Summary" with a note: "The entries in gray color are mapped by UPnP." Below the note is a table with the following data:

Index	Protocol	Internet		Local
		Start Port	End Port	Local IP Address
1	TCP	23	23	192.168.0.2
2	TCP	80	80	192.168.0.3

Figure 4 - 26. Port Redirection Summary

## Runtime Routing Table

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

Index	Item Name	Subnet	Gateway	Interface	Metric
1	ethernet	10.0.0.0/8	0.0.0.0	ethernet	1
2	ppp_device	200.7.7.0/24	0.0.0.0	ISP1	1
3	ppp_route	0.0.0.0/0	0.0.0.0	ISP1	1

Figure 4 - 27. Runtime Routing Table

Information listed in the Runtime Routing Table includes the following:

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

## Filter and Firewall Summary

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

Index	Item Name	Pass or Block	Interface	Protocol	Source			Destination		
					IP Address/ Subnet Mask	Start Port	End Port	IP Address/ Subnet Mask	Start Port	End Port
1	adsfasd	Pass	ethernet	ICMP	3.3.3.3/24	0	0	3.3.3.3/32	0	0
2	ddd	Pass	ISP1	ICMP	33.33.33.3/24	0	0	3.3.33.3/32	0	0

Figure 4 - 28. Filtering & Firewall Summary



## Line Condition

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

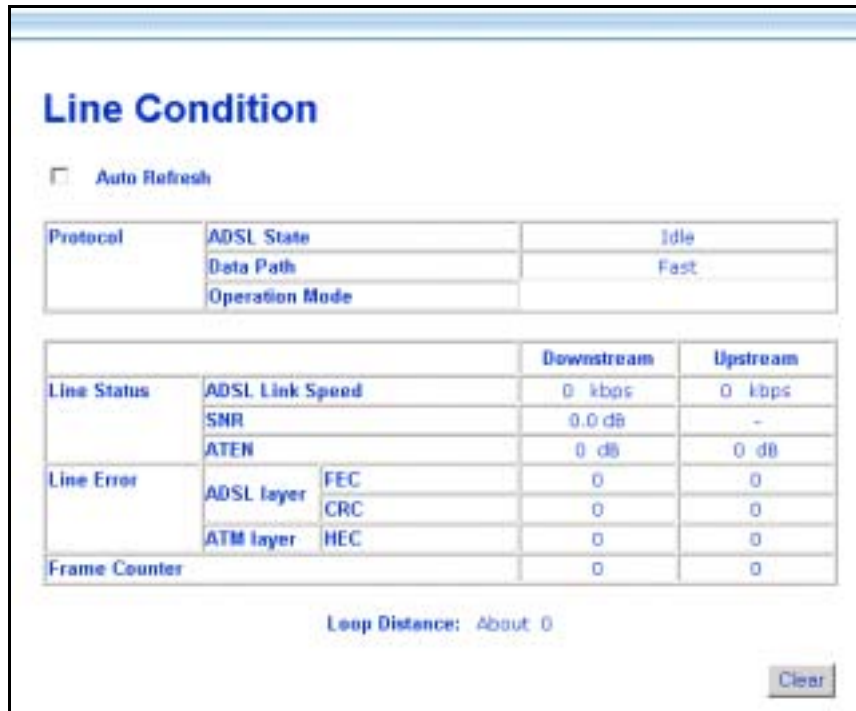


Figure 4 - 29. Line Condition

<b>Protocol</b>	<b>ADSL State</b>	<i>Disconnected</i> - ADSL connection failure <i>Idle</i> - valid connection currently not active <i>Active</i> - valid connection that currently transmitting packets
	<b>Data Path</b>	Current data path type Fast or Interleaved
	<b>Operation Mode</b>	Modulation technique used for ADSL connection, G.DMT or G.lite
<b>Link Status</b>	<b>ADSL Link Speed</b>	Downstream/Upstream data transfer rate in Kbps
	<b>SNR</b>	Downstream/Upstream Signal-to-Noise Ratio in dB
	<b>ATTEN</b>	Downstream/Upstream attenuation of signal in dB
<b>Line Error</b>	<b>FEC</b>	FEC Forward Error Correction
	<b>CRC</b>	CRC Cyclic Redundancy Control
	<b>HEC</b>	HEC Header Error Check
<b>Frame Counter</b>	Number of data packets received and transmitted	
<b>Loop Distance</b>		Loop in K ft. (range = 0 – 18 K ft.)

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

## Carrier Chart

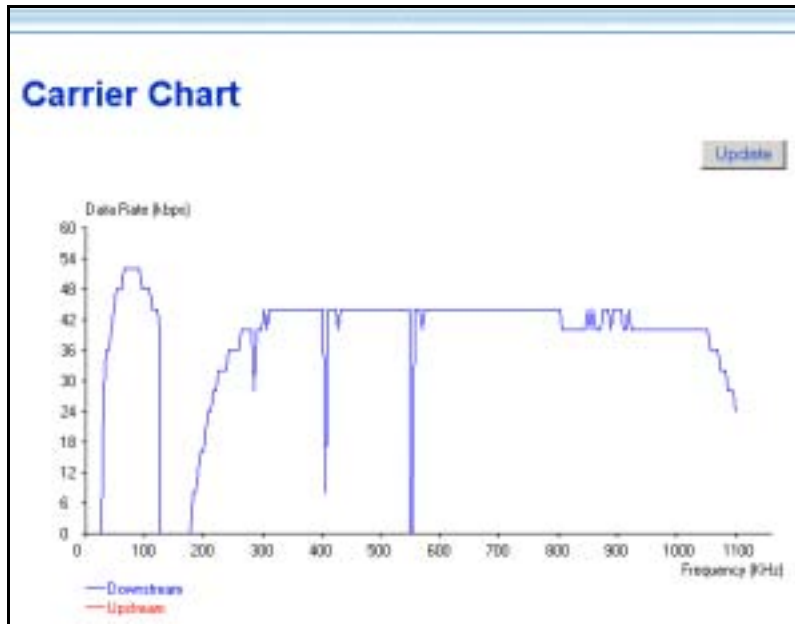


Figure 4 - 30. Carrier Chart

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



## Technical Specifications

GENERAL		
<b>STANDARDS:</b>	<ul style="list-style-type: none"> <li>• ITU G.992.1 (G.dmt)</li> <li>• ITU G.992.2 (G.lite)</li> <li>• ITU G.994.1 (G.Hs)</li> <li>• ITU-T Rec. I.361</li> <li>• ITU-T Rec. I.610</li> <li>• IEEE 802.3</li> <li>• IEEE 802.3u</li> <li>• IEEE 802.1d</li> <li>• RFC 791 (IP Routing)</li> <li>• RFC 792 (UDP)</li> <li>• RFC 826 (ARP)</li> <li>• RFC 1058 (RIP 1)</li> <li>• RFC 1389 (RIP 2)</li> <li>• RFC 1213 compliant</li> <li>• RFC 1483 (Bridged Ethernet)</li> <li>• RFC 1577 (IP over ATM)</li> </ul>	<ul style="list-style-type: none"> <li>• RFC 1661 (PPP)</li> <li>• RFC 1994 (CHAP)</li> <li>• RFC 1334 (PAP)</li> <li>• RFC 2364 (PPP over ATM)</li> <li>• RFC 1631 (NAT)</li> <li>• RFC 1877 (Automatic IP assignment)</li> <li>• RFC 2516 (PPP over Ethernet)</li> <li>• Supports RFC 2131 and RFC 2132 (DHCP)</li> <li>• Compatible with all T1.413 issue 2 (full rate DMT over analog POTS), and CO DSLAM equipment</li> <li>• Supports ATM Forum UNI V3.1 PVC</li> </ul>
<b>PROTOCOLS:</b>	TCP/IP UDP RIP-1 RIP-2 IGMP	DHCP BOOTP ARP AAL5
<b>DATA TRANSFER RATE:</b>	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	
<b>MEDIA INTERFACE EXCHANGE:</b>	RJ-11 port ADSL telephone line connection RJ-45 port for 10BASET Ethernet connection RS-232 (DB9 female) console port for local configuration	

Physical and Environmental	
DC inputs:	Input: 100V ~ 240V AC 50 ~ 60Hz
Power Adapter:	Output: 7.5V DC 1A
Power Consumption:	5 Watts (max)
Operating Temperature:	0° to 40° C (32° - 104° F)
Humidity:	5 to 95% (non-condensing)
Dimensions:	190 mm x 116.8 mm x 30.9 mm
Weight:	360 gm
EMI:	CE Class B FCC Class B
Safety:	UL/CUL TUV
Reliability:	Mean Time Between Failure (MTBF) min. 4 years



## LAN IP Setup

The DSL-504 is designed to provide network administrators maximum flexibility for IP addressing on the Ethernet LAN. The easiest IP setup choice in most cases is to let the Router do it using DHCP, which is enabled by default. This appendix briefly describes various options including DHCP, used for IP setup on a LAN. If you are new to IP networking, the next appendix provides some background information on basic IP concepts.

### ***Assigning Network IP Addresses***

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

### **Using the Default IP Address**

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

### **Manual IP Address Assignment**

Manually configuring IP settings for the LAN means you must manually set an IP address, subnet mask and IP address of the default gateway (the Router's IP address) on each networked computer. The example listed below describes IP configuration for computers running Windows 98 or Windows 95. Regardless of what operating system is used on each workstation, the three network IP settings must be defined so the network interface used by each workstation can be identified by the Router, and vice versa. For detailed information about configuring your workstations IP settings, consult the user's guide included with the operating system or the network interface card (NIC).

1. In Windows 95/98, click on the **START** button, go to **Settings** and choose **Control Panel**.
2. In the window that opens, double-click on the **Network** icon.
3. Under the Configuration tab, select the **TCP/IP** component and click *Properties*.
4. Choose the *Specify an IP address* option and edit the address settings accordingly. Consult the table below for IP settings on a Class C network.

Using Default IP without DHCP			
Host	IP Address	Subnet Mask	Gateway IP
<b>Router</b>	192.168.0.1	255.255.255.0	
<b>Computer #1</b>	192.168.0.2	255.255.255.0	192.168.0.1
<b>Computer #2</b>	192.168.0.3	255.255.255.0	192.168.0.1
<b>Computer #3</b>	192.168.0.4	255.255.255.0	192.168.0.1

### **LAN IP Setup - Example #1**

Please note that when using the default IP address as in the above example, the first three numbers in the IP address must always be the same with only the fourth number changing. The first three numbers define the network IP address (all machines must belong to the same IP network), while the last number denotes the host IP address (each computer must have a unique address to distinguish it on the network). The IP address scheme used in Example #1 can be used for any LAN that requires up to 253 separate IP addresses (excluding the Router). Notice that the subnet mask is the same for all machines and the default gateway address is the LAN IP address of the Router.

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

## **Using DHCP**

The second way to use the default settings is to allow the Router to automatically assign IP settings for workstation using DHCP. To do this, simply make sure your computers' IP addresses are set to 0.0.0.0 (under Windows, choose the option Obtain an IP address automatically in the TCP/IP network component described above). When the computers are restarted, their IP settings will automatically be assigned by the Router. The Router is set by default to use DHCP. See the discussion in Chapter 4 for information on how to use configure the Router for DHCP.

## **Changing the IP Address of the Router**

When planning your LAN IP address setup, you may use any scheme allowed by rules that govern IP assignment. It may be more convenient or easier to remember an IP scheme that use a different address for the Router. Or you may be installing the Router on a network that has already established the IP settings. Changing the IP address is a simple matter and can be done using the web manager. If you are incorporating the Router into a LAN with an existing IP structure, be sure to disable the DHCP function. Also, consider the effects of the NAT function which is enable by default.

An IP addressing scheme commonly used for Ethernet LANs establishes 10.0.0.1 as the base address for the network. Using Example #2 below, the Router is assigned the base address 10.0.0.1 and the remaining addresses are assigned manually or using DHCP.

<b>Alternative IP Assignment</b>			
<b>Host</b>	<b>IP Address</b>	<b>Subnet Mask</b>	<b>Gateway IP</b>
<b>Router</b>	10.0.0.1	255.255.255.0	
<b>Computer #1</b>	10.0.0.2	255.255.255.0	10.0.0.1
<b>Computer #2</b>	10.0.0.3	255.255.255.0	10.0.0.1
<b>Computer #3</b>	10.0.0.4	255.255.255.0	10.0.0.1

### **LAN IP Setup - Example #2**

These two examples are only examples you can use to help you get started. If you are interested in more advanced information on how to use IP addressing on a LAN there are numerous resources freely available on the Internet. There are also many books and chapters of books on the subject of IP address assignment, IP networking and the TCP/IP protocol suite.



## IP Concepts

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

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

### IP Addresses

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

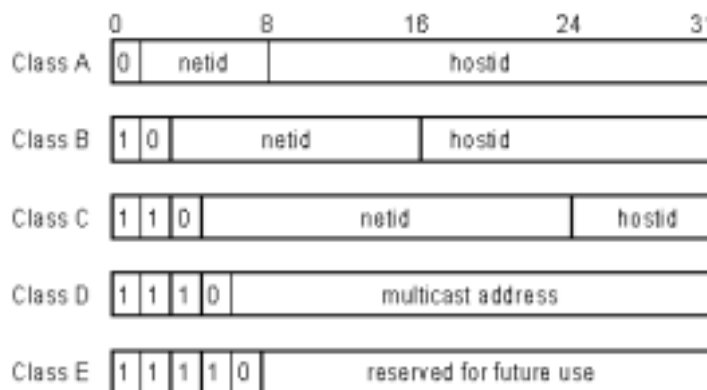
To make IP addresses easy to understand, the originators of IP adopted a system of representation called “dotted decimal” or “dotted quad” notation. Below are examples of IP addresses written in this format:

201.202.203.204      189.21.241.56      125.87.0.1

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

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

IP networks are divided into three classes on the basis of size. A full IP address contains a network portion and a “host” (device) portion. The network and host portions of the address are different lengths for different classes of networks, as shown in the table below.



Networks attached to the Internet are assigned class types that determine the maximum number of possible hosts per network. The previous figure illustrates how the net and host portions of the IP address differ among the three classes. Class A is assigned to networks that have more than 65,535 hosts; Class B is for networks that have 256 to 65534 hosts; Class C is for networks with less than 256 hosts.

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

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

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

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

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

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

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

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

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

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

<b>Class</b>	<b>Beginning Address</b>	<b>Ending Address</b>
A	10.0.0.0	10.255.255.255
B	172.16.0.0	172.31.255.255
C	192.168.0.0	192.168.255.255



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

## **Subnet Mask**

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

<b>IP Class</b>	<b>Subnet Mask</b>
Class A	255.0.0.0
Class B	255.255.0.0
Class C	255.255.255.0

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



## DSL-504 Firmware Upgrade Utility

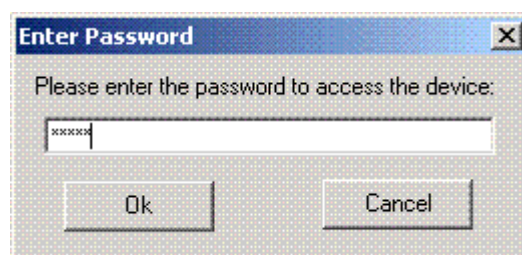
You can update system firmware using the DSL-504 Firmware Upgrade Utility. To upgrade the Router's firmware, first install the Upgrade Utility software on a computer running a Windows operating system. Install the utility by clicking the file titled **setup.exe** located on the Installation CD-ROM. It will be installed automatically. It is recommended that the PC be directly connected to the Router using a crossed cable, however you may upgrade it through the LAN from a remote host.

You also need to download the latest firmware version file from the D-Link web site to the PC on which you will use the Upgrade Utility. Instructions for downloading the firmware are located on the web site at [www.dlink.com](http://www.dlink.com) or your local D-Link URL. For URL web addresses for all D-Link offices worldwide, see the address list at the end of this document.

To launch the DSL-504 Firmware Upgrade Utility, click on the icon. Allow a few moments for the software to discover the Router on the network. After the discovery phase the following window will appear. You will see all the DSL-504 Routers on your network. You can identify individual devices by either its IP address or its MAC address. Select the device you wish to upgrade by double clicking on it.

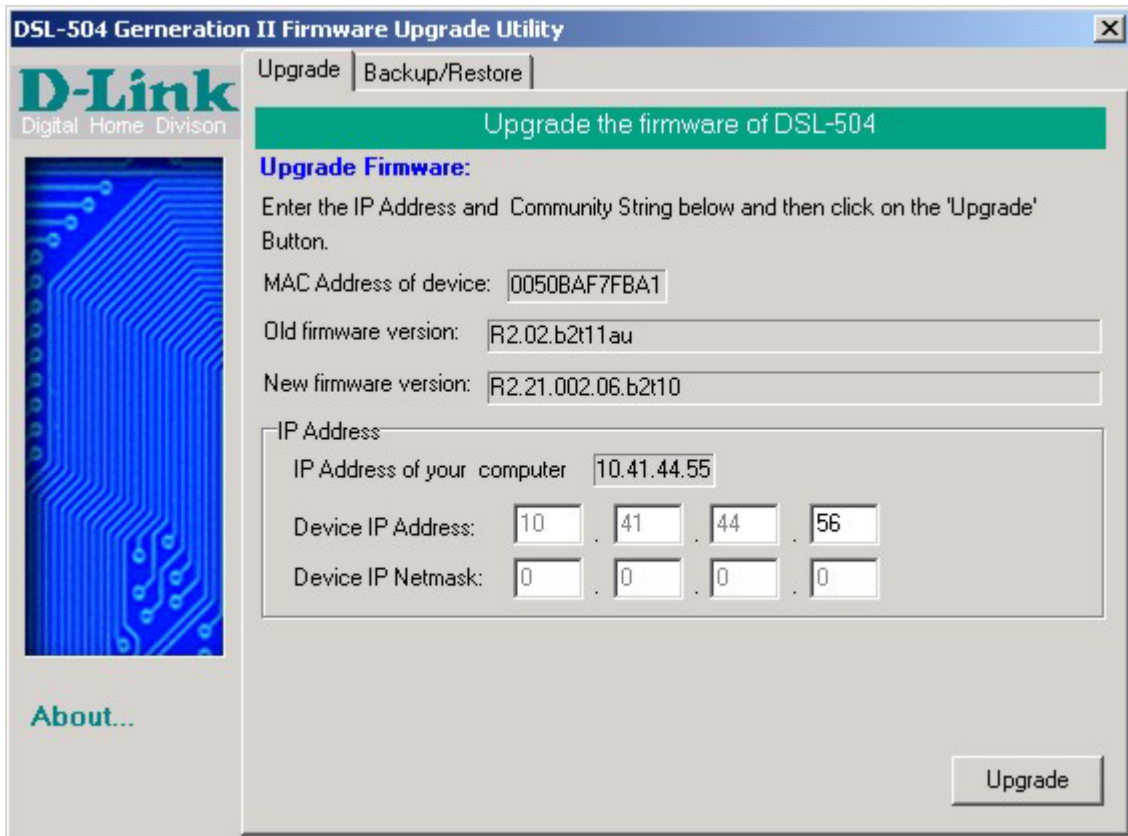


When you select a Router to upgrade you will be prompted for a password. The default password is **admin**. If you want to change the password, you can change it using the console manager interface as described in Chapter 4.

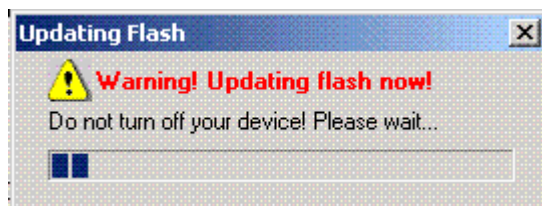


Enter the password and click OK.

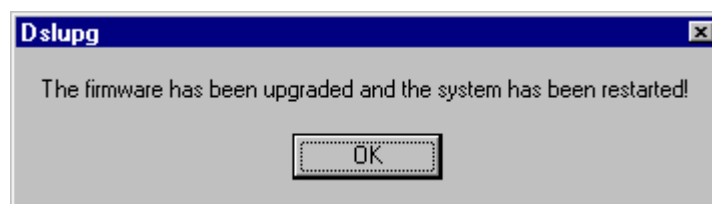
In the new window you will see the MAC address of the Router and the IP address of the PC you are using. The PC and the Router must be on the same subnet for the upgrade to be completed. The upgrade utility will suggest a new IP address to be temporarily assigned to the device during the firmware upgrade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



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



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





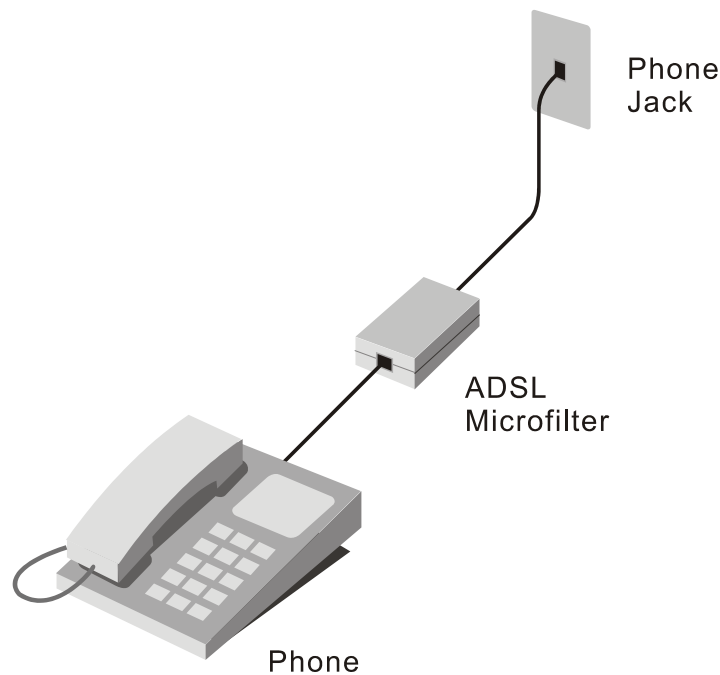
## Microfilters and Splitters

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

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

### Microfilters

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



**Microfilter Installation**

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

## Line Splitter

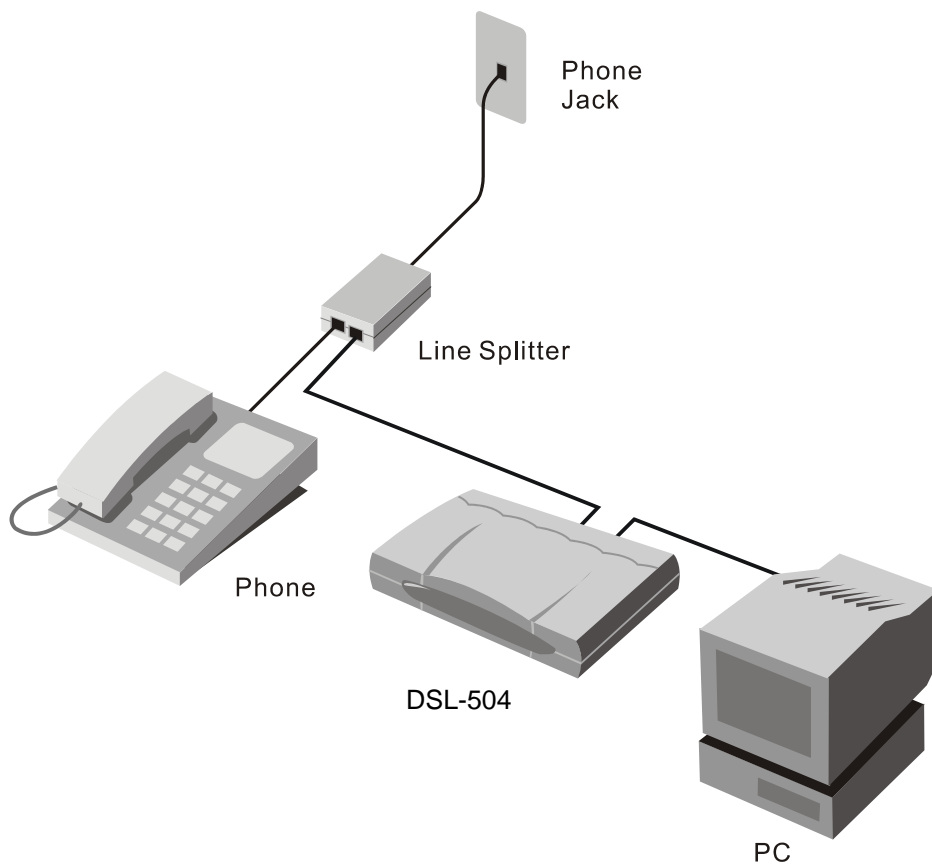
If you are instructed to use a “line splitter”, you must install the device between the Router and the phone jack. Use standard telephone cable with standard RJ-11 connectors. The splitter has three RJ-11 ports used to connect to the wall jack, the Router and if desired, a telephone or telephone device. 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 splitter.



**Line Splitter 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 Goyechea 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: liwei@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**  
4<sup>th</sup> 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?** \_\_\_\_\_

\_\_\_\_\_  
 \_\_\_\_\_  
 \_\_\_\_\_

PLEASE  
PLACE STAMP  
HERE

**TO:**

---

---

---

**D-Link®**