D-Link®

DSL-604+

802.11b Wireless ADSL Router

User's Guide

Wichtige Sicherheitshinweise

1. Bitte lesen Sie sich diese Hinweise sorgfältig durch.

2. Heben Sie diese Anleitung für den spätern Gebrauch auf.

3. Vor jedem Reinigen ist das Gerät vom Stromnetz zu trennen. Vervenden Sie keine Flüssig- oder Aerosolreiniger. Am besten dient ein angefeuchtetes Tuch zur Reinigung.

4. Um eine Beschädigung des Gerätes zu vermeiden sollten Sie nur Zubehörteile verwenden, die vom Hersteller zugelassen sind.

5. Das Gerät is vor Feuchtigkeit zu schützen.

6. Bei der Aufstellung des Gerätes ist auf sichern Stand zu achten. Ein Kippen oder Fallen könnte Verletzungen hervorrufen. Verwenden Sie nur sichere Standorte und beachten Sie die Aufstellhinweise des Herstellers.

7. Die Belüftungsöffnungen dienen zur Luftzirkulation die das Gerät vor Überhitzung schützt. Sorgen Sie dafür, daß diese Öffnungen nicht abgedeckt werden.

8. Beachten Sie beim Anschluß an das Stromnetz die Anschlußwerte.

9. Die Netzanschlußsteckdose muß aus Gründen der elektrischen Sicherheit einen Schutzleiterkontakt haben.

10. Verlegen Sie die Netzanschlußleitung so, daß niemand darüber fallen kann. Es sollete auch nichts auf der Leitung abgestellt werden.

11. Alle Hinweise und Warnungen die sich am Geräten befinden sind zu beachten.

12. Wird das Gerät über einen längeren Zeitraum nicht benutzt, sollten Sie es vom Stromnetz trennen. Somit wird im Falle einer Überspannung eine Beschädigung vermieden.

13. Durch die Lüftungsöffnungen dürfen niemals Gegenstände oder Flüssigkeiten in das Gerät gelangen. Dies könnte einen Brand bzw. Elektrischen Schlag auslösen.

14. Öffnen Sie niemals das Gerät. Das Gerät darf aus Gründen der elektrischen Sicherheit nur von authorisiertem Servicepersonal geöffnet werden.

15. Wenn folgende Situationen auftreten ist das Gerät vom Stromnetz zu trennen und von einer qualifizierten Servicestelle zu überprüfen:

a – Netzkabel oder Netzstecker sint beschädigt.

b – Flüssigkeit ist in das Gerät eingedrungen.

c – Das Gerät war Feuchtigkeit ausgesetzt.

d – Wenn das Gerät nicht der Bedienungsanleitung ensprechend funktioniert oder Sie mit Hilfe dieser Anleitung keine Verbesserung erzielen.

e – Das Gerät ist gefallen und/oder das Gehäuse ist beschädigt.

f – Wenn das Gerät deutliche Anzeichen eines Defektes aufweist.

16. Bei Reparaturen dürfen nur Orginalersatzteile bzw. den Orginalteilen entsprechende Teile verwendet werden. Der Einsatz von ungeeigneten Ersatzteilen kann eine weitere Beschädigung hervorrufen.

17. Wenden Sie sich mit allen Fragen die Service und Repartur betreffen an Ihren Servicepartner. Somit stellen Sie die Betriebssicherheit des Gerätes sicher.

18. Zum Netzanschluß dieses Gerätes ist eine geprüfte Leitung zu verwenden, Für einen Nennstrom bis 6A und einem Gerätegewicht großer 3kg ist eine Leitung nicht leichter als H05VV-F, 3G, 0.75mm2 einzusetzen

Limited Warranty

Hardware:

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

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

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

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

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

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

Software:

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

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

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

D-Link Offices for Registration and Warranty Service

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

LIMITATION OF WARRANTIES

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

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

LIMITATION OF LIABILITY

Trademarks

Copyright Statement

FCC Warning

This device complies with part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

-Reorient or relocate the receiving antenna.

-Increase the separation between the equipment and receiver.

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

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

CE Mark Warning

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

TABLE OF CONTENTS

About This Guide

Thank you for choosing the DSL-604+ Wireless ADSL Router. The DSL-604+ will provide your small office or home network with convenient Internet access, rapid download speeds, improved network efficiency and enhanced security.

If you would like to set up the device quickly in order to verify that the ADSL connection to the WAN (wide area network) is working properly, please read the Quick Installation Guide included in the DSL-604+ package.

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

http://www.dlink.com/learnbasic/

and

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

Terminology

This document uses the terms "Router" (first letter upper case) to refer specifically to the DSL-604+ Router, and "router" (first letter lower case) to refer to all such devices including the DSL-604+. ADSL service is provided by different types of businesses including telephone service providers, Internet service providers and other businesses that provide computer network and telecommunications services. The term "service provider" is used in this guide to refer to any service that sells or leases DSL services and equipment.

Guide Overview

Chapter 1 Introduction: A description of the Router and its features. A brief introduction to ADSL and Wireless LAN technologies and standards are listed.

Chapter 2 Hardware Installation: Discusses how to connect the Router to an Ethernet LAN.

Chapter 3 First Time Setup: Provides information on how to configure the Router and establish the ADSL connection using the web-based manager.

Chapter 4 Web-based Management Guide: Describes how to use the web-based manager and the management options available.

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

Before You Start

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

Installation Overview

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

1. Gather information and equipment needed to install the device. Before you begin the actual installation make sure you have all the necessary information and equipment.

2. Install the hardware, that is, connect the cables (Ethernet and telephone) to the device and connect the power adapter to the device and a power source.

3. Check the IP settings on your computer and change them if necessary so the computer can access the web-based software built used to configure the Router

4. Use the web-based management software to configure the device to suit the requirements of your ADSL account and to communicate with 802.11b wireless devices.

Requirements for Installation

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

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 signal interference on the line. A low pass filter device may be required for each telephone that shares the line with the ADSL line. Alternatively, it may be necessary only to install such a device at or near the point where the Router connects to the telephone 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.

Operating System

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

Web Browser

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

Ethernet Port (NIC Adapter)

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

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. Various terms are to describe a bridged ADSL connection including the terms "Bridge LLV" and "Bridge VC Mux" 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 (encapsulation method) you have.

ISP ACCOUNT INFORMATION
User Name:
Password:

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 larger telecommunications network. Setting up these virtual connections must be coordinated with your ISP or telephone services provider. Typically multiple PVCs are used to form private connections to remote private networks or used for public web servers. Chapter 4 contains instruction on how to set up additional PVCs for accounts using more than one virtual connection.

802.11b Wireless LAN Configuration

All the 802.11b wireless LAN settings are configured on a single page using the web-based manager. For basic wireless communication you need to decide what channel to use and what SSID to assign. These two settings must be the same for any wireless workstations or other wireless access point that communicate with the DSL-604+ through the wireless interface.

Security for wireless communication can be accomplished using two methods. The DSL-604+ is supports WEP encryption at the 64 bit (also called 40 bit) or 128 bit level. Wireless access can be controlled by selecting MAC addresses that are allowed to associate with the device. Please read the section on Wireless Configuration in the Web-based Management Guide (Chapter 4).

Packing List

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

1. One DSL-604+ 802.11b Wireless ADSL Ethernet Router

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

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

4. One straight-through Ethernet cable

5. One AC power adapter suitable for your electric service

6. One Quick Installation Guide

1

Introduction

This chapter describes the Router and it features and includes brief introduction to ADSL and 802.11b Wireless LAN. Front and rear panel diagrams are used to illustrate the LED indicators and cable connections.

Router Description and Operation

The DSL-604+ ADSL Router is designed to provide a simple, cost-effective and secure ADSL Internet connection for wired (Ethernet) and wireless (802.11b) stations on your network. The DSL-604+ combines high-speed ADSL connection technology, TCP/IP routing and 802.11b wireless connectivity in one compact unit.

The Router is easy to install and use. The DSL-604+ connects to an Ethernet LAN via a standard Ethernet 10BASE-T interface using RJ-45 connectors. The ADSL connection is made using ordinary twisted-pair telephone line with standard RJ-11 connectors. This arrangement allows wired and wireless workstations to share network resources and connect to the Internet using a single WAN interface and IP address.

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

All the 802.11b wireless settings for the Router are entered on a single page in the web manager. Security for the wireless interface comes in two forms, WEP Encryption and MAC Address Control.

Product Features

The DSL-604+ ADSL Router utilizes the latest ADSL enhancements and router technologies to provide a robust Internet gateway suitable for most small to medium sized offices.

PPP (Point-to-Point Protocol) Security

The DSL-604+ ADSL Router supports PAP (Password Authentication Protocol) and CHAP (Challenge Handshake Authentication Protocol) for PPP connections.

DHCP Support (Dynamic Host Configuration Protocol)

DHCP (Dynamic Host Configuration Protocol) automatically and dynamically assigns al LAN IP settings to each host on your network. This eliminates the need to reconfigure every host whenever changes in network topology occur.

Network Address Translation (NAT)

For small office environments, the DSL-604+ 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-604+ 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-604+ 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-604+ supports *Bridged Ethernet over ATM* (RFC1483), *IP over ATM* (RFC1577) and *PPP over ATM* (RFC 2364). The Router can support up to eight Virtual Circuit Connections (VCCs).

Precise ATM Traffic Shaping

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

G.hs (Auto-handshake)

This allows the Router to automatically choose either the G.lite or G.dmt ADSL connection standards.

High Performance

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

Full Network Management

The DSL-604+ 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-604+ 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.

Wireless Features

- Fully IEEE 802.11b compatible.

- Wireless data rate up to 22 Mbps

- Direct Sequence Spread Spectrum technology

- Operating in the unlicensed 2.4 GHz ISM band

- Supports 64/128/256 bits WEP security and user authentication

- Efficient antenna provides a range of per cell operation up to 100 meter indoor

Standards Compatibility and Compliance

The DSL-604+ complies with or is compatible with the following standards as recognized by their respective agencies.

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

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

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

- ITU-T Rec. I.361 compliant

- ITU-T Rec. I.610 compliant

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

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

- RFC 2364 *PPP over ATM* compliant

- RFC 2516 *PPP over Ethernet* compliant

- RFC 1334 PPP Authentication Protocol compliant

- RFC 1994 Challenge Handshake Authentication Protocol compliant

- RFC 791 *Internet Protocol* compliant

- RFC 826 Address Resolution Protocol compliant

- RFC 950 Internet Control Message Protocol compliant

- RFC 1631 Net Address Translator compliant

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

- IEEE 802.3 compliant

- IEEE 802.3u compliant

- IEEE 802.1d compliant

- IEEE 802.3x compliant

- IEEE 802.11b compliant

- Supports RIP v1 and RIP v2

- Supports Static Routing

- Supports ATM Forum UNI V3.1 PVC

- Minimum ATM cell forwarding rate: 640 Kbps

- Supports up to eight simultaneous ATM virtual connections

Front Panel LED Display

Place the Router in a location that permits an easy view of the LED indicators on the front panel.
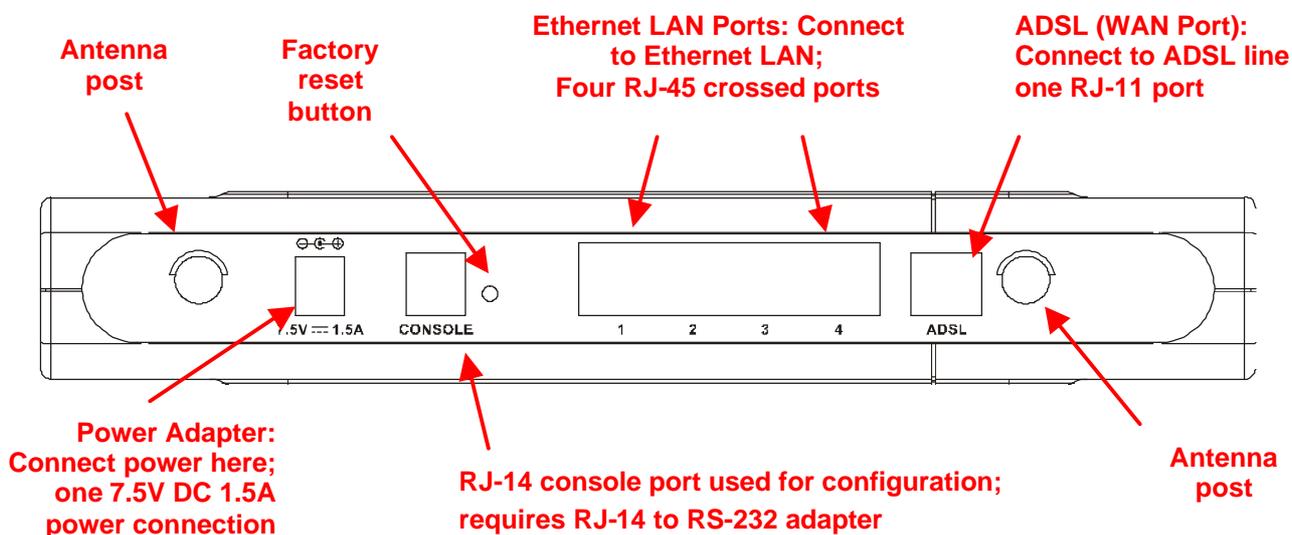
The LED indicators on the front panel include the Power, Status, ADSL Link/Activity, and WLAN indicators. Each Ethernet LAN port displays a pair of indicators for monitoring connection speed (10M/100M), link status and activity (Link/Act).
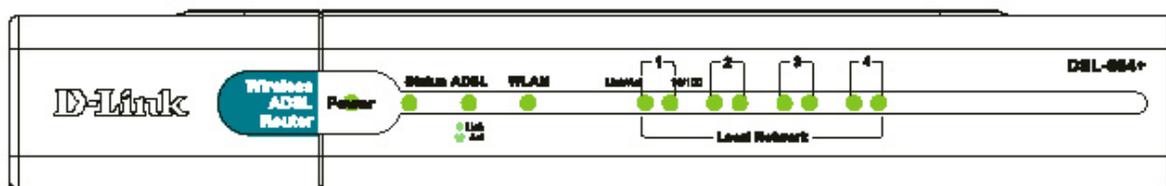
Power	Steady green light indicates the unit is powered on.
Status	Lights steady green during power on self-test. Once the connection status has been settled, the light will blink green.
ADSL: Link	Steady green light indicates a valid ADSL connection. This will light after the ADSL negotiation process has been settled.
ADSL: Act	Blinking green light indicates activity on the WAN interface.
WLAN	Blinking green light indicates activity on the WLAN.
Ethernet: 10M 100M	Steady green indicates a 100Mbps Fast Ethernet connection. For 10Mbps Ethernet connection it is dark.
Ethernet: Link Act	The rear panel of the Router provides access to the AC power adapter cord connection as well as the port connections.

Rear Panel Cable Connections

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

Antenna post

Factory reset button

Ethernet LAN Ports: Connect to Ethernet LAN; Four RJ-45 crossed ports

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

Power Adapter: Connect power here; one 7.5V DC 1.5A power connection

RJ-14 console port used for configuration; requires RJ-14 to RS-232 adapter

Antenna post

Introduction to 802.11b Wireless

The IEEE 802.11b standard is the most widely used standard for wireless LANs today. A wireless LAN (WLAN) is a cellular computer network that transmits data using radio signals instead of cables. WLAN technology is commonly used on home, small office and large corporate networks. WLAN devices have a high degree of mobility and flexibility that allow network to be quickly set up or dismantled and allow them to roam freely throughout the network.

Wireless LAN users can use the same network applications used on an Ethernet LAN. 802.11b adapter cards used on laptop and desktop computers support the same protocols as Ethernet adapter cards. For most users, there is no functional difference between a computer attached to a wired Ethernet LAN or a mobile 802.11b workstation except that hardware is not physically attached to the network. For most networks however, it may be desirable for mobile network devices to be able to link to the wired Ethernet LAN to use shared resources such as servers, printers or an Internet connection. The DSL-604+ unites Ethernet and 802.11b wireless private networks with an Internet connection. The DSL-604+ supports data rates of up to 22 Mbps for wireless operation when used in conjunction with other D-Link AirPlus devices.

D-Link Wireless LAN devices have earned a reputation for reliability, flexibility and value. D-Link offers a full range of IEEE 802.11b and IEEE 802.1a WLAN products including:

◆   802.11b and 802.11a Wireless Adapter cards for notebook computers
◆   802.11b and 802.11a Wireless PCI cards for desktop computers
◆   802.11b and 802.11a Wireless Access Points
◆   Dual-band (802.11b plus 802.11a) Wireless Access Points
◆   802.11b and 802.11a Wireless Home Gateways
◆   802.11b and 802.11a Wireless ADSL Routers

Wireless LAN Basics

Some basic understanding of 802.11b wireless technology and terminology when is useful when you are setting up the Router or any wireless access point. If you are not familiar with wireless networks please take a few minutes to learn the basics.

Radio Transmission

WLAN devices use electromagnetic waves within a broad, unlicensed range of the radio spectrum to transmit and receive radio signals. When a wireless access point is present, it becomes a base station for the WLAN nodes in its broadcast range. WLAN nodes transmit digital data using FM (frequency modulation) radio signals. WLAN devices generate a carrier wave and modulate this signal using various techniques. In this way, digital data can then be superimposed onto the carrier signal. This radio signal carries data to WLAN devices within range of the transmitting device. The antennae of WLAN devices listen for and receive the signal. The signal is demodulated and the transmitted data extracted. The transmission method used by the access point is called Direct Sequence Spread Spectrum (DSSS) and operates in a range of the radio spectrum between 2.4GHz and 2.5GHz for transmission. DSSS is preferred method used on many 802.11b devices.

Range

Range should not be a problem in most homes or small offices. If you experience low or no signal strength in some areas, consider positioning the device in a location between the WLAN devices maintaining a roughly equal straight-line distance to all devices that need to access the Router through the wireless interface. Adding more 802.11b access points to rooms where the signal is weak can improve signal strength. Read the section about placement of the Router titled Location in the next chapter, Hardware Installation, for more information.

SSID

Wireless networks use an SSID (Service Set Identifier) to allow wireless devices to roam within the range of the network. Wireless devices that wish to communicate with each other must use the same SSID. Several access

points can be set up using the same SSID so that wireless stations can move from one location to another without losing connection to the wireless network.

The DSL-604+ operates in *Infrastructure* mode. It controls network access on the wireless interface in its broadcast area. It will allow access to the wireless network to devices using the correct SSID after a negotiation process takes place. The DSL-604+ broadcasts its SSID so that any wireless station in range can learn the SSID and ask permission to associate with it. Many wireless adapters are able to survey or scan the wireless environment for access points. An access point in Infrastructure mode allows wireless devices to survey that network and select an access point with which to associate.

It is important to understand the difference between the SSID and a BSSID (Basic Service Set Identifier) or Preferred BSSID. The Preferred BSSID is defined by wireless stations to designate an access point used for access to the wireless network. The Preferred BSSID is the MAC address of the access point. Therefore any wireless stations (wireless clients) that use the DSL-604+ through the wireless interface must use its MAC address for the Preferred BSSID. A wireless stations that scans the network for available access points may present the user with a choice of access point identified by their BSSID.

ADSL Technology

Asymmetric Digital Subscriber Line (ADSL) is a broadband technology that utilizes ordinary copper telephone lines to enable high-speed digital data transmission and interactive multimedia applications for business and residential customers.

ADSL greatly increases the signal carrying capacity of copper telephone lines without interfering with regular telephone services for 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.

2

Hardware Installation

The DSL-604+ functions on three separate networks, a wired Ethernet LAN, a wireless LAN and a wired ADSL WAN. Placement of the Router must take into account the fact that it is connected to these three networks with three types of media. Ethernet cables connect the Router to computers and network devices and the ADSL line connects it to a wall socket. In addition, the device must be near an AC wall outlet for power. How to accommodate these wired connections is often not a complicated matter. However, the added dimension of wireless communication does complicate the decision of Router placement.

Location

Many environmental factors can affect the effective wireless function of the DSL-604+. If this is your first time setting up a wireless network device, read and consider the points listed below.

The access point can be placed on a shelf or desktop, ideally you should be able to see the LED indicators on the front if you need to view them for troubleshooting.

Designed to go up to 100 meters indoors and up to 300 meters outdoors, Wireless LAN lets you access your network from anywhere you want. However, the number of walls, ceilings, or other objects that the wireless signals must pass through can limit signal range. Typical ranges vary depending on the types of materials and background RF noise in your home or business. To range and signal strength, use these basic guidelines:

1. **Keep the number of walls and ceilings to a minimum:**
   The signal emitted from Wireless LAN devices can penetrate through ceilings and walls. However, each wall or ceiling can reduce the range Wireless LAN devices from 1 to 30M. Position your wireless devices so that the number of walls or ceilings obstructing the signal path is minimized.
2. **Consider the direct line between access points and workstations:** A wall that is 0.5 meters thick, at a 45-degree angle appears to be almost 1 meter thick. At a 2-degree angle, it is over 14 meters thick. Be careful to position access points and client adapters so the signal can travel straight through (90º angle) a wall or ceiling for better reception.
3. **Building Materials make a difference:** Buildings constructed using metal framing or doors can reduce effective range of the device. If possible, position wireless devices so that their signal can pass through drywall or open doorways, avoid positioning them so that their signal must pass through metallic materials. Poured concrete walls are reinforced with steel while cinderblock walls generally have little or no structural steel.
4. **Position the antennas for best reception.** Play around with the antenna position to see if signal strength improves. Some adapters or access points allow the user to judge the strength of the signal.
5. **Keep your product away (at least 1-2 meters) from electrical devices:**
   Position wireless devices away from electrical devices that generate RF noise such as microwave ovens, monitors, electric motors, etc.

Network Connection

Complete the connection to the wired networks through the ADSL port and the Ethernet port on the back of the Router. See the diagram on page 4.

Connect ADSL Line

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

Connect Router to Ethernet

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

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

Connect the Power

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

Factory Reset Button

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

3

Configuring the Router for the First Time

The first time you setup the Router it is recommended that you configure the WAN connection using a single computer making sure that both the computer and the Router are not connected to the LAN. Once the WAN connection is functioning properly you may continue change settings to suit your network. This chapter is only concerned with settings up the WAN connection. The following chapter, Web-based Management Guide, describes the various menus used to configure and monitor the Router including how to change IP settings, DHCP server setup and 802.11b wireless configuration.

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.
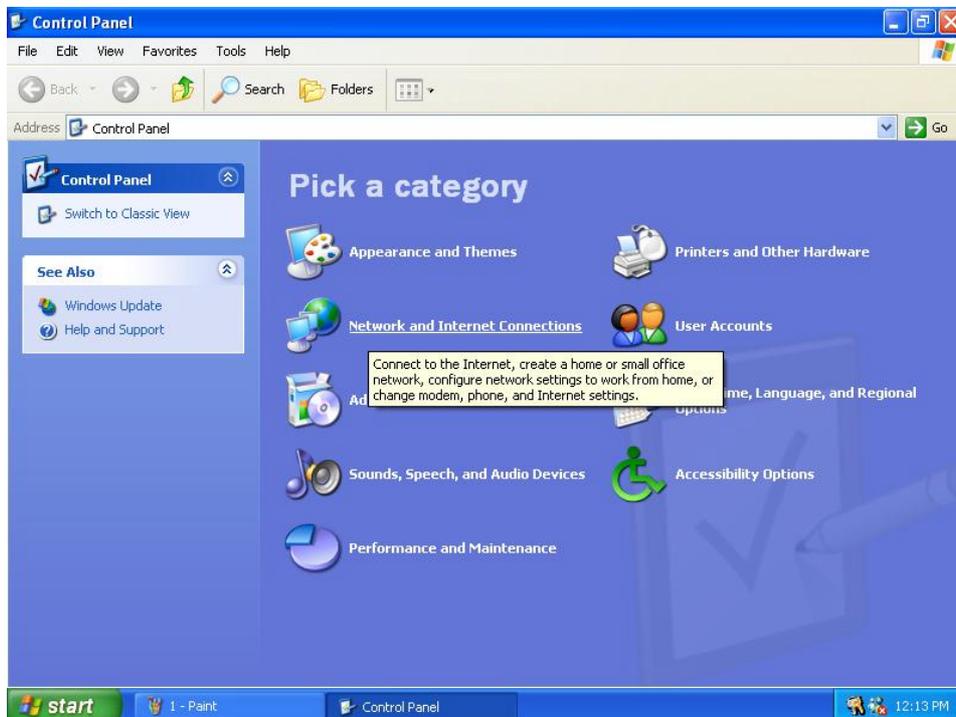
Configure Windows XP for DHCP

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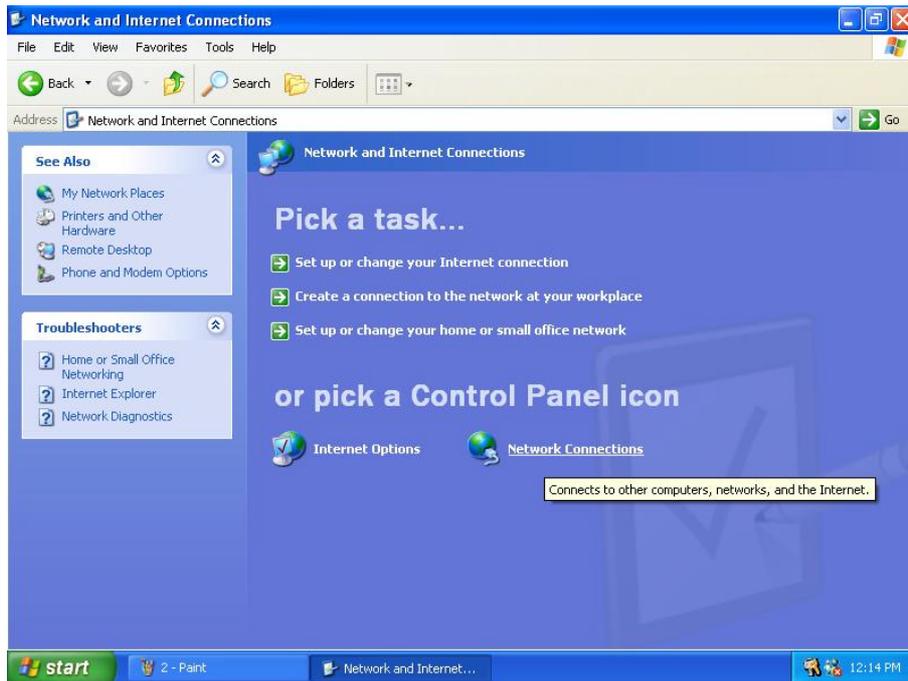
1. From the **Start** menu on your desktop, go to click on **Control Panel**.

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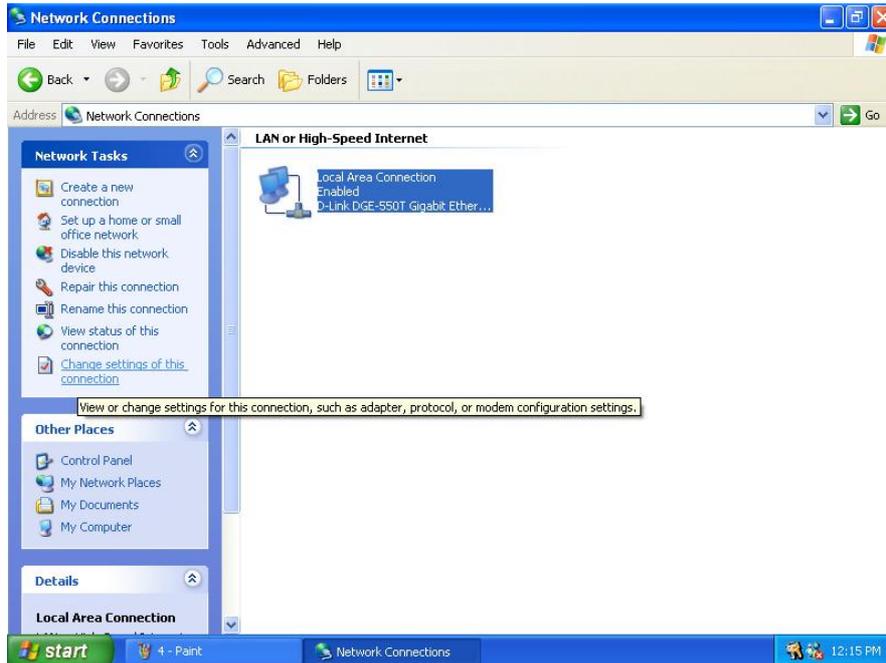
3.   In the Network and Internet Connections folder, click on **Network Connections**.

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.
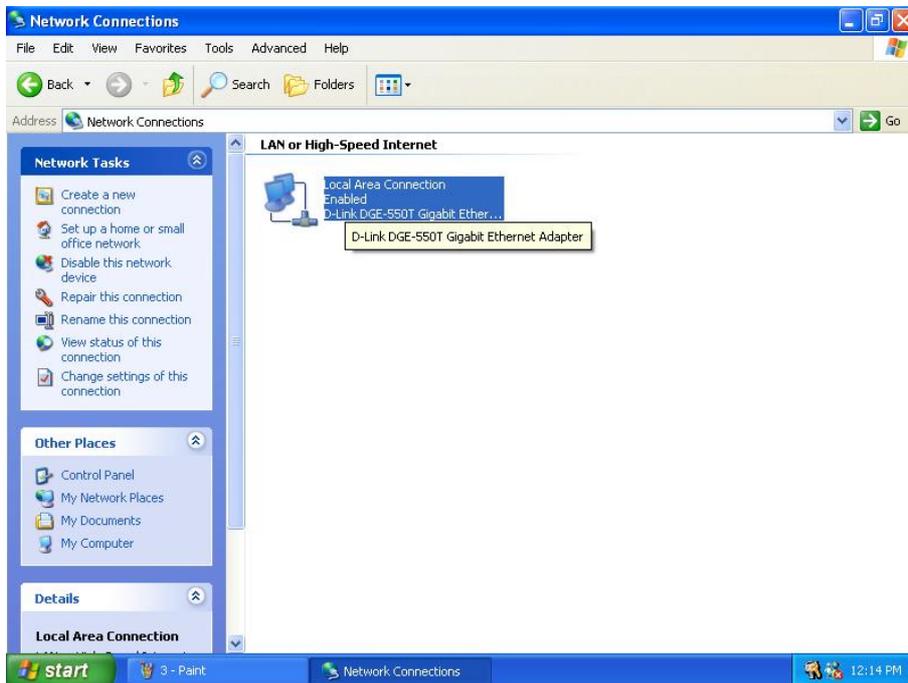
5. Click on **Change settings of the connection** under Network Tabs.

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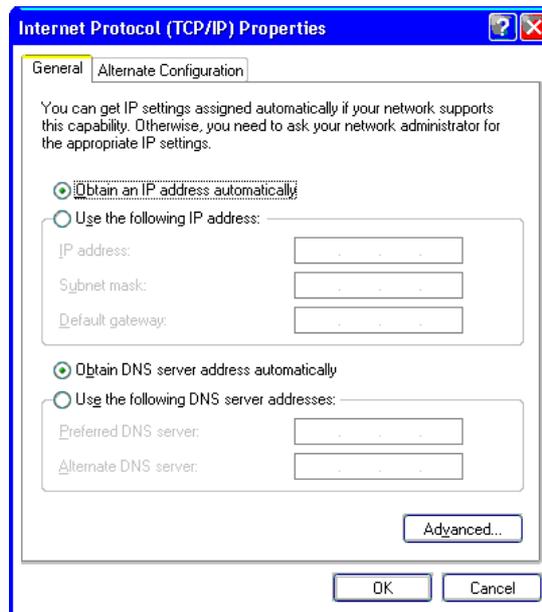
Your computer is now ready to use the Router's DHCP server.

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.
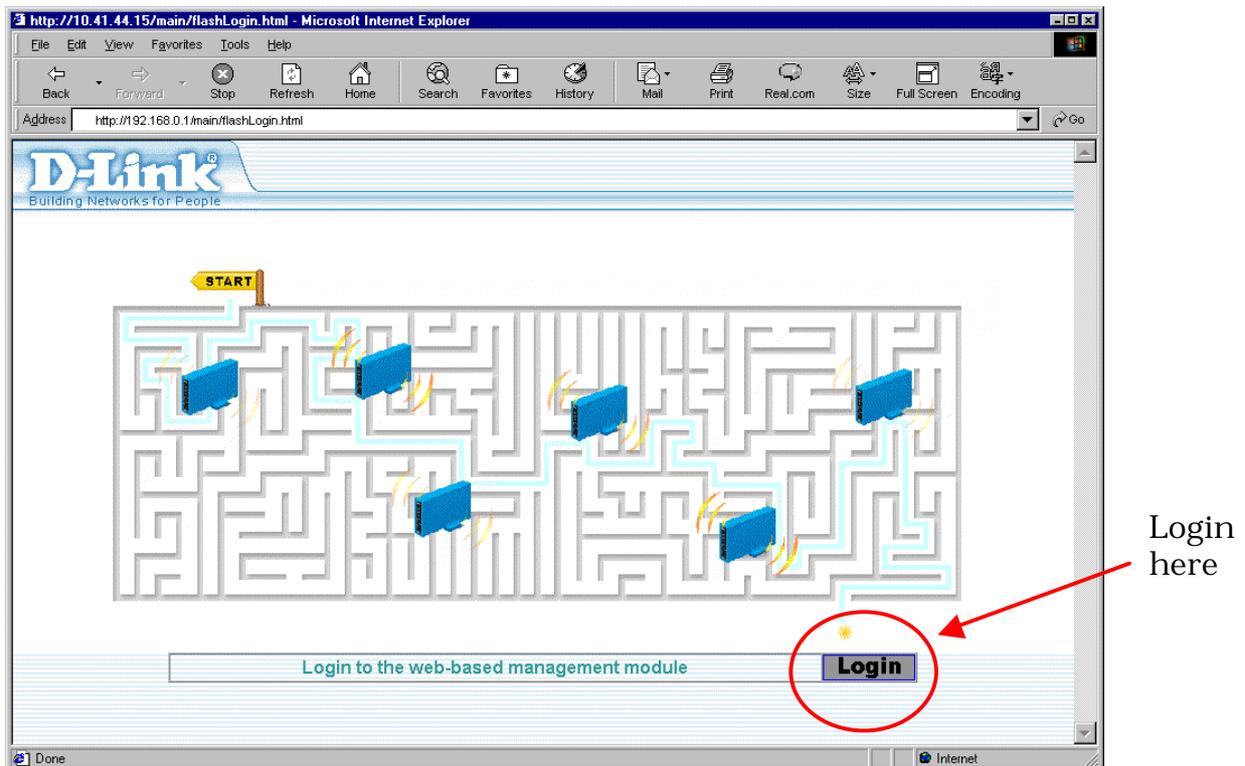
Figure 3-1. Login Page

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 3- 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 WAN Connection Configuration in the next chapter.

Note: Users in Australia and New Zealand may not see "Multiple PVC" page, router should have preset profiles for these countries under "Router/Bridge Configuration" menu. Please select suitable profile from "Connection Profile" list.

Note: Bigpond ADSL users (PPPoE or PPPoA) may need to enter their username in **username@bigpond** format.

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.

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.

4

Web-based Management Guide

The DSL-604+ offers a web-based (HTML) graphical user interface allowing users to manage the Router from anywhere on the LAN using a standard browser, software such as Netscape Navigator or Microsoft Internet Explorer. The web browser is used for direct communication with the Router using HTTP protocol.

Accessing the Web Manager

In order to 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.

> *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.*

Note

Folders and Menus

The web manager interface (GUI) displays two fields that can 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. 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.

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

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.

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 WAN Connection Configuration).

5. For IPoA connections, supply account IP settings if IP Unnumbered is disabled (see 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:
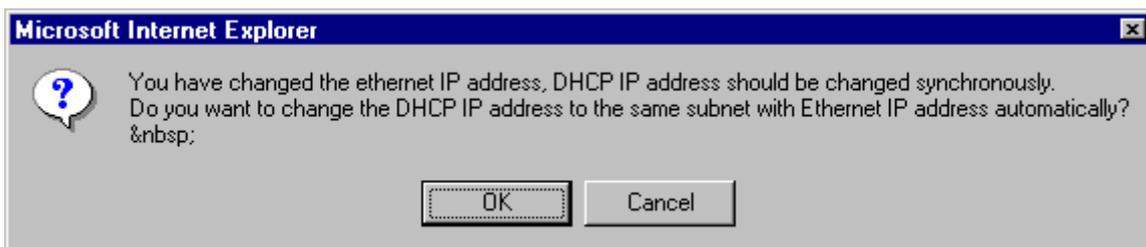
If you will continue to use the DHCP function, click the **OK** button. Otherwise you will need to manually configure the DHCP server addresses to reflect the change.

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

Wireless Configuration

All 802.11b wireless network settings for the Router are configured on this page. The Router supports data rates of up to 22 Mbps when it is used with other D-Link AirPlus devices. The data rate is automatically determined and set to the highest possible rate.

Basic Settings

The two essential settings for wireless LAN operation are the SSID and Channel Number. The SSID (Service Set Identifier) is used to identify a group of wireless LAN components. The basic wireless settings displayed at the top of the menu are described as follows:

SSID: The SSID identifies members of Service Set. All WLAN devices operating on a Service Set (or Extended Service Set) must use the same SSID. This can be any alphanumeric value of up to 32 characters long. Use this to prevent cross communication between two or more WLANs in one area. Type in the common SSID used for your wireless network or network segment.

Channel: What channels are available for use by the access point depends on the local regulatory environment. Remember that all devices communicating with the device must use the same channel (and use the same SSID). Use the drop down menu to select the channel used for your 802.11b wireless LAN.

Trans Rate: This is automatically determined and not user defined. The current data transfer rate used for this access point is displayed.

Note	*If you are accessing the DSL-604+ Web Manager via the wireless interface and change the Channel or SSID, contact with the device will end once the changes to the wireless settings are in effect. You will need to change the same settings for the wireless host you are using to regain access to the device.*

WEP Encryption

WEP (Wireless Encryption Protocol or Wired Equivalent Privacy) encryption can be enabled for security and privacy. WEP encrypts the data portion of each frame transmitted from the wireless adapter using one of the predefined keys. WEP keys used for the DSL-604+ are shared keys which means that it will allow only wireless devices that have the shared key to associate with it. Decryption of the data contained in each packet can only be done if the both the receiver and transmitter have the correct shared key.

Note	*If you are configuring the wireless settings for the first time, disable WEP on at least a few stations and use them to test for connectivity and signal strength before you configure WEP. It is important to first determine that basic wireless operation is possible before enabling WEP.*

Configure the following parameters for WEP:

WEP State: Use the drop down menu to select the type of WEP encryption or disable it (*Disabled* by default). Select *64 Bit* to enabled 64 bit Hexadecimal encryption, or select *128 Bit* to enable 128 bit Hexadecimal encryption. Up to four separate 64 bit keys can be listed, but only one may be active. A key becomes the active key by selecting it. If you have opted not to use a Passphrase, you can define the keys here by typing in 10 hexadecimal digits. Hexadecimal digits are defined as the numerical digits 0 – 9 and the letters A – F (upper and lower case are recognized as the same digit).

WEP Key: There are two options, select one:

Pass phrase: Choose the Passphrase option and type a passphrase used for conversion to a hexadecimal key. For 64 bit encryption, the (ASCII) characters are converted automatically and listed as 5-digit hexadecimal keys. 64 bit encryption allows you to select one of four active keys. For 128 bit encryption, the characters are converted and listed as a 13 digit hexadecimal key. 128 bit encryption allows you to select one of four active keys.

64 Bit Hex Key: Choose the 64 Bit Hex Key option and select an active 64 bit key used to encrypt data frames. Up to four separate 64 bit keys can be listed, but only one may be active. A key becomes the active key by selecting it. If you have opted not to use a Passphrase, you can define the keys here by typing in 10 hexadecimal digits. Hexadecimal digits are defined as the numerical digits 0 – 9 and the letters A – F (upper and lower case are recognized as the same digit).

128 Bit Hex Key: Choose the 128 Bit Hex Key option and define the 128 bit key. Enable the 128 bit key by selecting it and typing the key characters in the allotted spaces. If you have opted not to use a Passphrase, you can define the keys here by typing in 26 hexadecimal digits. Hexadecimal digits are defined as the numerical digits 0 – 9 and the letters A - F (upper and lower case are recognized as the same digit).

Figure 4- 4. WAN Configuration

Note

64 bit WEP = 40 bit WEP *The lower level of WEP encryption uses a 40 bit (10 Hex character) "secret key" (set by the user), and a 24 bit "Initialization Vector" (not under user control). Some vendors refer to this as 40 bit WEP, it is the same as 64 bit WEP only the name is different.*

MAC Access Control

For added security you can opt to use Access Control based on MAC address. This feature lets you create a list of MAC addresses that are allowed or denied association with the Router through the wireless interface. When it is enabled, the access point is instructed to forward packets only from wireless devices only if the MAC address of the device is granted association. Packets received through the wireless interface from non-authorized devices, including other access points, will be dropped. Packets received on the Ethernet port continue to be forwarded to authorized MAC addresses and broadcast packets from the Ethernet are broadcast to all stations, authorized and non-authorized, unless the destination MAC address has been explicitly denied association (see next paragraph).

You may also enter MAC addresses that are explicitly denied permission to associate. In this case, all packets with a destination MAC address that has been denied permission will be dropped. Broadcast and unicast packets are NOT forwarded to devices that are denied permission through the wireless interface.

Keep in mind that there are drawbacks to using Access Control. Any wireless device that is added to the network must be granted explicit permission to join by adding it to the Authorized MAC Table. Be sure to include the MAC address of other access points that you want to associate with the Router. As with other security measures, throughput can be affected since each packet header is examined before the packet is forwarded or dropped.

When you have completed making changes to the list of qualified MAC addresses, click the *OK* button. You can save and restart or continue to change Router settings.

To Grant Access

To grant permission to associate with the Router follow these steps:

1. Type in the MAC address with no spaces or dashes in the MAC address entry field. The entry field displays all zeros when empty. Attempts to enter an invalid MAC address will be detected and you will be informed with an error message.

2. Select *Granted* from the **State** drop-down menu.

3. Click the Add button to add the MAC address to the list of MAC addresses.

4. When the list of qualified MAC addresses is complete, click the **OK** button and save the changes.

To Deny Access

To deny permission to associate with the Router follow these steps:

1. Type in the MAC address with no spaces or dashes in the MAC address entry field. The entry field displays all zeros when empty. Attempts to enter an invalid MAC address will be detected and you will be informed with an error message.

2. Select *Denied* from the **State** drop-down menu.

3. Click the *Add* button to add the MAC address to the list of MAC addresses.

4. When the list of qualified MAC addresses is complete, click the *OK* button and save the changes.

To Delete a MAC Address from the List

To delete a MAC address from the list of qualified MAC addresses:

1. Select the MAC address from the list using the **MAC Address** drop-down menu.

2. Click the *Delete* button to remove the MAC address from the list of MAC addresses.

3. When you are finished modifying the list, click the *OK* button and save the changes.

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- 5. 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.

Figure 4- 6. Proxy DNS Menu

The Proxy DNS Menu presents the following user defined parameters:

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

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

DHCP Configuration

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

Figure 4- 7. DHCP Configuration Menu

Configure LAN DHCP services by defining the following parameters:

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

NAT Configuration

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

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

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

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

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

Figure 4- 8. NAT Configuration Menu

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

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

DMZ IP Address

NAT may conflict with certain interactive applications such as video conferencing or playing Internet video games. For these applications, a NAT bypass can be set up using a DMZ IP address. The DMZ IP address is a "visible" address and does not benefit from the full protection of the NAT function. Therefore it is advisable that other security precautions be enabled to protect the other computers and devices on the LAN. It may be wise to 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.
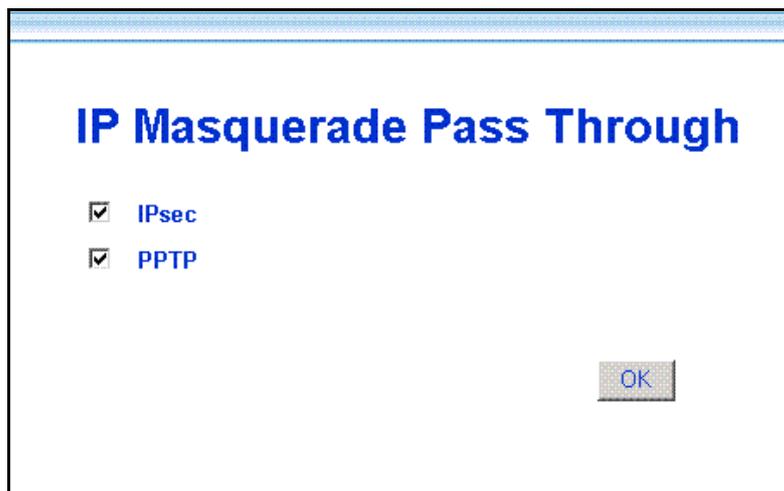
Figure 4- 9. IP Masquerade Pass Through

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.
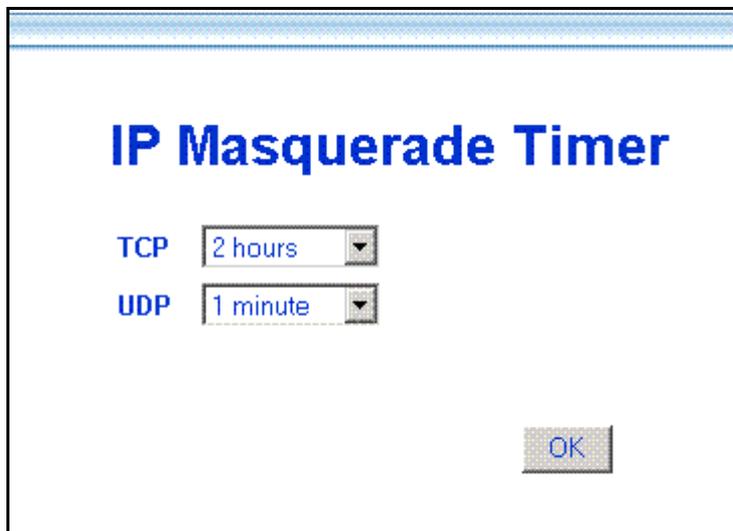

Figure 4- 10. IP Masquerade Timer

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

Figure 4- 11. 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.

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

Figure 4-12. Static Route Configuration Table

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

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

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

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

Advanced Filter & Firewall

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

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

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

Figure 4- 13. Filter & Firewall Main Menu

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

Define these variables for each filter rule:

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

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

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

RIP

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

Figure 4- 14. 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.

Figure 4- 15. 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.
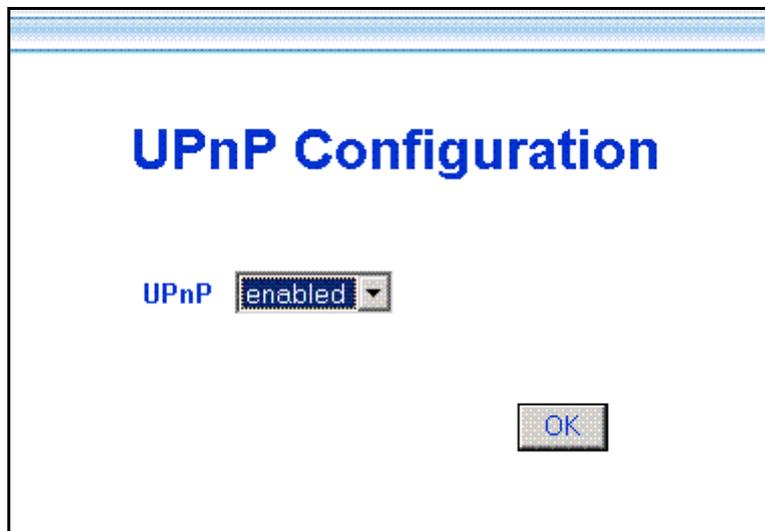
Figure 4-16. UPnP Configuration

System Maintenance

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

ATM Loopback Test

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

Figure 4- 17. ATM Loopback Screen

To perform the test, define the following parameters:

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

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

System Username and Password

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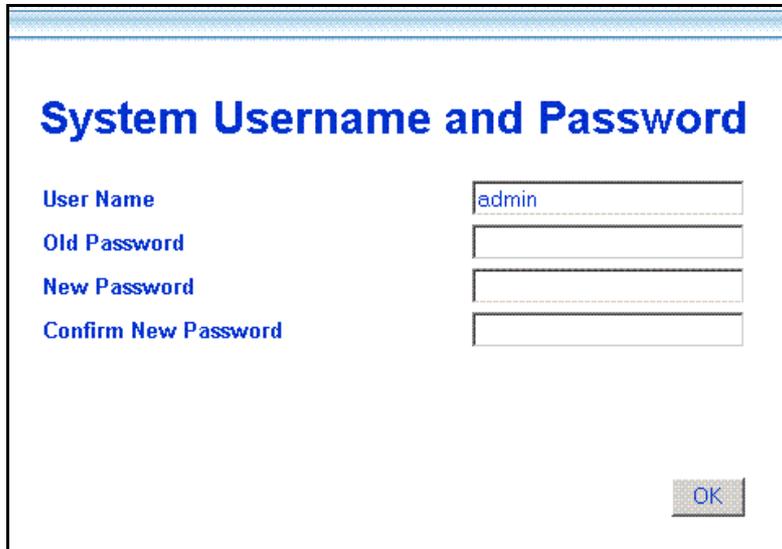

Figure 4- 18. System User Name and Password Menu

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:
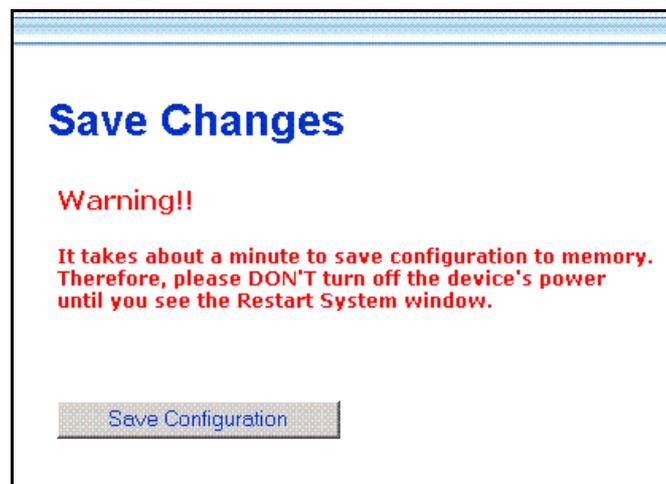
Figure 4- 19. Save Changes Menu

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.
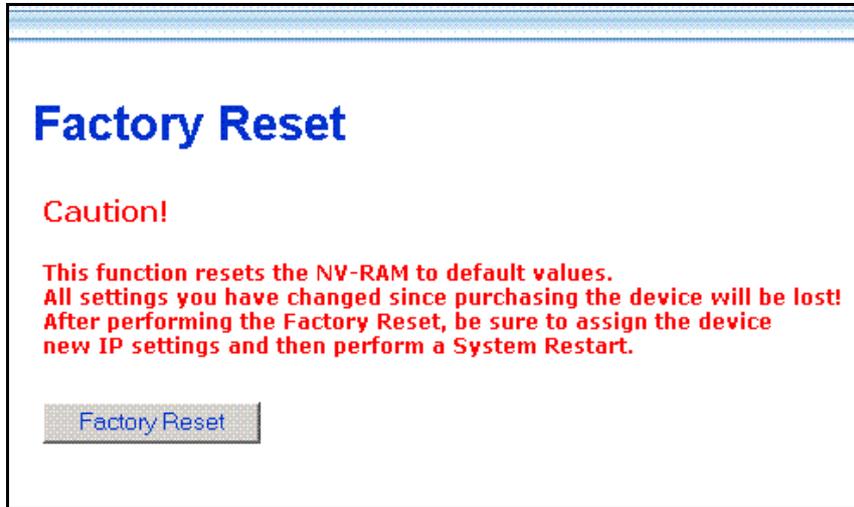

Figure 4- 20. Factory Reset Screen

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. 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- 21. 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.
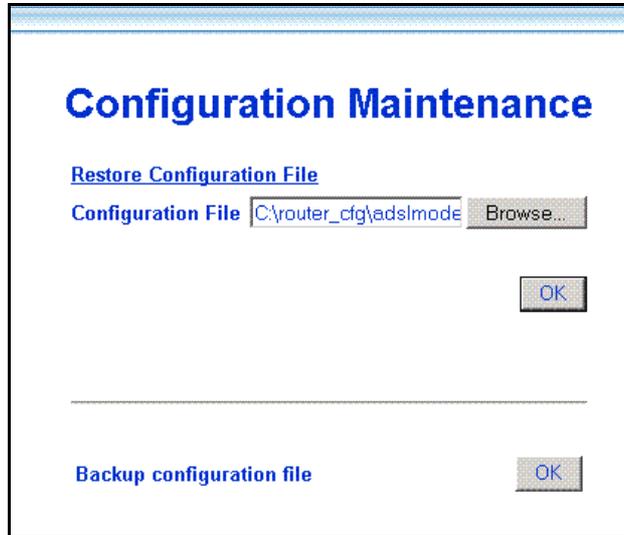

Figure 4- 22. Configuration Maintenance Screen

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

Remote Administration Access

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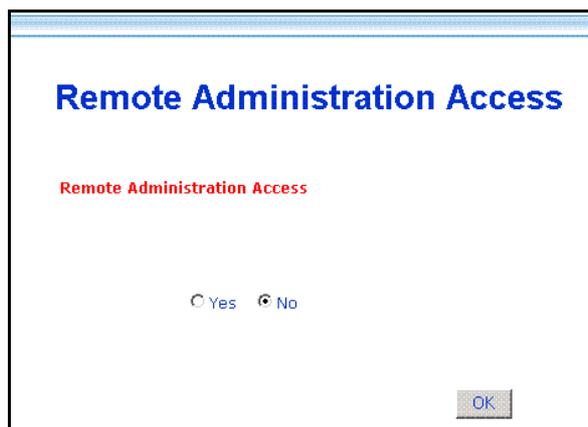

Figure 4- 23. Remote Administration Access

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- 24. ADSL Line Retrain

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

Summary

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

System Summary

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


Figure 4- 25. System Summary

See the Summary description on the following page.

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

DHCP Allocation Table

The DHCP Allocation Table provides a summary of current IP setting allocation for the network.
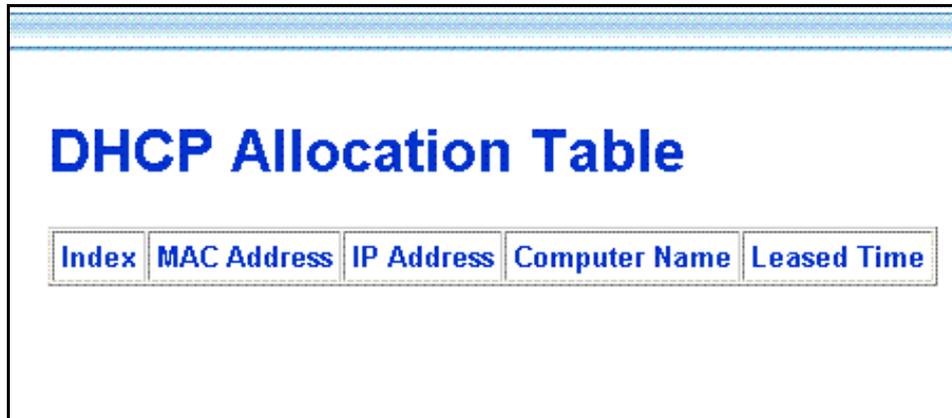
Figure 4- 26. DHCP Allocation Table

Information listed in the DHCP Allocation Table includes the following:

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

Port Redirection Summary

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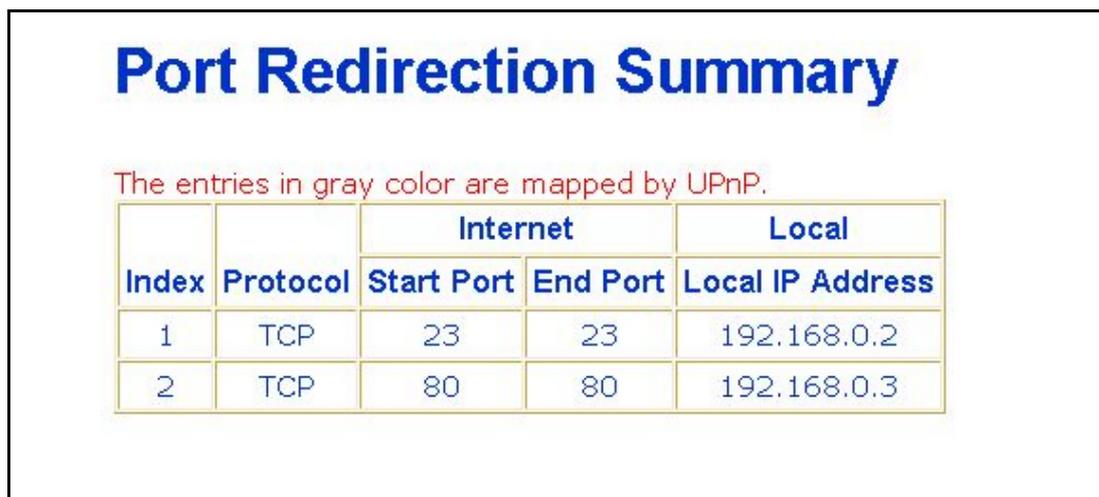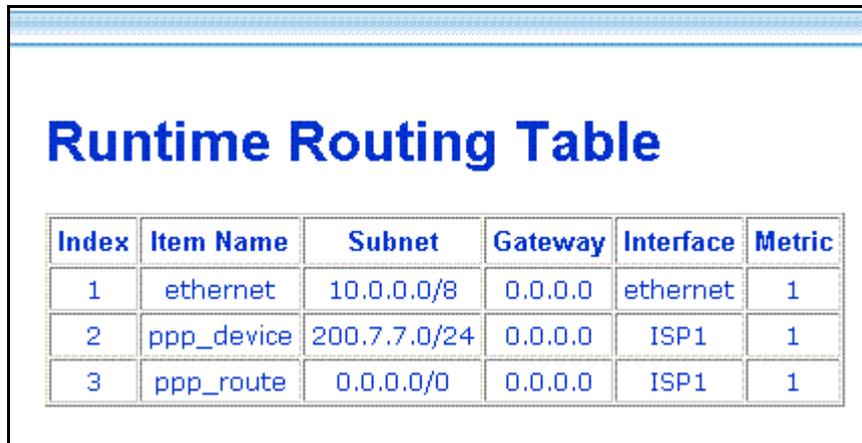

Figure 4- 27. Port Redirection Summary

Runtime Routing Table

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

Figure 4- 28. Runtime Routing Table

Information listed in the Runtime Routing Table includes the following:

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

Filter and Firewall Summary

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

Figure 4- 29. Filtering & Firewall Summary

Line Condition

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

Figure 4- 30. Line Condition

Protocol	**ADSL State**	*Disconnected* - ADSL connection failure	
		Idle - valid connection currently not active	
		Active - valid connection that currently transmitting packets	
	Data Path	Current data path type Fast or Interleaved	
	Operation Mode	Modulation technique used for ADSL connection, G.DMT or G.lite	
Link Status	**ADSL Link Speed**	Downstream/Upstream data transfer rate in Kbps	
	SNR	Downstream/Upstream Signal-to-Noise Ratio in dB	
	ATTEN	Downstream/Upstream attenuation of signal in dB	
Line Error	**FEC**	FEC Forward Error Correction	
	CRC	CRC Cyclic Redundancy Control	
	HEC	HEC Header Error Check	
Frame Counter	Number of data packets received and transmitted		
Loop Distance	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
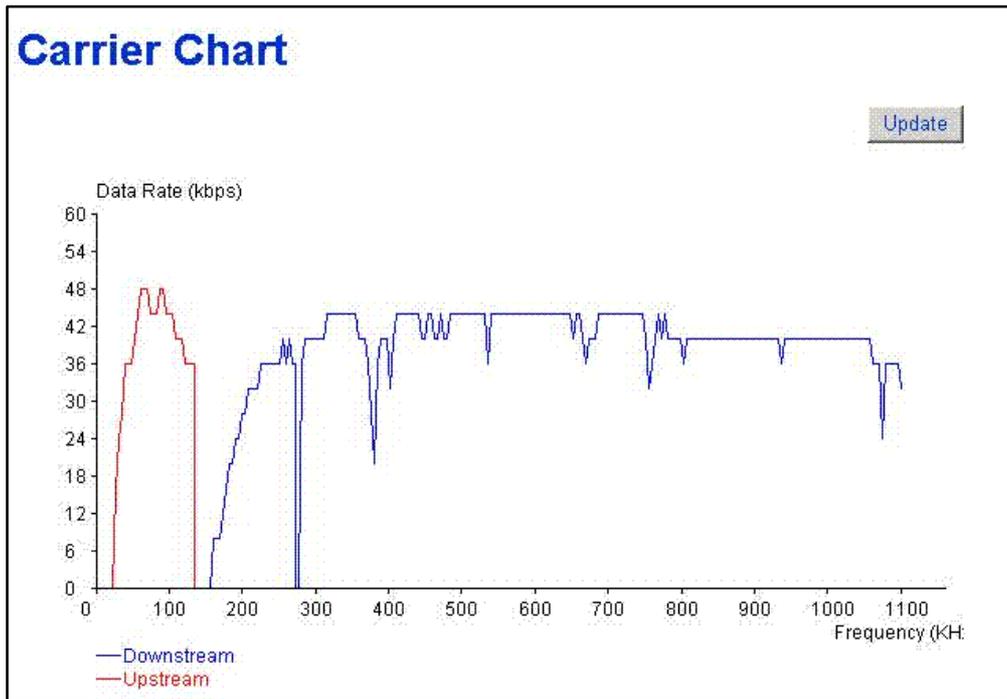
Figure 4- 31. Carrier Chart

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.

A

Technical Specifications

GENERAL		
STANDARDS:	- ITU G.992.1 (G.dmt) - ITU G.992.2 (G.lite) - ITU G.994.1 (G.Hs) - ITU-T Rec. I.361 - ITU-T Rec. I.610 - IEEE 802.3 - IEEE 802.3u - IEEE 802.1d - RFC 791 (IP Routing) - RFC 792 (UDP) - RFC 826 (ARP) - RFC 1058 (RIP 1) - RFC 1389 (RIP 2) - RFC 1213 compliant - RFC 1483 (Bridged Ethernet) - RFC 1577 (IP over ATM)	- RFC 1661 (PPP) - RFC 1994 (CHAP) - RFC 1334 (PAP) - RFC 2364 (PPP over ATM) - RFC 1631 (NAT) - RFC 1877 (Automatic IP assignment) - RFC 2516 (PPP over Ethernet) - Supports RFC 2131 and RFC 2132 (DHCP) - Compatible with all T1.413 issue 2 (full rate DMT over analog POTS), and CO DSLAM equipment - Supports ATM Forum UNI V3.1 PVC
PROTOCOLS:	TCP/IP UDP RIP-1 RIP-2 IGMP	DHCP BOOTP ARP AAL5
DATA TRANSFER RATE:	G.dmt full rate: Downstream up to 8 Mbps Upstream up to 640 Kbps G.lite: Downstream up to 1.5 Mbps Upstream up to 512 Kbps	
MEDIA INTERFACE EXCHANGE:	RJ-11 port ADSL telephone line connection RJ-45 port for 10/100 FAST Ethernet connection RJ-14 port for console connection (requires RJ-14 to RS-232/DB-9 adapter)	

Physical and Environmental	
DC inputs: Power Adapter:	Input: 100V AC 50 - 60Hz 24W Output: 7.5V DC 1.5 A
Power Consumption:	12 Watts (max)
Operating Temperature:	0° to 40° C (32° - 104° F)
Humidity:	5 to 95% (non-condensing)
Dimensions:	234.0 mm x 162.0 mm x 35.0 mm
Weight:	500 grams
EMI:	FCC Class B, CE Class B
Safety:	CSA International
Wireless Compatibility:	Wi-Fi (To Be Defined)
Reliability:	Mean Time Between Failure (MTBF) min. 4 years

D-Link Offices

Australia	**D-Link Australasia** Unit 16, 390 Eastern Valley Way, Roseville, NSW 2069 Australia TEL: 61-2-9417-7100 FAX: 61-2-9417-1077 TOLL FREE (Australia): 1800-177100 TOLL FREE (New Zealand): 0800-900900 URL: www.dlink.com.au E-MAIL: support@dlink.com.au & info@dlink.com.au Level 1, 434 St. Kilda Road, Melbourne, Victoria 3004 Australia TEL: 61-3-9281-3232 FAX: 61-3-9281-3229 MOBILE: 0412-660-064
Canada	**D-Link Canada** 2180 Winston Park Drive, Oakville, Ontario, L6H 5W1 Canada TEL: 1-905-829-5033 FAX: 1-905-829-5095 BBS: 1-965-279-8732 TOLL FREE: 1-800-354-6522 URL: www.dlink.ca FTP: ftp.dlinknet.com E-MAIL: techsup@dlink.ca
Chile	**D-Link South America** Isidora Goyeechea 2934 of 702, Las Condes, Santiago, Chile, S. A. TEL: 56-2-232-3185 FAX: 56-2-232-0923 URL: www.dlink.cl E-MAIL: ccasassu@dlink.cl & tsilva@dlink.cl
China	**D-Link China** 2F, Sigma Building, 49 Zhichun Road, Haidan District, 100080 Beijing, China TEL: 86-10-88097777 FAX: 86-10-88096789 URL: www.dlink.com.cn E-MAIL: liweii@digitalchina.com.cn
Denmark	**D-Link Denmark** Naverland 2, DK-2600 Glostrup, Copenhagen, Denmark TEL: 45-43-969040 FAX:45-43-424347 URL: www.dlink.dk E-MAIL: info@dlink.dk
Egypt	**D-Link Middle East** 7 Assem Ebn Sabet Street, Heliopolis, Cairo, Egypt TEL: 20-2-635-6176 FAX: 20-2-635-6192 URL: www.dlink-me.com E-MAIL: support@dlink-me.com & fateen@dlink-me.com
Finland	**D-Link Finland** Thlli-ja Pakkahuone Katajanokanlaituri 5, FIN– 00160 Helsinki TEL: 358-9-622-91660 FAX: 358-9-622-91661 URL: www.dlink-fi.com
France	**D-Link France** Le Florilege #2, Allee de la Fresnerie, 78330 Fontenay le Fleury, France TEL: 33-1-3023-8688 FAX: 33-1-3023-8689 URL: www.dlink-france.fr E-MAIL: info@dlink-france.fr
Germany	**D-Link Central Europe/D-Link Deutschland GmbH** Schwalbacher Strasse 74, D-65760 Eschborn, Germany TEL: 49-6196-77990 FAX: 49-6196-7799300 URL: www.dlink.de BBS: 49-(0) 6192-971199 (analog) BBS: 49-(0) 6192-971198 (ISDN) INFO: 00800-7250-0000 (toll free) HELP: 00800-7250-4000 (toll free) REPAIR: 00800-7250-8000 E-MAIL: info@dlink.de
India	**D-Link India** Plot No.5, Kurla-Bandra Complex Rd., Off Cst Rd., Santacruz (E), Bombay, 400 098 India TEL: 91-22-652-6696 FAX: 91-22-652-8914 URL: www.dlink-india.com E-MAIL: service@dlink.india.com
Italy	**D-Link Mediterraneo Srl/D-Link Italia** Via Nino Bonnet n. 6/b, 20154, Milano, Italy TEL: 39-02-2900-0676 FAX: 39-02-2900-1723 URL: www.dlink.it E-MAIL: info@dlink.it
Japan	**D-Link Japan** 10F, 8-8-15 Nishi-Gotanda, Shinagawa-ku, Tokyo 141, Japan TEL: 81-3-5434-9678 FAX: 81-3-5434-9868 URL: www.d-link.co.jp E-MAIL: kida@d-link.co.jp
Netherlands	**D-Link Benelux** Fellenoord 1305611 ZB, Eindhoven, the Netherlands TEL: 31-40-2668713 FAX: 31-40-2668666 URL: www.d-link-benelux.nl

Norway	**D-Link Norway** Waldemar Thranesgt. 77, 0175 Oslo, Norway TEL: 47-22-991890 FAX: 47-22-207039
Russia	**D-Link Russia** Michurinski Prospekt 49, 117607 Moscow, Russia TEL: 7-095-737-3389 & 7-095-737-3492 FAX: 7-095-737-3390 URL: www.dlink.ru E-MAIL: vl@dlink.ru
Singapore	**D-Link International** 1 International Business Park, #03-12 The Synergy, Singapore 609917 TEL: 65-774-6233 FAX: 65-774-6322 E-MAIL: info@dlink.com.sg URL: www.dlink-intl.com
South Africa	**D-Link South Africa** 102 – 106 Witchhazel Avenue, Einstein Park 2, Block B, Highveld Technopark, Centurion, South Africa TEL: 27 (0) 12-665-2165 FAX: 27 (0) 12-665-2186 URL: www.d-link.co.za E-MAIL: attie@d-link.co.za
Spain	**D-Link Iberia** C/Sabino De Arana, 56 Bajos, 08028 Barcelona, Spain TEL: 34 93 4090770 FAX: 34 93 4910795 URL: www.dlinkiberia.es E-MAIL: info@dlinkiberia.es
Sweden	**D-Link Sweden** P. O. Box 15036, S-167 15 Bromma, Sweden TEL: 46-(0) 8-564-61900 FAX: 46-(0) 8-564-61901 E-MAIL: info@dlink.se URL: www.dlink.se
Taiwan	**D-Link Taiwan** 2F, No. 119 Pao-Chung Rd, Hsin-Tien, Taipei, Taiwan TEL: 886-2-2910-2626 FAX: 886-2-2910-1515 URL: www.dlinktw.com.tw E-MAIL: dssqa@tsc.dlinktw.com.tw
Turkey	**D-Link Middle East** Deniz Bilgisayar, Buyukdere Cad. Naci Kasim Sk., No. 5 Mecidiyekoy, Istanbul, Turkey TEL: 90-212-213-3400 FAX: 90-212-213-3420 E-MAIL: smorovati@dlink-me.com
U.A.E.	**D-Link Middle East** CHS Aptec (Dubai), P.O. Box 33550 Dubai U.A.E. TEL: 971-4-366-885 FAX: 971-4-355-941 E-MAIL: Wxavier@dlink-me.com
U.K.	**D-Link Europe** 4th Floor, Merit House, Edgware Road, Colindale, London NW9 5AB United Kingdom TEL: 44 (0) 20-8731-5555 FAX: 44 (0) 20-8731-5511 BBS: 44 (0) 181-235-5511 URL: www.dlink.co.uk E-MAIL: info@dlink.co.uk
U.S.A.	**D-Link U.S.A.** 53 Discovery Drive, Irvine, CA 92618, USA TEL: 1-949-788-0805 FAX: 1-949-753-7033 BBS: 1-949-455-1779 & 1-949-455-9616 INFO: 1-800-326-1688 URL: www.dlink.com E-MAIL: tech@dlink.com & support@dlink.com

Registration Card

Print, type or use block letters.

Your name: Mr./Ms_____

Organization: _____Dept._____

Your title at organization:_____

Telephone:_____ Fax:_____

Organization's full address:_____

_____

Country:_____

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

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

(* Applies to adapters only)

Product was purchased from:

Reseller's name:_____

Telephone:_____ Fax:_____

Reseller's full address:_____

_____

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

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

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

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

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

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

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

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

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

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

10.Your comments on this product? _____

_____
_____
_____