

User Manual

Dual Band Wireless AC1200 Gigabit ADSL2+ Router

DSL-2880AL

Table of Contents

PACKAGE CONTENTS.....	3	ADVANCED LAN	71
SYSTEM REQUIREMENTS	4	PORT MAPPING	72
INTRODUCTION	5	SNMP SETUP	74
FEATURES.....	6	PARENTAL CONTROL.....	75
HARDWARE OVERVIEW.....	8	ROUTING SETUP	76
CONNECTIONS	8	WI-FI PROTECTED SETUP.....	78
LEDS	ERROR! BOOKMARK NOT DEFINED.	IPV6 FIREWALL	79
INSTALLATION	10	IPV6 ROUTING	81
BEFORE YOU BEGIN	10	BUDGET QUOTA	82
Installation Notes.....	11	LOGOUT.....	83
Information you will need from your ADSL service provider	13	MAINTENANCE	84
Information you will need about DSL-2880AL.....	15	PASSWORD.....	84
Information you will need about your LAN or computer:.....	16	SAVE/RESTORE SETTINGS.....	85
Wireless Installation Considerations	17	FIRMWARE UPDATE	86
DEVICE INSTALLATION.....	18	REMOTE MANAGEMENT	87
Power on Router	18	DIAGNOSTICS.....	88
Factory Reset Button.....	19	PING TEST.....	89
Network Connections	19	SYSTEM LOG	90
CONFIGURATION.....	21	SCHEDULE	92
WEB-BASED CONFIGURATION UTILITY	21	STATUS.....	93
SETUP	22	DEVICE INFO.....	93
INTERNET SETUP	22	CONNECTED CLIENTS.....	96
WIRELESS SETUP.....	30	STATISTICS	97
LAN SETUP	39	ROUTING INFO.....	99
TIME AND DATE	41	IPV6 STATUS.....	100
IPv6	44	IPV6 ROUTING INFO	101
USB SETUP	50	TROUBLESHOOTING	102
ADVANCED.....	54	APPENDIX	104
PORT FORWARDING.....	55	WIRELESS BASICS	104
APPLICATION RULES CONFIGURATION.....	56	NETWORKING BASICS.....	107
QOS SETUP	57	CHECK YOUR IP ADDRESS	107
OUTBOUND FILTER.....	59	STATICALLY ASSIGN AN IP ADDRESS.....	108
INBOUND FILTER.....	60	FCC CAUTION	109
WIRELESS FILTER.....	62	IC CAUTION	110
DNS SETUP	63	CONTACTING TECHNICAL SUPPORT	111
FIREWALL & DMZ	65	D-LINK LINK'N PRINT™	112
ADVANCED INTERNET.....	67	TECHNICAL SPECIFICATIONS	112
ADVANCED WIRELESS.....	69		

Package Contents

- DSL-2880AL Dual Band Wireless AC1200 Gigabit ADSL2+ Router
- 4 Internal Antennae
- Power Adapter
- CD-ROM with Installation Wizard, User Manual, and Special Offers
- One twisted-pair telephone cable used for ADSL connection
- One straight-through 8P8C RJ-45 Ethernet cable
- One Quick Installation Guide

Note: Using a power supply with a different voltage rating than the one included within the package will cause damage and void the warranty for this product.



System Requirements

1. ADSL Internet service

Computer with:

- 200MHz Processor
- 64MB Memory
- CD-ROM Drive
- Ethernet Adapter with TCP/IP Protocol Installed
- Windows 8/7/vista/XP/2000z
- MAC OS
- Internet Explorer v6 or later, FireFox v1.5

2. DCC (D-Link Click's Connect) Utility

Computer with:

- MS Windows - Win7/Vista/XP/2000



Introduction

HIGH-SPEED WAN (ADSL2/2+ or Gigabit Ethernet WAN) INTERNET CONNECTION

Latest ADSL2/2+ standards provide Internet transmission of up to 24Mbps downstream, 2.7Mbps upstream. Gigabit Ethernet WAN offers you plenty of bandwidth once you decide to employ Ethernet WAN to connect front end bridge modem.

HIGH-PERFORMANCE WIRELESS

Embedded 802.11ac* technology for high-speed wireless connection, complete compatibility with 802.11a/b/g/n wireless devices

TOTAL SECURITY

Firewall protection from Internet attacks, user access control, WPA/WPA2 wireless security.

ULTIMATE INTERNET CONNECTION

The DSL-2880AL ADSL2+ router is a versatile, high-performance remote router for home and the small office. With integrated ADSL2/2+ supporting up to 24Mbps download and 2.7Mbps upload speed, Gigabit Ethernet WAN Port, firewall protection, Quality of Service (QoS), 802.11ac wireless LAN and 4 Gigabit Ethernet LAN 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 MAXIMUM SECURITY

This router provides maximize wireless performance by connecting this router to computer interfaces and stay connected from virtually anywhere at home and in the office. The router can be used with 802.11a/b/g/n/ac 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.

*Maximum wireless signal rate derived from IEEE standard 802.11ac specifications. Actual data throughput will vary. Network conditions and environmental factors, including volume of network traffic, building materials and construction, and network overhead, lower actual data throughput rate. Environmental factors will adversely affect wireless signal range.

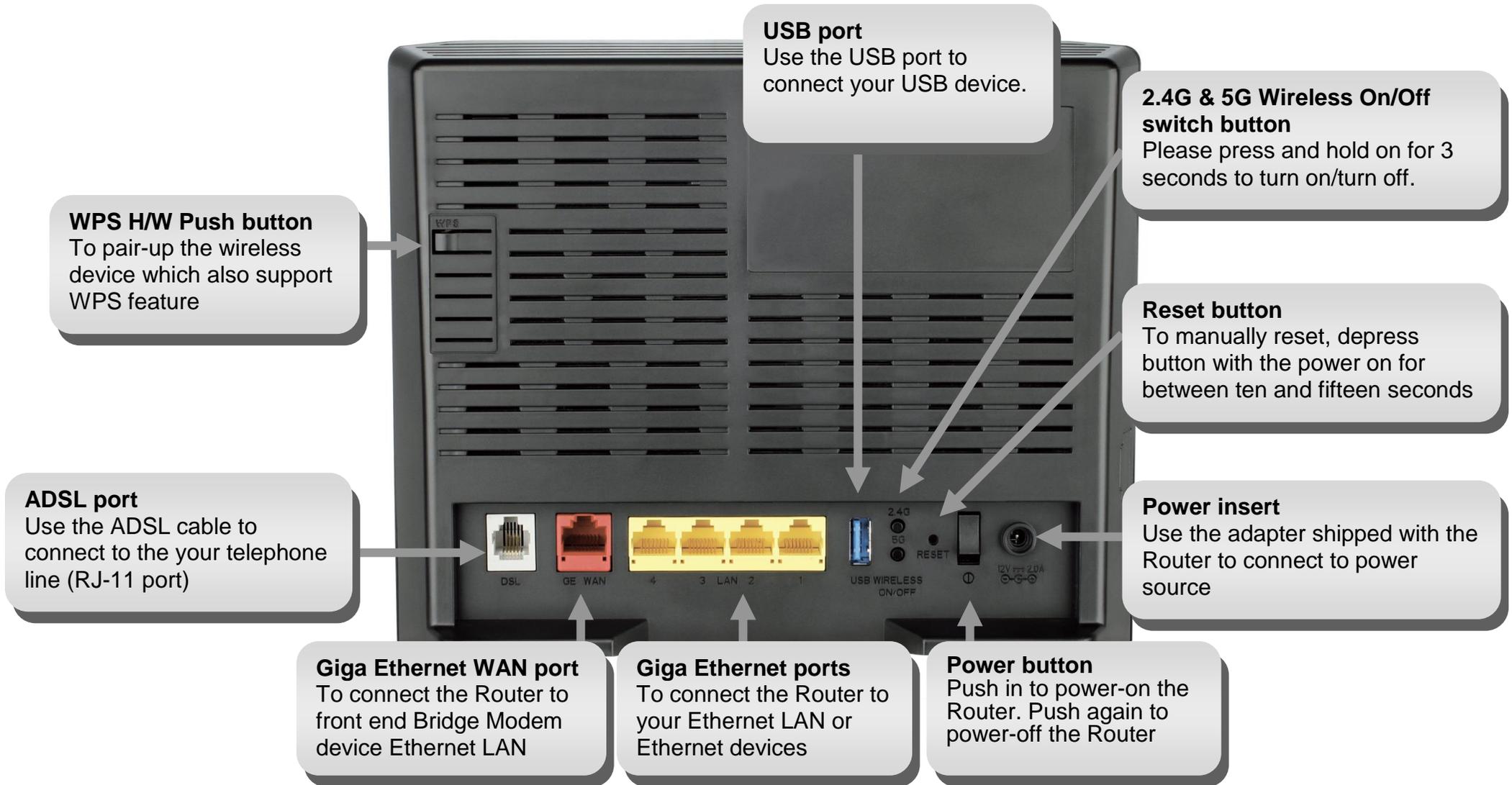
Features

- **Faster Wireless Networking** - The DSL-2880AL router provides up to 866Mbps* wireless connection with other 802.11ac wireless clients. This capability allows users to participate in real-time activities online, such as video streaming, online gaming, and real-time audio.
- **Compatible with 802.11a, 802.11b, 802.11g, 802.11n and 802.11ac* Devices** - The DSL-2880AL series router is still fully compatible with the IEEE 802.11a, b, g, n and ac standards. Thus it can connect with existing 802.11a, b, g, n and ac* PCI, USB and Card-bus adapters.
- **DHCP Support** - Dynamic Host Configuration Protocol automatically and dynamically assigns all LAN IP settings to each host on your network. This eliminates the need to reconfigure every host whenever changes in network topology occur.
- **Network Address Translation (NAT)** - For small office environments, the DSL-2880AL 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.
- **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 WAN** - Very high rates of data transfer are possible with the Router. Up to 24Mbps downstream bit rate over DSL interface by using the G.dmt standard (ADSL2+). Gigabit Ethernet WAN offers you plenty of bandwidth once you decide to employ Ethernet WAN to connect front end bridge modem with Ethernet LAN port.
- **Full Network Management** - The DSL-2880AL incorporates SNMP (Simple Network Management Protocol) support for web-based management and text-based network management via Telnet connection.
- **Easy Installation** - The DSL-2880AL 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.
- **USB Support**- The DSL-2880AL provides USB port for easy sharing files and printers. The DSL-2880AL supports USB storage device sharing files through SAMBA file server, FTP server, Web file server and in addition also supports sharing USB printer server to network members (Remark: The client computers are required to install additional software utility named D-Link Link'n Print.). Besides sharing function, the DSL-2880AL also supports connect to internet by USB 3G modem.
- **IPv6 Connection Support** – For IPv6 connection, the DSL-2880AL provides several connection types: Link-local, Static IPv6, DHCPv6, Stateless Auto-configuration, PPPoE, IPv6 in IPv4 Tunnel and 6to4.

Section 1 - Product Overview

*Maximum wireless signal rate derived from IEEE standard 802.11ac specifications. Actual data throughput will vary. Network conditions and environmental factors, including volume of network traffic, building materials and construction, and network overhead, lower actual data throughput rate. Environmental factors will adversely affect wireless signal range.

Hardware Overview – Connections



Hardware Overview – LED Indication

Ethernet LAN

A solid **Green** light indicates a valid link on startup at 1000Mbps. A solid **Amber** light indicates a valid link on startup at 100Mbps. These lights blink when there is activity currently passing through the Ethernet port.

WLAN

Steady **Green** light indicates 2.4G wireless connection. Steady **Amber** indicates 5G wireless connection. Blinking light indicates WLAN activity.

Internet

Steady **Green** light indicates a successful Internet connection. Steady **Red** light indicates failed Internet connection. Dark if no WAN protocol is configured.

Power

Steady **Green** light indicates the unit is powered on. When the device is powered off, this remains dark.

DSL

Steady **Green** light indicates a valid ADSL connection. This will light after the ADSL negotiation process has been settled. A blinking **Green** light indicates activity on the WAN (ADSL) interface.

WPS

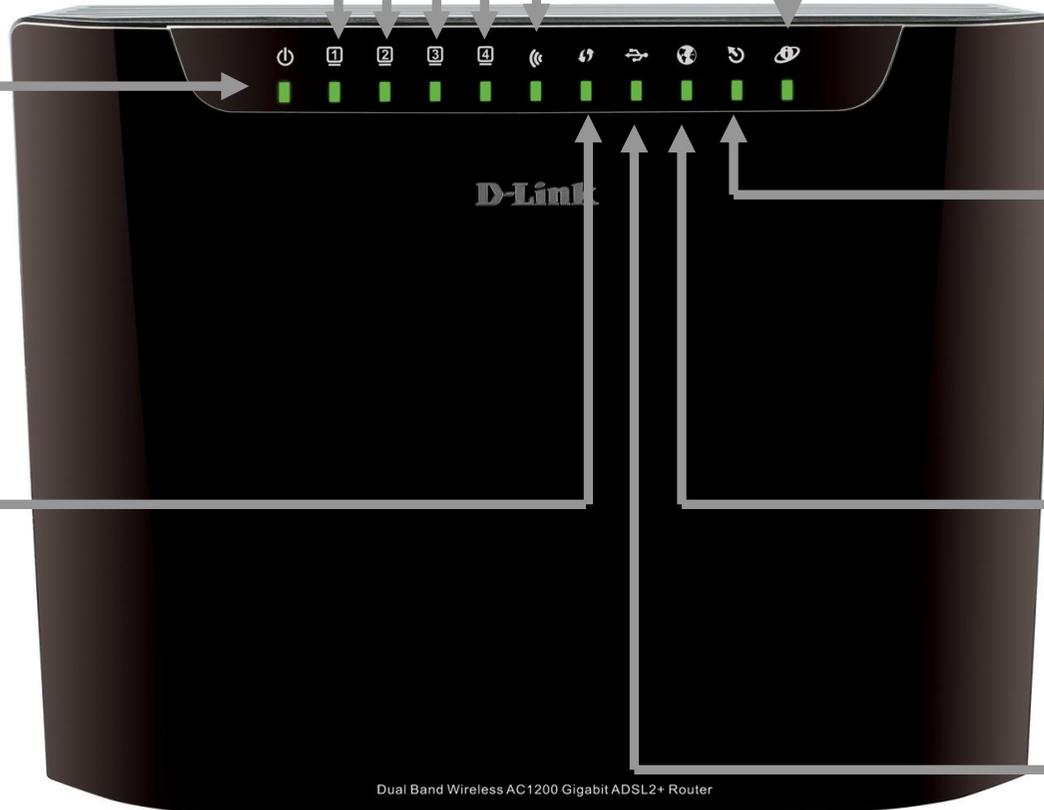
Dark indicates ready for new WPS connection. Blinking indicates WPS process is triggered and waiting for another WPS device joining. Steady **Blue** light indicates connection is successfully established between the router and the client. The LED will remain in solid **Blue** for 5 seconds.

Ethernet WAN

A solid **Green** light indicates a valid link on startup at 1000Mbps. A solid **Amber** light indicates a valid link on startup at 100Mbps. A solid **Green + Amber** light indicates link rate is 10Mbps. This light blinks when there is activity currently passing through the Ethernet port.

USB

Steady **Green** light indicates a successful USB connection. Dark if no USB device is plugged.



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-2880AL 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, Windows 7, and Windows 8.

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.

802.11 Wireless LAN Configuration

All the 802.11 wireless LAN settings may be configured on a single page using the web-based manager. For basic wireless communication you need to decide what channel to use and what SSID to assign. These two settings must be the same for any wireless workstations or other wireless access point that communicate with the DSL-2880AL through the wireless interface.

Security for wireless communication can be accomplished in a number of ways. DSL-2880AL supports WPA (Wi-Fi Protected Access), WPA2, and mixed WPA/WPA2. Wireless access can also be controlled by selecting MAC addresses that are allowed to associate with the device. Please read the section on Wireless Configuration.

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 need from the Internet service provider

Username

This is the Username used to log on to your ADSL service provider's network. It is commonly in the form user@isp.com.au or user@isp.co.nz. 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 / WAN Media Type / Connection Type

These settings describe the method your Internet 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):

- WAN Media Type (RJ-11 for DSL digital subscriber line or RJ-45 Ethernet for connecting your device to a VDSL bridge modem or a optical network unit, also known as ONU)
- PPPoE / PPPoA (PPPoE LLC, PPPoA LLC or PPPoA VC-Mux)
- Bridge Mode (1483 Bridged IP LLC or 1483 Bridged IP VC Mux)
- IPoA / MER (Static IP Address) (Bridged IP LLC, 1483 Bridged IP VC Mux, 1483 Routed IP LLC, 1483 Routed IP VC-Mux or IPoA)
- MER (Dynamic IP Address) (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 (ADSL2+ Multi-Mode) used for the Router automatically detects all types of ADSL, ADSL2, and ADSL2+ modulation. However, if you are instructed to specify the modulation type used for the Router, you may choose among the numerous options available on the Modulation Type drop-down menu on the ADSL Configuration window (Advanced > ADSL)

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 need to know about DSL-2880AL

System Administrator 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.

System Administrator 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-2880AL

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-2880AL

This is the subnet mask used by the DSL-2880AL, 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-2880AL to this Ethernet port using an Ethernet cable. You can also use the Ethernet ports on the DSL-2880AL to connect to other computer or Ethernet devices.

DHCP Client Status

Your DSL-2880AL 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-2880AL 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-2880AL Wireless ADSL Router.

Wireless Installation Considerations

DSL-2880AL lets you access your network using a wireless connection from virtually anywhere within the operating range of your wireless network. Keep in mind, however, that the number, thickness and location of walls, ceilings, or other objects that the wireless signals must pass through, may limit the range. Typical ranges vary depending on the types of materials and background RF (radio frequency) noise in your home or business. The key to maximizing wireless range is to follow these basic guidelines:

1. Keep the number of walls and ceilings between the D-Link router and other network devices to a minimum - each wall or ceiling can reduce your adapter's range from 3-90 feet (1-30 meters.) Position your devices so that the number of walls or ceilings is minimized.
2. Be aware of the direct line between network devices. A wall that is 1.5 feet thick (.5 meters), at a 45-degree angle appears to be almost 3 feet (1 meter) thick. At a 2-degree angle it looks over 42 feet (14 meters) thick! Position devices so that the signal will travel straight through a wall or ceiling (instead of at an angle) for better reception.
3. Building Materials make a difference. A solid metal door or aluminum studs may have a negative effect on range. Try to position access points, wireless routers, and computers so that the signal passes through drywall or open doorways. Materials and objects such as glass, steel, metal, walls with insulation, water (fish tanks), mirrors, file cabinets, brick, and concrete will degrade your wireless signal.
4. Keep your product away (at least 3-6 feet or 1-2 meters) from electrical devices or appliances that generate RF noise.
5. If you are using 2.4GHz cordless phones or X-10 (wireless products such as ceiling fans, lights, and home security systems), your wireless connection may degrade dramatically or drop completely. Make sure your 2.4GHz phone base is as far away from your wireless devices as possible. The base transmits a signal even if the phone is not in use.

Device Installation

DSL-2880AL Dual Band 802.11ac Wireless ADSL2+ Gigabit Ethernet Router maintains four separate interfaces, an Ethernet LAN, a wireless LAN, an Ethernet WAN and an ADSL Internet (WAN) connection. Carefully consider the Router's location suitable for connectivity for your Ethernet and wireless devices. You must have a functioning broadband connection via a bridge device such as a Cable or ADSL modem in order to use the Router's WAN function.

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, direct sunlight 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, desktop, or other stable platform. If possible, 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. Push down the Power button, and 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. Press and hold the reset button (the button just beside power button) while the device is powered off.
2. Turn on the power.
3. Wait for 10~15 seconds and then release the reset button.
4. To power off and power on again to make device boot-up in normal state

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 to ADSL Line

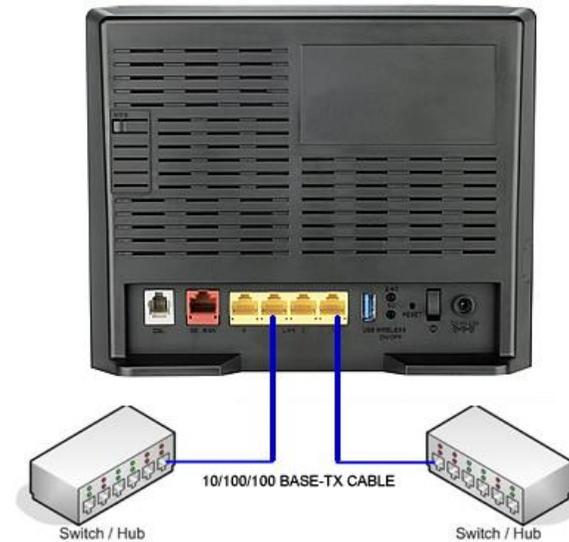
Use the ADSL cable included with the Router to connect it to a telephone wall socket or receptacle. Plug one end of the cable into the ADSL port (RJ-11 receptacle) on the rear panel of the Router and insert the other end into the RJ-11 wall socket. If you are using a low pass filter device, follow the 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 10/100/1000 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 8P8C RJ-45 Ethernet cable as shown in this diagram. 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 10/100/1000 BASE-TX Ethernet adapter card (NIC) installed on a PC using the straight-through 8P8C RJ-45 Ethernet cable provided as shown in this diagram.



Configuration

This section will show you how to configure your new D-Link wireless router using the web-based configuration utility.

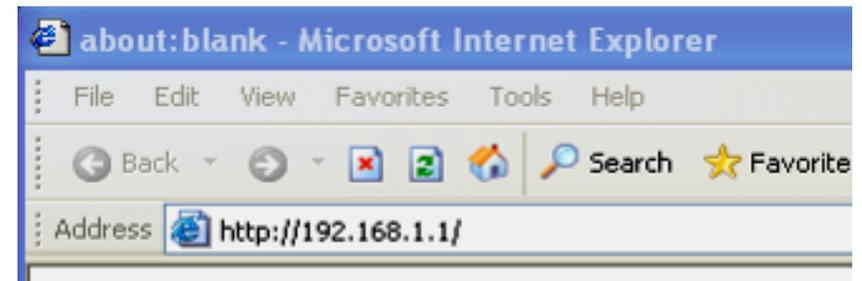
Web-based Configuration Utility

Connect to the Router

To configure the WAN connection used by the Router it is first necessary to communicate with the Router through its management interface, which is HTML-based and can be accessed using a web browser. The easiest way to make sure your computer has the correct IP settings is to configure it to use the DHCP server in the Router. The next section describes how to change the IP configuration for a computer running a Windows operating system to be a DHCP client.

To access the configuration utility, open a web-browser such as Internet Explorer and enter the IP address of the router (192.168.1.1).

Type “**admin**” for the User Name and “**admin**” in the Password field. If you get a **Page Cannot be Displayed** error, please refer to the **Troubleshooting** section for assistance.



SETUP

This chapter is concerned with using your computer to configure the WAN connection. The following chapter describes the various windows used to configure and monitor the Router including how to change IP settings and DHCP server setup.

INTERNET SETUP

To access the **INTERNET SETUP** (WAN) settings window, click on the **Internet Setup** button in the **SETUP** directory in this page:

INTERFACE SETUP:

ADSL INTERFACE

Click on the **Setup** button located over ADSL INTERFACE if you want to configure ADSL Interface WAN.

ETH INTERFACE

Click on the **Setup** button located over ETHERNET WAN INTERFACE if you want to configure Ethernet WAN.

The screenshot shows the 'Internet Setup' configuration page. On the left is a dark sidebar with a menu containing: Internet Setup (highlighted), Wireless Setup, LAN Setup, Time and Date, Parental Control, IPv6 Setup, USB Setup, and Logout. Below the menu are an 'Internet Online' status indicator, a language dropdown set to 'English', and a 'Reboot' button. The main content area has an orange header 'INTERFACE SETUP' with a grey box containing the text: 'There are 2 ways to setup your internet. You can use ADSL to configure the internet or you can assign one of the Ethernet ports as a WAN port to internet.' Below this are three sections: 'ADSL INTERFACE' with the text 'Use ADSL interface to setup your internet' and a 'Setup' button; 'ETHERNET WAN INTERFACE' with the text 'Assign one of the Ethernet ports as a WAN port to internet.' and a 'Setup' button; and 'USB3.5G INTERFACE' with the text 'use USB3.5G to configure you wan interface.' and a 'USB3.5G Interface' button.

ADSL WAN SETUP

Check **Manual Setup** box to configuring Internet connection manually or you can click on **Setup Wizard** button to configuring router step-by-step.

MANUAL ADSL CONNECTION SETUP

Please select the connection type for your internet connection.

If your Internet service supported IPv6, you can click **Enable IPv6 for this service** to setup IPv6 in this connection

ADSL SETUP

If you are configuring this device for the first time, D-Link recommends that you click Setup Wizard button, and follow the instructions on screen. If you wish to modify or configure the ADSL settings manually, tick Manual Setup to enable the ADSL Connection Setup.

Setup Wizard

Manual Setup

MANUAL ADSL CONNECTION SETUP

Please select the appropriate option to connect to your ISP.

- PPPoE/PPPoA** Choose this option if your ISP uses PPPoE/PPPoA. (For most DSL users).
- Dynamic IP Address** Choose this option if your ISP uses Dynamic IP Address over DSL.
- Static IP Address** Choose this option if your ISP uses Static IP assignments.
- Bridge** Choose this option if your ISP uses Bridge.
- Enable IPv6 for this service

Section 3 - Configuration

For PPPoE/PPPoA INTERNET CONNECTION TYPE:

Type in the **Username** and **Password** (and PPPoE **Service Name**, if required by your ISP).

Choose **PPPoE LLC/Snap-Bridging**, **PPPoE VC-mux**, **PPPoA LLC/encapsulation** and **PPPoA VC-mux** in drop-down menu.

You can use Static IPv4 Address check box and type **Static IP**.

Set **MTU** value which you want but should be less than 1492.

PPP IP Extension: Router passes the obtained IP address to the local PC and acts as a bridge only modem.

DNS AND DEFAULT GATEWAY

Select **Obtain DNS server address automatically** to get DNS from your ISP.

Or Select **Use the following DNS server addresses** to specify the DNS server IPs in the **Preferred DNS server** and **Alternate DNS server**.

PPPOE/PPPOA INTERNET CONNECTION TYPE :

Enter the information provided by your Internet Service Provider (ISP).

Username :

Password :

Service Name :

Static IP :

Connection Type :

MTU :

Idle Time Out : Minutes (0 = Always On)

PPP IP Extension :

DNS AND DEFAULT GATEWAY:

Obtain DNS server address automatically
WAN Interface selected:

Use the following DNS server addresses
Preferred DNS server:

Alternate DNS server:

Default Gateway interface
Selected Gateway Interface:

IPv6 DNS AND DEFAULT GATEWAY

Select **Obtain IPv6 DNS server address automatically** to get DNS from your ISP.

Or Select **Use the following IPv6 DNS server addresses** to type the DNS IPs in the **Preferred DNS server** and **Alternate DNS server**.

Select **Default IPv6 Gateway Interface** in drop-down menu

Set **VPI/VCI**, enable the **Enable NAT**

Enable the **Enable Firewall** when you want to have the basic filter function, for example, ICMP ping to DSL-2880AL.

Enable the **Enable IGMP Multicast Proxy** to send IGMP query packets to the IPTV clients.

Enable VLAN and type the **VLAN ID (0-4095)** which your ISP assigns.

Click on the **Apply** button to apply setting.

IPv6 DNS AND DEFAULT GATEWAY:

Obtain IPv6 DNS server address automatically
IPv6 WAN Interface selected:

Use the following IPv6 DNS server addresses
Preferred IPv6 DNS server:
Alternate IPv6 DNS server:

Default IPv6 Gateway interface
Selected IPv6 Gateway Interface:

VPI :
VCI :

Enable NAT :
Enable FIREWALL :
Enable IGMP Proxy :
Enable MLD Multicast Proxy :
Enable VLAN :

Section 3 - Configuration

For DYNAMIC IP ADDRESS INTERNET CONNECTION TYPE:

Type **Host Name** and select **Connection Type** in drop-down menu

DNS AND DEFAULT GATEWAY

Select **Obtain DNS server address automatically** to get DNS from your ISP.

Or Select **Use the following DNS server addresses** to type the DNS IP in the **Preferred DNS server** and **Alternate DNS server**.

IPv6 DNS AND DEFAULT GATEWAY

Select **Obtain IPv6 DNS server address automatically** to get DNS from your ISP.

Or Select **Use the following IPv6 DNS server addresses** to type the DNS IPs in the **Preferred DNS server** and **Alternate DNS server**.

Select **Default IPv6 Gateway Interface** in drop-down menu

Set **VPI/VCI**, enable the **Enable NAT**.

Enable the **Enable Firewall** when you want to have the basic filter function, for example, ICMP ping to DSL-2880AL.

Enable the **Enable IGMP Multicast Proxy** to send IGMP query packets to the IPTV clients.

Enable VLAN and type the **VLAN ID (0-4095)** which your ISP assigns.

Click on the **Apply** button to apply setting.

DYNAMIC IP ADDRESS INTERNET CONNECTION TYPE :

Use this Internet connection type if your Internet Service Provider (ISP) didn't provide you with IP Address information and/or a username and password.

Host Name :

Connection Type : 1483 Bridged IP LLC

Cloned MAC Address :

DNS AND DEFAULT GATEWAY:

Obtain DNS server address automatically
WAN Interface selected: CurrentIface

Use the following DNS server addresses
Preferred DNS server:

Alternate DNS server:

Default Gateway interface
Selected Gateway Interface: CurrentIface

IPv6 DNS AND DEFAULT GATEWAY:

Obtain IPv6 DNS server address automatically
IPv6 WAN Interface selected:

Use the following IPv6 DNS server addresses
Preferred IPv6 DNS server:

Alternate IPv6 DNS server:

Default IPv6 Gateway interface
Selected IPv6 Gateway Interface:

VPI :

VCI :

Enable NAT :

Enable FIREWALL :

Enable IGMP Proxy :

Enable MLD Multicast Proxy :

Enable VLAN :

For STATIC IP ADDRESS INTERNET CONNECTION TYPE

Type **IP Address**, **Subnet Mask**, **Default Gateway**, and select **Connection** in drop-down menu.

These information should be provided from your Internet Service Provider (ISP)

STATIC IPv6 ADDRESS INTERNET CONNECTION TYPE

Type **WAN IPv6 Address/Prefix Length** and **WAN Next-Hop IPv6 Address**

These information should be provided from your Internet Service Provider (ISP)

DNS AND DEFAULT GATEWAY

Select **Obtain DNS server address automatically** to get DNS from your ISP.

Or Select **Use the following DNS server addresses** to type the DNS IP in the **Preferred DNS server** and **Alternate DNS server**.

The screenshot displays the configuration interface for a router, divided into three main sections:

- STATIC IP ADDRESS INTERNET CONNECTION TYPE :** This section prompts the user to "Enter the static address information provided by your Internet Service Provider (ISP)". It contains four input fields: "IP Address", "Subnet Mask", and "Default Gateway", each with a text box. The "Connection Type" field is a dropdown menu currently set to "1483 Routed IP LLC".
- STATIC IPv6 ADDRESS INTERNET CONNECTION TYPE :** This section prompts the user to "Enter the static IPv6 address information provided by your Internet Service Provider (ISP)". It contains two input fields: "WAN IPv6 Address/Prefix Length" and "WAN Next-Hop IPv6 Address", each with a text box.
- DNS AND DEFAULT GATEWAY:** This section offers two options for DNS configuration:
 - Obtain DNS server address automatically**: This option is selected. Below it, "WAN Interface selected:" is set to "CurrentIface" via a dropdown menu.
 - Use the following DNS server addresses**: This option is unselected. Below it, there are two text boxes for "Preferred DNS server:" and "Alternate DNS server:".At the bottom of this section, under "Default Gateway interface", the "Selected Gateway Interface:" is set to "CurrentIface" via a dropdown menu.

IPv6 DNS AND DEFAULT GATEWAY

Select **Obtain IPv6 DNS server address automatically** to get DNS from your ISP.

Or Select **Use the following IPv6 DNS server addresses** to type the DNS IPs in the **Preferred DNS server** and **Alternate DNS server**.

Select **Default IPv6 Gateway Interface** in drop-down menu

Set **VPI/VCI**, enable the **Enable NAT**.

Enable the **Enable Firewall** when you want to have the basic filter function, for example, ICMP ping to DSL-2880AL.

Enable the **Enable IGMP Multicast Proxy** to send IGMP query packets to the IPTV clients.

Enable VLAN and type the **VLAN ID (0-4095)** which your ISP assigns.

Click on the **Apply** button to apply setting.

For BRIDGE CONNECTION TYPE

Select **Service Category**, **Encapsulation Mode** in drop-down menu.

Check **Enable Bridge Service** box and type **Service Name**.

Set **VPI/VCI**,

Enable VLAN and type the **VLAN ID (0-4095)** which your ISP assigns.

Click on the **Apply** button to apply setting.

The screenshot shows the 'IPv6 DNS AND DEFAULT GATEWAY' configuration window. It has two radio button options: 'Obtain IPv6 DNS server address automatically' (selected) and 'Use the following IPv6 DNS server addresses'. Below the second option are input fields for 'Preferred IPv6 DNS server' and 'Alternate IPv6 DNS server'. There is a section for 'Default IPv6 Gateway interface' with a dropdown menu for 'Selected IPv6 Gateway Interface'. Below this are input fields for 'VPI' (0) and 'VCI' (33). There are five checkboxes: 'Enable NAT', 'Enable FIREWALL', 'Enable IGMP Proxy', 'Enable MLD Multicast Proxy', and 'Enable VLAN', all of which are currently unchecked. At the bottom right are 'Apply' and 'Cancel' buttons.

The screenshot shows the 'BRIDGE CONNECTION TYPE' configuration window. It prompts the user to 'Enter following information provided by your Internet Service Provider (ISP)'. There are two dropdown menus: 'Service Category' (set to 'UBR Without PCR') and 'Encapsulation Mode' (set to 'LLC/SNAP-BRIDGING'). There is a checked checkbox for 'Enable Bridge Service' and an input field for 'Service Name' containing 'br_0_33'. Below this are input fields for 'VPI' (0) and 'VCI' (33), and an unchecked checkbox for 'Enable VLAN'. At the bottom right are 'Apply' and 'Cancel' buttons.

ETHERNET WAN SETUP

To click Setup button from ETHERNET WAN INTERFACE to initiate Ether WAN configuration.

INTERFACE SETUP

There are 2 ways to setup your internet. You can use ADSL to configure the internet or you can assign one of the Ethernet ports as a WAN port to internet.

ADSL INTERFACE

Use ADSL interface to setup your internet

ETHERNET WAN INTERFACE

Assign one of the Ethernet ports as a WAN port to internet.

USB3.5G INTERFACE

use USB3.5G to configure you wan interface.

MANUAL ETH WAN CONNECTION SETUP

This section is same as previous **MANUAL ADSL CONNECTION SETUP** section. Here you pick up the connection type, enter access authorization information, DNS server

ETHERNET WAN SETUP

You can setup this device to Internet by another ways, assigning one of the LAN ports to be a WAN port. Therefore, you can keep using this device even you changed your internet service from ADSL to others, e.g. Cable Modem, FTTH.

MANUAL ETH WAN CONNECTION SETUP

Please select the appropriate option to connect to your ISP.

PPPoE Choose this option if your ISP uses PPPoE.(For most DSL users)

Dynamic IP Address Choose this option if your ISP uses Dynamic IP Address over DSL.

Static IP Address Choose this option if your ISP uses Static IP assignments.

Enable IPv6 for this service

PPPOE INTERNET CONNECTION TYPE :

Enter the information provided by your Internet Service Provider (ISP).

Username :

Password :

Servername :

MTU :

Idle Time Out : Minutes
(0 = Always On)

PPP IP Extension :

WIRELESS SETUP

Use this section to configure the wireless settings for your D-Link router. Please note that changes made in this section will also need to be duplicated onto your wireless clients and PC.

To access the **WIRELESS** (WLAN) settings window, click on the **Wireless Setup** button in the **SETUP** tab.

Wireless Network Setting

Click on the **Wireless Connection Setup Wizard** button to setup the wireless connection in an easy way. It will use Web-based Wizard to assist you in connecting to your new D-Link Systems Wireless Router.

Note: Before launching the wizard, please make sure you have followed all steps outlined in the Quick Installation Guide included in the package.

Click on the **Add Wireless Device with WPS** button. This wizard is designed to assist you in connecting your wireless device to your router with WPS. It will guide you through step-by-step instructions on how to get your wireless device connected.

If you would like to configure the Wireless settings of you new D-Link Router manually, then click on the **Manual Wireless Connection Setup** button.

The screenshot displays the router's configuration interface. On the left, a vertical menu lists various setup options, with 'Wireless Setup' highlighted. The main panel is titled 'WIRELESS SETUP' and provides instructions and options for configuring the wireless network. It includes a wizard button, a WPS button, and a manual setup button, each accompanied by explanatory text and a note.

Section 3 - Configuration

Welcome to the D-Link Wireless Security Setup Wizard

Enable Your Wireless Network Your wireless network is enabled by default. You can simply uncheck the below checkbox to disable wireless

Network Name (SSID) identifies members of the Service Set. Accept the default name or change it to something else. If the default SSID is changed, all the previous connected wireless devices on the wireless network must reconfigure their wireless connection setting as the AP setting change will not apply to the client automatically.

Manually assign a network key You can also set it manually if you do not prefer the key we generate. Type a string (8-63 characters, such as a~z, A~Z, or 0~9.) on the **Pre-Shared** key.

Click **Next** button to go to the next page.

Click **Cancel** button to return to the main menu of Wireless Setup page.

Check your wireless network setting.

Click **Save** button to apply your setting.

Click **Prev** button to pre-page to modify your setting.

Click **Cancel** button to cancel your setting.

WELCOME TO THE D-LINK WIRELESS SECURITY SETUP WIZARD

Your wireless network is enabled by default. You can simply uncheck the below checkbox to disable wireless.

Enable Your Wireless Network

Give your network a name, using up to 32 characters.

Wireless Network Name (SSID) :
(1-32 characters)

Set your wireless encryption mode. We will automatically assign a security key to prevent outsiders from accessing your wireless network, the router will automatically assign a security key to your wireless network.

Wireless Security Mode : **Auto (WPA or WPA2)**

Pre-Shared Key :
(8-63 characters, such as a~z, A~Z, or 0~9.)

Note: We provide user a random pre-shared key by automatically. You can also set it manually if you do not prefer the key we generate.

WELCOME TO THE D-LINK WIRELESS SECURITY SETUP WIZARD

Please enter the following settings in the wireless device that you are adding to your wireless network and keep a note of it for future reference.

Wireless Status : Enabled

Network Name(SSID) : D-Link

Wireless Security Mode : Auto(WPA or WPA2)

Network Key : 4nl9qymzk

Add Wireless Device with WPS

The wizard shows the option to setup WPS by **Auto** or **Manual**.

Auto -- Select this option if your wireless device supports WPS(Wi-Fi Protected Setup)

Manual -- Select this option to display the current wireless settings for you to configure the wireless device manually.

Click **Next** button to go to the next page.

Click **Cancel** button to return to the main menu of Wireless Setup page.



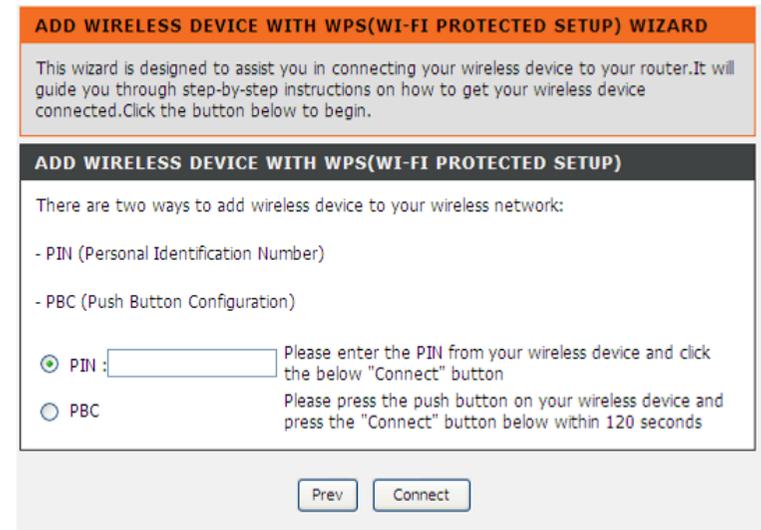
Add Wireless Device with WPS (Automatically)

This page allows you to select PIN or PBC to use WPS method.

PIN -- Enter the PIN code from your wireless device and click the below **Connect** button to start the handshaking.

PBC-- Please press the **Connect** button and hold on for 3 seconds on your wireless device and presses the **Connect** button below within 120 seconds to start the handshaking.

Click **Prev** to go back to previous page.



Section 3 - Configuration

Add Wireless Device with WPS (WI-FI PROTECTED SETUP) WIZARD

This page will count down the timer and please start WPS on the wireless device you are adding in time.

Add Wireless Device with WPS (Manually)

This screen shows the information for the SSID, Wireless Security Mode, the Network key and allow you to modify the current setting, if you select **Auto** in the previous page, you won't see this page and please refer to next column.

Please type network name on the **Network Name SSID**.

Please type network key on the **Network Key**

Click **OK** button to process the next page.

Add Wireless Device with WPS (WI-FI PROTECTED SETUP)

Finally it will show all the configurations. You can check if it is exact, please click the **Next** button.

ADD WIRELESS DEVICE WITH WPS(WI-FI PROTECTED SETUP) WIZARD

This wizard is designed to assist you in connecting your wireless device to your router. It will guide you through step-by-step instructions on how to get your wireless device connected. Click the button below to begin.

VIRTUAL PUSH BUTTON

Please press down the Push Button (Physical or virtual) on the wireless device you are adding to your wireless network within **80** seconds ...

AP button pushed or PIN entered

ADD WIRELESS DEVICE WITH WPS(WI-FI PROTECTED SETUP)

The WPA2 (Wi-Fi Protected Access) key must meet one of the following guidelines:

- Between 8 and 63 characters (A longer WPA key is more secure than a short one)
- Exactly 64 characters using 0-9 and A-F

Network Name (SSID) :

Network Key :

Prev Next Cancel

ADD WIRELESS DEVICE WITH WPS(WI-FI PROTECTED SETUP)

Please enter the following settings in the wireless device that you are adding to your wireless network and keep a note of it for future reference.

Network Name (SSID) : D-Link

Wireless Security Mode : WPA2-PSK (TKIP+AES)

Network Key : 1234567890

Prev Next Cancel

Manual WIRELESS Connection Setup SETTINGS

DSL-2880AL comes with 2 physical wireless interfaces (known 2.4GHz and 5GHz).

Click on the **Enable Wireless** box to activate the wireless interface. You can use the **Add New** button to create a schedule and apply to the wireless interface. (Remark: To have scheduler operate properly, please ensure you have activated NTP BEFORE you create a new schedule.)

The **SSID** identifies members of the Service Set. Accept the default name or change it to something you desire. Every time you change the SSID, all the previous connected wireless client(s) will lost connection. In order to get the wireless connection back, all the wireless client(s) MUST re-associate to the new SSID again.

How to configure wireless channel?

Enable Auto Channel Scan so that the router can select the best possible channel for your wireless network to operate on.

The **Wireless Channel** which allows you to specify the wireless channel of your access point employs. We would strongly recommend you to leave the setting as AUTO to prevent wireless interference.

Note: Amount of wireless channel available may various in different countries due to difference in regulation.

Suggestion from configuring 802.11 mode

Select **802.11 Mixed Mode** if you are not sure which type of wireless client may associate to this wireless interface or specify the desired wireless mode to employ.

WIRELESS

Use this section to configure the wireless settings for your D-Link router. Please note that changes made on this section will also need to be duplicated to your wireless clients and PC.

2.4G WIRELESS NETWORK SETTINGS

Enable Wireless :	<input checked="" type="checkbox"/>	Always	<input type="button" value="Add New"/>
Wireless Network Name (SSID) :	D-Link DSL2880		
Wireless Channel :	Auto		
802.11 Mode :	Mixed 802.11n, 802.11g and 802.11b		
Channel Width :	20/40 MHz(Auto)		
Visibility Status :	<input checked="" type="radio"/> Visible <input type="radio"/> Invisible		
AP Isolation :	<input type="checkbox"/>		

2.4G WIRELESS SECURITY MODE

To protect your privacy you can configure wireless security features. This device supports three wireless security modes including: WEP, WPA-Personal, and WPA-Enterprise. WEP is the original wireless encryption standard. WPA provides a higher level of security. WPA-Personal does not require an authentication server. The WPA-Enterprise option requires an external RADIUS server.

Security Mode : None

Channel Bandwidth

2.4G Wireless Interface

With 2.4G interface, you can choose 20MHz (up to 150Mbps) or Auto 20/40MHz to achieve maximum performance of 300Mbps (at 40MHz)*

Remark: When 20/40MHz is employed, wireless AP will dynamically scan the wireless channel condition. An additional wireless channel will be employed and bandwidth will therefore double up - ONLY when there is no wireless interference detected. The better performance the more bandwidth is required.

5G Wireless Interface

With 5G interface, you can choose 20MHz, 20/40 MHz or 20/40/80 MHz (Auto). Similar to 2.4G interface, better performance may achieve if you select 20/40 MHz (up to 400Mbps at 40MHz) or 20/40/80 MHz Auto mode (up to 866Mbps at 80MHz).

Visibility Status

Choose Visible or Invisible to decide if you want to have the SSID hidden for better security.

The image shows a configuration interface for a wireless network. It is divided into two main sections: "5G WIRELESS NETWORK SETTINGS" and "5G WIRELESS SECURITY MODE".

5G WIRELESS NETWORK SETTINGS:

- Enable Wireless:** A checked checkbox, followed by a dropdown menu set to "Always" and an "Add New" button.
- Wireless Network Name (SSID):** A text input field containing "D-Link DSL2880_5G".
- Wireless Channel:** A dropdown menu set to "Auto".
- 802.11 Mode:** A dropdown menu set to "Mixed 802.11ac, 802.11n and 802.11a".
- Channel Width:** A dropdown menu set to "20/40/80 MHz(Auto)".
- Visibility Status:** Two radio buttons: "Visible" (selected) and "Invisible".
- AP Isolation:** An unchecked checkbox.

5G WIRELESS SECURITY MODE:

To protect your privacy you can configure wireless security features. This device supports three wireless security modes including: WEP, WPA-Personal, and WPA-Enterprise. WEP is the original wireless encryption standard. WPA provides a higher level of security. WPA-Personal does not require an authentication server. The WPA-Enterprise option requires an external RADIUS server.

Security Mode: A dropdown menu set to "None".

Section 3 - Configuration

WIRELESS SECURITY Mode

To protect your privacy you can configure wireless security features. This device supports three wireless security modes including: **WEP, WPA, WPA2, Auto (WPA or WPA2)**. WEP is the original wireless encryption standard. WPA provides a higher level of security. WPA-Personal does not require an authentication server. The WPA-Enterprise option requires an external RADIUS server.

WIRELESS SECURITY MODE – WEP

WEP (Wireless Encryption Protocol) encryption can be enabled for security and privacy. WEP encrypts the data portion of each frame transmitted from the wireless adapter using one of the predefined keys. The router offers 64 or 128 bit encryption with four keys available.

Select **WEP Key Length** from the drop-down menu. (**128 bit** is stronger than **64 bit**)

Specify the encryption key from the **Current Network Key** drop-down menu.

Enter the key into the **WEP Key** field 1~4. (Key length is outlined at the bottom of the window.)

Select **Authentication** type from the drop-down menu. (**Shared** is better than **Open**)

Click on the **Apply Settings** button to apply settings.

WIRELESS SECURITY MODE

To protect your privacy you can configure wireless security features. This device supports three wireless security modes including: WEP, WPA-Personal, and WPA-Enterprise. WEP is the original wireless encryption standard. WPA provides a higher level of security. WPA-Personal does not require an authentication server. The WPA-Enterprise option requires an external RADIUS server.

Security Mode :

Please take note of your SSID and security Key as you will need to duplicate the same settings to your wireless devices and PC.

Apply Settings

Cancel

WEP

WEP is the wireless encryption standard. To use it you must enter the same key(s) into the router and the wireless stations. For 64 bit keys you must enter 10 hex digits into each key box. For 128 bit keys you must enter 26 hex digits into each key box. A hex digit is either a number from 0 to 9 or a letter from A to F. For the most secure use of WEP set the authentication type to "Shared Key" when WEP is enabled.

You may also enter any text string into a WEP key box, in which case it will be converted into a hexadecimal key using the ASCII values of the characters. A maximum of 5 text characters can be entered for 64 bit keys, and a maximum of 13 characters for 128 bit keys.

WEP Key Length : (length applies to all keys)

WEP Key 1 :

WEP Key 2 :

WEP Key 3 :

WEP Key 4 :

Default WEP Key :

Authentication :

Please take note of your SSID and security Key as you will need to duplicate the same settings to your wireless devices and PC.

Apply Settings

Cancel

Section 3 - Configuration

WIRELESS SECURITY MODE – WPA-Personal

Use **WPA** or **WPA2** mode to achieve a balance of strong security and best compatibility. This mode uses WPA for legacy clients while maintaining higher security with stations that are WPA2 capable. Also the strongest cipher that the client supports will be used. For best security, use **WPA2** mode. This mode uses AES (CCMP) cipher and legacy stations are not allowed access with WPA security. For maximum compatibility, use **WPA**. This mode uses TKIP cipher. Some gaming and legacy devices work only in this mode.

Choose **WPA / WPA2 / Auto(WPA or WPA2)** on the **WPA Mode**

Type the value seconds on the **Group Key Update Interval**. The default value is 1800.

WPA / WPA2 -PSK (Personal)

Type the string on the **Pre-Shared Key**

Click the **Apply Settings** button to save the configuration.

WIRELESS SECURITY MODE

To protect your privacy you can configure wireless security features. This device supports three wireless security modes including: WEP, WPA-Personal, and WPA-Enterprise. WEP is the original wireless encryption standard. WPA provides a higher level of security. WPA-Personal does not require an authentication server. The WPA-Enterprise option requires an external RADIUS server.

Security Mode :

WPA

Use **WPA** or **WPA2** mode to achieve a balance of strong security and best compatibility. This mode uses WPA for legacy clients while maintaining higher security with stations that are WPA2 capable. Also the strongest cipher that the client supports will be used. For best security, use **WPA2 Only** mode. This mode uses AES(CCMP) cipher and legacy stations are not allowed access with WPA security. For maximum compatibility, use **WPA Only**. This mode uses TKIP cipher. Some gaming and legacy devices work only in this mode.

WPA Mode : (TKIP)

Group Key Update Interval : (seconds)

PRE-SHARED KEY

Pre-Shared Key :

Please take note of your SSID and security Key as you will need to duplicate the same settings to your wireless devices and PC.

Section 3 - Configuration

WPA / WPA2 (Enterprise)

Some network-security experts now recommend that wireless networks use 802.1X security measures to overcome some weaknesses in standard WEP applications. A RADIUS server is used to authenticate all potential users. .

Enter your RADIUS server data: **IP Address**, **Port**, and **Key**.

Click on the **Apply Settings** button to apply settings.

WIRELESS SECURITY MODE

To protect your privacy you can configure wireless security features. This device supports three wireless security modes including: WEP, WPA-Personal, and WPA-Enterprise. WEP is the original wireless encryption standard. WPA provides a higher level of security. WPA-Personal does not require an authentication server. The WPA-Enterprise option requires an external RADIUS server.

Security Mode :

WPA

Use **WPA or WPA2** mode to achieve a balance of strong security and best compatibility. This mode uses WPA for legacy clients while maintaining higher security with stations that are WPA2 capable. Also the strongest cipher that the client supports will be used. For best security, use **WPA2 Only** mode. This mode uses AES(CCMP) cipher and legacy stations are not allowed access with WPA security. For maximum compatibility, use **WPA Only**. This mode uses TKIP cipher. Some gaming and legacy devices work only in this mode.

WPA Mode : **(TKIP or AES)**

Group Key Update Interval : (seconds)

EAP (802.1X)

When WPA enterprise is enabled, the router uses EAP (802.1x) to authenticate clients via a remote RADIUS server.

Authentication Timeout : (seconds)

RADIUS server IP Address :

RADIUS server Port :

RADIUS server Shared Secret :

Please take note of your SSID and security Key as you will need to duplicate the same settings to your wireless devices and PC.

LAN SETUP

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.

To access the **Local Network** setting window, click on the **Local Network** button in the **SETUP** tab.

ROUTER SETTINGS

To change the **Router IP Address** or **Subnet Mask**, type in the desired values.

DHCP SERVER SETTINGS (OPTIONAL)

The **Enable DHCP Server** is selected by default for the Router's Ethernet LAN interface.

Set the **DHCP IP Address Range** and the default is from **192.168.1.2** to **192.168.1.254**. The IP address pool can be up to 253 IP addresses.

Set the value hours on the **DHCP Lease Time**

If you don't want DSL-2880AL to be the DHCP server, you can enable

DHCP relay to pass the DHCP discover packets of the clients to another DHCP server.

Please set the DHCP server IP address on the **DHCP Server IP Address**

LAN SETUP

This section allows you to configure the local network settings of your router. Please note that this section is optional and you should not need to change any of the settings here to get your network up and running.

ROUTER SETTINGS

Use this section to configure the local network settings of your router. The IP Address that is configured here is the IP Address that you use to access the Web-based management interface. If you change the IP Address here, you may need to adjust your PC's network settings to access the network again.

Router IP Address :

Subnet Mask :

DHCP SERVER SETTINGS (OPTIONAL)

Use this section to configure the built-in DHCP Server to assign IP addresses to the computers on your network.

Enable DHCP Server :

DHCP IP Address Range : to

DHCP Lease Time : (hours)

DHCP Relay :

DHCP Server IP :

Section 3 - Configuration

ADD/EDIT DHCP RESERVATION (OPTIONAL)

Select the **Enable** to let you reserve the **IP Address** for the designated PC with the configured **MAC Address**.

Computer Name is user defined meaningful host name which can help you recognize each PC connecting to the device.

Clicking on the **Copy Your PC's MAC Address** button to copy the MAC address from the PC you are currently browsing this device management web page.

Click on the **Apply button** to save the new created DHCP Reservation entry

DHCP RESERVATIONS LIST

After saved the DHCP reservation, the **DHCP RESERVATIONS LIST** will list the configuration.

The **NUMBER OF DYNAMIC DHCP CLIENTS** shows amount of DHCP clients (PC or Laptop) connected to the router currently.

Click on the **Save Settings** button.

DHCP RESERVATION (OPTIONAL)				
	Enable	Computer Name	MAC Address	The IP Address
<input type="checkbox"/>	Enable	L421	e8:9a:8f:13:42:37	192.168.1.8

ADD/EDIT DHCP RESERVATION (OPTIONAL)	
Enable :	<input checked="" type="checkbox"/>
Computer Name :	<input type="text" value="D-Link"/>
The IP address " :	<input type="text" value="192.168.1.100"/>
MAC Address :	<input type="text" value="00:1a:2b:3c:4d:5e"/>
<input type="button" value="Copy Your PC's MAC Address"/>	

NUMBER OF DYNAMIC DHCP CLIENTS : 1			
Computer Name	MAC Address	The IP Address	Expire Time
TWHC1NB0037	e8:9a:8f:13:42:37	192.168.1.8	23 hours, 59 minutes, 37 seconds

TIME AND DATE

The **Time and Date** configuration option allows you to configure, update, and maintain the correct time on the internal system clock. From this section you can set the time zone that you are in and set the NTP (Network Time Protocol) Server. Daylight Saving can also be configured to automatically adjust the time when needed.

To access the **TIME** setting window, click on the **Time and Date** button in the **SETUP tab**

TIME SETTING:

Check the **Automatically synchronize with Internet time servers**

Select specific time server to use from the **First NTP time server** and **Second NTP time server** specific NTP server name.

TIME CONFIGURATION:

Select your operating time zone from the **Time Zone** drop-down menu.

If you need to use the daylight saving, just choose the **Enable Daylight Saving**. Daylight saving is a period from late Spring to early Fall.

Set how many hours to change the time for Daylight saving Offset.

Configure Daylight Saving Dates, Daylight Saving time starts in the most parts of the **United States** on the second Sunday of March. Each time zone in the United States starts Daylight Saving time at 2 A.M. Thus, in the United States you must use **March, Second, Sunday**, at **2:00 A.M.**

Daylight Saving time starts in the **European Union** on the last Sunday of March. Thus, in European Union, you must select **March, Last, Sunday**. The time must depend on your country's time zone. For example, In Germany you must type 2 because

The screenshot shows the router's configuration interface. On the left is a navigation menu with options: Wizard, WAN Setup, Wireless Setup, LAN Setup, Time and Date (highlighted), IPv6 Setup, USB Setup, and Logout. Below the menu is an 'Internet Online' status indicator and a 'Reboot' button. The main content area is titled 'TIME' and contains three sections: 1. 'TIME SETTINGS' with a checked checkbox for 'Automatically synchronize with Internet time servers', and two rows for 'First NTP time server' and 'Second NTP time server', each with a dropdown menu and a text input field. 2. 'TIME CONFIGURATION' showing 'Current Router Time' as Thursday, September 05, 2013 08:54:11 PM, a 'Time Zone' dropdown set to '(GMT+10:00) Canberra, Melbourne, Sydney', an unchecked 'Enable Daylight Saving' checkbox, a 'Daylight Saving Offset' dropdown set to '-2:00', and 'Daylight Saving Dates' with fields for Start and End (Month, Week, Day, Time).

Section 3 - Configuration

Germany's time zone is 1 hour ahead of GMT or UTC (GMT+1). Thus, in Germany you must use **March, Last, Sunday, at 1:00 A.M.**

Daylight Saving time ends in the most parts of the United States on the First Sunday of November. Each time zone in the United States must use Daylight Saving time at 2:00 A.M. Thus, in the United States you must set **November, First, Sunday, at 2:00 A.M.**

Daylight Saving time ends in the European Union on the Last Sunday of October. For instance, in Germany you must type 2 because Germany's time zone is 1 hour ahead of GMT (GMT+1). Thus, in Germany you must use **March, Last, Sunday, at 1:00 A.M.**

SET THE DATE AND TIME MANAULLY

You can also use the **Copy Your Computer's Time Settings** to synchronize the Date and Time to your local PC. Or, you also can adjust **Year/Month/Day/Hour/Minute/Second** manually.

Please click the **Apply** button to save the configuration.

SET THE DATE AND TIME MANAULLY

Date And Time :

Year: 2012 Month: Oct Day: 23

Hour: 7 pm Minute: 27 Second: 34

Copy Your Computer's Time Settings

Apply Cancel

IPv6

The **IPv6** configuration option allows you configure IPv6 internet connection. You can configure follow **IPv6 Internet Connection Setup Wizard** utilize or **Manually IPv6 Internet Connection Setup**.

To access the **IPv6** setting window, click on the **IPv6** button in the **SETUP** tab

Manual IPv6 Internet Connection Setup

Use this section to configure your IPv6 Connection type. If you are unsure of your connection method, please contact your Internet Service Provider.

IPv6 INTERFACE

Choose the IPv6 Interface in the drop-down menu.

IPv6 CONNECTION TYPE

Choose the IPv6 internet connection type from the drop-down menu:

- **Link-local only**
- **Static IPv6**
- **Autoconfiguration (SLAAC/DHCPv6)**
- **PPPoE**
- **DS-Lite**

The screenshot shows the IPv6 configuration wizard interface. On the left is a navigation menu with the following items: Internet Setup, Wireless Setup, LAN Setup, Time and Date, Parental Control, IPv6 Setup (highlighted), USB Setup, and Logout. Below the menu is the 'Internet Online' logo and a language dropdown menu set to 'English'. The main content area is titled 'IPv6' and contains the following sections:

- IPv6**: A header section with an orange background. Below it is a text box: "Use this section to configure your IPv6 Connection type. If you are unsure of your connection method, please contact your Internet Service Provider." At the bottom of this section are two buttons: "Save Settings" and "Don't Save Settings".
- IPv6 INTERFACE**: A section with a dark header. Below it is the text: "Choose the interface to be used by the router to the IPv6 Internet." Below this text is a label "My IPv6 Interface is:" followed by a dropdown menu showing "atm0".
- IPv6 CONNECTION TYPE**: A section with a dark header. Below it is the text: "Choose the mode to be used by the router to the IPv6 Internet." Below this text is a label "My IPv6 Connection is:" followed by a dropdown menu showing "PPPoE".

IPv6 Connection Type: [Link-local only](#)

LAN IPv6 ADDRESS SETTING

Link-local only is communication with in internal network. The **LAN IPv6 Link-local Address** is used as default setting.

IPv6 CONNECTION TYPE
Choose the mode to be used by the router to the IPv6 Internet.
My IPv6 Connection is : <input type="text" value="Link-local only"/>

LAN IPV6 ADDRESS SETTINGS
Use this section to configure the internal network settings of your router. If you change the LAN IPv6 Address here, you may need to adjust your PC networksettings to access the network again
LAN IPv6 Link-Local Address : FE80::21A:2BFF:FE12:3315/64

IPv6 Connection Type: **Static IPv6**

WAN IPv6 ADDRESS SETTINGS

You can check **Use Link-Local Address box** to Link-local only, or type the WAN IPv6 Address and **Subnet Prefix Length**.

Type **Default Gateway**, **Primary IPv6 DNS server** and **Secondary IPv6 DNS server**.

These information provided by your Internet Service Provider (ISP)

LAN IPv6 ADDRESS SETTINGS

Configure the internal network settings of your router. You can change the **LAN IPv6 Address**.

ADDRESS AUTOCONFIGURATION SETTINGS

SLAAC+Stateless DHCP to set computers on Router network obtained IPv6 address by stateless DHCP.

SLAAC+RDNSS to set computers on Router network obtained IPv6 address by RDNSS

Stateful DHCP to set computers on Router network obtained IPv6 address by Stateful DHCP, you need type the IPv6 Address Range (Start and End)

IPv6 CONNECTION TYPE

Choose the mode to be used by the router to the IPv6 Internet.

My IPv6 Connection is :

WAN IPv6 ADDRESS SETTINGS

Enter the IPv6 address information provided by your Internet Service Provider (ISP).

Use Link-Local Address :

IPv6 Address :

Subnet Prefix Length :

Default Gateway :

Primary IPv6 DNS Server :

Secondary IPv6 DNS Server :

LAN IPv6 ADDRESS SETTINGS

Use this section to configure the internal network settings of your router. If you change the LAN IPv6 Address here, you may need to adjust your PC network settings to access the network again

LAN IPv6 Address : /64

LAN IPv6 Link-Local Address : FE80::F27D:88FF:FED9:FFB/64

ADDRESS AUTOCONFIGURATION SETTINGS

Use this section to setup IPv6 Autoconfiguration to assign IP addresses to the computers on your network.

Enable automatic IPv6 address assignment :

Autoconfiguration Type :

Router Advertisement Lifetime : (minutes)

ADDRESS AUTOCONFIGURATION SETTINGS

Use this section to setup IPv6 Autoconfiguration to assign IP addresses to the computers on your network.

Enable automatic IPv6 address assignment :

Autoconfiguration Type :

IPv6 Address Range(Start) : ::

IPv6 Address Range(End) : ::

IPv6 Address Lifetime : (minutes)

IPv6 Connection Type: Autoconfiguration (SLAAC/DHCPv6)

IPv6 DNS SETTING

Choose Obtain IPv6 DNS servers automatically or type **Primary IPv6 DNS server** and **Secondary IPv6 DNS server**.

LAN IPv6 ADDRESS SETTINGS

Enable DHCP-PD to used Prefix Delegation assigned IPv6 Prefix. Or you can change the **LAN IPv6 Address**.

ADDRESS AUTOCONFIGURATION SETTINGS

SLAAC+Stateless DHCP to set computers on Router network obtained IPv6 address by stateless DHCP.

SLAAC+RDNSS to set computers on Router network obtained IPv6 address by RDNSS

Stateful DHCP to set computers on Router network obtained IPv6 address by Stateful DHCP, you need type the IPv6 Address Range (Start and End)

The screenshot displays a web-based configuration interface for IPv6 settings, organized into several sections:

- IPv6 CONNECTION TYPE:** A dropdown menu is set to "Autoconfiguration (SLAAC/DHCPv6)".
- IPv6 DNS SETTINGS:** The option "Obtain IPv6 DNS servers automatically" is selected. Below are empty input fields for "Primary IPv6 DNS Server" and "Secondary IPv6 DNS Server".
- LAN IPv6 ADDRESS SETTINGS:** "Enable DHCP-PD" is checked. The "LAN IPv6 Address" field is empty, followed by "/64". The "LAN IPv6 Link-Local Address" is pre-filled with "FE80::F27D:88FF:FED9:FFB/64".
- ADDRESS AUTOCONFIGURATION SETTINGS (top):** "Enable automatic IPv6 address assignment" is checked. The "Autoconfiguration Type" is set to "SLAAC + Stateless DHCP". The "Router Advertisement Lifetime" is set to 30 minutes.
- ADDRESS AUTOCONFIGURATION SETTINGS (bottom):** "Enable automatic IPv6 address assignment" is checked. The "Autoconfiguration Type" is set to "Stateful DHCP". Below are input fields for "IPv6 Address Range(Start)" (with "::0001" as a suffix), "IPv6 Address Range(End)" (with "::0200" as a suffix), and "IPv6 Address Lifetime" set to 30 minutes.

IPv6 Connection Type: PPPoE

PPPoE session set Share with IPv4

At **Address Mode** if you choose **Dynamic IP**, router will obtain WAN IPv6 address by Dynamically or you can set static IPv6 address in **Static IP Address/Prefix Length** to router.

Type **User Name**, **Password**, **Verify Password**, **Service Name**(if necessarily),

Reconnect Mode set to **Always on**, set MTU value which you want but should be less than 1492 on the **MTU**

These information provided by your Internet Service Provider (ISP)

IPv6 DNS SETTING

Choose Obtain IPv6 DNS servers automatically or type **Primary IPv6 DNS server** and **Secondary IPv6 DNS server**.

LAN IPv6 ADDRESS SETTINGS

Enable DHCP-PD to use Prefix Delegation assigned IPv6 Prefix. Or you can change the **LAN IPv6 Address**.

ADDRESS AUTOCONFIGURATION SETTINGS

SLAAC+Stateless DHCP to set computers on Router network obtained IPv6 address by stateless DHCP.

The screenshot displays the IPv6 configuration interface, organized into several sections:

- IPV6 CONNECTION TYPE:** A dropdown menu is set to "PPPoE".
- PPPOE:** This section contains fields for "PPPoE session" (radio buttons for "Share with IPv4" and "Create a new session"), "Address Mode" (radio buttons for "Dynamic IP" and "Static IP"), "IP Address/Prefix Length", "User Name", "Password", "Verify Password", "Service Name" (optional), "Reconnect Mode" (radio buttons for "Always on", "On demand", and "Manual"), "Maximum Idle Time" (minutes, 0=infinite), and "MTU" (1492 bytes, with a default of 1492).
- IPV6 DNS SETTINGS:** Radio buttons allow for "Obtain IPv6 DNS servers automatically" (selected) or "Use the following IPv6 DNS servers". Below are input fields for "Primary IPv6 DNS Server" and "Secondary IPv6 DNS Server".
- LAN IPV6 ADDRESS SETTINGS:** A checkbox for "Enable DHCP-PD" is checked. Below are input fields for "LAN IPv6 Address" (with a /64 suffix) and "LAN IPv6 Link-Local Address" (pre-filled with FE80::F27D:88FF:FED9:FB/64).
- ADDRESS AUTOCONFIGURATION SETTINGS:** A checkbox for "Enable automatic IPv6 address assignment" is checked. Below are a dropdown for "Autoconfiguration Type" (set to "SLAAC + Stateless DHCP") and a field for "Router Advertisement Lifetime" (30 minutes).

Section 3 - Configuration

SLAAC+RDNSS to set computers on Router network obtained IPv6 address by RDNSS

Stateful DHCP to set computers on Router network obtained IPv6 address by Stateful DHCP, you need type the IPv6 Address Range (Start and End)

IPv6 Connection Type: **DS-Lite**

Choose **DS-Lite DHCPv6 Option**, If you choose **Manual Configuration**, need type the **AFTR IPv6 Address**.

Type **B4 IPv4 Address** (if necessarily)

Type **WAN IPv6 Address** and **IPv6 WAN Default Gateway**.

ADDRESS AUTOCONFIGURATION SETTINGS

Use this section to setup IPv6 Autoconfiguration to assign IP addresses to the computers on your network.

Enable automatic IPv6 address assignment :

Autoconfiguration Type : Stateful DHCP

IPv6 Address Range(Start) : ::0001

IPv6 Address Range(End) : ::0200

IPv6 Address Lifetime : 30 (minutes)

IPv6 CONNECTION TYPE

Choose the mode to be used by the router to the IPv6 Internet.

My IPv6 Connection is : DS-Lite

AFTR ADDRESS INTERNET CONNECTION TYPE

Enter the AFTR address information provided by your Internet Service Provider(ISP)..

DS-Lite Configuration : DS-Lite DHCPv6 Option Manual Configuration

AFTR IPv6 Address : 3ffe:501:ffff:300::1/64

B4 IPv4 Address : 192.0.0.2 (Optional)

WAN IPv6 Address : 3ffe:501:ffff:200::1/64

IPv6 WAN Default Gateway : 3ffe:501:ffff:500::1/64

USB SETUP

The DSL router comes with a **USB 2.0** interface which you can connect a USB printer, a USB storage device (e.g. USB disk / USB external Hard Disk) or a USB 3G modem.

To configure the USB Device on the router, click USB Setup in the SETUP tab. Router can be configured as a USB network file server when you plug-in a USB Storage device. Router can be configured as a USB Printer server when you plug- in a USB Printer device. Router can connect to Internet via 3G network when you plug-in a USB 3G USB Modem.

To access the **USB SETUP** setting window, click on the **USB SETUP** button in the **SETUP tab**

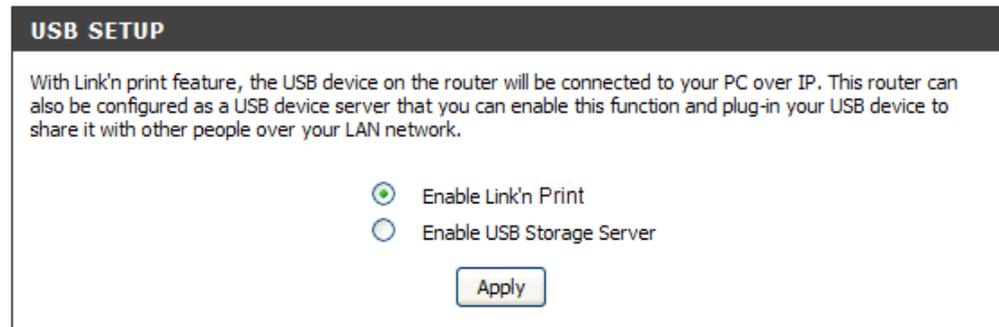
USB NETWORK PRINTER SERVER

D-Link Link'n Print allows you to share your USB printer as a network printer server to all the connected local hosts.

(Note: Link'n Print Printer Server is an USB printer server which requires users install a client utility in the computer before the user is able to send a print job to the router.)

To activate **USB Network Printer Server** feature, you have to tick **Enable Link'n Print Printer Server** in the USB Setup page and press **Apply** button,

Please refer to the Link'n Print Utility Manual which is shown as Appendix–F **D-Link Link'n Print** and as well install the client computer utility by using the install CD comes with this product package.



USB STORAGE FILE SERVER

USB Storage Server allows you to share your USB storage device to all the connected local hosts.

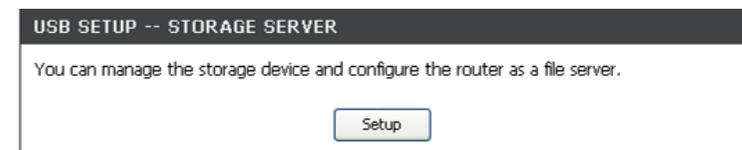
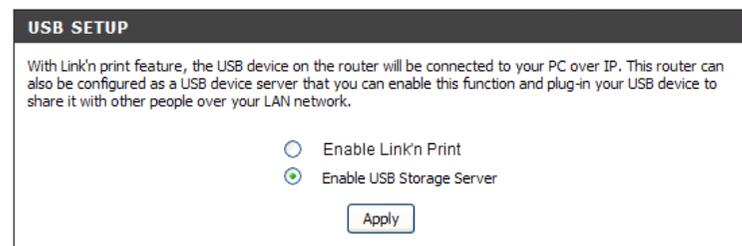
First connect your USB Storage device to the **USB** port. Then enter the data below.

To configure USB port to USB Storage server setting, choose **Enable USB Storage Server** in the USB Setup page and press **Apply** button,

To setup USB Storage Server, press **Setup** button in **STORAGE SETUP** window enter the server configuration page

USB DEVICE STATUS can check the USB Device Status and press **Status Refresh** button to refresh the status.

Press **Safely Remove Device** button to safely remove device.



Section 3 - Configuration

SAMBA FILE SERVER

Enable **SAMBA FILE SERVER** to configure USB Storage Device as a SAMBA File server.

Setup the **Server Name**, **Server Description** and **Group Name** of file server.

You can remote access when the **Remote Access** was hooked.

You can check **Add**, **Edit** and **Delete** the user in the **SAMBA FILE SERVER USER PROFILE**.

The screenshot shows the 'SAMBA FILE SERVER' configuration window. It has a title bar 'SAMBA FILE SERVER'. Below the title bar, there are several fields: 'Enable Samba File Server' with a checked checkbox, 'Server Name' with the text 'DSL-2880AL', 'Server Description' with the text 'File Server', 'Group Name' with the text 'WORKGROUP', and 'Remote Access' with an unchecked checkbox. At the bottom right, there are 'Apply' and 'Cancel' buttons.

FTP FILE SERVER

Enable **FTP SERVER** to configure USB Storage Device as a FTP file server.

Setup the **Port Name**, **Maximum connection**, and **Idle timeout** of FTP file server.

You can remote access when the **Remote Access** was hooked.

You can check **Add**, **Edit** and **Delete** the user in the **FTP SERVER USER PROFILE**.

The screenshot shows the 'SAMBA FILE SERVER USER PROFILE' window. It contains a table with the following data:

Enable	Username	Access Mode	Connected Device	Path
<input type="checkbox"/>	anonymous	Full-access	JetFlash(TS1GJF150), Volume 1	/

Below the table, there are 'Add', 'Edit', and 'Delete' buttons.

The screenshot shows the 'FTP FILE SERVER' configuration window. It has a title bar 'FTP FILE SERVER'. Below the title bar, there are several fields: 'Enable FTP Server' with a checked checkbox, 'Port Number' with the text '21', 'Maximum connections' with the text '10', 'Idle timeout' with the text '10 min. (0 for no timeout)', and 'Remote Access' with an unchecked checkbox. At the bottom right, there are 'Apply' and 'Cancel' buttons.

The screenshot shows the 'FTP SERVER USER PROFILE' window. It contains a table with the following data:

Enable	User ID	Access Mode	Connected Device	Path
<input type="checkbox"/>	anonymous	Read-only	JetFlash(TS1GJF150), Volume 1	/

Below the table, there are 'Add', 'Edit', and 'Delete' buttons.

Section 3 - Configuration

WEB FILE SERVER

Tick **Enable Web Server** to configure USB Storage Device as a web based file server.

Click the **Browse** to choose a folder for **Path**, and type **Port Number** of WEB file server.

You can remote access when the **Remote Access** was hooked.

The screenshot shows the 'WEB FILE SERVER' configuration window. It has a title bar 'WEB FILE SERVER'. Inside, there are several fields: 'Enable Web Server' with a checked checkbox, 'Volume' set to 'JetFlash(TS1GJF150)', a dropdown menu showing '1. FAT32', 'Path' with a text box containing '/' and a 'Browse' button, 'Port Number' with a text box containing '8000', and 'Remote Access' with an unchecked checkbox. At the bottom are 'Apply' and 'Cancel' buttons.

3G USB MODEM SETUP

Click **Setup** button in **3G USB MODEM SETUP** window to configure 3G USB MODEM

The screenshot shows the '3G USB MODEM SETUP' window. It has a title bar '3G USB MODEM SETUP'. The main content area contains the text: 'You can configure 3G USB Modem via USB port. And your device would be able to connect to Internet via 3G USB Modem.' At the bottom center is a 'Setup' button.

Enable the Enable 3G USB Modem

Type the **PIN Code**, **Telephone Number** (known the dial up phone number) and **APN**, which provide by your 3G ISP.

The screenshot shows the '3G USB MODEM SETTING' window. On the left is a navigation menu with items: 'Internet Setup', 'Wireless Setup', 'LAN Setup', 'Time and Date', 'IPv6 Setup', 'USB Setup', 'Logout', and 'Internet Online'. Below the menu are 'English' and 'Reboot' buttons. The main content area has a title bar '3G USB MODEM SETTING'. It contains the text: 'Please ensure the 3G USB Modem has been plugged into USB port firstly and continue to setup as below. Once Setting saved, please go to Internet setup to setup the priority of Internet connection.' Below this are fields: 'Enable 3G USB Modem' with a checked checkbox, 'PIN Code' with a text box containing '0000', 'Telephone Number' with a text box containing '*99#', and 'APN' with a text box containing 'internet'. At the bottom are 'Apply' and 'Cancel' buttons.

ADVANCED

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.

PORT FORWARDING

Use the **PORT FORWARDING** window to open ports in your router and re-direct data through those ports to a single PC on your network (WAN-to-LAN traffic). The Port Forwarding function allows remote users to access services on your LAN such as FTP for file transfers or SMTP and POP3 for e-mail. The DSL-2880AL will accept remote requests for these services at your Global IP Address, using the specified TCP or UDP protocol and port number, and then redirect these requests to the server on your LAN with the LAN IP address you specify. Remember that the specified Private IP Address must be within the useable range of the subnet occupied by the Router.

To access the **PORT FORWARDING** settings window, click on the **PORT FORWARDING** button in the **ADVANCED** tab

PORT FORWARDING RULES CONFIGURATION

Select an application type, e.g. FTP, from the **Application Name** drop-down menu for a pre-defined application to speed up configuration or type an application name manually in the **Name** input box in order to define your own application.

Select a name from the **Computer Name** drop-down menu or type an IP address in the **IP address** input box to appoint the PC to receive the forwarded packets.

The **External Port** shows the ports opened for remote users in the WAN side of the router. The **TCP/UDP** means the protocol type of the opened ports.

The **Internal Port** shows the ports opened in the PC with the appointed **IP Address**. The **TCP/UDP** means the protocol type of the opened ports.

- Port Forwarding
- Application Rules
- QoS Setup
- Outbound Filter
- Inbound Filter
- Wireless Filter
- DNS Setup
- Firewall & DMZ
- Advanced Internet
- Advanced Wireless
- Advanced LAN
- Port Mapping
- SNMP Setup
- Remote Management
- Routing Setup
- TR-069 Client
- Wi-Fi Protected Setup
- IPv6 Firewall
- IPv6 Routing
- Budget Quota
- Logout

PORT FORWARDING

This is the ability to open ports in your router and re-direct data through those ports to a single PC on your network.

PORT FORWARDING RULES CONFIGURATION

Remaining number of rules that can be created: 47

		External Port	Internal Port
Name	<< FTP	TCP 20-21	TCP 20-21
IP Address	<< 1421	UDP	UDP
Use Interface:		wizard_pvc_1/ppp0	

ACTIVE PORT FORWARDING RULES

Name	Address	External Port	Internal Port	Protocol	WAN Interface	Edit	Remove
Skype UDP at 192.168.1.2:8672 (2318)	192.168.1.2	8672	8672	UDP	ppp0	Edit	<input type="checkbox"/>
Skype TCP at 192.168.1.2:8672 (2318)	192.168.1.2	8672	8672	TCP	ppp0	Edit	<input type="checkbox"/>

APPLICATION RULES CONFIGURATION

Some applications such as games, video conferencing and remote access applications require specific ports on the Router's firewall to be opened for the applications to pass through.

To access **APPLICATION RULES** setting windows, click on the **APPLICATION RULES** button in the **ADVANCED** tab

APPLICATION RULES

Select a name from the **Application Name** drop-down menu for a pre-configured application or type a name in the **Name** input box to define your own application.

It will appear the Trigger and Firewall ports after you choose the application name by the drop-down menu.

Choose the Use Interface and click the **Add/Apply** button to save the configuration, and then it will be added in the list.

APPLICATION RULES

This option is used to pre-configure single or multiple trigger ports on your router that will automatically activate when the router senses data sent to the Internet from one of these applications.

APPLICATION RULES CONFIGURATION

Remaining number of rules that can be created: 12

Name	Trigger	Port	Traffic Type
MSN Messenger	<< MSN Messenger	1863,5190,689	Both
Use Interface:	PPPoE_0_33_1/ppp1	Firewall 1863,5190,689	Both

Apply

ACTIVE APPLICATION RULES

Remove Selected

Name	Trigger Port	Traffic Type	Firewall Port	Traffic Type	WAN Interface	Edit	Remove
MSN Messenger	1863	TCP or UDP	1863	TCP or UDP	ppp0	Edit	<input type="checkbox"/>
MSN Messenger	5190	TCP or UDP	5190	TCP or UDP	ppp0	Edit	<input type="checkbox"/>
MSN Messenger	6891	TCP or UDP	6891	TCP or UDP	ppp0	Edit	<input type="checkbox"/>
MSN Messenger	6901	TCP or UDP	6901	TCP or UDP	ppp0	Edit	<input type="checkbox"/>

QOS SETUP

Quality of Service Setup can be used to improve data flow for different applications by prioritizing the network traffic based on selected criteria.

To access the **QOS SETUP** settings window, click on the **QOS SETUP** button in the **ADVANCED** tab

QOS SETUP

You have to define the service ports. For example,

VoIP(RTP) is from 700(**Start Port**) to 900(**End Port**)

H.323 is 1720

FTP is from 20(**Start Port**) to 21(**End Port**)

MSN messenger is from 1863(**Start Port**) to 1864(**End Port**)

WIRELESS QOS SETUP

You can choose **Enable** or **Disable** to decide if the data has the WMM on the **WMM(Wi-Fi Multimedia)**

WMM No Acknowledge means that the receiver doesn't have to send back the Acknowledge packet.

ADVANCED QoS Setup

Click the **Wireless QoS** button to set wireless data priority.

Click the **LAN QoS** button to set Ethernet data priority.

The screenshot shows the configuration interface for QoS Setup. On the left is a sidebar with a list of menu items: Port Forwarding, Application Rules, QoS Setup (highlighted), Outbound Filter, Inbound Filter, Wireless Filter, DNS Setup, Firewall & DMZ, Advanced Internet, Advanced Wireless, Advanced LAN, Port Mapping, SNMP Setup, Remote Management, Routing Setup, TR-069 Client, Wi-Fi Protected Setup, IPv6 Firewall, IPv6 Routing, Budget Quota, Logout, and Internet Online. The main content area is divided into three sections:

- QOS SETUP:** Contains a header with the title and a descriptive paragraph. Below it are several rows of settings, each with a checkbox and two input fields for Start Port and End Port:
 - VOIP(RTP) : Start Port [] End Port []
 - H.323 : Start Port [] End Port []
 - FTP : Start Port [] End Port []
 - MSN messenger : Start Port [] End Port []
 - IPSEC(VPN Passthrough) :
 - RTSP(Video Streaming) :
 - MMS :
 A "Save Settings" button is located at the bottom of this section.
- WIRELESS QOS SETUP:** Contains two settings:
 - WMM(Wi-Fi Multimedia): Enabled (dropdown menu)
 - WMM No Acknowledgement: Disabled (dropdown menu)
 An "Apply WMM Settings" button is at the bottom.
- ADVANCED QOS SETUP:** Contains two buttons: "Wireless QoS" and "LAN QoS".

WIRELESS QOS RULES CONFIGURATION

Type the policy name on the **Name**, set the priority value on the **Priority**.

Select the **Protocol**, ANY, ICMP, TCP and UDP.

Set the **Source IP Range** and the **Destination IP Range**.

Set the **Source Port Range** and the **Destination Port Range**.

Click the **Add/Apply** button to add the policy to the list.

LAN QOS RULES CONFIGURATION

Type the policy name on the **Name**, set the priority value on the **Priority**

Select the **Protocol**, ANY, ICMP, TCP and UDP.

Set the **Source IP Range** and the **Destination IP Range**.

Set the **Source Port Range** and the **Destination Port Range**.

Click the **Add/Apply** button to add the policy to the list

WIRELESS QOS RULES CONFIGURATION

Remaining number of rules that can be created: 16

Name <input type="text"/>	Priority <input type="text"/> (1..7)	Protocol <input type="text"/> << Select Protocol ▼
Source IP Range <input type="text"/> to <input type="text"/>	Source Port Range <input type="text"/> to <input type="text"/>	
Destination IP Range <input type="text"/> to <input type="text"/>	Destination Port Range <input type="text"/> to <input type="text"/>	

ACTIVE WIRELESS QOS RULES

Name	Priority	Protocol	Src. IP Range	Src. Port	Dest. IP Range	Dest. Port	Remove

LAN QOS RULES CONFIGURATION

Remaining number of rules that can be created: 16

Name <input type="text"/>	Priority <input type="text"/> (1..7)	Protocol <input type="text"/> << Select Protocol ▼
Source IP Range <input type="text"/> to <input type="text"/>	Source Port Range <input type="text"/> to <input type="text"/>	
Destination IP Range <input type="text"/> to <input type="text"/>	Destination Port Range <input type="text"/> to <input type="text"/>	

ACTIVE LAN QOS RULES

Name	Priority	Protocol	Src. IP Range	Src. Port	Dest. IP Range	Dest. Port	Remove

OUTBOUND FILTER

By default, all outgoing IP traffic from the LAN is not restricted. The Outbound Filter allows you to create a filter rule to block outgoing IP traffic by specifying a 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.

To access the **OUTBOUND FILTER** settings window, click on the **OUTBOUND FILTER** button in the **ADVANCED tab**

ADD OUTBOUND IP FILTER

To create the new policy and fill in the **filter name**.

Choose ICMP, TCP/UDP, TCP or UDP on the **Protocol**.

Type **Source IP address**, **Source Subnet Mask** and **Source Port** (can be single port or port range in “start port::end port” syntax)

Type **Destination IP address**, **Destination Subnet Mask** and **Destination Port** (can be single port or port range in “start port::end port” syntax)

Set the policy schedule on the Schedule, Always or never, or **View Available Schedules**

Please click **Add/Apply** button to add the policy in the list.

The screenshot shows the 'OUTBOUND IP FILTER' configuration page. On the left is a sidebar menu with options like Port Forwarding, Application Rules, QoS Setup, Outbound Filter (selected), Inbound Filter, Wireless Filter, DNS Setup, Firewall & DMZ, Advanced Internet, Advanced Wireless, Advanced LAN, Port Mapping, SNMP Setup, Remote Management, Routing Setup, TR-069 Client, Wi-Fi Protected Setup, IPv6 Firewall, IPv6 Routing, Budget Quota, and Logout. The main content area has an orange header 'OUTBOUND IP FILTER' with a note: 'By default, all outgoing IP traffic from the LAN is allowed. The Outbound Filter allows you to create a filter rule to block outgoing IP traffic by specifying a 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.' Below this is the 'ADD OUTBOUND IP FILTER' section with fields for Filter Name, IP Version (IPv4), 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), and Schedule (Always). An 'Apply' button is at the bottom. Below that is the 'ACTIVE OUTBOUND IP FILTER' section with a table header: Name, Protocol, Src. Addr./Mask, Src. Port, Dest. Addr./Mask, Dest. Port, Schedule, Remove. A 'Remove Selected' button is at the bottom of the table.

INBOUND FILTER

Remark: Inbound filter feature MUST work in conjunction with firewall feature.

In order to use the inbound filter feature, you will have to create the filter policy reflecting to application scenario. Only the packet which can satisfy the filter policy will be able to pass through the inbound filter without being blocked.

WAN to LAN Access – Inbound filter restricts WAN side remote nodes to access the device itself or any node located within the device LAN side. It is commonly used to prevent unsecure remote access – a typical example is to employ an inbound filter to allow a trusted WAN side remote peer to access LAN side file sharing resources like FTP service. The inbound filter feature over this device will behave as a *white list filter*. Unless the incoming packet can satisfy the filter policy, any other incoming IP traffic that does not originate from the internal network will be blocked by the firewall.

LAN to WAN Internet Access – Inbound filter will not block WAN to LAN traffic which is initiated from LAN side internet applications, e.g. web browsing, sending/receiving email and file transferring.

To access the **INBOUND FILTER** settings window, click on the **INBOUND FILTER** button in the **ADVANCED** tab

Section 3 - Configuration

ADD INBOUND IP FILTER

To create the new policy and fill in the **filter name**.

To pick up ICMP, TCP/UDP, TCP or UDP from **Protocol**.

To type in **Source IP address**, **Source Subnet Mask** and **Source Port** (can be single port or port range in “start port::end port” syntax)

Type **Destination IP address**, **Destination Subnet Mask** and **Destination Port** (can be single port or port range in “start port::end port” syntax)

Set the policy schedule on the Schedule, Always or never, or **View Available Schedules**

Please click **Add/Apply** button to add the policy in the list.

The screenshot displays the configuration interface for the D-Link DSL-2880AL. On the left is a vertical navigation menu with the following items: Port Forwarding, Application Rules, QoS Setup, Outbound Filter, Inbound Filter (highlighted), Wireless Filter, DNS Setup, Firewall & DMZ, Advanced Internet, Advanced Wireless, Advanced LAN, Port Mapping, SNMP Setup, Remote Management, Routing Setup, TR-069 Client, Wi-Fi Protected Setup, IPv6 Firewall, IPv6 Routing, Budget Quota, Logout, Internet Online, English (dropdown), and Reboot.

The main content area is titled 'INBOUND IP FILTER' and contains a note: 'Note: This section only applies when the Firewall is enabled.' Below the note, a paragraph explains: 'By default, all incoming IP traffic that does not originate from the internal network is blocked when the firewall is enabled. Normal outgoing Internet requests created by web browsing, email and other software you run will work as usual as the requests originate from inside your internal network.' Another paragraph states: '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 below. All of the specified conditions in this filter rule must be satisfied for the rule to take effect.'

The 'ADD INBOUND IP FILTER' form includes the following fields:

- Filter Name:
- Use Interface: PPPoE_1_32_1/ppp0 (dropdown)
- IP Version: IPv4 (dropdown)
- Protocol: (dropdown)
- Source IP address:
- Source Subnet Mask:
- Source Port (port or port:port):
- Destination IP address:
- Destination Subnet Mask:
- Destination Port (port or port:port):
- Schedule: Always (dropdown) with a link to [View Available Schedules](#)

An 'Apply' button is located at the bottom of the form.

Below the form is the 'ACTIVE INBOUND IP FILTER' section, which contains a table with the following columns: Name, WAN Interface, Protocol, Src.Addr./Mask, Src.Port, Dest.Addr./Mask, Dest.Port, Schedule, and Remove. A 'Remove Selected' button is positioned below the table.

WIRELESS FILTER

This feature can let you add a policy to deny or allow WLAN devices connected to the router

To access the **WIRELESS FILTER** settings window, click on the **WIRELESS FILTER** button in the **ADVANCED** tab

WIRELESS FILTER POLICY

You can choose the Disable/ Allow All/ Deny All of **Wireless Filter Policy**.
 Disable: You don't want to launch the feature.

Allow All: Support WLAN devices make connection, except the mac address which is added in the filter table.

Deny All: Support deny all WLAN devices make connection, except the mac address which is added in the filter table.

WIRELESS FILTER

Type filter name on the **FILTER NAME**
 Type wireless MAC address on the **Wireless MAC Address**

WIRELESS FILTER - MAXIMUM 32 ENTRIES CAN BE ADDED.

Please click the Add/Apply button to add the policy in the list.

DNS SETUP

The DNS feature is designed for resolving the DNS host name into IPs. Unless you want the router query the specific DNS servers; otherwise, you can leave the setting as obtain DNS server address automatically.

The Dynamic DNS feature allows you to host a server (Web, FTP, Game Server, etc...) using a domain name that you have purchased (for example: www.whateveryournameis.com) with your dynamically assigned IP address. Most broadband Internet Service Providers assign dynamic (changing) IP addresses. Using a DDNS service provider, your friends can enter your host name to connect to your game server and your friends don't mind what your IP address is, and then just type the DDNS name to reach. You can subscribe the free D-Link DDNS service from <https://www.dlinkddns.com>.

To access the **DNS** setting window, click on the **DNS** button under the **ADVANCED** tab.

DNS SERVER CONFIGURATION

If you are using the Router for DHCP service on the LAN and are using DNS servers on the ISP's network, check **Obtain DNS server address automatically** box.

If you have DNS IP addresses provided by your ISP, enter these IP addresses in the available entry fields for the **Primary DNS Server** and the **Secondary DNS Server**.

If IPv6 Internet connection service was enabled, you can check **obtain IPv6 DNS server address automatically** box. Or you can enter **Primary IPv6 DNS Server** and the **Secondary IPv6 DNS Server**.

Port Forwarding	<div style="background-color: #f4a460; padding: 5px;">DNS SETUP</div> <p>The Dynamic DNS feature allows you to host a server (Web, FTP, Game Server, etc...) using a domain name that you have purchased (www.whateveryournameis.com) with your dynamically assigned IP address. Most broadband Internet Service Providers assign dynamic (changing) IP addresses. Using a DDNS service provider, your friends can enter your host name to connect to our game server no matter what your IP address is.</p> <p>Sign up for D-Link's Free DDNS service at www.DLinkDDNS.com.</p>
Application Rules	
QoS Setup	
Outbound Filter	
Inbound Filter	
Wireless Filter	
DNS Setup	
Firewall & DMZ	
Advanced Internet	
Advanced Wireless	
Advanced LAN	
Port Mapping	
SNMP Setup	
Remote Management	
Routing Setup	
TR-069 Client	<div style="background-color: #333; color: white; padding: 5px;">DNS SERVER CONFIGURATION</div> <p> <input checked="" type="radio"/> Obtain DNS server address automatically <input type="radio"/> Use the following DNS server addresses </p> <p> Preferred DNS server : <input type="text"/> Alternate DNS server : <input type="text"/> </p> <p> <input checked="" type="radio"/> Obtain IPv6 DNS server address automatically <input type="radio"/> Use the following Static IPv6 DNS server addresses </p> <p> Preferred IPv6 DNS server : <input type="text"/> Alternate IPv6 DNS server : <input type="text"/> </p>

DDNS CONFIGURATION

Please enable the **Enable Dynamic DNS** if you want to use DDNS.

Choose which DDNS web site to use on the **Server Address**.

Type which Host name which you registered with your DDNS service provider. on the **Host Name**.

Please choose which interface name to use on the **Interface**.

Type the username/password on the **username/password** for your DDNS account.

After configure the DNS settings as desired, click on the **Apply Setting** button to apply settings.

The screenshot shows a web interface titled "DDNS CONFIGURATION". It contains the following fields and controls:

- Enable Dynamic DNS :** A checkbox that is checked.
- Server Address :** A dropdown menu with "dlinkddns.com(Free)" selected.
- Host Name :** A text input field containing "DLink.domain.com".
- Interface :** A dropdown menu with "PPPoE_0_42_1/ppp0" selected.
- Username :** A text input field containing "DLink".
- Password :** A text input field with five dots representing a masked password.
- At the bottom right, there are two buttons: "Apply" and "Cancel".

FIREWALL & DMZ

The router already provides a simple firewall by virtue of the way NAT works. By default NAT does not respond to unsolicited incoming requests on any port, thereby making your WAN invisible to Internet cyber attackers.

DMZ means 'De Militarized Zone'. DMZ allows computers behind the router firewall to be accessible to Internet traffic. Typically, your DMZ would contain Web servers, FTP servers, and others.

To access the **Firewall & DMZ** setting window, click on the **Firewall & DMZ** button under the **ADVANCED** tab

Firewall SETTING

Check the **Enable SPI** box

Check the **Enable DOS and Portscan Protection** box, you can Choose the below attack firewall setting:

SYN attack,
FIN/URG/PSH attack,
Ping attack,
Xmas Tree attack,
TCP reset attack,
Null scanning attack,
Ping of Death attack,
SYN/RST SYN/FIN attack.

Port Forwarding
Application Rules
QoS Setup
Outbound Filter
Inbound Filter
Wireless Filter
DNS Setup
Firewall & DMZ
Advanced Internet
Advanced Wireless
Advanced LAN
Port Mapping
SNMP Setup
Remote Management
Routing Setup

FIREWALL & DMZ

The router already provides a simple firewall by virtue of the way NAT works. By default NAT does not respond to unsolicited incoming requests on any port, thereby making your LAN invisible to Internet cyber attackers.

DMZ means 'Demilitarised Zone'. DMZ allows computers behind the router firewall to be accessible to Internet traffic. Typically, your DMZ would contain Web servers, FTP servers, and others.

FIREWALL SETTINGS

Enable SPI :

Enable DOS and Portscan Protection :

SYN attack :

FIN/URG/PSH attack :

Ping attack :

Xmas Tree attack :

TCP reset attack :

Null scanning attack :

Ping of Death attack :

SYN/RST SYN/FIN attack :

DMZ Setting

Please tick the **Enable DMZ** and type the DMZ computer IP on the **DMZ IP Address** or you also can choose the DMZ host from the drop-down menu instead of type in IP manually.

Application Level Gateway (ALG) Configuration

Please choose the following ALG to enable:

- PPTP (VPN Passthrough)
- IPSec (VPN Passthrough)
- RTSP(Online Video Streaming)
- Windows/MSN Messenger
- FTP
- H.323(Video Conferencing)
- SIP
- Wake-On-LAN
- MMS

DMZ SETTING

The DMZ (Demilitarized Zone) option lets you set a single computer on your network outside of the router. If you have a computer that cannot run Internet applications successfully from behind the router, then you can place the computer into the DMZ for unrestricted Internet access.

Note: Putting a computer in the DMZ may expose that computer to a variety of security risks. Use of this option is only recommended as a last resort.

Enable DMZ :

DMZ IP Address :



Computer Name



APPLICATION LEVEL GATEWAY (ALG) CONFIGURATION

PPTP :

IPSec (VPN Passthrough) :

RTSP (Online Video Streaming) :

Windows/MSN Messenger :

FTP :

H.323(Video Conferencing) :

SIP :

Wake-On-LAN :

MMS :

ADVANCED INTERNET

The Multiple PVC Settings allow you to Add (up to 8 PVC in total), Delete or Edit multiple PVCs connection for advanced ADSL service.

The Advanced ADSL settings allow you to choose which ADSL modulation settings your modem router will support. D-Link does not recommend you to change these settings unless directed to do so by your ISP.

To access the **ADVANCED INTERNET** setting window, click on the **ADVANCED INTERNET** button under the **ADVANCED** tab

Section 3 - Configuration

Multiple PVC Settings

Please click the **Add / delete** button to add / delete the multiple PVC. And the following step same as pre internet setup.

Advanced ADSL Settings

Please select following ADSL profile to link.

G.Dmt, G.lite, T1.413, ADSL2, AnnexL, ADSL2+, Annex M (available only on Annex A model)

Please choose the **Inner pair** or **Outer pair** on the Select the phone line pair below.

Please select to enable **Bitswap** and **SRA** on the Capability.

The screenshot displays the configuration interface for the D-Link DSL-2880AL. On the left is a navigation menu with the following items: Port Forwarding, Application Rules, QoS Setup, Outbound Filter, Inbound Filter, Wireless Filter, DNS Setup, Firewall & DMZ, Advanced Internet (highlighted), Advanced Wireless, Advanced LAN, Port Mapping, SNMP Setup, Parental Control, Routing Setup, TR-069 Client, Wi-Fi Protected Setup, IPv6 Firewall, IPv6 Routing, Budget Quota, Logout, Internet Online, English (dropdown), and Reboot.

The main content area is divided into three sections:

- ADVANCED ADSL**: Contains introductory text stating that Multiple PVC Settings allow adding, deleting, or editing PVC connections, and that Advanced ADSL settings allow choosing modulation settings. A note from D-Link advises against changing these settings unless directed by an ISP.
- MULTIPLE PVC SETTINGS**: Features a table with columns for VPI/VCI, Description, Protocol, IGMP, Nat, State, Edit, and Action. Two entries are shown: 'wizard_pvc_1' (VPI/VCI 0/42) and 'ppp7_usb35g_0' (VPI/VCI N/A). Below the table are 'Add' and 'Delete' buttons.
- ADVANCED ADSL SETTINGS**: Lists various ADSL profiles with checkboxes, all of which are checked: G.Dmt Enabled, G.lite Enabled, T1.413 Enabled, ADSL2 Enabled, AnnexL Enabled, ADSL2+ Enabled, and AnnexM Enabled. Below this, it asks to 'Select the phone line pair below:' with radio buttons for 'Inner pair' (selected) and 'Outer pair'. Finally, it lists 'Capability' options: 'Bitswap Enable' (checked) and 'SRA Enable' (unchecked).

ADVANCED WIRELESS

These options are for users that wish to change the behavior of their wireless radio from the standard setting. D-Link does not recommend changing these settings from the factory default. Incorrect settings may impair the performance of your wireless radio. The default settings should provide the best wireless radio performance in most environments.

To access the **Advanced Wireless** setting window, click on the **Advanced Wireless** button in the **ADVANCED tab**

Advanced WIRELESS Settings

If you need to change the default behavior,

Please type the value on the **Fragmentation Threshold**

Please type the value on the **RTS Threshold**

Please type the value on the **DTIM Interval**

Please type the value on the **Beacon Interval**

Please choose 20%, 40%, 60%, 80% and 100% on the **Transmit Power**.

Port Forwarding	<div style="background-color: #f4a460; padding: 5px; font-weight: bold;">ADVANCE WIRELESS</div> <p style="font-size: small; margin-top: 5px;">These options are for users that wish to change the behaviour of their 802.11g wireless radio from the standard setting. D-Link does not recommend changing these settings from the factory default. Incorrect settings may impair the performance of your wireless radio. The default settings should provide the best wireless radio performance in most environments.</p> <div style="background-color: #333; color: white; padding: 2px; margin-top: 10px;">2.4GHZ ADVANCE WIRELESS SETTINGS</div> <table style="width: 100%; margin-top: 5px;"> <tr> <td style="text-align: right;">Wireless Band :</td> <td colspan="2">2.4GHz Band</td> </tr> <tr> <td style="text-align: right;">Fragmentation Threshold :</td> <td><input type="text" value="2346"/></td> <td>(256..2346)</td> </tr> <tr> <td style="text-align: right;">RTS Threshold :</td> <td><input type="text" value="2347"/></td> <td>(0..2347)</td> </tr> <tr> <td style="text-align: right;">DTIM Interval :</td> <td><input type="text" value="1"/></td> <td>(1..255)</td> </tr> <tr> <td style="text-align: right;">Beacon Interval :</td> <td><input type="text" value="100"/></td> <td>(20..1000)</td> </tr> <tr> <td style="text-align: right;">Transmit Power :</td> <td colspan="2"><input type="button" value="100%"/></td> </tr> </table> <div style="background-color: #333; color: white; padding: 2px; margin-top: 10px;">5GHZ ADVANCE WIRELESS SETTINGS</div> <table style="width: 100%; margin-top: 5px;"> <tr> <td style="text-align: right;">Wireless Band :</td> <td colspan="2">5GHz Band</td> </tr> <tr> <td style="text-align: right;">Fragmentation Threshold :</td> <td><input type="text" value="2346"/></td> <td>(256..2346)</td> </tr> <tr> <td style="text-align: right;">RTS Threshold :</td> <td><input type="text" value="2347"/></td> <td>(0..2347)</td> </tr> <tr> <td style="text-align: right;">DTIM Interval :</td> <td><input type="text" value="1"/></td> <td>(1..255)</td> </tr> <tr> <td style="text-align: right;">Beacon Interval :</td> <td><input type="text" value="100"/></td> <td>(20..1000)</td> </tr> <tr> <td style="text-align: right;">Transmit Power :</td> <td colspan="2"><input type="button" value="100%"/></td> </tr> </table>	Wireless Band :	2.4GHz Band		Fragmentation Threshold :	<input type="text" value="2346"/>	(256..2346)	RTS Threshold :	<input type="text" value="2347"/>	(0..2347)	DTIM Interval :	<input type="text" value="1"/>	(1..255)	Beacon Interval :	<input type="text" value="100"/>	(20..1000)	Transmit Power :	<input type="button" value="100%"/>		Wireless Band :	5GHz Band		Fragmentation Threshold :	<input type="text" value="2346"/>	(256..2346)	RTS Threshold :	<input type="text" value="2347"/>	(0..2347)	DTIM Interval :	<input type="text" value="1"/>	(1..255)	Beacon Interval :	<input type="text" value="100"/>	(20..1000)	Transmit Power :	<input type="button" value="100%"/>	
Wireless Band :		2.4GHz Band																																			
Fragmentation Threshold :		<input type="text" value="2346"/>	(256..2346)																																		
RTS Threshold :		<input type="text" value="2347"/>	(0..2347)																																		
DTIM Interval :		<input type="text" value="1"/>	(1..255)																																		
Beacon Interval :		<input type="text" value="100"/>	(20..1000)																																		
Transmit Power :		<input type="button" value="100%"/>																																			
Wireless Band :		5GHz Band																																			
Fragmentation Threshold :		<input type="text" value="2346"/>	(256..2346)																																		
RTS Threshold :		<input type="text" value="2347"/>	(0..2347)																																		
DTIM Interval :		<input type="text" value="1"/>	(1..255)																																		
Beacon Interval :		<input type="text" value="100"/>	(20..1000)																																		
Transmit Power :		<input type="button" value="100%"/>																																			
Application Rules																																					
QoS Setup																																					
Outbound Filter																																					
Inbound Filter																																					
Wireless Filter																																					
DNS Setup																																					
Firewall & DMZ																																					
Advanced Internet																																					
Advanced Wireless																																					
Advanced LAN																																					
Port Mapping																																					
SNMP Setup																																					
Parental Control																																					
Routing Setup																																					
TR-069 Client																																					
Wi-Fi Protected Setup																																					
IPv6 Firewall																																					
IPv6 Routing																																					

GUEST WIRELESS SETTING

Guest wireless domain, only available on 2.4GHz interface, is an isolated zone from device LAN and main SSID domain.

Please enable the **Enable Wireless Guest Network**

Type SSID on the **Wireless Network Name**

Please choose **Visible** or **Invisible** on the **Visibility Status**

Please select **Off/On** on the **AP Isolation**.

GUEST WIRELESS SECURITY

By default guest wireless domain is not applied with any security. To offer security mechanism, please select the encryption methodology and input pre-share key.

GUEST WIRELESS SETTINGS(2.4GHZ)

Enable Wireless Guest Network :

Wireless Network Name (SSID) :

Visibility Status : Visible Invisible

AP Isolation :

2.4GHZ WIRELESS SECURITY MODE

To protect your privacy you can configure wireless security features. This device supports three wireless security modes including: WEP, WPA, WPA2 and Auto.

The **WEP** mode is the original wireless encryption standard. WPA provides a higher level of security.

For maximum compatibility, use **WPA**. This mode uses TKIP cipher. Some gaming and legacy devices work only in this mode. For best security, use **WPA2** mode. This mode uses AES (CCMP) cipher and legacy stations are not allowed access with WPA security. For maximum compatibility, use **Auto (WPA or WPA2)** mode to achieve a balance of strong security and best compatibility. This mode uses WPA for legacy clients while maintaining higher security with stations that are WPA2 capable. Also the strongest cipher that the client supports will be used.

To achieve better wireless performance use **WPA2** security mode (or in other words AES cipher).

Security Mode :

ADVANCED LAN

These options are for users that wish to change the LAN settings. D-Link does not recommend changing these settings from factory default. Changing these settings may affect the behavior of your network.

To access the **Advanced LAN** setting window, click on the **Advanced LAN** button in the **ADVANCED tab**

UPnP

Please select the **Enable UPnP** when you want to have Universal Plug and Play (UPnP) supports peer-to-peer Plug and Play functionality for network devices.

Block ICMP Ping

Enable the WAN Ping Respond on the **Enable WAN Ping Respond**. Please select **Allow All** or **Deny All** on the WAN Ping Inbound Filter and you can also type a string on the **Details** to describe the action.

Multicast Streams

Please enable the **Enable Multicast Streams (IGMP)** to let IGMP stream can pass through DSL-2880AL.

Port Forwarding	ADVANCED LAN
Application Rules	These options are for users that wish to change the LAN settings. D-Link does not recommend changing these settings from factory default. Changing these settings may affect the behaviour of your network.
QoS Setup	UPnP
Outbound Filter	Universal Plug and Play(UPnP) supports peer-to-peer Plug and Play functionality for network devices. Enable UPnP : <input checked="" type="checkbox"/>
Inbound Filter	BLOCK ICMP PING
Wireless Filter	If you enable this feature, the Internet port of your router will respond to ping requests from the Internet that are directed to your ISP assigned public IP address. Enable WAN Ping Respond : <input type="checkbox"/> WAN Ping Inbound Filter : Allow All ▾ Details : <input type="text"/>
DNS Setup	MULTICAST STREAMS
Firewall & DMZ	Enable Multicast Streams (IGMP) : <input checked="" type="checkbox"/>
Advanced Internet	<input type="button" value="Apply"/> <input type="button" value="Cancel"/>
Advanced Wireless	
Advanced LAN	
Port Mapping	
SNMP Setup	
Remote Management	
Routing Setup	
TR-069 Client	
Wi-Fi Protected Setup	
IPv6 Firewall	
IPv6 Routing	
Budget Quota	
Logout	

PORT MAPPING

Port Mapping 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 if Remove is checked. Only the default group has IP interface.

To access the **Port Mapping** setting window, click on the **Port Mapping** button in the **ADVANCED** tab

PORT MAPPING

Click **Add** button to add Port Mapping rule.

- Port Forwarding
- Application Rules
- QoS Setup
- Outbound Filter
- Inbound Filter
- Wireless Filter
- DNS Setup
- Firewall & DMZ
- Advanced Internet
- Advanced Wireless
- Advanced LAN
- Port Mapping
- SNMP Setup
- Remote Management
- Routing Setup
- TR-069 Client
- Wi-Fi Protected Setup
- IPv6 Firewall
- IPv6 Routing
- Budget Quota
- Logout

PORT MAPPING SETTINGS

This section is used to configure the port mapping to support VLAN.

Port Mapping 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 if Remove is checked. Only the default group has IP interface.

PORT MAPPING

Group Name	Interfaces	Remove	Edit
Default	LAN4,LAN3,LAN2,LAN1,WAN,wireless,ppp0,ppp1		

Add
Delete

PORT MAPPING CONFIGURATION

Type **Group Name** and select **WAN Interface** used in the grouping in drop-down menu

Choose **Grouped LAN Interface** from **Available LAN Interfaces**.

Type DHCP vendor IDs in the **Automatically Add Clients With the following DHCP Vendor IDs** for auto add clients.

Click on the **Apply** Button to save the setting.

The screenshot shows the 'PORT MAPPING CONFIGURATION' web interface. At the top, there is a header bar with the title 'PORT MAPPING CONFIGURATION'. Below the header, the 'Group Name' field contains the text 'DATA'. The 'WAN Interface used in the grouping' dropdown menu is set to 'PPPoE_0_42_1/ppp0'. There are two list boxes: 'Grouped LAN Interfaces' on the left, containing 'lan1', 'lan4', and 'wireless'; and 'Available LAN Interfaces' on the right, containing 'lan2' and 'lan3'. Between these two list boxes are two buttons: a right-pointing arrow ('->') and a left-pointing arrow ('<-'). Below these list boxes is a section titled 'Automatically Add Clients With the following DHCP Vendor IDs', which contains five empty text input fields. At the bottom right of the interface are two buttons: 'Apply' and 'Cancel'.

SNMP SETUP

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.

To access the **SNMP SETUP** setting window, click on the **SNMP SETUP** button in the ADVANCED tab

SNMP CONFIGURATION

Please tick **Enable the SNMP Agent**

Please type the **Read Community, Set Community** to match with the SNMP query.

Please type **System Name, System Location** and **System Contact** to describe the DSL-2880AL's related information.

Please type the trap IP on the **Trap Manager IP**

Please click the **Apply** button to save the setting.

Port Forwarding	<div style="background-color: #f4a460; padding: 5px;">SNMP</div> <div style="background-color: #e0e0e0; padding: 5px; margin-top: 5px;"> 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. </div> <div style="background-color: #333; color: white; padding: 5px; margin-top: 5px;">SNMP -- CONFIGURATION</div> <div style="padding: 10px; margin-top: 5px;"> <p>Enable SNMP Agent : <input checked="" type="checkbox"/></p> <p>Read Community : <input type="text" value="public"/></p> <p>Set Community : <input type="text" value="private"/></p> <p>System Name : <input type="text" value="DSL2751"/></p> <p>System Location : <input type="text" value="D-Link"/></p> <p>System Contact : <input type="text" value="Administrator"/></p> <p>Trap Manager IP : <input type="text" value="192.168.1.123"/></p> </div> <div style="text-align: right; margin-top: 10px;"> <input type="button" value="Apply"/> <input type="button" value="Cancel"/> </div>
Application Rules	
QoS Setup	
Outbound Filter	
Inbound Filter	
Wireless Filter	
DNS Setup	
Firewall & DMZ	
Advanced Internet	
Advanced Wireless	
Advanced LAN	
Port Mapping	
SNMP Setup	
Remote Management	
Routing Setup	
TR-069 Client	
Wi-Fi Protected Setup	

PARENTAL CONTROL

Parental Control provides two useful tools for restricting Internet access. Block Websites allows you to quickly create a list of all web sites that you wish to stop users from accessing. Time Restrictions allows you to control when clients connected to Router are allowed to access the Internet.

To access **PARENTAL CONTROL** setting windows, click on the **PARENTAL CONTROL** button in the **ADVANCED** tab

BLOCK WEBSITES SCHEDULING

To type the **Website** URL which you want to block.

To specify Blocked Days as **All Week** or specific **Days**.

To specify Blocked Hour **All DAY-24hrs** or specific **Start Time** to **End Time**.

Click on the **Block Website** button to add web site block rule.

INTERNET ACCESS TIME RESTRICTIONS

Check the **Start Time** to **End Time** and **days** for Internet Access Restriction **Allow** or **Deny**.

PARENTAL CONTROL

Parental Control provides two useful tools for restricting Internet access. Block Websites allows you to quickly create a list of all web sites that you wish to stop users from accessing. Time Restrictions allows you to control when clients or PCs connected to Router are allowed to access the Internet

BLOCKED WEBSITES SCHEDULING

Website:

Day(s): All Week Select Day(s)

Sun Mon Tue Wed Thu Fri Sat

All Day - 24 hrs

Start Time : (hour:minute, 24 hour time)

End Time : (hour:minute, 24 hour time)

Website	Days and Time	Unblock

INTERNET ACCESS TIME RESTRICTIONS

Time	Mon	Tue	Wed	Thu	Fri	Sat	Sun	All Days	Allow	Deny
Start <input type="text"/> - End <input type="text"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>								
Start <input type="text"/> - End <input type="text"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>								
Start <input type="text"/> - End <input type="text"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>								

ROUTING SETUP

Over the Routing Setup page, you can configure static routing policies or RIP protocol settings.

To access the **Routing** setting window, click on the **Routing** button under the **ADVANCED** tab.

Routing -- Static Route

Enter the destination network address, subnet mask, gateway AND/OR available WAN interface then click "Apply" to add the entry to the routing table. A maximum 32 entries can be configured

Please click the **Add** or **Edit** button to set a static routing policy in the list.

Please type the **Destination Network Address** and **Subnet Mask**.

Please choose type **Use the Gateway IP**, **Use the IPv4 interface** or **Use the IPv6 interface** to be the routing interface.

Click the **Apply** the button to save the configuration.

ROUTING -- STATIC ROUTE

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

A maximum 32 entries can be configured

Allows you to configure RIP (Routing Information Protocol) in case wan is MER and nat is disabled. To activate RIP for the device, select the 'Enabled' radio button for Global RIP Mode. To configure an individual interface, select the desired RIP version and operation, followed by placing a check in the 'Enabled' checkbox for the interface. Click the 'Apply' button to save the configuration, and to start or stop RIP based on the Global RIP mode selected.

Destination	Subnet Mask	Gateway	Interface

Add Edit Delete

STATIC ROUTE ADD/EDIT

Destination Network Address :

Subnet Mask :

Use Gateway IP Address :

Use Interface :

Back Apply Cancel

Section 3 - Configuration

Routing -- RIP Configuration

Allows you to configure RIP (Routing Information Protocol). To activate RIP for the device, select the 'Enabled' radio button for Global RIP Mode. To configure an individual interface, select the desired RIP version and operation, followed by placing a check in the 'Enabled' checkbox for the interface. Click the 'Apply' button to save the configuration, and to start or stop RIP based on the Global RIP mode selected.

Please choose the **Version** and **Operation**, and then decide to **Enable** or not.

ROUTING -- RIP CONFIGURATION

Interface	VPI/VCI	Version	Operation	Enabled
atm0	0/33	2	Passive	<input type="checkbox"/>
br0	(LAN)	2	Passive	<input type="checkbox"/>

Wi-Fi PROTECTED SETUP

Wi-Fi Protected Setup (also known as WPS) is a standard designed to pair up a new joined client devices to a AP network by using a PIN or hardware push button. In order to pair up AP and wireless client, you have to ensure both AP and client devices must support Wi-Fi Protected Setup.

To access the **WI-FI PROTECTED SETUP** window, click on the **WI-FI Protected Setup** button under the **ADVANCED** tab.

Wi-Fi Protected Setup

Please select to **Enable** or **Lock** Wireless Security Settings

PIN Settings: Choose to click the **Reset PIN to Default** button or **Generate New PIN** button to show the PIN on the Current PIN.

ADD WIRELESS STATION: Please click the **Add Wireless Device** with WPS button to set the WPS.

The screenshot displays the configuration page for Wi-Fi Protected Setup. On the left is a vertical menu with the following items: Port Forwarding, Application Rules, QoS Setup, Outbound Filter, Inbound Filter, Wireless Filter, DNS Setup, Firewall & DMZ, Advanced Internet, Advanced Wireless, Advanced LAN, Port Mapping, SNMP Setup, Remote Management, Routing Setup, **Wi-Fi Protected Setup** (highlighted), IPv6 Firewall, and IPv6 Routing.

The main content area is divided into three sections:

- WI-FI PROTECTED SETUP:** This section contains two checked checkboxes: Enable and Lock Wireless Security Settings. Below them, it shows "WPS Configured State : Configured" and a button labeled "Back to Unconfigured".
- PIN SETTINGS:** This section shows "Current PIN : 15624697" in a text field. Below the field are two buttons: "Reset PIN to Default" and "Generate New PIN".
- ADD WIRELESS STATION:** This section contains a single button labeled "Add Wireless Device with WPS".

At the bottom of the configuration area, there are two buttons: "Apply" and "Cancel".

IPV6 FIREWALL

The Firewall settings section is an advance feature used to allow or deny traffic from passing through the device. It works in the same way as ip filters with additional settings. You can create more detail rules for the device.

To access the **IPv6 Firewall** setting window, click on the **IPv6 Firewall** button in the **ADVANCE** table

ACTIVE FIREWALL RULES

Click **Add** button to add Firewall Rules.

IPV6 FIREWALL RULE

Type **Rule Name**, select **Schedule** (Schedule Rule can be set as following).

Type **Source Address Range**, select **Use Interface** and **Protocol** in drop-down menu.

Type **Dest Address Range**, **Dest Port Range** and select **Use Interface** in drop-down menu.

The screenshot displays the IPv6 Firewall configuration page. On the left is a sidebar menu with the following items: Port Forwarding, Application Rules, QoS Setup, Outbound Filter, Inbound Filter, Wireless Filter, DNS Setup, Firewall & DMZ, Advanced Internet, Advanced Wireless, Advanced LAN, Port Mapping, SNMP Setup, Remote Management, Routing Setup, Wi-Fi Protected Setup, **IPv6 Firewall**, IPv6 Routing, Budget Quota, and Logout. The main content area is titled 'IPV6_FIREWALL' and contains a descriptive paragraph. Below this is a section titled 'ACTIVE FIREWALL RULES' which features a table with the following columns: Name, Src. Addr Range, Use Interface, Src. Protocol, Dest. Addr Range, Dest. Port, and Schedule Rule. Underneath the table are 'Add', 'Edit', and 'Delete' buttons. The bottom section, 'IPV6 FIREWALL RULE', contains a form with the following fields: 'Rule Name' (text input), 'Schedule' (dropdown menu set to 'Always' with a 'View Available Schedules' link), 'Source Address Range' (text input), 'Use Interface' (dropdown menu set to 'PPPoE_0_42_1/'), 'Protocol' (dropdown menu set to '(Click to select)'), 'Dest Address Range' (text input), and 'Dest Port Range' (two text inputs separated by a tilde '~').

SCHEDULE RULE

Click **Add** button to add a new schedule.

ADD SCHEDULE RULE

Type **Name** for this rule and select **Day(s)**, you can sele **All Week** or select **Day(s)**.

Check **All Day-24hr** or set **Start time** to **End Time**

SCHEDULE RULE									
<input type="text"/>	<input type="checkbox"/>								
Rule Name	Sun	Mon	Tue	Wed	Thu	Fri	Sat	Start	Stop

ADD SCHEDULE RULE	
Name :	<input type="text"/>
Day(s) :	<input type="radio"/> All Week <input checked="" type="radio"/> Select Day(s)
	<input type="checkbox"/> Sun <input type="checkbox"/> Mon <input type="checkbox"/> Tue <input type="checkbox"/> Wed <input type="checkbox"/> Thu <input type="checkbox"/> Fri <input type="checkbox"/> Sat
All Day - 24 hrs :	<input type="checkbox"/>
Start Time :	<input type="text"/> : <input type="text"/> (hour:minute, 24 hour time)
End Time :	<input type="text"/> : <input type="text"/> (hour:minute, 24 hour time)

IPV6 ROUTING

This Routing page allows you to specify custom routes that determine how data is moved around your network. A maximum 20 entries can be configured

To access the **IPv6 Routing** setting window, click on the **IPv6 Routing** button in the **ADVANCE** table

STATIC IPV6 ROUTES

Click **Add** button to add **Rules**.

STATIC ROUTE ADD/EDIT

Type **Rule/Name** for this rule.

Type **Destination IPv6/Prefix**, **Metric** and **Gate way IP Address**.

Select **Use Interface** in drop-down menu.

The screenshot displays the IPv6 Routing configuration page. On the left is a vertical navigation menu with the following items: Port Forwarding, Application Rules, QoS Setup, Outbound Filter, Inbound Filter, Wireless Filter, DNS Setup, Firewall & DMZ, Advanced Internet, Advanced Wireless, Advanced LAN, Port Mapping, SNMP Setup, Remote Management, Routing Setup, Wi-Fi Protected Setup, IPv6 Firewall, IPv6 Routing (highlighted), and Budget Quota.

The main content area is divided into two sections:

- ROUTING** (orange header): Contains the text "This Routing page allows you to specify custom routes that determine how data is moved around your network." and "A maximum 20 entries can be configured".
- STATIC IPV6 ROUTES** (dark grey header): Contains a table with columns: Name, Destination Addr/Prefix Length, Metric, Gateway Addr, and Interface. Below the table are buttons for Add, Edit, and Delete.

The **STATIC ROUTE ADD/EDIT** form (dark grey header) includes the following fields:

- Rule Name: [Text Input]
- Destination IPv6/Prefix: [Text Input] / [Text Input]
- Metric: [Text Input]
- Gateway IP Address: [Text Input]
- Use Interface: [Dropdown Menu] (currently showing LAN/br0)

At the bottom of the form are buttons for Back, Apply, and Cancel.

BUDGET QUOTA

Budget Quota is a traffic meter feature offers

- Traffic quota metering on the user specified interface over the user defined period
- Traffic quota metering in different direction (both ingress and egress direction)
- Interface locking down in order to prevent traffic over flow.

Budget Quota is designed mainly for user who subscribe non flat rate internet access plan. To prevent download traffic over monthly quota, user can specify the WAN interface and download traffic quota.

Budget Quota

To access the **Budget Quota** window, click on the **Budget Quota** button under the **ADVANCED** tab.

Please tick **Enable Limitation Quota** to activate Budget Quota

Select interface to limit the data transmission quota.

Set meter duration over **Limit time(days)**

Check **Enable Download quota** and set **Download quota(Max, GB)**

Check **Enable Upload quota** and set **Upload quota(Max, GB)**

Remark:

- Before you activated Budget Quota, you MUST activate NTP and have device sytem time adjusted accurately
- Before you configure Budgt Quota, please have your WAN interface connected (otherwise, the WAN interface will not show over the Budget Quota interface option)

Port Forwarding	BUDGET QUOTA
Application Rules	Budget Quota can be used to implement the limitation quota and other functions.
QoS Setup	LIMITATION QUOTA SETTINGS
Outbound Filter	<p>Enable limitation quota : <input checked="" type="checkbox"/></p> <p>Select interface : <input type="text" value="ppp0"/></p> <p>Start router time : Friday, May 10, 2013 19:31:34 PM</p> <p>Limit time(days) : <input type="text" value="30"/></p> <p>Enable download quota : <input checked="" type="checkbox"/></p> <p>Download quota(Max, MB) : <input type="text" value="1000"/></p> <p>Enable upload quota : <input type="checkbox"/></p> <p>Upload quota(Max, MB) : <input type="text"/></p>
Inbound Filter	<input type="button" value="Traffic Info"/> <input type="button" value="Apply"/> <input type="button" value="Reset"/>
Wireless Filter	
DNS Setup	
Firewall & DMZ	
Advanced Internet	
Advanced Wireless	
Advanced LAN	
Port Mapping	
SNMP Setup	
Remote Management	
Routing Setup	
TR-069 Client	
Wi-Fi Protected Setup	
IPv6 Firewall	
IPv6 Routing	
Budget Quota	
Logout	

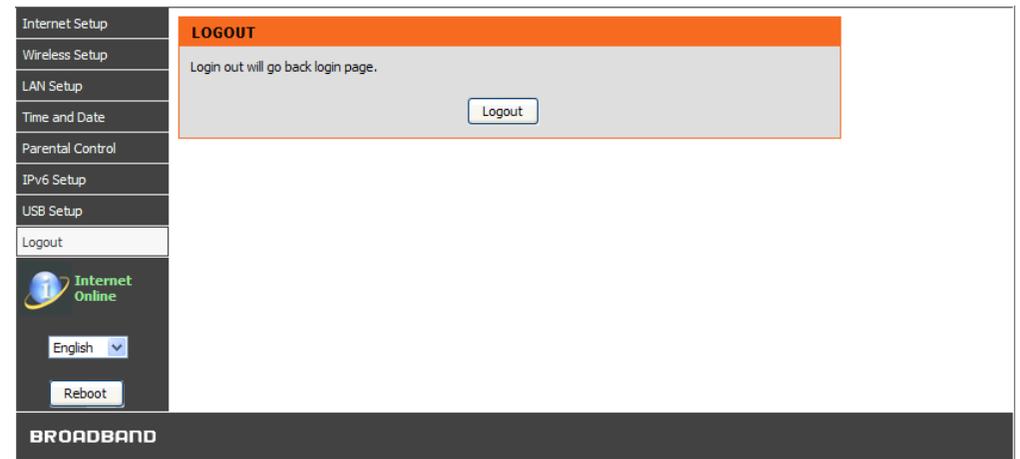
LOGOUT

The **LOGOUT** page enables you to logout of management GUI and as well closes the browser.

To access the **LOGOUT** setting window, click on the **Logout** button in the **SETUP** tab

LOGOUT

Click on the **Logout** button to logout of the router configuration settings and close the web browser.



MAINTENANCE

Click on the **MAINTENANCE** tab to reveal the window buttons for various functions located in this directory.

PASSWORD

The factory default password of this router is 'admin'. To help secure your network, D-Link recommends that you should choose a new password.

To access the **PASSWORD** setting window, click on the **PASSWORD** button in the **MAINTENANCE** tab

PASSWORD

Set Password (optional)

Please type the **Current Password**, **New Password**, **Confirm Password** and the **Idle Time Out**.

Please click the **Apply** Settings button to save the settings.

GRAPHIC LOG-IN AUTHENTICATION (CAPTCHA)

To enhance your router login security, you can **enable CAPTCHA**.

Please click the **Apply** Settings button to save the configuration.

The screenshot shows the router's maintenance interface. On the left is a sidebar menu with options: Password, Save/Restore Settings, Firmware Update, Diagnostics, Ping Test, System Log, Schedules, Logout, Internet Online (with a globe icon), English (dropdown), and Reboot. The main content area is titled 'PASSWORD' and contains a warning message: 'The factory default password of this router is 'admin'. To help secure your network, D-Link recommends that you should choose a new password.' Below this is a section titled 'SET PASSWORD (OPTIONAL)' with the instruction: 'To change the router password, please type in the current password, then the new password twice.' It includes four input fields: 'Current Password:', 'New Password:', 'Confirm Password:', and 'Session Idle Time Out:' (with '10' entered). At the bottom of this section are 'Apply' and 'Cancel' buttons. Below that is a section titled 'GRAPHIC LOG-IN AUTHENTICATION (CAPTCHA)' with the instruction: 'To enhance your router login security.' It includes a checkbox labeled 'Enable CAPTCHA:' which is currently unchecked. At the bottom of this section are 'Apply' and 'Cancel' buttons.

SAVE/RESTORE SETTINGS

The device firmware offers you configuration backup feature which you can backup the configuration settings as a plain text file and store on your computer hard drive. You also have the option to restore configuration settings, or reset the device configuration back to manufactory default settings.

To access the **Save/Restore Configuration** setting window, click on the **Save/Restore Configuration** button in the **MAINTENACE** tab

Save/Restore Configuration

Please click the **Save** button on the Save Settings to Local Hard Drive.

Please click **Browse** button to choose the configurations file and then click the **Update Settings** button to upload.

If necessary, please click the **Restore** Device button to have the default settings.

The screenshot displays the web interface for the D-Link DSL-2880AL. On the left is a vertical navigation menu with the following items: Password, Save/Restore Settings (highlighted), Firmware Update, Diagnostics, Ping Test, System Log, Schedules, Logout, Internet Online (with a globe icon), English (dropdown menu), and Reboot. The main content area is titled "SAVE/RESTORE SETTINGS" in an orange header. Below this is a grey box containing the text: "Once the router is configured you can save the configuration settings to a configuration file on your hard drive. You also have the option to load configuration settings, or restore the factory default settings." Underneath is a section titled "SAVE/RESTORE CONFIGURATION" with three rows of controls: "Save Settings to Local Hard Drive" with a "Backup Settings" button; "Load Settings From Local Hard Drive" with a text input field and a "Browse..." button, followed by an "Update Settings" button; and "Restore To Factory Default Settings" with a "Restore Device" button. At the bottom of the interface is a dark grey bar with the word "BROADBAND" in white.

FIRMWARE UPDATE

Use the FIRMWARE UPGRADE window to load the latest firmware for the device. Note that the device configuration settings may return to the factory default settings, so make sure you first save the configuration settings with the SAVE/RESTORE SETTINGS window described above.

To access the **FIRMWARE UPGRADE** setting window, click on the **Firmware Update** button under the **MAINTENANCE** tab.

FIRMWARE UPDATE

To upgrade firmware, click on the **Browse** button to search for the firmware file and then click the **Upload** button to begin copying the file.

The Router will load the file and restart automatically.

WARNING: Please **DO NOT** power off the router during the time device upgrading the firmware image as it may damage the hardware.

The screenshot shows the router's web interface. On the left is a navigation menu with options: Password, Save/Restore Settings, Firmware Update (highlighted), Remote Management, Diagnostics, Ping Test, System Log, Schedules, and Logout. Below the menu is an 'Internet Online' status indicator and a 'Reboot' button.

The main content area is titled 'FIRMWARE UPDATE' and contains a warning: 'Note: Please do not update the firmware on this router unless instructed to do so by D-Link technical support or your ISP.'

Below the warning is the 'FIRMWARE INFORMATION' section, which displays the following details:

- Board ID : DSL-2880AL
- Software Version : AU_1.00
- Bootloader (CFE) Version : 1.0.38-114.-86
- Wireless Driver Version : 6.30.102.7.cpe4.12L07.0

The bottom section is 'FIRMWARE UPGRADE', which includes another warning: 'Note: Some firmware upgrades reset the configuration options to factory defaults. Before performing an upgrade, be sure to save the current configuration from the Maintenance -> Save/Restore Settings screen.' It also provides instructions: 'To upgrade the firmware, your PC must have a wired connection to the router. Enter the name of the firmware upgrade file, and click on the Upload button.'

At the bottom of this section is an 'Upload:' label followed by a text input field, a 'Browse...' button, and an 'Upload' button.

REMOTE MANAGEMENT

This section allows you to enable/disable remote access to the router from the Internet. Advanced access control allows you to configure access via specific services. Most users will not need to change any of these settings.

To access the **REMOTE MANAGEMENT** setting window, click on the **REMOTE MANAGEMENT** button in the **MAINTENANCE** tab

REMOTE MANAGEMENT SETTINGS

Please enable the **ENABLE Remote Management**

Please specify the HTTP remote access port number which you want to replace the standard service port 80.

Please select **Allow All** or **Deny All** on the Remote Admin Inbound Filter

Please type a string to describe the action on the **Details**.

REMOTE ACCESS CONTROL

To tick the specific Service(s) which you wish to enable over the device LAN interface or the device WAN interface

REMOTE MANAGEMENT

This section allows you to enable/disable remote access to the router from the Internet. Advanced access control allows you to configure access via specific services. Most users will not need to change any of these settings.

REMOTE MANAGEMENT SETTINGS

Enable Remote Management :

Remote Admin Port :

Remote Admin Inbound Filter : Allow All

Details :

REMOTE ACCESS CONTROL

Service	LAN	WAN
HTTP	<input checked="" type="checkbox"/> Enabled	<input type="checkbox"/> Enabled
ICMP	<input checked="" type="checkbox"/> Enabled	<input type="checkbox"/> Enabled
SNMP	<input checked="" type="checkbox"/> Enabled	<input type="checkbox"/> Enabled
SSH	<input type="checkbox"/> Enabled	<input type="checkbox"/> Enabled
TELNET	<input checked="" type="checkbox"/> Enabled	<input type="checkbox"/> Enabled
TFTP	<input type="checkbox"/> Enabled	<input type="checkbox"/> Enabled

DIAGNOSTICS

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

To access the **Diagnostics** setting window, click on the **Diagnostics** button under the **MAINTENANCE** tab.

System check

There are Test your eth0/eth1/eth2/eth3 Connection, Test your Wireless Connection and Test ADSL Synchronization and they will show PASS or FAIL

INTERNET CONNECTIVITY Check

There are Ping ISP Default Gateway/ Primary DNS server and they will show PASS or FAIL

Please click the **Test** button to Diagnostic the above test items.

DIAGNOSTICS		
Your router is capable of testing your DSL connection. The individual tests are listed below. If a test displays a fail status,click "Return Diagnostics Tests" at the bottom of this page to make sure fail status is consistent. If the test continues to fail,click "Help" and follow the troubleshooting procedures.		
SYSTEM CHECK		
Test your lan4 Connection:	FAIL	Help
Test your lan3 Connection:	PASS	Help
Test your lan2 Connection:	FAIL	Help
Test your lan1 Connection:	FAIL	Help
Test your Wireless Connection:	PASS	Help
Test ADSL Synchronization:	PASS	Help
INTERNET CONNECTIVITY CHECK		
Test PPP server connection:	PASS	
Test Authentication:	PASS	
Test the assigned IP address:	PASS	
Ping ISP Default Gateway:	PASS	
Ping Primary DNS server:	PASS	
<input type="button" value="TEST"/>		

PING TEST

The tests on this page can be used to verify whether or not your router is working correctly. If you have rerun the tests and consulted the help file and you are still experiencing difficulties,

To access the **Ping test** setting window, click on the **Ping test Diagnostics** button under the **MAINTENANCE** tab.

PING TEST

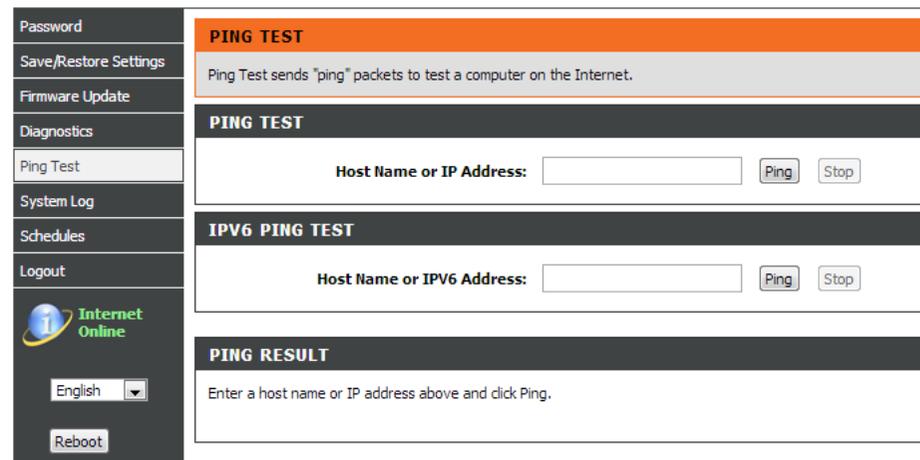
You can type **Host Name or IP Address** and click **Ping** button

IPv6 PING TEST

You can type Host Name or IPv6 Address and click **Ping** button

PING RESULT

When you click **Stop** button, the ping results will show in **PING RESULT** windows



SYSTEM LOG

The system Log allows you to configure local, remote and email logging, and to view the logs that have been created.

To access the **SYSTEM LOG** setting window, click on the **System Log** button under the **MAINTENANCE** tab.

Remote Log Setting

Check **Log Enable** box:

Log Level: All events above or equal to the selected level will be logged.

Display Level: All logged events above or equal to the selected level will be displayed.

Mode: Display mode of system log. Local: Display on local host only

Server IP Address: IP address of the remote system log server

Server UDP Port: UDP port number of the remote system log server

The screenshot shows a web interface for configuring the SYSTEM LOG. On the left is a navigation menu with options: Password, Save/Restore Settings, Firmware Update, Diagnostics, Ping Test, System Log (highlighted), Schedules, Logout, Internet Online, English (language selector), and Reboot. The main content area is titled 'SYSTEM LOG' and contains the following sections:

- SYSTEM LOG**: A header section with an orange background and a grey box containing the text: "The system Log allows you to configure local, remote and email logging, and to view the logs that have been created."
- REMOTE LOG SETTING**: A section with a dark grey header containing:
 - Log Enable:
 - Log Level: Debugging (dropdown menu)
 - Display Level: Error (dropdown menu)
 - Mode: Local (dropdown menu)
 - Server IP Address: [text input field]
 - Server UDP Port: [text input field]
- ENABLE EMAIL NOTIFICATION**: A section with a dark grey header containing:
 - Enable EMAIL Notification:

ENABLE EMAIL NOTIFICATION

Please enable. If any logs occur, the system will send mail to the mail address you set.

EMAIL SETTINGS

Please input the **From MAIL Address**, **To MAIL Address** and **SMTP Server Address**.

Please Enable the **Enable Authentication** and then set the **Account Name**, **Account Password** and **Verify Password** if the outgoing mail server requires authentication for relay.

EMAIL LOG WHEN FULL

Please Enable the **On Log Full**. When the log file is full, the system will send mail to the mail address you set.

View System Log

The system will show logs in the list by Date/Time, Facility, Severity and Message.

Please click the **Apply Settings** button to save the configuration.

The screenshot displays a configuration interface with the following sections:

- ENABLE EMAIL NOTIFICATION**: A checkbox labeled "Enable EMAIL Notification" is checked.
- EMAIL SETTINGS**: Fields for "From MAIL Address" (admin@mail.dlink.com), "To MAIL Address" (user@mail.dlink.com), and "SMTP Server Address" (mail.dlink.com). There is an unchecked checkbox for "Enable Authentication" and three password fields for "Account Name", "Account Password", and "Verify Password".
- EMAIL LOG WHEN FULL**: A checkbox labeled "On Log Full" is checked.
- VIEW SYSTEM LOG**: A "System Log" window with a table header: Date/Time | Facility | Severity | Message. Below the table are "Refresh" and "Close" buttons.

At the bottom of the interface are "Apply" and "Cancel" buttons.

SCHEDULE

Schedule allows you to create scheduling rules to be applied for your firewall. Maximum of 16 entries

To access the **SCHEDULE RULE** setting window, click on the **SCHEDULE RULE** button under the **MAINTENANCE** tab.

SCHEDULE RULE

Press **Add / Edit / Delete** button to modify your **SCHEDULE RULE** list.

ADD SCHEDULE RULE

Type **Name** for your schedule.

Select **Day(s)** or **ALL Day-24hrs** to active your firewall and type **Star Time** to **End Time**.

Click the **Apply** the button to save the configuration.

The screenshot displays the 'SCHEDULE' configuration window. On the left is a sidebar menu with the following items: Password, Save/Restore Settings, Firmware Update, Diagnostics, Ping Test, System Log, Schedules (highlighted), and Logout. Below the menu is the 'Internet Online' status indicator and a language dropdown set to 'English', along with a 'Reboot' button. The main content area is titled 'SCHEDULE' and contains the following sections:

- SCHEDULE**: A header section with an orange background, containing the text: "Schedule allows you to create scheduling rules to be applied for your firewall. Maximum of 16 entries."
- SCHEDULE RULE**: A table with columns: Rule Name, Sun, Mon, Tue, Wed, Thu, Fri, Sat, Start, Stop. The table is currently empty.
- Buttons**: 'Add', 'Edit', and 'Delete' buttons are located below the table.
- ADD SCHEDULE RULE**: A form with the following fields:
 - Name**: WeekDay
 - Day(s)**: Radio buttons for 'All Week' and 'Select Day(s)'. Under 'Select Day(s)', checkboxes for Sun, Mon, Tue, Wed, Thu, Fri, and Sat are shown, with Mon, Tue, Wed, and Thu checked.
 - All Day - 24 hrs**: An unchecked checkbox.
 - Start Time**: 08 : 30 (hour:minute, 24 hour time)
 - End Time**: 18 : 00 (hour:minute, 24 hour time)
- Buttons**: 'Apply' and 'Cancel' buttons are located at the bottom of the form.

STATUS

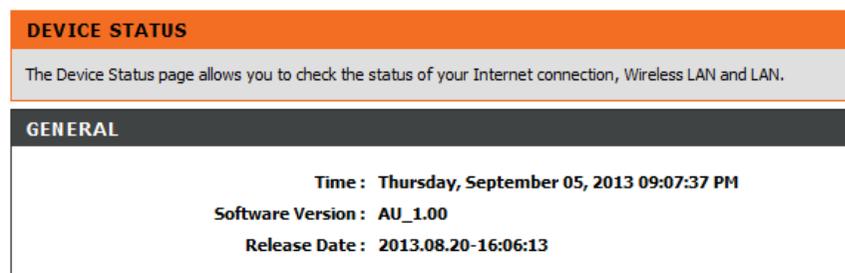
Click on the **STATUS** tab to reveal the window buttons for various functions located in this directory. The **DEVICE STATUS** window is the first item in the **STATUS** directory. Use these windows to view system information and monitor performance.

DEVICE INFO

The **Device Info** page displays a summary overview of your router status, including: Device software version and summary of your Internet configuration (both wireless and Ethernet status).

To access the **DEVICE INFO** setting window, click on the **Device Info** button in the **STATUS** tab.

This window displays current **SYSTEM INFO**, **INTERNET INFO**, **WIRELESS INFO** and **LOCAL NETWORK INFO**.



The screenshot shows the 'DEVICE STATUS' page. It has an orange header with the text 'DEVICE STATUS'. Below the header is a grey box with the text: 'The Device Status page allows you to check the status of your Internet connection, Wireless LAN and LAN.' Below that is a dark grey header with the text 'GENERAL'. The main content area is white and contains the following information: 'Time : Thursday, September 05, 2013 09:07:37 PM', 'Software Version : AU_1.00', and 'Release Date : 2013.08.20-16:06:13'.

DEVICE STATUS
The Device Status page allows you to check the status of your Internet connection, Wireless LAN and LAN.
GENERAL
Time : Thursday, September 05, 2013 09:07:37 PM
Software Version : AU_1.00
Release Date : 2013.08.20-16:06:13

Section 3 - Configuration

INTERNET INFO

This window displays WAN information including IP address, Mask, Default Gateway, Primary/Secondary DNS Server.

WIRELESS LAN

This session displays the 2.4GHz and the 5GHz wireless interface On/Off status, SSID names, wireless channel selected and security mode currently employed.

INTERNET INFO

Internet Connection:

Internet Connection Status:	CONNECTED
Internet Connection Up Time	0 days 0 hours 41 minutes 6 seconds
Default Gateway:	168.95.98.254
Preferred DNS Server:	168.95.192.1
Alternate DNS Server:	168.95.1.1
Downstream Line Rate (Kbps):	26051
Upstream Line Rate (Kbps):	2625

Interface	Description	Link Type	IGMP	QoS	Status	IP Address
ppp0	PPPoE_0_42_1	PPPoE	Disabled	Enabled	Connected	1.169.145.210

2.4GHZ WIRELESS LAN

Wireless Radio : ON
MAC Address : 1A:2B:3C:35:80:02
Network NAME(SSID) : D-Link DSL-2880AL
Channel : Auto
Security Type : None

5GHZ WIRELESS LAN

Wireless Radio : ON
MAC Address : 1A:2B:3C:35:80:03
Network NAME(SSID) : D-Link DSL-2880AL_5G
Channel : Auto
Security Type : None

LOCAL NETWORK INFO

This window displays LAN information including MAC, IP address, Mask, and DHCP Server.

LAN
MAC Address: 1A:2B:3C:35:80:01
IP Address: 192.168.1.1
Subnet Mask: 255.255.255.0
DHCP Server: ON

USB 3G DONGLE INFO

This session show you USB 3G dongle signal strength and as well the operation mode. When 3G internet connection is dropped unexpectedly, you can check here to find out whether the root cause is related to poor signal strength.

3G INFO

3G Signal Strength:	Good
3G dongle Mode:	UMTS

Marginal: -95dBm or lower
Workable: -85dBm to -95dBm
Good: -75dBm to -85dBm
Excellent: above -75dBm

CONNECTED CLIENTS

This feature shows all the client devices and computers currently associated wirelessly or connected over Ethernet LAN.

To access the Wireless clients setting window, click on the **Connected Clients** button in the **STATUS** tab.

CONNECTED WIRELESS CLIENTS

This window displays authenticated wireless stations and their status.

CONNECTED LAN CLIENTS

This window displays all the entities which link to the LAN interface successfully.

You can choose to block which entities and click the **Block** button

CONNECTED CLIENTS

This page shows all the currently connected wireless and LAN computers or PCs.

CONNECTED WIRELESS CLIENTS

BSSID	Associated	Authorized	SSID

CONNECTED LAN CLIENTS

Host Name	MAC Address	IP Address	Expires In	Block
TWHC1NB0037	e8:9a:8f:13:42:37	192.168.1.2	0 seconds	<input type="checkbox"/>

BLOCKED MAC ADDRESS

Host Name	MAC Address	Unblock

STATISTICS

This information reflects the current status of your router.

To access the **STATISTICS** window, click on the Logs button in the **STATISTICS** tab.

WAN STATISTICS

This window displays all the **Receiver** and **Transmitted** packet status on the WAN interface.

LAN STATISTICS

This window displays all the **Receiver** and **Transmitted** packet status on the LAN interface.

Device Info

Connected Clients

Statistics

Routing Info

IPv6 Status

IPv6 Routing Info

Logout

 Internet Online

English

Reboot

STATISTICS

This information reflects the current status of your DSL connection.

LAN STATISTICS

Interface	Received				Transmitted			
	Bytes	Pkts	Errs	Drops	Bytes	Pkts	Errs	Drops
eth1	3100579	25410	0	0	17878766	22571	0	0
eth2	0	0	0	0	0	0	0	0
eth3	0	0	0	0	0	0	0	0
wl0	0	0	0	0	309929	1822	0	0

WAN STATISTICS

Interface	PVC	Protocol	Service Name	Received				Transmitted			
				Bytes	Pkts	Errs	Drops	Bytes	Pkts	Errs	Drops
eth0	N/A	IPOE	MER_eth0	11497250	16882	0	0	2436321	20395	0	0

ADSL STATISTICS

This window displays all the **ADSL status**

You can click the **ADSL BER Test** button to test the ADSL connection.

You can click the **Reset Statistics** button to set all statistics to recount.

ADSL STATISTICS		
Mode:	ADSL_2plus	
Traffic Type:	ATM	
Status:	Up	
Link Power State:	LO	
	Downstream	Upstream
Line Coding(Trellis):	On	On
SNR Margin (0.1 dB):	66	66
Attenuation (0.1 dB):	0	4
Output Power (0.1 dBm):	94	93
Attainable Rate (Kbps):	27560	1339
	Path 0	
	Downstream	Upstream
Rate (Kbps):	27323	1245
MSGc (# of bytes in overhead channel message):	51	14
B (# of bytes in Mux Data Frame):	243	13
M (# of Mux Data Frames in FEC Data Frame):	1	16
T (Mux Data Frames over sync bytes):	4	9
R (# of check bytes in FEC Data Frame):	0	8
S (ratio of FEC over PMD Data Frame length):	0.2854	5.7107
L (# of bits in PMD Data Frame):	6838	325
D (interleaver depth):	1	8
Delay (msec):	0.7	11.42
INP (DMT symbol):	0.0	0.78
Super Frames:	0	0
Super Frame Errors:	0	0
RS Words:	0	1809532
RS Correctable Errors:	0	0
RS Uncorrectable Errors:	0	0
HEC Errors:	0	0
OCD Errors:	0	0
LCD Errors:	0	0
Total Cells:	166570819	7584863
Data Cells:	71414	27980
Bit Errors:	0	0
Total ES:	0	0
Total SES:	0	0
Total UAS:	19	19

[ADSL BER Test](#) [Reset Statistics](#)

ROUTING INFO

To access the **ROUTE INFO** setting window, click on the **ROUTE INFO** button under the **STATUS** tab.

The Route Info section displays route information showing the IP addresses of the destination, gateway, and subnet mask as well as other route information

ROUTING TABLE LIST			
ROUTING -- STATIC ROUTE			
Destination	Subnet Mask	Gateway	Interface

IPv6 STATUS

To access the **IPv6 Status** setting window, click on the **IPv6 Status** button under the **STATUS** tab.

All of your IPv6 Internet and network connection details are displayed on this page.

Device Info	IPv6 NETWORK INFORMATION				
Connected Clients	All of your IPv6 Internet and network connection details are displayed on this page.				
Statistics	IPv6 CONNECTION INFORMATION				
Routing Info	<p>IPv6 Connection Type : pppoe Network status : Wan IPv6 Address : IPv6 Default Gateway : Primary IPv6 DNS Server : Secondary IPv6 DNS Server : LAN IPv6 Link-Local Address : FE80::21A:2BFF:FE27:5000/64 DHCP-PD : IPv6 Network assignend by DHCP-PD : LAN IPv6 Address :</p>				
IPv6 Status	LAN IPv6 COMPUTERS				
IPv6 Routing Info	<table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th style="width: 60%;">IPv6 Address</th> <th style="width: 40%;">Name(if any)</th> </tr> </thead> <tbody> <tr> <td style="height: 20px;"> </td> <td> </td> </tr> </tbody> </table>	IPv6 Address	Name(if any)		
IPv6 Address	Name(if any)				
Logout					
 Internet Online					
English ▼					
Reboot					

IPv6 ROUTING INFO

To access the **IPv6 Routing Info** setting window, click on the **IPv6 Routing Info** button under the **STATUS** tab.

This Routing page displays the IPv6 routing policies currently configured on your router.

The screenshot shows the IPv6 Routing Info page. On the left is a sidebar menu with the following items: Device Info, Connected Clients, Statistics, Routing Info, IPv6 Status, IPv6 Routing Info (highlighted), Logout, Internet Online status, a language dropdown menu set to English, and a Reboot button. The main content area has an orange header for 'IPv6 ROUTING TABLE' and a grey message box stating 'This Routing page displays the IPv6 routing details configured for your router'. Below this is a section titled 'STATIC IPv6 ROUTES' with a table header containing the following columns: Name, Destination Addr/Prefix Length, Metric, Gateway Addr, and Interface.

Troubleshooting

This chapter provides solutions to problems that can occur during the installation and operation of the DSL-2880AL. 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.)

1. Why can't I access the web-based configuration utility?

When entering the IP address of the D-Link router (192.168.1.1 for example), you are not connecting to a website on the Internet or have to be connected to the Internet. The device has the utility built-in to a ROM chip in the device itself. Your computer must be on the same IP subnet to connect to the web-based utility.

- Make sure you have an updated Java-enabled web browser. We recommend the following:
 - Internet Explorer 6.0 or higher
 - Firefox 1.5 or higher
- Verify physical connectivity by checking for solid link lights on the device. If you do not get a solid link light, try using a different cable or connect to a different port on the device if possible. If the computer is turned off, the link light may not be on.
- Disable any internet security software running on the computer. Software firewalls such as Zone Alarm, Black Ice, Sygate, Norton Personal Firewall, and Windows® XP firewall may block access to the configuration pages. Check the help files included with your firewall software for more information on disabling or configuring it.
-

Section 4 - Troubleshooting

- Configure your Internet settings:
 - Go to **Start > Settings > Control Panel**. Double-click on the **Internet Options** icon. From the **Security** tab, click on the button to restore the settings to their defaults.
 - Click on the **Connection** tab and set the dial-up option to Never Dial a Connection. Click on the LAN Settings button. Make sure nothing is checked. Click on the **OK**.
 - Go to the **Advanced** tab and click on the button to restore these settings to their defaults. Click on the **OK** button three times.
 - Close your web browser (if open) and open it.
- Access the web management. Open your web browser and enter the IP address of your D-Link router in the address bar. This should open the login page for the web management.
- If you still cannot access the configuration, unplug the power to the router for 10 seconds and plug back in. Wait about 30 seconds and try accessing the configuration. If you have multiple computers, try connecting using a different computer.

2. What can I do if I forgot my password?

If you forgot your password, you must reset your router. Unfortunately this process will change all your settings back to the factory defaults.

To reset the router, locate the reset button (hole) on the rear panel of the unit. With the router powered on, use a paperclip to hold the button down for 10 seconds. Release the button and the router will go through its reboot process.

Wait about 30 seconds to access the router. The default IP address is 192.168.1.1. When logging in, type in the default User Name “admin,” and the default Password “admin” then click on the OK button to access the web-based manager.

APPENDIX

Wireless Basics

D-Link wireless products are based on industry standards to provide easy-to-use and compatible high-speed wireless connectivity within your home, business or public access wireless networks. Strictly adhering to the IEEE standard, the D-Link wireless family of products will allow you to securely access the data you want, when and where you want it. You will be able to enjoy the freedom that wireless networking delivers.

A wireless local area network (WLAN) is a cellular computer network that transmits and receives data with radio signals instead of wires. Wireless LANs are used increasingly in both home and office environments, and public areas such as airports, coffee shops and universities. Innovative ways to utilize WLAN technology are helping people to work and communicate more efficiently. Increased mobility and the absence of cabling and other fixed infrastructure have proven to be beneficial for many users.

Wireless users can use the same applications they use on a wired network. Wireless adapter cards used on laptop and desktop systems support the same protocols as Ethernet adapter cards.

Under many circumstances, it may be desirable for mobile network devices to link to a conventional Ethernet LAN in order to use servers, printers or an Internet connection supplied through the wired LAN. A Wireless Router is a device used to provide this link.

What is Wireless?

Wireless or Wi-Fi technology is another way of connecting your computer to the network without using wires. Wi-Fi uses radio frequency to connect wirelessly, so you have the freedom to connect computers anywhere in your home or office network.

Why D-Link Wireless?

D-Link is the worldwide leader and award winning designer, developer, and manufacturer of networking products. D-Link delivers the performance you need at a price you can afford. D-Link has all the products you need to build your network.

How does wireless work?

Wireless works similar to how cordless phone work, through radio signals to transmit data from one point A to point B. But wireless technology has restrictions as to how you can access the network. You must be within the wireless network range area to be able to connect your computer. There are two different types of wireless networks Wireless Local Area Network (WLAN), and Wireless Personal Area Network (WPAN).

Wireless Local Area Network (WLAN)

In a wireless local area network, a device called an Access Point (AP) connects computers to the network. The access point has a small antenna attached to it, which allows it to transmit data back and forth over radio signals. With an indoor access point as seen in the picture, the signal can travel up to 300 feet. With an outdoor access point the signal can reach out up to 30 miles to serve places like manufacturing plants, industrial locations, college and high school campuses, airports, golf courses, and many other outdoor venues.

Wireless Personal Area Network (WPAN)

Bluetooth is the industry standard wireless technology used for WPAN. Bluetooth devices in WPAN operate in a range up to 30 feet away. Compared to WLAN the speed and wireless operation range are both less than WLAN, but in return it doesn't use nearly as much power which makes it ideal for personal devices, such as mobile phones, PDAs, headphones, laptops, speakers, and other devices that operate on batteries.

Who uses wireless?

Wireless technology has become so popular in recent years that almost everyone is using it, whether it's for home, office, business, D-Link has a wireless solution for it.

Home

- Gives everyone at home broadband access
- Surf the web, check email, instant message, download multimedia files.
- Gets rid of the cables around the house
- Simple and easy to use

Small Office and Home Office

- Stay on top of everything at home as you would at the office
- Remotely access your office network from home
- Share the Internet connection and printer with multiple computers
- No need to dedicate office space

Where is wireless used?

Wireless technology is expanding everywhere not just at home or office. People like the freedom of mobility and it's becoming so popular that more and more public facilities now provide wireless access to attract people. The wireless connection in public places is usually called "hotspots".

Using a D-Link Cardbus Adapter with your laptop, you can access the hotspot to connect to Internet from remote locations like: Airports, Hotels, Coffee Shops, Libraries, Restaurants, and Convention Centers.

Wireless network is easy to setup, but if you're installing it for the first time it could be quite a task not knowing where to start. That's why we've put together a few setup steps and tips to help you through the process of setting up a wireless network.

Tips

Here are a few things to keep in mind, when you install a wireless network.

Centralize your router or Access Point

Make sure you place the router/access point in a centralized location within your network for the best performance. Try to place the router/access point as high as possible in the room, so the signal gets dispersed throughout your home. If you have a two-story home, you may need a repeater to boost the signal to extend the range.

Eliminate Interference

Place home appliances such as cordless telephones, microwaves, and televisions as far away as possible from the router/access point. This would significantly reduce any interference that the appliances might cause since they operate on same frequency.

Security

Don't let you next-door neighbors or intruders connect to your wireless network. Secure your wireless network by turning on the WPA security feature on the router. Refer to product manual for detail information on how to set it up.

Wireless Modes

There are basically two modes of networking:

- **Infrastructure** – All wireless clients will connect to an access point or wireless router.
- **Ad-Hoc** – Directly connecting to another computer, for peer-to-peer communication, using wireless network adapters on each computer, such as two or more D-Link wireless network adapters.

An Infrastructure network contains an Access Point or wireless router. All the wireless devices, or clients, will connect to the wireless router or access point.

An Ad-Hoc network contains only clients, such as laptops with wireless cardbus adapters. All the adapters must be in Ad-Hoc mode to communicate.

Networking Basics

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.

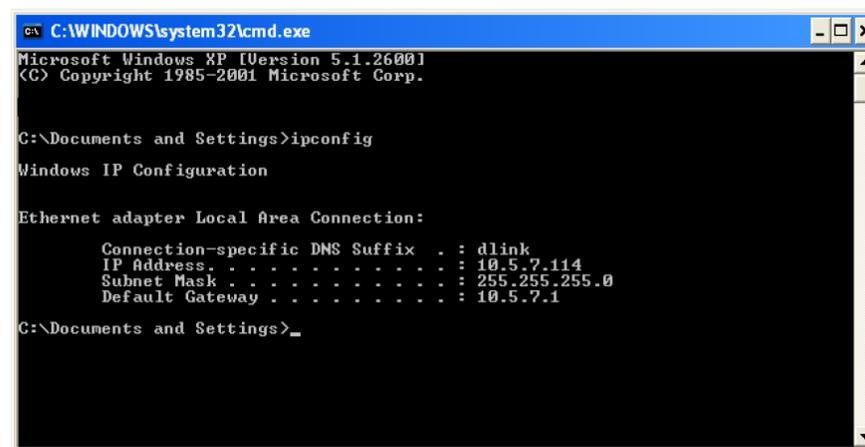
Click on **Start > Run**. In the run box type **cmd** and click on the **OK**.

At the prompt, type **ipconfig** and press **Enter**.

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 on **Start > Control Panel > Network Connections**.

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

Step 2

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

Step 3

Highlight **Internet Protocol (TCP/IP)** and click on the **Properties**.

Step 4

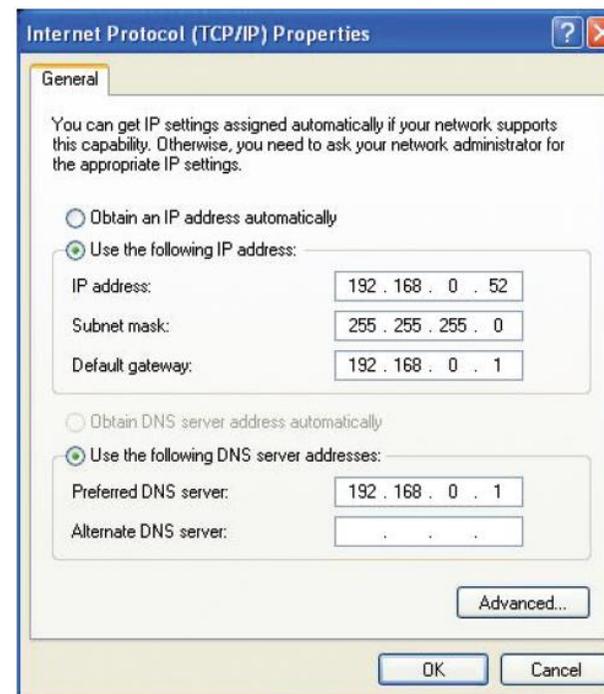
Click on the **Use the following IP address** and enter an IP address that is on the same subnet as your network or the LAN IP address on your router.

Example: If the router's LAN IP address is 192.168.0.1, make your IP address 192.168.0.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 (192.168.0.1).

Set Primary DNS the same as the LAN IP address of your router (192.168.0.1). The Secondary DNS is not needed or you may enter a DNS server from your ISP.

Step 5

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



FCC Caution

Statement :

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.

Class B:

FEDERAL COMMUNICATIONS COMMISSION INTERFERENCE 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 communications. However, there is no guarantee that interference will not occur in a Particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning 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.

CAUTION:

Any changes or modifications not expressly approved by the grantee of this device could void the user's authority to operate the equipment.

IC Caution

English:

This Class B digital apparatus complies with Canadian ICES-003 and RSS-210. Operation is subject to the following two conditions: (1) this device may not cause interference, and (2) this device must accept any interference, including interference that may cause undesired operation of the device.

Française:

Cet appareil numérique de classe B est conforme aux normes canadiennes ICES-003 et RSS-210. Son fonctionnement est soumis aux deux conditions suivantes : (1) cet appareil ne doit pas causer d'interférence et (2) cet appareil doit accepter toute interférence, notamment les interférences qui peuvent affecter son fonctionnement.

Contacting Technical Support

You can find software updates and user documentation on the D-Link websites.

If you require product support, we encourage you to browse our FAQ section on the Web Site before contacting the Support line.

We have many FAQ's which we hope will provide you a speedy resolution for your problem.

D-Link Link'n Print

Introduction

D-Link Link'n Print allows you to share USB devices such as external storage drives and multifunction printers with other users across your network by simply connecting the device to select D-Link routers. This allows you to use an external storage drive or printer located across your network as if it were connected to your local PC.

System Requirements

- Microsoft® Windows
- 2000 / 2003 / XP / Vista / 7 / 8 (32-bit / 64-bit)
- Pentium 3 800MHz or better
- 256MB RAM or higher
- CD-ROM drive
- A compatible D-Link router

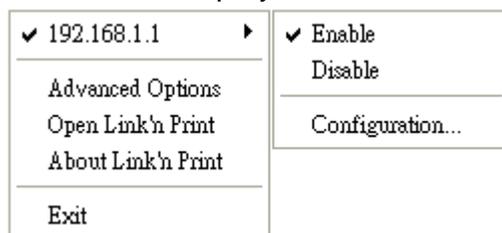
Installation

1. Insert the CD-ROM into your computer.
2. Follow the on-screen instructions.
3. The  icon should appear in the System Tray at the lower-right corner on the desktop and a new Icon should be created on the desktop.



Set up the D-Link Router

1. Connect the D-Link Router to the network.
2. Power on the D-Link Router.
3. Double-click on the  icon to open the D-Link D-Link Link'n Print.
4. Right-click on  in the System Tray at the lower-right corner on your Windows Desktop. To click on “[Configuration...](#)” and a pops up window will display the D-Link Router management GUI.



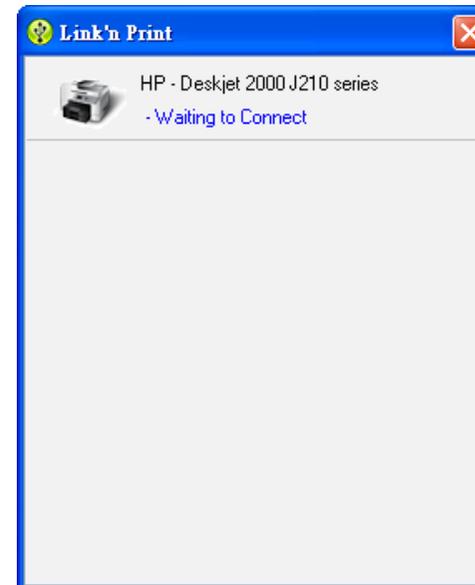
5. To logon the device management GUI and navigate to USB setup page.
6. To select “[Enable Link'n Print](#)” and following by click “Apply” button.



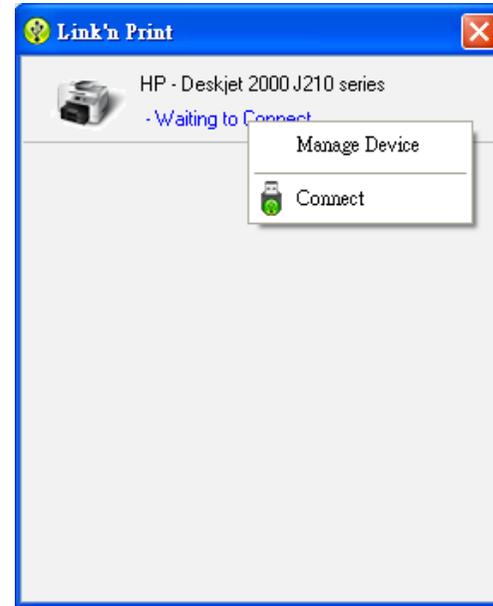
7. The  icon in the Windows System Tray should change to an  icon.

Connect USB Devices to the D-Link Router

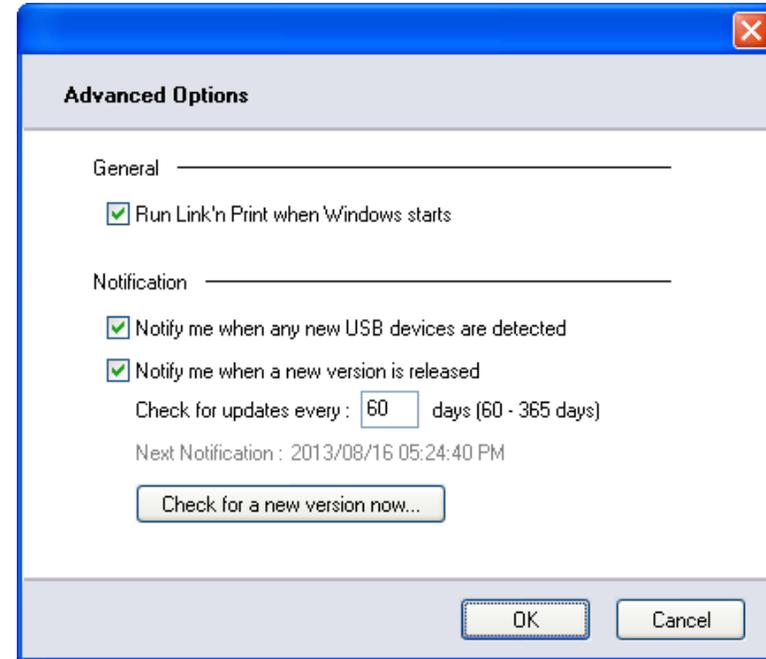
The D-Link Link'n Print automatically detects for each connected USB device. A window will pop up for each detected USB device.



1. Right-click on the  icon.
2. Click on Open D-Link Link'n Print.
3. The D-Link Link'n Print displays the connected USB devices on the network. To click "Connect" to have the USB device connected.

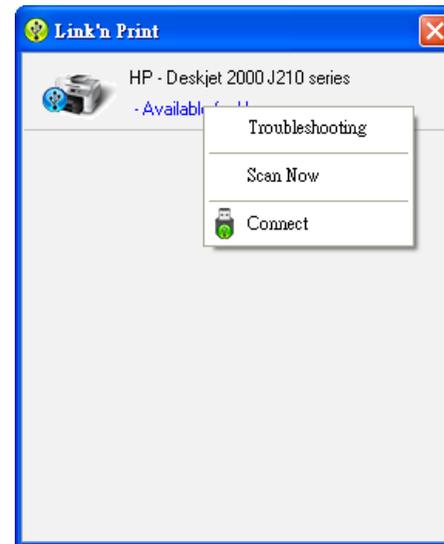


4. Advanced Options can be set by clicking on Advanced Options.



Virtually Connect and Disconnect a USB Device

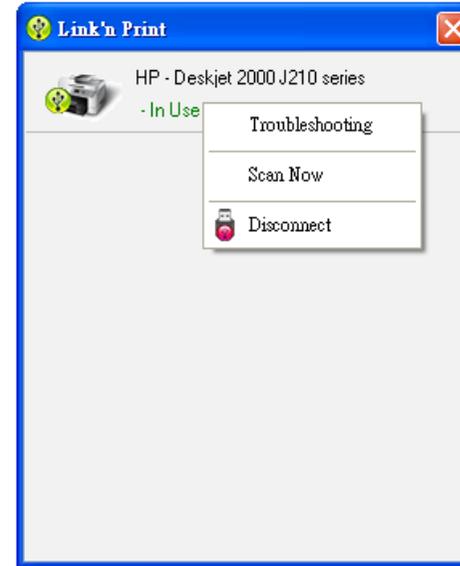
1. Move the cursor to Waiting to Connect and click on **Connect** to virtually connect a USB device.



2. The D-Link Link'n Print displays which user is virtually connecting this USB device.

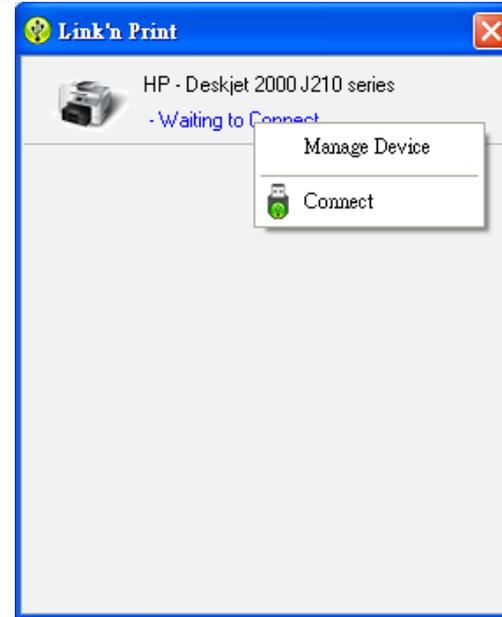


3. Move the cursor to In Use By (Owner) and click on **Disconnect** to virtually disconnect the USB device.

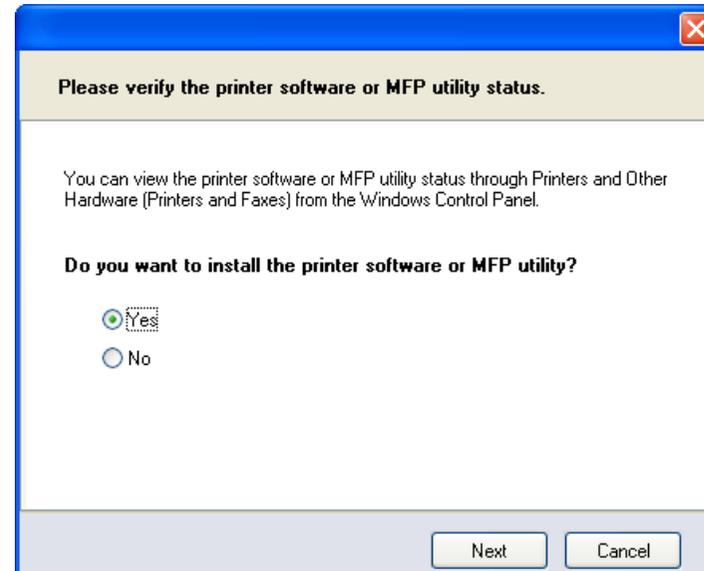


When the USB Device is a Multifunction Printer

1. Move the cursor to Waiting to Connect and click on **Manage Device**.

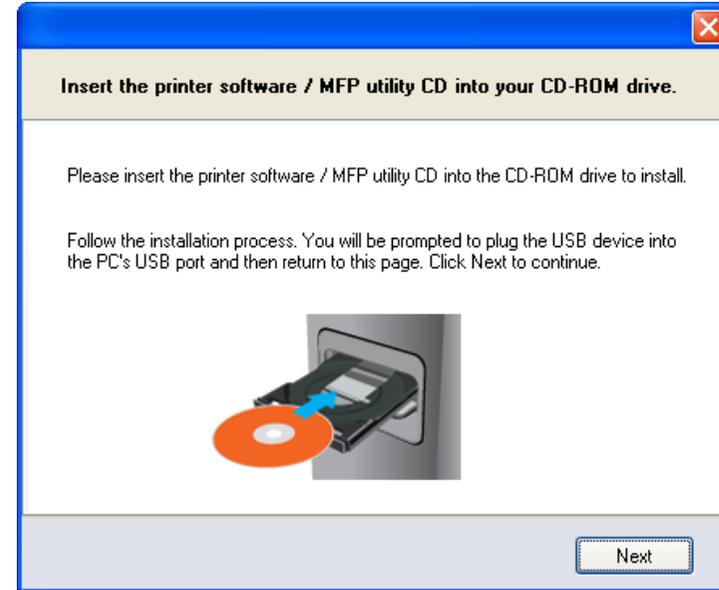


2. Click **Yes** on the question “Do you want to install the printer software or MFP utility?”

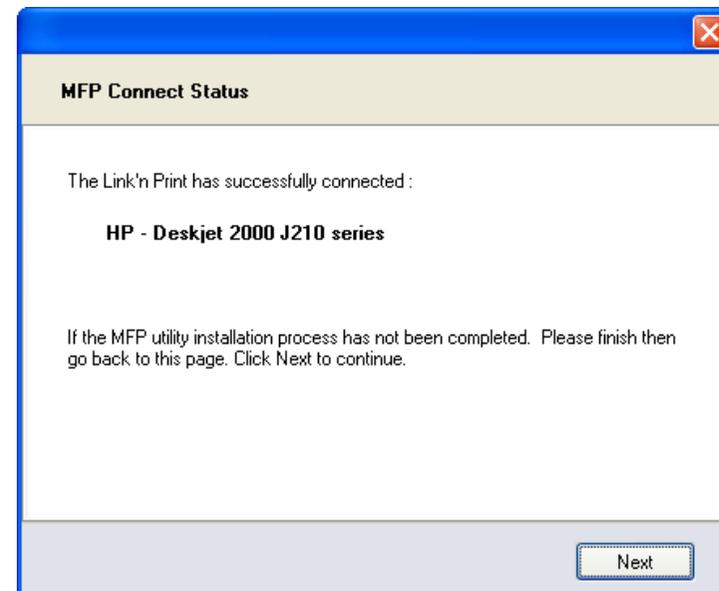


Appendix – F D-Link Link'n Print

3. Insert the CD-ROM of the multifunction printer and follow the instructions to install the multifunction printer's driver. When the installation process prompts you to connect the multifunction printer to your PC, click **Next**.

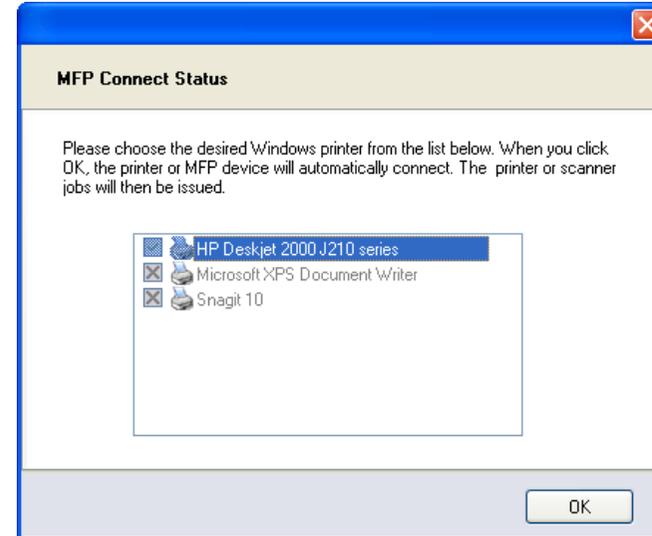


4. The D-Link Link'n Print virtually connects to this multifunction printer. Click **Next**



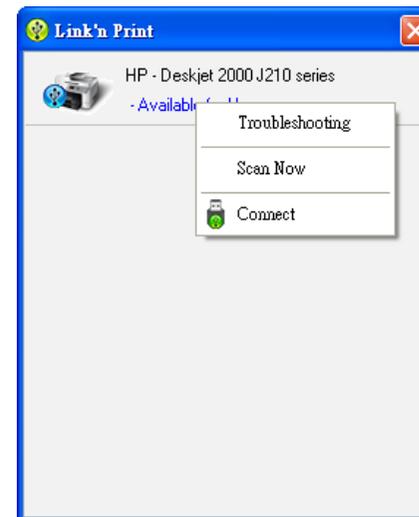
Appendix – F D-Link Link'n Print

5. Choose the printer driver that you want D-Link Link'n Print to auto-connect when you print.



When You Want to Scan

1. Move the cursor to Available for Use and click on **Scan Now**.



Technical Specifications

ADSL Standards

- ANSI T1.413 Issue 2
- ITU G.992.1 (G.dmt) AnnexA
- ITU G.992.2 (G.lite) Annex A

ADSL2 Standards

- ITU G.992.3 (G.dmt.bis) Annex A
- ITU G.992.4 (G.lite.bis) Annex A

ADSL2+ Standards

- ITU G.992.5 Annex A
- ITU G.992.5 Annex M

Protocols

- IEEE 802.1d Spanning Tree
- TCP/UDP
- ARP
- RARP
- ICMP
- RFC1058 RIP v1
- RFC1213 SNMP v1 & v2c
- RFC1334 PAP
- RFC1389 RIP v2
- RFC1577 Classical IP over ATM
- RFC1483/2684 Multiprotocol Encapsulation over ATM Adaptation Layer 5 (AAL5)
- RFC1661 Point to Point Protocol
- RFC1994 CHAP
- RFC2131 DHCP Client / DHCP Server
- RFC2364 PPP over ATM
- RFC2516 PPP over Ethernet

Data Rate

ADSL

- G.dmt: full rate downstream: up to 8 Mbps / upstream: up to 1 Mbps
- G.lite: downstream up to 1.5 Mbps / upstream up to 512 Kbps

ADSL2

- G.dmt.bis full rate downstream: up to 12 Mbps / upstream: up to 1 Mbps

ADSL 2+

- Full rate downstream: up to 24 Mbps / upstream: up to 1 Mbps
- Full rate downstream: up to 24 Mbps / upstream: up to 3 Mbps (Annex M)

Media Interface

- ADSL interface: RJ-11 connector for connection to 24/26 AWG twisted pair telephone line
- Giga Ethernet WAN interface: RJ-45 port for 10/100/1000 BASE-T Ethernet connection
- LAN interface: RJ-45 ports for 10/100/1000 BASE-T Ethernet connection

WIRELESS LAN

- 802.11ac/b/g/n standards
- Wireless speed:
 - 2.4GHz: up to 300Mbps (802.11n)
 - 5GHz: up to 866Mbps * (802.11ac; 2-antenna AP, 2-antenna STA, 80MHz)
- Frequency range:
 - 2.4GHz: 2.412 GHz to 2.472GHz
 - 5GHz: 5.150 GHz to 5.725 GHz
- Antennas: 2 internal antennas.
- WEP data encryption
- WPA/WPA2 (Wi-Fi Protected Access) security
- Multiple SSID
- 802.11e Wireless QoS (WMM/WME)
- MAC address-based access control

* Maximum wireless signal rate derived from IEEE Standard 802.11ac specifications. Actual data throughput will vary. Network conditions and environmental factors, including volume of network traffic, building materials and construction, and network overhead, lower actual data throughput rate.