



**User Manual**

## **ADSL 2+ Modem with Wireless N 300 Router**

---

# Table of Contents

<b>General Information</b> .....	4	MAC Encapsulation Routing or DHCP .....	30
Package Contents .....	4	Network Address Translation Settings (MER/DHCP) .....	31
Important Safety Instructions.....	5	DNS Server Configuration (MER/DHCP).....	32
Front Panel View .....	6	Default Gateway (MER/DHCP) .....	33
Rear Panel View.....	7	Setup Summary (MER/DHCP) .....	34
Angle View .....	8	Bridging .....	35
<b>Installing the Router</b> .....	9	Setup Summary (Bridging) .....	36
<b>Installation Diagram</b> .....	11	Wireless Settings .....	37
<b>Configuring Your Computer</b> .....	12	Wireless Connection Setup Wizard.....	38
Windows® 7, Vista®, Windows XP, 2000 .....	12	Wi-Fi Protected Setup .....	39
Mac .....	14	Manual Wireless Setup .....	40
<b>Log In To The Router</b> .....	15	Local Network.....	42
<b>Setup</b> .....	16	Time and Date .....	43
Setup Wizard.....	16	<b>Advanced Wireless</b> .....	44
Configure Wireless Network.....	20	<b>Advanced Settings</b> .....	45
LAN Settings.....	21	MAC Filter.....	46
Apply Settings.....	21	Wireless Bridge.....	47
Internet Setup .....	22	Wireless QoS.....	48
ATM PVC Configuration.....	23	Port Forwarding .....	49
Connection Type .....	24	Port Triggering .....	51
PPP over Ethernet (PPPoE).....	25	DMZ Host .....	52
DNS Server Configuration.....	27	Parental Control.....	53
Default Gateway .....	28	Block MAC Address.....	54
Setup Summary (PPPoE).....	29	Filtering Options.....	55
		Incoming IP Filtering Setup.....	56

Outgoing IP Filtering Setup.....	57	<b>Status .....</b>	<b>82</b>
Bridge Filtering Setup.....	58	Device Info.....	82
Firewall .....	59	Wireless Clients .....	83
DNS.....	60	DHCP Clients.....	84
Dynamic DNS.....	61	Logs.....	85
Network Tools.....	62	Statistics.....	86
Port Mapping.....	63	Route Info.....	87
IGMP.....	64	<b>Troubleshooting .....</b>	<b>88</b>
Quality of Service .....	65	<b>Networking Basics.....</b>	<b>90</b>
ADSL Setting.....	66	Check your IP address.....	90
SNMP .....	67	Statically Assign an IP address.....	91
UPnP .....	68	<b>Contacting Technical Support.....</b>	<b>92</b>
TR-069 .....	69	<b>Warranty.....</b>	<b>93</b>
Routing .....	70	<b>Registration .....</b>	<b>97</b>
Static Route .....	70		
Default Gateway.....	71		
RIP .....	72		
<b>Schedules.....</b>	<b>73</b>		
<b>Maintenance.....</b>	<b>74</b>		
System.....	74		
Firmware Update.....	75		
Access Control.....	76		
Account Password .....	76		
Services.....	77		
IP Address .....	78		
Diagnostics.....	79		
System Log .....	80		
Logout.....	81		

# General Information

The D-Link DSL-2740B is an ADSL2+ router offering the convenience of 4 LAN ports for additional computers. This user manual provides you with a simple and easy-to-understand format to install and configure your router.

## Package Contents



ADSL2+ Modem with Wireless N 300 Router



12VDC, 1A DC CEC-compliant switching power adapter



RJ-11 telephone cable



RJ-45 Ethernet cable



Installation CD-ROM



QIG

**Note:** Using a power supply with a different voltage rating than the one included with the DSL-2740B will cause damage and void the warranty for this product.

# Important Safety Instructions

- Place your router on a flat surface close to the cables in a location with sufficient ventilation.
- To prevent overheating, do not obstruct the ventilation openings of this equipment.
- Plug this equipment into a surge protector to reduce the risk of damage from power surges and lightning strikes.
- Operate this equipment only from an electrical outlet with the correct power source as indicated on the adapter.
- Do not open the cover of this equipment. Opening the cover will void any warranties on the equipment.
- Unplug equipment first before cleaning. A damp cloth can be used to clean the equipment. Do not use liquid/aerosol cleaners or magnetic/static cleaning devices.
- To reduce the risk of fire, use only No. 26 AWG (or a larger diameter/smaller AWG) RJ-11 telephone cable.

# Front Panel View



<b>1</b>	<b>Power LED</b>	<ul style="list-style-type: none"><li>• A solid green light indicates the unit is powered on.</li><li>• A red light indicates a malfunction.</li></ul>
<b>2</b>	<b>LAN LEDs</b>	<ul style="list-style-type: none"><li>• A solid light indicates a connection to an Ethernet-enabled computer on ports 1-4. This LED blinks during data transmission.</li></ul>
<b>3</b>	<b>Wireless LED</b>	<ul style="list-style-type: none"><li>• A solid green light indicates the wireless function is operating correctly. A flashing green light indicates wireless traffic is passing through the router.</li></ul>
<b>4</b>	<b>DSL LED</b>	<ul style="list-style-type: none"><li>• A solid light indicates the DSL is synchronized.</li><li>• A flashing LED indicates the modem is attempting to synchronize with the DSL provider.</li></ul>
<b>5</b>	<b>Internet LED</b>	<ul style="list-style-type: none"><li>• A solid green light indicates that the modem has an IP address and is connected to the Internet.</li><li>• A red light indicates that the modem does not have an IP address or authentication has failed.</li><li>• No light indicates that an ADSL connection is not present or the modem is in bridge mode.</li></ul>

# Rear Panel View



<b>1</b>	<b>DSL Line</b>	• Connect to an active telephone line (RJ-11).
<b>2</b>	<b>LAN Ports (1-4)</b>	• Connect Ethernet devices such as computers, switches, and hubs.
<b>3</b>	<b>Wireless ON/OFF</b>	• Pressing this button to turn the Wireless feature on or off.
<b>4</b>	<b>Reset</b>	• Pressing the Reset button for 10 seconds restores the modem to its original factory default settings.
<b>5</b>	<b>ON/OFF</b>	• Press this button to turn the unit on or off.
<b>6</b>	<b>Power Receptor</b>	• Receptor for the supplied power adapter.

# Angle View



<b>1</b>	<b>WPS Button</b>	<ul style="list-style-type: none"><li>• Press this button to add your device to an existing network or to create a new network.</li></ul>
----------	-------------------	---

# Installing the Router

## Connect the ADSL and Telephone Lines

- Connect an RJ-11 cable between the wall phone jack and the **ADSL** port on the rear panel of the router.

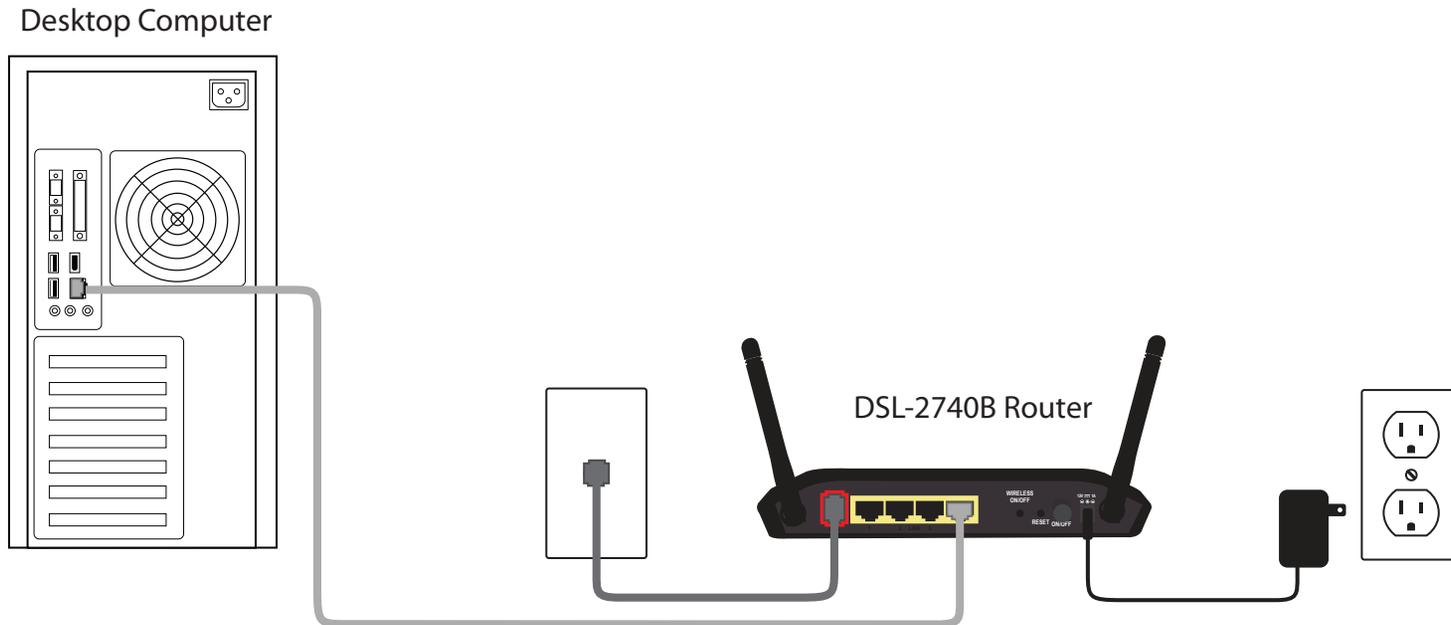
## Connect the PC to the Router

- To use the Ethernet connection, connect the Ethernet cable from the computer directly to the router. Connect one end of the Ethernet cable to the port labeled **LAN** on the back of the router and attach the other end to the Ethernet port of your computer.
- If your LAN has more than one computer, you can attach one end of an Ethernet cable to a hub or a switch and the other to the Ethernet port (labeled LAN) on the router. Note that either a crossover or straight-through Ethernet cable can be used. The router automatically recognizes the type of connection that is required.

## Connect the Power Adapter

- Complete the process by connecting the supplied 12VAC, 1A power adapter to the POWER connector on the back of the device and plug the adapter into a wall outlet or power strip. Then turn on and boot up your PC and any LAN devices, such as hubs or switches, and any computers connected to them.

# Installation Diagram



# Configuring Your Computer

Prior to accessing the router through the LAN port, note the following necessary configurations:

- Your PC's TCP/IP address: 192.168.1.x (where "x" is any number between 2 and 254)
- The router's default IP address: 192.168.1.1
- Subnet mask: 255.255.255.0

Below are the procedures for configuring your computer. Follow the instructions for the operating system that you are using.

## Windows<sup>®</sup> 7, Vista<sup>®</sup>, Windows XP, 2000

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

### Step 1

Windows<sup>®</sup> 7 - Click on **Start > Control Panel > Network and Internet > Network and Sharing Center**.

Windows Vista<sup>®</sup> - Click on **Start > Control Panel > Network and Internet > Network and Sharing Center > Manage Network Connections**.

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

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

### Step 2

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

### Step 3

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

**Step 4**

In the Internet Protocol (TCP/IP) Properties dialog box, click on the radio buttons labeled **Obtain an IP address automatically** and **Obtain DNS server address automatically**.

**Step 5**

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

# Mac

These are instructions for configuring your Mac OS X operating system

1. In the Mac OS X Dock, click on the **System Preferences** icon.
2. Under **Internet & Network**, click **Network**. In the **Show** menu, select **Built-in Ethernet** or Ethernet (Depending on your Mac OS version.)
3. Click the **TCP/IP** tab.
4. In the Configure menu, select **Using DHCP**.
5. Click **Apply** Now and Save if your computer prompts you to save changes.

# Log In To The Router

This section will explain how to log in to your router using the following steps:

1. Launch your web browser.
2. Enter the URL `http://192.168.1.1` in the address bar and press **Enter**.

A login screen like the one below will be displayed after you connect to the user interface.



**Note:** Use *admin/admin* as default for username and password.

- The admin account can perform all functions (username / password: **admin / admin**).

**Note:** Passwords can be changed at any time.

A screenshot of the login form on the D-Link router web interface. The form has a grey background and a dark grey header with the word 'Login' in white. Below the header, it says 'Log in to the router'. There are two input fields: 'User Name :' and 'Password :'. To the right of the password field is a 'Log In' button. Below the input fields is a checkbox labeled 'Remember my login info. on this computer'.

- 
3. Enter your user name and password, and then click **OK** to display the user interface.

**Note:** This manual has been prepared using the admin user name.

# Setup

This section will show you how to configure your new D-Link wireless router using the web-based configuration utility. Please prepare your DSL account information provided by your Internet Service Provider (ISP).

## Setup Wizard

To quickly configure your router, click **Setup Wizard**.

The screenshot displays the web-based configuration utility for a D-Link DSL-2740B router. At the top, it shows 'Product Page: DSL-2740B' and 'Firmware Version: NA\_1.00'. The D-Link logo is prominently displayed. Below the logo, there are navigation tabs: 'DSL-2740B', 'Setup', 'Advanced', 'Maintenance', 'Status', and 'Help'. The 'Setup' tab is selected. On the left side, there is a sidebar menu with options: 'Wizard', 'Internet Setup', 'Wireless Settings', 'Local Network', 'Time and Date', and 'Logout'. The main content area is titled 'Setting up your internet' and contains the following text: 'There are two ways to set up your Internet connection: you can use the Web-based Internet Connection Setup Wizard, or you can manually configure the connection. Please make sure you have your ISP's connection settings first if you choose to setup manually.' Below this text is a section titled 'Internet Connection Wizard' with the text: 'You can use this wizard for assistance and quick connection of your new D-Link Router to the Internet. You will be presented with step-by-step instructions in order to get your Internet connection up and running. Click the button below to begin.' A 'Setup Wizard' button is located below the text. A 'Note' at the bottom of the wizard section states: 'Note: Before launching the wizard, please ensure you have correctly followed the steps outlined in the Quick Installation Guide included with the router.' On the right side, there is a 'Helpful Hints...' section with two paragraphs of text and a 'More...' link.

Product Page: DSL-2740B [Site Map](#) Firmware Version: NA\_1.00

**D-Link**

DSL-2740B **Setup** Advanced Maintenance Status Help

Wizard  
Internet Setup  
Wireless Settings  
Local Network  
Time and Date  
Logout

**Setting up your internet**

There are two ways to set up your Internet connection: you can use the Web-based Internet Connection Setup Wizard, or you can manually configure the connection. Please make sure you have your ISP's connection settings first if you choose to setup manually.

**Internet Connection Wizard**

You can use this wizard for assistance and quick connection of your new D-Link Router to the Internet. You will be presented with step-by-step instructions in order to get your Internet connection up and running. Click the button below to begin.

[Setup Wizard](#)

**Note:** Before launching the wizard, please ensure you have correctly followed the steps outlined in the Quick Installation Guide included with the router.

**Helpful Hints...**

If you are new to networking and have never configured a router before, click on "setup wizard" and the router will run you through a step by step process to successfully connect you to the internet.

If you consider yourself an advanced user or have configured a router before, click [Setup -> Internet Setup](#) to input all the settings manually.

[More...](#)

Click **Next** to continue.



Create a new password and click **Next** to continue or click **Skip** to keep your current password.



In this section you may configure, update, and maintain the correct time for the internal system clock. Set the time zone that you are in and set the NTP (Network Time Protocol) Server. Select the time zone from the drop-down menu and then click **Next** to continue.

**1 > Step 2: Set Time and Date > 3 > 4 > 5 > 6**

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

**Time settings** **Automatically synchronize with Internet time servers**

First NTP time server: ntp1.dlink.com

Second NTP time server: ntp.dlink.com.tw

**Time Configuration**

Current Router Time : 1.01.2000,00:01:51 Sat

Time Zone :

(GMT-08:00) Pacific Time, Tijuana

Enable Daylight Saving : 

Daylight Saving Offset : -2:00

Daylight Saving Dates :

	Month	Week	Day	Time
Start	Jan	1st	Sun	12 am
End	Jan	1st	Sun	12 am

**Set the Date and Time Manually**

Date And Time :

Year: 2011 Month: Jan Day: 1  
Hour: 1 am Minute: 44 Second: 21

Copy Your Computer's Time Settings

Back Next Cancel

Select your Country and Internet Service provider from the drop-down menus. If your Country or ISP is not on the list, please select “**others**”. Refer to your DSL account information and select the proper Protocol and Connection Type. Next, enter your ISP assigned VPI and VCI settings.

Alternatively, you may check the box labeled Enable DSL Auto-Scan. Click **Next** to continue.

1 > 2 > Step 3: Setup Internet Connection > 4 > 5 > 6

**Country :** (Click to select) ▼

**ISP Provider :** (Click to select) ▼

**Protocol :** (Click to select) ▼

**Connection Type :** (Click to Select) ▼

**VPI :** (Enter a number)

**VCI :** (Enter a number)

Enable DSL Auto-scan :

To log out of the router’s user interface at any time during the setup, click on the **Logout** button. A confirmation screen will appear confirming that you really want to log out.

**LOGOUT**

Logging out will close the browser.

Logout

# Configure Wireless Network

**Enable Your Wireless Network:** If you would like to make wireless available, this box must be checked. To Disable wireless, uncheck this box.

**Visibility Status:** Choose Invisible if you would like to hide any access point for your router so a station cannot obtain the SSID through passive scanning.

**Wireless Network Name (SSID):** Give your wireless network a name. For security reasons it is recommended to change the pre-configured network name.

**Security Level:** It is suggested to use WPA2-PSK for the highest level of wireless security.

1 > 2 > 3 > **Step 4: Configure Wireless Network** > 5 > 6

Your wireless network is enabled by default. You can simply uncheck to disable it and click "Next" to skip configuration of wireless network.

**Enable Your Wireless Network :**

Your wireless network needs a name so it can be easily recognized by wireless clients. For security purposes, it is highly recommended to change the pre-configured network name.

**Wireless Network Name (SSID) :**

Select "Visible" to publish your wireless network and SSID can be found by wireless clients, or select "Invisible" to hide your wireless network so that users need to manually enter SSID in order to your wireless network.

**Visibility Status:**  Visible  Invisible

In order to protect your network from hackers and unauthorized users, it is highly recommended you choose one of the following wireless network security settings.

None	Security Level	Best
<input type="radio"/> None	<input type="radio"/> WEP	<input type="radio"/> WPA-PSK
		<input checked="" type="radio"/> WPA2-PSK

**Security Mode :** WPA2  
Select this option if you wireless adapters support WPA2

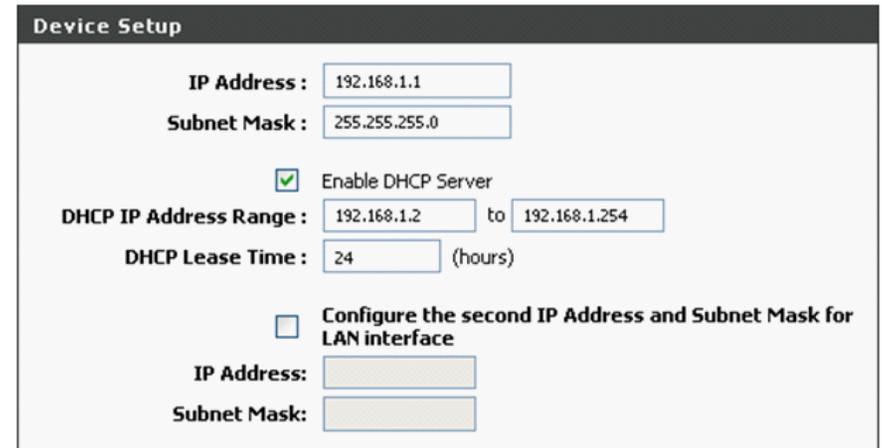
Now, please enter your wireless adapters support WPA2

**WPA2 Pre-Shared Key :**  (8-63 ASCII characters or 64 hexadecimal digits, Example '%Fortress123&')

Note: you will need to enter the same key here into your wireless clients in order to enable proper wireless connection.

# LAN Settings

In this section, you can configure the DSL Router IP Address and Subnet Mask for the LAN interface.

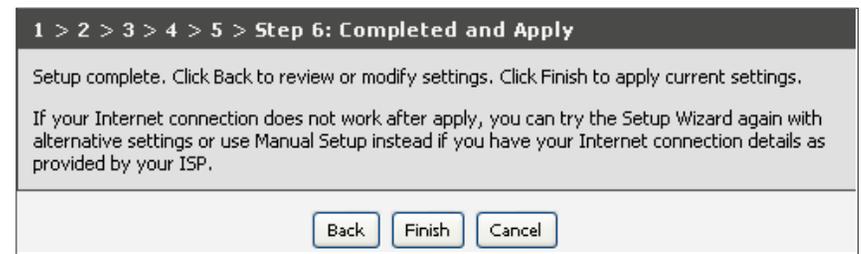


The screenshot shows the 'Device Setup' configuration page. It includes the following fields and options:

- IP Address :** 192.168.1.1
- Subnet Mask :** 255.255.255.0
- Enable DHCP Server**
- DHCP IP Address Range :** 192.168.1.2 to 192.168.1.254
- DHCP Lease Time :** 24 (hours)
- Configure the second IP Address and Subnet Mask for LAN interface**
- IP Address:** [Empty field]
- Subnet Mask:** [Empty field]

## Apply Settings

The Setup is now complete. Click Finish to apply the current settings.



The screenshot shows the 'Step 6: Completed and Apply' screen. It contains the following text and buttons:

**1 > 2 > 3 > 4 > 5 > Step 6: Completed and Apply**

Setup complete. Click Back to review or modify settings. Click Finish to apply current settings.

If your Internet connection does not work after apply, 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.

**Back** **Finish** **Cancel**

# Internet Setup

Internet Setup is an advanced version of the Setup Wizard. If you want to manually configure your DSL connection, consider going through this advanced setup for a more comprehensive configuration. Configure the DSL settings as provided by your ISP.

Click on the **Add** button if you want to add a new connection for the Wide Area Network (WAN) interface and to proceed to the ATM PVC Configuration screen. The ATM PVC Configuration screen allows you to configure your Internet connection.

Find your account settings from your ISP before you proceed.

Product Page: DSL-2740B Site Map Firmware Version: NA\_1.00

**D-Link**

DSL-2740B **Setup** Advanced Maintenance Status Help

Wizard  
Internet Setup  
Wireless Settings  
Local Network  
Time and Date  
Logout

**WAN**

Choose Add, Edit, or Remove to configure WAN interfaces.

**WAN Service Setup**

	Interface	PVC	Description	Protocol	ConnId	Igmp	NAT	State	Edit	Action
<input type="checkbox"/>	ppp0_2	PVC: 0/35	pppoe_atm0_1	PPPoE	1	Disabled	Enabled	Enabled	<a href="#">Edit</a>	DOWN

[Add](#) [Remove](#)

# ATM PVC Configuration

**VPI/VCI:** These values are required for all DSL connection types and are provided by your ISP.

**Service Category:** Use the default setting unless otherwise instructed by your ISP.

**Enable QoS:** Use the default setting unless otherwise instructed by your ISP. For more information about QoS, see the Quality of Service section in this user manual.

The screenshot shows a configuration window with a dark header labeled "Connection Type". Below the header, there are five radio button options: "PPP over ATM (PPPoA)", "PPP over Ethernet (PPPoE)", "MAC Encapsulation Routing (MER)", "IP over ATM (IPoA)", and "Bridging". The "PPP over Ethernet (PPPoE)" option is selected, indicated by a green dot in the center of the radio button. Below these options, there is a section titled "Encapsulation Mode" in blue text, followed by a dropdown menu currently showing "LLC/SNAP-BRIDGING".

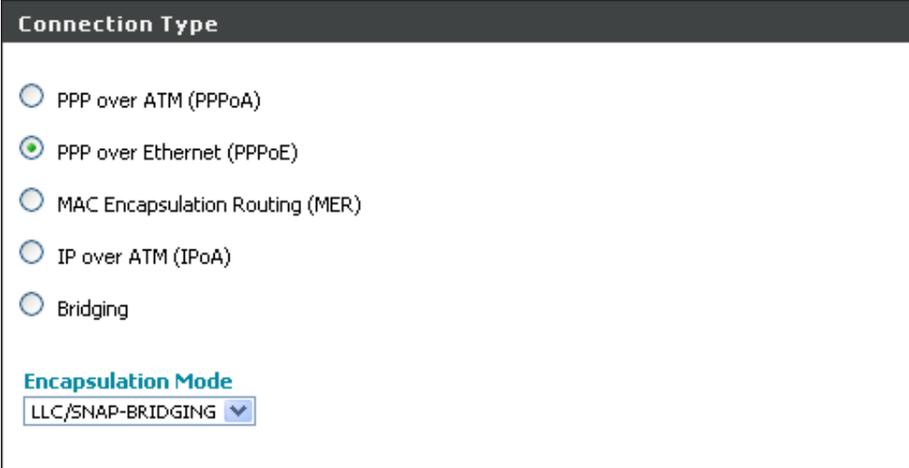
# Connection Type

This field shows the types of network protocols and encapsulation modes that can be configured.

Connection Type: Select the connection type that your ISP has instructed to use.

- PPP over ATM (PPPoA)
- PPP over Ethernet (PPPoE)
- MAC Encapsulation Routing (MER)/DHCP
- IP over ATM (IPoA)
- Bridging

PPPoE, MER (also referred to as DHCP) and Bridging are the most common connection types in North America. To set up a PPPoE, MER or Bridging connection, follow the instructions on the following pages of this user manual. PPPoA and IPoA are more widely utilized in other regions. Setup for PPPoA and IPoA are similar to PPPoE and MER, respectively.



**Connection Type**

PPP over ATM (PPPoA)

PPP over Ethernet (PPPoE)

MAC Encapsulation Routing (MER)

IP over ATM (IPoA)

Bridging

**Encapsulation Mode**

LLC/SNAP-BRIDGING

**Encapsulation Mode:** Use the default setting unless otherwise instructed by your ISP.

**Note:** *These settings are ISP dependant. For information regarding proper configuration, contact your ISP.*

# PPP over Ethernet (PPPoE)

**PPP Username:** Enter your username as provided by your ISP.

**PPP Password:** Enter your password as provided by your ISP.

**PPPoE Service Name:** Enter any name that will help you identify your connection. This field will not affect your connection.

**Authentication Method:** Use the default setting unless otherwise instructed by your ISP.

## Method:

**MTU:** Use the default setting of 1492 unless otherwise instructed by your ISP.

**MRU:** Use the default setting unless otherwise instructed by your ISP.

**Enable NAT:** Select if you would like to share your internet connection with multiple computers. The router will share your DSL connection with wired and wirelessly connected computers.

**Enable Fullcone NAT:** Select this option if you would like to utilize a one-to-one Network Address Translation. It will map a single internal IP address to a single external IP address.

**Enable Firewall:** Select if you would like to utilize the firewall to help protect you from unwanted internet threats

### PPP Username and Password

PPP Username:

PPP Password:

PPPoE Service Name:

Authentication Method: AUTO ▼

MTU:

MRU:

Enable NAT

Enable Fullcone NAT

Enable Firewall

Dial on demand (with idle timeout timer)

PPP IP extension

Use Static IPv4 Address

Retry PPP password on authentication error

Enable PPP Debug Mode

Bridge PPPoE Frames Between WAN and Local Ports

**IGMP Multicast**

Enable IGMP Multicast

Enable VLAN

**Dial on demand (with idle timeout timer):** Allows you to manually connect to the Internet so you are not permanently connected. Idle timeout timer is included.

**PPP IP extension:** Used by some ISPs. Check with your ISP to see if it is required.

**Use Static IPv4 Address:** Select if your ISP has provided you with a static IP address. If selected, you will be asked to enter the static IP address.

**Retry PPP authentication error:** Select if you want the router to automatically retry your PPP username and password when there is an authentication error on your DSL line.

**Enable PPP Debug Mode:** Select if you want to keep a log of connection negotiation transactions. This option is used for troubleshooting connection issues.

**Bridge PPPoE Frames Between WAN and Local Ports:** Use the default setting unless otherwise instructed by your ISP.

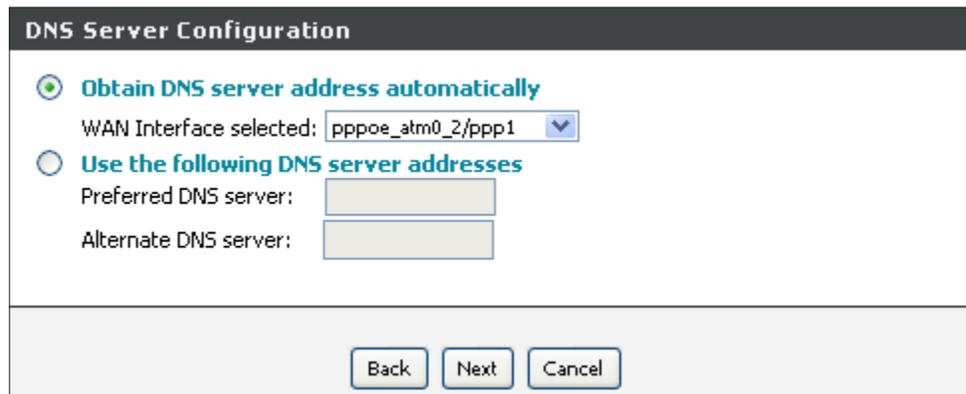
**Enable IGMP Multicast:** Use the default setting unless otherwise instructed by your ISP.

**Enable VLAN:** Use the default setting unless otherwise instructed by your ISP.

# DNS Server Configuration

If **Obtain DNS Server address automatically** is selected, this router accepts the first received DNS assignment from the PPPoE enabled PVC during the connection establishment.

If **Use the following DNS server addresses** is selected, enter the primary and secondary (optional) DNS server IP addresses



The screenshot shows a web interface titled "DNS Server Configuration". It features two radio button options. The first option, "Obtain DNS server address automatically", is selected. Below it, a dropdown menu for "WAN Interface selected:" shows "pppoe\_atm0\_2/ppp1". The second option, "Use the following DNS server addresses", is unselected and has two empty text input fields for "Preferred DNS server:" and "Alternate DNS server:". At the bottom of the form are three buttons: "Back", "Next", and "Cancel".

# Default Gateway

From this page, you can select a preferred WAN interface as the system default gateway.

**Routing -- Default Gateway**

Select a preferred wan interface as the system default gateway. Click "Apply" button to save it.

---

**Default Gateway**

Use Interface :  ▼

---

# Setup Summary (PPPoE)

Confirm the settings on this page match the settings provided by your ISP. To make any changes, click **Back**.

If your settings are correct, click **Apply**.

**Note:** After clicking **Apply**, you will have to reboot the router in order to activate your connection

### WAN

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

Click "Apply" to save these settings. Click "Back" to make any modifications.

**NOTE: You need to reboot to activate this WAN interface and further configure services over this interface.**

### SETUP - SUMMARY

VPI / VCI:	0 / 35
Connection Type:	PPPoE
Service Name:	pppoe_0_0_35
Service Category:	UBR
IP Address:	Automatically Assigned
Service State:	Enabled
NAT:	Enabled
Firewall:	Enabled
IGMP Multicast:	Disabled
Quality Of Service:	Disabled

# MAC Encapsulation Routing or DHCP

This page allows you to configure your MER/DHCP connection. Use default settings unless otherwise instructed by your ISP. This might include using a static IP address. In such a case, select Use the following Static IP address and enter your static IP address as provided by your ISP.

### WAN IP Settings

Obtain an IP address automatically

Option 60 Vendor ID:

Option 61 IAID:  (8 hexadecimal digits)

Option 61 DUID:  (hexadecimal digit)

Option 125:  Disable  Enable

Use the following Static IP address:

WAN IP Address:

WAN Subnet Mask:

WAN gateway IP Address:

# Network Address Translation Settings (MER/DHCP)

**Enable NAT:** Select if you would like to share your internet connection with multiple computers. The router will share your DSL connection with wired and wirelessly connected computers.

**Enable Fullcone NAT:** Select this option if you would like to utilize a one-to-one Network Address Translation. It will map a single internal IP address to a single external IP address.

**Enable Firewall:** Select if you would like to utilize the firewall to help protect you from unwanted internet threats.

**Enable IGMP Multicast:** Use default setting unless otherwise instructed by your ISP.

**Enable VLAN:** Use the default setting unless otherwise instructed by your ISP.

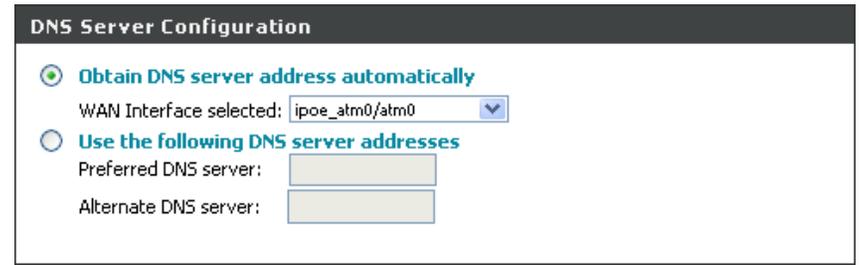
Click **Next**.

The screenshot shows the 'WAN IP Settings' configuration page. Under the 'Network Address Translation Settings' section, there is a descriptive paragraph: 'Network Address Translation (NAT) allows you to share one Wide Area Network (WAN) IP address for multiple computers on your Local Area Network (LAN)'. Below this, there are three checkboxes: 'Enable NAT' (checked), 'Enable Fullcone NAT' (unchecked), and 'Enable Firewall' (checked). Under the 'IGMP Multicast' section, there are two checkboxes: 'Enable IGMP Multicast' (unchecked) and 'Enable VLAN' (unchecked). At the bottom of the page, there are 'Back' and 'Next' buttons.

# DNS Server Configuration (MER/DHCP)

If Obtain DNS Server address automatically is selected, this router accepts the first received DNS assignment from the MER/DHCP enabled PVC during the connection establishment.

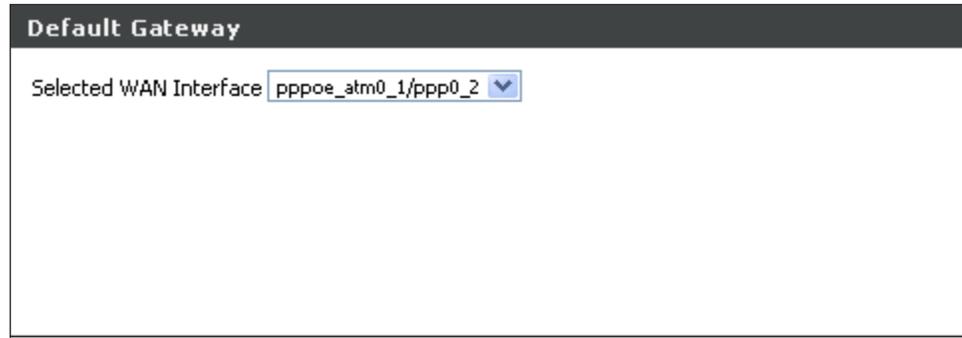
If Use the following DNS server addresses is selected, enter the primary and secondary (optional) DNS server IP addresses.



The screenshot shows the 'DNS Server Configuration' page. It features two radio button options. The first option, 'Obtain DNS server address automatically', is selected. Below it, a dropdown menu for 'WAN Interface selected' is set to 'ipoe\_atm0/atm0'. The second option, 'Use the following DNS server addresses', is unselected. Under this option, there are two empty text input fields labeled 'Preferred DNS server' and 'Alternate DNS server'.

# Default Gateway (MER/DHCP)

In this section, you can select a preferred WAN interface as the system default gateway.



The screenshot shows a web interface titled "Default Gateway". Below the title, there is a label "Selected WAN Interface" followed by a dropdown menu. The dropdown menu is currently set to "pppoe\_atm0\_1/ppp0\_2".

# Setup Summary (MER/DHCP)

Confirm the settings on this page match the settings provided by your ISP. To make any changes, click **Back**.

If your settings are correct, click **Apply**.

**Note:** After clicking *Apply*, you will have to reboot the router in order to activate your connection.

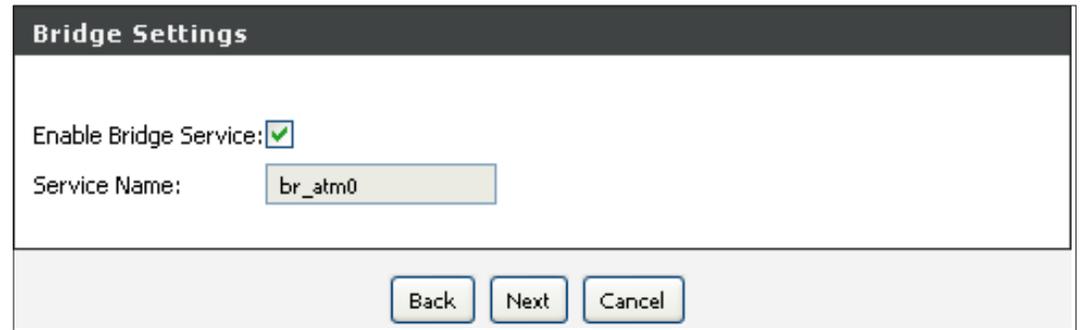
Setup - Summary	
PORT / VPI / VCI:	0 / 0 / 35
Connection Type:	IPoE
Description:	ipoe_atm0
Service Category:	UBR
IP Address:	Automatically Assigned
Service State:	Enabled
NAT:	Enabled
Full Cone NAT:	Disabled
Firewall:	Enabled
IGMP Multicast:	Disabled

# Bridging

**Enable WAN Service:** This option is Enabled by default. Deselecting this option will cause your DSL connection to be disabled.

**Service Name:** Enter any name that will help you identify your connection. This field will not affect your connection.

Click **Next**.



The screenshot shows a window titled "Bridge Settings". It contains two main configuration items: "Enable Bridge Service:" with a checked checkbox, and "Service Name:" with a text input field containing the value "br\_atm0". At the bottom of the window, there are three buttons: "Back", "Next", and "Cancel".

# Setup Summary (Bridging)

Confirm the settings on this page match the settings provided by your ISP. To make any changes, click **Back**.

If your settings are correct, click **Apply**.

**Note:** After clicking **Apply**, you will have to reboot the router in order to activate your connection.

Setup - Summary	
PORT / VPI / VCI:	0 / 0 / 35
Connection Type:	Bridge
Description:	br_atm0
Service Category:	UBR
IP Address:	Not Applicable
Service State:	Enabled
NAT:	Disabled
Full Cone NAT:	Disabled
Firewall:	Disabled
IGMP Multicast:	Not Applicable

# Wireless Settings

This section allows you to configure your wireless settings by using the **Wireless Connection Setup Wizard** or by doing it manually by selecting **Add Wireless Device with WPS**.

If you want to configure the wireless settings on your router using the wizard, click **Wireless Connection Setup Wizard**.

Click **Add Wireless Device with WPS** If you want to add a wireless device using **Wi-Fi Protected Setup (WPS)**

Product Page: DSL-2740B [Site Map](#) Firmware Version: NA\_1.00

**D-Link**

DSL-2740B **Setup** Advanced Maintenance Status Help

Wizard  
Internet Setup  
**Wireless Settings**  
Local Network  
Time and Date  
Logout

**Wireless Connection**

There are 2 ways to setup your wireless connection. You can use the Wireless Connection Setup wizard or you can manually configure the connection.

Please note that changes made on this section will also need to be duplicated to your wireless clients and PC.

**Wireless Connection Setup Wizard**

If you would like to utilize our easy to use Web-based Wizard to assist you in connecting your new D-Link Systems Wireless Router to the Internet, click on the button below.

[Wireless Connection Setup Wizard](#)

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

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

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

[Add Wireless Device with WPS](#)

**MANUAL WIRELESS CONNECTION OPTIONS**

If you would like to configure the Internet settings of your new D-Link Router manually, then click on the button below.

[Manual Wireless Connection Setup](#)

**Helpful Hints**

Changing your Wireless Network Name (SSID) is the first step in securing your wireless network. Change it to a familiar name that does not contain any personal information.

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

Choosing to hide your wireless network also helps to secure your wireless network, it will mean that wireless clients will not see your network listed when they scan for available networks. To connect your wireless devices to the router you will need to manually enter the Wireless Network Name (SSID) on each device. (Please take a note of your SSID and keep it to hand).

If you have enabled wireless security, please make sure you take a note of your encryption key. You will need to enter this and the SSID on any wireless device that you connect to your network.

[More](#)

# Wireless Connection Setup Wizard

**Network Name SSID:** The SSID (Service Set Identification) is the unique name shared among all devices in a wireless network. The SSID must be identical for all devices in the wireless network.

**Network Key:** You can either have an automatically assigned network key, or choose Manually assign a network key to create one yourself.

**WPA:** Select this option for a higher level of wireless security.

Click **Next**

Review your wireless settings and click **Save** to finish the Setup Wizard.

The screenshot shows the 'WELCOME TO THE D-LINK WIRELESS SECURITY SETUP WIZARD' window. It contains the following elements:

- A header bar with the text: **WELCOME TO THE D-LINK WIRELESS SECURITY SETUP WIZARD**
- Instructional text: Give your network a name, using up to 32 characters.
- A text input field for **Network Name (SSID) :**
- Two radio button options for network key assignment:
  - Automatically assign a network key (Recommended)** (selected with a green dot)
  - Manually assign a network key** (unselected)
- Explanatory text: To prevent outsiders from accessing your network, the router will automatically assign a security key (also called WEP or WPA key) to your network.
- Additional text: Use this option if you prefer to create your own key.
- A checked checkbox for **Use WPA encryption instead of WEP (WPA is stronger than WEP and all D-Link wireless client adapters support WPA)**.
- Two buttons at the bottom: **Next** and **Cancel**.

# Wi-Fi Protected Setup

Select Auto to add a wireless client using WPS. Once you select Auto and click Connect, you will have a 120 second time limit to apply the settings to your wireless client(s) and successfully establish a connection.

If you select Manual, you will be prompted to enter a Network Name (SSID) and Network Key. Click Next and a settings summary screen will appear. Write down the security key and enter this on your wireless clients.

**Pin:** Select this option to use PIN method. In order to use this method you must know the wireless client's 8 digit PIN and click Connect.

**PBC:** Select this option to use PBC (Push Button) method to add a wireless client. Click Connect.

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

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

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

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 press the "Connect" button below within 120 seconds

Prev Connect

# Manual Wireless Setup

**Enable Wireless:** If you would like to make wireless available, you must check this box first.

**Wireless Network Name (SSID):** The SSID (Service Set Identification) is the unique name shared among all devices in a wireless network. The SSID must be identical for all devices in the wireless network.

**Country:** The channel will adjust according to nations to adapt to each nation's frequency provision.

**Wireless Channel:** Auto setting can be selected to allow the device to choose the channel with the least amount of interference.

**802.11 Mode:** Select one of the following:

**802.11g Only** – Select if all of your wireless clients are 802.11g.

**Mixed 802.11g and 802.11b** – Select if you are using both 802.11g and 802.11b wireless clients.

**802.11b Only** – Select if all of your wireless clients are 802.11b.

**802.11n Only** – Select if all of your wireless clients are 802.11n.

**Mixed 802.11n, 802.11b, and 802.11g** – Select if you are using a mix of 802.11n, 11g, and 11b wireless clients.

**Bandwidth:** Select the channel width:

**Auto 20/40** – Select if you are using both 802.11n and non-802.11n wireless devices.

**20MHZ** – Select if you are not using any 802.11n wireless clients. This is the default setting.

**Wireless**

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

---

**Wireless Network Settings**

**Enable Wireless:**  Always  New Schedule

**Wireless Network Name (SSID):**

**Country:** UNITED\_STATES-US

**Wireless Channel:** Auto

**802.11 Mode:** Mixed 802.11n, 802.11g and 802.11b

**Bandwidth:** 20 MHz

**Transmission Rate:** Best (automatic)  (Mbit/s)

**Hide Wireless Network:**

**Clients Isolation:**

**Disable WMM Advertisement:**

---

**Wireless Security Mode**

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

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

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

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

**Security Mode:** WPA2  (AES)

---

**WPA2**

WPA-Personal does not require an authentication server. The WPA-Enterprise option requires an external RADIUS server.

**WPA Mode:** WPA2-PSK (Personal)

**Group Key Update Interval:** 1800 (seconds)

---

**Pre-Shared Key**

**Pre-Shared Key:**

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

**Transmission Rate:** Select the transmission rate. It is strongly suggested to select Best (Auto) for best performance

**Hide Wireless Network:** Check this box if you would like to hide any access point for your router, so a station cannot obtain the SSID through passive scanning.

**Wireless Security Mode:** This device is equipped with 802.1X and WPA/WPA2 (Wi-Fi Protected Access), the latest security standard. Before selecting security mode, consider your network size, complexity and existing authentication infrastructure in order to determine which solution is best.

# Local Network

You can configure the DSL Modem IP address and Subnet Mask for the LAN interface. This section is optional and you do not need to change any of the settings here to get your network up and running.

Click the **Apply** button to save the LAN configuration data. The router will automatically reboot to apply the new configuration.

The screenshot shows the D-Link DSL-2740B web management interface. The main content area is titled "Local Network" and contains the following sections:

- LAN Setup:** A text box explaining that this section is optional and should not be changed if the network is already running.
- Router Settings:** A section for configuring the local network settings. It includes fields for "Router IP Address" (192.168.1.1) and "Subnet Mask" (255.255.255.0). There is a checkbox for "Configure the second IP Address and Subnet Mask for LAN interface" which is currently unchecked. Below it are fields for "IP Address" and "Subnet Mask".
- DHCP Server Settings (Optional):** A section for configuring the built-in DHCP server. It includes a checkbox for "Enable DHCP Server" which is checked. Below it are fields for "DHCP IP Address Range" (192.168.1.2 to 192.168.1.254) and "DHCP Lease Time" (24 hours). A "Save Settings" button is located below these fields.
- DHCP Reservations List:** A table with columns for "Enable", "Computer Name", "MAC Address", and "IP Address". Below the table are "Add", "Edit", and "Delete" buttons.
- Number of Dynamic DHCP Clients:** A table listing dynamic DHCP clients with columns for "Computer Name", "MAC Address", "IP Address", and "Expire Time".

Computer Name	MAC Address	IP Address	Expire Time
DIR-625	00:1e:c9:05:29:58	192.168.1.5	22 hours, 23 minutes, 24 seconds
DHM-4017	f0:7d:68:c8:22:6a	192.168.1.2	20 hours, 44 minutes, 36 seconds
129-katakash2	00:1f:29:98:50:e9	192.168.1.3	20 hours, 51 minutes, 6 seconds
129-katakash2	00:1f:3c:9a:1a:18	192.168.1.4	21 hours, 3 minutes, 32 seconds
DIR-625	00:18:e7:e6:a3:f4	192.168.1.6	22 hours, 32 minutes, 0 seconds
android_9774d56482e549c	00:11:22:33:44:55	192.168.1.7	23 hours, 48 minutes, 3 seconds

# Time and Date

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

The screenshot displays the D-Link DSL-2740B web interface. At the top, it shows 'Product Page: DSL-2740B', 'Site Map', and 'Firmware Version: NA\_1.00'. The D-Link logo is prominently displayed. Below the logo, there are navigation tabs for 'Setup', 'Advanced', 'Maintenance', 'Status', and 'Help'. A sidebar on the left contains a menu with options: 'Wizard', 'Internet Setup', 'Wireless Settings', 'Local Network', 'Time and Date' (which is highlighted), and 'Logout'. The main content area is titled 'Time' and includes a brief description: 'The Time Configuration option allows you to configure, update, and maintain the correct time on the internal system clock. From this section you can set the time zone that you are in and set the NTP (Network Time Protocol) Server. Daylight Saving can also be configured to automatically adjust the time when needed.' Below this, there are three main sections: 1. 'Time settings' with a checkbox for 'Automatically synchronize with Internet time servers' (unchecked) and two NTP server fields (both set to 'ntp.dlink.com.tw'). 2. 'Time Configuration' showing 'Current Router Time: Thursday, January 1, 1970 03:17:14 AM', a 'Time Zone' dropdown set to '(GMT-08:00) Pacific Time, Tijuana', an 'Enable Daylight Saving' checkbox (unchecked), a 'Daylight Saving Offset' dropdown set to '-2:00', and 'Daylight Saving Dates' with 'Start' and 'End' fields set to 'Jan 1st Sun 12 am'. 3. 'Set the Date and Time Manually' with 'Date And Time' fields for Year (2005), Month (Jan), Day (1), Hour (3 am), Minute (8), and Second (55), and a 'Copy Your Computer's Time Settings' button. At the bottom, there are 'Apply' and 'Cancel' buttons. A 'Helpful Hints...' sidebar on the right provides additional information: 'Good timekeeping is important for accurate logs and scheduled firewall rules. Click on the 'Copy your Computer's ...' button will copy your PC's current time. More...'

# Advanced Wireless

You may use this section to manage your wireless settings.

The screenshot displays the D-Link DSL-2740B Advanced Wireless settings page. The page is titled "Product Page: DSL-2740B" and "Firmware Version: NA\_1.00". The D-Link logo is prominently displayed at the top. The navigation menu includes "Setup", "Advanced", "Maintenance", "Status", and "Help". The "Advanced" menu is expanded, showing "Advanced Wireless" as the selected option. The main content area is divided into four sections, each with a description and a button to access the settings:

- Wireless -- Advanced Settings**: Allows you to configure advanced features of the wireless LAN interface. Button: [Advanced Settings](#)
- Wireless -- MAC Filter**: Allows you to configure wireless firewall by denying or allowing designated MAC addresses. Button: [MAC Filter](#)
- Wireless -- Bridge**: Allows you to configure wireless bridge (also known as Wireless Distribution System) features of the wireless LAN interface. Button: [Bridge](#)
- Wireless -- QoS (Quality of Service)**: Allows you to configure wireless QoS. Button: [Quality of Service](#)

# Advanced Settings

You can select a particular channel on which to operate, force the transmission rate to a particular speed, set the fragmentation threshold, set the RTS threshold, set the wake-up interval for clients in power-save mode, set the beacon interval for the access point, set XPress mode and set short or long preambles.

**Band:** Select 802.11b/g using wireless frequency band range. The radio frequency remains at 2.437 GHz.

**Channel:** Fill in the appropriate channel to correspond with your network settings. All devices in your wireless network must use the same channel in order to work correctly. This router supports auto channeling functionality.

**Auto Channel** Specifies the auto channelling timing.

**Timer:**

**54g™ Rate:** Select the transmission rate for the network. The rate of data transmission should be set depending on the speed of your wireless network. You can select from a range of transmission speeds, or you can select Auto to have the Router automatically use the fastest possible data rate and enable the Auto-Fallback feature. Auto-Fallback will negotiate the best possible connection speed between the Router and a wireless client. The default value is Auto.

**Multicast Rate:** Select the multicast transmission rate for the network. The rate of data transmission should be set depending on the speed of your wireless network. You can select from a range of transmission speeds, or you can select Auto to have the Router automatically use the fastest possible data rate and enable the Auto-Fallback feature. Auto-Fallback will negotiate the best possible connection speed between the Router and a wireless client. The default value is Auto.

**Basic Rate:** Select the basic transmission rate ability for the access point.

**Guest Wireless:** Allows you to create a temporary zone that can be used by guests to access the internet. This zone will be separate from your main wireless network.

**Wireless -- Advanced Settings**

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

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

**Advanced Settings**

Band:	<input type="text" value="2.4GHz"/>
Channel:	<input type="text" value="Auto"/>
Auto Channel Timer(min):	<input type="text" value="0"/>
802.11n/EWC:	<input type="text" value="Auto"/>
Bandwidth:	<input type="text" value="20MHz"/>
802.11n Rate:	<input type="text" value="Auto"/>
802.11n Protection:	<input type="text" value="Off"/>
Support 802.11n Client Only:	<input type="text" value="Off"/>
OBS5 Co-Existence:	<input type="text" value="Disable"/>
54g™ Rate:	<input type="text" value="1 Mbps"/>
Multicast Rate:	<input type="text" value="Auto"/>
Basic Rate:	<input type="text" value="Default"/>
Fragmentation Threshold(byte):	<input type="text" value="2346"/>
RTS Threshold(byte):	<input type="text" value="2347"/>
DTIM Interval(ms):	<input type="text" value="1"/>
Beacon Interval(ms):	<input type="text" value="100"/>
XPress™ Technology:	<input type="text" value="Disabled"/>
Transmit Power:	<input type="text" value="100%"/>

**GUEST Wireless Settings**

**Enable Wireless Guest Network:**

**Wireless Network Name (SSID):**

**Hide Wireless Network:**

**AP Isolation:**

**GUEST Wireless Security Mode**

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

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

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

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

**Security Mode:**

# MAC Filter

The web page allows you to create a list of MAC addresses that are banned or allowed association with the wireless access point.

**MAC Restrict** The function can be turned on/off, select **Disabled** to disable this function. Vice versa, to enable the function. After enabling the function, you can filter wireless users according to their MAC address, either allowing or denying access. Select **Allow** to make any wireless MAC address in the Wireless Access Control List can be linked to. And select **Deny** to ban any wireless MAC address in the Wireless Access Control List.

**Add a MAC** To add a new MAC address to your wireless MAC address filters, click **Access Control: Add** to show the next page. Type the MAC Address in the entry field provided.

**Remove a MAC** Select the checkbox in the right column of the list for the MAC address **Access Control:** to be removed and click **Remove**.

Click **Save/Apply** to add the MAC address to the list.

**Wireless -- MAC Filter**

Sets wireless MAC filter.

Enter the MAC address and click "Add" to add the MAC address to the wireless MAC address filters.

**Wireless -- MAC Filter**

Select SSID:

MAC Restrict Mode:  Disabled  Allow  Deny

MAC Address	Remove
<input type="text"/>	<input type="button" value="Remove"/>

# Wireless Bridge

The Wireless Distribution System (WDS) allows you to extend the range of your wireless network by introducing one or more WDS-enabled devices into your wireless network. You can only establish WDS links with WDS-enabled devices.

**AP Mode:** Select Access Point's functionality to be Access Point or pure Wireless Bridge. You can select Wireless Bridge (also known as Wireless Distribution System) to disable access point functionality. Selecting Access Point enables access point functionality and Wireless bridge functionality will still be available and wireless stations will be able to associate to the AP.

**Bridge Restrict:** Select Disabled to turn off wireless bridge restrictions. Any wireless bridge will be granted access. Selecting Enabled or Enabled (Scan) enables wireless bridge restriction. If enabled, only the specified bridges are granted access.

Click **Save/Apply** to configure the wireless bridge options and put the modifications into effect.

**Wireless -- Bridge**

This page allows you to configure wireless bridge features of the wireless LAN interface. Wireless Bridge (also known as Wireless Distribution System) allows wireless interconnection of access points. WDS can be used in combination with bridge mode to extend the range of a wireless network, without need for a wired backbone to link the access points. You can select AP mode to Access Point or Wireless Bridge mode by this feature. Selecting Enabled or Enabled(Scan) enables wireless bridge restriction, and only those bridges selected in Remote Bridges will be granted access.

**Wireless bridge support only the repeaters which have same channel with it.**  
Click "Refresh" to update the remote bridges. Wait for few seconds to update.  
Click "Save/Apply" to configure the wireless bridge options.

**Wireless -- Bridge**

AP Mode:	<input type="text" value="Access Point"/>
Bridge Restrict:	<input type="text" value="Enabled"/>

# Wireless QoS

This page allows you to control the wireless traffic QoS rule which consists of a class name and at least one condition.

**Wireless -- QoS**

The screen controls a wireless traffic QoS rule. A rule consists of a class name and at least one condition below. All of the specified conditions in this classification rule must be satisfied for the rule to take effect. Click 'Apply' to save and activate the rule.

**Add/Edit Wireless Quality of Service Rule**

Traffic Class Name:

**Assign Wireless Priority**

Wireless Transmit Priority:

**Specify Traffic Classification Rules**

Protocol:

Source IP Address:

Source Subnet Mask:

UDP/TCP Source Port (port or port:port):

Destination IP Address:

Destination Subnet Mask:

UDP/TCP Destination Port (port or port:port):

# Port Forwarding

Port forwarding allows you to direct incoming traffic from the WAN side to the internal server with a private IP address on the LAN side.

Product Page: DSL-2740B [Site Map](#) Firmware Version: NA\_1.00

**D-Link**

DSL-2740B **Setup** **Advanced** Maintenance Status Help

Advanced Wireless  
**Port Forwarding**  
 Port Triggering  
 DMZ  
 Parental Control  
 Filtering Options  
 Firewall Settings  
 DNS  
 Dynamic DNS  
 Network Tools  
 Routing  
 Schedules  
 TR-069 Client  
 WI-FI Protected Setup  
 Power Management  
 Logout

**Port Forwarding**

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

Select the service name, and enter the server IP address and click "Apply" to forward IP packets for this service to the specified server. **NOTE: The "Internal Port End" cannot be changed. It is the same as "External Port End" normally and will be the same as the "Internal Port Start" or "External Port End" if either one is modified**

**Port Forwarding Setup**

Server Name	External Port Start	External Port End	Protocol	Internal Port Start	Internal Port End	Server IP Address	Remote IP Address	Inbound Filter	WAN Interface
<input type="text"/>									

**Helpful Hints...**  
 Check the Application Name drop down menu for a list of predefined applications.  
[More...](#)

Select the **Service Name** and enter the IP server Address, then click **Apply**.

**Port Forwarding Setup**

Remaining number of entries that can be configured:32

Use Interface :

Server Name :

**Select a Service :**

**Custom Server :**

Inbound Filter :

Server IP Address :  [192.168.1.1 - 192.168.1.254]

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

# Port Triggering

If you configure port triggering for a certain application, you must determine a so-called trigger port and the protocol (TCP or UDP) that this port uses. You then assign the public ports that are to be opened for the application to this trigger port. You can select known Internet services or manually assign ports or port blocks.

Product Page: DSL-2740B [Site Map](#) Firmware Version: NA\_1.00

**D-Link**

DSL-2740B **Setup** **Advanced** Maintenance Status Help

Advanced Wireless  
Port Forwarding  
**Port Triggering**  
DMZ  
Parental Control  
Filtering Options  
Firewall Settings  
DNS  
Dynamic DNS  
Network Tools  
Routing  
Schedules  
TR-069 Client  
Wi-Fi Protected Setup  
Power Management  
Logout

**Port Triggering**

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

Some applications such as games, video conferencing, remote access applications and others require that specific ports in the Router's firewall be opened for access by the applications. You can configure the port settings from this screen by selecting an existing application or creating your own (Custom application) and click "Apply" to add it. The addition of the differences of trigger port range should not be higher than 1000.

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

**Port Triggering**

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

Add Edit Delete

**Port Triggering**

Remaining number of entries that can be configured :32

Use Interface : pppoe\_atm0\_1/ppp0\_2

Application Name :  
 Select an application : (Click to select)   
 Custom application :   
 Schedule : Always [View Available Schedules](#)

Trigger Port Start	Trigger Port End	Trigger Protocol	Open Port Start	Open Port End	Open Protocol
		TCP			TCP
		TCP			TCP
		TCP			TCP
		TCP			TCP
		TCP			TCP
		TCP			TCP
		TCP			TCP
		TCP			TCP
		TCP			TCP
		TCP			TCP

Apply Cancel

**Helpful Hints...**

Use this feature if you are trying to execute one of the listed network applications and it is not communicating as expected.

Check the Application Name drop down menu for a list of predefined applications.

[More...](#)

# DMZ Host

The demilitarized military zone (DMZ) host feature allows one local network device to be exposed to the Internet. This function is applicable for:

- Users who want to use a special-purpose Internet service, such as an on-line game or video conferencing program, that is not in the port forwarding list and for which no port range information is available.
- Users who are not concerned with security and wish to expose one computer to all services without restriction.

**Note:** A DMZ host is not protected by the firewall and may be vulnerable to attack. This may also put other computers in the home network at risk. Hence, when designating a DMZ host, you must consider the security implications and take the appropriate precautions.

You can set up a client in your local network as a DMZ host. Your device then forwards all incoming data traffic from the Internet to this client. You can, for example, operate your own Web server on one of the clients in your local network and make it accessible to Internet users. As the exposed host, the local client is directly visible to the Internet and therefore particularly vulnerable to attacks (for example, hacker attacks). Enable this function only when necessary (for example, to operate a Web server) and when other functions (for example, port forwarding) are inadequate. In this case, you should take appropriate measures for the clients concerned.

**Note:** Only one PC per public IP address can be setup as an exposed host.

### Demilitarized Zone

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

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

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

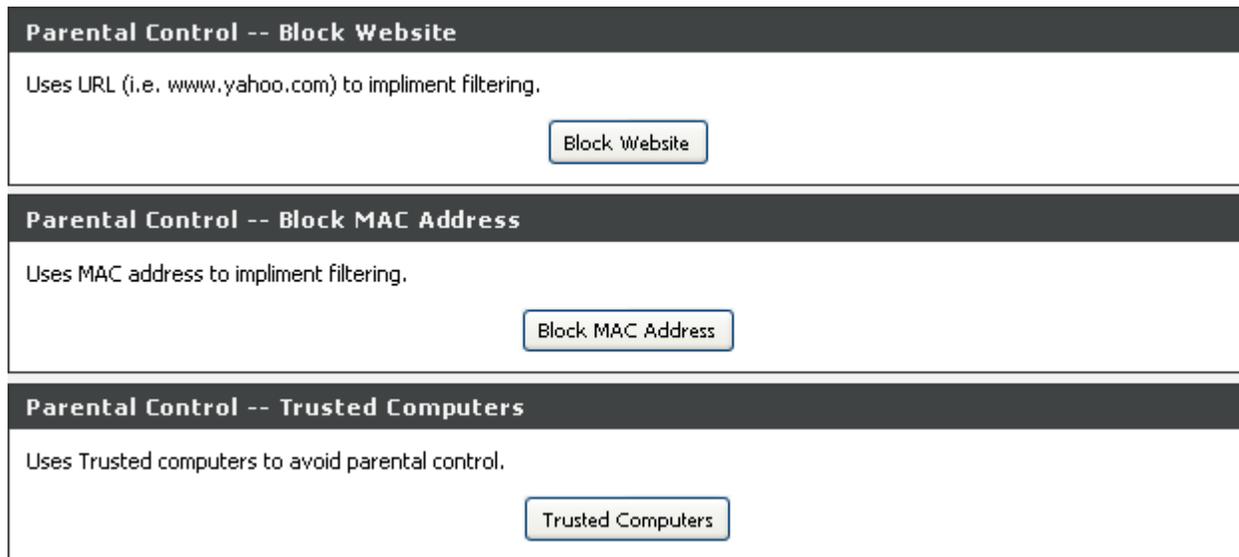
### DMZ Host

**DMZ Host IP Address :**  [192.168.1.1 - 192.168.1.254]

# Parental Control

Click on **Advanced > Parental Control** and the following page will appear.

Click **Block MAC Address** to continue and be directed to the next page.



## Block MAC Address

In this page, you can add a time of day restriction to a particular LAN device connected to the Router. The Browser's MAC Address automatically displays the MAC address of the LAN device where the browser is running. To restrict other LAN device, click Other MAC Address and enter the MAC address of the another LAN device. To obtain the MAC address of a Windows based PC, enter ipconfig /all in the DoS window.

### Block MAC Address

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

### Block MAC Address

Username	MAC	Schedule Rule
----------	-----	---------------

### Time of Day Restriction

User Name:

**Browser's MAC Address:**

**Other MAC Address:**

**Blocking on Schedule:**  [View Schedule Details](#)

# Filtering Options

This screen allows you to choose the Filtering Options you would like to access. You may select: **Inbound IP Filtering**, **Outbound IP Filtering** or **Bridge Filtering** to be directed to the page.

The screenshot displays the D-Link DSL-2740B Advanced Setup interface. At the top, it shows 'Product Page: DSL-2740B', a 'Site Map' link, and 'Firmware Version: NA\_1.00'. The D-Link logo is prominently displayed. Below the logo, a navigation bar includes 'DSL-2740B', 'Setup', 'Advanced' (highlighted), 'Maintenance', 'Status', and 'Help'. A left sidebar lists various settings: 'Advanced Wireless', 'Port Forwarding', 'Port Triggering', 'DMZ', 'Parental Control', 'Filtering Options' (highlighted), 'Firewall Settings', 'DNS', 'Dynamic DNS', 'Network Tools', 'Routing', 'Schedules', 'TR-069 Client', 'WI-FI Protected Setup', 'Power Management', and 'Logout'. The main content area is divided into three sections:

- Filter -- Inbound IP Filter**: Manage incoming traffic. Includes an 'Inbound' button.
- Filter -- Outbound IP Filter**: Manage outgoing traffic. Includes an 'Outbound' button.
- Filter -- Bridge Filter**: Uses MAC address to implement filtering. Useful only in bridge mode. Includes a 'Bridge' button.

## Incoming IP Filtering Setup

The Inbound Filter option is an advanced method of controlling data received from the Internet. With this feature you can configure inbound data filtering rules that control data based on an IP address range. Inbound Filters can be used with Virtual Server, Port Forwarding, or Remote Administration features.

The Add IP Filter screen will appear when you click **Add**. Enter a filter name, protocol, source address information (from the WAN side) and destination address information (to the LAN side). Select the WAN interface and when ready, click **Apply** to add the filter.

**Incoming IP Filtering**

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

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

**Active Inbound Filter**

Name	VPI/VCI	Protocol	Source Address / Mask	Source Port	Dest. Address / Mask	Dest. Port	Schedule Rule
<div style="display: flex; justify-content: center; gap: 10px;"> <span>Add</span> <span>Edit</span> <span>Delete</span> </div>							

**Inbound IP Filtering**

**Filter Name :**

**Protocol :** (Click to select) ▾

**Source IP Type :** Single IP ▾

**Source IP address :**

**Source Subnet Mask :**

**Source Port :**  (port or port:port)

**Destination IP Type :** Single IP ▾

**Destination IP address :**

**Destination Subnet Mask :**

**Destination Port :**  (port or port:port)

**Schedule :** Always ▾ [View Available Schedules](#)

**WAN Interfaces (Configured in Routing mode and with firewall enabled only)**  
 Select at least one or multiple WAN interfaces displayed below to apply this rule.

Select All

pppoe\_atm0\_1/ppp0\_2

br0/br0

Apply
Cancel

## Outgoing IP Filtering Setup

This feature allows you to create a filter rule to identify outgoing IP traffic by specifying a new filter name and at least one condition. All of the specified conditions in the filter rule must be satisfied for the rule to take effect.

This next screen will appear when you click **Add**. Enter the **Filter Name**, the **Source IP Address**, and destination information (from the WAN side). Then click **Apply** to save.

**Outgoing IP Filtering**

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

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

**Active Outbound Filter**

Name	Protocol	Source Address / Mask	Source Port	Dest. Address / Mask	Dest. Port	Schedule Rule
<input type="button" value="Add"/> <input type="button" value="Edit"/> <input type="button" value="Delete"/>						

**Outbound IP Filtering**

**Filter Name :**

**Protocol :** (Click to select) ▼

**Source IP Type :** Single IP ▼

**Source IP address :**

**Source Subnet Mask :**

**Source Port :**  (port or port:port)

**Destination IP Type :** Single IP ▼

**Destination IP address :**

**Destination Subnet Mask :**

**Destination Port :**  (port or port:port)

**Schedule :** Always ▼ [View Available Schedules](#)

# Bridge Filtering Setup

Bridge Filtering is only effective on ATM PVC's configured in Bridge mode. MAC filtering can forward or block traffic by MAC address. You can change the policy or add settings to the MAC filtering table using the MAC Filtering Setup screen.

If you want to add an entry to the MAC filtering table, Select **Add** from the MAC Filtering Setup screen. The Add MAC Filter screen should then appear. Select a Protocol Type, enter the Destination and Source MAC address, the necessary Frame Direction, and WAN interface (bridge mode only). Click **Apply** to save.

**Bridge Filtering**

Bridge Filtering is only effective on ATM PVCs configured in Bridge mode. **ALLOW** means that all MAC layer frames will be **ALLOWED** except those matching with any of the specified rules in the following table. **DENY** means that all MAC layer frames will be **DENIED** except those matching with any of the specified rules in the following table.

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

**Bridge Filtering Policy(Configured in Bridge mode only)**

FORWARD:**ALLOW** all packets but **DENY** those matching any of specific rules listed  
 BLOCKED:**DENY** all packets but **ALLOW** those matching any of specific rules listed

Bridge Interface	Policy

**Bridge Filter Setup**

Name	VPI/VCI	Protocol	Destination MAC	Source MAC	Frame Direction	Schedule Rule

**Add Bridge Filter**

Filter Name:

Protocol Type:

Destination MAC Address:

Source MAC Address:

Frame Direction:

Schedule:  [View Schedule Details](#)

WAN Interfaces (Configured in Bridge mode only)

Select All

# Firewall

A firewall protects your network from the outside world. Check the box marked Enable Attack Prevention to prevent cyber attacks.

**Firewall Settings**

Click "Apply" button to make the changes effective immediately.

**Firewall Configuration**

**Enable Attack Prevention**

Type	Rate(pkt/sec)	Burst
TCP DoS:	<input type="text"/>	<input type="text"/>
Ping DoS:	<input type="text"/>	<input type="text"/>
Port Scan:	<input type="text"/>	<input type="text"/>

Prevent IP Spoofing:

# DNS

If **Obtained DNS server address automatically** is selected, this router accepts the first received DNS assignment from one of the PPPoA, PPPoE or MER/DHCP enabled PVC(s) during the connection establishment.

If the checkbox is not selected, enter the primary and secondary (optional) DNS server IP addresses. The interface is as follows.

Click **Save** to save the new configuration.

**Note:** You must reboot the router to make the new configuration take effect.

**DNS**

Click "Apply" button to save the new configuration. You must reboot the router to make the new configuration effective.

**DNS Server Configuration**

**Obtain DNS server address automatically**

WAN Interface selected: pppoe\_atm0\_1/ppp0\_2

**Use the following DNS server addresses**

Preferred DNS server:

Alternate DNS server:

Apply Cancel

# Dynamic DNS

The DDNS feature allows you to host a server (Web, FTP, Game Server, etc...) using a domain name that you have purchased (www.whateveryournameis.com) with your dynamically assigned IP address. Most broadband Internet Service Providers assign dynamic (changing) IP addresses. Using a DDNS service provider, your friends can enter in your domain name to connect to your server no matter what your IP address is.

**D-DNS** Choose your DDNS provider from the drop down

**Provider:** menu.

**Hostname:** Enter the Host Name that you registered with your DDNS service provider.

**Interface:** Select your interface from the drop down menu.

**Username Name:** Enter the Username for your DDNS account.

**Password:** Enter the Password for your DDNS account.

The screenshot shows the 'Dynamic DNS' configuration page. At the top, there is a header 'DDNS' and a sub-header 'Dynamic DNS'. Below the sub-header, there is a table with four columns: 'Hostname', 'Username', 'Service', and 'Interface'. Below the table, there are three buttons: 'Add', 'Edit', and 'Delete'. Below the buttons, there is a section titled 'Add dynamic DNS' with the following fields: 'D-DNS provider' (a dropdown menu with 'dlink.ddns.com(Free)' selected), 'Hostname' (a text input field), 'Interface' (a dropdown menu with 'pppoe\_atm0\_1/ppp0\_2' selected), 'Username' (a text input field), and 'Password' (a text input field). At the bottom of the section, there are two buttons: 'Apply' and 'Cancel'.

# Network Tools

Product Page: DSL-2740B [Site Map](#) Firmware Version: NA\_1.00

**D-Link**

DSL-2740B **Setup** **Advanced** Maintenance Status Help

Advanced Wireless

Port Forwarding

Port Triggering

DMZ

Parental Control

Filtering Options

Firewall Settings

DNS

Dynamic DNS

**Network Tools**

Routing

Schedules

TR-069 Client

WI-FI Protected Setup

Power Management

Logout

**Network Tools -- Port Mapping**

Port Mapping supports multiple port to PVC and bridging groups. Each group will perform as an independent network.

[Port Mapping](#)

**Network Tools -- IGMP**

Transmission of identical content, such as multimedia, from a source to a number of recipients.

[IGMP](#)

**Network Tools -- QoS**

Allows you to manually configure special routes that your network might need.

[Quality of Service](#)

**Network Tools -- ADSL**

Allows you to configure Default Gateway used by WAN Interface.

[ADSL Settings](#)

**Network Tools -- SNMP**

Allows you to configure SNMP (Simple Network Management Protocol).

[SNMP](#)

**Network Tools -- UPNP**

Allows you to configure UPNP.

[UPNP](#)

# Port Mapping

Port Mapping supports multiple ports to PVC and bridging groups. Each group performs as an independent network. To support this feature, you must create mapping groups with appropriate LAN and WAN interfaces using the **Add** button. The **Delete** button removes the grouping and adds the ungrouped interfaces to the Default group. Only the default group has the IP interface.

### Port Mapping

To create a new mapping group:

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

### Port Mapping Configuration

Group Name:

WAN Interface used in the grouping:

Grouped LAN Interfaces

Available LAN Interfaces

WIRELESS1  
ath1  
LAN1  
LAN2  
LAN3  
LAN4

Automatically Add Clients With the following DHCP Vendor IDs

Apply Cancel

Please take notice that you should reboot your device after you apply the port mapping settings. This makes sure that the port mapping works well.

# IGMP

If you choose to **Enable IGMP Snooping** the device can make intelligent multicast forwarding toward those hosts which request to join a specific multicast group within the broadcast domain.

**IGMP**

Transmission of identical content, such as multimedia, from a source to a number of recipients.

**IGMP Setup**

**Enable IGMP Snooping**

Standard Mode

Blocking Mode

Apply Cancel

# Quality of Service

QoS (Quality of Service) is a method for identifying, classifying, and assigning priorities to traffic that passes through the router. This ensures that time sensitive data (e.g. video streaming) is given priority over other non-essential data.

This screen allows you to add a network traffic class rule. A rule consists of a traffic class name and at least one condition. All configured conditions must first be met before the rule takes effect. Click **Apply** to save any changes.

### Wireless -- QoS

This page lets you add, remove, enable and disable wireless QoS.

#### WMM(Wi-Fi Multimedia) Settings

WMM(Wi-Fi Multimedia):  ▾  
WMM No Acknowledgement:  ▾  
WMM APSD:  ▾

#### Wireless QoS Classes

Class Name	Priority	TRAFFIC CLASSIFICATION RULES				
		Protocol	Source Addr./Mask	Source Port	Dest. Addr./Mask	Dest. Port

# ADSL Setting

In this page, you can configure the modem's ADSL modulation. Select from the settings below and click **Apply**.

### DSL

This page allows you to configure the modems DSL modulation.  
Select the modulation below.

### DSL Settings

Select the modulation below.

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

Select the phone line pair below.

- Inner pair
- Outer pair

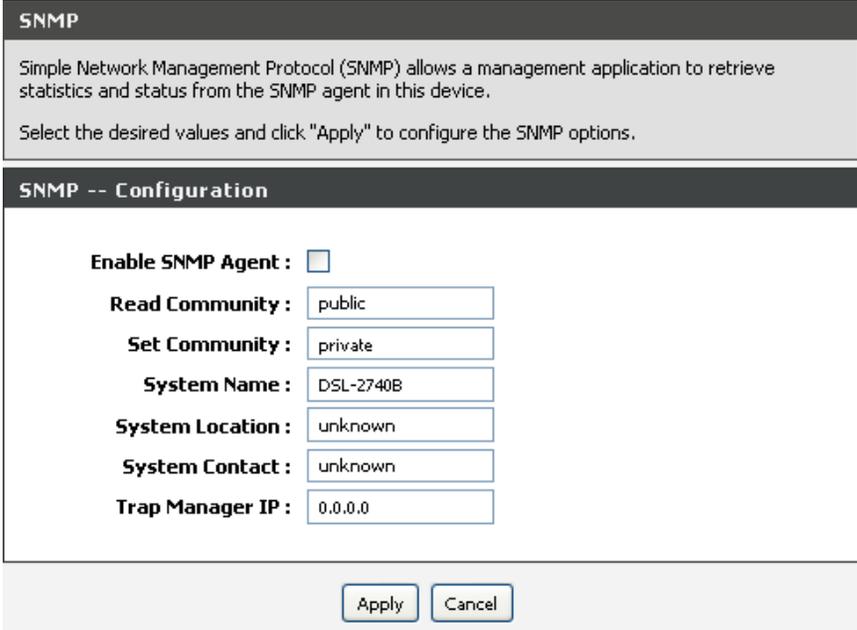
Capability

- Bitswap Enable
- SRA Enable

# SNMP

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

Check the box marked Enable SNMP Agent to use this feature.



The image shows a configuration window titled "SNMP". It contains an introductory text block and a "Configuration" section with several input fields. At the bottom are "Apply" and "Cancel" buttons.

**SNMP**

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

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

**SNMP -- Configuration**

**Enable SNMP Agent :**

**Read Community :** public

**Set Community :** private

**System Name :** DSL-2740B

**System Location :** unknown

**System Contact :** unknown

**Trap Manager IP :** 0.0.0.0

Apply Cancel

# UPnP

Universal Plug and Play (UPnP) provides compatibility with networking equipment, software and peripherals.

Check the box marked Enable UPNP support to use this feature.

**UPNP**

UPNP function allows you to easily config your connected lan pc to automatic port map in order to transversal the NAT in your router. If enable UPNP, you router will auto open ports related to P2P clients such as BT/Emule, etc.

**UNPN -- Configuration**

Enable UPNP support :

Apply Cancel

# TR-069

TR-69 allows a Auto-Configuration Server (ACS) to perform auto-configuration, provision, collection, and diagnostics to this device.

### TR-069 Client

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

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

#### TR-069 client -- Configuration

Inform  Disable  Enable

Inform Interval (sec):

ACS URL:

ACS User Name:

ACS Password:

WAN Interface used by TR-069 client:

Display SOAP messages on serial console  Disable  Enable

Connection Request Authentication

Connection Request User Name:

Connection Request Password:

Connection Request URL:

# Routing

## Static Route

The Static Route page can be used to add a routing table (a maximum of 32 entries can be configured). To proceed, click **Add**.

**Routing**

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

**A maximum 32 entries can be configured**

**Static Route**

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

**Static Route Add/Edit**

**Destination Network Address :**

**Subnet Mask :**

**Use Gateway IP Address :**

**Use Interface :**

For the **Static Route Add** page, enter the destination network address, subnet mask, gateway and select an available WAN interface. When complete, click **Apply**.

**Static Route Add/Edit**

**Destination Network Address :**

**Subnet Mask :**

**Use Gateway IP Address :**

**Use Interface :**

## Default Gateway

In this page, you can modify the default gateway settings. If you select **Enable Automatic Assigned Default Gateway**, this router can accept the first received default gateway assignment from one of the PPPoA, PPPoE or MER/DHCP enabled PVC(s). If the check box is not selected, you must enter the static default gateway and/or a WAN interface. Then, click **Save/Apply**.

**Note:** If the Automatic Assigned Default Gateway check box is changed from deselected to selected, you must reboot the router to obtain the automatic assigned default gateway.

**Routing -- Default Gateway**

Select a preferred wan interface as the system default gateway. Click "Apply" button to save it.

**Default Gateway**

Use Interface:

# RIP

To activate RIP for the device, select the **Enabled** checkbox for Global RIP Mode.

To configure an individual interface, select the desired RIP version and operation, followed by placing a check in the **Enabled** checkbox for the interface.

Click the “Apply” button to save the configuration, and to start or stop RIP based on the Global RIP Mode selected.

### Routing -- RIP

**NOTE: RIP CANNOT BE CONFIGURED on the WAN interface which has NAT enabled and un-ppoe .**

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

### Routing -- RIP Configuration

Interface	Version	Operation	Enabled
atm0	2	Passive	<input type="checkbox"/>

Save/Apply

# Schedules

This section allows you to create scheduling rules to be applied to your firewall. Give each schedule a name and time that is meaningful you.

### Schedule

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

### Schedule Rule

Rule Name	Sun	Mon	Tue	Wed	Thu	Fri	Sat	Start	Stop

### Add Schedule Rule

**Name:**

**Day(s):**  All Week  Select Day(s)  
 Sun  Mon  Tue  Wed  Thu  Fri  Sat

**All Day - 24 hrs:**

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

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

# Maintenance

This page allows you to reboot your router or save your router configuration to a file in your computer as a precaution or in case you have to reset your computer to factory default settings. You will be able to restore your router settings from a previously saved configuration file.

## System

The screenshot displays the maintenance interface for a D-Link DSL-2740B router. At the top, it shows the product page information: "Product Page: DSL-2740B", "Site Map", and "Firmware Version: NA\_1.00". The D-Link logo is prominently displayed. Below the logo, there is a navigation menu with tabs for "DSL-2740B", "Setup", "Advanced", "Maintenance" (which is currently selected), "Status", and "Help".

The main content area is divided into several sections under the "System" heading:

- System -- Reboot:** Contains the instruction "Click the button below to reboot the router." and a "Reboot" button.
- System -- Backup Settings:** Contains the instruction "Backup DSL Router configurations. You may save your router configurations to a file on your PC." and a "Backup Settings" button.
- System -- Update Settings:** Contains the instruction "Update DSL Router settings. You may update your router settings using your saved files." and a form with a "Settings File Name:" label, a text input field, a "Browse..." button, and an "Update Settings" button.
- System -- Restore Default Settings:** Contains the instruction "Restore DSL Router settings to the factory defaults." and a "Restore Default Settings" button.

On the right side of the page, there is a "Helpful Hints..." section with a "More..." link. The hints text reads: "This page allows you to reboot your router or save your router configuration to a file on your computer as a precaution in case you have to reset your router to factory default settings. You will be able to restore your router settings from a previously saved configuration file. There is also a function to allow you to reset your router to factory default settings. Resetting your router to factory default settings will erase your current configuration."

# Firmware Update

This page displays your device's firmware version and information that will be helpful for D-Link technicians should you need technical support. You may also upload new firmware to your router through this page.

Product Page: DSL-2740B [Site Map](#) Firmware Version: NA\_1.00

**D-Link**

DSL-2740B **Setup** **Advanced** **Maintenance** **Status** **Help**

System  
**Firmware Update**  
Access Controls  
Diagnostics  
System Log  
Logout

**Firmware**

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

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

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

NOTE: The update process takes about 2 minutes to complete, and your DSL Router will reboot. Please DO NOT power off your router before the update is complete.

**Firmware Update**

Firmware Date: Dec 22 2010  
Board ID: AW4339U  
Software Version: NA\_1.00  
Bootloader (CFE) Version: 1.0.37-106.5  
Wireless Driver Version: CR-LSDK-1.4.0.112

Firmware File Name:

**Helpful Hints...**

**Please Note:** As firmware is often released to correct a specific issue, it is recommended that there is no need to update your firmware if you are not experiencing any technical concerns or difficulties in the operation of your product.

[More...](#)

# Access Control Account Password

In this section, you can modify your router's password which is needed to access the Web management Interface. It is recommended that you change the factory default password for security purposes. To change your password, choose between 1 and 16 characters.

The screenshot displays the D-Link DSL-2740B web management interface. At the top, it shows 'Product Page: DSL-2740B' and 'Firmware Version: NA\_1.00'. The D-Link logo is prominently displayed. Below the logo, there are navigation tabs for 'Setup', 'Advanced', 'Maintenance' (which is selected), 'Status', and 'Help'. On the left side, there is a sidebar menu with options: 'System', 'Firmware Update', 'Access Controls' (highlighted), 'Diagnostics', 'System Log', and 'Logout'. The main content area is titled 'Access Control -- Passwords'. It contains the following text: 'Access to your DSL Router is controlled through three user accounts: admin, support, and user. The user name "support" is used to allow an ISP technician to access your DSL Router for maintenance and to run diagnostics. The user name "user" can access the DSL Router, view configuration settings and statistics, as well as, update the router's firmware. Use the fields below to enter up to 16 characters and click "Apply" to change or create passwords. Note: Password cannot contain a space.' Below this text is the 'Administrator Settings' section, which includes a 'Username:' dropdown menu (currently showing '(Click to Select)'), and three text input fields for 'Old Password:', 'New Password:', and 'Confirm Password:'. At the bottom of this section are 'Apply' and 'Cancel' buttons. Below the Administrator Settings is the 'GRAPHIC LOG-IN AUTHENTICATION (CAPTCHA)' section, which contains the text 'To enhance your router login security.' and a checkbox for 'Enable CAPTCHA:' which is currently unchecked. At the bottom of this section are 'Apply' and 'Cancel' buttons. On the right side of the interface, there is a 'Helpful Hints...' section with the text: 'For security reasons, it is recommended that you change the password for the Admin and User accounts. Be sure to write down the new passwords to avoid having to reset the router in case they are forgotten.' and a 'More...' link.

# Services

In this page, you will be able to enable or disable services from being used.

Product Page: DSL-2740B Site Map Firmware Version: NA\_1.00

---

**D-Link**

DSL-2740B Setup Advanced Maintenance Status Help

System

Firmware Update

Access Controls

Diagnostics

System Log

Logout

**Access Control -- Services**

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

**Access Control -- Services**

Service	LAN	WAN	Remote WAN Port
FTP	<input type="checkbox"/> Enabled	<input type="checkbox"/> Enabled	<input type="text" value="21"/>
HTTP	<input checked="" type="checkbox"/> Enabled	<input type="checkbox"/> Enabled	<input type="text" value="80"/>
ICMP	<input checked="" type="checkbox"/> Enabled	<input type="checkbox"/> Enabled	
SNMP	<input checked="" type="checkbox"/> Enabled	<input type="checkbox"/> Enabled	<input type="text" value="161"/>
SSH	<input type="checkbox"/> Enabled	<input type="checkbox"/> Enabled	<input type="text" value="22"/>
TELNET	<input type="checkbox"/> Enabled	<input type="checkbox"/> Enabled	<input type="text" value="23"/>
TFTP	<input type="checkbox"/> Enabled	<input type="checkbox"/> Enabled	<input type="text" value="69"/>

[Helpful Hints...](#)

Remote Management by default should be disabled. However if you wish to login and manage your Router from another Internet device then you can enable the router to accept such commands from the Internet port. This option may be useful if your network administrator is not onsite or Technical Support request such access.

[More...](#)

# IP Address

This page allows you to restrict users from accessing the local management using IP address. Check **Enable Access Control Mode** to access local management services from IP addresses contained in the Access Control List. If Access Control Mode is disabled, the system will not validate IP addresses for incoming packets.

**Note:** Add your IP address to the list before you enable the service.

The screenshot displays the D-Link DSL-2740B web interface. At the top, it shows 'Product Page: DSL-2740B' and 'Firmware Version: NA\_1.00'. The main navigation bar includes 'DSL-2740B', 'Setup', 'Advanced', 'Maintenance' (highlighted), 'Status', and 'Help'. A left sidebar lists 'System', 'Firmware Update', 'Access Controls' (highlighted), 'Diagnostics', 'System Log', and 'Logout'. The main content area is titled 'Access Control -- IP Address' and contains the following text: 'The IP Address Access Control mode, if enabled, permits access to local management services from IP addresses contained in the Access Control List. If the Access Control mode is disabled, the system will not validate IP addresses for incoming packets. The services are the system applications listed in the Service Control List.' Below this, it says 'Enter the IP address of the management station permitted to access the local management services, and click 'Apply.''. There are two radio buttons for 'Access Control Mode': 'Disabled' (selected) and 'Enabled'. Below the radio buttons is a table with two columns: 'IP Address' and 'Select'. At the bottom of the main content area are three buttons: 'Add', 'Edit', and 'Delete'. On the right side, there is a 'Helpful Hints...' section with the text: 'You can restrict users who can access the local management using IP address.' and a note: 'Note: Be sure to add your IP Address in the list before you enable the service.' There is also a 'More...' link.

# Diagnostics

This page displays your router's self diagnostic and connection test results. The internet connectivity status will only show PASS if you have correctly configured your Internet connection and if your router is currently online.

Product Page: DSL-2740B [Site Map](#) Firmware Version: NA\_1.00

**D-Link**

DSL-2740B **Setup** **Advanced** **Maintenance** **Status** **Help**

System  
Firmware Update  
Access Controls  
**Diagnostics**  
System Log  
Logout

**dlink pvc Diagnostics**

**Diagnostics**

Your modem is capable of testing your DSL connection. The individual tests are listed below. If a test displays a fail status, click "Help" and follow the troubleshooting procedures.

Virtual Circuit :

**Test the connection to your local network**

Test your LAN1 Connection:	PASS	<a href="#">Help</a>
Test your LAN2 Connection:	FAIL	<a href="#">Help</a>
Test your LAN3 Connection:	FAIL	<a href="#">Help</a>
Test your LAN4 Connection:	PASS	<a href="#">Help</a>
Test your Wireless Connection:	PASS	<a href="#">Help</a>
Test ADSL Synchronization:	PASS	<a href="#">Help</a>

**Test the connection to your Internet service provider**

Ping default gateway:	PASS	<a href="#">Help</a>
Ping primary Domain Name Server:	PASS	<a href="#">Help</a>

**Helpful Hints...**

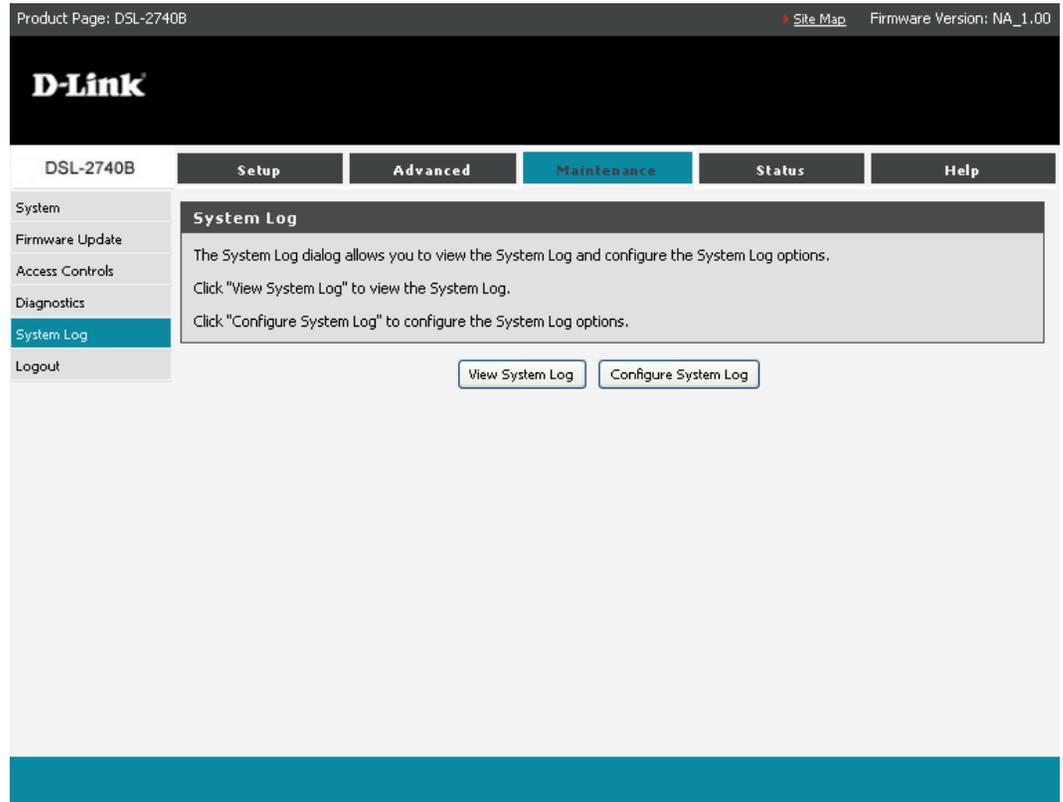
The tests on this page can be used to verify whether or not your router is working correctly. If you have rerun the tests and consulted the help file and you are still experiencing difficulties, please contact D-link or visit our support website at [support.dlink.co.uk](http://support.dlink.co.uk)

[More...](#)

# System Log

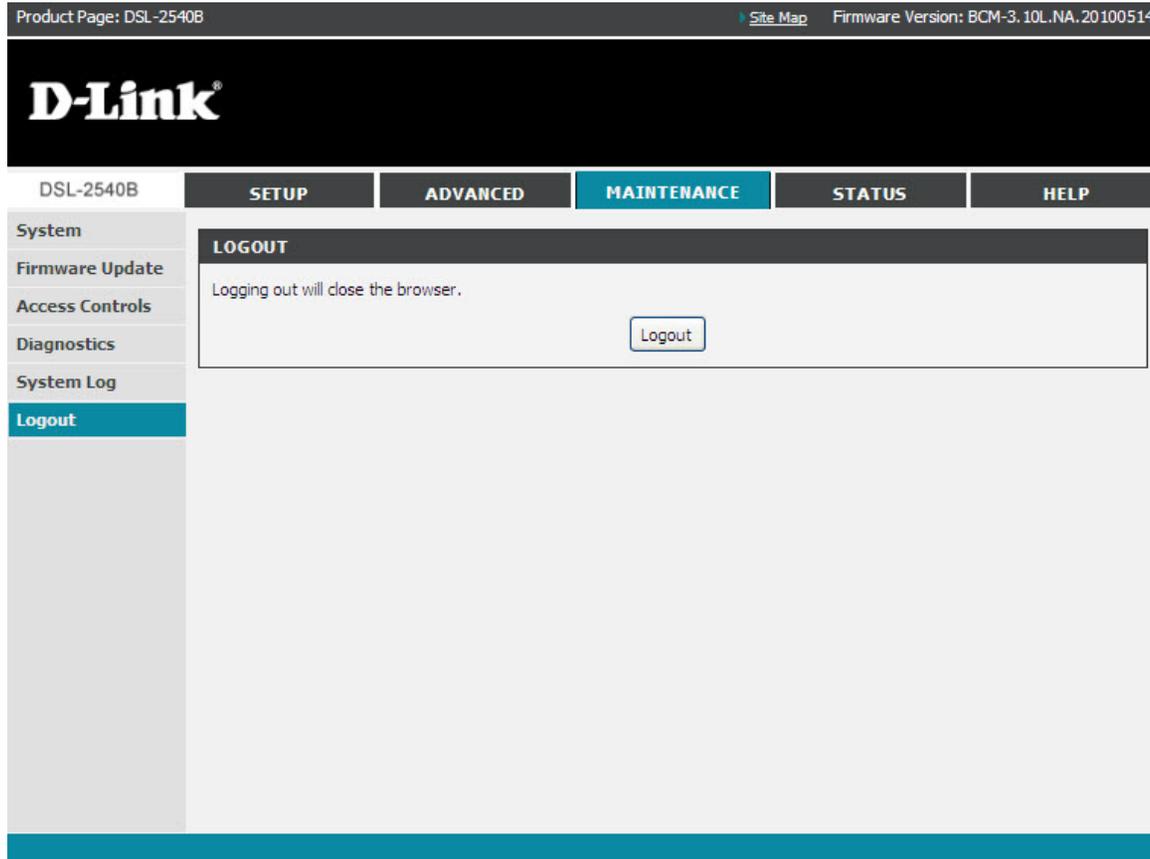
The System Log screen allows you to view the system log and configure the system log options.

To view the system log, click on the **View System Log** button.



# Logout

Select **Logout** to exit the web user interface.



# Status

The status section allows you to view general and status information for your router's connection.

## Device Info

The Device Info page shows details of the router such as the version of the software, LAN IP address, etc. It also displays the current status of your DSL connection.

Product Page: DSL-2740B [Site Map](#) Firmware Version: NA\_1.00

**D-Link**

DSL-2740B [Setup](#) [Advanced](#) [Maintenance](#) [Status](#) [Help](#)

**Device Info**

Wireless Clients  
DHCP Clients  
Logs  
Statistics  
Route Info  
Logout

**Device Information**

This information reflects the current status of your DSL connection.

**System Info**

<b>Model Name:</b>	DSL-2740B
<b>Time and Date:</b>	Saturday, January 1, 2011 01:35:52 AM
<b>Firmware Version:</b>	NA_1.00
<b>Release Date:</b>	2010/12/22

**Internet Info**

**Connection Status:** **CONNECTED**

**Default Gateway:** ppp0\_2

**Preferred DNS Server:** 192.168.1.1

**Alternate DNS Server:** N/A

Interface	Description	Link Type	IGMP	QoS	Status	IP Address
ppp0_2	pppoe_atm0_1	PPPoE	Disabled	Disabled	Connected	99.55.111.94

**Wireless Info**

**MAC Address :** F0:7D:68:D9:0F:A2

**Status:** Enabled

**Network Name (SSID):** spbu.ntu (NEW FW)

**Visibility:** Visible

**Security Mode:** WPA2-Personal(AES)

**Local Network Info**

**MAC Address :** f0:7d:68:d9:0f:a1

**IP Address:** 192.168.1.1

**Subnet Mask:** 255.255.255.0

**DHCP Server:** Enabled

**Helpful Hints...**

All of your Modem's Information, WLAN, WAN and LAN status and details are shown here.

Details include firmware version, Modem MAC address, Default gateway, WLAN SSID, WLAN security type, Modem IP and etc.

[More...](#)

# Wireless Clients

The wireless client table displays a list of currently connected wireless clients. The table also displays the connection time and MAC address of the connected wireless clients.

## Wireless Station Info

This page shows authenticated wireless stations and their status, and will be refreshed every 30 seconds.

## Wireless -- Authenticated Stations

MAC	Associated	Authorized	SSID	Interface
00:1f:3c:9a:1a:18	Yes	Yes	spbu.ntu (NEW FW)	ath0
00:11:22:33:44:55	Yes	Yes	spbu.ntu (NEW FW)	ath0

# DHCP Clients

Access the DHCP Leases screen by clicking **DHCP** under **Status**. This shows the computers identified by the Hostname and the MAC address that have acquired IP addresses by the DHCP server. The table will also show the time the DHCP lease will expire.

DHCP Clients			
This information reflects the current DHCP client of your modem.			
DHCP Leases			
Hostname	MAC Address	IP Address	Expires In
	00:18:e7:e6:a3:f4	192.168.1.6	22 hours, 23 minutes, 49 seconds
	00:1f:3c:9a:1a:18	192.168.1.3	22 hours, 27 minutes, 42 seconds
	00:11:22:33:44:55	192.168.1.4	23 hours, 46 minutes, 33 seconds
	00:1f:29:98:50:e9	192.168.1.5	22 hours, 24 minutes, 43 seconds

# Logs

The System Log screen shows the date/time of the log, the facility that was logged, the severity level and the log message. Click on **Refresh** to view any new information that has been logged.

If the log is enabled, the system will log selected events including Emergency, Alert, Critical, Error, Warning, Notice, Informational, and Debugging. All events above or equal to the selected log level will be logged and displayed.

Product Page: DSL-2740B Site Map Firmware Version: NA\_1.00

**D-Link**

DSL-2740B Setup Advanced Maintenance Status Help

Device Info  
Wireless Clients  
DHCP Clients  
**Logs**  
Statistics  
Route Info  
Logout

**Logs**  
This page allows you to view system logs.

**System Log**

Date/Time	Facility	Severity	Message
Mar 21 14:48:38	user	crit	kernel: Line 0: ADSL G.992 channel analysis
Mar 21 14:48:38	user	crit	kernel: Line 0: ADSL G.992 message exchange
Mar 21 14:48:38	user	crit	kernel: Line 0: ADSL link up, fast, us=512, ds=3008
Mar 21 14:48:38	user	err	kernel: : MAC address: f0 7d 68 d9 0f 9d
Mar 21 14:48:38	user	alert	kernel: IntrusionXXX -> IN=ppp0_2_OUT= MAC=
Mar 21 14:48:38	user	alert	kernel: IntrusionXXX -> IN=ppp0_2_OUT= MAC=
Mar 21 14:48:38	user	alert	kernel: IntrusionXXX -> IN=ppp0_2_OUT= MAC=
Mar 21 14:48:38	user	alert	kernel: IntrusionXXX -> IN=ppp0_2_OUT= MAC=
Mar 21 14:48:38	user	alert	kernel: IntrusionXXX -> IN=ppp0_2_OUT= MAC=
Mar 21 14:48:38	user	alert	kernel: IntrusionXXX -> IN=ppp0_2_OUT= MAC=
Mar 21 14:48:38	user	alert	kernel: IntrusionXXX -> IN=ppp0_2_OUT= MAC=
Mar 21 14:48:38	user	alert	kernel: IntrusionXXX -> IN=ppp0_2_OUT= MAC=
Mar 21 14:48:38	user	alert	kernel: IntrusionXXX -> IN=ppp0_2_OUT= MAC=

Helpful Hints...  
Check the log frequently to detect unauthorized network usage.  
[More...](#)

# Statistics

This page will display a summary of the number of packets that have passed between the WAN and the LAN since the LAN and the WAN were initialized.

**Statistics**

This information reflects the current status of your DSL connection.

---

**LAN**

Interface	Received				Transmitted			
	Bytes	Pkts	Errs	Drops	Bytes	Pkts	Errs	Drops
eth0	1200	2	0	0	115007	644	0	0
eth1	425511	3299	0	0	4582963	4745	0	0
eth2	0	0	0	0	0	0	0	0
eth3	476173	2461	0	0	401943	2589	0	0
ath0	13572138	124132	0	0	284313441	211102	0	1

---

**WAN**

Interface	Service Name	Received				Transmitted			
		Bytes	Pkts	Errs	Drops	Bytes	Pkts	Errs	Drops
ppp0_2	0/35 EoA	pppoe_atm0_1	276172886	206279	0	0	11805073	121482	

<
>

---

**ADSL Statistics**

Mode:	ADSL_G_dmt			
Traffic Type:	ATM			
Status:	Up			
Link Power State:	L0			
	Downstream	Upstream		
Line Coding(Trellis):	On	On		
SNR Margin (0.1 dB):	176	200		
Attenuation (0.1 dB):	215	125		
Output Power (0.1 dBm):	102	119		
Attainable Rate (Kbps):	10656	1264		
	Path 0	Path 1		
	Downstream	Upstream	Downstream	Upstream
Rate (Kbps):	6016	768	0	0
K (number of bytes in DMT frame):	189	25	0	0
R (number of check bytes in RS code word):	0	0	0	0
S (RS code word size in DMT frame):	0.50	1.00	0.0	0.0
D (interleaver depth):	1	1	0	0
Delay (msec):	0.13	0.25	0.0	0.0
INP (DMT symbol):	0.00	0.00	0.0	0.0
Super Frames:	0	0	0	0
Super Frame Errors:	0	0	0	0
RS Words:	0	0	0	0
RS Correctable Errors:	0	0	0	0
RS Uncorrectable Errors:	0	0	0	0
HEC Errors:	7	0	0	0
OCD Errors:	1	0	0	0
LCD Errors:	1	0	0	0
Total Cells:	86127453	0	0	0
Data Cells:	5959846	0	0	0
BK Errors:	0	0	0	0
Total ES:	0	0		
Total SES:	0	0		
Total UAS:	12	12		

ADSL BER Test
Reset Statistics

# Route Info

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

Routing						
Flags: U - up, ! - reject, G - gateway, H - host, R - reinstate D - dynamic (redirect), M - modified (redirect).						
Device Info -- Route						
Destination	Gateway	Subnet Mask	Flag	Metric	Service	Interface
151.164.186.13	0.0.0.0	255.255.255.255	UH	0	pppoe_atm0_1	ppp0_2
192.168.1.0	0.0.0.0	255.255.255.0	U	0		br0
239.0.0.0	0.0.0.0	255.0.0.0	U	0		br0
0.0.0.0	0.0.0.0	0.0.0.0	U	0	pppoe_atm0_1	ppp0_2

---

# Troubleshooting

This chapter provides solutions to problems that can occur during the installation and operation of the DSL-2740B. Read the following descriptions if you are having problems. (The examples below are illustrated in Windows® XP. If you have a different operating system, the screenshots on your computer will look similar to the following examples.)

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

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

- Make sure you have an updated Java-enabled web browser. We recommend the following:
  - Internet Explorer 6.0 or higher
  - Firefox 3.0 or higher
- Verify physical connectivity by checking for solid link lights on the device. If you do not get a solid link light, try using a different cable or connect to a different port on the device if possible. If the computer is turned off, the link light may not be on.
- Disable any Internet security software running on the computer. Software firewalls such as Zone Alarm, Black Ice, Sygate, Norton Personal Firewall, and Windows® XP firewall may block access to the configuration pages. Check the help files included with your firewall software for more information on disabling or configuring it.

---

• Configure your Internet settings:

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

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

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

To reset the router, locate the reset button (hole) on the rear panel of the unit. With the router powered on, use a paperclip to hold the button down for 10 seconds. Release the button and the router will go through its reboot process. Wait about 30 seconds to access the router. For information about logging into the router see page 12.

# Networking Basics

## Check your IP address

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

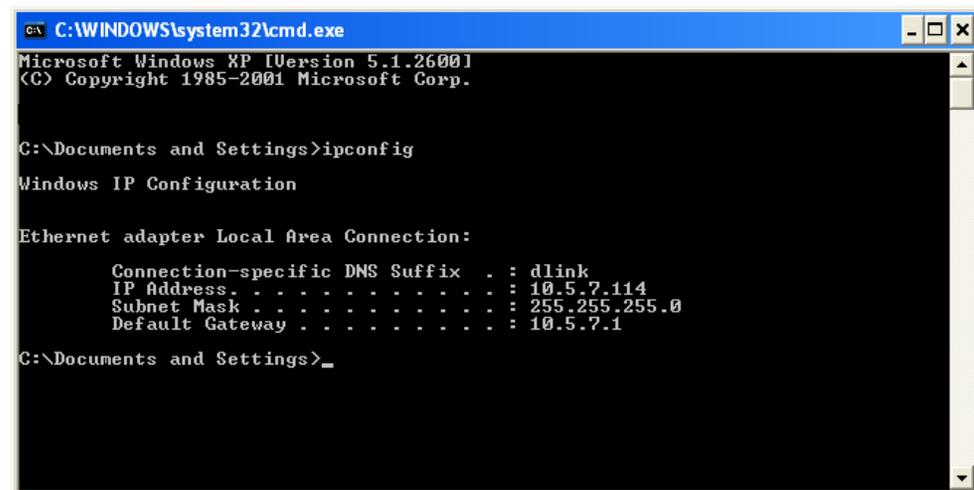
Click on **Start > Run**. In the run box type *cmd* and click **OK**.

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

This will display the IP address, subnet mask, and the default gateway of your adapter.

If the address is 0.0.0.0, check your adapter installation, security settings, and the settings on your router. Some firewall software programs may block a DHCP request on newly installed adapters.

If you are connecting to a wireless network at a hotspot (e.g. hotel, coffee shop, airport), please contact an employee or administrator to verify their wireless network settings.



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

C:\Documents and Settings>ipconfig

Windows IP Configuration

Ethernet adapter Local Area Connection:

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

C:\Documents and Settings>_
```

## Statically Assign an IP address

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

### Step 1

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

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

### Step 2

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

### Step 3

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

### Step 4

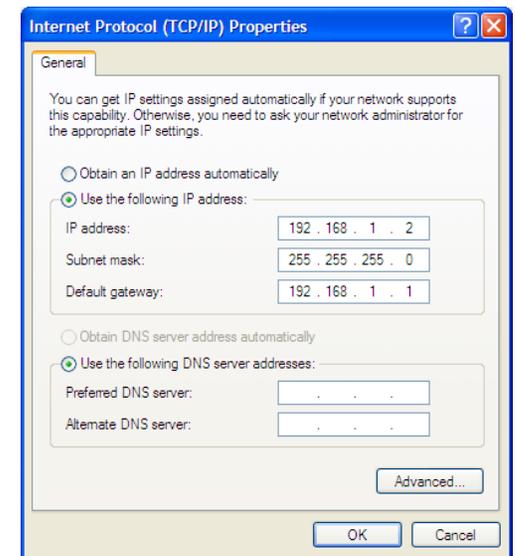
Click **Use the following IP address** and enter an IP address that is on the same subnet as your network or the LAN IP address on your router.

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

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

### Step 5

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



# Contacting Technical Support

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

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

- Model number of the product (e.g. DSL-2740B)
- Hardware Revision (located on the label on the bottom of the router (e.g. rev F1))
- Serial Number (s/n number located on the label on the bottom of the router).

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

## For customers within the United States:

**Phone Support:**

(877) 453-5465

**Internet Support:**

<http://support.dlink.com>

## For customers within Canada:

**Phone Support:**

(800) 361-5265

**Internet Support:**

<http://support.dlink.ca>

# Warranty

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

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

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

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

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

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

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

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

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

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

D-Link may reject or return any product that is not packaged and shipped in strict compliance with the foregoing requirements, or for which an RMA number is not visible from the outside of the package. The product owner agrees to pay D-Link's reasonable handling and return shipping charges for any product that is not packaged and shipped in accordance with the foregoing requirements, or that is determined by D-Link not to be defective or non-conforming.

**What Is Not Covered:** The Limited Warranty provided herein by D-Link does not cover: Products that, in D-Link's judgment, have been subjected to abuse, accident, alteration, modification, tampering, negligence, misuse, faulty installation, lack of reasonable care, repair or service in any way that is not contemplated in the documentation for the product, or if the model or serial number has been altered, tampered with, defaced or removed; Initial installation, installation and removal of the product for repair, and shipping costs; Operational adjustments covered in the operating manual for the product, and normal maintenance; Damage that occurs in shipment, due to act of God, failures due to power surge, and cosmetic damage; Any hardware, software, firmware or other products or services provided by anyone other than D-Link; and Products that have been purchased from inventory clearance or liquidation sales or other sales in which D-Link, the sellers, or the liquidators expressly disclaim their warranty obligation pertaining to the product. While necessary maintenance or repairs on your Product can be performed by any company, we recommend that you use only an Authorized D-Link Service Office. Improper or incorrectly performed maintenance or repair voids this Limited Warranty.

**Disclaimer of Other Warranties:** EXCEPT FOR THE LIMITED WARRANTY SPECIFIED HEREIN, THE PRODUCT IS PROVIDED "AS-IS" WITHOUT ANY WARRANTY OF ANY KIND WHATSOEVER INCLUDING, WITHOUT LIMITATION, ANY WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NON-INFRINGEMENT. IF ANY IMPLIED WARRANTY CANNOT BE DISCLAIMED IN ANY TERRITORY WHERE A PRODUCT IS SOLD, THE DURATION OF SUCH IMPLIED WARRANTY SHALL BE LIMITED TO THE DURATION OF THE APPLICABLE WARRANTY PERIOD SET FORTH ABOVE. EXCEPT AS EXPRESSLY COVERED UNDER THE LIMITED WARRANTY PROVIDED HEREIN, THE ENTIRE RISK AS TO THE QUALITY, SELECTION AND PERFORMANCE OF THE PRODUCT IS WITH THE PURCHASER OF THE PRODUCT.

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

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

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

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

Copyright 2010 by D-Link Corporation/D-Link Systems, Inc. All rights reserved.

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

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

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

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

# Registration

Register your product online at [support.dlink.com/register](http://support.dlink.com/register)



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

Version 1.0  
May 25, 2011