

USER MANUAL

DSL-2760U

VERSION 1.0



D-Link[®]

BROADBAND

Table of Contents

TABLE OF CONTENTS	2	ARP	22
ABOUT THIS USER'S GUIDE	4	DHCP	23
INTRODUCTION	4	ADVANCED SETUP	24
PACKAGE CONTENTS	5	LAYER2 INTERFACE	25
SYSTEM REQUIREMENTS	5	WIDE AREA NETWORK (WAN) SERVICE.....	27
FEATURES AND BENEFITS	6	LAN	47
HARDWARE OVERVIEW	7	NAT – VIRTUAL SERVERS	49
FRONT VIEW.....	7	NAT – PORT TRIGGERING.....	51
REAR VIEW (CONNECTIONS).....	8	NAT – DMZ HOST	53
INSTALLATION	9	NAT – ALG	53
BEFORE YOU BEGIN.....	9	SECURITY – IP FILTERING.....	54
INSTALLATION NOTES	9	SECURITY – MAC FILTERING	57
INFORMATION YOU WILL NEED FROM YOUR ADSL SERVICE PROVIDER.....	11	PARENTAL CONTROL – TIME RESTRICTION.....	59
INFORMATION YOU WILL NEED ABOUT DSL-2760U	12	PARENTAL CONTROL – URL FILTER.....	60
INFORMATION YOU WILL NEED ABOUT YOUR LAN OR COMPUTER.....	13	QUALITY OF SERVICE (QOS).....	61
DEVICE INSTALLATION	14	ROUTING.....	64
POWER ON ROUTER.....	14	DOMAIN NAME SERVER (DNS) CONFIGURATION	66
FACTORY RESET BUTTON	14	DYNAMIC DNS CONFIGURATION	67
NETWORK CONNECTIONS.....	15	DSL SETTINGS	69
WEB USER INTERFACE	16	UNIVERSAL PLUG AND PLAY (UPNP) CONFIGURATION	72
DEVICE INFO	17	PRINT SERVER SETTINGS	72
SUMMARY	18	SAMBA USB STORAGE	73
WAN.....	19	PPTP	74
STATISTICS	20	INTERFACE GROUPING	75
ROUTE	22	LAN PORTS CONFIGURATION	77
		WIRELESS	78
		BASIC WIRELESS CONFIGURATION	79
		SECURITY.....	80
		MAC FILTER.....	86

WIRELESS BRIDGE	88	ADD A NETWORK PRINTER IN WINDOWS XP	106
ADVANCED	90	TROUBLESHOOTING.....	115
STATION INFO	91	HOW DO I CONFIGURE MY DSL-2760U ROUTER WITHOUT THE CD-ROM? ..	115
DIAGNOSTICS	92	HOW DO I RESET MY ROUTER TO THE FACTORY DEFAULT SETTINGS?	115
ETHERNET CONNECTION TEST	93	WHAT CAN I DO IF MY ROUTER IS NOT WORKING CORRECTLY?	116
USB CONNECTION TEST	93	WHY CAN'T I GET AN INTERNET CONNECTION?	116
WIRELESS CONNECTION TEST	94	WHAT CAN I DO IF MY ROUTER CAN'T BE DETECTED BY RUNNING THE	
ADSL SYNCHRONIZATION TEST	94	INSTALLATION CD?	117
ATM OAM SEGMENT PING TEST	95	KNOWLEDGE BASE	118
ATM OAM END-TO-END PING TEST	96	CHECK YOUR IP ADDRESS	118
MANAGEMENT	97	STATICALLY ASSIGN AN IP ADDRESS	119
SETTINGS	98	TECHNICAL SPECIFICATIONS	120
SYSTEM LOG	99	D-LINK WORLDWIDE OFFICES.....	122
SNMP AGENT	100	WARRANTY	123
TR-069 CLIENT	101	REGISTRATION	128
INTERNET TIME	102		
ACCESS CONTROL	103		
UPDATE SOFTWARE	104		
REBOOT	105		

About this User's Guide

This user's guide provides a wonderful insight into the functionality of the product called the DSL-2760U. This guide is based on the current running firmware/software version available for this product and might touch on some new and exciting topics never seen on this product line before providing a rewarding reading experience and in the end acts as a guide when installing and maintaining this product.

Introduction

ULTIMATE INTERNET CONNECTION

The DSL-2760U router is a versatile, high-performance remote router for home and the small office. With integrated ADSL2/2+ supporting up to 24Mbps download speed, firewall protection, Quality of Service (QoS), draft 802.11n wireless LAN and 4 Ethernet switch ports, this router provides all the functions that a home or small office needs to establish a secure and high-speed remote link to the outside world.

ULTIMATE WIRELESS CONNECTION WITH MAXIMAL SECURITY

Powered by RangeBooster N technology, this router provides wireless speeds that are up to 4 times faster than 802.11g. Maximize wireless performance by connecting this router to computers equipped with RangeBooster N wireless interfaces and stay connected from virtually anywhere at home and in the office. The router can also be used with 802.11g and 802.11b wireless networks to enable significantly improved reception. It supports WPA/WPA2 and WEP for flexible user access security and data encryption methods.

FIREWALL PROTECTION & QoS

Security features prevents unauthorized access to the home and office network, be it from the wireless devices or from the internet. The router provides firewall security using Stateful Packet Inspection (SPI) and hacker attack logging for Denial of Service (DoS) attack protection. SPI inspects the contents of all incoming packet headers before deciding what packets are allowed to pass through. Router access control is provided with packet filtering based on port and source/destination MAC/IP addresses. For Quality of Service (QoS), the router supports multiple priority queues to enable a group of home or office users to experience the benefit of smooth network connection of inbound and outbound data without concern of traffic congestion. This QoS support allows users to enjoy high ADSL transmission for applications such as VoIP and streaming multimedia over the Internet.

Package Contents

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

- One DSL-2760U Wireless N ADSL2+ Modem Router
- One External Power Adapter
- One CD-ROM with User Manual
- One Twisted-pair telephone cable used for ADSL connection
- One Straight-through Ethernet cable
- One Quick Installation Guide

If any of the packaging content is damaged or missing, please contact your dealer immediately. Also keep the box and packaging materials in case you need to ship the unit in the future.



CAUTION: If powering up the router with DC power, the router must be used with the power adapter included with the device.



System Requirements

Please note that the following requirements are the bare minimum requirements needed to successfully use this router:

1. ADSL Internet connection service normally provided by an Internet Service Provider (ISP).
2. Computer with: CPU Processor 200MHz or above, Memory (RAM) 64MB or above, CD-ROM Drive.
3. Ethernet Adapter with TCP/IP Protocol Installed.
4. Internet Browser for the setup. (Internet Explorer v6 or later, Firefox v1.5, or Safari 1.3 or above)
5. Operating System (Microsoft Windows 2000/XP/Vista)
6. D-Link Click'n Connect Utility

Features and Benefits

- **PPP (Point-to-Point Protocol) Security** – The Router supports PAP (Password Authentication Protocol) and CHAP (Challenge Handshake Authentication Protocol) for PPP connections. The Router also supports MSCHAP.
- **DHCP Support** – Dynamic Host Configuration Protocol automatically and dynamically assigns all LAN IP settings to each host on your network. This eliminates the need to reconfigure every host whenever changes in network topology occur.
- **Network Address Translation (NAT)** – For small office environments, the Router 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 Router 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 Router 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 an 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 Router supports Bridged Ethernet over ATM (RFC1483), IP over ATM (RFC1577), and PPP over ATM (RFC 2364).
- **Precise ATM Traffic Shaping** – Traffic shaping is a method of controlling the flow rate of ATM data cells. This function helps to establish the Quality of Service for ATM data transfer.
- **High Performance** – Very high rates of data transfer are possible with the Router. Up to 24 Mbps downstream bit rate using ADSL 2+ standard.
- **Full Network Management** – The Router 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 Router 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.

Hardware Overview

Front View



- Power Light:** This light will be solid green indicating that the unit is powered on.
- LAN (1-4) Lights:** This light (if active) will be blinking in green indicating that there is network activity.
- WLAN Light:** This light (if enabled) will be blinking in green indicating that there is network activity.
- DSL Light:** This light will be solid green when the ADSL line has successfully synchronized.
- Internet Light:** This light will be solid green when the Internet dialup has authenticated successfully.

Rear View (Connections)



- DSL Port:** This is an RJ-11 ADSL line port that connects the router to the ADSL line.
- USB Ports:** The USB ports are for USB storage devices and/or USB printers.
- LAN (1-4) Ports:** These are Fast Ethernet LAN Ports that connects this router to the local network using CAT5 cables.
- WLAN Button:** Press the button to turn Wireless LAN on or off.
- Reset Button:** Press this button and hold it for 6 seconds to revert the Router back to factory defaults.
- Power Button:** Press the button to turn the power on or off.
- Power Receptacle:** The supplied power adapter connects here.

Installation

This section will walk you through the installation process. Placement of the Router is very important. Do not place the Router in an enclosed area such as a closet, cabinet, or in the attic or garage.

Before You Begin

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 Notes

In order to establish a connection to the Internet it will be necessary to provide information to the Router that will be stored in its memory. For some users, only their account information (Username and Password) is required. For others, various parameters that control and define the Internet connection will be required. You can print out the two pages below and use the tables to list this information. This way you have a hard copy of all the information needed to setup the Router. If it is necessary to reconfigure the device, all the necessary information can be easily accessed. Be sure to keep this information safe and private.

Low Pass Filters

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

Operating Systems

The DSL-2760U 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, including Windows 98 SE, Windows ME, Windows 2000, Windows XP, and Windows Vista.

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 Opera, Microsoft Internet Explorer® version 6.0, Netscape Navigator® version 6.2.3, 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 the device a simple bridge. For a bridged connection, the information needed to make and maintain the Internet connection is stored on another computer or gateway device, not in the Router itself.

If your ADSL service is delivered through a PPPoE or PPPoA connection, the information needed to establish and maintain the Internet connection can be stored in the Router. In this case, it is not necessary to install software on your computer. It may however be necessary to change some settings in the device, including account information used to identify and verify the connection.

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

Information you will need from your ADSL service provider

Username

This is the Username used to log on to your ADSL service provider's network. Your ADSL service provider uses this to identify your account.

Password

This is the Password used, in conjunction with the Username above, to log on to your ADSL service provider's network. This is used to verify the identity of your account.

WAN Setting / Connection Type

These settings describe the method your ADSL service provider uses to transport data between the Internet and your computer. Most users will use the default settings. You may need to specify one of the following WAN Setting and Connection Type configurations (Connection Type settings listed in parenthesis):

- PPPoE/PPoA (PPPoE LLC, PPPoE VC-Mux, PPpOA LLC, or PPpOA VC-Mux)
- Dynamic IP Address (1483 Bridged IP LLC or 1483 Bridged IP VC-Mux)
- Static IP Address (Bridged IP LLC, 1483 Bridged IP VC Mux, 1483 Routed IP LLC, 1483 Routed IP VC-Mux)
- Bridge Mode (1483 Bridged IP LLC or 1483 Bridged IP VC Mux)

Modulation Type

ADSL uses various standardized modulation techniques to transmit data over the allotted signal frequencies. Some users may need to change the type of modulation used for their service. The default DSL modulation (Autosense) used for the Router automatically detects all types of ADSL, ADSL2, and ADSL2+ modulation.

Security Protocol

This is the method your ADSL service provider will use to verify your Username and Password when you log on to their network. Your Router supports the PAP and CHAP protocols.

VPI

Most users will not be required to change this setting. The Virtual Path Identifier (VPI) is used in conjunction with the Virtual Channel Identifier (VCI) to identify the data path between your ADSL service provider's network and your computer. If you are setting up the Router for multiple virtual connections, you will need to configure the VPI and VCI as instructed by your ADSL service provider for the additional connections. This setting can be changed in the WAN Settings window of the web management interface.

VCI

Most users will not be required to change this setting. The Virtual Channel Identifier (VCI) used in conjunction with the VPI to identify the data path between your ADSL service provider's network and your computer. If you are setting up the Router for multiple virtual connections, you will need to configure the VPI and VCI as instructed by your ADSL service provider for the additional connections. This setting can be changed in the WAN Settings window of the web management interface.

Information you will need about DSL-2760U

Username

This is the Username needed access the Router's management interface. When you attempt to connect to the device through a web browser you will be prompted to enter this Username. The default Username for the Router is "admin." The user cannot change this.

Password

This is the Password you will be prompted to enter when you access the Router's management interface. The default Password is "admin." The user may change this.

LAN IP addresses for the DSL-2760U

This is the IP address you will enter into the Address field of your web browser to access the Router's configuration graphical user interface (GUI) using a web browser. The default IP address is 192.168.1.1. This may be changed to suit any IP address scheme the user desires. This address will be the base IP address used for DHCP service on the LAN when DHCP is enabled.

LAN Subnet Mask for the DSL-2760U

This is the subnet mask used by the DSL-2760U, and will be used throughout your LAN. The default subnet mask is 255.255.255.0. This can be changed later.

Information you will need about your LAN or computer

Ethernet NIC

If your computer has an Ethernet NIC, you can connect the DSL-2760U to this Ethernet port using an Ethernet cable. You can also use the Ethernet ports on the DSL-2760U to connect to other computer or Ethernet devices.

DHCP Client status

Your DSL-2760U ADSL Router is configured, by default, to be a DHCP server. This means that it can assign an IP address, subnet mask, and a default gateway address to computers on your LAN. The default range of IP addresses the DSL-2760U will assign are from 192.168.1.2 to 192.168.1.254. Your computer (or computers) needs to be configured to obtain an IP address automatically (that is, they need to be configured as DHCP clients.)

It is recommended that you collect and record this information here, or in some other secure place, in case you have to re-configure your ADSL connection in the future.

Once you have the above information, you are ready to setup and configure your DSL-2760U.

Device Installation

The DSL-2760U connects two separate physical interfaces, an ADSL (WAN) and an Ethernet (LAN) interface. Place the Router in a location where it can be connected to the various devices as well as to a power source. The Router should not be located where it will be exposed to moisture or excessive heat. Make sure the cables and power cord are placed safely out of the way so they do not create a tripping hazard. As with any electrical appliance, observe common sense safety procedures.

The Router 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.

Power on Router

The Router must be used with the power adapter included with the device.

1. Insert the AC Power Adapter cord into the power receptacle located on the rear panel of the Router and plug the adapter into a suitable nearby power source.
2. Depress the Power button into the on position. You should see the Power LED indicator light up and remain lit.
3. If the Ethernet port is connected to a working device, check the Ethernet Link/Act LED indicators to make sure the connection is valid. The Router will attempt to establish the ADSL connection, if the ADSL line is connected and the Router is properly configured this should light up after several seconds. If this is the first time installing the device, some settings may need to be changed before the Router can establish a connection.

Factory Reset Button

The Router may be reset to the original factory default settings by using a ballpoint or paperclip to gently push down the reset button in the following sequence:

1. Ensure the Router is powered on.
2. Press and hold the reset button on the back of the device for approximately 6 to 10 seconds.
3. This process should take around 1 to 2 minutes.

Remember that this will wipe out any settings stored in flash memory including user account information and LAN IP settings. The device settings will be restored to the factory default IP address **192.168.1.1** and the subnet mask is **255.255.255.0**, the default management Username is "admin" and the default Password is "admin."

Network Connections

Connect ADSL Line

Use the ADSL cable included with the Router to connect it to a telephone wall socket or receptacle. 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, the connection to the Internet. It is the physical link to the service provider's network backbone and ultimately to the Internet.

Connect Router to Ethernet

The Router may be connected to a single computer or Ethernet device through the 10BASE-TX Ethernet port on the rear panel. Any connection to an Ethernet concentrating device such as a switch or hub must operate at a speed of 10/100 Mbps only. When connecting the Router to any Ethernet device that is capable of operating at speeds higher than 10Mbps, be sure that the device has auto-negotiation (NWay) enabled for the connecting port. Use standard twisted-pair cable with RJ-45 connectors. The RJ-45 port on the Router is a crossed port (MDI-X). Follow standard Ethernet guidelines when deciding what type of cable to use to make this connection. When connecting the Router directly to a PC or server use a normal straight-through cable. You should use a crossed cable when connecting the Router to a normal (MDI-X) port on a switch or hub. Use a normal straight-through cable when connecting it to an uplink (MDI-II) port on a hub or switch. The rules governing Ethernet cable lengths apply to the LAN to Router connection. Be sure that the cable connecting the LAN to the Router does not exceed 100 meters.

Hub or Switch to Router Connection

Connect the Router to an uplink port (MDI-II) on an Ethernet hub or switch with a straight-through cable. If you wish to reserve the uplink port on the switch or hub for another device, connect to any on the other MDI-X ports (1x, 2x, etc.) with a crossed cable.

Computer to Router Connection

You can connect the Router directly to a 10/100BASE-TX Ethernet adapter card (NIC) installed on a PC using the Ethernet cable provided.

Web User Interface

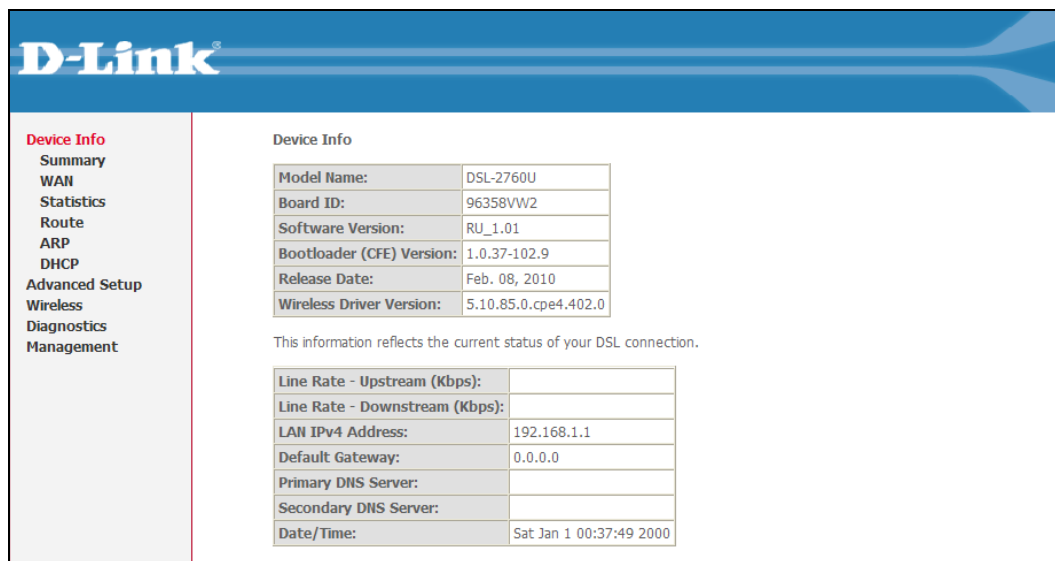
The DSL-2760U Web UI defaults to the Device Information page. The main categories for configuration are located in the menu tabs on the left of the page. These categories include:

- **Device Info** – The Device Info category will display information about the current configuration and running processes configured on the router.
- **Advanced Setup** – The Advanced Setup category allows the user to configure basic and advanced features on this router.
- **Wireless** – The Wireless category allows the user to configure specifically the wireless features of this router.
- **Diagnostics** – The Diagnostics category will run a series of tests and inform the user the outcome.
- **Management** – The Management category allows the user to configure settings concerning the manageability of the router.

These pages and their configuration options will be discussed in detail in the following pages of this manual.

Device Info

To access the **Device Info** window, click either the **Device Info** or **Summary** button in the **Device Info** directory. The following page opens:



D-Link

Device Info

- Summary
- WAN
- Statistics
- Route
- ARP
- DHCP
- Advanced Setup
- Wireless
- Diagnostics
- Management

Device Info

Model Name:	DSL-2760U
Board ID:	96358VW2
Software Version:	RU_1.01
Bootloader (CFE) Version:	1.0.37-102.9
Release Date:	Feb. 08, 2010
Wireless Driver Version:	5.10.85.0.cpe4.402.0

This information reflects the current status of your DSL connection.

Line Rate - Upstream (Kbps):	
Line Rate - Downstream (Kbps):	
LAN IPv4 Address:	192.168.1.1
Default Gateway:	0.0.0.0
Primary DNS Server:	
Secondary DNS Server:	
Date/Time:	Sat Jan 1 00:37:49 2000

Summary

Device Info: This window displays the current status of your DSL connection, including the software version, LAN IP address, and DNS server address.

Device Info

Model Name:	DSL-2760U
Board ID:	96358VW2
Software Version:	RU_1.01
Bootloader (CFE) Version:	1.0.37-102.9
Release Date:	Feb. 08, 2010
Wireless Driver Version:	5.10.85.0.cpe4.402.0

This information reflects the current status of your DSL connection.

Line Rate - Upstream (Kbps):	
Line Rate - Downstream (Kbps):	
LAN IPv4 Address:	192.168.1.1
Default Gateway:	0.0.0.0
Primary DNS Server:	
Secondary DNS Server:	
Date/Time:	Sat Jan 1 00:36:28 2000

WAN

To access the **WAN Info** window, click the **WAN** button in the **Device Info** directory.

WAN Info: This window displays the current status of your DSL connection, including the Interface name, type, VLAN Mux ID, IGMP, NAT Firewall and IPv4 Address.

WAN Info								
Interface	Description	Type	VlanMuxId	Igmp	NAT	Firewall	Status	IPv4 Address

Statistics

To access the Router's first **Statistics window**, click the **Statistics** button in the **Device Info** directory.

LAN

This window displays the Router's LAN statistics. Click the **Reset Statistics** button to refresh these statistics.

Statistics -- LAN

Interface	Received				Transmitted			
	Bytes	Pkts	Errs	Drops	Bytes	Pkts	Errs	Drops
eth0	36462	318	0	0	227732	410	0	0
usb0	0	0	0	0	0	0	0	0
wl0	0	0	0	0	12489	89	69	0

Reset Statistics

WAN Services

This window displays the Router's WAN statistics. Click the **Reset Statistics** button to refresh these statistics.

Statistics -- WAN

Interface	Description	Received				Transmitted			
		Bytes	Pkts	Errs	Drops	Bytes	Pkts	Errs	Drops

Reset Statistics

xTM

This window displays the Router's xTM statistics. Click the **Reset** button to refresh these statistics.

Interface Statistics

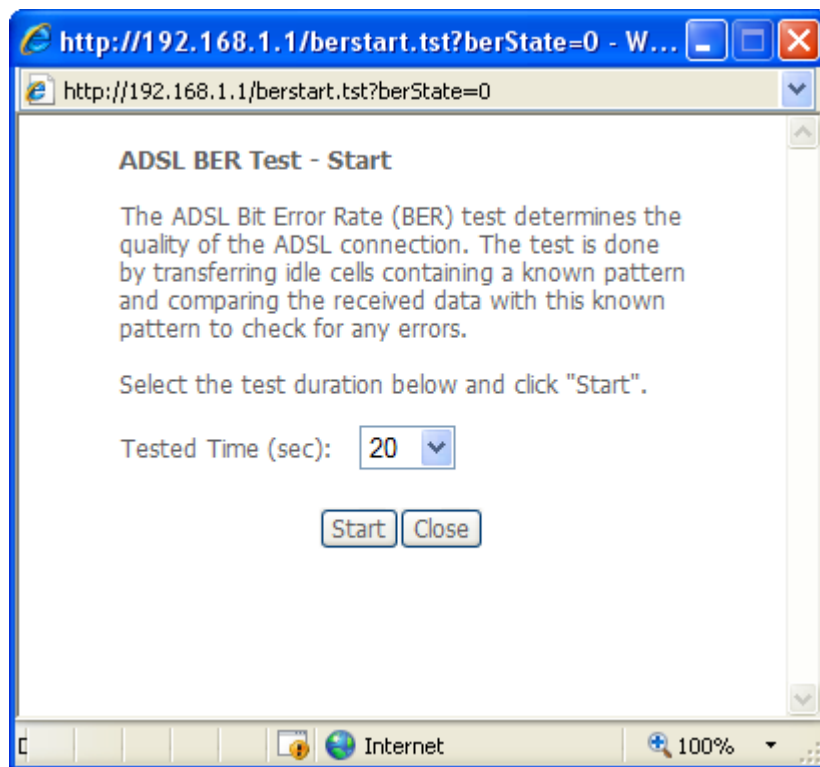
Port Number	In Octets	Out Octets	In Packets	Out Packets	In OAM Cells	Out OAM Cells	In ASM Cells	Out ASM Cells	In Packet Errors	In Cell Errors
-------------	-----------	------------	------------	-------------	--------------	---------------	--------------	---------------	------------------	----------------

Reset

xDSL

This window displays the Router's xDSL statistics.
Click the **Reset Statistics** button to refresh these statistics.

Click the **xDSL BER Test** button to access the ADSL Bit Error Rate Test window displayed below:



Statistics -- xDSL

Mode:		
Traffic Type:		
Status:		Disabled
Link Power State:		
	Downstream	Upstream
Line Coding(Trellis):		
SNR Margin (0.1 dB):		
Attenuation (0.1 dB):		
Output Power (0.1 dBm):		
Attainable Rate (Kbps):		
Rate (Kbps):		
Super Frames:		
Super Frame Errors:		
RS Words:		
RS Correctable Errors:		
RS Uncorrectable Errors:		
HEC Errors:		
OCD Errors:		
LCD Errors:		
Total Cells:		
Data Cells:		
Bit Errors:		
Total ES:		
Total SES:		
Total UAS:		

Route

To access the **Device Info – Route** window, click the **Route** button in the **Device Info** directory.

Route:	This read-only window displays routing info.
---------------	--

Device Info -- Route						
Flags: U - up, ! - reject, G - gateway, H - host, R - reinstate D - dynamic (redirect), M - modified (redirect).						
Destination	Gateway	Subnet Mask	Flag	Metric	Service	Interface
192.168.1.0	0.0.0.0	255.255.255.0	U	0		br0

ARP

To access the **Device Info – ARP** window, click the **ARP** button in the **Device Info** directory.

ARP:	This read-only window displays Address Resolution Protocol info.
-------------	--

Device Info -- ARP			
IP address	Flags	HW Address	Device
192.168.1.10	Complete	00:0C:6E:AA:B9:C0	br0

DHCP

To access the **Device Info – DHCP** window, click the **DHCP** option in the **Device Info** directory. This option will only be available if DHCP is enabled in the LAN settings.

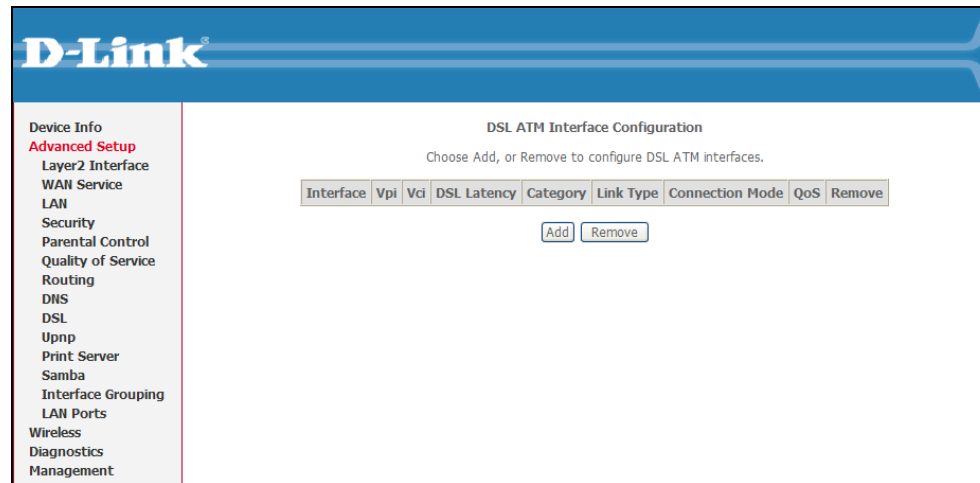
DHCP: This read-only window displays a list of current DHCP clients that are connected to this router.

Device Info -- DHCP Leases

Hostname	MAC Address	IP Address	Expires In
----------	-------------	------------	------------

Advanced Setup

This chapter includes the more advanced features used for network management and security as well as administrative tools to manage the Router view status and other information used to examine performance and for troubleshooting.



The screenshot displays the D-Link web interface for DSL ATM Interface Configuration. The left sidebar contains a navigation menu with the following items: Device Info, **Advanced Setup**, Layer2 Interface, WAN Service, LAN, Security, Parental Control, Quality of Service, Routing, DSL, Upnp, Print Server, Samba, Interface Grouping, LAN Ports, Wireless, Diagnostics, and Management. The main content area is titled "DSL ATM Interface Configuration" and includes the instruction "Choose Add, or Remove to configure DSL ATM interfaces." Below this instruction is a table with the following headers: Interface, Vpi, Vci, DSL Latency, Category, Link Type, Connection Mode, QoS, and Remove. Underneath the table are two buttons: "Add" and "Remove".

Layer2 Interface

ATM Interface:

Choose **Add**, or **Remove** to configure DSL ATM interfaces.

This screen allows you to configure an **ATM PVC identifier** (VPI and VCI), select DSL latency, and select a service category. Otherwise choose an existing interface by selecting the checkbox to enable it.

Select **Select DSL Link Type (EoA is for PPPoE, IPoE, and Bridge.), Encapsulation Mode and Service Category.**

Enabling packet level QoS for PVC improves performance for selected classes of applications. QoS cannot be set for CBR and Real-time VBR. QoS consumes system resources; therefore the number of PVCs will be reduced. Use Advanced Setup/Quality of Service to assign priorities for the applications.

Click **Apply/Save** to add the new ATM Interface.

DSL ATM Interface Configuration

Choose Add, or Remove to configure DSL ATM interfaces.

Interface	Vpi	Vci	DSL Latency	Category	Link Type	Connection Mode	QoS	Remove
<input type="button" value="Add"/> <input type="button" value="Remove"/>								

ATM PVC Configuration

This screen allows you to configure an ATM PVC identifier (VPI and VCI), select DSL latency, select a service category. Otherwise choose an existing interface by selecting the checkbox to enable it.

VPI: [0-255]

VCI: [32-65535]

Select DSL Link Type (EoA is for PPPoE, IPoE, and Bridge.)

- EoA
 PPPoA
 IPoA

Encapsulation Mode:

Service Category:

Select Connection Mode

- Default Mode - Single service over one connection
 VLAN MUX Mode - Multiple Vlan service over one connection
 MSC Mode - Multiple Service over one Connection

Enable Quality Of Service

Enabling packet level QoS for a PVC improves performance for selected classes of applications. QoS cannot be set for CBR and Realtime VBR. QoS consumes system resources; therefore the number of PVCs will be reduced. Use **Advanced Setup/Quality of Service** to assign priorities for the applications.

Enable Quality Of Service.

Point-to-Point over ATM (PPPoA) is a network protocol for encapsulating PPP frames over ATM.

When selecting **PPPoA**, the user can still change the **Encapsulation Mode** and the **Service Category** but the **Connection Mode** will no longer be available to edit.

When selecting **IPoA**, the user can still change the **Encapsulation Mode** and the **Service Category** but the **Connection Mode** will no longer be available to edit.

Select DSL Link Type (EoA is for PPPoE, IPoE, and Bridge.)

EoA
 PPPoA
 IPoA

Encapsulation Mode: VC/MUX

Service Category: UBR Without PCR

Enable Quality Of Service

Enabling packet level QoS for a PVC improves performance for selected classes of applications. QoS cannot be set for CBR and Realtime VBR. QoS consumes system resources; therefore the number of PVCs will be reduced. Use **Advanced Setup/Quality of Service** to assign priorities for the applications.

Enable Quality Of Service.

Back Apply/Save

Select DSL Link Type (EoA is for PPPoE, IPoE, and Bridge.)

EoA
 PPPoA
 IPoA

Encapsulation Mode: LLC/SNAP-ROUTING

Service Category: UBR Without PCR

Enable Quality Of Service

Enabling packet level QoS for a PVC improves performance for selected classes of applications. QoS cannot be set for CBR and Realtime VBR. QoS consumes system resources; therefore the number of PVCs will be reduced. Use **Advanced Setup/Quality of Service** to assign priorities for the applications.

Enable Quality Of Service.

Back Apply/Save

Wide Area Network (WAN) Service

The Wide Area Network (WAN) Service Setup page can be used to setup services regarding the WAN interface. The WAN interface on this router is the DSL port side. When setting up the WAN configuration you can choose between various WAN interface connection methods. Before configuring WAN Service, the information in Layer2 Interface section needs to be configured.

Display:	<p>This window is used to configure the WAN interface. You can add, delete and modify WAN interfaces on this window.</p> <p>If you are setting up the WAN interface for the first time, click the Add button.</p> <p>Make sure Layer2 Interface is configured before clicking the Add button.</p>
Add:	<p>WAN Service Interface Configuration – Select Interface:</p> <p>Select a Layer 2 Interface for this service from the drop-down menu, and click the Next button.</p>

Wide Area Network (WAN) Service Setup

Choose Add, Remove, or Edit to configure a WAN service over a selected interface.

Interface	Description	Type	Vlan8021p	VlanMuxId	ConnId	IgmP	NAT	Firewall	Remove	Edit
<div style="display: flex; justify-content: center; gap: 10px;"> Add Remove Save/Reboot </div>										

WAN Service Interface Configuration

Select a layer 2 interface for this service

Note: For ATM interface, the descriptor string is (portId_vpi_vci)
 For PTM interface, the descriptor string is (portId_high_low)
 Where portId=0 --> DSL Latency PATH0
 portId=1 --> DSL Latency PATH1
 portId=4 --> DSL Latency PATH0&1
 low =0 --> Low PTM Priority not set
 low =1 --> Low PTM Priority set
 high =0 --> High PTM Priority not set
 high =1 --> High PTM Priority set

atm0/(0_0_35) ▼

Back
Next

PPP over Ethernet

WAN Service Configuration – PPPoE:

Step 1: To setup a PPPoE Interface select the **PPP over Ethernet (PPPoE)** and click the **Next** button.

The Service Description will be added automatically.

WAN Service Configuration

Select WAN service type:

- PPP over Ethernet (PPPoE)
- IP over Ethernet
- Bridging

Enter Service Description:

Step 2 - PPPoE:

- PPP Username:** Enter the PPP Account Username here.
- PPP Password:** Enter the PPP Account Password here.
- PPPoE Service Name:** Type in a Service Name here.
- Authentication Method:** Choose an Authentication Method. If you don't know the Authentication Method, leave this on Auto.
- Enable Fullcone NAT:** Tick to enable Fullcone NAT
- Enable NAT:** Tick this option to enable NAT for this connection.
- Enable Firewall:** Tick this option to enable firewall for this connection.
- Keep Alive PPP connection:** Tick the option to enable keep alive function of PPP connection.
- LCP echo interval (seconds):** Enter a time in second to determine how often to send an echo message to an idle link.
- IP fragmentation low threshold:** The lowest threshold value for the LCP packet.
- IP fragmentation high threshold:** The highest threshold value for the LCP packet
- IP fragmentation time (seconds):** Enter a time in second for IP fragmentation time.
- Dial on demand:** Tick to enable Dial on Demand.
- PPP IP extension:** Tick to enable PPP IP Extension.
- Static IPv4 Address:** Tick to enable Static IP version 4 address.
- IPv4 Address:** The option appears when **Use Static IPv4 Address** is selected. Enter the Static IP version 4 address used here.
- PPP Debug Mode:** Tick to enable PPP Debug Mode.
- Bridge PPPoE:** Tick to bridge of PPPoE frames between the WAN interface and the local ports.
- IGMP Multicast Proxy:** Tick to enable IGMP Multicast Proxy.
- MTU:** Enter a maximum transmission unit value here.
Click **Next** to continue the setup.

PPP Username and Password

PPP usually requires that you have a user name and password to establish your connection. In the boxes below, enter the user name and password that your ISP has provided to you.

PPP Username:

PPP Password:

PPPoE Service Name:

Authentication Method:

Enable Fullcone NAT

Enable NAT

Enable Firewall

Keep alive PPP connection

LCP echo interval(seconds):

IP fragmentation low threshold:

IP fragmentation high threshold:

IP fragmentation time (seconds):

Dial on demand (with idle timeout timer)

PPP IP extension

Use Static IPv4 Address

Enable PPP Debug Mode

Bridge PPPoE Frames Between WAN and Local Ports

Multicast Proxy

Enable IGMP Multicast Proxy

PPP Link Setting

MTU

Step 3 - PPPoE Routing – Default Gateway:

Select a preferred wan interface as the system default gateway.

Click **Next** to continue the setup.

Routing -- Default Gateway

Select a preferred wan interface as the system default gateway.

Selected WAN Interface

<p>Step 4 – PPPoE</p> <p>Obtain DNS:</p> <p>Static DNS:</p>	<p>DNS Server Configuration:</p> <p>Get DNS server information from the selected WAN interface OR enter static DNS server IP addresses. If only single PVC with IPoA or static MER protocol is configured, you must enter static DNS server IP addresses.</p> <p>Select this option to enable automatic DNS discovery from the WAN interface.</p> <p>Select this option and enter the DNS IP addresses if needed.</p> <p>Click Next to continue the setup</p>	<p>DNS Server Configuration</p> <p>Get DNS server information from the selected WAN interface OR enter static DNS server IP addresses. If only a single PVC with IPoA or static MER protocol is configured, you must enter static DNS server IP addresses.</p> <p><input checked="" type="radio"/> Obtain DNS info from a WAN interface:</p> <p>WAN Interface selected: <input type="text" value="pppoe_0_0_35/ppp0"/></p> <p><input type="radio"/> Use the following Static DNS IP address:</p> <p>Primary DNS server: <input type="text"/></p> <p>Secondary DNS server: <input type="text"/></p> <p><input type="button" value="Back"/> <input type="button" value="Next"/></p>
--	---	--

Step 5 - PPPoE WAN Setup – Summary:

Make sure that the settings below match the settings provided by your ISP.

Click **Apply/Save** to have this interface to be effective. Click **Back** to make any modifications.

WAN Setup - Summary

Make sure that the settings below match the settings provided by your ISP.

PORT / VPI / VCI:	0 / 0 / 35
Connection Type:	Bridge
Service Name:	
Service Category:	UBR
IP Address:	Not Applicable
Service State:	Enabled
NAT:	Disabled
Full Cone NAT:	Disabled
Firewall:	Disabled
IGMP Multicast:	Not Applicable
Quality Of Service:	Disabled

Click "Apply/Save" to have this interface to be effective. Click "Back" to make any modifications.

[Back](#) [Apply/Save](#)

IP over Ethernet (IPoE) WAN Service Configuration

Step 1 - IPoE: To setup an IPoE Interface select the **IP over Ethernet** and click the **Next** button.

The Service Description will be added automatically.

Click **Next** to continue the setup

WAN Service Configuration

Select WAN service type:

- PPP over Ethernet (PPPoE)
 IP over Ethernet
 Bridging

Enter Service Description:

[Back](#) [Next](#)

Step 2 - IPoE WAN IP Settings:

Enter information provided to you by your ISP to configure the WAN IP settings.

Notice: If **Obtain an IP address automatically** is chosen, DHCP will be enabled for PVC in MER mode.

If **Use the following Static IP address** is chosen, enter the WAN IP address, subnet mask and interface gateway.

Click **Next** to continue the setup

WAN IP Settings

Enter information provided to you by your ISP to configure the WAN IP settings.
Notice: If "Obtain an IP address automatically" is chosen, DHCP will be enabled for PVC in MER mode.
If "Use the following Static IP address" is chosen, enter the WAN IP address, subnet mask and interface gateway.

Obtain an IP address automatically

Option 60 Vendor ID:

Option 61 IAID: (8 hexadecimal digits)

Option 61 DUID: (hexadecimal digit)

Option 125: Disable Enable

Use the following Static IP address:

WAN IP Address:

WAN Subnet Mask:

WAN gateway IP Address:

Step 3 - IPoE Network Address Translation Settings:

Network Address Translation (NAT) allows you to share one Wide Area Network (WAN) IP address for multiple computers on your Local Area Network (LAN).

Select **Enable Firewall** to use the default firewall options on this interface.

Select **Enable IGMP Multicast** to allow IGMP Multicasting on this interface.

Click **Next** to continue the setup

Network Address Translation Settings

Network Address Translation (NAT) allows you to share one Wide Area Network (WAN) IP address for multiple computers on your Local Area Network (LAN).

Enable NAT

Enable Firewall

IGMP Multicast

Enable IGMP Multicast

Back Next

Step 4 - IPoE Routing – Default Gateway:

Select a preferred wan interface as the system default gateway.

Click **Next** to continue the setup.

Routing -- Default Gateway

Select a preferred wan interface as the system default gateway.

Selected WAN Interface ipoe_0_0_35/atm0 ▼

Back Next

<p>Step 5 – IPoE</p> <p>Obtain DNS:</p> <p>Static DNS:</p>	<p>DNS Server Configuration:</p> <p>Get DNS server information from the selected WAN interface OR enter static DNS server IP addresses. If only single PVC with IPoA or static MER protocol is configured, you must enter static DNS server IP addresses.</p> <p>Select this option to enable automatic DNS discovery from the WAN interface.</p> <p>Select this option and enter the DNS IP addresses if needed.</p> <p>Click Next to continue the setup</p>	<p>DNS Server Configuration</p> <p>Get DNS server information from the selected WAN interface OR enter static DNS server IP addresses. If only a single PVC with IPoA or static MER protocol is configured, you must enter static DNS server IP addresses.</p> <p><input checked="" type="radio"/> Obtain DNS info from a WAN interface:</p> <p>WAN Interface selected: / <input type="button" value="v"/></p> <p><input type="radio"/> Use the following Static DNS IP address:</p> <p>Primary DNS server: <input type="text"/></p> <p>Secondary DNS server: <input type="text"/></p> <p><input type="button" value="Back"/> <input type="button" value="Next"/></p>
---	---	--

Step 6 - IPoE WAN Setup – Summary:

Make sure that the settings below match the settings provided by your ISP.

Click **Apply/Save** to have this interface to be effective. Click **Back** to make any modifications.

WAN Setup - Summary

Make sure that the settings below match the settings provided by your ISP.

PORT / VPI / VCI:	0 / 0 / 35
Connection Type:	Bridge
Service Name:	
Service Category:	UBR
IP Address:	Not Applicable
Service State:	Enabled
NAT:	Disabled
Full Cone NAT:	Disabled
Firewall:	Disabled
IGMP Multicast:	Not Applicable
Quality Of Service:	Disabled

Click "Apply/Save" to have this interface to be effective. Click "Back" to make any modifications.

[Back](#) [Apply/Save](#)

Bridging WAN Service Configuration

Step 1 - Bridging: To setup a Bridging Interface select the **Bridging** and click the **Next** button.

The Service Description will be added automatically.

Click **Next** to continue the setup

WAN Service Configuration

Select WAN service type:

- PPP over Ethernet (PPPoE)
- IP over Ethernet
- Bridging

Enter Service Description:

[Back](#) [Next](#)

Step 2 - Bridging**WAN Setup – Summary:**

Make sure that the settings below match the settings provided by your ISP.

Click **Apply/Save** to have this interface to be effective. Click **Back** to make any modifications.

WAN Setup - Summary

Make sure that the settings below match the settings provided by your ISP.

PORT / VPI / VCI:	0 / 0 / 35
Connection Type:	Bridge
Service Name:	br_0_0_35
Service Category:	UBR
IP Address:	Not Applicable
Service State:	Enabled
NAT:	Disabled
Full Cone NAT:	Disabled
Firewall:	Disabled
IGMP Multicast:	Not Applicable
Quality Of Service:	Disabled

Click "Apply/Save" to have this interface to be effective. Click "Back" to make any modifications.

[Back](#)[Apply/Save](#)

<p>PPP over ATM</p> <p>Step 1:</p>	<p>WAN Service Interface Configuration:</p> <p>Select a Layer 2 Interface with PPPoA settings for this service from the drop-down menu, and click the Next button.</p>
--	--

WAN Service Interface Configuration

Select a layer 2 interface for this service

Note: For ATM interface, the descriptor string is (portId_vpi_vci)
 For PTM interface, the descriptor string is (portId_high_low)
 Where portId=0 --> DSL Latency PATH0
 portId=1 --> DSL Latency PATH1
 portId=4 --> DSL Latency PATH0&1
 low =0 --> Low PTM Priority not set
 low =1 --> Low PTM Priority set
 high =0 --> High PTM Priority not set
 high =1 --> High PTM Priority set

<p>Step 2 - PPPoA</p>	<p>WAN Service Configuration – PPPoA:</p> <p>The Service Description will be added automatically.</p> <p>Click the Next button.</p>
------------------------------	---

WAN Service Configuration

Enter Service Description:

Step 3 - PPPoA	
PPP Username:	Enter the PPP Account Username here.
PPP Password:	Enter the PPP Account Password here.
Authentication Method:	Choose an Authentication Method. If you don't know the Authentication Method, leave this on Auto.
Enable Fullcone NAT:	Tick to enable Fullcone NAT
Enable NAT:	Tick this option to enable NAT for this connection.
Enable Firewall:	Tick this option to enable firewall for this connection.
Keep Alive PPP connection:	Tick the option to enable keep alive function of PPP connection.
LCP echo interval (seconds):	Enter a time in second to determine how often to send an echo message to an idle link.
IP fragmentation low threshold:	The lowest threshold value for the LCP packet.
IP fragmentation high threshold:	The highest threshold value for the LCP packet
IP fragmentation time (seconds):	Enter a time in second for IP fragmentation time.
Dial on demand:	Tick to enable Dial on Demand.
PPP IP extension:	Tick to enable PPP IP Extension.
Static IPv4 Address:	Tick to enable Static IP version 4 address.
IPv4 Address:	The option appears when Use Static IPv4 Address is selected. Enter the Static IP version 4 address used here.
PPP Debug Mode:	Tick to enable PPP Debug Mode.
IGMP Multicast Proxy:	Tick to enable IGMP Multicast Proxy.
MTU:	Enter a maximum transmission unit value here.
Click Next to continue the setup.	

PPP Username and Password

PPP usually requires that you have a user name and password to establish your connection. In the boxes below, enter the user name and password that your ISP has provided to you.

PPP Username:

PPP Password:

Authentication Method: AUTO

Enable Fullcone NAT

Enable NAT

Enable Firewall

Keep alive PPP connection

LCP echo interval(seconds):

IP fragmentation low threshold:

IP fragmentation high threshold:

IP fragmentation time (seconds):

Dial on demand (with idle timeout timer)

PPP IP extension

Use Static IPv4 Address

Enable PPP Debug Mode

Multicast Proxy

Enable IGMP Multicast Proxy

PPP Link Setting

MTU


Step 4 - PPPoA Routing – Default Gateway:

Select a preferred WAN interface as the system default gateway.

Click **Next** to continue the setup.

Routing -- Default Gateway

Select a preferred wan interface as the system default gateway.

Selected WAN Interface / 

[Back](#) [Next](#)

Step 5 – PPPoA DNS Server Configuration:

Get DNS server information from the selected WAN interface OR enter static DNS server IP addresses. If only single PVC with IPoA or static MER protocol is configured, you must enter static DNS server IP addresses.

Obtain DNS: Select this option to enable automatic DNS discovery from the WAN interface.

Static DNS: Select this option and enter the DNS IP addresses if needed.

Click **Next** to continue the setup

DNS Server Configuration

Get DNS server information from the selected WAN interface OR enter static DNS server IP addresses. If only a single PVC with IPoA or static MER protocol is configured, you must enter static DNS server IP addresses.

Obtain DNS info from a WAN interface:

WAN Interface selected: /

Use the following Static DNS IP address:

Primary DNS server:

Secondary DNS server:

Step 5 - PPPoA WAN Setup – Summary:

Make sure that the settings below match the settings provided by your ISP.

Click **Apply/Save** to have this interface to be effective. Click **Back** to make any modifications.

WAN Setup - Summary

Make sure that the settings below match the settings provided by your ISP.

PORT / VPI / VCI:	0 / 0 / 35
Connection Type:	PPPoA
Service Name:	pppoa_0_0_35
Service Category:	UBR
IP Address:	Automatically Assigned
Service State:	Enabled
NAT:	Enabled
Full Cone NAT:	Disabled
Firewall:	Enabled
IGMP Multicast:	Disabled
Quality Of Service:	Disabled

Click "Apply/Save" to have this interface to be effective. Click "Back" to make any modifications.

[Back](#)[Apply/Save](#)

IP over ATM WAN Service Interface Configuration – IPoA:

Step 1: Select a Layer 2 Interface with IPoA settings for this service from the drop-down menu, and click the **Next** button.

WAN Service Interface Configuration

Select a layer 2 interface for this service

Note: For ATM interface, the descriptor string is (portId_vpi_vci)
 For PTM interface, the descriptor string is (portId_high_low)
 Where portId=0 --> DSL Latency PATH0
 portId=1 --> DSL Latency PATH1
 portId=4 --> DSL Latency PATH0&1
 low =0 --> Low PTM Priority not set
 low =1 --> Low PTM Priority set
 high =0 --> High PTM Priority not set
 high =1 --> High PTM Priority set

ipoa0/(0_10_40) ▼

Back Next

Step 2 - IPoA: WAN Service configuration

The Service Description will be added automatically.

Click the **Next** button.

WAN Service Configuration

Enter Service Description: ipoa_0_10_40

Back Next

Step 3 - IPoA:	<p>WAN IP Settings</p> <p>WAN IP Address: Enter the WAN IP address used here. WAN Subnet Mask: Enter the subnet of the WAN IP address.</p> <p>Click Next to continue the setup.</p>
-----------------------	--

WAN IP Settings

Enter information provided to you by your ISP to configure the WAN IP settings.

WAN IP Address:

WAN Subnet Mask:

Step 4 – IPoA	<p>Network Address Translation Settings:</p> <p>Enable NAT: Tick this option to enable NAT for this connection. Enable Firewall: Tick this option to enable firewall for this connection. IGMP Multicast: Tick to enable IGMP Multicast Proxy.</p> <p>Click Next to continue the setup.</p>
----------------------	--

Network Address Translation Settings

Network Address Translation (NAT) allows you to share one Wide Area Network (WAN) IP address for multiple computers on your Local Area Network (LAN).

Enable NAT

Enable Firewall

IGMP Multicast

Enable IGMP Multicast

Step 5 – IPoA Routing -- Default Gateway

Select a preferred WAN interface as the system default gateway.

Click **Next** to continue the setup

Routing -- Default Gateway

Select a preferred wan interface as the system default gateway.

Selected WAN Interface ▼

Step 5 - IPoA WAN Setup – Summary:

Make sure that the settings below match the settings provided by your ISP.

Click **Apply/Save** to have this interface to be effective. Click **Back** to make any modifications.

WAN Setup - Summary

Make sure that the settings below match the settings provided by your ISP.

PORT / VPI / VCI:	0 / 10 / 40
Connection Type:	IPoA
Service Name:	ipoa_0_10_40
Service Category:	UBR
IP Address:	192.168.0.1
Service State:	Enabled
NAT:	Disabled
Full Cone NAT:	Disabled
Firewall:	Disabled
IGMP Multicast:	Disabled
Quality Of Service:	Disabled

Click "Apply/Save" to have this interface to be effective. Click "Back" to make any modifications.

[Back](#)[Apply/Save](#)

LAN

You can configure the LAN IP address to suit your preference. Many users will find it convenient to use the default settings together with DHCP service to manage the IP settings for their private network. The IP address of the Router is the base address used for DHCP. In order to use the Router for DHCP on your LAN, the IP address pool used for DHCP must be compatible with the IP address of the Router. The IP addresses available in the DHCP IP address pool will change automatically if you change the IP address of the Router.

Display:	To access the Local Area Network (LAN) Setup window, click the LAN button in the Advanced Setup directory.
GroupName:	Select the appropriate group name. By default there is only one group
IP Address:	Enter the LAN IP address for the router here.
Subnet Mask:	Enter the Subnet Mask for the router here.
Enable IGMP Snooping:	Tick this option to enable IGMP Snooping.
Standard Mode:	Select to use Standard Mode. (If IGMP Snooping is enabled)
Blocking Mode:	Select to use Blocking Mode. (If IGMP Snooping is enabled)
Disable/ Enable DHCP Server:	Choose to enable or disable the DHCP Server here.
Start IP Address:	Enter a starting IP Address for the DHCP pool here.
End IP Address:	Enter an end IP Address for the DHCP pool here.
Lease Time:	Enter a DHCP Lease Time value here.
	To add reserve an IP to a specific host click the Add Entries button.

Local Area Network (LAN) Setup

Configure the DSL Router IP Address and Subnet Mask for LAN interface. GroupName Default

IP Address:

Subnet Mask:

Enable IGMP Snooping

Disable DHCP Server

Enable DHCP Server

Start IP Address:

End IP Address:

Leased Time (hour):

Static IP Lease List: (A maximum 32 entries can be configured)

MAC Address	IP Address	Remove

Configure the second IP Address and Subnet Mask for LAN interface

<p>Mac Address: IP Address:</p>	<p>To reserve an IP for a specific host the user must know the specific host's Mac Address.</p> <p>Enter the reserved host's Mac Address in here. Enter the reserved host's IP Address in here.</p> <p>Click Apply/Save to continue.</p>
---	---

<p>Static IP Lease List:</p>	<p>All the reserved DHCP client entries will be listed here.</p>
-------------------------------------	--

<p>Second IP Address:</p>	<p>To enable a second LAN interface IP tick this option and enter a second IP address and Subnet Mask for the router here.</p> <p>Note: The second LAN IP Address must be of a different IP range than the current first IP Address.</p>
----------------------------------	---

DHCP Static IP Lease

Enter the Mac address and Static IP address then click "Apply/Save" .

MAC Address:

IP Address:

Static IP Lease List: (A maximum 32 entries can be configured)

MAC Address	IP Address	Remove
00:12:34:56:78:90	192.168.1.10	<input type="checkbox"/>

Configure the second IP Address and Subnet Mask for LAN interface

IP Address:

Subnet Mask:

NAT – Virtual Servers

Virtual Server allows you to direct incoming traffic from WAN side (identified by Protocol and External port) to the internal server with private IP address on the LAN side. The Internal port is required only if the external port needs to be converted to a different port number used by the server on the LAN side. The **NAT** button appears when configuring WAN interface in PPPoE, or IPoA.

To Add a Virtual Server Rule, click the **Add** button.

NAT -- Virtual Servers Setup

Virtual Server allows you to direct incoming traffic from WAN side (identified by Protocol and External port) to the Internal server with private IP address on the LAN side. The Internal port is required only if the external port needs to be converted to a different port number used by the server on the LAN side. A maximum 32 entries can be configured.

Server Name	External Port Start	External Port End	Protocol	Internal Port Start	Internal Port End	Server IP Address	WAN Interface	Remove
-------------	---------------------	-------------------	----------	---------------------	-------------------	-------------------	---------------	--------

Select the **service name**, and enter the **server IP address** and click **Apply/Save** to forward IP packets for this service to the specified server.

NOTE: The "Internal Port End" cannot be modified directly. Normally, it is set to the same value as "External Port End". However, if you modify "Internal Port Start", then "Internal Port End" will be set to the same value as "Internal Port Start".

A **maximum** number of **32 entries** can be configured.

View the newly added rule.

NAT -- Virtual Servers

Select the service name, and enter the server IP address and click "Apply/Save" to forward IP packets for this service to the specified server. **NOTE: The "Internal Port End" cannot be modified directly. Normally, it is set to the same value as "External Port End". However, if you modify "Internal Port Start", then "Internal Port End" will be set to the same value as "Internal Port Start".** Remaining number of entries that can be configured:32

Use Interface:

Service Name:

Select a Service:

Custom Service:

Server IP Address:

External Port Start	External Port End	Protocol	Internal Port Start	Internal Port End
<input type="text"/>	<input type="text"/>	TCP	<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>	TCP	<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>	TCP	<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>	TCP	<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>	TCP	<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>	TCP	<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>	TCP	<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>	TCP	<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>	TCP	<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>	TCP	<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>	TCP	<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>	TCP	<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>	TCP	<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>	TCP	<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>	TCP	<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>	TCP	<input type="text"/>	<input type="text"/>

NAT -- Virtual Servers Setup

Virtual Server allows you to direct incoming traffic from WAN side (identified by Protocol and External port) to the Internal server with private IP address on the LAN side. The Internal port is required only if the external port needs to be converted to a different port number used by the server on the LAN side. A maximum 32 entries can be configured.

Server Name	External Port Start	External Port End	Protocol	Internal Port Start	Internal Port End	Server IP Address	WAN Interface	Remove
Web Server (HTTP)	80	80	TCP	80	80	192.168.1.20	ppp0	<input type="checkbox"/>

NAT – Port Triggering

Some applications require that specific ports in the Router's firewall be opened for access by the remote parties. Port Trigger dynamically opens up the 'Open Ports' in the firewall when an application on the LAN initiates a TCP/UDP connection to a remote party using the 'Triggering Ports'. The Router allows the remote party from the WAN side to establish new connections back to the application on the LAN side using the 'Open Ports'. A maximum 32 entries can be configured.

To Add a Port Triggering Rule click the **Add** button.

NAT -- Port Triggering Setup

Some applications require that specific ports in the Router's firewall be opened for access by the remote parties. Port Trigger dynamically opens up the 'Open Ports' in the firewall when an application on the LAN initiates a TCP/UDP connection to a remote party using the 'Triggering Ports'. The Router allows the remote party from the WAN side to establish new connections back to the application on the LAN side using the 'Open Ports'. A maximum 32 entries can be configured.

Application Name	Trigger		Open			WAN Interface	Remove
	Protocol	Port Range	Protocol	Port Range			
		Start		End	Start		

Some applications such as games, video conferencing, remote access applications and others require that specific ports in the Router's firewall be opened for access by the applications.

You can configure the port settings from this screen by selecting an existing application or creating your own (Custom application) and click **Save/Apply** to add it.

A maximum number of 32 entries can be configured.

View the newly added rule.

NAT -- Port Triggering

Some applications such as games, video conferencing, remote access applications and others require that specific ports in the Router's firewall be opened for access by the applications. You can configure the port settings from this screen by selecting an existing application or creating your own (Custom application) and click "Save/Apply" to add it.

Remaining number of entries that can be configured:0

Use Interface:

Application Name:

Select an application:

Custom application:

Trigger Port Start	Trigger Port End	Trigger Protocol	Open Port Start	Open Port End	Open Protocol
<input type="text"/>	<input type="text"/>	TCP	<input type="text"/>	<input type="text"/>	TCP
<input type="text"/>	<input type="text"/>	TCP	<input type="text"/>	<input type="text"/>	TCP
<input type="text"/>	<input type="text"/>	TCP	<input type="text"/>	<input type="text"/>	TCP
<input type="text"/>	<input type="text"/>	TCP	<input type="text"/>	<input type="text"/>	TCP
<input type="text"/>	<input type="text"/>	TCP	<input type="text"/>	<input type="text"/>	TCP
<input type="text"/>	<input type="text"/>	TCP	<input type="text"/>	<input type="text"/>	TCP
<input type="text"/>	<input type="text"/>	TCP	<input type="text"/>	<input type="text"/>	TCP
<input type="text"/>	<input type="text"/>	TCP	<input type="text"/>	<input type="text"/>	TCP
<input type="text"/>	<input type="text"/>	TCP	<input type="text"/>	<input type="text"/>	TCP

NAT -- Port Triggering Setup

Some applications require that specific ports in the Router's firewall be opened for access by the remote parties. Port Trigger dynamically opens up the 'Open Ports' in the firewall when an application on the LAN initiates a TCP/UDP connection to a remote party using the 'Triggering Ports'. The Router allows the remote party from the WAN side to establish new connections back to the application on the LAN side using the 'Open Ports'. A maximum 32 entries can be configured.

Application Name	Trigger		Open			WAN Interface	Remove
	Protocol	Port Range	Protocol	Port Range			
		Start End		Start	End		
ICQ	UDP	4000 4000	TCP	20000	20059	ppp0	<input type="checkbox"/>

NAT – DMZ Host

The DSL router will forward IP packets from the WAN that do not belong to any of the applications configured in the Virtual Servers table to the DMZ host computer.

Enter the computer's IP address and click **Save/Apply** to activate the DMZ host.

Clear the IP address field and click **Save/Apply** to deactivate the DMZ host.

NAT -- DMZ Host

The DSL router will forward IP packets from the WAN that do not belong to any of the applications configured in the Virtual Servers table to the DMZ host computer.

Enter the computer's IP address and click "Apply" to activate the DMZ host.

Clear the IP address field and click "Apply" to deactivate the DMZ host.

DMZ Host IP Address:

Save/Apply

NAT – ALG

ALG, known as Application Level Gateway or Application Layer Gateway, consists of a security component that augments a firewall or NAT employed in a computer network. The main function for ALG on this gateway is to allow NAT traversal to SIP applications.

Tick the **SIP Enabled** check box to enable ALG on this router and click **Save/Apply**.

ALG

Select the ALG below.

SIP Enabled

Save/Apply

Security – IP Filtering

When a computer connects to the Internet, it begins communicating with other networking device and computers and by the norm is taking a risk. Internet Security is the method to safely secure a local network from unwanted intrusions from the Internet and also to the Internet. This page allow for two main security methods that can be used. The first method is to block any node and ONLY allowing certain users to connect through this router. The second method is to allow any node and ONLY blocking certain users to connect through this router.

The basic firewall of this router should be sufficient enough to keep unwanted guests from browsing your network from the Internet. This page will add to this already applied security feature

IP Filtering - Outgoing

This window allows you to create a filter rule to block outgoing IP traffic by specifying a filter name and at least one condition on this window. All of the specified conditions in this filter rule must be satisfied for the rule to take effect. Filters are used to allow or deny LAN or WAN users from accessing the Internet or your internal network. Click the **Change Policy** to change between **BLOCK** and **ACCEPT** the rules.

If you are setting up the outgoing IP filtering, click the **Add** button.

IP Filtering – Incoming

The Inbound Filter allows you to create a filter rule to allow incoming IP traffic by specifying a filter name and at least one condition on this window. All of the specified conditions in this filter rule must be satisfied for the rule to take effect. By default, all incoming IP traffic from the Internet is blocked when the firewall is enabled. Click the **Change Policy** to change between **BLOCK** and **ACCEPT** the rules.

If you are setting up the incoming IP filtering, click the **Add** button.

Outgoing IP Filtering Setup

By default, all outgoing IP traffic from LAN is allowed, but some IP traffic can be **BLOCK** by setting up filters.

[Change Policy](#)

Choose Add or Remove to configure outgoing IP filters.

Filter Name	Protocol	Source Address / Mask	Source Port	Dest. Address / Mask	Dest. Port	Remove
Add Remove						

Incoming IP Filtering Setup

By default, all incoming IP traffic from WAN is denied, but some IP traffic can be **ACCEPT** by setting up filters.

[Change Policy](#)

Choose Add or Remove to configure incoming IP filters.

Filter Name	Interfaces	Protocol	Source Address / Mask	Source Port	Dest. Address / Mask	Dest. Port	Remove
Add Remove							

<p>Filter Name: Protocol: Source IP Address: Source Subnet Mask: Source Port: Destination IP Address: Destination Subnet Mask: Destination Port:</p>	<p>Outgoing Rule - Add</p> <p>Enter a name for the new rule here. Select the appropriate protocol used here. Enter the Source IP address here. Enter the Source Subnet Mask here. Enter the Source port number here. Enter the Destination IP address here. Enter the Destination Subnet Mask here. Enter the Destination port number here.</p> <p>Click Apply/Save to add the rule.</p>
<p>Filter Name: Protocol: Source IP Address: Source Subnet Mask: Source Port: Destination IP Address: Destination Subnet Mask: Destination Port: WAN/LAN Interfaces:</p>	<p>Incoming Rule - Add</p> <p>Enter a name for the new rule here. Select the appropriate protocol used here. Enter the Source IP address here. Enter the Source Subnet Mask here. Enter the Source port number here. Enter the Destination IP address here. Enter the Destination Subnet Mask here. Enter the Destination port number here.</p> <p>Here you can select the appropriate WAN/LAN interface that this rule will use.</p> <p>Click Apply/Save to add the rule.</p>

Add IP Filter -- Outgoing

The screen allows you to create a filter rule to identify outgoing IP traffic by specifying a new filter name and at least one condition below. All of the specified conditions in this filter rule must be satisfied for the rule to take effect. Click 'Apply/Save' to save and activate the filter.

Filter Name:

Protocol:

Source IP address:

Source Subnet Mask:

Source Port (port or port:port):

Destination IP address:

Destination Subnet Mask:

Destination Port (port or port:port):

Add IP Filter -- Incoming

The screen allows you to create a filter rule to identify incoming IP traffic by specifying a new filter name and at least one condition below. All of the specified conditions in this filter rule must be satisfied for the rule to take effect. Click 'Apply/Save' to save and activate the filter.

Filter Name:

Protocol:

Source IP address:

Source Subnet Mask:

Source Port (port or port:port):

Destination IP address:

Destination Subnet Mask:

Destination Port (port or port:port):

WAN Interfaces (Configured in Routing mode and with firewall enabled)
 Select one or more WAN interfaces displayed below to apply this rule.

Select All

pppoe_0_0_35/ppp0

IP Filtering – Outgoing

The new rule is added.

IP Filtering – Incoming

The new rule is added.

Outgoing IP Filtering SetupBy default, all outgoing IP traffic from LAN is allowed, but some IP traffic can be **BLOCKED** by setting up filters.

Choose Add or Remove to configure outgoing IP filters.

Filter Name	Protocol	Source Address / Mask	Source Port	Dest. Address / Mask	Dest. Port	Remove
Name	TCP/UDP	192.168.1.10 / 255.255.255.0	10	192.168.1.10 / 255.255.255.0	10	<input type="checkbox"/>

Incoming IP Filtering SetupBy default, all incoming IP traffic from the WAN is blocked when the firewall is enabled. However, some IP traffic can be **ACCEPTED** by setting up filters.

Choose Add or Remove to configure incoming IP filters.

Filter Name	Interfaces	Protocol	Source Address / Mask	Source Port	Dest. Address / Mask	Dest. Port	Remove
Name	ppp0	TCP/UDP	192.168.1.10 / 255.255.255.0	12	192.168.1.10 / 255.255.255.0	12	<input type="checkbox"/>

Security – Mac Filtering

MAC Filtering is only effective on ATM PVCs configured in Bridge mode.

FORWARDED means that all MAC layer frames will be FORWARDED except those matching with any of the specified rules in the following table.

BLOCKED means that all MAC layer frames will be BLOCKED except those matching with any of the specified rules in the following table.

WARNING: Changing from one policy to another of an interface will cause all defined rules for that interface to be REMOVED AUTOMATICALLY! You will need to create new rules for the new policy.

MAC Filtering Policy For Each Interface:

To change the Policy simply tick the **Change** check box and click the **Change Policy** button.

Choose **Add** or **Remove** to configure MAC filtering rules.

Interface	Policy	Change
atm1	BLOCKED	<input type="checkbox"/>

[Change Policy](#)

Interface	Policy	Change
atm1	FORWARD	<input type="checkbox"/>

[Change Policy](#)

Interface	Protocol	Destination MAC	Source MAC	Frame Direction	Remove
Add Remove					

Create a filter to identify the MAC layer frames by specifying at least one condition below. If multiple conditions are specified, all of them take effect.

Click **Save/Apply** to save and activate the filter.

View the newly added rule.

Add MAC Filter

Create a filter to identify the MAC layer frames by specifying at least one condition below. If multiple conditions are specified, all of them take effect. Click "Apply" to save and activate the filter.

Protocol Type:

Destination MAC Address:

Source MAC Address:

Frame Direction:

WAN Interfaces (Configured in Bridge mode only)

Interface	Protocol	Destination MAC	Source MAC	Frame Direction	Remove
atm1	IGMP	00:12:34:56:78:90	01:23:45:67:89:01	BOTH	<input type="checkbox"/>

Parental Control – Time Restriction

Another powerful security feature is by simply making the router inactive or inaccessible at certain times. This page allows the user to setup a time schedule to block a specific Mac address.

Use this window to deny access to specified MAC address. If you are setting up the MAC address blocking, click the **Add** button.

MAC address is a specially formatted text string (xx:xx:xx:xx:xx:xx) that uniquely identification of a device. This section will allow users to block devices with certain MAC addresses on the LAN.

To configure for MAC address blocking, enter the username into the Username field, click **Browser's MAC Address** to have MAC address of the LAN device, or click **Other MAC Address** and enter a MAC address manually. Tick the checkboxes for the desired individual days of the week and enter desired Start Blocking Time and End Blocking Time.

Click the **Apply/Save** button to save the configuration

An added rule will look like this.

Access Time Restriction -- A maximum 16 entries can be configured.

Username	MAC	Mon	Tue	Wed	Thu	Fri	Sat	Sun	Start	Stop	Remove

Access Time Restriction

This page adds time of day restriction to a special LAN device connected to the Router. The 'Browser's MAC Address' automatically displays the MAC address of the LAN device where the browser is running. To restrict other LAN device, click the "Other MAC Address" button and enter the MAC address of the other LAN device. To find out the MAC address of a Windows based PC, go to command window and type "ipconfig /all".

User Name

Browser's MAC Address

Other MAC Address

(xx:xx:xx:xx:xx:xx)

Days of the week	Mon	Tue	Wed	Thu	Fri	Sat	Sun
Click to select	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Start Blocking Time (hh:mm)

End Blocking Time (hh:mm)

URL Filter -- Please select the list type first then configure the list entries. Maximum 100 entries can be configured.

URL List Type: Exclude Include

Address	Port	Remove
http://www.game.com	80	<input type="checkbox"/>

Parental Control – URL Filter

Another powerful security measure that this router provides is the blocking or allowing of certain URL addresses. This page allows the user to configure URL filtering.

Use this window to allow or deny access to a specified URL address. If you are setting up the URL filtering, click the **Add** button.

To configure URL Filtering, enter a URL in the **URL address** space and also specify the **port number**. By default a website's port used is port number 80.

Click **Apply/Save** to continue.

The new rule is added.

URL Filter -- Please select the list type first then configure the list entries. Maximum 100 entries can be configured.

URL List Type: Exclude Include

Address	Port	Remove

Parental Control -- URL Filter Add

Enter the URL address and port number then click "Apply/Save" to add the entry to the URL filter.

URL Address:

Port Number: (Default 80 will be applied if leave blank.)

URL Filter -- Please select the list type first then configure the list entries. Maximum 100 entries can be configured.

URL List Type: Exclude Include

Address	Port	Remove
http://www.game.com	80	<input type="checkbox"/>

Quality of Service (QoS)

QoS or Quality of Service allows the router to help prioritize the data packet flow in your Router and network. This is very important for time sensitive applications such as VoIP where it may help prevent dropped calls. Large amounts of non-critical data can be scaled so as not to affect these prioritized sensitive real-time programs.

Queue Management Configuration

If Enable QoS checkbox is selected, choose a default DSCP mark to automatically mark incoming traffic without reference to a particular classifier. Click **Apply/Save** button to save it.

NOTE: If the **Enable QoS** checkbox is not selected, all QoS will be disabled for all interfaces.

NOTE: The default DSCP mark is used to mark all egress packets that do not match any classification rules.

QoS Queue Setup

If you disable WMM function in Wireless Page, queues related to wireless will not take effects

Click the **Add** button to add a Queue Setup rule.

QoS -- Queue Management Configuration

If Enable QoS checkbox is selected, choose a default DSCP mark to automatically mark incoming traffic without reference to a particular classifier. Click 'Apply/Save' button to save it.

Note: If Enable QoS checkbox is not selected, all QoS will be disabled for all interfaces.

Note: The default DSCP mark is used to mark all egress packets that do not match any classification rules.

Enable QoS

Apply/Save

QoS Queue Setup -- A maximum 16 entries can be configured.

If you disable WMM function in Wireless Page, queues related to wireless will not take effects

The QoS function has been disabled. Queues would not take effects.

Name	Key	Interface	Precedence	DSL Latency	PTM Priority	Enable	Remove
WMM Voice Priority	1	wl0	1			Enabled	
WMM Voice Priority	2	wl0	2			Enabled	
WMM Video Priority	3	wl0	3			Enabled	
WMM Video Priority	4	wl0	4			Enabled	
WMM Best Effort	5	wl0	5			Enabled	
WMM Background	6	wl0	6			Enabled	
WMM Background	7	wl0	7			Enabled	
WMM Best Effort	8	wl0	8			Enabled	

Add

Adding a Queue Setup Rule

The screen allows you to configure a QoS queue entry and assign it to a specific network interface. Each of the queues can be configured for a specific precedence. The queue entry configured here will be used by the classifier to place ingress packets appropriately. **NOTE:** Lower integer values for precedence imply higher priority for this queue relative to others. Click **Apply/Save** to save and activate the queue.

QoS Classification Setup

Choose **Add** or **Remove** to configure network traffic classes. If you disable WMM function in Wireless Page, classification related to wireless will not take effects.

A maximum 32 entries can be configured.

QoS Queue Configuration

The screen allows you to configure a QoS queue entry and assign it to a specific network interface. Each of the queues can be configured for a specific precedence. The queue entry configured here will be used by the classifier to place ingress packets appropriately. **Note: Lower integer values for precedence imply higher priority for this queue relative to others.** Click 'Apply/Save' to save and activate the queue.

Name:

Enable: ▾

Interface:

Precedence: ▾

QoS Classification Setup -- A maximum 32 entries can be configured.

Choose Add or Remove to configure network traffic classes.
If you disable WMM function in Wireless Page, classification related to wireless will not take effects.

The QoS function has been disabled. Classification rules would not take effects.

		CLASSIFICATION CRITERIA										CLASSIFICATION RESULTS						
Class Name	Order	Class Intf	Ether Type	SrcMAC/ Mask	DstMAC/ Mask	SrcIP/ Mask	DstIP/ Mask	Proto	Src Port	Dst Port	DSCP Check	802.1P Check	Queue Key	DSCP Mark	802.1P Mark	VlanID Tag	Enable	Remove
<input type="button" value="Add"/>																		

Add Network Traffic Class Rule

The screen creates a traffic class rule to classify the upstream traffic, assign queue which defines the precedence and the interface and optionally overwrite the IP header DSCP byte. A rule consists of a class name and at least one condition below. All of the specified conditions in this classification rule must be satisfied for the rule to take effect.

Click **Apply/Save** to save and activate the rule.

Add Network Traffic Class Rule

The screen creates a traffic class rule to classify the upstream traffic, assign queue which defines the precedence and the interface and optionally overwrite the IP header DSCP byte. A rule consists of a class name and at least one condition below. All of the specified conditions in this classification rule must be satisfied for the rule to take effect. Click 'Save/Apply' to save and activate the rule.

Traffic Class Name:

Rule Order: ▼

Rule Status: ▼

Specify Classification Criteria

A blank criterion indicates it is not used for classification.

Class Interface: ▼

Ether Type: ▼

Source MAC Address:

Source MAC Mask:

Destination MAC Address:

Destination MAC Mask:

Specify Classification Results

Must select a classification queue. A blank mark or tag value means no change.

Assign Classification Queue: ▼

Mark Differentiated Service Code Point (DSCP): ▼

Mark 802.1p priority: ▼

Tag VLAN ID [0-4094]:

Routing

Routing is the process of selecting paths in a network along which to send network traffic. The router allows the user to configure routing in 3 ways. Specifying the **Default Route**, setting up **Static Route** or configuring **RIP**.

Default Gateway

Select a preferred wan interface as the system default gateway.

Click **Save/Apply** to save and activate the rule.

Routing -- Default Gateway

Select a preferred wan interface as the system default gateway.

Selected WAN Interface

Save/Apply

Static Route

To add a static route, click the **Add** button.

Routing -- Static Route (A maximum 32 entries can be configured)

Destination	Subnet Mask	Gateway	Interface	Remove
-------------	-------------	---------	-----------	--------

Add

Remove

Enter the Destination Network Address, Subnet Mask, and the available WAN interface from the **User Interface** drop-down menu. Click the **Apply/Save** button to add the entry to the routing table.

Routing -- Static Route Add

Enter the destination network address, subnet mask, gateway AND/OR available WAN interface then click "Apply/Save" to add the entry to the routing table.

Destination Network Address:

Subnet Mask:

Use Interface

Apply/Save

Routing Interface Protocol (RIP) Configuration

To activate RIP for the WAN Interface, select the desired RIP version and operation and place a check in the 'Enabled' checkbox. To stop RIP on the WAN Interface, uncheck the 'Enabled' checkbox. Click the **Apply/Save** button to star/stop RIP and save the configuration.

NOTE: RIP CANNOT BE CONFIGURED on the WAN interface which has NAT enabled (such as PPPoE).

Routing -- RIP Configuration

NOTE: RIP CANNOT BE CONFIGURED on the WAN interface which has NAT enabled (such as PPPoE).

To activate RIP for the WAN Interface, select the desired RIP version and operation and place a check in the 'Enabled' checkbox. To stop RIP on the WAN Interface, uncheck the 'Enabled' checkbox. Click the 'Apply/Save' button to star/stop RIP and save the configuration.

Interface	Version	Operation	Enabled
atm1	2	Passive	<input type="checkbox"/>

Apply/Save

Domain Name Server (DNS) Configuration

The Domain Name System (DNS) is a hierarchical naming system for computers, services, or any resource participating in the Internet. On this router the user can either let the WAN interface automatically configure the DNS settings or the user can manually setup the DNS configuration.

DNS Server Configuration

Select the configured WAN interface for DNS server information OR enter the static DNS server IP Addresses for single PVC with IPoA, static IPoE protocol.

DNS Server Configuration

Select the configured WAN interface for DNS server information OR enter the static DNS server IP Addresses for single PVC with IPoA, static IPoE protocol.

Obtain DNS info from a WAN interface:

WAN Interface selected:

Use the following Static DNS IP address:

Primary DNS server:

Secondary DNS server:

Dynamic DNS Configuration

The Dynamic DNS service allows you to alias a dynamic IP address to a static hostname in any of the many domains, allowing your DSL router to be more easily accessed from various locations on the Internet.

Dynamic DNS Configuration

Choose Add or Remove to configure Dynamic DNS.

Adding a Rule

This page allows you to add a Dynamic DNS address from DynDNS.org, TZO, or dlinkddns.com.

Dynamic DNS

The Dynamic DNS service allows you to alias a dynamic IP address to a static hostname in any of the many domains, allowing your DSL router to be more easily accessed from various locations on the Internet.

Choose Add or Remove to configure Dynamic DNS.

Hostname Username Service Interface Remove

Add Remove

Add Dynamic DNS

This page allows you to add a Dynamic DNS address from DynDNS.org or TZO.

D-DNS provider

DynDNS.org ▼

Hostname

Interface

pppoe_0_0_35/ppp0 ▼

DynDNS Settings

Username

Password

Apply/Save

Viewing

After add the rule you can view it here.

Dynamic DNS

The Dynamic DNS service allows you to alias a dynamic IP address to a static hostname in any of the many domains, allowing your DSL router to be more easily accessed from various locations on the Internet.

Choose Add or Remove to configure Dynamic DNS.

Hostname	Username	Service	Interface	Remove
DynamicDNS	Username	dyndns	ppp0	<input type="checkbox"/>

DSL Settings

On the DSL Settings page the user can configure the DSL modulation settings, phone line pairing, test modes and even the tone selection.

Modulation, Phone line pairing and Capability

Choose the appropriate modulation type needed for the DSL connection here.

Choose the phone line pair to be used here.

Choose the appropriate capability used here.

Click **Apply/Save** to save and activate the change.

To change some of the advanced settings, click the **Advanced Settings** button.

DSL Settings

Select the modulation below.

- G.Dmt Enabled
- G.lite Enabled
- T1.413 Enabled
- ADSL2 Enabled
- AnnexL Enabled
- ADSL2+ Enabled
- AnnexM Enabled

Select the phone line pair below.

- Inner pair
- Outer pair

Capability

- Bitswap Enable
- SRA Enable

Advanced Settings

Here the user can choose which test mode the router must use.

Click **Apply** to save and activate the change.

To change the Tone Selection, click the **Tone Selection** button.

DSL Advanced Settings

Select the test mode below.

- Normal
- Reverb
- Medley
- No retrain
- L3

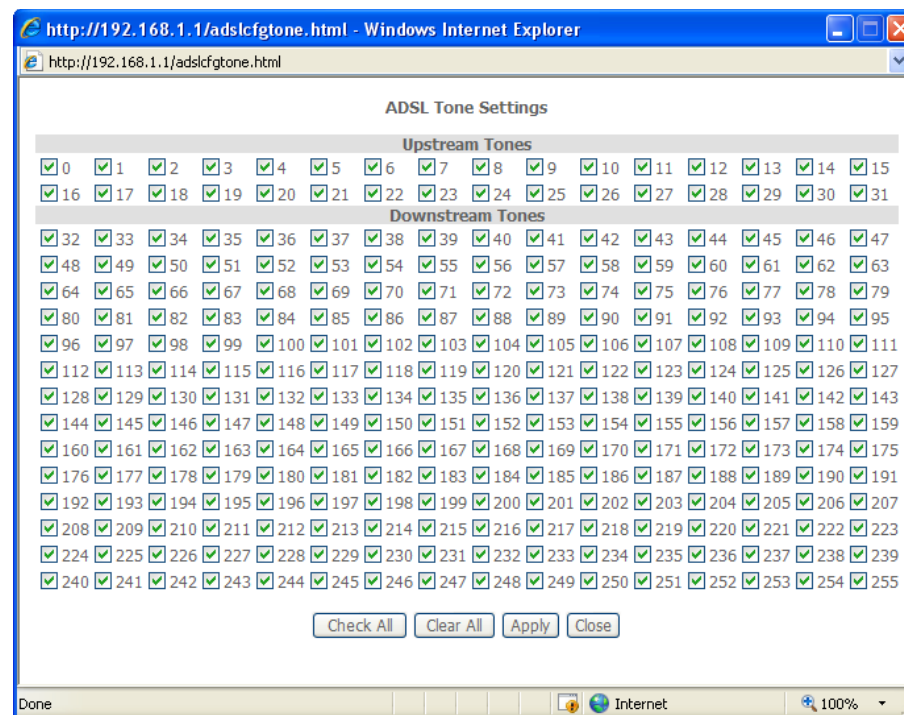
Apply

Tone Selection

ADSL Tone Settings

Select the appropriate upstream and downstream tones for your ADSL Connection.

Click **Apply** to save and activate the change.



Universal Plug and Play (UPnP) Configuration

UPnP supports zero-configuration networking and automatic discovery for many types of networked devices. When enabled, it allows other devices that support UPnP to dynamically join a network, obtain an IP address, convey its capabilities, and learn about the presence and capabilities of other devices. DHCP and DNS service can also be used if available on the network. UPnP also allows supported devices to leave a network automatically without adverse effects to the device or other devices on the network. UPnP is a protocol supported by diverse networking media including Ethernet, Firewire, phone line, and power line networking.

UPnP Configuration

To enable UPnP for any available connection, tick the Enable or disable UPnP protocol check box and click the **Apply/Save** button.

Upnp Configuration

Enable UPnP protocol.

Apply/Save

Print Server Settings

The router can be configured as a print server. Plug a USB printer into the USB port of the Router to share the printer within the local network. To access the **Print Server** window, click the **Print Server** button in the **Advanced Setup** directory.

Print Server Settings

Tick the **Enable on-board print server** check box. Enter the **Printer Name**, and **Make and model** to make the Router act as a print server.

Click the **Save/Apply** button to save the changes.

Note: Refer to p.106 Add a Network Printer in Windows XP section to see how to add a printer to the network.

Print Server settings

This page allows you to enable / disable printer support.

Enable on-board print server.

Printer name

Make and model

Apply/Save

Samba USB Storage

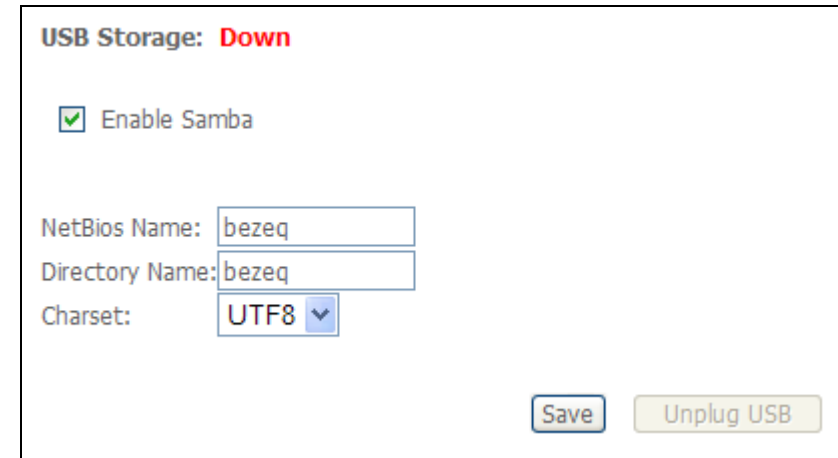
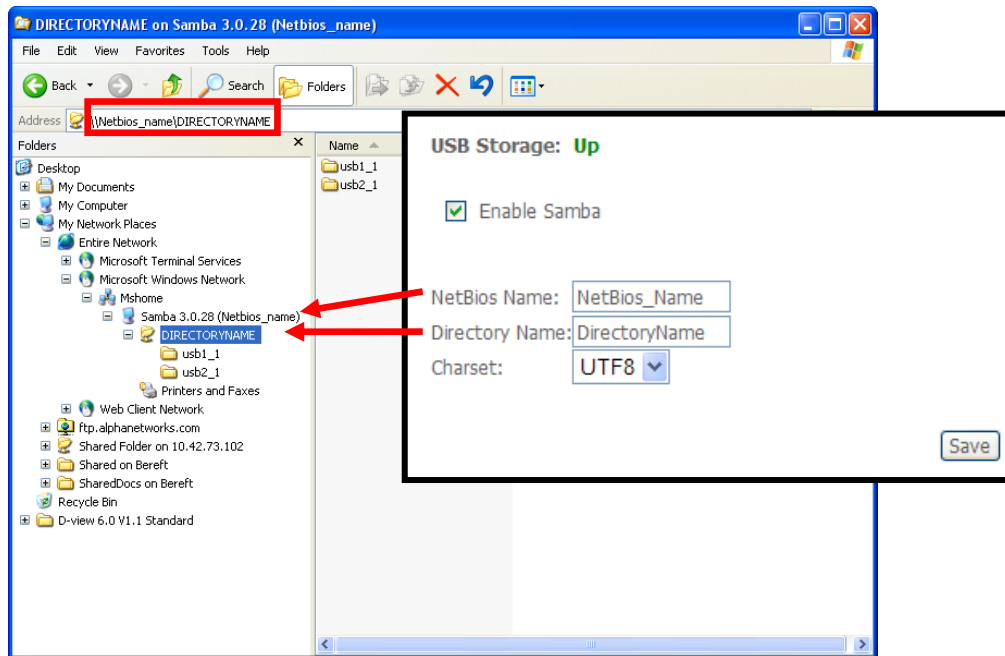
Samba is an Open Source/Free Software suite that provides USB storage device file sharing functions. The Router offers two USB ports to plug in USB storage devices. You can share the files in the USB devices with multiple PCs or laptops within the local network. To access the **Samba Config** window, click the **Samba Config** button in the **Advanced Setup** directory.

USB Storage

To activate the Samba function, tick the Enable Samba check box, and enter the NetBIOS Name and Directory Name.

Click **Save** to save and activate the change.

You can also safely remove the USB storage device by clicking the **Unplug USB** button before removing the USB storage device.



PPTP

To access the **PPTP Setting** window, click the **PPTP** button in the **Advanced Setup** directory.

To set up Point-to-Point Tunnel Protocol, tick the Enable check box, enter the appropriate information in the fields offered, and then click the **Save/Apply** button when you are finished.

PPTP Setting

Set Point to Point Tunnel Protocol (VPN)

Enable	<input type="checkbox"/>
Tunnel Name	<input type="text"/>
PPTP Server IP Address	<input type="text"/>
User Name	<input type="text"/>
Password	<input type="text"/>
Authentication Method	AUTO <input type="button" value="v"/>
Compression Method	AUTO <input type="button" value="v"/>
Default Route	<input type="checkbox"/>
Peer IP Address	<input type="text"/>
Peer Subnet Mask	<input type="text"/>

Interface Grouping

Interface Grouping supports multiple ports to PVC and bridging groups. Each group will perform as an independent network.

Interface Grouping

To support this feature, you must create mapping groups with appropriate LAN and WAN interfaces using the Add button. The Remove button will remove the grouping and add the ungrouped interfaces to the Default group. Only the default group has IP interface.

A maximum 16 entries can be configured.

Interface Grouping -- A maximum 16 entries can be configured

Interface Grouping supports multiple ports to PVC and bridging groups. Each group will perform as an independent network. To support this feature, you must create mapping groups with appropriate LAN and WAN interfaces using the Add button. The Remove button will remove the grouping and add the ungrouped interfaces to the Default group. Only the default group has IP interface.

Group Name	Remove	WAN Interface	LAN Interfaces	DHCP Vendor IDs
Default		ppp0	ENET(1-4)	
		atm1	USB	
			wlan0	
			wl0_Guest1	
			wl0_Guest2	
		wl0_Guest3		

Adding an interface group

To create a new interface group:

1. Enter the Group name and the group name must be unique and select either 2. (dynamic) or 3. (static) below:
2. If you like to automatically add LAN clients to a WAN Interface in the new group add the DHCP vendor ID string. By configuring a DHCP vendor ID string any DHCP client request with the specified vendor ID (DHCP option 60) will be denied an IP address from the local DHCP server.
3. Select interfaces from the available interface list and add it to the grouped interface list using the arrow buttons to create the required mapping of the ports. Note that these clients may obtain public IP addresses
4. Click the **Apply/Save** button to make the changes effective immediately

IMPORTANT: If a vendor ID is configured for a specific client device please REBOOT the client device attached to the modem to allow it to obtain an appropriate IP address.

Interface grouping Configuration

To create a new interface group:

1. Enter the Group name and the group name must be unique and select either 2. (dynamic) or 3. (static) below:
2. If you like to automatically add LAN clients to a WAN Interface in the new group add the DHCP vendor ID string. By configuring a DHCP vendor ID string any DHCP client request with the specified vendor ID (DHCP option 60) will be denied an IP address from the local DHCP server.
3. Select interfaces from the available interface list and add it to the grouped interface list using the arrow buttons to create the required mapping of the ports. **Note that these clients may obtain public IP addresses**
4. Click Save/Apply button to make the changes effective immediately

IMPORTANT If a vendor ID is configured for a specific client device, please REBOOT the client device attached to the modem to allow it to obtain an appropriate IP address.

Group Name:

WAN Interface used in the grouping

	<input type="button" value=">"/> <input type="button" value="<"/>	<input type="text" value="wlan0"/> <input type="text" value="w10_Guest1"/> <input type="text" value="w10_Guest2"/> <input type="text" value="w10_Guest3"/>
--	--	---

Automatically Add Clients With the following DHCP Vendor IDs

LAN Ports Configuration

Use this page to enable/disable the Virtual LAN Ports feature.

LAN Ports Configuration

Tick the ENET (1-4) option to include ports 1-4 to the Virtual LAN ports feature.

Click **Apply/Save** to save and activate the change.

LAN Ports Configuration

Use this page to enable/disable the Virtual LAN Ports feature.

ENET(1-4)

Apply/Save

LAN Port
ENET(1-4)
USB
wlan0

Wireless

Wireless communication is to transfer data from point A to point B without the need for physical cabling.

D-Link

Device Info
Advanced Setup
Wireless
Basic
Security
MAC Filter
Wireless Bridge
Advanced
Station Info
Diagnostics
Management

Wireless -- Basic

This page allows you to configure basic features of the wireless LAN interface. You can enable or disable the wireless LAN interface, hide the network from active scans, set the wireless network name (also known as SSID) and restrict the channel set based on country requirements. Click "Apply/Save" to configure the basic wireless options.

Enable Wireless
 Hide Access Point
 Clients Isolation
 Disable WMM Advertise
 Enable Wireless Multicast Forwarding (WMM)

SSID:
 BSSID: 00:15:e9:d1:f8:bc
 Country:
 Max Clients:

Wireless - Guest/Virtual Access Points:

Enabled	SSID	Hidden	Isolate Clients	Disable WMM Advertise	Enable WMM	Max Clients	BSSID
<input type="checkbox"/>	<input type="text" value="wl0_Guest1"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="text" value="16"/>	N/A
<input type="checkbox"/>	<input type="text" value="wl0_Guest2"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="text" value="16"/>	N/A
<input type="checkbox"/>	<input type="text" value="wl0_Guest3"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="text" value="16"/>	N/A

Basic Wireless Configuration

This page allows you to configure basic features of the wireless LAN interface.

Basic Configuration

You can enable or disable the wireless LAN interface, hide the network from active scans, set the wireless network name (also known as SSID) and restrict the channel set based on country requirements.

Click **Apply/Save** to configure the basic wireless options.

Wireless -- Basic

This page allows you to configure basic features of the wireless LAN interface. You can enable or disable the wireless LAN interface, hide the network from active scans, set the wireless network name (also known as SSID) and restrict the channel set based on country requirements. Click "Apply/Save" to configure the basic wireless options.

- Enable Wireless
- Hide Access Point
- Clients Isolation
- Disable WMM Advertise
- Enable Wireless Multicast Forwarding (WMF)

SSID:

BSSID: 00:15:e9:d1:f8:bc

Country:

Max Clients:

Wireless - Guest/Virtual Access Points:

Enabled	SSID	Hidden	Isolate Clients	Disable WMM Advertise	Enable WMF	Max Clients	BSSID
<input type="checkbox"/>	<input type="text" value="wl0_Guest1"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="text" value="16"/>	N/A
<input type="checkbox"/>	<input type="text" value="wl0_Guest2"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="text" value="16"/>	N/A
<input type="checkbox"/>	<input type="text" value="wl0_Guest3"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="text" value="16"/>	N/A

Security

This page allows you to configure security features of the wireless LAN interface. You may setup configuration manually or through Wi-Fi Protected Setup (WPS). The Windows Security Center (WSC) or Action Center is a component included with Microsoft's Windows XP (beginning with Service Pack 2), Windows Vista and Windows 7 operating systems that provides users with the ability to view the status of computer security settings and services.

Wireless Security

You can set the network authentication method manually, selecting data encryption, specifying whether a network key is required to authenticate to this wireless network and specify the encryption strength.

Click **Apply/Save** when done.

Wireless -- Security

This page allows you to configure security features of the wireless LAN interface.
You may setup configuration manually

Manual Setup AP

You can set the network authentication method, selecting data encryption, specify whether a network key is required to authenticate to this wireless network and specify the encryption strength.
Click "Apply/Save" when done.

Select SSID:

Network Authentication:

WEP Encryption:

Wired Equivalent Privacy (WEP)

WEP is the most basic form of wireless security. There are two variations of WEP known as Open System and Shared authentication. Open System allows for a two-way hand shake authentication whereas Shared authentication allows for a four-way handshake before authentication is completed.

Using WEP the user will be prompt to select one of the four key spaces and then to enter a security key according to the strength specified.

Enter 13 ASCII characters or 26 hexadecimal digits for 128-bit encryption keys

Enter 5 ASCII characters or 10 hexadecimal digits for 64-bit encryption keys

Click **Apply/Save** to save and activate the changes.

Wireless -- Security

This page allows you to configure security features of the wireless LAN interface.
You may setup configuration manually

Manual Setup AP

You can set the network authentication method, selecting data encryption, specify whether a network key is required to authenticate to this wireless network and specify the encryption strength.
Click "Apply/Save" when done.

Select SSID:

Network Authentication:

WEP Encryption:

Encryption Strength:

Current Network Key:

Network Key 1:

Network Key 2:

Network Key 3:

Network Key 4:

Enter 13 ASCII characters or 26 hexadecimal digits for 128-bit encryption keys
Enter 5 ASCII characters or 10 hexadecimal digits for 64-bit encryption keys

802.1X

802.1X security allow for the addition of a Radius Server to your network for added security. This is the strongest form of wireless security available.

When choosing 802.1X you'll need to specify and Radius Server IP Address. A Radius Port number and a Radius Key used.

Click **Apply/Save** to save and activate the change.

Wireless -- Security

This page allows you to configure security features of the wireless LAN interface. You may setup configuration manually

Manual Setup AP

You can set the network authentication method, selecting data encryption, specify whether a network key is required to authenticate to this wireless network and specify the encryption strength. Click "Apply/Save" when done.

Select SSID:	dlink
Network Authentication:	802.1X
RADIUS Server IP Address:	0.0.0.0
RADIUS Port:	1812
RADIUS Key:	
WEP Encryption:	Enabled
Encryption Strength:	128-bit
Current Network Key:	2
Network Key 1:	1234567890123
Network Key 2:	1234567890123
Network Key 3:	1234567890123
Network Key 4:	1234567890123

Enter 13 ASCII characters or 26 hexadecimal digits for 128-bit encryption keys
Enter 5 ASCII characters or 10 hexadecimal digits for 64-bit encryption keys

Apply/Save

Wi-Fi Protected Access (WPA)-Enterprise

WPA is the replacement for WEP (which is seen by many administrators as a 'weak' security method). There are two variations of WPA known as WPA-EAP (Enterprise) and WPA-PSK (Personal).

When choosing to use WPA-EAP the user has to specify a Radius Server IP Address, Radius Server Port and a Radius Key.

Click **Apply/Save** to save and activate the change.

Wi-Fi Protected Access (WPA)-Personal

When choosing to use WPA-PSK the user only has to specify a Pre-Shared Key. Note that there is NO Radius Server settings required when configuring WPA-PSK.

Enter the Group Key Interval and Encryption if needed.

Click **Apply/Save** to save and activate the change.

Wireless -- Security

This page allows you to configure security features of the wireless LAN interface.
You may setup configuration manually

Manual Setup AP

You can set the network authentication method, selecting data encryption, specify whether a network key is required to authenticate to this wireless network and specify the encryption strength.
Click "Apply/Save" when done.

Select SSID:	<input type="text" value="dlink"/>
Network Authentication:	<input type="text" value="WPA"/>
WPA Group Rekey Interval:	<input type="text" value="0"/>
RADIUS Server IP Address:	<input type="text" value="0.0.0.0"/>
RADIUS Port:	<input type="text" value="1812"/>
RADIUS Key:	<input type="text"/>
WPA Encryption:	<input type="text" value="TKIP"/>
WEP Encryption:	<input type="text" value="Disabled"/>
<input type="button" value="Apply/Save"/>	

Wireless -- Security

This page allows you to configure security features of the wireless LAN interface.
You may setup configuration manually

Manual Setup AP

You can set the network authentication method, selecting data encryption, specify whether a network key is required to authenticate to this wireless network and specify the encryption strength.
Click "Apply/Save" when done.

Select SSID:	<input type="text" value="dlink"/>
Network Authentication:	<input type="text" value="WPA-PSK"/>
WPA Pre-Shared Key:	<input type="text"/> Click here to display
WPA Group Rekey Interval:	<input type="text" value="0"/>
WPA Encryption:	<input type="text" value="TKIP"/>
WEP Encryption:	<input type="text" value="Disabled"/>
<input type="button" value="Apply/Save"/>	

Wi-Fi Protected Access (WPA2)-Enterprise

WPA2 is the upgrade for WPA. WPA2 sorts out a couple of security vulnerabilities the WPA might encounter. There are also two variations of WPA2 known as WPA2-EAP (Enterprise) and WPA2-PSK (Personal). When choosing to use WPA2-EAP the user has to specify a Radius Server IP Address, Radius Server Port and a Radius Key.

Click **Apply/Save** to save and activate the change.

Wi-Fi Protected Access (WPA2)-Personal

When choosing to use WPA2-PSK the user only has to specify a Pre-Shared Key. Note that there is NO Radius Server settings required when configuring WPA2-PSK.

Enter the Group Key Interval and Encryption if needed.

Click **Apply/Save** to save and activate the change.

Wireless -- Security

This page allows you to configure security features of the wireless LAN interface. You may setup configuration manually.

Manual Setup AP

You can set the network authentication method, selecting data encryption, specify whether a network key is required to authenticate to this wireless network and specify the encryption strength. Click "Apply/Save" when done.

Select SSID:	<input type="text" value="dlink"/>
Network Authentication:	<input type="text" value="WPA2"/>
WPA2 Preauthentication:	<input type="text" value="Disabled"/>
Network Re-auth Interval:	<input type="text" value="36000"/>
WPA Group Rekey Interval:	<input type="text" value="0"/>
RADIUS Server IP Address:	<input type="text" value="0.0.0.0"/>
RADIUS Port:	<input type="text" value="1812"/>
RADIUS Key:	<input type="text"/>
WPA Encryption:	<input type="text" value="AES"/>
WEP Encryption:	<input type="text" value="Disabled"/>
<input type="button" value="Apply/Save"/>	

Wireless -- Security

This page allows you to configure security features of the wireless LAN interface. You may setup configuration manually.

Manual Setup AP

You can set the network authentication method, selecting data encryption, specify whether a network key is required to authenticate to this wireless network and specify the encryption strength. Click "Apply/Save" when done.

Select SSID:	<input type="text" value="dlink"/>
Network Authentication:	<input type="text" value="WPA2-PSK"/>
WPA Pre-Shared Key:	<input type="text"/> Click here to display
WPA Group Rekey Interval:	<input type="text" value="0"/>
WPA Encryption:	<input type="text" value="AES"/>
WEP Encryption:	<input type="text" value="Disabled"/>
<input type="button" value="Apply/Save"/>	

Mixed Wi-Fi Protected Access (WPA2/WPA)-Enterprise

Mixed WPA2/WPA-EAP provides the functionality of having wireless clients running WPA2-EAP or WPA-EAP. It provides backwards compatibility from WPA2 to WPA.

When choosing to use Mixed WPA2/WPA-EAP the user has to specify a Radius Server IP Address, Radius Server Port and a Radius Key.

Click **Apply/Save** to save and activate the change.

Mixed Wi-Fi Protected Access (WPA2/WPA)-Personal

When choosing to use Mixed WPA2/WPA-PSK the user only has to specify a Pre-Shared Key. Note that there is NO Radius Server settings required when configuring Mixed WPA2/WPA-PSK.

Enter the Group Key Interval and Encryption if needed.

Click **Apply/Save** to save and activate the change.

Wireless -- Security

This page allows you to configure security features of the wireless LAN interface.
You may setup configuration manually

Manual Setup AP

You can set the network authentication method, selecting data encryption, specify whether a network key is required to authenticate to this wireless network and specify the encryption strength.
Click "Apply/Save" when done.

Select SSID:

Network Authentication:

WPA2 Preauthentication:

Network Re-auth Interval:

WPA Group Rekey Interval:

RADIUS Server IP Address:

RADIUS Port:

RADIUS Key:

WPA Encryption:

WEP Encryption:

Wireless -- Security

This page allows you to configure security features of the wireless LAN interface.
You may setup configuration manually

Manual Setup AP

You can set the network authentication method, selecting data encryption, specify whether a network key is required to authenticate to this wireless network and specify the encryption strength.
Click "Apply/Save" when done.

Select SSID:

Network Authentication:

WPA Pre-Shared Key: [Click here to display](#)

WPA Group Rekey Interval:

WPA Encryption:

WEP Encryption:

MAC Filter

Wireless MAC filter is a security option that allows the user to block or allow certain MAC address to and from connecting to the Access Point wireless.

Mac Filter

Select the appropriate SSID from the drop-down list, and click the radio buttons under **MAC Restrict Mode**.

When choosing **Allow**, all users will be blocked and only the allowing MAC Addresses will have access to the wireless network.

When choosing **Block**, all users will be allowed and only the blocked MAC Addresses will not have access to the wireless network.

Click the **Add** button to add a new MAC address for the MAC filter.

Adding a MAC Address

Enter the Wireless Client's MAC Address.

Click **Apply/Save** to save and activate the change.

Wireless -- MAC Filter

Disabled mode: Disable wireless MAC filter policy.
 Allow mode: Only ALLOW computers listed to access wireless network.
 Deny mode: Only DENY computers listed will be blocked to access wireless network

Select SSID:

MAC Restrict Mode: Disabled Allow Deny

Wireless -- MAC Filter

Enter the MAC address and click "Apply/Save" to add the MAC address to the wireless MAC address filters.

MAC Address:

Viewing MAC Filter

The new rule should look like this.

Wireless -- MAC Filter

Disabled mode: Disable wireless MAC filter policy.

Allow mode: Only ALLOW computers listed to access wireless network.

Deny mode: Only DENY computers listed will be blocked to access wireless network

Select SSID:

MAC Restrict Mode: Disabled Allow Deny

MAC Address	Remove
01:23:45:67:89:01	<input type="checkbox"/>

Wireless Bridge

This page allows you to configure wireless bridge features of the wireless LAN interface. You can select Wireless Bridge (also known as Wireless Distribution System) to disable access point functionality. Selecting Access Point enables access point functionality. Wireless bridge functionality will still be available and wireless stations will be able to associate to the AP.

Access Point

There are three options to choose in the Bridge Restrict option: **Enabled**, **Enabled (Scan)** and **Disabled**.

Choose **Enabled** to allow the user entering the remote bridge's MAC address manually.

Choose **Enabled (Scan)** to allow the user selecting remote bridges from a list of bridges automatically picked up.

Choose **Disabled** to disable the wireless bridge option.

Click **Apply/Save** to save the wireless bridge options.

Wireless -- Bridge

This page allows you to configure wireless bridge features of the wireless LAN interface. You can select Wireless Bridge (also known as Wireless Distribution System) to disable access point functionality. Selecting Access Point enables access point functionality. Wireless bridge functionality will still be available and wireless stations will be able to associate to the AP. Select Disabled in Bridge Restrict which disables wireless bridge restriction. Any wireless bridge will be granted access. Selecting Enabled or Enabled(Scan) enables wireless bridge restriction. Only those bridges selected in Remote Bridges will be granted access. Click "Refresh" to update the remote bridges. Wait for few seconds to update. Click "Apply/Save" to configure the wireless bridge options.

AP Mode:

Bridge Restrict:

Remote Bridges MAC Address:

Wireless -- Bridge

This page allows you to configure wireless bridge features of the wireless LAN interface. You can select Wireless Bridge (also known as Wireless Distribution System) to disable access point functionality. Selecting Access Point enables access point functionality. Wireless bridge functionality will still be available and wireless stations will be able to associate to the AP. Select Disabled in Bridge Restrict which disables wireless bridge restriction. Any wireless bridge will be granted access. Selecting Enabled or Enabled(Scan) enables wireless bridge restriction. Only those bridges selected in Remote Bridges will be granted access. Click "Refresh" to update the remote bridges. Wait for few seconds to update. Click "Apply/Save" to configure the wireless bridge options.

AP Mode:

Bridge Restrict:

Remote Bridges MAC Address:

	SSID	BSSID
<input type="checkbox"/>	james1150	00:05:5D:65:59:4A
<input type="checkbox"/>	james54g	00:13:46:E5:3C:72

Wireless -- Bridge

This page allows you to configure wireless bridge features of the wireless LAN interface. You can select Wireless Bridge (also known as Wireless Distribution System) to disable access point functionality. Selecting Access Point enables access point functionality. Wireless bridge functionality will still be available and wireless stations will be able to associate to the AP. Select Disabled in Bridge Restrict which disables wireless bridge restriction. Any wireless bridge will be granted access. Selecting Enabled or Enabled(Scan) enables wireless bridge restriction. Only those bridges selected in Remote Bridges will be granted access. Click "Refresh" to update the remote bridges. Wait for few seconds to update. Click "Apply/Save" to configure the wireless bridge options.

AP Mode:

Bridge Restrict:

Wireless Bridge

There are three options to choose in the Bridge Restrict option: **Enabled**, **Enabled (Scan)** and **Disabled**.

Choose **Enabled** to allow the user entering the remote bridge's MAC address manually.

Choose **Enabled (Scan)** to allow the user selecting remote bridges from a list of bridges automatically picked up.

Choose **Disabled** to disable the wireless bridge option.

Click **Apply/Save** to save the wireless bridge options.

Wireless -- Bridge

This page allows you to configure wireless bridge features of the wireless LAN interface. You can select Wireless Bridge (also known as Wireless Distribution System) to disable access point functionality. Selecting Access Point enables access point functionality. Wireless bridge functionality will still be available and wireless stations will be able to associate to the AP. Select Disabled in Bridge Restrict which disables wireless bridge restriction. Any wireless bridge will be granted access. Selecting Enabled or Enabled(Scan) enables wireless bridge restriction. Only those bridges selected in Remote Bridges will be granted access. Click "Refresh" to update the remote bridges. Wait for few seconds to update. Click "Apply/Save" to configure the wireless bridge options.

AP Mode:

Bridge Restrict:

Remote Bridges MAC Address:

	SSID	BSSID
<input type="checkbox"/>	MD-6117-4	00:50:8A:79:11:45
<input type="checkbox"/>	james1150	00:05:5D:65:59:4A

Wireless -- Bridge

This page allows you to configure wireless bridge features of the wireless LAN interface. You can select Wireless Bridge (also known as Wireless Distribution System) to disable access point functionality. Selecting Access Point enables access point functionality. Wireless bridge functionality will still be available and wireless stations will be able to associate to the AP. Select Disabled in Bridge Restrict which disables wireless bridge restriction. Any wireless bridge will be granted access. Selecting Enabled or Enabled(Scan) enables wireless bridge restriction. Only those bridges selected in Remote Bridges will be granted access. Click "Refresh" to update the remote bridges. Wait for few seconds to update. Click "Apply/Save" to configure the wireless bridge options.

AP Mode:

Bridge Restrict:

Remote Bridges MAC Address:

Wireless -- Bridge

This page allows you to configure wireless bridge features of the wireless LAN interface. You can select Wireless Bridge (also known as Wireless Distribution System) to disable access point functionality. Selecting Access Point enables access point functionality. Wireless bridge functionality will still be available and wireless stations will be able to associate to the AP. Select Disabled in Bridge Restrict which disables wireless bridge restriction. Any wireless bridge will be granted access. Selecting Enabled or Enabled(Scan) enables wireless bridge restriction. Only those bridges selected in Remote Bridges will be granted access. Click "Refresh" to update the remote bridges. Wait for few seconds to update. Click "Apply/Save" to configure the wireless bridge options.

AP Mode:

Bridge Restrict:

Advanced

This page allows you to configure some advanced features of the wireless LAN interface.

Advanced

The user can select a particular channel on which to operate, force the transmission rate to a particular speed, set the fragmentation threshold, set the RTS threshold, set the wakeup interval for clients in power-save mode, set the beacon interval for the access point, set XPress mode and set whether short or long preambles are used and more.

Click **Apply/Save** to configure the advanced wireless options.

Wireless -- Advanced

This page allows you to configure advanced features of the wireless LAN interface. You can select a particular channel on which to operate, force the transmission rate to a particular speed, set the fragmentation threshold, set the RTS threshold, set the wakeup interval for clients in power-save mode, set the beacon interval for the access point, set XPress mode and set whether short or long preambles are used. Click "Apply/Save" to configure the advanced wireless options.

Band:	2.4GHz	
Channel:	6	Current: 6
Auto Channel Timer(min)	0	
802.11n/EWC:	Auto	
Bandwidth:	20MHz in 2.4G Band and 40MHz in 5G Band	Current: 20MHz
Control Sideband:	Lower	Current: None
802.11n Rate:	Auto	
802.11n Protection:	Auto	
Support 802.11n Client Only:	Off	
54g™ Rate:	1 Mbps	
Multicast Rate:	Auto	
Basic Rate:	Default	
Fragmentation Threshold:	2346	
RTS Threshold:	2347	
DTIM Interval:	1	
Beacon Interval:	100	
Global Max Clients:	16	
XPress™ Technology:	Disabled	
Transmit Power:	100%	
WMM(Wi-Fi Multimedia):	Enabled	
WMM No Acknowledgement:	Disabled	
WMM APSD:	Enabled	

Apply/Save

Station Info

This page shows authenticated wireless stations and their status.

Authenticated Stations

This page will display all the current authenticated users connect to this router wireless.

Click the **Refresh** button to refresh this page.

Wireless -- Authenticated Stations

This page shows authenticated wireless stations and their status.

MAC	Associated	Authorized	SSID	Interface
-----	------------	------------	------	-----------

Refresh

Diagnostics

This router is capable of testing the DSL connection. The individual tests are listed below. If a test displays a fail status, click "Re-Run Diagnostic Tests" at the bottom of this page to make sure the fail status is consistent. If the test continues to fail, click **Help** and follow the troubleshooting procedures.

D-Link

Device Info
Advanced Setup
Wireless
Diagnostics
Management

pppoe_0_0_35 Diagnostics

Your modem is capable of testing your DSL connection. The individual tests are listed below. If a test displays a fail status, click "Re-run Diagnostic Tests" at the bottom of this page to make sure the fail status is consistent. If the test continues to fail, click "Help" and follow the troubleshooting procedures.

Test the connection to your local network

Test your ENET(1-4) Connection:	PASS	Help
Test your USB Connection:	FAIL	Help
Test your Wireless Connection:	PASS	Help

Test the connection to your DSL service provider

Test xDSL Synchronization:	FAIL	Help
Test ATM OAM F5 segment ping:	DISABLED	Help
Test ATM OAM F5 end-to-end ping:	DISABLED	Help

Test the connection to your Internet service provider

Test PPP server connection:	DISABLED	Help
Test authentication with ISP:	DISABLED	Help
Test the assigned IP address:	DISABLED	Help
Ping default gateway:	FAIL	Help
Ping primary Domain Name Server:	FAIL	Help

Next Connection
Test Test With OAM F4

Ethernet Connection Test

Pass:	Indicates that the Ethernet interface from your computer is connected to the LAN port of your DSL Router. A flashing or solid green LAN LED on the router also signifies that an Ethernet connection is present and that this test is successful.
Fail:	Indicates that the DSL Router does not detect the Ethernet interface on your computer.

If the test fails, follow the troubleshooting procedures listed below and re-run the diagnostics tests by clicking the 'Rerun Diagnostic Tests' button at the bottom of this page. If all the tests pass, close and restart your Web browser to access the Internet.

Troubleshooting:

1. If you are not able to access this page, verify that the Ethernet cable from your computer or your hub is connected to the LAN port on DSL Router. Reseat the cable by unplugging both ends and reconnecting them to their respective ports.
2. Turn off the DSL Router, wait 10 seconds and turn it back ON.
3. Make sure you are using the Ethernet cable supplied with your DSL Router
4. With the router on, press the reset button on the DSL Router for at least six seconds and release it. This resets the DSL Router to its default settings. Wait for the DSL Router to initialize, then close and restart your Web browser. To reconfigure the router, type your DSL Account username and password.

USB Connection Test

Pass:	Indicates that the USB interface from your computer is connected to the LAN port of your DSL Router.
Fail:	Indicates that the DSL Router does not detect the USB interface on your computer.

If the test fails, follow the troubleshooting procedures listed below and re-run the diagnostics tests by clicking the 'Rerun Diagnostic Tests' button at the bottom of this page. If all the tests pass, close and restart your Web browser to access the Internet.

Troubleshooting:

1. If there is no connection to the USB port of the DSL Router, this test should fail.
2. If you are not able to access this page, verify that the USB cable from your computer or your hub is connected to the LAN port on the DSL Router. Reseat the USB cable by unplugging both ends and reconnecting them to their respective ports.
3. Turn off the DSL Router, wait 10 seconds and turn it back ON.
4. With the router on, press the reset button on the DSL Router for at least six seconds and release it. This resets the DSL Router to its default settings. Wait for the DSL Router to initialize, then close and restart your Web browser. To reconfigure the router, type your DSL Account username and password.

Wireless Connection Test

Pass:	Indicates that the Wireless interface from your computer is connected to the LAN port of your DSL Router. A flashing or solid green LAN LED on the router also signifies that a Wireless connection is present and that this test is successful.
Fail:	Indicates that the DSL Router does not detect the Wireless interface on your computer.

If the test fails, follow the troubleshooting procedures listed below and re-run the diagnostics tests by clicking the 'Rerun Diagnostic Tests' button at the bottom of this page. If all the tests pass, close and restart your Web browser to access the Internet.

Troubleshooting:

1. Verify that the Wireless configurations from your computer and your DSL router are matched and corrected.
2. Turn off the DSL Router, wait 10 seconds and turn it back ON.
3. With the router on, press the reset button on the DSL Router for at least six seconds and release it. This resets the DSL Router to its default settings. Wait for the DSL Router to initialize, then close and restart your Web browser. To reconfigure the router, type your DSL Account username and password.

ADSL Synchronization Test

Pass:	Indicates that the DSL modem has detected a DSL signal from the telephone company. A solid DSL LED on the modem also indicates the detection of a DSL signal from the telephone company.
Fail:	Indicates that the DSL modem does not detect a signal from the telephone company's DSL network. The DSL LED will continue to flash green.

If the test fails, follow the troubleshooting procedures listed below and re-run the diagnostics tests by clicking the 'Rerun Diagnostic Tests' button at the bottom of this page. If all the tests pass, close and restart your Web browser to access the Internet.

Troubleshooting:

1. Make sure your phone line is plugged into the modem.
2. After turning on your DSL modem, wait for at least one minute to establish a connection. Run the diagnostic tests again by clicking the Rerun Diagnostic Tests button at the bottom of this page.
3. Make sure there is no DSL micro filter on the phone cord connecting the DSL modem to the wall jack.
4. Make sure you are using the phone cord that was supplied with your DSL modem or another similar phone cord with four copper wires visible in the plug.
5. If your DSL has been functioning properly for a long period of time and you suddenly are experiencing this problem, there may be a problem with the DSL network. You may need to wait from 30 minutes to a couple of hours, and if you still do not have a solid DSL LED on your modem, call Technical Support.
6. Turn off the power to the DSL modem, wait 10 seconds and turn it back on. Wait at least one minute and if the DSL LED on the modem remains a solid color,

close your Web browser and restart it.

ATM OAM Segment Ping Test

Pass:	Indicates that the DSL modem can communicate with the DSL provider network.
Fail:	Indicates that the DSL modem may not be able to communicate with the DSL provider network. This test may have an effect on your Internet connectivity. Occasionally the DSL provider network may intentionally block this traffic. Therefore if this test fails but you are still able to access the Internet, there is no need to troubleshoot this issue.

If the test fails, follow the troubleshooting procedures listed below and re-run the diagnostics tests by clicking the 'Rerun Diagnostic Tests' button at the bottom of this page. If all the tests pass, close and restart your Web browser to access the Internet.

Troubleshooting:

NOTE: This test will fail if Test ADSL Synchronization also fails. Troubleshoot the Test ADSL Synchronization test first.

1. Turn off the DSL modem, wait 10 seconds and turn it back on.
2. With the modem on, press the external reset button on the DSL modem for at least six seconds and release it. This resets the DSL modem to its default settings. Wait for the DSL modem to completely restart, then close and restart your Web browser. To reconfigure the modem, type your DSL Account username and password.
3. If this is the first time you are setting up your DSL modem, you may need to reconfigure your VPI/VCI settings. Contact ISP Technical Support for assistance.

ATM OAM End-to-end Ping Test

Pass:	Indicates that the DSL modem can communicate with the DSL provider network.
Fail:	Indicates that the DSL modem may not be able to communicate with the DSL provider network. Occasionally the DSL provider network may intentionally block this traffic. Therefore if this test fails but you are still able to access the Internet, there is no need to troubleshoot this issue.

If the test fails, follow the troubleshooting procedures listed below and re-run the diagnostics tests by clicking the 'Rerun Diagnostic Tests' button at the bottom of this page. If all the tests pass, close and restart your Web browser to access the Internet.

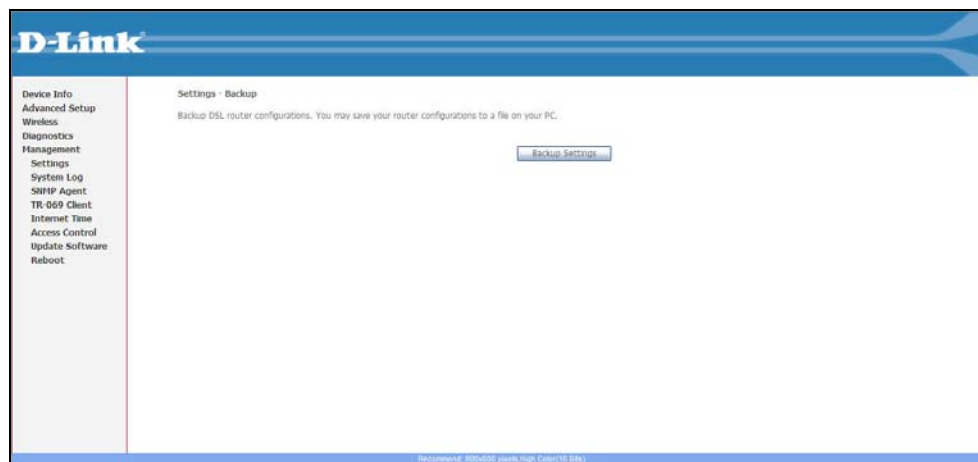
Troubleshooting:

NOTE: This test will fail if Test ADSL Synchronization also fails. Troubleshoot the Test ADSL Synchronization test first.

1. Turn off the DSL modem, wait 10 seconds and turn it back on.
2. With the modem on, press the external reset button on the DSL modem for at least six seconds and release it. This resets the DSL modem to its default settings. Wait for the DSL modem to completely restart, then close and restart your Web browser. To reconfigure the modem, type your DSL Account username and password.
3. If this is the first time you are setting up your DSL modem, you may need to reconfigure your VPI/VCI settings. Contact ISP Technical Support for assistance.

Contact ISP Technical Support if you have tried all of the above and still are experiencing a fail condition.

Management



Settings

In the settings section the user can backup and upload the router's configuration and also perform a factory reset when needed.

Backup

This page allows the user to backup the current running configuration of the router.

Click the **Backup Settings** button to save the file in a safe location.

Update Settings

This page allows the user the restore a backed up running configuration to the router.

Click the **Browse** button and locate the saved backup file. Then click the **Update Settings** button to restore the running configuration.

Restore Default Settings

The page allows the user to perform a factory reset on the router. **Important:** After clicking the **Restore Default Settings** button, the router will return to its factory default setup.

This should be the last option when troubleshooting a problem.

Settings - Backup

Backup DSL router configurations. You may save your router configurations to a file on your PC.

Backup Settings

Tools -- Update Settings

Update DSL router settings. You may update your router settings using your saved files.

Settings File Name:

Update Settings

Tools -- Restore Default Settings

Restore DSL router settings to the factory defaults.

Restore Default Settings

System Log

The System Log dialog allows you to view the System Log and configure the System Log options.

System Log

Click **View System Log** to view the System Log.
Click **Configure System Log** to configure the System Log options.

Configuration

If the log mode is enabled, the system will begin to log all the selected events.
For the Log Level, all events above or equal to the selected level will be logged.
For the Display Level, all logged events above or equal to the selected level will be displayed.
If the selected mode is **Remote** or **Both**, events will be sent to the specified IP address and UDP port of the remote syslog server. If the selected mode is **Local** or **Both**, events will be recorded in the local memory.

Select the desired values and click **Apply/Save** to configure the system log options.

System Log

Click **View System Log** to view the System Log.
Click **Refresh** to update the status.

System Log

The System Log dialog allows you to view the System Log and configure the System Log options.

Click "View System Log" to view the System Log.

Click "Configure System Log" to configure the System Log options.

System Log -- Configuration

If the log mode is enabled, the system will begin to log all the selected events. For the Log Level, all events above or equal to the selected level will be logged. For the Display Level, all logged events above or equal to the selected level will be displayed. If the selected mode is 'Remote' or 'Both,' events will be sent to the specified IP address and UDP port of the remote syslog server. If the selected mode is 'Local' or 'Both,' events will be recorded in the local memory.

Select the desired values and click 'Apply/Save' to configure the system log options.

Log: Disable Enable

Log Level:

Display Level:

Mode:

System Log

Date/Time	Facility	Severity	Message

SNMP Agent

Simple Network Management Protocol (SNMP) allows a management application to retrieve statistics and status from the SNMP agent in this device.

SNMP Configuration

Select the desired values and click **Save/Apply** to configure the SNMP options.

SNMP - Configuration

Simple Network Management Protocol (SNMP) allows a management application to retrieve statistics and status from the SNMP agent in this device.

Select the desired values and click "Apply" to configure the SNMP options.

SNMP Agent Disable Enable

Read Community:
Set Community:
System Name:
System Location:
System Contact:
Trap Manager IP:

Save/Apply

TR-069 Client

To access the **TR-069 Client** window, click the **TR-069 Client** button in the **Management** directory.

TR069 management allows the remote configuration to the Router. Click the **Enable** radio button in **Inform** and configure the TR069 management access information.

Click the **Apply** button when you are satisfied that all the settings are configured correctly.

TR-069 client - Configuration

WAN Management Protocol (TR-069) allows a Auto-Configuration Server (ACS) to perform auto-configuration, provision, collection, and diagnostics to this device.

Select the desired values and click "Apply/Save" to configure the TR-069 client options.

Inform Disable Enable

Inform Interval:

ACS URL:

ACS User Name:

ACS Password:

WAN Interface used by TR-069 client:

Display SOAP messages on serial console Disable Enable

Connection Request Authentication

Connection Request User Name:

Connection Request Password:

Connection Request URL:

Apply/Save

GetRPCMethods

Internet Time

This page allows you to the modem's time configuration.

Time Settings

On this page the user can choose to automatically settings time synchronization to a host of available time server globally. The user can also specify the time zone offset.

Click **Apply/Save** to configure the internet time options.

Time settings

This page allows you to the modem's time configuration.

Automatically synchronize with Internet time servers

First NTP time server:

Second NTP time server:

Third NTP time server:

Fourth NTP time server:

Fifth NTP time server:

Time zone offset:

Access Control

Passwords

Access to your DSL router is controlled through three user accounts: admin, support, and user.

The user name "admin" has unrestricted access to change and view configuration of your DSL Router.

The user name "support" is used to allow an ISP technician to access your DSL Router for maintenance and to run diagnostics.

The user name "user" can access the DSL Router, view configuration settings and statistics, as well as, update the router's software.

The user can use the fields to enter up to 16 characters and click **Apply/Save** to change or create passwords.

NOTE: Password cannot contain a space.

Services

This page allows to configure the Service Control. Tick the corresponding **Enable** check boxes to enable the services on LAN or WAN. Click **Apply/Save** to save the settings.

Access Control -- Passwords

Access to your DSL router is controlled through three user accounts: admin, support, and user.

The user name "admin" has unrestricted access to change and view configuration of your DSL Router.

The user name "support" is used to allow an ISP technician to access your DSL Router for maintenance and to run diagnostics.

The user name "user" can access the DSL Router, view configuration settings and statistics, as well as, update the router's software.

Use the fields below to enter up to 16 characters and click "Apply/Save" to change or create passwords. Note: Password cannot contain a space.

Username:

Old Password:

New Password:

Confirm Password:

Apply/Save

Access Control -- Services

A Service Control List ("SCL") enables or disables services from being used.

Services	LAN	WAN
FTP	<input checked="" type="checkbox"/> Enable	<input type="checkbox"/> Enable
HTTP	<input checked="" type="checkbox"/> Enable	<input type="checkbox"/> Enable
ICMP	<input checked="" type="checkbox"/> Enable	<input type="checkbox"/> Enable
SNMP	<input checked="" type="checkbox"/> Enable	<input type="checkbox"/> Enable
TELNET	<input checked="" type="checkbox"/> Enable	<input type="checkbox"/> Enable
TFTP	<input checked="" type="checkbox"/> Enable	<input type="checkbox"/> Enable

Save/Apply

IP Address

Tick the **Enable Access Control Mode** check box to allow the IP addresses listed in the table below to access the local management.

Enter the IP Address in the field and click the **Apply** button to see the IP address displays in the table below.

Tick the corresponding check box in the table and click the **Remove** button to delete the IP address.

Click the **Apply** button to take effect.

Access Control -- IP Addresses

The IP Address Access Control mode, if enabled, permits access to local management services from IP addresses contained in the Access Control List. If the Access Control mode is disabled, the system will not validate IP addresses for incoming packets. The services are the system applications listed in the Service Control List.

Enter the IP address of the management station permitted to access the local management services, and click "Apply".

Enable Access Control Mode

IP Address :

Update Software

On this page the user can update the firmware of the router by simply download the latest firmware file and uploading it through this page. It's important to keep the router up to date with the latest firmware to prevent future problems.

Obtain an updated software image file from your ISP. Enter the path to the image file location in the box below, or click the **Browse** button to locate the image file. Click the **Update Software** button once to upload the new image file.

NOTE: The update process takes about 2 minutes to complete, and your DSL Router will reboot.

Tools -- Update Software

Step 1: Obtain an updated software image file from your ISP.

Step 2: Enter the path to the image file location in the box below or click the "Browse" button to locate the image file.

Step 3: Click the "Update Software" button once to upload the new image file.

NOTE: The update process takes about 3 minutes to complete, and your DSL Router will reboot.

Software File Name:

Reboot

On this page the user can manually reboot or restart the router.

To reboot the router click the **Reboot** button.

The DSL router will take 2 minutes to complete the reboot process.

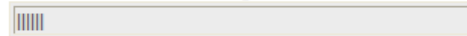
Click the button below to reboot the router.

Reboot

DSL Router Reboot

The DSL Router is rebooting.

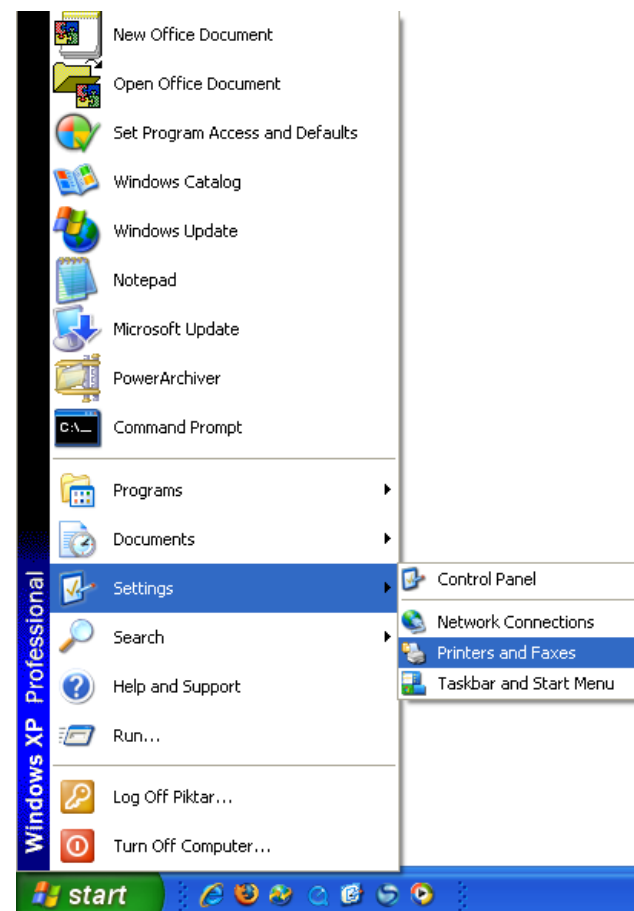
Close the DSL Router Configuration window and wait for 2 minutes before reopening your web browser.



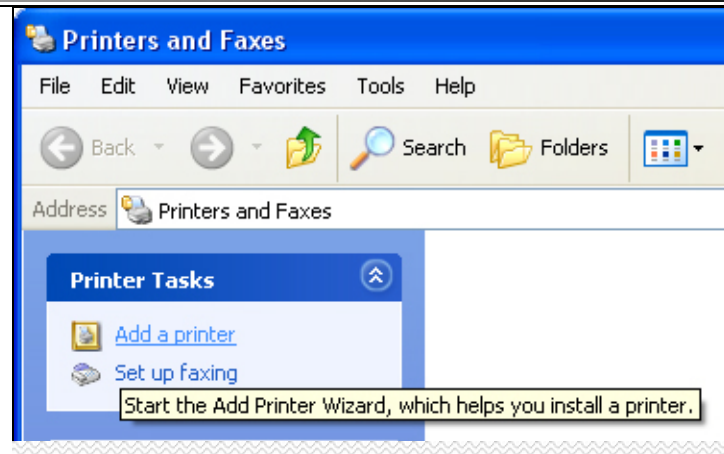
Add a Network Printer in Windows XP

Before adding a network printer to your computer, make sure the printer is properly connected with the Router.

Go to **Start -> Settings -> Printers and Faxes** to see the Printers and Faxes window.



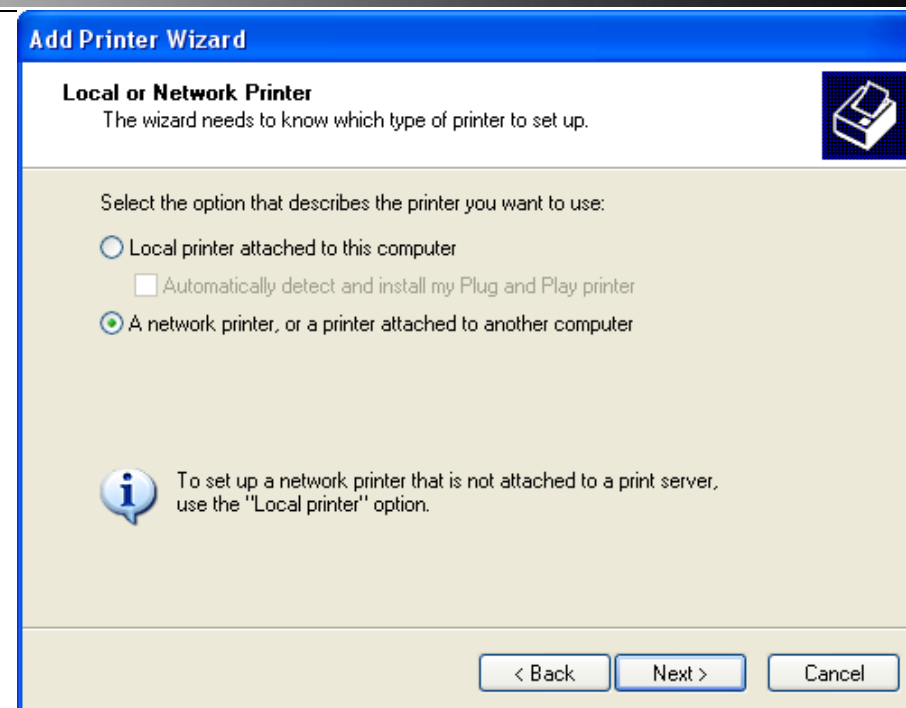
Click **Add a printer** to install a new printer.



When the Add Printer Wizard window appears, click the **Next** button to proceed.



Click the **A network printer, or a printer attached to another computer** radio button, and click the **Next** button to proceed.



Click the **Connect to a printer on the Internet or on a home or office network** radio button.

Enter "http://LAN IP Address:631/printers/Printer name" in the URL field (The example here is *http://192.168.1.1:631/printers/Printer6200*). Make sure the name of the printer in the URL field is the same as the Printer name configured in the Router's Web interface.

Click the **Next** button to continue.

Print Server settings

This page allows you to enable / disable printer support.

Enable on-board print server.

Printer name

Make and model

Add Printer Wizard

Specify a Printer

If you don't know the name or address of the printer, you can search for a printer that meets your needs.

What printer do you want to connect to?

Browse for a printer

Connect to this printer (or to browse for a printer, select this option and click Next):

Name:

Example: \\server\printer

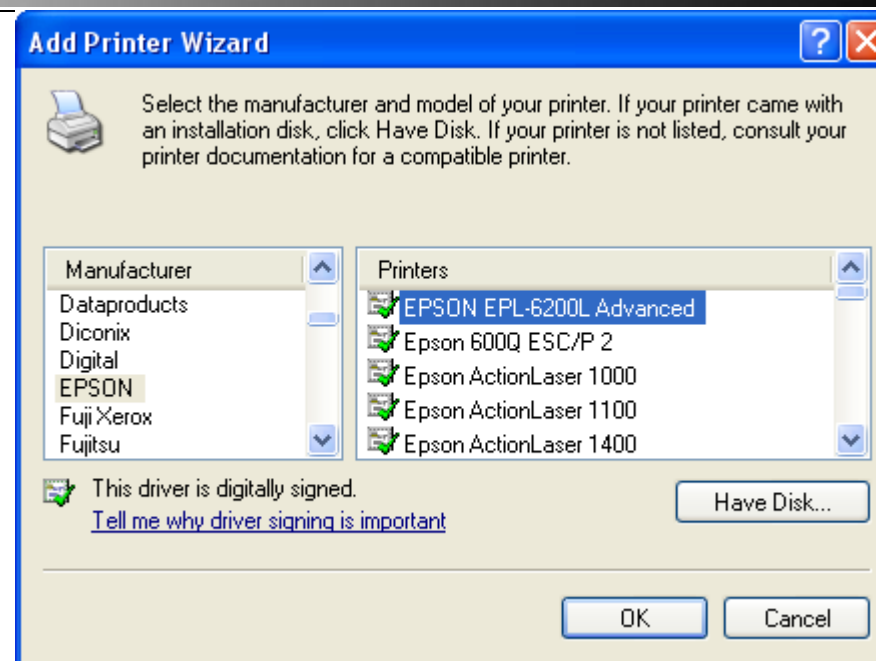
Connect to a printer on the Internet or on a home or office network:

URL:

Example: http://server/printers/myprinter/.printer

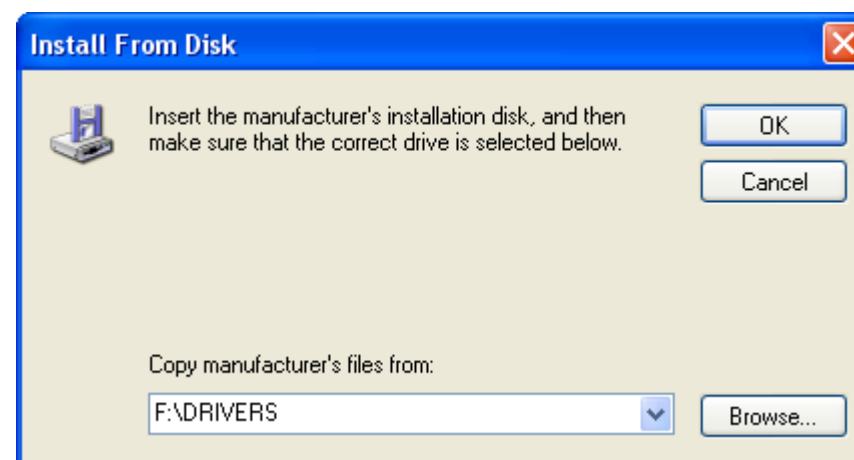
Select the printer driver from the list and click **OK** to proceed.

If the desired printer is not on the list, click **Have Disk** and insert the printer driver disk that came with your printer to install the printer drivers.

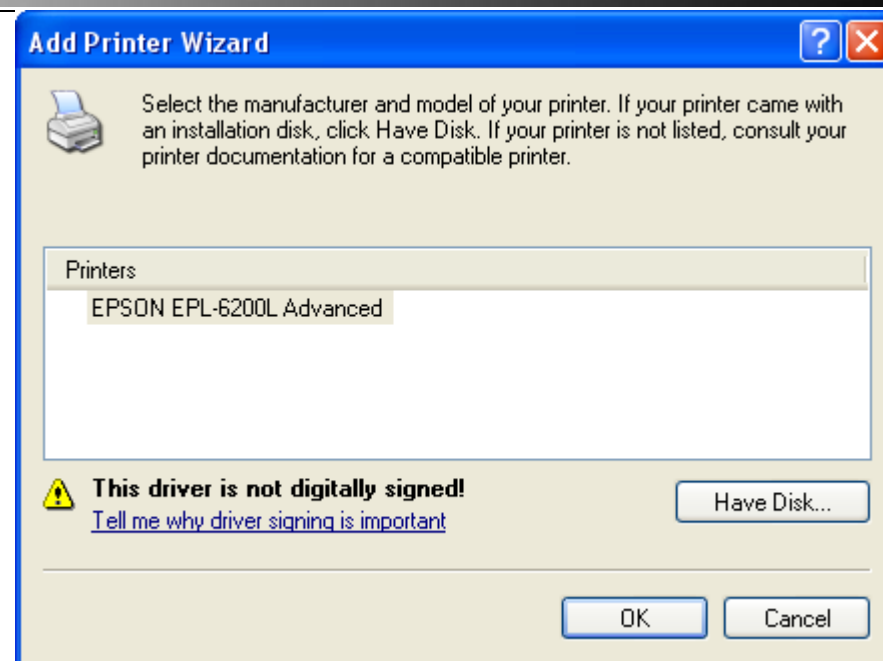


Select the directory of the printer driver from the **Copy manufacturer's files from** list. Or, click the **Browse** button to find the directory.

Click **OK** to proceed.



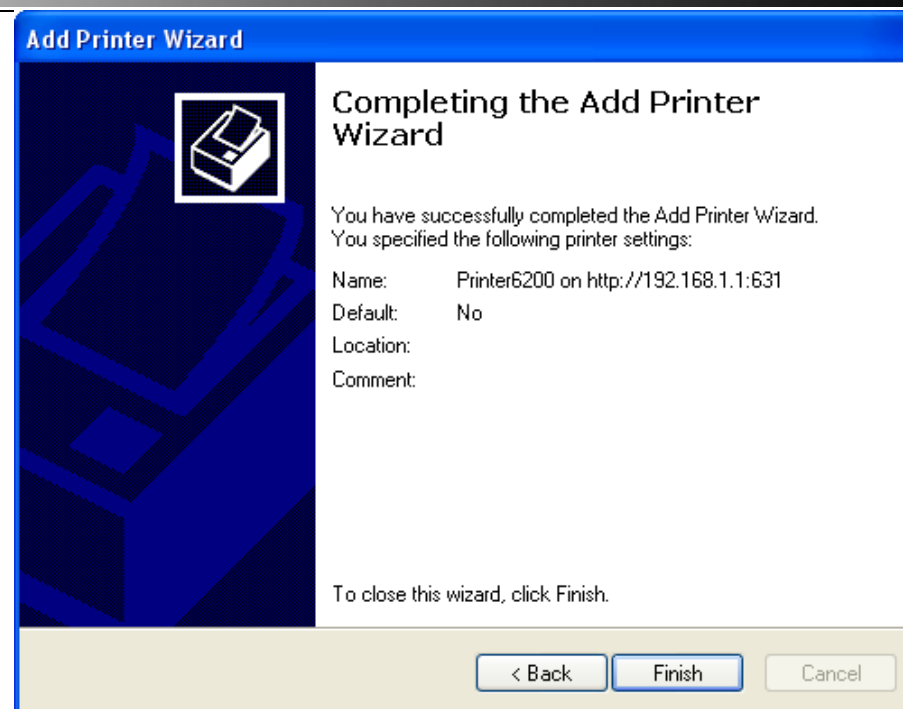
The printer driver will appear in the list. Click **OK** to proceed.



The window appears asking if you want to set the printer as the default printer. Click the **Next** button to proceed.



The window appears to show the printer information. Click the **Finish** button to complete the printer settings.



Troubleshooting

This chapter provides solutions to problems that might occur during the installation and operation of the DSL-2760U. Read the following descriptions if you are having problems. (The examples below are illustrated in Windows® XP. If you have a different operating system, the screenshots on your computer will look similar to the following examples.)

How do I configure my DSL-2760U Router without the CD-ROM?

Connect your PC to the Router using an Ethernet cable.

- Open a web browser and enter the address `http://192.168.1.1`
- The default username is 'admin' and the default password is 'admin'.
- If you have changed the password and cannot remember it, you will need to reset the Router to the factory default setting (see question 2), which will set the password back to 'admin'.

NOTE: Please refer to the next section "Networking Basics" to check your PC's IP configuration if you can't see the login windows.

How do I reset my Router to the factory default settings?

- Ensure the Router is powered on.
- Press and hold the reset button on the back of the device for approximately 6 to 10 seconds.
- This process should take around 1 to 2 minutes.

NOTE: Resetting the Router to the factory default settings will erase the current configuration settings. To reconfigure your settings, login to the Router as outlined in question 1, and then run the Quick Setup wizard.

What can I do if my Router is not working correctly?

There are a few quick steps you can take to try and resolve any issues:

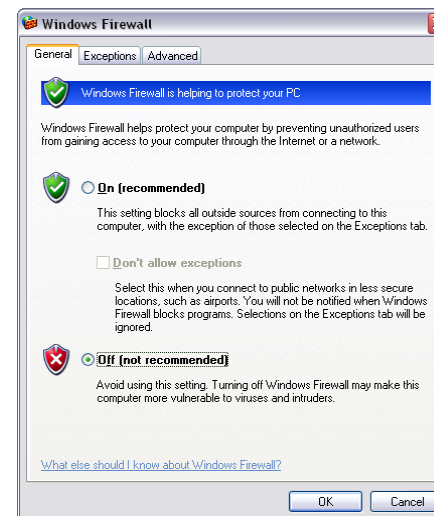
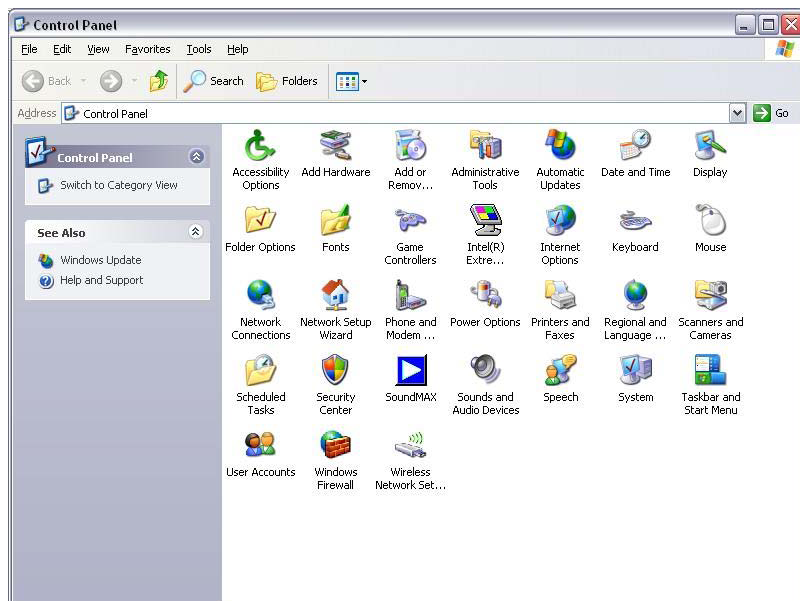
- Follow the directions in Question 2 to reset the Router.
- Check that all the cables are firmly connected at both ends.
- Check the LEDs on the front of the Router. The Power indicator should be on, the Internet indicator should flash, and the DSL and LAN indicators should be on as well.
- Please ensure that the settings in the Web-based configuration manager, e.g. ISP username and password, are the same as the settings that have been provided by your ISP.

Why can't I get an Internet connection?

For ADSL ISP users, please contact your ISP to make sure the service has been enabled/connected by your ISP and that your ISP username and password are correct.

What can I do if my Router can't be detected by running the installation CD?

- Ensure the Router is powered on.
- Check that all the cables are firmly connected at both ends and all LEDs work correctly.
- Ensure only one network interface card on your PC is activated.
- Click **Start > Control Panel > Security Center** to disable the firewall.



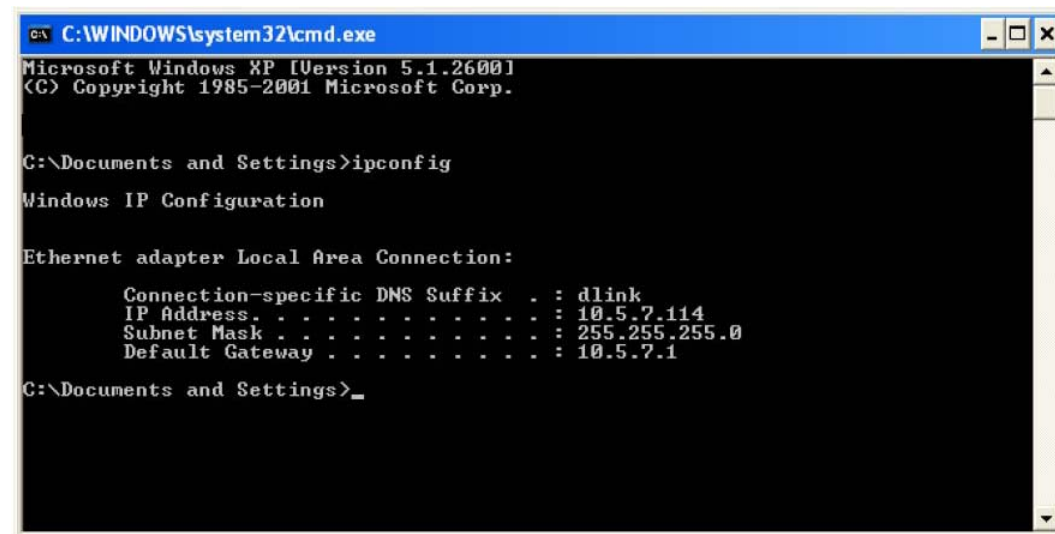
NOTE: There is a potential security issue if the firewall is disabled on your PC. Please remember to turn it back on once you have finished the whole installation procedure. This will enable you to be able to surf the Internet without any problem.

Knowledge Base

Check Your IP Address

After you install your new D-Link adapter, by default, the TCP/IP settings should be set to obtain an IP address from a DHCP server (i.e. wireless router) automatically. To verify your IP address, please follow the steps below.

- Click **Start > Run**. In the run box type *cmd* and click **OK**.
- At the prompt, type *ipconfig* and press the **Enter** key.
- This will display the IP address, subnet mask, and the default gateway of your adapter.
- If the address is 0.0.0.0, check your adapter installation, security settings, and the settings on your router. Some firewall software programs may block a DHCP request on newly installed adapters.
- If you are connecting to a wireless network at a hotspot (e.g. hotel, coffee shop, airport), please contact an employee or administrator to verify their wireless network settings.



```
C:\WINDOWS\system32\cmd.exe
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings>ipconfig

Windows IP Configuration

Ethernet adapter Local Area Connection:

    Connection-specific DNS Suffix  . : dlink
    IP Address. . . . .                : 10.5.7.114
    Subnet Mask . . . . .              : 255.255.255.0
    Default Gateway . . . . .          : 10.5.7.1

C:\Documents and Settings>
```

Statically assign an IP Address

If you are not using a DHCP capable gateway/router, or you need to assign a static IP address, please follow the steps below:

Step 1

Windows® XP - Click **Start > Control Panel > Network Connections**.

Windows® 2000 - From the desktop, right-click **My Network Places > Properties**.

Step 2

Right-click **Local Area Connection** which represents your D-Link network adapter and select Properties.

Step 3

Select **Internet Protocol (TCP/IP)** in the list and click the **Properties** button.

Step 4

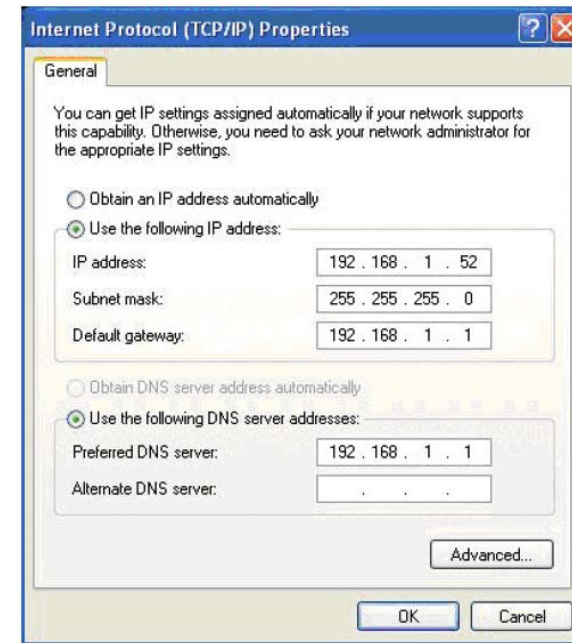
Click the **Use the following IP address** and enter an IP address that is on the same subnet as your network or the LAN IP address on your router.

Example: If the router's LAN IP address is 192.168.1.1, make your IP address 192.168.1.X where X is a number between 2 and 99. Make sure that the number you choose is not in use on the network. Set Default Gateway the same as the LAN IP address of your router (192.168.1.1).

Set Primary DNS the same as the LAN IP address of your router (192.168.1.1). The Secondary DNS is not needed or you may enter a DNS server from your ISP.

Step 5

Click **OK** twice to save your settings.



Technical Specifications

DEVICE INTERFACES

- RJ-11 ADSL port
- 4 x RJ-45 10/100BASE-TX Ethernet ports with auto MDI/MDIX
- 2 x USB (Type A connector) ports
- Built-in draft 802.11n wireless LAN
- Factory reset button

WIRELESS LAN

- 802.11b/g standards, 802.11n draft 2.0
- Wireless speed: up to 54Mbps (802.11g), 130Mbps (802.11n)
- Frequency range: 2.4 GHz to 2.484G Hz
- WEP 64/128 bits data encryption
- WPA/WPA2 (Wi-Fi Protected Access) security
- Multiple SSID
- 802.11e Wireless QoS (WMM/WME)
- MAC address-based access control

ADSL STANDARDS

- ADSL standards: Multi-mode, ANSI T1.413 Issue 2, ITU G.992.1 (G.dmt) Annex A, ITU G.992.2 (G.lite) Annex A, ITU G.994.1 (G.hs)
- ADSL2 standards: ITU G.992.3 (G.dmt.bis) Annex A/L/M, ITU G.992.4 (G.lite.bis) Annex A
- ADSL2+ standards: ITU G.992.5 Annex A/M

ADSL DATA RATES

- G.dmt: 8Mbps downstream, 832Kbps upstream
- G.lite: 1.5Mbps downstream, 512Kbps upstream
- ADSL2: 12Mbps downstream, 1Mbps upstream
- ADSL2+: 24Mbps downstream, 1Mbps upstream

ATM & PPP PROTOCOLS

- ATM Forum UNI3.1/4.0 PVC (up to 16PVCs)
- ATM Adaptation Layer Type 5 (AAL5)
- ATM QoS (Traffic Shaping)
- Bridged or routed Ethernet encapsulation
- VC and LLC based multiplexing
- PPP over Ethernet (PPPoE)
- PPP over ATM (RFC 2364)
- ITU-T I.610 OAM F4/F5

ROUTER FEATURES

- NAT (maximum 1024 NAT sessions)
- DHCP server/client/relay
- Static Routing, RIP v.1, v.2
- Universal Plug and Play (UPnP) Compliant
- Dynamic Domain Name System (DDNS)
- Virtual Server
- SNTP, DNS proxy and IGMP proxy

FIREWALL

- Built-in NAT firewall
- Stateful Packet Inspection (SPI)
- DoS attacks prevention
- Packet filtering (IP/ICMP/TCP/UDP)
- Intrusion Detection System (IDS)
- DMZ

VIRTUAL PRIVATE NETWORK (VPN)

Multiple PPTP/IPSec/L2TP pass-throughs

DEVICE CONFIGURATION/MANAGEMENT

- Installation Wizard
- Web-based GUI for configuration, firmware upgrade
- Code lock to prevent improper firmware upgrade
- Telnet with SSH support
- Syslog monitoring
- SNMP v1, v2c support with built-in MIB-II (RFC 1213)

QUALITY OF SERVICE

- LAN to WAN traffic prioritization/Classification
- 802.1p (0 to 7) traffic prioritization
- Traffic Shaping

SECURITY

- IGMP Snooping with 32 Multicast groups
- PVC/VLAN port mapping (bridge mode)
- Parental Control (URL blocking, scheduling)

POWER INPUT

- Through 12VAC 1.5A external power adapter

DIAGNOSTIC LEDS

- Power
- LAN (1 to 4)
- WLAN
- DSL
- USB (1 to 2)
- Internet

DIMENSIONS

- 220 x 150 x 32 mm (8.66 x 5.90 x 1.26 inches)

WEIGHT

- 474 grams (1.05 lb)

OPERATING TEMPERATURE

- 0° to 40° C (32° to 104° F)

STORAGE TEMPERATURE

- -20° to 70° C (-4° to 158° F)

OPERATING HUMIDITY

- 10% to 95% non-condensing

CERTIFICATIONS

- CE (EN55022/EN55024/EN300 328/ EN301 489)
- Wi-Fi Certified
- K.21 Certified

D-Link Worldwide Offices

Headquarters	TEL: 886-2-6600-0123	FAX: 886-2-6600-9898	Italy	TEL: 39-02-2900-0676	FAX: 39-02-2900-1723
U.S.A.	TEL: 1-800-326-1688	FAX: 1-866-743-4905	Japan	TEL: 81-3-5781-0963	FAX: 81-3-5781-0965
Australia	TEL: 61-2-8899-1800	FAX: 61-2-8899-1868	Latin America	TEL: 56-2-232-3185	FAX: 56-2-232-0923
Belgium	TEL: 32(0)2-517-7111	FAX: 32(0)2-517-6500	Luxemburg	TEL: 32-(0)2-517-7111	FAX: 32-(0)2-517-6500
Brazil	TEL: 55-11-218-59300	FAX: 55-11-218-59322	Middle East (Dubai)	TEL: 971-4-3916480	FAX: 971-4-3908881
Canada	TEL: 1-905-8295033	FAX: 1-905-8295223	Netherlands	TEL: 31-10-282-1445	FAX: 31-10-282-1331
China	TEL: 86-10-58635800	FAX: 86-10-58635799	Norway	TEL: 47-99-300-100	FAX: 47-22-309580
Czech Republic	TEL: 420-(603)-276-589		Poland	TEL: 48-(0)-22-583-92-75	FAX: 48-(0)-22-583-92-76
Denmark	TEL: 45-43-969040	FAX: 45-43-424347	Portugal	TEL: 351-21-8688493	
Egypt	TEL: 202-291-9035	FAX: 202-291-9051	Russia	TEL: 7-495-744-0099	FAX: 7-495-744-0099 #350
Europe (U. K.)	TEL: 44-20-8955-9000	FAX: 44-20-8955-9001	Singapore	TEL: 65-6774-6233	FAX: 65-6774-6322
Finland	TEL: 358-9-2707 5080	FAX: 358-9-2707-5081	South Africa	TEL: 27-12-665-2165	FAX: 27-12-665-2186
France	TEL: 33-1-30238688	FAX: 33-1-30238689	Spain	TEL: 34-93-4090770	FAX: 34-93-4910795
Germany	TEL: 49-6196-77990	FAX: 49-6196-7799300	Sweden	TEL: 46-(0)8564-61900	FAX: 46-(0)8564-61901
Greece	TEL: 30-210-9914 512	FAX: 30-210-9916902	Switzerland	TEL: 41-(0)-1-832-11-00	FAX: 41(0)-1-832-11-01
Hungary	TEL: 36-(0)-1-461-30-00	FAX: 36-(0)-1-461-30-09	Taiwan	TEL: 886-2-6600-0123	FAX: 886-2-6600-8168
India	TEL: 91-022-26526696	FAX: 91-022-26528914	Turkey	TEL: 90-312-473-40-55	FAX: 90-312-473-40-58
Israel	TEL: 972-9-9715700	FAX: 972-9-9715601			

D-Link customers can contact D-Link technical support through our web site or by phone.

Before you contact technical support, please have the following ready:

- Model number of the product (e.g. DSL-2760U)
- Hardware Revision (located on the label on the bottom of the access point (e.g. rev A1))
- Serial Number (s/n number located on the label on the bottom of the access point).

You can find software updates and user documentation on the D-Link website as well as frequently asked questions and answers to technical issues.

Warranty

Subject to the terms and conditions set forth herein, D-Link Systems, Inc. ("D-Link") provides this Limited Warranty:

- Only to the person or entity that originally purchased the product from D-Link or its authorized reseller or distributor, and
- Only for products purchased and delivered within the fifty states of the United States, the District of Columbia, U.S. Possessions or Protectorates, U.S. Military Installations, or addresses with an APO or FPO.

Limited Warranty:

D-Link warrants that the hardware portion of the D-Link product described below ("Hardware") will be free from material defects in workmanship and materials under normal use from the date of original retail purchase of the product, for the period set forth below ("Warranty Period"), except as otherwise stated herein.

- Hardware (excluding power supplies and fans): One (1) year
- Power supplies and fans: One (1) year
- Spare parts and spare kits: Ninety (90) days

The customer's sole and exclusive remedy and the entire liability of D-Link and its suppliers under this Limited Warranty will be, at D-Link's option, to repair or replace the defective Hardware during the Warranty Period at no charge to the original owner or to refund the actual purchase price paid. Any repair or replacement will be rendered by D-Link at an Authorized D-Link Service Office. The replacement hardware need not be new or have an identical make, model or part. D-Link may, at its option, replace the defective Hardware or any part thereof with any reconditioned product that D-Link reasonably determines is substantially equivalent (or superior) in all material respects to the defective Hardware. Repaired or replacement hardware will be warranted for the remainder of the original Warranty Period or ninety (90) days, whichever is longer, and is subject to the same limitations and exclusions. If a material defect is incapable of correction, or if D-Link determines that it is not practical to repair or replace the defective Hardware, the actual price paid by the original purchaser for the defective Hardware will be refunded by D-Link upon return to D-Link of the defective Hardware. All Hardware or part thereof that is replaced by D-Link, or for which the purchase price is refunded, shall become the property of D-Link upon replacement or refund.

Limited Software Warranty:

D-Link warrants that the software portion of the product ("Software") will substantially conform to D-Link's then current functional specifications for the Software, as set forth in the applicable documentation, from the date of original retail purchase of the Software for a period of ninety (90) days ("Software Warranty Period"), provided that the Software is properly installed on approved hardware and operated as contemplated in its documentation. D-Link further warrants that, during the Software Warranty Period, the magnetic media on which D-Link delivers the Software will be free of physical defects. The customer's sole and exclusive remedy and the entire liability of D-Link and its suppliers under this Limited Warranty will be, at D-Link's option, to replace the non-conforming Software (or defective media) with software that substantially conforms to D-Link's functional specifications for the Software or to refund the portion of the actual purchase price paid that is attributable to the Software. Except as otherwise agreed by D-Link in writing, the replacement Software is provided only to the original licensee, and is subject to

the terms and conditions of the license granted by D-Link for the Software. Replacement Software will be warranted for the remainder of the original Warranty Period and is subject to the same limitations and exclusions. If a material non-conformance is incapable of correction, or if D-Link determines in its sole discretion that it is not practical to replace the non-conforming Software, the price paid by the original licensee for the non-conforming Software will be refunded by D-Link; provided that the non-conforming Software (and all copies thereof) is first returned to D-Link. The license granted respecting any Software for which a refund is given automatically terminates.

Non-Applicability of Warranty:

The Limited Warranty provided hereunder for Hardware and Software portions of D-Link's products will not be applied to and does not cover any refurbished product and any product purchased through the inventory clearance or liquidation sale or other sales in which D-Link, the sellers, or the liquidators expressly disclaim their warranty obligation pertaining to the product and in that case, the product is being sold "As-Is" without any warranty whatsoever including, without limitation, the Limited Warranty as described herein, notwithstanding anything stated herein to the contrary.

Submitting a Claim:

The customer shall return the product to the original purchase point based on its return policy. In case the return policy period has expired and the product is within warranty, the customer shall submit a claim to D-Link as outlined below:

- The customer must submit with the product as part of the claim a written description of the Hardware defect or Software nonconformance in sufficient detail to allow D-Link to confirm the same, along with proof of purchase of the product (such as a copy of the dated purchase invoice for the product) if the product is not registered.
- The customer must obtain a Case ID Number from D-Link Technical Support at 1-877-453-5465, who will attempt to assist the customer in resolving any suspected defects with the product. If the product is considered defective, the customer must obtain a Return Material Authorization ("RMA") number by completing the RMA form and entering the assigned Case ID Number at <https://rma.dlink.com/>.
- 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. Do not include any manuals or accessories in the shipping package. D-Link will only replace the defective portion of the product and will not ship back any accessories.
- The customer is responsible for all in-bound shipping charges to D-Link. No Cash on Delivery ("COD") is allowed. Products sent COD will either be rejected by D-Link or become the property of D-Link. Products shall be fully insured by the customer and shipped to D-Link Systems, Inc., 17595 Mt. Herrmann, Fountain Valley, CA 92708. D-Link will not be held responsible for any packages that are lost in transit to D-Link. The repaired or replaced packages will be shipped to the customer via UPS Ground or any common carrier selected by D-Link. Return shipping charges shall be prepaid by D-Link if you use an address in the United States, otherwise we will ship the product to you freight collect. Expedited shipping is available upon request and provided shipping charges are prepaid by the customer. D-Link may reject or return any product that is not packaged and shipped in strict compliance with the foregoing requirements, or for which an RMA number is not visible from the outside of the package. The product owner agrees to pay D-Link's reasonable handling and return shipping charges for any product that is not packaged and shipped in accordance with the foregoing requirements, or that is determined by

D-Link not to be defective or non-conforming.

What Is Not Covered?

The Limited Warranty provided herein by D-Link does not cover:

Products that, in D-Link's judgment, have been subjected to abuse, accident, alteration, modification, tampering, negligence, misuse, faulty installation, lack of reasonable care, repair or service in any way that is not contemplated in the documentation for the product, or if the model or serial number has been altered, tampered with, defaced or removed; Initial installation, installation and removal of the product for repair, and shipping costs; Operational adjustments covered in the operating manual for the product, and normal maintenance; Damage that occurs in shipment, due to act of God, failures due to power surge, and cosmetic damage; Any hardware, software, firmware or other products or services provided by anyone other than D-Link; and Products that have been purchased from inventory clearance or liquidation sales or other sales in which D-Link, the sellers, or the liquidators expressly disclaim their warranty obligation pertaining to the product.

While necessary maintenance or repairs on your Product can be performed by any company, we recommend that you use only an Authorized D-Link Service Office. Improper or incorrectly performed maintenance or repair voids this Limited Warranty.

Disclaimer of Other Warranties:

EXCEPT FOR THE LIMITED WARRANTY SPECIFIED HEREIN, THE PRODUCT IS PROVIDED "AS-IS" WITHOUT ANY WARRANTY OF ANY KIND WHATSOEVER INCLUDING, WITHOUT LIMITATION, ANY WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT.

IF ANY IMPLIED WARRANTY CANNOT BE DISCLAIMED IN ANY TERRITORY WHERE A PRODUCT IS SOLD, THE DURATION OF SUCH IMPLIED WARRANTY SHALL BE LIMITED TO THE DURATION OF THE APPLICABLE WARRANTY PERIOD SET FORTH ABOVE. EXCEPT AS EXPRESSLY COVERED UNDER THE LIMITED WARRANTY PROVIDED HEREIN, THE ENTIRE RISK AS TO THE QUALITY, SELECTION AND PERFORMANCE OF THE PRODUCT IS WITH THE PURCHASER OF THE PRODUCT.

Limitation of Liability:

TO THE MAXIMUM EXTENT PERMITTED BY LAW, D-LINK IS NOT LIABLE UNDER ANY CONTRACT, NEGLIGENCE, STRICT LIABILITY OR OTHER LEGAL OR EQUITABLE THEORY FOR ANY LOSS OF USE OF THE PRODUCT, INCONVENIENCE OR DAMAGES OF ANY CHARACTER, WHETHER DIRECT, SPECIAL, INCIDENTAL OR CONSEQUENTIAL (INCLUDING, BUT NOT LIMITED TO, DAMAGES FOR LOSS OF GOODWILL, LOSS OF REVENUE OR PROFIT, WORK STOPPAGE, COMPUTER FAILURE OR MALFUNCTION, FAILURE OF OTHER EQUIPMENT OR COMPUTER PROGRAMS TO WHICH D-LINK'S PRODUCT IS CONNECTED WITH, LOSS OF INFORMATION OR DATA CONTAINED IN, STORED ON, OR INTEGRATED WITH ANY PRODUCT RETURNED TO D-LINK FOR WARRANTY SERVICE) RESULTING FROM THE USE OF THE PRODUCT, RELATING TO WARRANTY SERVICE, OR ARISING OUT OF ANY BREACH OF THIS LIMITED WARRANTY, EVEN IF D-LINK HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. THE SOLE REMEDY FOR A BREACH OF THE FOREGOING LIMITED WARRANTY IS REPAIR, REPLACEMENT OR REFUND OF THE DEFECTIVE OR NONCONFORMING PRODUCT. THE MAXIMUM LIABILITY OF D-LINK UNDER THIS WARRANTY IS LIMITED TO

THE PURCHASE PRICE OF THE PRODUCT COVERED BY THE WARRANTY. THE FOREGOING EXPRESS WRITTEN WARRANTIES AND REMEDIES ARE EXCLUSIVE AND ARE IN LIEU OF ANY OTHER WARRANTIES OR REMEDIES, EXPRESS, IMPLIED OR STATUTORY.

Governing Law:

This Limited Warranty shall be governed by the laws of the State of California. Some states do not allow exclusion or limitation of incidental or consequential damages, or limitations on how long an implied warranty lasts, so the foregoing limitations and exclusions may not apply. This Limited Warranty provides specific legal rights and you may also have other rights which vary from state to state.

Trademarks:

D-Link is a registered trademark of D-Link Corporation/D-Link Systems, Inc. Other trademarks or registered trademarks are the property of their respective owners.

Copyright Statement:

No part of this publication or documentation accompanying this product may be reproduced in any form or by any means or used to make any derivative such as translation, transformation, or adaptation without permission from D-Link Corporation/D-Link Systems, Inc., as stipulated by the United States Copyright Act of 1976 and any amendments thereto. Contents are subject to change without prior notice.

Copyright ©2007 by D-Link Corporation/D-Link Systems, Inc. All rights reserved.

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.

FCC Statement:

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 equipment 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 communication. 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 the 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.

FCC Caution:

Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate this equipment.

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.

If this device is going to be operated in 5.15 ~ 5.25GHz frequency range, then it is restricted in indoor environment only.

IMPORTANT NOTICE:

FCC Radiation Exposure Statement:

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 20cm between the radiator & your body. This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

The availability of some specific channels and/or operational frequency bands are country dependent and are firmware programmed at the factory to match the intended destination. The firmware setting is not accessible by the end user.

For detailed warranty information applicable to products purchased outside the United States, please contact the corresponding local D-Link office.

Industry Canada Notice:

This device complies with RSS-210 of the Industry Canada 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.

IMPORTANT NOTE:

FCC Radiation Exposure Statement:

This equipment complies with IC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 20cm between the radiator & your body.

This device has been designed to operate with an antenna having a maximum gain of 2 dB. Antenna having a higher gain is strictly prohibited per regulations of Industry Canada. The required antenna impedance is 50 ohms.

Registration



Product registration is entirely voluntary and failure to complete or return this form will not diminish your warranty rights.

Version 1.0
July 2, 2009