FCC Notices

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.

**CAUTION:** Change or modification not expressly approved by the party responsible for compliance could void the user’s authority to operate this equipment.

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.

**RF exposure warning:**
The equipment complies with FCC RF exposure limits set forth for an uncontrolled environment. The equipment must not be co-located or operating in conjunction with any other antenna or transmitter.
# Table of Contents

## Overview
- Package Contents ........................................... 1
- System Requirements ........................................... 1
- Features ............................................................ 2
- Hardware Overview .............................................. 3
  - Rear Panel - Connections .................................. 3
  - Front Panel - LED Indicators ............................... 4
  - Right Side Panel - WPS Button ............................. 5

## Installation
- Before You Begin ............................................... 6
- Installation Notes ............................................... 6
- Information you will need from your ADSL service provider ......................................................... 8
- Information you will need about your Router ............. 9
- Information you will need about your LAN or computer ............................................................... 9
- Device Installation ............................................... 10
  - Power on Router .............................................. 10
  - Factory Reset Button ....................................... 10
  - Network Connections ...................................... 11

## Setup
- Web-based Configuration Utility ................................. 12
- Configure the Router ............................................ 13
- ADSL Setup - Setup Wizard .................................... 14
  - Setup Wizard Step 1: Change Password ............... 15
- Setup Wizard Step 2: Select Internet Connection Type .......................................................... 15
- Setup Wizard Step 2: Internet Connection Type, Country and ISP .............................................. 16
- Setup Wizard Step 3: Finish .................................... 16
- Setup Wizard Step 2: Internet Connection Type - Other Connection Types .................................. 17
- Setup Wizard Step 2: Internet Connection Type - PPPoE/PPPoA .................................................... 18
- Setup Wizard Step 3: Finish .................................... 18
- Setup Wizard Step 2: Internet Connection Type - Dynamic IP Address ........................................ 19
- Setup Wizard Step 3: Finish .................................... 19
- Setup Wizard Step 2: Internet Connection Type - Static IP Address .............................................. 20
- Setup Wizard Step 3: Finish .................................... 20
- Setup Wizard Step 2: Internet Connection Type - Bridge Mode ..................................................... 21
- Setup Wizard Step 3: Finish .................................... 21
- ADSL Setup - Manual Configuration ............................. 22
  - Manual ADSL Setup - PPPoE/PPPoA ...................... 23
  - Manual ADSL Setup - Dynamic IP Address ............ 24
  - Manual ADSL Setup - Static IP Address ................. 25
  - Manual ADSL Setup - Bridge Mode ....................... 26
  - Configure VPI and VCI ....................................... 27
  - ATM Traffic Shaping .......................................... 28

## Wireless Setup ................................................. 29
Table of Contents

<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Wireless Network Setup Wizard</td>
<td>30</td>
</tr>
<tr>
<td>Add Wireless Clients with WPS</td>
<td>33</td>
</tr>
<tr>
<td>WPS – Push Button method 1</td>
<td>33</td>
</tr>
<tr>
<td>WPS – Push Button method 2</td>
<td>34</td>
</tr>
<tr>
<td>WPS – Pin Code method</td>
<td>36</td>
</tr>
<tr>
<td>Getting the PIN number from the WPS Wireless Client</td>
<td>37</td>
</tr>
<tr>
<td>Manual Wireless Network Setup</td>
<td>38</td>
</tr>
<tr>
<td>Manually Set Up Wireless Network Security - WPA</td>
<td>39</td>
</tr>
<tr>
<td>Manually Set Up Wireless Network Security - WEP</td>
<td>40</td>
</tr>
<tr>
<td>LAN Setup</td>
<td>41</td>
</tr>
<tr>
<td>DHCP Server Configuration</td>
<td>42</td>
</tr>
<tr>
<td><strong>Advanced Setup</strong></td>
<td>43</td>
</tr>
<tr>
<td>Port Forwarding</td>
<td>44</td>
</tr>
<tr>
<td>DNS Setup</td>
<td>45</td>
</tr>
<tr>
<td>VLAN</td>
<td>46</td>
</tr>
<tr>
<td>Firewall &amp; DMZ</td>
<td>47</td>
</tr>
<tr>
<td>Advanced ADSL</td>
<td>48</td>
</tr>
<tr>
<td>Advanced Wireless</td>
<td>49</td>
</tr>
<tr>
<td>Wi-Fi Protected Setup</td>
<td>50</td>
</tr>
<tr>
<td>Wireless MAC Filter</td>
<td>51</td>
</tr>
<tr>
<td>Advanced LAN</td>
<td>52</td>
</tr>
<tr>
<td><strong>Maintenance</strong></td>
<td>53</td>
</tr>
<tr>
<td>Password</td>
<td>54</td>
</tr>
<tr>
<td>Save/Restore Settings</td>
<td>55</td>
</tr>
<tr>
<td><strong>Firmware Update</strong></td>
<td>56</td>
</tr>
<tr>
<td><strong>Diagnostics</strong></td>
<td>57</td>
</tr>
<tr>
<td><strong>System Log</strong></td>
<td>58</td>
</tr>
<tr>
<td><strong>Status</strong></td>
<td>59</td>
</tr>
<tr>
<td>Device Info</td>
<td>60</td>
</tr>
<tr>
<td>Connected Clients</td>
<td>61</td>
</tr>
<tr>
<td>Statistics</td>
<td>62</td>
</tr>
<tr>
<td><strong>Help</strong></td>
<td>63</td>
</tr>
<tr>
<td><strong>Technical Specifications</strong></td>
<td>64</td>
</tr>
</tbody>
</table>

D-Link DSL-2680 User Manual
Overview

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.

Package Contents

- DSL-2680 Wireless ADSL 2+ Ethernet Router
- Power Adapter
- CD-ROM with User Manual
- One twisted-pair telephone cable used for ADSL connection
- One straight-through Ethernet cable
- Quick Installation Guide

If any of the above items are missing, please contact your reseller.

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

System Requirements

- ADSL Internet service

  Computer with:
  - 200MHz Processor or faster
  - 64MB Memory or bigger
  - CD or DVD-ROM Drive
  - Ethernet Adapter with TCP/IP Protocol Installed
  - Internet Explorer v6.0 or later, Mozilla Firefox v1.0 or later, Safari 2.0 or later, Google Chrome 1.0 or later
  - Windows, Macintosh, or Linux-based operating system, with an installed Ethernet adapter
Chapter 1 - Overview

Features

- **PPP (Point-to-Point Protocol) Security** – The Router supports PAP (Password Authentication Protocol) and CHAP (Challenge Handshake Authentication Protocol) for PPP connections. The Router also supports MSCHAP.

- **DHCP Support** – Dynamic Host Configuration Protocol automatically and dynamically assigns all LAN IP settings to each host on your network. This eliminates the need to reconfigure every host whenever changes in network topology occur.

- **Network Address Translation (NAT)** – For small office environments, the Router allows multiple users on the LAN to access the Internet concurrently through a single Internet account. This provides Internet access to everyone in the office for the price of a single user. NAT improves network security in effect by hiding the private network behind one global and visible IP address. NAT address mapping can also be used to link two IP domains via a LAN-to-LAN connection.

- **TCP/IP (Transfer Control Protocol/Internet Protocol)** – The Router supports TCP/IP protocol, the language used for the Internet. It is compatible with access servers manufactured by major vendors.

- **Default Routing** – This allows you to choose a default path for incoming data packets for which the destination address is unknown. This is particularly useful when/if the Router functions as the sole connection to the Internet.

- **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.

- **Easy Installation** – The Router uses a Web-based graphical user interface program for convenient management access and easy set up. Any common Web browser software can be used to manage the Router.
Hardware Overview

Rear Panel - Connections

- **ADSL Port**: Use the ADSL cable to connect to your telephone line (RJ-11 port).
- **Power Receptacle**: Use the adapter shipped with the Router to connect to the power source.
- **Power On/Off Button**: Use this button to power the Router on and off.
- **Ethernet Ports**: Use the Ethernet ports to connect the Router to a computer or an Ethernet LAN.
- **Reset Button**: To manually reset the Router to factory settings, depress button with the power on for about 6 to 8 seconds.
Front Panel - LED Indicators

**Internet**
A solid green light indicates that the WAN IP address from IPCP or DHCP and DSL is up, or a static IP address is configured and PPP negotiation has been successfully completed. If the indicator blinks green, this means the Router is active. If the Router power is off, this remains dark. A solid red light indicates there is no DHCP response, no PPPoE response, PPPoE authentication has failed, or there is no IP.

**Power**
A steady green light indicates the unit is powered on. This remains dark when power is off. A red colored LED indicates system failure.

**LAN**
A solid green light indicates a valid link on startup. This light will blink when there is activity currently passing through the Ethernet port.

**DSL**
A steady green light indicates a valid ADSL connection. This will light after the ADSL negotiation process has been settled. A blinking green light indicates the ADSL line is in the process of synchronizing.

**WLAN**
A steady green indicates a wireless connection. A blinking green light indicates activity on the wireless LAN interface.

**WPS**
A steady green light indicates a connection has been successfully established between the Router and the client. The LED will remain solid for 5 seconds. This light will blink when WPS is successfully triggered. A dark light means the device is ready for new WPS setup.
Chapter 1 - Overview

Right Side Panel - WPS Button

Note: For instructions on how to use the WPS button, please see “Wi-Fi Protected Setup” on page 50.
Chapter 2 - Installation

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. Place the Router in a location where it can be easily connected to Ethernet devices, the telephone line, and a power source.

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 set up 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 a standard telephone cable. Ask your service provider for more information about the use of low pass filters with your installation.

Operating Systems
The Router uses an HTML-based Web interface for setup and management. The Web configuration manager may be accessed using any operating system capable of running Web browser software, including Microsoft Windows 98 SE, Windows ME, Windows 2000, Windows XP, Windows Vista, Windows 7, and Macintosh Mac OSX.

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 Internet Explorer v6.0 or later, Mozilla Firefox v1.0 or later, Safari 2.0 or later, and Google Chrome 1.0 or later. 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. The 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 need to install an adapter, follow the installation instructions that come with the Ethernet NIC adapter.
Chapter 2 - Installation

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 as 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.

Wireless LAN
Computers using the wireless network can access the Internet using the embedded wireless access point. Wireless workstations must have an 802.1n, 802.1g, or 802.1b wireless network card installed to use the Router. In addition, the workstation must be configured to operate on the same channel and SSID as the Router. If wireless security is used, the wireless workstations must be properly configured for the security settings used.
Information you will need from your ADSL service provider

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

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

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

- PPPoE/PPPoA (PPPoE LLC, PPPoE VC-Mux, PPPoA LLC, or PPPoA VC-Mux)
- Bridge Mode (1483 Bridged IP LLC or 1483 Bridged IP VC Mux)
- Static IP Address (1483 Bridged IP LLC, 1483 Bridged IP VC Mux, 1483 Routed IP LLC (IPoA), or 1483 Routed IP VC-Mux)
- 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 (Auto Synch-Up) used for the Router automatically detects all types of ADSL, ADSL2 and ADSL2+ modulation.

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

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

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

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

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

**LAN IP addresses for the Router**
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 Router**
This is the subnet mask used by the Router 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 Router to the Ethernet port using an Ethernet cable. You can also use the Ethernet ports on the Router to connect to other computers or Ethernet devices.

**DHCP Client status**
Your 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 Router 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 set up and configure your Router.
Chapter 2 - Installation

Device Installation

The Router maintains three separate physical interfaces, an ADSL, an Ethernet, and a wireless Interface. Place the Router in a location where it can be easily connected to Ethernet devices, the telephone line, and a power source. The Router should not be located where it will be exposed to moisture or excessive heat. Make sure the cables and power cord are placed safely out of the way so they do not create a tripping hazard. As with any electrical appliance, observe common sense safety procedures.

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

Power on Router

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

1. Connect the Power Adapter to the power receptacle located on the rear panel of the Router and plug the other end of the power adapter to a wall outlet or power strip.
2. Depress the Power button into the on position. You should see the Power LED indicator on the front panel shine bright green to indicate the device is powered on.
3. If the Ethernet port is connected to a working device, check the LAN LED indicator 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 you have installed 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. With the Router powered on (check the Power LED to make sure it lights steady green), press and hold down the reset button using a paper clip or similar object for about 6 to 8 seconds.
2. The Router will restart. Watch the Power LED to verify that it is restarting.
3. When it is powered on again it is ready to be configured. The whole process takes about 30 seconds.
4. 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.”

Note: A factory reset will erase the current configuration settings and reset them to the default settings. After it has restarted, log in to the router’s Web-based management interface and use the Setup Wizard to configure the basic settings.
Network Connections

Connect ADSL Line
Use the ADSL cable included with the Router to connect it to a telephone wall socket or receptacle. Plug one end of the cable into the ADSL port (RJ-11 receptacle) on the rear panel of the Router and insert the other end into the RJ-11 wall socket. If you are using a low pass filter device, follow the instructions included with the device or the instructions 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 10/100 BASE-TX Ethernet port on the rear panel. Any connection to an Ethernet concentrating device such as a switch or hub must operate at a speed of 10/100 Mbps only. When connecting the Router to any Ethernet device that is capable of operating at speeds higher than 10Mbps, be sure that the device has auto-negotiation (NWay) enabled for the connecting port. Use standard twisted-pair cabling with RJ-45 connectors. The RJ-45 port on the Router is a crossed port (MDI-X). Follow standard Ethernet guidelines when deciding what type of cable to use to make this connection. When connecting the Router directly to a PC or server use a normal straight-through cable. You should use a crossed cable when connecting the Router to a normal (MDI-X) port on a switch or hub. Use a normal straight-through cable when connecting it to an uplink (MDI-II) port on a hub or switch. The rules governing Ethernet cable lengths apply to the LAN to Router connection. Be sure that the cable connecting the LAN to the Router does not exceed 100 meters.

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

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

Wireless Connection to Router
The Router’s embedded 802.11b/g/n wireless access point should be configured to suit the local wireless network. All 802.11b/g/n devices that associate with the Router’s wireless access point must have the same SSID and channel. If wireless security is used, the wireless clients must be configured with the correct security information to use the Router. More information on configuring the wireless settings is found later in this manual.
Chapter 3 - Setup

Setup

This section will show you how to set up and configure your new D-Link router using the Web-based configuration utility.

Web-based Configuration Utility

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 v6.0 or later, Mozilla Firefox v1.0 or later, Safari 2.0 or later, or Google Chrome 1.0 or later and enter the IP address of the Router (default is 192.168.1.1).

The login dialog box will appear:

1. Type admin in the User Name field.
2. Enter admin in the Password field.
3. Click the OK button to log into the Router.
Configure the Router

When you successfully connect to the Web manager, the main ADSL Setup menu is displayed. Use this menu to configure the WAN settings for Internet connection.

All configuration and management of the Router is done using the Web-based management interface pictured in the example. The Setup Wizard is recommended for most users. It allows you to configure the basic settings for the ADSL Internet connection and Ethernet (including DHCP) settings. To launch the Setup Wizard click on the Setup Wizard button.

Note: The Setup Wizard is the easiest and quickest way to configure the Internet connection for most users.
Chapter 3 - Setup

ADSL Setup - Setup Wizard

The quickest way for most users to establish the Internet connection is to use the Setup Wizard accessed from the ADSL Setup menu. Alternatively the WAN connection can be set up manually by selecting the Manual Setup option and using the ADSL Setup menu to configure the device (described in ADSL Setup – Manual Configuration below).

Go to the Setup directory to view the ADSL Setup menu.

To use the Setup Wizard, click the Setup Wizard button in the first browser menu and follow the instructions in the menus that appear.

The initial menu summarizes the setup process. Click the Next button to proceed. You may stop using the Setup Wizard at any time by clicking the Cancel button. If you exit the wizard you will return to the ADSL Setup menu without saving any of the settings changed during the process.

The first menu of the Setup Wizard lists the basic steps in the process. These steps are as follows:

1. Change the Router's login password.
2. Configure the Internet connection
3. Finish.

Click Next to continue configuring the Router.
Chapter 3 - Setup

Setup Wizard Step 1: Change Password

The password used for management access of the Router can be changed now if desired. If you prefer to keep the existing password, click on the Skip button to go to the next step without changing the password. Change the password and click Next to set the new password and continue or click Skip to keep the existing password.

<table>
<thead>
<tr>
<th>SETUP</th>
<th>ADVANCED</th>
<th>MAINTENANCE</th>
<th>STATUS</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image" alt="Change Password Form" /></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Setup Wizard Step 2: Select Internet Connection Type

The new menu that appears is used to select the Internet connection type. Choose your Country from the pull-down menu. If you see your country listed, follow the instructions beginning on the next page. If you do not see your country listed, choose Others and click Next, skip ahead to Setup Wizard Step 2: Internet Connection – Other Connection Types.

<table>
<thead>
<tr>
<th>SETUP</th>
<th>ADVANCED</th>
<th>MAINTENANCE</th>
<th>STATUS</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image" alt="Select Internet Connection Form" /></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Setup Wizard Step 2: Internet Connection Type, Country and ISP

If your country appears listed in the Country menu options, select it and wait a few seconds for the menu display to adjust. When the menu options reappear, there will be options available to choose in the ISP Provider pull-down menu. Find your ISP in the list, again the menu will be inoperable for a few seconds while it adjusts. Some users will be required to select the Connection Type as well. If necessary, choose the Connection Type and click the Next button and continue to configure the connection as instructed by your ISP. If you are configuring a Bridged connection, the Wizard will go to the Finish menu.

Many users will use a form of PPP connection. PPP connections require a Username and Password to establish the Internet connection.

Setup Wizard Step 3: Finish

After configuring the connection as instructed by your ISP, the Router will need to be restarted.

Click the Finish button to save the configuration and restart the Router.
Setup Wizard Step 2: Internet Connection Type - Other Connection Types

ADSL clients whose country is not listed as an option in the Country menu should choose Others. Click the Next button and proceed to configure the Router as instructed by your ISP.

Choosing the Others option will disable the VPI/VCI and Connection Type menus. Click Next to choose the type of connection used for your account.

Select the connection type used by your ISP and click the Next button.
Setup Wizard Step 2: Internet Connection Type - PPPoE/PPPoA

Type in the Username and Password used to identify and verify your account to the ISP.

If you are instructed to change the VPI or VCI number, type in the correct setting in the available entry fields. Most users will not need to change these settings. The Internet connection cannot function if these values are incorrect.

Some users may have to adjust the Connection Type from the drop-down menu.

Click Next to go to the last Setup Wizard menu.

Setup Wizard Step 3: Finish

Click the Finish button to save the configuration and restart the Router.
Chapter 3 - Setup

Setup Wizard Step 2: Internet Connection Type - Dynamic IP Address

If you are instructed to change the VPI or VCI numbers, type in the correct setting in the available entry fields. Most users will not need to change these settings. The Internet connection cannot function if these values are incorrect.

Select the specific **Connection Type** from the drop-down menu. You may want to copy the MAC address of your Ethernet adapter to the Router. Some ISPs record the unique MAC address of your computer’s Ethernet adapter when you first access their network. This can prevent the Router (which has a different MAC address) from being allowed access to the ISPs network (and the Internet). To clone the MAC address of your computer’s Ethernet adapter, type in the MAC address in the **Cloned MAC Address** field and click the **Clone MAC Address** button. This will copy the information to a file used by the Router to present to the ISP’s server used for DHCP.

Click **Next** to go to the last **Setup Wizard** menu.

---

**STEP 2: SELECT INTERNET CONNECTION TYPE**

You have selected Dynamic IP Internet connection. Please enter the appropriate information below as provided by your ISP.

Some ISPs require that you clone your PC MAC address to the DSL router, simply Click on the button provided.

Click Next to continue.

- **VPI:** 8
- **VCI:** 35
- **Connection Type:** 1483 Bridged IP LLC
- **Cloned MAC Address:** 00:00:00:00:00:00

Click **Clone MAC Address**

---

Setup Wizard Step 3: Finish

Click the **Finish** button to save the configuration and restart the Router.

---

**STEP 3: FINISH**

Setup complete. Click Back to review or modify settings. Click Finish to apply current settings. If your Internet connection does not work after apply the settings, you can try the Setup Wizard again with alternative settings or use Manual Setup instead if you have your Internet connection details as provided by your ISP.
Chapter 3 - Setup

Setup Wizard Step 2: Internet Connection Type - Static IP Address

Change the **IP Address, Subnet Mask, and Default Gateway** as instructed by your ISP. Select the specific **Connection Type** from the drop-down menu.

If you are instructed to change the **VPI** or **VCI** numbers, type in the correct setting in the available entry fields. Most users will not need to change these settings. The Internet connection cannot function if these values are incorrect.

Click **Next** to go to the last **Setup Wizard** menu.

![STEP 2: SELECT INTERNET CONNECTION TYPE](image)

**STEP 2: FINISH**

Setup complete. Click **Back** to review or modify settings. Click **Finish** to apply current settings. If your Internet connection does not work after apply the settings, you can try the Setup Wizard again with alternative settings or use Manual Setup instead if you have your Internet connection details as provided by your ISP.

Click the **Finish** button to save the configuration and restart the Router.

![STEP 3: FINISH](image)
Chapter 3 - Setup

Setup Wizard Step 2: Internet Connection Type - Bridge Mode

Select the specific Connection Type from the drop-down menu.

If you are instructed to change the VPI or VCI numbers, type in the correct setting in the available entry fields—in this example no changes are needed so this setting is grayed out. Most users will not need to change these settings. The Internet connection cannot function if these values are incorrect.

Click Next to go to the last Setup Wizard menu.

Setup Wizard Step 3: Finish

Click the Finish button to save the configuration and restart the Router.
ADSL Setup - Manual Configuration

To configure the Router’s basic configuration settings without running the Setup Wizard, you can access the menus used to configure ADSL Setup, Wireless Setup, and LAN Setup settings directly from the Setup directory. To access the ADSL Setup menus for PPPoE/PPPoA, Dynamic IP Address, Static IP Address and Bridge Mode connections, click on the ADSL Setup link button on the left side of the first menu that appears when you successfully access the Web manager.

Choose the ADSL connection type used for your service listed under the heading Manual ADSL Connection Setup, the menu changes according to the type of connection to be configured. Configure the settings for the chosen Internet Connection Type. Follow the instructions presented below for the type of connection used for your ADSL service. The default Internet connection type is PPPoE/PPPoA.

**Note:** Most users DO NOT need to change configuration settings for the Virtual Circuit at the bottom of this menu. Normally these settings are changed only for special circumstances and applications. Do not change these unless your ISP has given specific instructions to do so.

For information about these configuration settings, go to “Configure VPI and VCI” on page 27.
Manual ADSL Setup - PPPoE/PPPoA

Follow the instructions below to configure the Router to use a PPPoE or PPPoA for the Internet connection. Most users will only need to change some or all of the settings listed under WAN Connection Setting and PPPoE/PPPoA.

To configure a PPPoE or PPPoA type WAN connection, follow these steps:

1. Under the PPPoE/PPPoA heading, type the Username and Password used for your ADSL account. A typical Username will be in the form user1234@isp.co.uk. The Password may be assigned to you by your ISP or you may have selected it when you set up the account with your ISP.

2. Choose the Connection Type from the pull-down menu located under the User Name and Password entry fields. This defines both the connection protocol and encapsulation method used for your ADSL service. The available options are PPPoA VC-Mux, PPPoA LLC, PPPoE VC-Mux and PPPoE LLC. If you have not been provided specific information for the Connection Type setting, leave the default setting.

3. Leave the MTU value at the default setting (default = 1450) unless you have specific reasons to change this.

4. For time-based accounts, type an Idle Time Out in minutes. Accounts that are not time-based will want to choose the default connection setting 0=Always ON.

5. The default setting Auto for Authentication will work for most users. If instructed to change by your ISP, this can be changed to specify the authentication method used, select PAP or CHAP as instructed.

6. NAT (Network Address Translation) should remain Enable. If you disable NAT, you will not be able to use more than one computer for Internet connections.

7. Most users should leave the IGMP setting as Enable. IGMP is used to manage multicasts (such as audio or video streaming). Some network managers might prefer to disable this function to prevent certain types of DoS attacks. To disable IGMP select Disable. This will block all IP multicast traffic through the Router.

8. Leave the Default Route enabled if you want to use the Router as the default route to the Internet for your LAN. Whenever a computer on the LAN attempts to access the Internet, the Router becomes the Internet gateway to the computer. If you have an alternative route for Internet traffic you may disable this without effecting the Router’s connection.

9. Click the Save Settings button at the bottom of the menu to apply and save the new ADSL configuration.

Note: Use the Connect button at the bottom of the menu to reestablish the PPP connection if it is not connected automatically when the router is restarted. Press Disconnect to terminate the Internet connection.
Manual ADSL Setup - Dynamic IP Address

Follow the instructions below to configure the Router to use a Dynamic IP Address for the Internet connection.

To configure a Dynamic IP Address connection, follow these steps:

1. Choose the **Connection Type** from the pull-down menu. This defines both the connection type and encapsulation method used for your ADSL service. The available options are **1483 Bridged IP LLC** and **1483 Bridged IP VC Mux**. If you have not been provided specific information for the Connection Type setting, leave the default setting.

2. Some ISPs record the unique MAC address of your computer’s Ethernet adapter when you first access their network. This can prevent the Router (which has a different MAC address) from being allowed access to the ISPs network (and the Internet). To clone the MAC address of your computer’s Ethernet adapter, type in the MAC address in the **MAC Address** field and click the **Clone MAC Address** button.

3. **NAT** should remain **Enable**. If you disable NAT, you will not be able to use more than one computer for Internet connections. NAT is enabled and disabled system-wide, therefore if you are using multiple virtual connections, NAT will be disabled on all connections.

4. Most users should leave the **IGMP** setting as **Enable**. IGMP is used to manage multicasts (such as audio or video streaming). Some network managers might prefer to disable this function to prevent certain types of DoS attacks. To disable IGMP select **Disable**. This will block all IP multicast traffic through the router.

5. Leave the **Default Route** enabled if you want to use the Router as the default route to the Internet for your LAN. Whenever a computer on the LAN attempts to access the Internet, the Router becomes the Internet gateway to the computer. If you have an alternative route for Internet traffic you may disable this without effecting the Router’s connection.
Manual ADSL Setup - Static IP Address

Follow the instructions below to configure the Router to use a Static IP Address for the Internet connection.

To configure a Static IP type connection for the WAN, follow these steps:

1. Choose the **Connection Type** from the pull-down menu. This defines both the connection type and encapsulation method used for your ADSL service. The available options are **1483 Bridged IP LLC**, **1483 Bridged IP VC-Mux**, **1483 Routed IP LLC**, and **1483 Routed IP VC-Mux**. If you have not been provided specific information for the Connection Type setting, leave the default setting.

2. Change the **IP Address**, **Subnet Mask**, and **Default Gateway** address as instructed by your ISP. These are the global IP settings for the WAN interface. This is the “visible” IP address of your account.

3. **NAT** should remain **Enable**. If you disable NAT, you will not be able to use more than one computer for Internet connections. NAT is enabled and disabled system-wide, therefore if you are using multiple virtual connections, NAT will be disabled on all connections.

4. Most users should leave the **IGMP** setting as **Enable**. IGMP is used to manage multicasts (such as audio or video streaming). Some network managers might prefer to disable this function to prevent certain types of DoS attacks. To disable IGMP select **Disable**. This will block all IP multicast traffic through the router.

5. Leave the **Default Route** enabled if you want to use the Router as the default route to the Internet for your LAN. Whenever a computer on the LAN attempts to access the Internet, the Router becomes the Internet gateway to the computer. If you have an alternative route for Internet traffic you may disable this without effecting the Router’s connection.
Manual ADSL Setup - Bridge Mode

Follow the instructions below to configure the Router to use Bridge Mode for the Internet connection.

To configure a Bridge Mode connection, choose the **Connection Type** from the pull-down menu. This defines both the connection type and encapsulation method used for your ADSL service. The available options are *1483 Bridged IP LLC* or *1483 Bridged IP VC-Mux*. If you have not been provided specific information for the Connection Type setting, leave the default setting.

<table>
<thead>
<tr>
<th>Connection Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>1483 Bridged IP LLC</td>
</tr>
<tr>
<td>1483 Bridged IP VC-Mux</td>
</tr>
</tbody>
</table>
Configure VPI and VCI

Follow the instructions below to configure the virtual connection.

To configure the virtual connection, follow these steps:
1. Enter the values for the VPI and VCI given to you by your service provider.
2. Select Enable from the Virtual Circuit pull-down menu to make the connection active. If you prefer to leave the connection inactive leave this as Disable, and activate it when it is needed.
3. Choose the type of connection used for the virtual connection and configure the settings according to the instructions of your service provider.
4. Click the Save Settings button to save the configuration. If you want to establish the connection now, click the Connect button.

VPI - The Virtual Path Identifier is used with the VCI to define a dedicated circuit on the ATM network portion of the connection to the Internet and WAN. Most users will not need to change this setting.
VCI - The Virtual Channel Identifier is used with the VPI to define a dedicated circuit on the ATM network portion of the connection to the Internet and WAN. Most users will not need to change this setting.
Virtual Circuit - Use this to enable or disable the PVC you are currently configuring. By default, the PVC0 is set to Enable.
Chapter 3 - Setup

ATM Traffic Shaping

Settings used for ATM traffic shaping are located beneath the VPI/VCI configuration menu. These settings allow the user to adjust ATM Quality of Service (QoS) or traffic parameters to suit specific traffic requirements. For applications or circumstances where packet loss or packet delay is a concern, ATM QoS can be adjusted to minimize problems. For most accounts, it will not be necessary to change these settings. Altering QoS settings can adversely affect performance of some commonly used Internet applications.

If you plan to change QoS or traffic parameters, contact your ISP or network services provider for information on what types of adjustment are available or possible for your account. Your ISP may not support the class of service you want to use.

To adjust ATM QoS parameters, select one of the Service Categories listed here and type in the PCR value in the entry field below. For the VBR service category, an additional parameter (SCR) must also be defined.

- **UBR** – Unspecified Bit Rate, this is the default category used for general-purpose Internet traffic where normal levels of packet loss and delay are acceptable. For some applications or for multiple connection accounts, it may be desirable to specify the PCR.
- **CBR** – Constant Bit Rate, usually used in circumstances where very low packet loss and very low Cell Delay Variable (CDV) are desirable.
- **VBR-rt** – Real-time Variable Bit Rate. This models bursty traffic with specified peak and sustainable rates. Please note that when VBR-rt is specified, both PCR and SCR are required (by ATM standards).
- **VBR-nrt** – Non-real-time Variable Bit Rate, usually used when network traffic is characterized by bursts of packets at variable intervals, and some moderate packet loss and delay is acceptable. This category is typically used for audio and video applications such as teleconferencing. The network must support QoS Class 2 to use VBR-nrt.

Depending on which **Service Category** is selected, it will be necessary to change one or more of the following parameters:

- **PCR** - Peak Cell Rate – The PCR is inversely related to the time interval between ATM cells. It is specified for all three service categories (UBR, CBR and VBR) in Kbps.
- **SCR** - Sustainable Cell Rate – The SCR is defined for the VBR service category. This is the rate that can be sustained for “bursty”, on-off traffic sources. It is a function of Maximum Burst Size (MBS) and the time interval (between cells).
Chapter 3 - Setup

Wireless Setup

The Router’s basic wireless and wireless network security settings are configured in the Wireless Settings configuration menu. To access this menu, click on the Wireless Setup link in the left panel of the Setup menu directory. It is the first page that appears when you successfully access the Web manager.

The Wireless Settings menu presents three options for configuration. Choose from one of the three following configuration procedures:

1. Launch the Wireless Network Setup Wizard to configure the Network Name (SSID) and WPA wireless network security. Click the Wireless Network Setup Wizard button to begin. This option is recommended for most users.


2. Use the WPS (Wi-Fi Protected Setup) Wizard to add individual wireless clients. Click the Add Wireless Device with WPS button to use begin configuration with WPS.

   Note: Wireless clients added to using this method must support WPS.

3. Configure the SSID, channel and wireless network security settings manually. Click the Manual Wireless Network Setup button to go to the general wireless network settings menu.

---

**Wireless Settings**

The following Web-based wizards are designed to assist you in your wireless network setup and wireless device connection.

---

**Wireless Network Setup Wizard**

This wizard is designed to assist you in your wireless network setup. It will guide you through step-by-step instructions on how to set up your wireless network and how to make it secure.

---

**Add Wireless Device with WPS (Wi-Fi Protected Setup) Wizard**

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

---

**Manual Wireless Network Setup**

If your wireless network is already set up with Wi-Fi Protected Setup, manual configuration of the wireless network will destroy the existing wireless network. If you would like to configure the wireless settings of your new D-Link Systems Router manually, then click on the Manual Wireless Network Setup button below.
Click on the **Wireless Network Setup Wizard** button in the **Wireless Settings** menu to begin configuration of basic wireless network settings and WPA wireless network security.

In the first Wireless Setup Wizard menu, enter the name used for the wireless network in the **Network Name (SSID)** entry field. The **SSID** or Service Set Identifier is the name used for the wireless network or a part of the wireless network. Wireless clients must use this SSID in order to access the wireless network and use the Router.

To configure WPA wireless network security, the Wizard menu offers two options. The easiest and recommended method will configure WPA network key automatically. To automatically configure WPA network security, choose the option **Automatically assign a network key** and click on the **Next** button to complete the wireless configuration. The new **Pre-Shared Key** and WPA wireless security settings are displayed in the **Setup Complete!** menu. For later reference, be sure to print this menu; or copy the new automatically created Pre-Shared Key and paste it into a document to be saved. Click on the **Save** button to save the new wireless settings. The automatically created pre-shared key is randomly generated.

**Note:** For future reference, print out the **Setup Complete!** wizard menu that lists the **SSID**, **Security Mode**, **Cipher Type**, and most importantly, the **Pre-Shared Key**.

To manually enter the WPA network key, click the **Manually assign a network key** option and click on the **Next** button. (See the description beginning on the next page.)
To configure a WPA network security key manually using the **Wireless Network Setup Wizard**, first enter the name used for the wireless network in the **Network Name (SSID)** entry field, then choose the **Manually assign a network key** option and click on the **Next** button.

### STEP 1: WELCOME TO THE D-LINK WIRELESS SECURITY SETUP WIZARD

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

| Network Name (SSID) : | D-Link |

- **Automatically assign a network key (Recommended)**
  - To prevent outsiders from accessing your network, the router will automatically assign a security to your network.

- **Manually assign a network key**
  - Use this option if you prefer to create your own key.

**Note:** All D-Link wireless adapters currently support WPA.

In the new menu, type the **Wireless Security Password** used for wireless network access in the space provided. WPA password or network pre-shared key must be a character string of 8 to 64 alphanumeric characters (alphanumeric characters are standard keyboard characters A-Z, a-z and 0-9); or enter exactly 64 hexadecimal characters (hexadecimal characters are numbers 0-9 and alphabet letters A-F and are not case specific). Click the **Next** button to go to the final wizard menu.

**Note:** Choose a password that is easy to remember but difficult for others to guess.
The new **Pre-Shared Key** and WPA wireless security settings are displayed in the **Setup Complete!** menu. For later reference, be sure to print this menu; or copy the new Pre-Shared Key and paste it into a document to be saved. Click the **Save** button to save the new wireless settings.

**Note:** For future reference, print out the **Setup Complete!** wizard menu that lists the **SSID**, **Security Mode**, **Cipher Type**, and most importantly, the **Pre-Shared Key**.
Add Wireless Clients with WPS

The Router supports WPS (Wi-Fi Protected Setup). WPS is a standard for easy and secure establishment of a wireless network. With WPS you can setup and protect your wireless network in just a few easy steps.

**Note:** To use WPS with the Router, you need to have wireless clients that support WPS. If you have one or more Wireless Clients without WPS support, it is advised to secure your network manually using the Setup Wizard.

The Router supports two ways to activate and establish a WPS connection:

- Push Button method
- Pin Code technology

### WPS – Push Button method 1

The WPS Push Button technology requires a (virtual) button on your Wireless Client to establish a connection between the Router and your Wireless Client. Some Wireless Clients work with a real button to activate the WPS Push Button technology; some Wireless Clients use a software-based virtual button.

Follow the steps below to activate and establish a WPS connection with the Push Button technology:

1. Press the WPS Button at the right side of the Router, the button will blink green.
2. Press the WPS Button at your wireless client. This can be a hardware button or a virtual button in the software of your wireless client. The Router will activate WPA security over your wireless network and accepts the wireless connection of your Wireless Client.

**Note:** The Router will keep the WPS authentication active for up to 120 seconds or until the connection is established. During this process, the WPS button will blink green. If there is no connection in these 120 seconds, the button stops blinking and the WPS authentication process is stopped.

3. If the authentication of the wireless client succeeds, the WPS button on the router will stop blinking and go dark. Test the wireless client to make sure it is now connected to the Router. Repeat this procedure to add more WPS wireless clients. A successful WPS connection means the wireless client is able to use the router and the wireless network is secured with WPA encryption.

**Note:** The WPA Key generated by the Router is random.
WPS – Push Button method 2

The WPS Push Button technology requires a (virtual) button on your Wireless Client to establish a connection between the Router and your Wireless Client. Some Wireless Clients work with a real button to activate the WPS Push Button technology; some Wireless Clients use a software-based virtual button.

Follow the steps below to activate and establish a WPS connection with the Push Button technology:

1. Click on the **Add Wireless Device with WPS** button in the **Wireless Settings** menu to launch the **WPS (Wi-Fi Protected Setup) Wizard**. Choose the **Auto** option and click on the **Next** button.

   **STEP 1: SELECT CONFIGURATION METHOD FOR YOUR WIRELESS NETWORK**

   Please select one of following configuration methods and click next to continue.

   - **Auto** Select this option if your wireless device supports WPS (Wi-Fi Protected Setup)
   - **Manual** Select this option will display the current wireless settings for you to configure the wireless device manually

   ![Configuration Options]

   **Note**: *Click the Manual option to go to the manual configuration menu for wireless settings.*

2. Choose the **PBC** option and click **Connect**.

   **STEP 2: CONNECT YOUR WIRELESS DEVICE**

   There are two ways to add wireless device to your wireless network:
   - **PIN** (Personal Identification Number)
   - **PBC** (Push Button Configuration)

   - **PIN**: please enter the PIN from your wireless device and click the below 'Connect' Button
   - **PBC**: please press the push button on your wireless device and click the below 'Connect' Button within 120 seconds

   ![Connection Options]
3. You are now prompted to connect to the client using WPS. You have 120 seconds to establish the link.

![STEP 2: CONNECT YOUR WIRELESS DEVICE](image)

You have 120 seconds to establish the link. Press the WPS button (or virtual button) on your wireless client. This can be a hardware button or a virtual button in the WPS software of your wireless client (see example below).

4. Press the WPS button (or virtual button) on your wireless client. This can be a hardware button or a virtual button in the WPS software of your wireless client (see example below).

![D-Link Wi-Fi Protected Setup](image)

5. A successful WPS connection means the wireless client is able to use the Router and the wireless network is secured with WPA encryption. Test the wireless client to make sure it is now connected to the Router. Repeat this procedure to add more WPS wireless clients.

*Note: The WPA Key generated by the Router is random.*
WPS – Pin Code method

Follow the steps below to use the PIN Code method to establish a WPS connection to a WPS wireless client.

1. Click on the Add Wireless Device with WPS button in the Wireless Settings menu to launch the WPS (Wi-Fi Protected Setup) Wizard. Choose the Auto option and click on the Next button.

   ![STEP 1: SELECT CONFIGURATION METHOD FOR YOUR WIRELESS NETWORK]

   Please select one of following configuration methods and click next to continue.

   Auto ☑ Select this option if your wireless device supports WPS (Wi-Fi Protected Setup)
   Manual ☑ Select this option will display the current wireless settings for you to configure the wireless device manually

2. In the next menu it is necessary to enter a PIN code that is generated by the wireless client. If the client has a software utility such as a Setup Wizard, this is used to generate the PIN code for the device. (See the example on the next page).

   ![STEP 2: CONNECT YOUR WIRELESS DEVICE]

   There are two ways to add wireless device to your wireless network:
   - PIN (Personal Identification Number)
   - PBC (Push Button Configuration)

   ⚫ PIN:
   please enter the PIN from your wireless device and click the below ‘Connect’ Button

   ⚫ PBC:
   please press the push button on your wireless device and click the below ‘Connect’ Button within 120 seconds

3. Choose the PIN option and enter the PIN code obtained from the wireless client (see example below) in the space provided and click Connect.

4. The Router will activate WPA security on your wireless network and accept the connection of your wireless client with the PIN code just entered.
Getting the PIN number from the WPS Wireless Client

For example, the D-Link client Wi-Fi Protected Setup Wizard includes an option to use the PIN code method. The generated PIN number appears in a menu screen like those pictured here:
Enable Wireless – Left-click on this box to enable Wireless Network function for the Router. A tick in the check box indicates the wireless network is enabled. To disable wireless function, left-click on the box to remove the tick.

Wireless Network Name (SSID) - The Wireless Network Name or SSID can be changed to suit your wireless network. Remember that any wireless device must have the same SSID and use the same channel in order to use the router. The SSID can be a continuous character string (i.e. no spaces) of up to 16 characters in length.

Enable Auto Channel Scan – Enable this to allow the access point to automatically detect the channel used for local 802.11 wireless operation. This can be used if there are other wireless access points within range operating on the wireless network.

Wireless Channel – The Wireless Channel may be changed to channels that are available in your region. Channels available for wireless LAN communication are subject to regional and national regulation. Remember that any wireless device must have the same SSID and use the same channel in order to use the Router.

802.11 Mode – The default setting is simultaneous 802.11b, 802.11g, and 802.11n compatible operation. The access point can be forced to operate as an 802.11b only, 802.11g only, or 802.11n access point if preferred. Additional options are 802.11b plus 802.11g or 802.11g plus 802.11n.

Hide Wireless Network – When enabled, this stops broadcasts from the access point of the SSID (Wireless Network Name) for roaming wireless stations. This is disabled by default.

Wireless Security Mode – Choose the wireless encryption method used for the wireless network. See the description on the next page for the type of security selected.
Manually Set Up Wireless Network Security - WPA

Wi-Fi Protected Access (WPA) was designed to provide improved data encryption, perceived as weak in WEP, and to provide user authentication, largely nonexistent in WEP. There are two versions of WPA, both are supported by the access point. WPA-Personal encryption uses a pre-shared key for authentication and requires periodic re-authentication from associating wireless stations.

To configure WPA settings:

1. Select the **Security Mode** to use WPA-Personal.
2. The WPA Mode can be set to **WPA2 Only** for WPA Version 2 operation (this excludes use of wireless clients that do not support WPA2), or set to **WPA Only** for operation with clients that do not support WPA2. The default setting **Auto (WPA or WPA2)** accepts clients using either version.
3. The **Group Key Update Interval** specifies the interval of time in seconds when a new group key is generated. This is the key used to encrypt wireless frames. The Group Key is changed according to the interval set here in order to prevent attempts to decrypt data in wireless frames.
4. Enter the **Pre-Shared Key**. The Pre-Shared Key acts as a password for wireless clients to gain entry to the network. The Pre-Shared Key is static. It is used to generate the group key (which is changes according to the schedule set with the Group Key Update Interval) that is in turn used for encryption.
5. Click **Apply Settings** to use the new WPA security settings and restart the access point.
Manually Set Up Wireless Network Security - WEP

Wireless Encryption Protocol (WEP) encryption can be enabled for basic 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-bit, or 128-bit encryption with four keys available.

To configure WEP settings:

1. Select a **WEP Key Length** encryption level from the drop-down menu, and enter the proper-length hexadecimal key in the available entry fields. Up to 4 keys can be configured for use.
2. Choose the **Default WEP Key** from those just entered, used as the active key.
3. Select an **Authentication** type, from the drop-down menu: Open or Shared Key or Shared Key.
4. Click **Apply Settings** to use the new WEP settings and restart the access point.

---

**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 None. WEP is the original wireless encryption standard. WPA provides a higher level of security. WPA-Personal does not require an authentication server.

<table>
<thead>
<tr>
<th>Security Mode:</th>
<th>WEP</th>
</tr>
</thead>
</table>

**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 8 text characters can be entered for 64 bit keys, and a maximum of 13 characters for 128 bit keys.

<table>
<thead>
<tr>
<th>WEP Key Length:</th>
<th>128 bit(26 hex digits)</th>
</tr>
</thead>
<tbody>
<tr>
<td>WEP Key 1:</td>
<td></td>
</tr>
<tr>
<td>WEP Key 2:</td>
<td></td>
</tr>
<tr>
<td>WEP Key 3:</td>
<td></td>
</tr>
<tr>
<td>WEP Key 4:</td>
<td></td>
</tr>
<tr>
<td>Default WEP Key:</td>
<td>WEP Key 1</td>
</tr>
<tr>
<td>Authentication:</td>
<td>Open or Shared Key</td>
</tr>
</tbody>
</table>

Please take note of your SSID and security key as you will need to duplicate the same settings to your wireless devices and PC.
Chapter 3 - Setup

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. See the next section for information on DHCP setup.

To access the **LAN Setup** menu, click the **LAN Setup** button in the **Setup** directory.

To change the **LAN IP Address** or **Subnet Mask**, type in the desired values and click the **Save Settings** button. Your Web browser should automatically be redirected to the new IP address. You will be asked to login again to the Router’s Web manager.

The DHCP server is enabled by default for the Router’s Ethernet LAN interface. DHCP service will supply IP settings to workstations configured to automatically obtain IP settings that are connected to the Router through the Ethernet port. When the Router is used for DHCP it becomes the default gateway for DHCP client connected to it. Keep in mind that if you change the IP address of the Router the range of IP addresses in the pool used for DHCP on the LAN will also be changed. The IP address pool can be up to 253 IP addresses.

There are two options for DHCP service:

- You can use the Router as a DHCP server for your LAN.
- You can disable DHCP service and manually configure IP settings for workstations.

---

**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**: 192.168.1.1
- **Subnet Mask**: 255.255.255.0

**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**: 192.168.1.2 to 192.168.1.254
- **DHCP Lease Time**: 86400 (seconds)

**DHCP TABLE**

<table>
<thead>
<tr>
<th>Host Name</th>
<th>IP Address</th>
<th>MAC Address</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>192.168.1.2</td>
<td></td>
<td>Manual Config</td>
</tr>
</tbody>
</table>

[Save Settings]
DHCP Server Configuration

Follow the instructions below according to which of the above DHCP options you want to use. When you have configured the DHCP Server Settings as you want them, click the Save Settings button to commit the new settings.

Use the Router for DHCP
To use the built-in DHCP server, click to select the Enable DHCP Server option if it is not already selected. The IP address pool settings can be adjusted beginning with the first address in the DHCP IP Address Range.

The second IP address entered is the highest IP address number in the pool. Type in the DHCP Lease Time in the entry field provided. This is the amount of time in seconds that a workstation is allowed to reserve an IP address in the pool if the workstation is disconnected from the network or powered off.

If you opt to disable DHCP service, all IP devices connected to the Router will require manual IP settings configuration or another DHCP server.

Static IP Address Assignment
The router supports static IP address assignment for the LAN. This means that an IP address is manually configured for a specified MAC address that does not age out. Static IP addresses may be assigned to hosts on the LAN that have already received IP settings and are listed in the DHCP Table. Alternatively the administrator can manually enter a MAC address in the entry field provided. Type the MAC address using the standard format 00:00:00:00:00:00 and selecting an IP address within the subnet from the IP Address pull-down menu. Click the Save Settings button to create the static IP assignment.
Advanced Setup

The Advanced directory tab offers the following configuration menus: Port Forwarding, DNS Setup, VLAN, Firewall & DMZ, Advanced ADSL, Advanced Wireless, Wi-Fi Protected Setup, Wireless MAC Filter, and Advanced LAN. Click the corresponding link in the left panel of the window. Port Forwarding is the first menu listed and the first to appear when accessing the Advanced directory.

---

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.

Maximum number of entries which can be configured: 12

ACTIVE PORT FORWARDING

<table>
<thead>
<tr>
<th>Private IP</th>
<th>Protocol Type</th>
<th>Public Start Port</th>
<th>Public End Port</th>
<th>Connection</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Add
Port Forwarding

The Port Forwarding menu allows configuration for remote users access to various services outside of their LAN through a public IP address, such as FTP (File Transfer Protocol) or HTTPS (Secure Web). After configuring the Router for these features, the Router will redirect these external services to an appropriate server on the users LAN.

Enter an IP address in the Private IP field, select a Protocol Type from the drop-down menu, enter a range of ports in the Public Start Port and Public End Port fields, and then click the Add/Apply button. Finally, click the Reboot button on the left panel to let your changes take effect.

![Port Forwarding Screenshot]

<table>
<thead>
<tr>
<th>PORT FORWARDING</th>
</tr>
</thead>
<tbody>
<tr>
<td>This is the ability to open ports in your router and redirect data through those ports to a single PC on your network.</td>
</tr>
<tr>
<td>Maximum number of entries which can be configured: 12</td>
</tr>
</tbody>
</table>

### ADD PORT FORWARDING

<table>
<thead>
<tr>
<th>Private IP</th>
<th>Protocol Type</th>
<th>Public Start Port</th>
<th>Public End Port</th>
<th>Connection</th>
</tr>
</thead>
<tbody>
<tr>
<td>0.0.0.0</td>
<td>All</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

[Apply] [Cancel]
Chapter 4 - Advanced Setup

DNS Setup

Use the **DNS Setup** menu to configure standard DNS server IP settings or to configure and enable DDNS for the Router.

**DNS Server**
Choose to “Obtain DNS server address automatically” from the ISP or enter DNS IP address information manually. The **Preferred DNS Server** address is required, the **Alternate DNS Server** address is used for a back up DNS server.

**DDNS**
Dynamic DNS allows a dynamic public IP address to be associated with a static host name in any of the many domains, allowing access to a specific host from various locations on the Internet. With this function enabled, remote access to a host will be allowed by clicking a URL hyperlink in the following form: dlinkddns.com Because many ISPs assign public IP addresses using DHCP, it can be difficult to locate a specific host on the LAN using the standard DNS. For example, if you are running a public web server or VPN server on your LAN, DDNS ensures that the host can be located from the Internet if the public IP address changes. DDNS requires that an account be set up with one of the supported DDNS servers.

To implement Dynamic DNS, first select the **Enable Dynamic DNS** option and choose the **Server Address** from the list in the pull-down menu. Enter the **Host Name** of the LAN to be accessed, and the **Username** and **Password** for the DDNS account. Click the **Apply Settings** button to save changes made.
Chapter 4 - Advanced Setup

VLAN

Use the VLAN menu to create VLAN groups for the wireless and Ethernet LANs.

**VLAN Group Setting**

Use the VLAN menu to choose a number for the VLAN group. To make sure additional VLAN groups use unique index numbers, the menu will automatically select a new index number for configuration after applying the VLAN group settings.

Click to select the member ports of each VLAN group for the two Ethernet ports and WLAN interface and the ATM VCs port for each VLAN. Any port may be specified as Tagged.

Packets that are tagged (are carrying the 802.1Q VID information) can be transmitted from one 802.1Q compliant network device to another with the VLAN information intact. This allows 802.1Q VLANs to span network devices (and indeed, the entire network, if all network devices are 802.1Q compliant).

Select the Tagged option to enable tagging for the port. Ports with tagging enabled will put the VID number, priority and other VLAN information into the header of all packets that flow into and out of it. If a packet has previously been tagged, the port will not alter the packet, thus keeping the VLAN information intact. Other 802.1Q compliant devices on the network to make packet-forwarding decisions can then use the VLAN information in the tag.

VLAN Group is enabled by default. VLAN Groups can be disabled without changing the previously configured VLAN arrangement. To disable VLAN Groups, click the Enable VLAN Group check box to remove the tick.

Click the Add/Apply button to apply the settings.
Firewall & DMZ

Use the Firewall & DMZ menu to enable or disable basic firewall protection from Denial of Service and other attacks from the WAN.

Firewall Settings
Enable the Firewall to block Denial of Service attacks, flood pings, port scans and other common exploitative attacks that might come from the Internet. This is enabled by default. To disable it, click the Enable Firewall box to remove the check mark and click the Apply Settings button.

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

For example, if you want to use video conferencing and still use a firewall, you can place the server in the DMZ. The IP address of this server will then be the DMZ IP address. You can designate the server’s IP address as the DMZ by typing in the IP address in the DMZ IP Address space provided and then enabling its status by selecting the Enable DMZ option. Click the Apply Settings button at the bottom of the window when you are finished.
Advanced ADSL

ADSL modulation is configured in the **Advanced ADSL** menu. The default setting automatically detects the appropriate modulation for the connection, therefore it should not be necessary to change this setting for the Router to function.

Modulation types supported by the Router include: **ADSL2, ADSL2+, G.DMT T1.143** and **G.lite**. If the **Modulation Mode** is changed from the default **Auto Synch-Up**, the mode used must be supported by the ISP in order for the ADSL signal to function. Likewise for changing the **ANNEX** type, if the **Type** used is not supported by the ISP in your region, the ADSL signal will not function.

The **Bitswap** and **SRA** (Seamless Rate Adaptation) features can be enabled here. If your ADSL modulation is ADSL2 or ADSL2+, these features will only be useful if supported by the ISP. If you opt to use either of these, some experimentation might be advisable to test ADSL synchronization and signal performance for improvement or degradation.
Advanced Wireless

Advanced Wireless settings are used to tweak various wireless transmission parameters and to enable an additional SSID or Guest SSID.

Transmit Power
Allows the user to adjust the transmit power of the router. A high transmit power allows a greater area range of accessibility to the router. When multiple overlapping access points are present, it may be desirable to reduce transmission power.

Bandwidth
Select the desired bandwidth. Toggle between Up to 65Mbps and Up to 135Mbps.

MCS
Select the MCS, between 0 and 15, or use Auto.

Fragmentation Threshold
The fragmentation threshold will determine if packets are to be fragmented. Packets over the 2346 byte limit will be fragmented before transmission. 2346 is the default setting.

RTS Threshold
The RTS (Request to Send) Threshold controls the size of data packets issued to a RTS packet. A lower level will send packets more frequently which may consume a great amount of the available bandwidth. A high threshold will allow the router to recover from interference or collisions which is more prevalent in a network with high traffic or high electromagnetic interference. The default setting is 2347.

DTIM Interval
DTIM (Delivery Traffic Indication Message) Interval is a countdown informing clients of the next menu for listening to broadcast and multicast messages. The default setting is 1.

Beacon Period
Beacons are emitted from the router in order to synchronize the wireless network. You may set the Beacon Interval range between 20 and 1000 microseconds per beacon sent. The default is 100.

Click the Apply Settings button to save and apply the advanced wireless configuration settings.
Wi-Fi Protected Setup

Use the Wi-Fi Protected Setup (WPS) menu to enable or disable WPS, lock the current settings, remove the current WPS settings, reset the PIN to the default value or generate a new PIN code. To add a WPS wireless client, click the Add Wireless Device with WPS button and follow the procedure as described in Add Wireless Clients with WPS.

Enable
Left-click on this box to enable WPS, a check mark indicates WPS is enabled. Click to remove the check mark to disable WPS.

Lock Wireless Security Settings
Left-click on this box to lock the current wireless security settings.

Current PIN
This is the PIN used by WPS supporting clients to establish the WPS connection. This is done either by using the wireless client to generate the PIN, then entering the client generated PIN into the access point (the router). This first method is generally the preferred method since many WPS enabled wireless clients do not include the ability to enter a PIN generated by another system. Alternatively, the access point (the router) is used to generate the PIN and this is entered into the WPS enabled wireless client. The router’s PIN used to establish WPS connections to other WPS enabled wireless devices.

Reset PIN to Default
Click on this button to reset the router’s PIN to the factory default setting.

Generate New PIN
Click on this button to generate a new PIN for the router.

Add Wireless Device with WPS
Click on this button to go to the WPS (Wi-Fi Protected Setup) Wizard menu.
Wireless MAC Filter

Use the **Wireless MAC Filter** menu to designate MAC addresses that are denied access or allowed access to the wireless LAN through the device.

Up to eight MAC addresses can be listed with the MAC Filter. It is important to understand that when the MAC filter is activated there are two options for the rule or **Action** used for the listed MAC addresses. When the **Status** is **Activated**, the administrator must choose one of the following:

- **Allow Association** to the listed MAC addresses (and deny all other MAC addresses to associate).
- **Deny Association** to the listed MAC addresses (and allow association to others not on the list).

To use Wireless MAC Filters,

1. Select the **Activated** option for **Status**.
2. Choose the **Action** to either **Allow Association** or **Deny Association** of the listed MAC addresses.
3. Type the MAC addresses effected by the chosen Action in the standard MAC address format.
4. Click on the **Apply Settings** button.

When activated the filter rule becomes effective immediately. The MAC filter rule can be deactivated by selecting the **Deactivated** option for Status. Deactivating MAC filters will not change any MAC addresses entered on the list.
Advanced LAN

Use the **Advanced LAN** menu to enable or disable UPnP and multicast streaming. **UPnP** or Universal Plug and Play is disabled by default. This network protocol is used to simplify networking and is supported on many types of networking devices. Devices that support UPnP advertise their services and capabilities to other UPnP enabled devices to facilitate network applications such as streaming audio or video. To use UPnP, tick the **Enable UPnP** check box.

Multicast streaming support is enabled by default to allow streaming of audio and video and other multicast applications to pass through the Router. To disable multicast streams, click the **Enable Multicast Streams** check box to remove the tick. Keep in mind that Internet radio and similar multicast services will not function if the Enable Multicast Streams option is not ticked.

Click the **Apply Settings** button to save and apply the advanced LAN configuration.
Use the menus in the **Maintenance** directory to perform routine maintenance functions such as saving configuration settings to hard disk, upgrading device firmware, viewing system logs, and performing device diagnostic tests.

### 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 between 1 and 15 characters.

### SET PASSWORD (OPTIONAL)

To change the router password, please type in the current password, then the new password twice.

- **Current Password:**
- **New Password:**
- **Confirm Password:**

[Apply Settings] [Cancel]
Typically one of the first things the administrator is likely to change is the device password used to access the management software. The administrator's user name, admin, cannot be changed. The default password can be changed with the Password menu.

Change the password and click the Apply Settings button to establish the new password.
Save/Restore Settings

It is a good idea to store a back up copy of the configuration settings file on the hard drive of the system used to administer the Router. Use this menu to save a settings file, load a settings file or restore the device to factory default settings.

To save the current configuration settings to your computer, click the **Save/Restore Settings** button in the **Maintenance** directory to display the **System Settings** menu. Click the **Save** button to Save Settings to Local Hard Drive. You will be prompted to select a location on your computer to put the file.

To load a previously saved configuration file, click the **Browse** button and locate the file on your computer. Click the **Update Settings** button to Load Settings From Local Hard Drive. Confirm that you want to load the file when prompted and the process is completed automatically. The Router will reboot and begin operating with the configuration settings that have just been loaded.

To reset the Router to its factory default settings, click the **Restore Device** button. You will be prompted to confirm your decision to reset the Router. The Router will reboot with the factory default settings including IP address (**192.168.1.1**) with DHCP enabled and default administrator password (**admin**)
Firmware Update

Use this menu 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 save the configuration settings with the Save/Restore Settings menu described above or click the Backup Now button to go through the same procedure.

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

**FIRMWARE INFORMATION**

- Current Firmware Version: EU_1.00
- Current Firmware Date: 2010/06/23

**FIRMWARE UPDATE**

Note: Some firmware updates reset the configuration options to factory defaults. Before performing an update, be sure to save the current configuration from the Maintenance > Save/Restore Settings screen.

To update the firmware, your PC must have a wired connection to the router. Enter the name of the firmware update file, and click on the Upload button.
Diagnostics

This menu is used to test connectivity of the Router. A Ping test may be done through the local or external interface to test connectivity to known IP addresses. The diagnostics feature executes a series of tests of your system software and hardware connections. Use this menu when working with your ISP to troubleshoot problems.

Click the **Re_run Diagnostics Tests** button to view the connectivity status of the WAN connection.
System Log

Use the System Log to view a log of events that occur on the Router.

<table>
<thead>
<tr>
<th>Date/Time</th>
<th>Message</th>
</tr>
</thead>
<tbody>
<tr>
<td>01/01/2000 01:23:03</td>
<td>No DNS server available</td>
</tr>
<tr>
<td>01/01/2000 01:23:03</td>
<td>adjTimeTask: fail, wrong domain name</td>
</tr>
<tr>
<td>01/01/2000 01:23:03</td>
<td>adjTimeTask: fail, no server available</td>
</tr>
<tr>
<td>01/01/2000 01:23:03</td>
<td>adjTimeTask: pause 60 seconds</td>
</tr>
<tr>
<td>01/01/2000 01:23:03</td>
<td>No DNS server available</td>
</tr>
<tr>
<td>01/01/2000 01:23:03</td>
<td>adjTimeTask: fail, wrong domain name</td>
</tr>
<tr>
<td>01/01/2000 01:23:03</td>
<td>adjTimeTask: fail, no server available</td>
</tr>
<tr>
<td>01/01/2000 01:23:03</td>
<td>adjTimeTask: pause 60 seconds</td>
</tr>
<tr>
<td>01/01/2000 01:23:03</td>
<td>No DNS server available</td>
</tr>
<tr>
<td>01/01/2000 01:23:03</td>
<td>adjTimeTask: fail, wrong domain name</td>
</tr>
<tr>
<td>01/01/2000 01:23:03</td>
<td>adjTimeTask: fail, no server available</td>
</tr>
<tr>
<td>01/01/2000 01:23:03</td>
<td>adjTimeTask: pause 1 day</td>
</tr>
<tr>
<td>01/01/2000 01:24:03</td>
<td>No DNS server available</td>
</tr>
<tr>
<td>01/01/2000 01:24:03</td>
<td>adjTimeTask: fail, wrong domain name</td>
</tr>
<tr>
<td>01/01/2000 01:24:03</td>
<td>adjTimeTask: fail, no server available</td>
</tr>
<tr>
<td>01/01/2000 01:24:03</td>
<td>adjTimeTask: pause 1 day</td>
</tr>
<tr>
<td>01/01/2000 01:24:03</td>
<td>No DNS server available</td>
</tr>
<tr>
<td>01/01/2000 01:24:03</td>
<td>adjTimeTask: fail, wrong domain name</td>
</tr>
<tr>
<td>01/01/2000 01:24:03</td>
<td>adjTimeTask: fail, no server available</td>
</tr>
<tr>
<td>01/01/2000 01:24:03</td>
<td>adjTimeTask: pause 60 seconds</td>
</tr>
<tr>
<td>01/01/2000 01:24:03</td>
<td>No DNS server available</td>
</tr>
<tr>
<td>01/01/2000 01:24:03</td>
<td>adjTimeTask: fail, wrong domain name</td>
</tr>
<tr>
<td>01/01/2000 01:24:03</td>
<td>adjTimeTask: fail, no server available</td>
</tr>
<tr>
<td>01/01/2000 01:24:03</td>
<td>adjTimeTask: pause 1 day</td>
</tr>
</tbody>
</table>
## Status

Use these read-only menus to view system information and monitor performance.

### DEVICE INFO

The Device Status page allows you to check the status of your Internet connection, Wireless LAN and LAN.

### GENERAL

<table>
<thead>
<tr>
<th>Time</th>
<th>01.01.2000, 01:07:17, Sat</th>
</tr>
</thead>
<tbody>
<tr>
<td>Firmware Version</td>
<td>EU_1.00</td>
</tr>
</tbody>
</table>

### INTERNET STATUS

<table>
<thead>
<tr>
<th>ADSL Modulation</th>
<th>Error</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cable Status</td>
<td>ADSL Link Down</td>
</tr>
<tr>
<td>Virtual Circuit</td>
<td>PVC-0</td>
</tr>
<tr>
<td>Connection Type</td>
<td>PPPoE/PPPoA</td>
</tr>
<tr>
<td>Network Status</td>
<td>Not Connected</td>
</tr>
<tr>
<td>Connection Up Time</td>
<td>N/A</td>
</tr>
<tr>
<td>Downstream Line Rate</td>
<td>0 kbps</td>
</tr>
<tr>
<td>Upstream Line Rate</td>
<td>0 kbps</td>
</tr>
</tbody>
</table>

[DHCP Renew] [DHCP Release]

<table>
<thead>
<tr>
<th>MAC Address</th>
<th>N/A</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP Address</td>
<td>N/A</td>
</tr>
<tr>
<td>Subnet Mask</td>
<td>N/A</td>
</tr>
<tr>
<td>Default Gateway</td>
<td>N/A</td>
</tr>
<tr>
<td>Preferred DNS Server</td>
<td>N/A</td>
</tr>
<tr>
<td>Alternate DNS Server</td>
<td>N/A</td>
</tr>
</tbody>
</table>
Device Info

Use this menu to quickly view basic current information about the Internet status, WLAN, and LAN interfaces, as well as device information including Firmware Version and MAC Address.

**GENERAL**

- **Time**: 01.01.2000, 01:07:17, Sat
- **Firmware Version**: 5.1.0.0

**INTERNET STATUS**

- **ADSL Modulation**: Error
- **Cable Status**: ADSL Link Down
- **Virtual Circuit**: PVC 0
- **Connection Type**: PPoE/PPPoEA
- **Network Status**: Not Connected
- **Connection Up Time**: N/A
- **Downstream Line Rate**: 512 Kbps
- **Upstream Line Rate**: 512 Kbps

**WIRELESS LAN**

- **Wireless Radio**: ON
- **MAC Address**: 1c:af:17:ca:7:be
- **Network Name (SSID)**: D-Link
- **Channel**: Channel 6
- **Security Type**: None

**LAN**

- **MAC Address**: 1c:af:17:ca:7:be
- **IP Address**: 192.168.1.1
- **Subnet Mask**: 255.255.255.0
- **DHCP Server**: ON
Connected Clients

The Connected LAN Clients list displays active DHCP clients (when DHCP mode is enabled) and currently associated wireless clients.

<table>
<thead>
<tr>
<th>CONNECTED CLIENTS</th>
</tr>
</thead>
<tbody>
<tr>
<td>This page shows all the currently connected LAN computers or PCs.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>CONNECTED DHCP LAN CLIENTS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hostname</td>
</tr>
<tr>
<td>-----------</td>
</tr>
</tbody>
</table>


Chapter 6 - Status

Statistics

Use this menu to monitor traffic on the Ethernet LAN, Wireless LAN, or ADSL interface. This menu also displays information on the ADSL signal status.

STATISTICS

This information reflects the current status of your router.

WAN STATISTICS

<table>
<thead>
<tr>
<th>Service</th>
<th>VPI/VCI</th>
<th>Protocol</th>
<th>Received</th>
<th>Transmitted</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>0</td>
<td>PPPoE</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>0</td>
<td>RFC 1483</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

LAN STATISTICS

<table>
<thead>
<tr>
<th>Interface</th>
<th>Received</th>
<th>Transmitted</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Bytes</td>
<td>818</td>
</tr>
<tr>
<td>Ethernet</td>
<td>188046</td>
<td>0</td>
</tr>
<tr>
<td>Wireless</td>
<td>40573364</td>
<td>64343</td>
</tr>
</tbody>
</table>

ADSL STATISTICS

<table>
<thead>
<tr>
<th>Mode</th>
<th>Error</th>
<th>Type</th>
<th>ANNEX_A</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td>Down</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Up</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Rate (Kbps):</td>
<td>Downstream</td>
<td>Upstream</td>
<td></td>
</tr>
<tr>
<td>SNR Margin (dB):</td>
<td>N/A</td>
<td>N/A</td>
<td></td>
</tr>
<tr>
<td>Attenuation (dB):</td>
<td>N/A</td>
<td>N/A</td>
<td></td>
</tr>
<tr>
<td>Output Power (dBm):</td>
<td>N/A</td>
<td>N/A</td>
<td></td>
</tr>
<tr>
<td>Super Frames:</td>
<td>0</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>RS Correctable Errors:</td>
<td>0</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>RS Uncorrectable Errors:</td>
<td>0</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>HEC Errors:</td>
<td>0</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>Total Cells:</td>
<td>0</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>Data Cells:</td>
<td>0</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>CRC Errors:</td>
<td>0</td>
<td>0</td>
<td></td>
</tr>
</tbody>
</table>
To access the **Help** window, click the **Help** directory.

**HELP MENU**
- Setup
- Advanced
- Maintenance
- Status

**SETUP HELP**
- ADSL Setup
- Wireless Setup
- LAN Setup

**ADVANCED HELP**
- Port Forwarding
- DNS Setup
- Firewall & DMZ
- Advanced Wireless
- WPA/Pre-Shared Key

**MAINTENANCE HELP**
- Password
- Save/Restore Settings
- Firmware Update
- Reboot
- System Log

**STATUS HELP**
- Device Info
- Connected Clients
- Statistics
### Technical Specifications

#### ADSL Standards
- Full-rate ANSI T1.413 Issue 2
- ITU G.992.1 (G.dmt)
- ITU G.992.2 (G.lite)
- ITU G.994.1 (G.hs)

#### ADSL2 Standards
- ITU G.992.3 (G.dmt.bis)

#### ADSL2+ Standards
- ITU G.992.5

#### Protocols
- IEEE 802.1d Spanning Tree
- TCP/UDP
- ARP
- RARP
- ICMP
- RFC 1334 PAP
- RFC 1577 Classical IP over ATM
- RFC 1661 Point to Point Protocol
- RFC 1994 CHAP
- RFC 2131 DHCP Client/DHCP Server
- RFC 2364 PPP over ATM
- RFC 2516 PPP over Ethernet
- RFC 1483/2684 Multiprotocol Encapsulation over ATM Adaptation Layer 5 (AAL5)

#### DC Power
- Input: 100-120V 0.5A, 50-60Hz
- Output: 12V 0.5A

#### Data Transfer Rates
- G.dmt full rate downstream: up to 8 Mbps/upstream: up to 1 Mbps
- G.lite: ADSL downstream: up to 1.5 Mbps/upstream: up to 512 Kbps
- G.dmt.bis full rate downstream: up to 12 Mbps/upstream: up to 1 Mbps
- ADSL2+ full rate downstream: up to 24 Mbps/upstream: up to 1 Mbps

#### Wireless Transfer Rates
- IEEE 802.11b: 11, 5.5, 2, 1 Mbps
- IEEE 802.11g: 6, 9, 12, 18, 24, 36, 48, and 54 Mbps
- IEEE 802.11n: 20MHz - 6.5, 13, 19.5, 26, 39, 52, 58.5 & 65 40MHz - 13.5, 27, 40.5, 54, 81, 108, 121.5 & 135

#### Media Interface
- ADSL Interface: RJ-11 connector for connection to 24/26 AWG twisted pair telephone line
- LAN Interface: two RJ-45 ports for 10/100BASE-T Ethernet connection

#### Default Settings
- IP Address: 192.168.1.1
- Netmask: 255.255.255.0
- User Name: admin
- Password: admin
- DHCP Server: enabled