

Resetting the DI-824VUP to the Factory Default Settings

After you have tried other methods for troubleshooting your network, you may choose to **Reset** the DI-824VUP to the factory default settings.



To hard-reset the D-Link DI-824VUP to the Factory Default Settings, please do the following:

- Locate the **Reset** button on the back of the DI-824VUP.
- Use a paper clip to press the **Reset** button and power on.
- Hold for about 5 seconds (do not hold for too long) and then release. (Or, release when the status LEDflashes.)
- After you have completed the above steps, the DI-824VUP will be reset to the factory default settings.

Technical Specifications

Standards

- IEEE 802.11b
- IEEE 802.3
- IEEE 802.3u 100BASE-TX Fast Ethernet
- IEEE 802.11g
- USB 1.1

VPN Pass Through Function

- PPTP
- L2TP
- IPSec

LEDs

- Power
- WAN
- LAN
- WLAN
- Status
- COM
- USB
- LPT

Operating Temperature

- 32°F to 131°F (0°C to 55°C)

Humidity

- 10-90%

Power

- 5V DC / 2.5A

Dimensions

- L = 9.25 inches (233mm)
- W = 6.5 inches (165mm)
- H = 1.375 inches (35mm)

Weight

- ~2.0oz. (907g)

Ports

- 4 x 10/100 LAN Ports (MDI/MDIX)
- 1 x 10/100 WAN Port (MDI/MDIX)
- 1 COM Port (Dial-up Modem)
- 1 Parallel Port (DB25)
- 1 USB Port

Frequently Asked Questions

Why can't I access the Web-based configuration?

When entering the IP Address of the DI-824VUP (192.168.0.1), you are not connecting to 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.

To resolve difficulties accessing a Web utility, please follow the steps below.

Step 1 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.

What type of cable should I be using?

The following connections require a Crossover Cable:

- Computer to Computer
- Computer to Uplink Port
- Computer to Access Point
- Computer to Print Server
- Computer/XBOX/PS2 to DWL-810
- Computer/XBOX/PS2 to DWL-900AP+
- Uplink Port to Uplink Port (hub/switch)
- Normal Port to Normal Port (hub/switch)

The following connections require a Straight-through Cable:

- Computer to Residential Gateway/Router
- Computer to Normal Port (hub/switch)
- Access Point to Normal Port (hub/switch)
- Print Server to Normal Port (hub/switch)
- Uplink Port to Normal Port (hub/switch)

Rule of Thumb:

"If there is a link light, the cable is right."

Frequently Asked Questions (continued)

Why can't I access the Web-based configuration? (continued)

What type of cable should I be using? (continued)

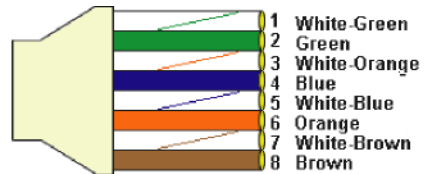
What's the difference between a crossover cable and a straight-through cable?

The wiring in crossover and straight-through cables are different. The two types of cable have different purposes for different LAN configurations. EIA/TIA 568A/568B define the wiring standards and allow for two different wiring color codes as illustrated in the following diagram.

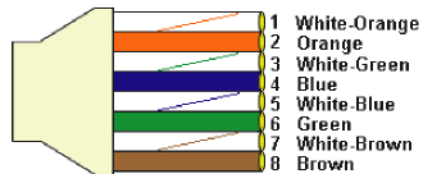
**The wires with colored backgrounds may have white stripes and may be denoted that way in diagrams found elsewhere.*

How to tell straight-through cable from a crossover cable:

The main way to tell the difference between the two cable types is to compare the wiring order on the ends of the cable. If the wiring is the same on both sides, it is straight-through cable. If one side has opposite wiring, it is a crossover cable.



568A CABLE END



568B CABLE END

All you need to remember to properly configure the cables is the pinout order of the two cable ends and the following rules:

A straight-through cable has identical ends

A crossover cable has different ends

It makes no functional difference which standard you follow for straight-through cable ends, as long as both ends are the same. You can start a crossover cable with either standard as long as the other end is the other standard. It makes no functional difference which end is which. The order in which you pin the cable is important. Using a pattern other than what is specified in the above diagram could cause connection problems.

When to use a crossover cable and when to use a straight-through cable:

Computer to Computer – Crossover

Computer to an normal port on a Hub/Switch – Straight-through

Computer to an uplink port on a Hub/Switch – Crossover

Hub/Switch uplink port to another Hub/Switch uplink port – Crossover

Hub/Switch uplink port to another Hub/Switch normal port – Straight-through

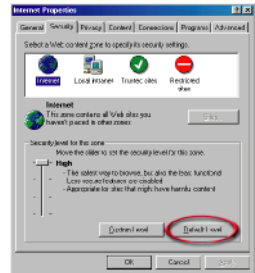
Frequently Asked Questions (continued)

Why can't I access the Web-based configuration? (continued)

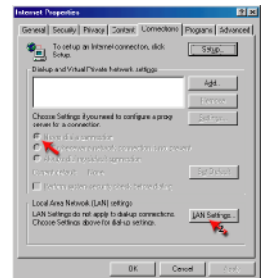
Step 2 Disable any Internet security software running on the computer. Software firewalls like Zone Alarm, Black Ice, Sygate, Norton Personal Firewall, etc. might block access to the configuration pages. Check the help files included with your firewall software for more information on disabling or configuring it.

Step 3 Configure your Internet settings.

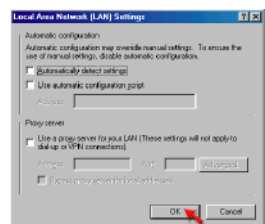
Go to **Start > Settings > Control Panel**. Double click the **Internet Options** icon. From the **Security** tab, click the **Default Level** button to restore the settings to their defaults.



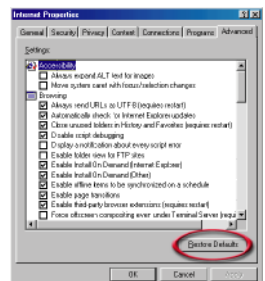
Click to the **Connection** tab and set the dial-up option to **Never Dial a Connection**. Click the **LAN Settings** button.



Nothing should be checked. Click **OK**.



Go to the **Advanced** tab and click the **Restore Defaults** button to restore these settings to their factory defaults.



Click **OK**. Go to the desktop and close any open windows.

Frequently Asked Questions (continued)

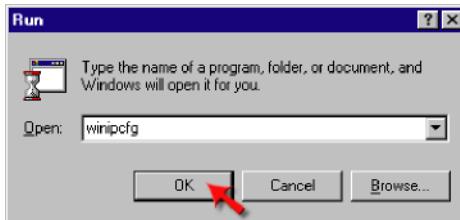
Why can't I access the Web-based configuration? (continued)

Step 4 Check your IP address. Your computer must have an IP address in the same range of the device you are attempting to configure. Most D-Link devices use the 192.168.0.X range.

How can I find my IP Address in Windows 95, 98, or ME?

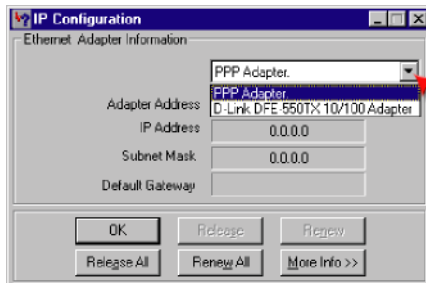
Step 1 Click on **Start**, then click on **Run**.

Step 2 The Run Dialogue Box will appear. Type **wiipcfg** in the text field and click **OK**.



Step 3 The **IP Configuration** window will appear, displaying your **Ethernet Adapter Information**.

- Select your adapter from the drop down menu.
- If you do not see your adapter in the drop down menu, your adapter is not properly installed.



Step 4 After selecting your adapter, it will display your IP Address, subnet mask, and default gateway.

Step 5 Click **OK** to close the IP Configuration window

Frequently Asked Questions (continued)

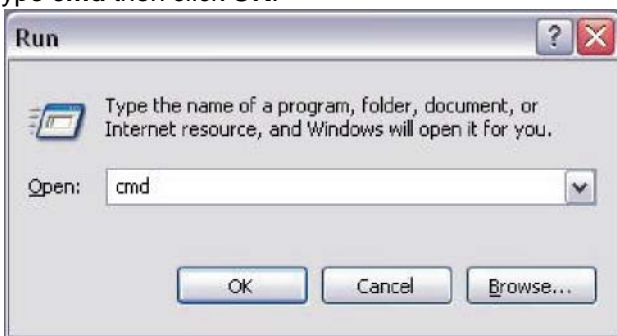
Why can't I access the Web-based configuration? (continued)

Step 4 (continued) Check your IP address. Your computer must have an IP Address in the same range of the device you are attempting to configure. Most D-Link devices use the 192.168.0.X range.

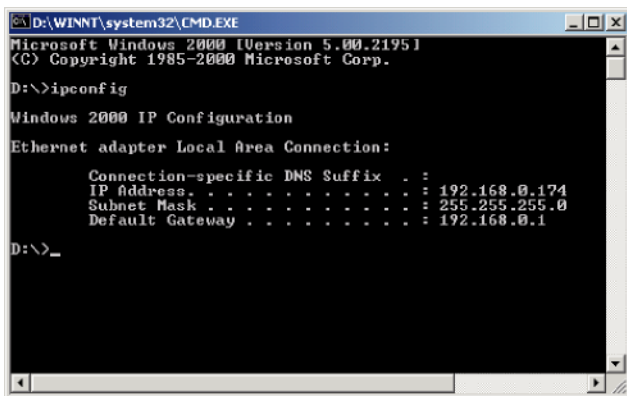
How can I find my IP Address in Windows 2000/XP?

Step 1 Click on **Start** and select **Run**.

Step 2 Type **cmd** then click **OK**.



Step 3 From the Command Prompt, enter **ipconfig**. It will return your IP Address, subnet mask, and default gateway



Step 4 Type **exit** to close the command prompt.

Frequently Asked Questions (continued)

Why can't I access the Web-based configuration? (continued)

Step 4 (continued) Check your IP address. Your computer must have an IP address in the same range of the device you are attempting to configure. Most D-Link devices use the 192.168.0.X range.

Make sure you take note of your computer's Default Gateway IP Address. The Default Gateway is the IP Address of the D-Link Router. By default, it should be 192.168.0.1.

How can I assign a Static IP Address in Windows XP?

Step 1

Click on **Start > Control Panel > Network and Internet Connections > Network connections.**

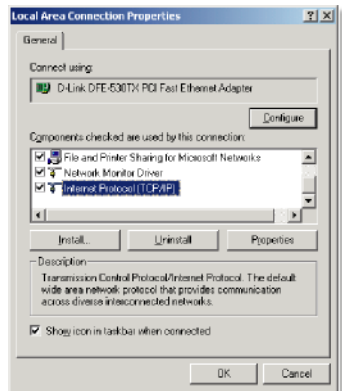
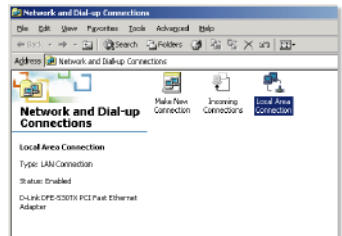
Step 2 See [Step 2](#) for Windows 2000 and continue from there.

How can I assign a Static IP Address in Windows 2000?

Step 1 Right-click on **My Network Places** and select **Properties.**

Step 2 Right-click on the **Local Area Connection** which represents your network card and select **Properties.**

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



Frequently Asked Questions (continued)

Why can't I access the Web-based configuration? (continued)

How can I assign a Static IP Address in Windows 2000? (continued)

Click **Use the following IP Address** and enter an IP Address that is on the same subnet as the LAN IP address on your router. Example: If the router's LAN IP address is 192.168.0.1, make your IP address 192.168.0.X where X = 2-99. Make sure that the number you choose is not in use on the network.

Set the **Default Gateway** to be the same as the LAN IP address of your router (192.168.0.1).

Set the **Preferred DNS server** to be the same as the LAN IP address of your router (192.168.0.1).

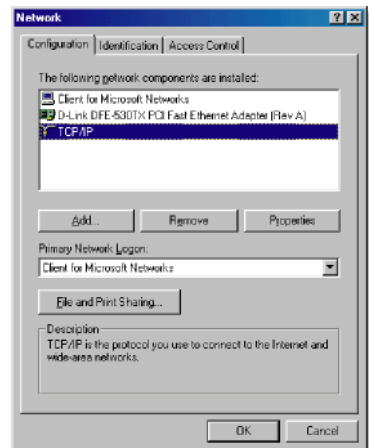
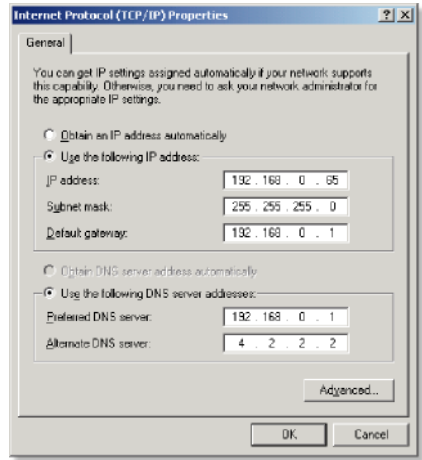
The **Alternate DNS server** is not needed or enter a DNS server from your ISP.

Click **OK** twice. You may be asked if you want to reboot your computer. Click **Yes**.

How can I assign a Static IP Address in Windows 98/Me?

Step 1 From the desktop, right-click on the **Network Neighborhood** icon (Win ME - My Network Places) and select **Properties**

Highlight **TCP/IP** and click the **Properties** button. If you have more than one adapter, then there will be a TCP/IP "Binding" for each adapter. Highlight **TCP/IP > (your network adapter)** and then click **Properties**.



Frequently Asked Questions (continued)

Why can't I access the Web-based configuration? (continued)

How can I assign a Static IP Address in Windows 98/Me? (continued)

Step 2 Click **Specify an IP Address**.

Enter in an IP Address that is on the same subnet as the LAN IP Address on your router.

Example: If the router's LAN IP Address is 192.168.0.1, make your IP Address 192.168.0.X where X is between 2-99. Make sure that the number you choose is not in use on the network.

Step 3 Click on the **Gateway** tab.

Enter the LAN IP Address of your router here (192.168.0.1).

Click **Add** when finished.

Step 4 Click on the **DNS Configuration** tab.

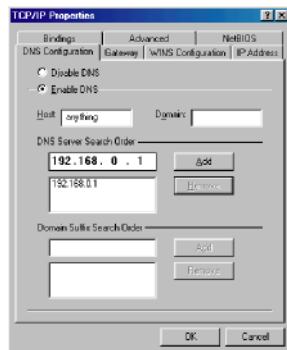
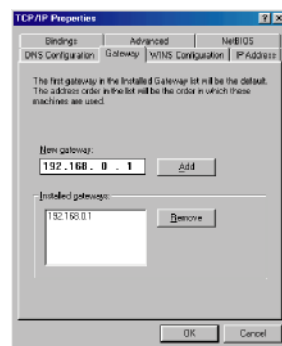
Click **Enable DNS**. Type in a **Host** (can be any word). Under DNS server search order, enter the LAN IP Address of your router (192.168.0.1). Click **Add**.

Step 5 Click **OK** twice.

When prompted to reboot your computer, click **Yes**.

After you reboot, the computer will now have a static, private IP Address.

Step 5 Access the Web management. Open your Web browser and enter the IP Address of your D-Link device in the address bar. This should open the log-in page for the web management. Follow instructions to log in and complete the configuration.



Frequently Asked Questions (continued)

How can I setup my DI-824VUP to work with a cable modem connection?

Dynamic Cable connection

(i.e. Cox, Adelphia, Rogers, Roadrunner, Charter, and Comcast).

Note: Please configure the router with the computer that was last connected directly to the cable modem.

Step 1 Log into the Web based configuration by typing in the IP Address of the router (default:192.168.0.1) in your web browser. The username is **admin** (all lowercase) and the password is **blank** (nothing).

Step 2 Click the **Home** tab and click the **WAN** button. Dynamic IP address is the default value, however, if Dynamic IP address is not selected as the WAN type, select Dynamic IP address by clicking on the radio button. Click **Clone Mac address**. Click on **Apply** and then **Continue** to save the changes.



D-Link
Building Networks for People

AirPlus™ G+
High-Speed 2.4GHz Wireless VPN Router

DI-824VUP+

Wizard
Wireless
WAN
LAN
DHCP
VPN

Home Advanced Tools Status Help

WAN Settings
Please select the appropriate option to connect to your ISP.

- Dynamic IP Address Choose this option to obtain an IP address automatically from your ISP. (For most Cable modem users)
- Static IP Address Choose this option to set static IP information provided to you by your ISP.
- PPPoE Choose this option if your ISP uses PPPoE. (For most DSL users)
- Dial-up Network To surf the Internet via PSTN/ISDN.
- Others PPTP, L2TP and BigPond Cable.

Dynamic IP Address

Host Name (Optional)

MAC Address FF FF FF FF FF FF

Primary DNS Address

Secondary DNS Address

MTU 1500

Auto-reconnect Enabled Disabled

Auto-backup Enabled Disabled

Frequently Asked Questions (continued)

How can I setup my DI-824VUP to work with a cable modem connection? (continued)

Step 3 Power cycle the cable modem and router:

First turn the cable modem off. Then turn the router off. Leave them off for 2 minutes.** Next turn the cable modem on. Wait until you get a solid cable light on the cable modem, and then turn the router on. Wait 30 seconds.

** If you have a DCM-201 modem, leave off for at least 5 minutes.

Step 4 Follow step 1 again and log back into the web configuration. Click the **Status** tab and click the **Device Info** button. If you do not already have a public IP Address under the **WAN** heading, click on the **DHCP Renew** and **Continue** buttons.

Static Cable Connection

Step 1 Log into the Web-based configuration by typing in the IP address of the router (default:192.168.0.1) in your Web browser. The username is **admin** (all lowercase) and the password is blank (empty).

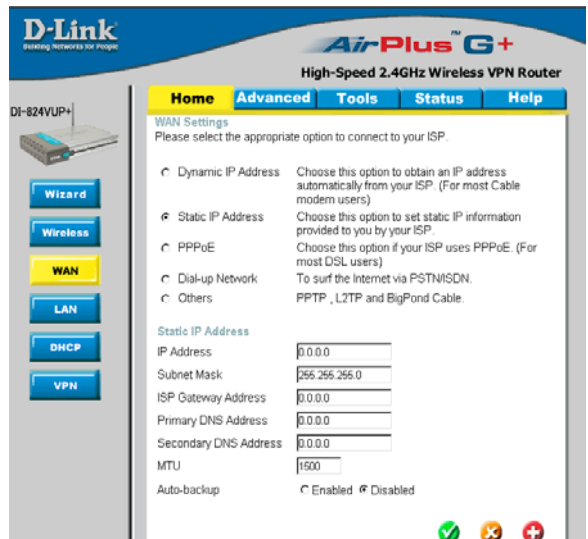


Step 2 Click the **Home** tab and click the **WAN** button. Select **Static IP Address** and enter your static settings obtained from the ISP in the fields provided.

If you do not know your settings, you must contact your ISP.

Step 3 Click on **Apply** and then click **Continue** to save the changes.

Step 4 Click the **Status** tab and click the **Device Info** button. Your IP Address information will be displayed under the **WAN** heading.



Frequently Asked Questions (continued)

How can I setup my DI-824VUP to work with Earthlink DSL or any PPPoE connection?

Make sure you disable or uninstall any PPPoE software such as WinPoet or Internet 300 from your computer or you will not be able to connect to the Internet.

Step 1 Upgrade Firmware if needed.

(Please visit the D-Link tech support website at: <http://support.dlink.com> for the latest firmware upgrade information.)

Step 2 Take a paperclip and perform a hard reset. With the unit on, use a paperclip and hold down the reset button on the back of the unit for 10 seconds. Release it and the router will recycle, the lights will blink, and then stabilize.

Step 3 After the Router stabilizes, open your browser and enter 192.168.0.1 into the address window and hit the **Enter** key. When the password dialog box appears, enter the username **admin** and leave the password blank. Click **OK**.

If the password dialog box does not come up repeat **Step 2**.

Note: Do not run Wizard.

Step 4 Click on the **WAN** tab on left-hand side of the screen. Select **PPPoE**.

Step 5 Select **Dynamic PPPoE** (unless your ISP supplied you with a static IP Address).

Step 6 In the username field enter **ELN/username@earthlink.net** and your password, where username is your own username.

For SBC Global users, enter **username@sbcglobal.net**.

For Ameritech users, enter **username@ameritech.net**.

For BellSouth users, enter **username@bellsouth.net**.

For Mindspring users, enter **username@mindspring.com**.

For most other ISPs, enter **username**.

Step 7 **Maximum Idle Time** should be set to zero. Set **MTU** to 1492, unless specified by your ISP, and set **Autoreconnect** to **Enabled**.

Note: If you experience problems accessing certain websites and/or email issues, please set the MTU to a lower number such as 1472, 1452, etc. Contact your ISP for more information and the proper MTU setting for your connection.

Frequently Asked Questions (continued)

How can I setup my DI-824VUP to work with Earthlink DSL or any PPPoE connection? (continued)

Step 8 Click **Apply**. When prompted, click **Continue**. Once the screen refreshes, unplug the power to the D-Link Router.

Step 9 Turn off your DSL modem for 2-3 minutes. Turn back on. Once the modem has established a link to your ISP, plug the power back into the D-Link Router. Wait about 30 seconds and log back into the router.

Step 10 Click on the **Status** tab in the web configuration where you can view the device info. Under **WAN**, click **Connect**. Click **Continue** when prompted. You should now see that the device info will show an IP Address, verifying that the device has connected to a server and has been assigned an IP Address.

Can I use my DI-824VUP to share my Internet connection provided by AOL DSL Plus?

In most cases yes. AOL DSL Plus may use PPPoE for authentication bypassing the client software. If this is the case, then our routers will work with this service. Please contact AOL if you are not sure.

To set up your router:

Step 1 Log into the Web-based configuration (192.168.0.1) and configure the WAN side to use PPPoE.

Step 2 Enter your screen name followed by @aol.com for the user name. Enter your AOL password in the password box.

Step 3 You will have to set the MTU to 1400. AOL DSL does not allow for anything higher than 1400.

Step 4 Apply settings.

Step 5 Recycle the power to the modem for 1 minute and then recycle power to the router. Allow 1 to 2 minutes to connect.

If you connect to the Internet with a different Internet Service Provider and want to use the AOL software, you can do that without configuring the router's firewall settings. You need to configure the AOL software to connect using TCP/IP.

Go to <http://www.aol.com> for more specific configuration information of their software.

Frequently Asked Questions (continued)

I have two DI-824VUP Routers, how can I set them up to work with each other?

Step 1 Log into the web based configuration of the router by typing in the IP address of the router (default: 192.168.0.1) in your web browser. By default the username is **admin** and there is no password.



Connect to 192.168.0.1

DI-824VUP +

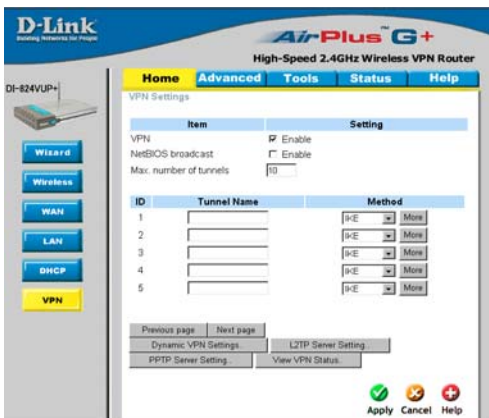
User name: admin

Password:

Remember my password

OK Cancel

Step 2 Click the **VPN** button on the left column, select the checkbox to Enable the VPN, and then in the box next to Max. number of tunnels, enter the maximum numbers of VPN tunnels that you would like to have connected.



D-Link Air-Plus G+ High-Speed 2.4GHz Wireless VPN Router

DI-824VUP+

Home Advanced Tools Status Help

VPN Settings

Item	Setting
VPN	<input checked="" type="checkbox"/> Enable
NetBIOS broadcast	<input type="checkbox"/> Enable
Max. number of tunnels	10

ID	Tunnel Name	Method
1		IKE More
2		IKE More
3		IKE More
4		IKE More
5		IKE More

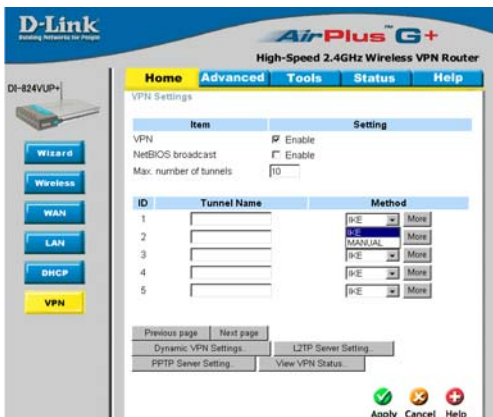
Previous page Next page

Dynamic VPN Settings L2TP Server Setting

PPTP Server Setting View VPN Status

Apply Cancel Help

Step 3 In the space provided, enter the Tunnel Name for ID number 1, select IKE, and then click More.



D-Link Air-Plus G+ High-Speed 2.4GHz Wireless VPN Router

DI-824VUP+

Home Advanced Tools Status Help

VPN Settings

Item	Setting
VPN	<input checked="" type="checkbox"/> Enable
NetBIOS broadcast	<input type="checkbox"/> Enable
Max. number of tunnels	10

ID	Tunnel Name	Method
1		IKE More
2		IKE More
3		IKE More
4		IKE More
5		IKE More

Previous page Next page

Dynamic VPN Settings L2TP Server Setting

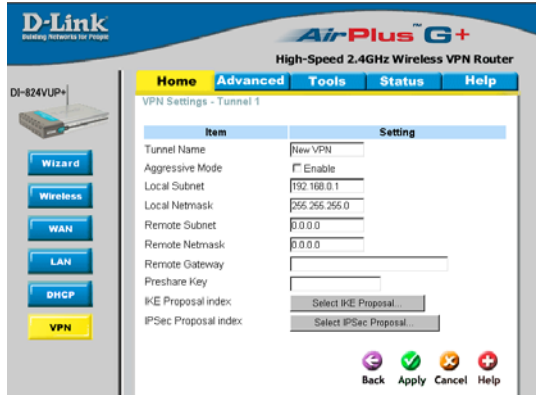
PPTP Server Setting View VPN Status

Apply Cancel Help

Frequently Asked Questions (continued)

I have two DI-824VUP Routers, how can I set them up to work with each other?(continued)

Step 4 In the **Local Subnet** and **Local Netmask** fields enter the network identifier for the local DI-824VUP's LAN and the corresponding subnet mask.

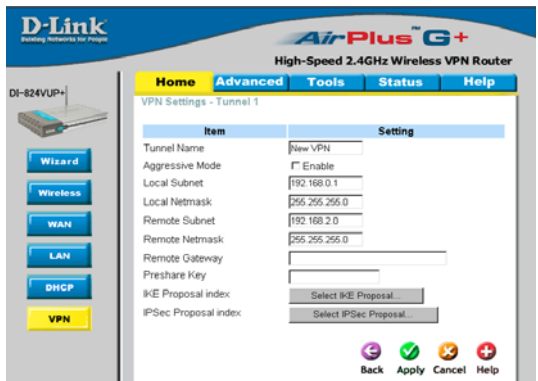


The screenshot shows the 'VPN Settings - Tunnel 1' configuration page for a D-Link AirPlus G+ High-Speed 2.4GHz Wireless VPN Router. The 'Advanced' tab is selected. The configuration table is as follows:

Item	Setting
Tunnel Name	New VPN
Aggressive Mode	<input type="checkbox"/> Enable
Local Subnet	192.168.0.1
Local Netmask	255.255.255.0
Remote Subnet	0.0.0.0
Remote Netmask	0.0.0.0
Remote Gateway	
Preshare Key	
IKE Proposal index	Select IKE Proposal...
IPSec Proposal index	Select IPSec Proposal...

Navigation buttons at the bottom: Back, Apply, Cancel, Help.

Step 5 In the **Remote Subnet** and **Remote Netmask** fields enter the network identifier for the remote DI-824VUP's LAN and the corresponding subnet mask.



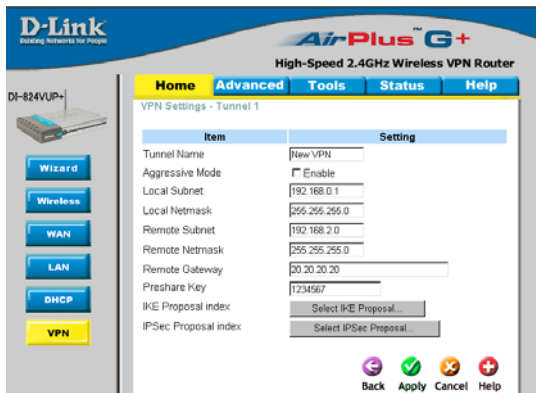
The screenshot shows the 'VPN Settings - Tunnel 1' configuration page for a D-Link AirPlus G+ High-Speed 2.4GHz Wireless VPN Router. The 'Advanced' tab is selected. The configuration table is as follows:

Item	Setting
Tunnel Name	New VPN
Aggressive Mode	<input type="checkbox"/> Enable
Local Subnet	192.168.0.1
Local Netmask	255.255.255.0
Remote Subnet	192.168.2.0
Remote Netmask	255.255.255.0
Remote Gateway	
Preshare Key	
IKE Proposal index	Select IKE Proposal...
IPSec Proposal index	Select IPSec Proposal...

Navigation buttons at the bottom: Back, Apply, Cancel, Help.

Step 6 In the **Remote Gateway** field enter the WAN IP address of the remote DI-824VUP and in the **Preshare Key** field, enter a key which must be exactly the same as the Preshare Key that is configured on the remote DI-824VUP.

Step 7 Click Apply.



The screenshot shows the 'VPN Settings - Tunnel 1' configuration page for a D-Link AirPlus G+ High-Speed 2.4GHz Wireless VPN Router. The 'Advanced' tab is selected. The configuration table is as follows:

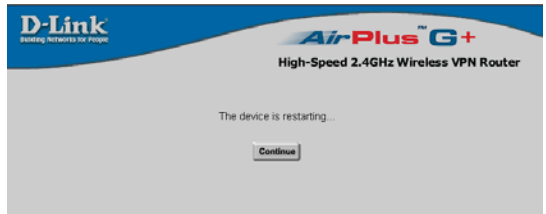
Item	Setting
Tunnel Name	New VPN
Aggressive Mode	<input type="checkbox"/> Enable
Local Subnet	192.168.0.1
Local Netmask	255.255.255.0
Remote Subnet	192.168.2.0
Remote Netmask	255.255.255.0
Remote Gateway	20.20.20.20
Preshare Key	1234567
IKE Proposal index	Select IKE Proposal...
IPSec Proposal index	Select IPSec Proposal...

Navigation buttons at the bottom: Back, Apply, Cancel, Help.

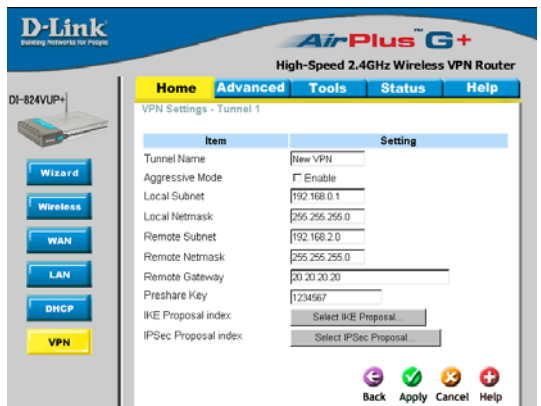
Frequently Asked Questions (continued)

I have two DI-824VUP Routers, how can I set them up to work with each other? (continued)

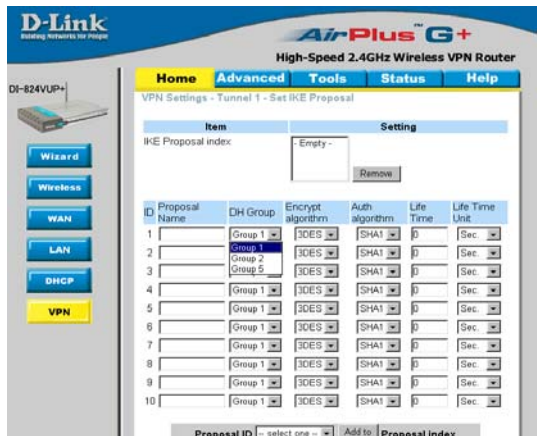
Step 8 The device will restart. Click on the Continue button.



Step 9 Click on Select IKE Proposal.



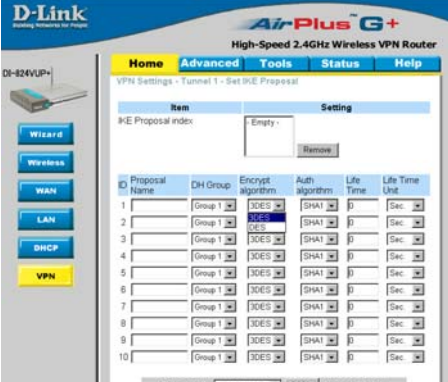
Step 10 Enter a name for proposal ID number 1 and select Group 1, 2, or 5 from the DH Group dropdown menu.



Frequently Asked Questions (continued)

I have two DI-824VUP Routers, how can I set them up to work with each other? (continued)

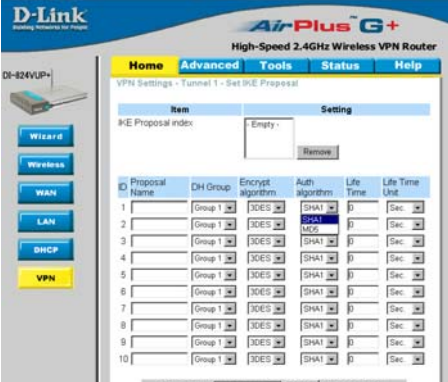
Step 11 Select DES or 3DES as the Encryption Algorithm.



The screenshot shows the 'VPN Settings - Tunnel 1 - Set IKE Proposal' page. The 'Encrypt algorithm' dropdown for proposal 1 is set to 'DES'. The 'Auth algorithm' dropdown is set to 'SHA1'. The 'Life Time' is set to '0' and the 'Life Unit' is set to 'Sec.'.

ID	Proposal Name	DH Group	Encrypt algorithm	Auth algorithm	Life Time	Life Time Unit
1		Group 1	DES	SHA1	0	Sec.
2		Group 1	DES	SHA1	0	Sec.
3		Group 1	DES	SHA1	0	Sec.
4		Group 1	DES	SHA1	0	Sec.
5		Group 1	DES	SHA1	0	Sec.
6		Group 1	DES	SHA1	0	Sec.
7		Group 1	DES	SHA1	0	Sec.
8		Group 1	DES	SHA1	0	Sec.
9		Group 1	DES	SHA1	0	Sec.
10		Group 1	DES	SHA1	0	Sec.

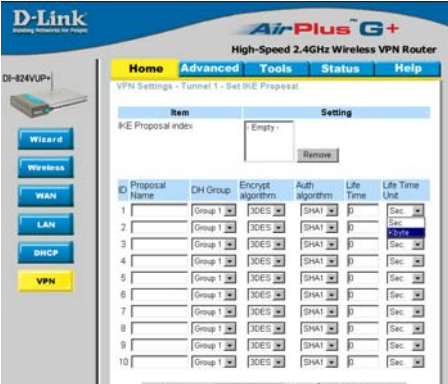
Step 12 Select SHA-1 or MD5 as the Authentication Algorithm.



The screenshot shows the 'VPN Settings - Tunnel 1 - Set IKE Proposal' page. The 'Auth algorithm' dropdown for proposal 1 is set to 'MD5'. The 'Encrypt algorithm' dropdown is set to 'DES'. The 'Life Time' is set to '0' and the 'Life Unit' is set to 'Sec.'.

ID	Proposal Name	DH Group	Encrypt algorithm	Auth algorithm	Life Time	Life Time Unit
1		Group 1	DES	MD5	0	Sec.
2		Group 1	DES	SHA1	0	Sec.
3		Group 1	DES	SHA1	0	Sec.
4		Group 1	DES	SHA1	0	Sec.
5		Group 1	DES	SHA1	0	Sec.
6		Group 1	DES	SHA1	0	Sec.
7		Group 1	DES	SHA1	0	Sec.
8		Group 1	DES	SHA1	0	Sec.
9		Group 1	DES	SHA1	0	Sec.
10		Group 1	DES	SHA1	0	Sec.

Step 13 Enter a Lifetime value of 2800 and then either select Sec. or KByte as the unit for the lifetime value.



The screenshot shows the 'VPN Settings - Tunnel 1 - Set IKE Proposal' page. The 'Life Time' dropdown for proposal 1 is set to '2800' and the 'Life Unit' dropdown is set to 'KByte'. The 'Encrypt algorithm' dropdown is set to 'DES' and the 'Auth algorithm' dropdown is set to 'SHA1'.

ID	Proposal Name	DH Group	Encrypt algorithm	Auth algorithm	Life Time	Life Time Unit
1		Group 1	DES	SHA1	2800	KByte
2		Group 1	DES	SHA1	0	Sec.
3		Group 1	DES	SHA1	0	Sec.
4		Group 1	DES	SHA1	0	Sec.
5		Group 1	DES	SHA1	0	Sec.
6		Group 1	DES	SHA1	0	Sec.
7		Group 1	DES	SHA1	0	Sec.
8		Group 1	DES	SHA1	0	Sec.
9		Group 1	DES	SHA1	0	Sec.
10		Group 1	DES	SHA1	0	Sec.

Frequently Asked Questions (continued)

I have two DI-808HV Routers, how can I set them up to work with each other? (continued)

Step 14 Select 1 out of the Proposal ID dropdown menu and click Add To, which will add the proposal that was just configured to the IKE Proposal Index. Click Apply.

The screenshot shows the 'VPN Settings - Tunnel 1 - Set IKE Proposal' page. On the left is a navigation menu with buttons for Wizard, Wireless, WAN, LAN, DHCP, and VPN. The main content area has tabs for Home, Advanced, Tools, Status, and Help. Below the tabs is a table with columns for Item and Setting. The 'Item' column contains 'IKE Proposal index' and a 'Remove' button. Below this is a table of IKE Proposals:

ID	Proposal Name	DH Group	Encrypt algorithm	Auth algorithm	Life Time	Life Time Unit
1	IKE Proposal	Group 1	3DES	SHA1	0	Kbyte
2		Group 1	3DES	SHA1	0	Sec
3		Group 1	3DES	SHA1	0	Sec
4		Group 1	3DES	SHA1	0	Sec
5		Group 1	3DES	SHA1	0	Sec
6		Group 1	3DES	SHA1	0	Sec
7		Group 1	3DES	SHA1	0	Sec
8		Group 1	3DES	SHA1	0	Sec
9		Group 1	3DES	SHA1	0	Sec
10		Group 1	3DES	SHA1	0	Sec

At the bottom, there is a 'Proposal ID' dropdown menu set to '1' and an 'Add to' button next to 'Proposal index'.

Step 15 The device will restart. Click on the Continue button. Then click Back.

The screenshot shows the 'High-Speed 2.4GHz Wireless VPN Router' interface. The main content area displays the message 'The device is restarting...' with a 'Continue' button below it.

Step 16 Click on Select IPsec Proposal.

The screenshot shows the 'VPN Settings - Tunnel 1' page. On the left is a navigation menu with buttons for Wizard, Wireless, WAN, LAN, DHCP, and VPN. The main content area has tabs for Home, Advanced, Tools, Status, and Help. Below the tabs is a table with columns for Item and Setting. The 'Item' column contains 'Tunnel Name', 'Aggressive Mode', 'Local Subnet', 'Local Netmask', 'Remote Subnet', 'Remote Netmask', 'Remote Gateway', 'Preshare Key', 'IKE Proposal index', and 'IPsec Proposal index'. The 'Setting' column contains 'New VPN', 'Enable', '192.168.0.1', '255.255.255.0', '192.168.2.0', '255.255.255.0', '20.20.20.20', '1234567', 'Select IKE Proposal...', and 'Select IPsec Proposal...'. At the bottom right, there are four buttons: Back, Apply, Cancel, and Help.

Frequently Asked Questions (continued)

I have two DI-824VUP Routers, how can I set them up to work with each other?(continued)

Step 17 Enter a name for proposal ID number 1 and select Group 1, 2, 5, or None from the DH Group dropdown menu.

VPN Settings - Tunnel 1 - Set IPSEC Proposal

ID	Proposal Name	DH Group	Encap protocol	Encrypt algorithm	Auth algorithm	Life Time	Life Time Unit
1	FSec Proposal	None	ESP	3DES	None	0	Sec
2		Group 1	ESP	3DES	None	0	Sec
3		Group 2	ESP	3DES	None	0	Sec
4		Group 5	ESP	3DES	None	0	Sec
5		None	ESP	3DES	None	0	Sec
6		None	ESP	3DES	None	0	Sec
7		None	ESP	3DES	None	0	Sec
8		None	ESP	3DES	None	0	Sec
9		None	ESP	3DES	None	0	Sec
10		None	ESP	3DES	None	0	Sec

Step 18 Select ESP or AH as the Encapsulation Protocol.

VPN Settings - Tunnel 1 - Set IPSEC Proposal

ID	Proposal Name	DH Group	Encap protocol	Encrypt algorithm	Auth algorithm	Life Time	Life Time Unit
1	FSec Proposal	None	ESP	3DES	None	0	Sec
2		None	ESP/AH	3DES	None	0	Sec
3		None	ESP	3DES	None	0	Sec
4		None	ESP	3DES	None	0	Sec
5		None	ESP	3DES	None	0	Sec
6		None	ESP	3DES	None	0	Sec
7		None	ESP	3DES	None	0	Sec
8		None	ESP	3DES	None	0	Sec
9		None	ESP	3DES	None	0	Sec
10		None	ESP	3DES	None	0	Sec

Step 19 Select DES or 3DES as the Encryption Algorithm.

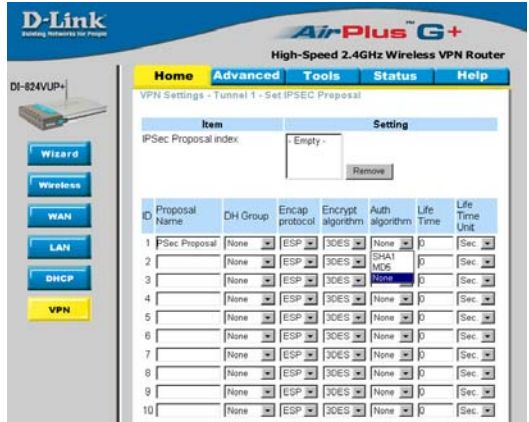
VPN Settings - Tunnel 1 - Set IPSEC Proposal

ID	Proposal Name	DH Group	Encap protocol	Encrypt algorithm	Auth algorithm	Life Time	Life Time Unit
1	FSec Proposal	None	ESP	3DES	None	0	Sec
2		None	ESP	DES	None	0	Sec
3		None	ESP	DES	None	0	Sec
4		None	ESP	3DES	None	0	Sec
5		None	ESP	3DES	None	0	Sec
6		None	ESP	3DES	None	0	Sec
7		None	ESP	3DES	None	0	Sec
8		None	ESP	3DES	None	0	Sec
9		None	ESP	3DES	None	0	Sec
10		None	ESP	3DES	None	0	Sec

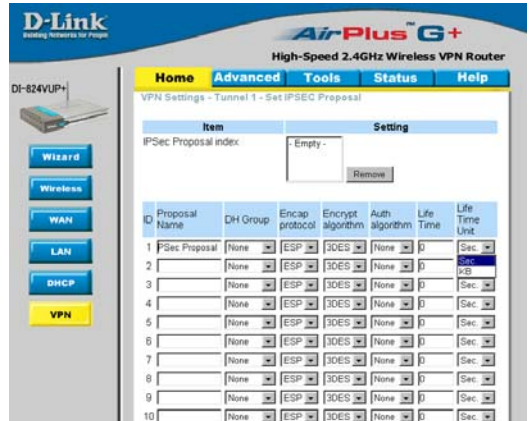
Frequently Asked Questions (continued)

I have two DI-824VUP Routers, how can I set them up to work with each other? (continued)

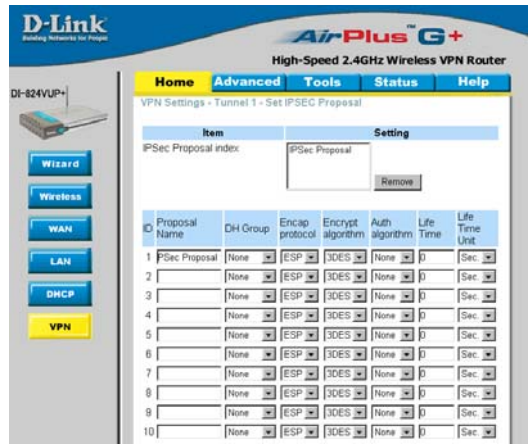
Step 20 Select SHA-1, MD5, or None as the Authentication Algorithm.



Step 21 Enter a Lifetime value and then either select Sec. or KB as the unit for the lifetime value.



Step 22 Select 1 out of the Proposal ID dropdown menu and click Add To, which will add the proposal that was just configured to the IPSec Proposal Index. Click Apply and the device will restart.



Frequently Asked Questions (continued)

I have two DI-824VUP Routers, how can I set them up to work with each other? (continued)

Step 23 Follow these instructions to configure your other DI-824VUP using the exact same settings for the IKE Proposal and the IPSec Proposal. Also make sure that Step 4 is configured to reflect the LAN settings for what is now the Local DI-824VUP and that Steps 5 & 6 are configured to reflect the Subnet and WAN IP of what is now the remote DI-824VUP.

Step 24 To establish the connection, open a command prompt and ping an IP address of a computer on the remote LAN. Once you receive replies the tunnel has been established.

How can I set up my DI-824VUP to work with a DI-804V or DI-804HV Router?

You need to first configure your DI-824VUP router.

Step 1 Log into the Web-based configuration of the router by typing in the IP address of the router (default: 192.168.0.1) in your web browser. By default the username is “admin” and there is no password.



Connect to 192.168.0.1

DI-824VUP+

User name: admin

Password:

Remember my password

OK Cancel

Step 2 Click the VPN button on the left column, select the checkbox to Enable the VPN, and then in the box next to Max. number of tunnels, enter the maximum numbers of VPN tunnels that you would like to have connected.

Frequently Asked Questions (continued)

How can I set up my DI-824VUP to work with a DI-804V or DI-804HV Router? (continued)

Step 3 In the space provided, enter the Tunnel Name for ID number 1, select IKE, and then click More.

D-Link AirPlus G+ High-Speed 2.4GHz Wireless VPN Router

Home Advanced Tools Status Help

VPN Settings

Item	Setting
VPN	<input checked="" type="checkbox"/> Enable
NetBIOS broadcast	<input type="checkbox"/> Enable
Max. number of tunnels	10

ID	Tunnel Name	Method
1	New VPN	IKE More
2		MANUAL More
3		IKE More
4		IKE More
5		IKE More

Previous page Next page

Dynamic VPN Settings L2TP Server Setting

PPTP Server Setting... View VPN Status

Apply Cancel Help

Step 4 In the **Local Subnet** and **Local Netmask** fields enter the network identifier for DI-824VUP's LAN and the corresponding subnet mask.

D-Link AirPlus G+ High-Speed 2.4GHz Wireless VPN Router

Home Advanced Tools Status Help

VPN Settings - Tunnel 1

Item	Setting
Tunnel Name	New VPN
Aggressive Mode	<input type="checkbox"/> Enable
Local Subnet	192.168.0.0
Local Netmask	256.25.256.0
Remote Subnet	0.0.0.0
Remote Netmask	0.0.0.0
Remote Gateway	
Preshare Key	
IKE Proposal index	Select IKE Proposal
IPSec Proposal index	Select IPSec Proposal

Back Apply Cancel Help

Step 5 In the **Remote Subnet** and **Remote Netmask** fields enter the network identifier for the DI-804V or DI-804HV's LAN and the corresponding subnet mask. Click Apply.

D-Link AirPlus G+ High-Speed 2.4GHz Wireless VPN Router

Home Advanced Tools Status Help

VPN Settings - Tunnel 1

Item	Setting
Tunnel Name	New VPN
Aggressive Mode	<input type="checkbox"/> Enable
Local Subnet	192.168.0.0
Local Netmask	256.25.256.0
Remote Subnet	192.168.2.0
Remote Netmask	256.25.256.0
Remote Gateway	
Preshare Key	
IKE Proposal index	Select IKE Proposal
IPSec Proposal index	Select IPSec Proposal

Back Apply Cancel Help

Frequently Asked Questions (continued)

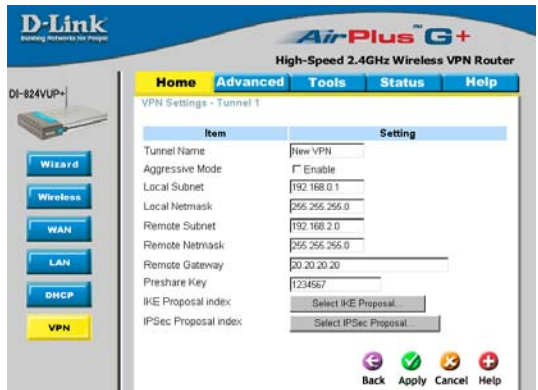
How can I set up my DI-824VUP to work with a DI-804V or DI-804HV Router? (continued)

Step 6 The device will restart. Click on the Continue button.



Step 7 In the **Remote Gateway** field enter the WAN IP address of the remote DI-804V or DI-804HV and in the **Preshare Key** field, enter a key which must be exactly the same as the Preshare Key that is configured on the DI-804V or DI-804HV.

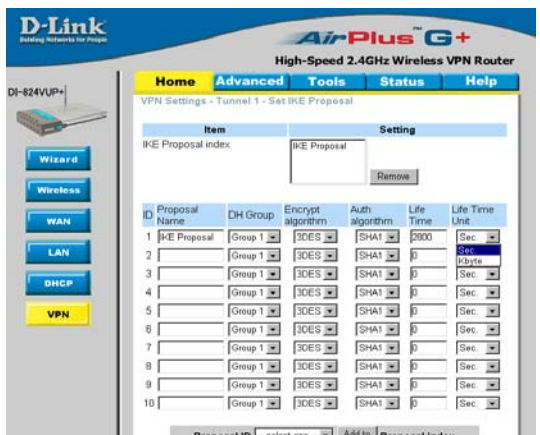
Step 8 Click Apply and then click on Select IKE Proposal.



Step 9 Enter a name for proposal ID number 1 and select Group 2 from the DH Group drop down menu.

Step 10 Select 3DES as the Encryption Algorithm and SHA-1 as the Authentication Algorithm.

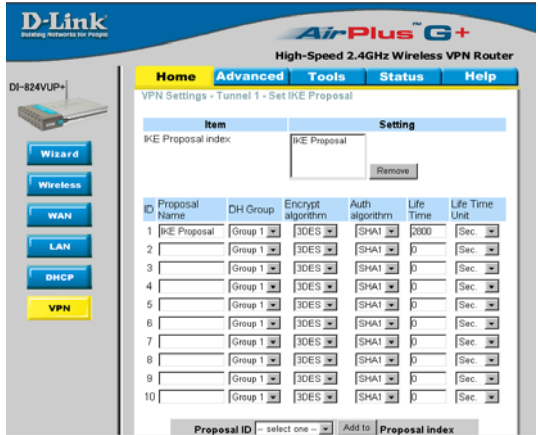
Step 11 Enter a Lifetime value of 28800 and then select Sec. as the unit for the lifetime value.



Frequently Asked Questions (continued)

How can I set up my DI-824VUP to work with a DI-804V or DI-804HV Router? (continued)

Step 12 Select 1 out of the Proposal ID dropdown menu and click Add To, which will add the proposal that was just configured to the IKE Proposal Index. Click Apply.



The screenshot shows the 'VPN Settings - Tunnel 1 - Set IKE Proposal' page. On the left is a sidebar with navigation buttons: Wizard, Wireless, WAN, LAN, DHCP, and VPN. The main content area has tabs for Home, Advanced, Tools, Status, and Help. Below the tabs is a table with columns 'Item' and 'Setting'. The 'Item' column contains 'IKE Proposal index' and the 'Setting' column contains a dropdown menu with 'IKE Proposal' selected and a 'Remove' button. Below this is a table with columns: ID, Proposal Name, DH Group, Encrypt algorithm, Auth algorithm, Life Time, and Life Time Unit. The table contains 10 rows, with the first row having 'IKE Proposal' in the Proposal Name column, 'Group 1' in the DH Group column, '3DES' in the Encrypt algorithm column, 'SHA1' in the Auth algorithm column, and '3000' in the Life Time column. At the bottom, there is a 'Proposal ID' dropdown menu set to 'select one --', an 'Add to' button, and a 'Proposal index' dropdown menu.

Step 13 The device will restart. Click on the Continue button.

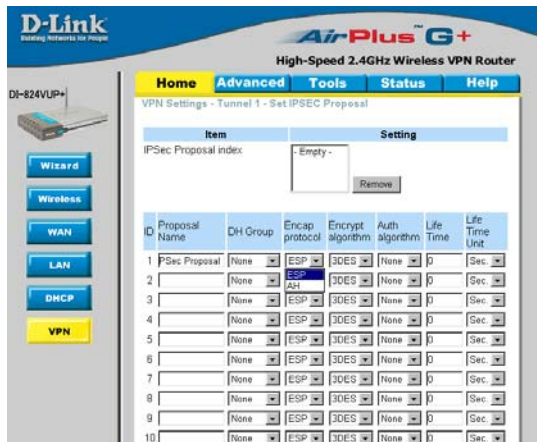


The screenshot shows the 'VPN Settings - Tunnel 1 - Set IPSEC Proposal' page. The main content area displays the message 'The device is restarting...' and a 'Continue' button.

Step 14 Click Back and click on Select IPsec Proposal.

Step 15 Enter a name for proposal ID number 1 and select None from the DH Group drop-down menu.

Step 16 Select ESP as the Encapsulation Protocol.

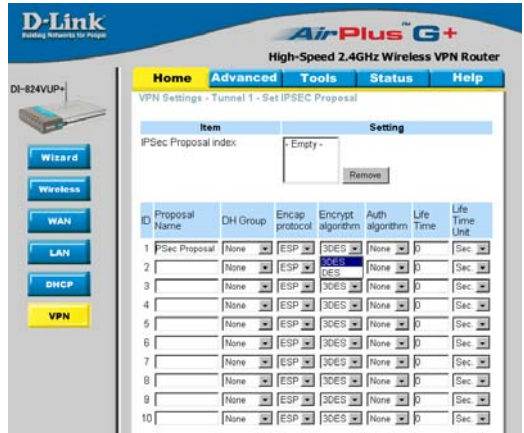


The screenshot shows the 'VPN Settings - Tunnel 1 - Set IPSEC Proposal' page. On the left is a sidebar with navigation buttons: Wizard, Wireless, WAN, LAN, DHCP, and VPN. The main content area has tabs for Home, Advanced, Tools, Status, and Help. Below the tabs is a table with columns 'Item' and 'Setting'. The 'Item' column contains 'IPSec Proposal index' and the 'Setting' column contains a dropdown menu with 'Empty -' selected and a 'Remove' button. Below this is a table with columns: ID, Proposal Name, DH Group, Encap protocol, Encrypt algorithm, Auth algorithm, Life Time, and Life Time Unit. The table contains 10 rows, with the first row having 'IPSec Proposal' in the Proposal Name column, 'None' in the DH Group column, 'ESP' in the Encap protocol column, '3DES' in the Encrypt algorithm column, 'None' in the Auth algorithm column, and '0' in the Life Time column. At the bottom, there is a 'Proposal ID' dropdown menu set to 'select one --', an 'Add to' button, and a 'Proposal index' dropdown menu.

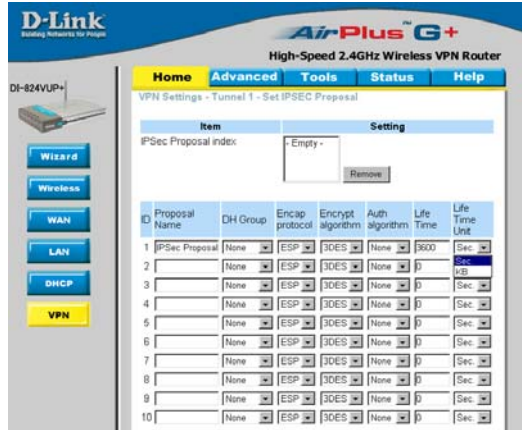
Frequently Asked Questions (continued)

How can I set up my DI-824VUP to work with a DI-804V or DI-804HV Router? (continued)

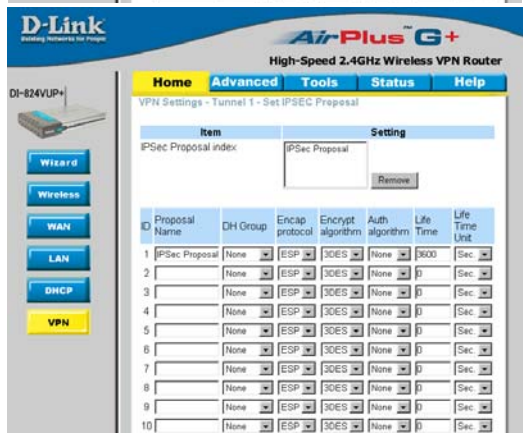
Step 17 Select 3DES as the Encryption Algorithm and MD5 as the Authentication Algorithm. Click Apply.



Step 18 Enter a Lifetime value of 3600 and then select Sec. as the unit for the lifetime value.



Step 19 Select 1 out of the Proposal ID dropdown menu and click Add To, which will add the proposal that was just configured to the IPsec Proposal Index. Click Apply. The device will restart. Click on the Continue button.



Frequently Asked Questions (continued)

How can I set up my DI-824VUP to work with a DI-804V or DI-804HV Router? (continued)

Next you need to configure the DI-804V or DI-804HV Router.

Step 1 Access the router's web configuration by entering the router's IP address in your web browser. The default IP address is 192.168.0.1. Login using your password. The default username is "admin" and the password is blank.

Step 2 Click on Basic Setup and then select Device IP Settings on the left.

Step 3 Change the LAN IP address so that it is on a different subnet than the LAN of the DI-824VUP.

The screenshot shows the D-Link VPN Router DI-804V web interface. The top navigation bar includes tabs for DEVICE INFORMATION, DEVICE STATUS, BASIC SETUP (highlighted), ADVANCED SETTINGS, SYSTEM TOOLS, and HELP. On the left, a 'Main menu' sidebar lists various settings categories, with 'DEVICE IP SETTINGS' highlighted. The main content area is titled 'DEVICE LAN IP SETTINGS' and contains the following text: 'The device LAN IP address and subnet Mask settings'. Below this, there are two rows of input fields: 'IP Address' with values 192, 168, 1, 1 and 'IP Subnet Mask' with values 255, 255, 255, 0. At the bottom right of the form are '< BACK' and 'NEXT >' buttons. A note at the bottom of the page reads: 'NOTE: Please click "Next" to accept the settings.' The footer indicates 'Copyright © 2000'.

Step 4 Click Next until you reach the Save & Restart screen. Click Save & restart and then click Basic Setup once until the unit has rebooted.

Step 5 Click on VPN Settings.

Step 6 Name your VPN connection and click ADD.

The screenshot shows the D-Link VPN Router DI-804V web interface. The top navigation bar includes tabs for DEVICE INFORMATION, DEVICE STATUS, BASIC SETUP (highlighted), ADVANCED SETTINGS, SYSTEM TOOLS, and HELP. On the left, a 'Main menu' sidebar lists various settings categories, with 'VPN SETTINGS' highlighted. The main content area is titled 'VPN SETTINGS' and contains a 'Connection Name' field with the value 'NewVPN' and an 'ADD' button. Below this is a table with the following structure:

Enable	Connection Name	Local IPSEC ID	Remote IPSEC ID	Command
<input type="checkbox"/>				

At the bottom right of the form are '< BACK' and 'NEXT >' buttons. The footer indicates 'Copyright © 2000'.

Step 7 In Remote IP Network and Remote IP Netmask fields enter the network identifier and corresponding subnet mask of the DI-824VUP's LAN.

Step 8 In the Remote Gateway IP field enter the WAN IP address of the DI-824VUP and make sure that the Network Interface is set to WAN Ethernet.

Step 9 Verify that Secure Association is set to IKE and that Perfect Forward Secure is Disabled.

Frequently Asked Questions (continued)

How can I set up my DI-824VUP to work with a DI-804V or DI-804HV Router? (continued)

Step 10 Verify the Encryption Protocol is set to 3DES and enter in your Preshared Key.

Note: The Preshared Key needs to be identical to the one configured on the DI-824VUP.

Step 11 Leave the Key Life and IKE Life Time values at their default levels and click SAVE.

D-Link VPN Router DI-804V

DEVICES INFORMATION DEVICES STATUS BASIC SETUP ADVANCED SETTINGS SYSTEM TOOLS HELP

Main menu

VPN SETTINGS

Connection Name: NewVPN

Local IPSEC Identifier: Local

Remote IPSEC Identifier: Remote

Remote IP Network: 192.168.0.0

Remote IP Netmask: 255.255.255.0

Remote Gateway IP: 10.10.10.10

Network Interface: WAN ETHERNET

Secure Association: IKE Manual

Perfect Forward Secure: Enabled Disabled

Encryption Protocol: 3DES

PreShared Key: 132456

Key Life: 3600 Seconds

IKE Life Time: 28800 Seconds

SAVE

Step 12 Click Next and then click on Save & Restart.

SAVE & RESTART

After you have configured both routers, you need to establish a connection.

Step 1 Open a command prompt and from a computer on the internal LAN of the DI-824VUP and ping the IP address of a computer that is on the internal LAN of the DI-804V or DI-804HV, or vice versa.

```
D:\>ipconfig
Windows 2000 IP Configuration

Ethernet adapter Local Area Connection 10:

    Connection-specific DNS Suffix  . : 
    IP Address. . . . .               : 192.168.1.2
    Subnet Mask . . . . .             : 255.255.255.0
    Default Gateway . . . . .         : 192.168.1.1

D:\>ping 192.168.0.100

Pinging 192.168.0.100 with 32 bytes of data:

Reply from 192.168.0.100: bytes=32 time=10ms TTL=126
Reply from 192.168.0.100: bytes=32 time<10ms TTL=126
Reply from 192.168.0.100: bytes=32 time<10ms TTL=126
Reply from 192.168.0.100: bytes=32 time<10ms TTL=126

Ping statistics for 192.168.0.100:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 10ms, Average = 2ms
```

Step 2 Once you begin to receive replies, the VPN connection has been established.

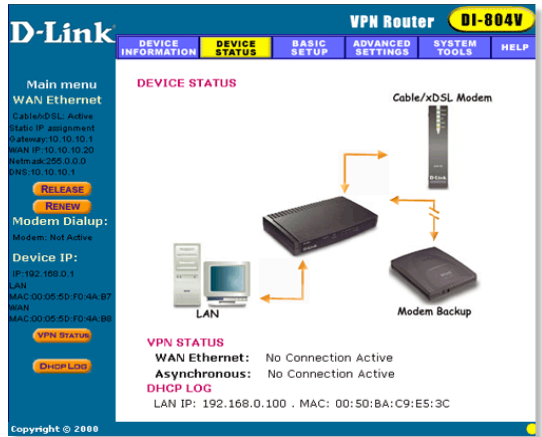
Frequently Asked Questions (continued)

How can I set up my DI-824VUP to work with a DI-804V or DI-804HV router? (continued)

Step 3 To view the Status of the VPN on the DI-804V or DI-804HV, click on Device Status.

Step 4 From the Device Status screen click on VPN Status.

Step 5 When the VPN has been established the Status will be Active.



How can I set up my DI-824VUP to work with a DFL-300 Firewall?

You need to first configure your DI-824VUP router.

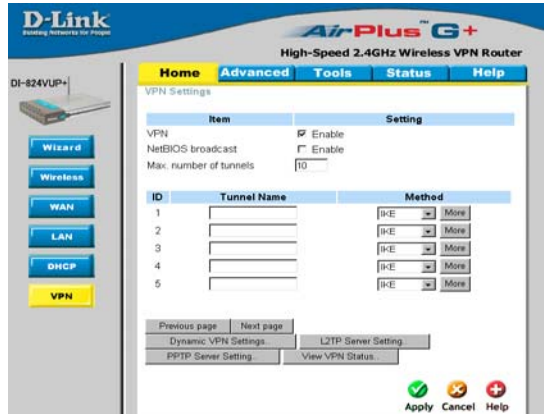
Step 1 Log into the web based configuration of the router by typing in the IP address of the router (default: 192.168.0.1) in your web browser. By default the username is “admin” and there is no password.

Step 2 Click the VPN button on the left column, select the checkbox to Enable the VPN, and then in the box next to Max. number of tunnels, enter the maximum numbers of VPN tunnels that you would like to have connected.

Frequently Asked Questions (continued)

How can I set up my DI-824VUP to work with a DFL-300 Firewall? (continued)

Step 3 In the space provided, enter the TunnelName for ID number 1, select IKE, and then click More.



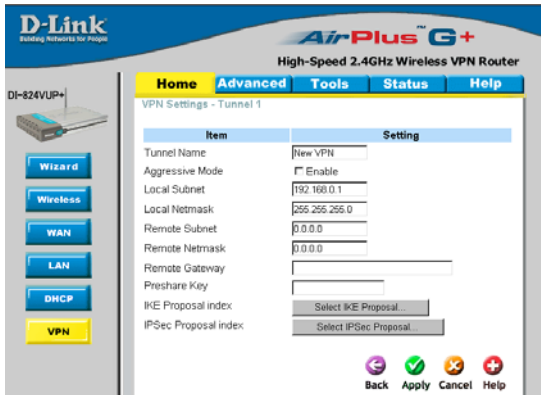
The screenshot shows the 'VPN Settings' page for a D-Link AirPlus G+ High-Speed 2.4GHz Wireless VPN Router. The 'Advanced' tab is selected. On the left, there is a navigation menu with buttons for Wizard, Wireless, WAN, LAN, DHCP, and VPN (highlighted in yellow). The main content area has a table for VPN settings:

Item	Setting
VPN	<input checked="" type="checkbox"/> Enable
NetBIOS broadcast	<input type="checkbox"/> Enable
Max. number of tunnels	10

ID	Tunnel Name	Method
1		IKE More
2		IKE More
3		IKE More
4		IKE More
5		IKE More

At the bottom, there are buttons for 'Previous page', 'Next page', 'Dynamic VPN Settings', 'L2TP Server Setting', 'PPTP Server Setting', and 'View VPN Status'. There are also 'Apply', 'Cancel', and 'Help' buttons at the bottom right.

Step 4 In the **Local Subnet** and **Local Netmask** fields enter the network identifier for DI-824VUP's LAN and the corresponding subnet mask.

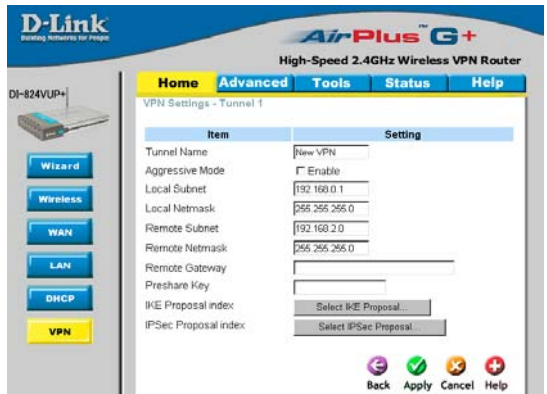


The screenshot shows the 'VPN Settings - Tunnel 1' page. The 'Advanced' tab is selected. The left navigation menu is the same as in Step 3. The main content area has a table for Tunnel 1 settings:

Item	Setting
Tunnel Name	New VPN
Aggressive Mode	<input type="checkbox"/> Enable
Local Subnet	192.168.0.1
Local Netmask	255.255.255.0
Remote Subnet	0.0.0.0
Remote Netmask	0.0.0.0
Remote Gateway	
Preshare Key	
IKE Proposal index	Select IKE Proposal...
IPSec Proposal index	Select IPSec Proposal...

At the bottom right, there are 'Back', 'Apply', 'Cancel', and 'Help' buttons.

Step 5 In the **Remote Subnet** and **Remote Netmask** fields enter the network identifier for the DFL-300's Internal interface and the corresponding subnet mask.



The screenshot shows the 'VPN Settings - Tunnel 1' page with updated values for the Remote Subnet and Remote Netmask fields:

Item	Setting
Tunnel Name	New VPN
Aggressive Mode	<input type="checkbox"/> Enable
Local Subnet	192.168.0.1
Local Netmask	255.255.255.0
Remote Subnet	192.168.2.0
Remote Netmask	255.255.255.0
Remote Gateway	
Preshare Key	
IKE Proposal index	Select IKE Proposal...
IPSec Proposal index	Select IPSec Proposal...

The 'Apply' button is highlighted in green, indicating the settings have been saved.

Frequently Asked Questions (continued)

How can I set up my DI-824VUP to work with a DFL-300 Firewall? (continued)

Step 6 In the Remote Gateway field enter the WAN IP address of the remote DFL-300 and in the Preshared Key field, enter a key which must be exactly the same as the Preshared Key that is configured on the DFL-300.

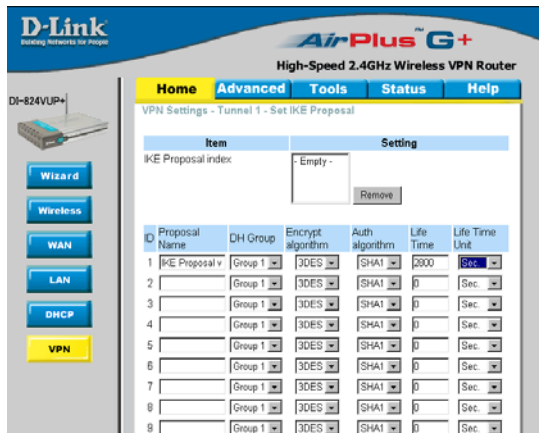
Step 7 Click Apply. The device will restart. Click on the Continue button and then click on Select IKE Proposal.



Step 8 Enter a name for proposal ID number 1 and select Group 2 from the DH Group dropdown menu.

Step 9 Select 3DES as the Encryption Algorithm and SHA-1 as the Authentication Algorithm.

Step 10 Enter a Lifetime value of 28800 and then select Sec. as the unit for the lifetime value.



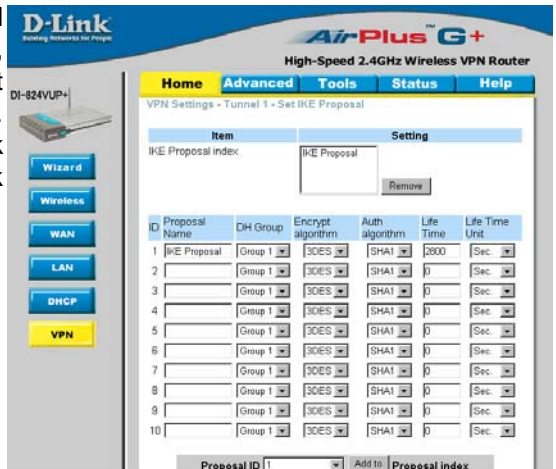
Frequently Asked Questions (continued)

How can I set up my DI-824VUP to work with a DFL-300 Firewall? (continued)

Step 11 Select 1 out of the Proposal ID dropdown menu and click Add To, which will add the proposal that was just configured to the IKE Proposal Index. Click Apply. The device will restart. Click on the Continue button and then click Back.

Step 12 Click on Select IPsec Proposal.

Step 13 Enter a name for proposal ID number 1 and select None from the DH Group dropdown menu.



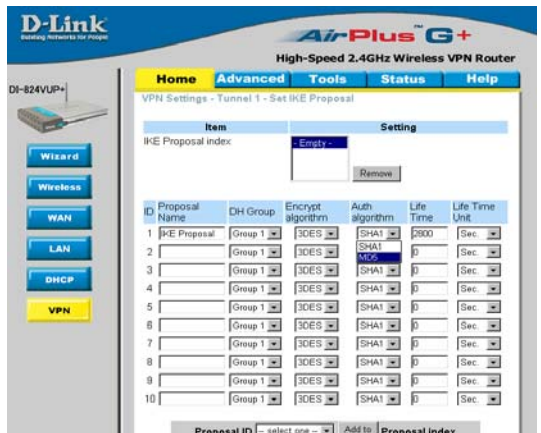
The screenshot shows the VPN Settings - Tunnel 1 - Set IKE Proposal page. On the left is a navigation menu with buttons for Wizard, Wireless, WAN, LAN, DHCP, and VPN. The main area has tabs for Home, Advanced, Tools, Status, and Help. Below the tabs is a table for IKE Proposal Index. The table has columns for Proposal Name, DH Group, Encrypt algorithm, Auth algorithm, Life Time, and Life Time Unit. Row 1 is selected and has 'IKE Proposal' in the Proposal Name column, 'None' in the DH Group column, '3DES' in the Encrypt algorithm column, 'SHA1' in the Auth algorithm column, '2800' in the Life Time column, and 'Sec.' in the Life Time Unit column. Below the table is a 'Proposal ID' dropdown menu with '1' selected and an 'Add to Proposal index' button.

ID	Proposal Name	DH Group	Encrypt algorithm	Auth algorithm	Life Time	Life Time Unit
1	IKE Proposal	None	3DES	SHA1	2800	Sec.
2		Group 1	3DES	SHA1	0	Sec.
3		Group 1	3DES	SHA1	0	Sec.
4		Group 1	3DES	SHA1	0	Sec.
5		Group 1	3DES	SHA1	0	Sec.
6		Group 1	3DES	SHA1	0	Sec.
7		Group 1	3DES	SHA1	0	Sec.
8		Group 1	3DES	SHA1	0	Sec.
9		Group 1	3DES	SHA1	0	Sec.
10		Group 1	3DES	SHA1	0	Sec.

Step 14 Select ESP as the Encapsulation Protocol.

Step 15 Select 3DES as the Encryption Algorithm and MD5 as the Authentication Algorithm.

Step 16 Enter a Lifetime value of 28800 and then select Sec. as the lifetime value.



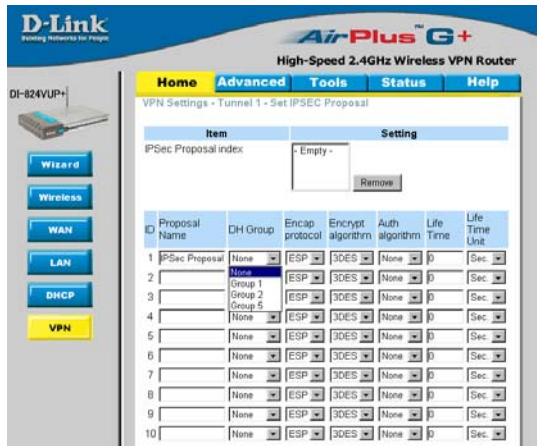
The screenshot shows the same VPN Settings - Tunnel 1 - Set IKE Proposal page. The IKE Proposal Index table now shows that proposal 1 has been updated. The Proposal Name is 'IKE Proposal', the DH Group is 'None', the Encrypt algorithm is '3DES', the Auth algorithm is 'MD5', the Life Time is '28800', and the Life Time Unit is 'Sec.'. The 'Proposal ID' dropdown menu now shows '- select one -' and the 'Add to Proposal index' button is still present.

ID	Proposal Name	DH Group	Encrypt algorithm	Auth algorithm	Life Time	Life Time Unit
1	IKE Proposal	None	3DES	MD5	28800	Sec.
2		Group 1	3DES	SHA1	0	Sec.
3		Group 1	3DES	SHA1	0	Sec.
4		Group 1	3DES	SHA1	0	Sec.
5		Group 1	3DES	SHA1	0	Sec.
6		Group 1	3DES	SHA1	0	Sec.
7		Group 1	3DES	SHA1	0	Sec.
8		Group 1	3DES	SHA1	0	Sec.
9		Group 1	3DES	SHA1	0	Sec.
10		Group 1	3DES	SHA1	0	Sec.

Frequently Asked Questions (continued)

How can I set up my DI-824VUP to work with a DFL-300 Firewall? (continued)

Step 17 Select 1 out of the Proposal ID dropdown menu and click Add To, which will add the proposal that was just configured to the IPsec Proposal Index. Click Apply and then click Restart.



Step 18 The device will restart. Click on the Continue button.

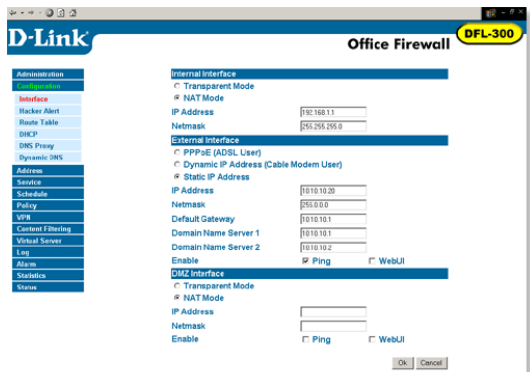


Next you need to configure the DFL-300 firewall.

Step 1 Access the configuration screen of the DFL-300 by opening a web browser such as Internet Explorer and type the IP address of the DFL-300 in the address bar (192.168.1.1).

Step 2 Enter the username (admin) and the password (admin). Click OK.

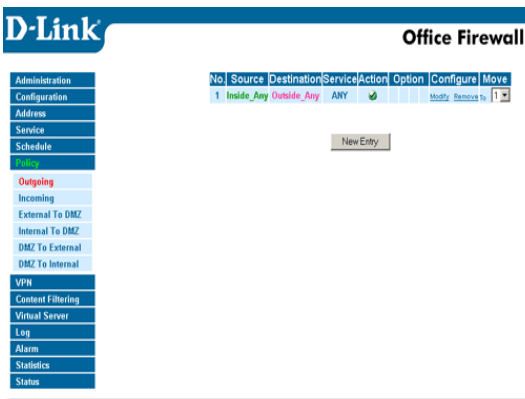
Step 3 Click on Configuration and take note of the IP address that your ISP has assigned you.



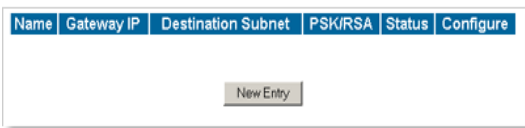
Frequently Asked Questions (continued)

How can I set up my DI-824VUP to work with a DFL-300 Firewall? (continued)

Step 4 Click on Policy and verify that you have an Outgoing policy configured. If not, click on New Entry, accept the default values, and click OK.



Step 5 Click on VPN and then click New Entry.



Step 6 Give the VPN connection a name with no spaces.

Step 7 Enter the network identifier and subnet mask of the Internal interface.

Step 8 In the To Destination section, select either Remote Gateway—Fixed IP or Remote Gateway—Dynamic IP. Enter the WAN IP address of the DI-824VUP if Remote Gateway—Fixed IP is selected.

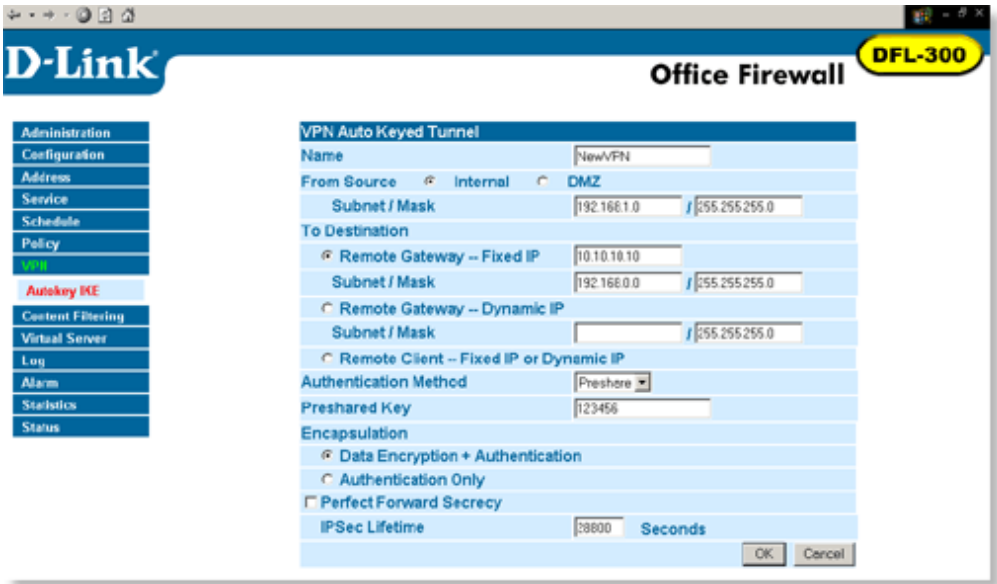
Step 9 Enter the network identifier corresponding subnet mask of the DI-824VUP's LAN.

Step 10 Enter a Preshared Key. The Preshared Key needs to be identical to the one configured on the DI-824VUP.

Step 11 Select Data Encryption and Authentication as the Encapsulation and click OK.

Frequently Asked Questions (continued)

How can I set up my DI-824VUP to work with a DFL-300 Firewall?
(continued)



After you have configured both the router and firewall, you need to establish a connection.

Step 1 Open a command prompt and from a computer connected to the Internal interface of the DFL-300 and ping the IP address of a computer that is on the internal LAN of the DI-824VUP, or vice versa.

```
D:\>ipconfig

Windows 2000 IP Configuration

Ethernet adapter Local Area Connection 10:

    Connection-specific DNS Suffix  . : 
    IP Address. . . . . : 192.168.1.2
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.1.1

D:\>ping 192.168.0.100

Pinging 192.168.0.100 with 32 bytes of data:

Reply from 192.168.0.100: bytes=32 time<10ms TTL=126
Reply from 192.168.0.100: bytes=32 time<10ms TTL=126
Reply from 192.168.0.100: bytes=32 time<10ms TTL=126
Reply from 192.168.0.100: bytes=32 time<10ms TTL=126

Ping statistics for 192.168.0.100:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 10ms, Average = 2ms
```

Step 2 Once you begin to receive replies, the VPN connection has been established.

Frequently Asked Questions (continued)

How do I open ports on my DI-824VUP?

To allow traffic from the internet to enter your local network, you will need to open up ports or the router will block the request.

Step 1 Open your Web browser and enter the IP Address of your D-Link router (192.168.0.1). Enter username (admin) and your password (blank by default).

Step 2 Click on **Advanced** on top and then click **Virtual Server** on the left side.

Step 3 Check **Enabled** to activate entry.

Step 4 Enter a name for your virtual server entry.

Step 5 Next to **Private IP**, enter the IP Address of the computer on your local network that you want to allow the incoming service to.

Step 6 Choose **Protocol Type** - either TCP, UDP, or both. If you are not sure, select both.

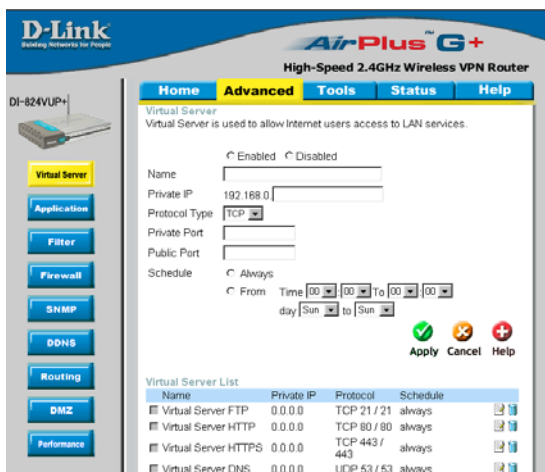
Step 7 Enter the port information next to **Private Port** and **Public Port**. The private and public ports are usually the same. The public port is the port seen from the WAN side, and the private port is the port being used by the application on the computer within your local network.

Step 8 Enter the **Schedule** information.

Step 9 Click **Apply** and then click **Continue**.

Note: Make sure DMZ host is disabled. If DMZ is enabled, it will disable all Virtual Server entries.

Because our routers use NAT (Network Address Translation), you can only open a specific port to one computer at a time. For example: If you have 2 web servers on your network, you cannot open port 80 to both computers. You will need to configure 1 of the web servers to use port 81. Now you can open port 80 to the first computer and then open port 81 to the other computer.



Frequently Asked Questions (continued)

What is DMZ?

Demilitarized Zone:

In computer networks, a DMZ (demilitarized zone) is a computer host or small network inserted as a neutral zone between a company's private network and the outside public network. It prevents outside users from getting direct access to a server that has company data. (The term comes from the geographic buffer zone that was set up between North Korea and South Korea following the UN police action in the early 1950s.) A DMZ is an optional and more secure approach to a firewall and effectively acts as a proxy server as well.

In a typical DMZ configuration for a small company, a separate computer (or host in network terms) receives requests from users within the private network for access to Web sites or other companies accessible on the public network. The DMZ host then initiates sessions for these requests on the public network. However, the DMZ host is not able to initiate a session back into the private network. It can only forward packets that have already been requested.

Users of the public network outside the company can access only the DMZ host. The DMZ may typically also have the company's Web pages so these could be served to the outside world. However, the DMZ provides access to no other company data. In the event that an outside user penetrated the DMZ hosts security, the Web pages might be corrupted but no other company information would be exposed. D-Link, a leading maker of routers, is one company that sells products designed for setting up a DMZ.

How do I configure the DMZ Host?

The DMZ feature allows you to forward all incoming ports to one computer on the local network. The DMZ, or Demilitarized Zone, will allow the specified computer to be exposed to the Internet. DMZ is useful when a certain application or game does not work through the firewall. The computer that is configured for DMZ will be completely vulnerable on the Internet, so it is suggested that you try opening ports from the Virtual Server or Firewall settings before using DMZ.

Step 1 Find the IP address of the computer you want to use as the DMZ host.

To find out how to locate the IP Address of the computer in Windows XP/2000/ME/9x or Macintosh operating systems please refer to Step 4 of the first question in this section (Frequently Asked Questions).

Frequently Asked Questions (continued)

How do I configure the DMZ Host? (continued)

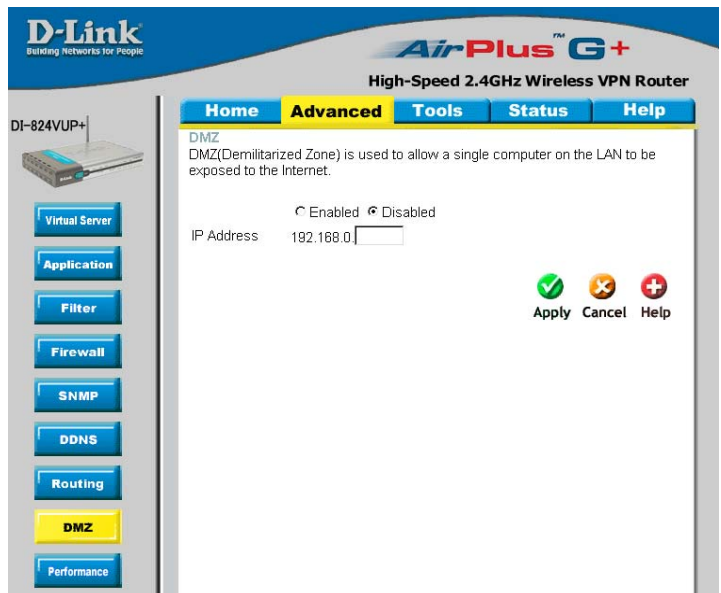
Step 2 Log into the web based configuration of the router by typing in the IP Address of the router (default:192.168.0.1) in your web browser. The username is **admin** (all lowercase) and the password is blank (empty).



Step 3 Click the **Advanced** tab and then click on the **DMZ** button. Select **Enable** and type in the IP Address from step 1.

Step 4 Click **Apply** and then **Continue** to save the changes.

Note: When DMZ is enabled, Virtual Server settings will still be effective. Remember, you cannot forward the same port to multiple IP Addresses, so the Virtual Server settings will take priority over DMZ settings.



Frequently Asked Questions (continued)

How do I open a range of ports on my DI-824VUP using Firewall rules?

Step 1 Access the router's web configuration by entering the router's IP Address in your web browser. The default IP Address is **192.168.0.1**. Login using your password. The default username is "**admin**" and the password is blank.

If you are having difficulty accessing web management, please see the first question in this section.

Step 2 From the web management Home page, click the **Advanced** tab then click the **Firewall** button.

Step 3 Click on **Enabled** and type in a name for the new rule.

Step 4 Choose **WAN** as the **Source** and enter a range of IP Addresses out on the internet that you would like this rule applied to. If you would like this rule to allow all internet users to be able to access these ports, then put an **Asterisk** in the first box and leave the second box empty.

The screenshot shows the D-Link DI-824VUP+ web configuration interface. The page title is "AirPlus G+ High-Speed 2.4GHz Wireless VPN Router". The "Advanced" tab is selected, and the "Firewall" button is highlighted in the left sidebar. The main content area is titled "Firewall Rules" and contains the following configuration options:

- Enabled/Disabled:** Enabled Disabled
- Name:** [Text input field]
- Action:** Allow Deny
- Interface:** [Dropdown menu]
- IP Start:** [Text input field]
- IP End:** [Text input field]
- Protocol:** [Dropdown menu]
- Port Range:** [Text input field]
- Source:** [Dropdown menu] [Text input field]
- Destination:** [Dropdown menu] [Text input field]
- Schedule:** Always From [Time dropdown] [Time dropdown] To [Time dropdown] [Time dropdown] day [Day dropdown] to [Day dropdown]

Buttons for **Apply**, **Cancel**, and **Help** are located below the configuration options. Below the configuration area is a "Firewall Rules List" table:

Action Name	Source	Destination	Protocol	
<input type="checkbox"/> Allow	Allow to Ping WAN port	WAN,*	LAN,192.168.0.1 ICMP,*	
<input type="checkbox"/> Deny	Default	*,*	LAN,192.168.0.1	
<input type="checkbox"/> Allow	Default	LAN,*	*,192.168.0.1	

Step 5 Select **LAN** as the **Destination** and enter the IP Address of the computer on your local network that you want to allow the incoming service to. This will not work with a range of IP Addresses.

Step 6 Enter the port or range of ports that are required to be open for the incoming service.

Step 7 Click **Apply** and then click **Continue**.

Note: Make sure DMZ host is disabled.

Because our routers use NAT (Network Address Translation), you can only open a specific port to one computer at a time. For example: If you have 2 web servers on your network, you cannot open port 80 to both computers. You will need to configure 1 of the web servers to use port 81. Now you can open port 80 to the first computer and then open port 81 to the other computer.

Frequently Asked Questions (continued)

What are virtual servers?

A Virtual Server is defined as a service port, and all requests to this port will be redirected to the computer specified by the server IP. For example, if you have an FTP Server (port 21) at 192.168.0.5, a Web server (port 80) at 192.168.0.6, and a VPN (port 1723) server at 192.168.0.7, then you need to specify the following virtual server mapping table:

Server Port	Server IP	Enable
21	192.168.0.5	X
80	192.168.0.6	X
1723	192.168.0.7	X

How do I use *PC Anywhere* with my DI-824VUP?

You will need to open 3 ports in the Virtual Server section of your D-Link router.

Step 1 Open your web browser and enter the IP Address of the router (192.168.0.1).

Step 2 Click on **Advanced** at the top and then click **Virtual Server** on the left side.

Step 3 Enter the information as seen below. The **Private IP** is the IP Address of the computer on your local network that you want to connect to.

Step 4 The first entry will read as shown here:

Step 5 Click **Apply** and then click **Continue**.

D-Link
Building Networks for People

AirPlus™ G+
High-Speed 2.4GHz Wireless VPN Router

Home **Advanced** Tools Status Help

Virtual Server
Virtual Server is used to allow Internet users access to LAN services.

Enabled Disabled

Name: pcanewhere1

Private IP: 192.168.0.1

Protocol Type: TCP

Private Port:

Public Port:

Schedule: Always
 From Time [00] : [00] To [00] : [00]
day [Sun] to [Sun]

Apply Cancel Help

Virtual Server List

Name	Private IP	Protocol	Schedule	
Virtual Server FTP	0.0.0.0	TCP 21 / 21	always	
Virtual Server HTTP	0.0.0.0	TCP 80 / 80	always	
Virtual Server HTTPS	0.0.0.0	TCP 443 / 443	always	
Virtual Server DNS	0.0.0.0	UDP 53 / 53	always	

Frequently Asked Questions (continued)

How do I use *PC Anywhere* with my DI-824VU? (continued)

Step 6 Create a second entry as shown here:

DI-824VU+ High-Speed 2.4GHz Wireless VPN Router

Virtual Server

Virtual Server is used to allow Internet users access to LAN services.

Enabled Disabled

Name: pcanywhere2

Private IP: 192.168.0.1

Protocol Type: TCP

Private Port: []

Public Port: []

Schedule: Always

From Time [00] [00] To [00] [00] day [Sun] to [Sun]

Apply Cancel Help

Name	Private IP	Protocol	Schedule
Virtual Server FTP	0.0.0.0	TCP 21 / 21	always
Virtual Server HTTP	0.0.0.0	TCP 80 / 80	always
Virtual Server HTTPS	0.0.0.0	TCP 443 / 443	always
Virtual Server DNS	0.0.0.0	UDP 53 / 53	always

Step 7 Click **Apply** and then click **Continue**.

Step 8 Create a third and final entry as shown here:

DI-824VU+ High-Speed 2.4GHz Wireless VPN Router

Virtual Server

Virtual Server is used to allow Internet users access to LAN services.

Enabled Disabled

Name: pcanywhere3

Private IP: 192.168.0.1

Protocol Type: TCP

Private Port: []

Public Port: []

Schedule: Always

From Time [00] [00] To [00] [00] day [Sun] to [Sun]

Apply Cancel Help

Name	Private IP	Protocol	Schedule
Virtual Server FTP	0.0.0.0	TCP 21 / 21	always
Virtual Server HTTP	0.0.0.0	TCP 80 / 80	always
Virtual Server HTTPS	0.0.0.0	TCP 443 / 443	always
Virtual Server DNS	0.0.0.0	UDP 53 / 53	always

Step 9 Click **Apply** and then click **Continue**.

Step 10 Run *PCAnywhere* from the remote site and use the WAN IP Address of the router, not your computer's IP Address.

Frequently Asked Questions (continued)

How can I use eDonkey behind my DI-824VUP?

You must open ports on your router to allow incoming traffic while using eDonkey.

eDonkey uses three ports (4 if using CLI):

4661 (TCP) To connect with a server

4662 (TCP) To connect with other clients

4665 (UDP) To communicate with servers other than the one you are connected to.

4663 (TCP) *Used with the command line (CLI) client when it is configured to allow remote connections. This is the case when using a Graphical Interface (such as the Java Interface) with the client.

Step 1 Open your web browser and enter the IP Address of your router (192.168.0.1). Enter username (admin) and your password (leave blank).

Step 2 Click on **Advanced** and then click **Firewall**.

Step 3 Create a new firewall rule:

Click **Enabled**.

Enter a name (edonkey).

Click **Allow**.

Next to Source, select **WAN** under interface. In the first box, enter an *. Leave the second box empty.

Next to Destination, select **LAN** under interface. Enter the IP Address of the computer you are running eDonkey from. Leave the second box empty. Under Protocol, select *. In the port range boxes, enter **4661** in the first box and then **4665** in the second box.

Click **Always** or set a schedule.

The screenshot shows the D-Link AirPlus G+ router's web interface. The 'Advanced' tab is selected, and the 'Firewall' sub-tab is active. A new firewall rule named 'edonkey' is being configured. The rule is enabled, has an 'Allow' action, and is applied to the WAN interface. The source is set to 'WAN' with an IP range of '*.*.*.*'. The destination is set to 'LAN' with an IP range of '192.168.0.100'. The protocol is 'TCP' and the port range is '4661-4665'. The schedule is set to 'Always'. The 'Apply' button is highlighted.

ActionName	Source	Destination	Protocol
<input type="checkbox"/> Allow Allow to Ping WAN port	WAN,*	LAN,192.168.0.1	ICMP,*
<input type="checkbox"/> Deny Default	*.*	LAN,192.168.0.1	*.*
<input type="checkbox"/> Allow Default	LAN,*	*.-192.168.0.1	*.*

Step 4 Click **Apply** and then **Continue**.

Frequently Asked Questions (continued)

How do I set up my DI-824VUP for SOCOM on my Playstation 2?

To allow you to play SOCOM and hear audio, you must download the latest firmware for the router (if needed), enable Game Mode, and open port 6869 to the IP Address of your Playstation.

Step 1 Upgrade firmware (follow link above).

Step 2 Open your web browser and enter the IP Address of the router (192.168.0.1). Enter username (admin) and your password (blank by default).

Step 3 Click on the **Advanced** tab and then click on **Virtual Server** on the left side.

Step 4 You will now create a new Virtual Server entry. Click **Enabled** and enter a name (socom). Enter the IP Address of your Playstation for **Private IP**.

Step 5 For **Protocol Type** select Both. Enter **6869** for both the **Private Port** and **Public Port**. Click **Always**. Click **Apply** to save changes and then **Continue**

D-Link
Binding Networks for People

AirPlus G+
High-Speed 2.4GHz Wireless VPN Router

DI-824VUP+

Virtual Server

Virtual Server is used to allow Internet users access to LAN services.

Enabled Disabled

Name:

Private IP:

Protocol Type:

Private Port:

Public Port:

Schedule: Always
 From Time : To :
day to

Apply Cancel Help

Virtual Server List

Name	Private IP	Protocol	Schedule		
<input type="checkbox"/> Virtual Server FTP	0.0.0.0	TCP 21 / 21	always	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> Virtual Server HTTP	0.0.0.0	TCP 80 / 80	always	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> Virtual Server HTTPS	0.0.0.0	TCP 443 / 443	always	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> Virtual Server DNS	0.0.0.0	UDP 53 / 53	always	<input type="checkbox"/>	<input type="checkbox"/>

Step 6 Click on the **Tools** tab and then **Misc** on the left side.

Step 7 Make sure **Gaming Mode** is Enabled. If not, click **Enabled**. Click **Apply** and then **Continue**.

Frequently Asked Questions (continued)

How can I use Gamespy behind my DI-824VUP?

Step 1 Open your web browser and enter the IP Address of the router (192.168.0.1). Enter admin for the username and your password (blank by default).

Step 2 Click on the Advanced tab and then click Virtual Server on the left side.

Step 3 You will create 2 entries.

Step 4 Click Enabled and enter Settings:

NAME - Gamespy1

PRIVATE IP - The IP Address of your computer that you are running Gamespy from.

PROTOCOL TYPE - Both

PRIVATE PORT - 3783

The screenshot shows the 'Virtual Server' configuration page for a D-Link DI-824VUP+ router. The 'Advanced' tab is selected. The 'Virtual Server' section is enabled. The configuration for 'Gamespy1' is as follows:

Name	Private IP	Protocol	Schedule
Virtual Server FTP	0.0.0.0	TCP 21 / 21	always
Virtual Server HTTP	0.0.0.0	TCP 80 / 80	always
Virtual Server HTTPS	0.0.0.0	TCP 443 / 443	always
Virtual Server DNS	0.0.0.0	UDP 53 / 53	always

Click **Apply** and then **continue**

Step 5 Enter 2nd entry:

Click Enabled

NAME - Gamespy2

PRIVATE IP - The IP Address of your computer that you are running Gamespy from.

PROTOCOL TYPE - Both

PRIVATE PORT - 6500

PUBLIC PORT - 6500

SCHEDULE - Always.

The screenshot shows the 'Virtual Server' configuration page for a D-Link DI-824VUP+ router. The 'Advanced' tab is selected. The 'Virtual Server' section is enabled. The configuration for 'Gamespy2' is as follows:

Name	Private IP	Protocol	Schedule
Virtual Server FTP	0.0.0.0	TCP 21 / 21	always
Virtual Server HTTP	0.0.0.0	TCP 80 / 80	always
Virtual Server HTTPS	0.0.0.0	TCP 443 / 443	always
Virtual Server DNS	0.0.0.0	UDP 53 / 53	always

Click **Apply** and then **continue**.

Frequently Asked Questions (continued)

How do I configure my DI-824VUP for KaZaA and Grokster?

The following is for KaZaA, Grokster, and others using the FastTrack P2P file sharing system.

In most cases, you do not have to configure anything on the router or on the Kazaa software. If you are having problems, please follow steps below:

Step 1 Enter the IP Address of your router in a web browser (192.168.0.1).

Step 2 Enter your username (admin) and your password (blank by default).

Step 3 Click on Advanced and then click Virtual Server.

Step 4 Click Enabled and then enter a Name (kazaa for example).

Step 5 Enter the IP Address of the computer you are running KaZaA from in the Private IP box. Select TCP for the Protocol Type.

Step 6 Enter 1214 in the Private and Public Port boxes. Click Always under schedule or set a time range. Click Apply.

The screenshot shows the configuration page for a D-Link DI-824VUP+ router. The page is titled "AirPlus™ G+ High-Speed 2.4GHz Wireless VPN Router". The navigation tabs are Home, Advanced (selected), Tools, Status, and Help. The "Virtual Server" section is active, showing the following configuration:

- Virtual Server: Enabled (radio button selected), Disabled (radio button unselected)
- Name: kazaa
- Private IP: 192.168.0.100
- Protocol Type: TCP
- Private Port: 6859
- Public Port: 6859
- Schedule: Always (radio button selected), From Time [00][00] To [00][00] day [Sun] to [Sun] (radio button unselected)

Buttons for Apply, Cancel, and Help are visible. Below the configuration is a "Virtual Server List" table:

Name	Private IP	Protocol	Schedule	
Virtual Server FTP	0.0.0.0	TCP 21 / 21	always	[icon] [icon]
Virtual Server HTTP	0.0.0.0	TCP 80 / 80	always	[icon] [icon]
Virtual Server HTTPS	0.0.0.0	TCP 443 / 443	always	[icon] [icon]
Virtual Server DNS	0.0.0.0	UDP 53 / 53	always	[icon] [icon]

Make sure that you did not enable proxy/firewall in the KaZaA software.

Frequently Asked Questions (continued)

How do I configure my DI-824VUP to play Warcraft 3?

To host a Warcraft 3 game, you must open ports on your router to allow incoming traffic. To play a game, you do not have to configure your router.

Warcraft 3 (Battlenet) uses port 6112.

For the DI-824VUP:

Step 1 Open your web browser and enter the IP Address of your router (192.168.0.1). Enter username (admin) and your password (leave blank).

Step 2 Click on **Advanced** and then click **Virtual Server**.

Step 3 Create a new entry: Click **Enabled**. Enter a name (warcraft3). Private IP - Enter the IP Address of the computer you want to host the game. Select **Both** for Protocol Type. Enter **6112** for both Private Port and Public Port. Click **Always** or set a schedule.

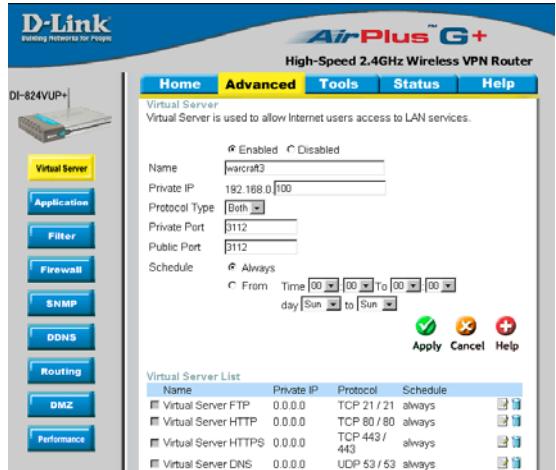
Step 4 Click **Apply** and then **Continue**.

Note: If you want multiple computers from your LAN to play in the same game that you are hosting, then repeat the steps above and enter the IP Addresses of the other computers. You will need to change ports. Computer #2 can use port 6113, computer #3 can use 6114, and so on.

You will need to change the port information within the Warcraft 3 software for computers #2 and up.

Configure the Game Port information on each computer:

Start Warcraft 3 on each computer, click **Options > Gameplay**. Scroll down and you should see **Game Port**. Enter the port number as you entered in the above steps.



Frequently Asked Questions (continued)

How do I use NetMeeting with my DI-824VUP?

Unlike most TCP/IP applications, NetMeeting uses **DYNAMIC PORTS** instead of STATIC PORTS. That means that each NetMeeting connection is somewhat different than the last. For instance, the HTTP web site application uses port 80. NetMeeting can use any of over 60,000 different ports.

All broadband routers using (only) standard NAT and all internet sharing programs like Microsoft ICS that use (only) standard NAT will NOT work with NetMeeting or other h.323 software packages.

The solution is to put the router in DMZ.

Note: A few hardware manufacturers have taken it on themselves to actually provide H.323 compatibility. This is not an easy task since the router must search each incoming packet for signs that it might be a netmeeting packet. This is a whole lot more work than a router normally does and may actually be a **weak point in the firewall**. D-Link is not one of the manufacturers.

To read more on this visit <http://www.HomenetHelp.com>

How do I set up my DI-824VUP to use iChat? -for Macintosh users-

You must open ports on your router to allow incoming traffic while using iChat.

iChat uses the following ports: 5060 (UDP), 5190 (TCP), and File Sharing 16384-16403 (UDP) to video conference with other clients.

Step 1 Open your web browser and enter the IP Address of your router (192.168.0.1). Enter username (admin) and your password (leave blank).

Step 2 Click on **Advanced** and then click **Firewall**.

Frequently Asked Questions (continued)

How do I set up my DI-824VUP to use iChat? -for Macintosh users- (continued)

Step 3 Create a new firewall rule:

Click **Enabled**.

Enter a name (ichat1).

Click **Allow**.

Next to Source, select **WAN** under interface.

In the first box, enter an *.

Leave the second box empty.

Next to Destination, select **LAN** under interface.

Enter the IP Address of the computer you are running iChat from.

D-Link Building Networks for People
AirPlus G+ High-Speed 2.4GHz Wireless VPN Router

Home **Advanced** Tools Status Help

Firewall Rules
Firewall Rules can be used to allow or deny traffic from passing through the DI-824VUP+.

Enabled Disabled

Name:

Action: Allow Deny

Interface: IP Start IP End Protocol Port Range

Source: WAN

Destination: LAN UDP

Schedule: Always
 From Time To
day to

Apply Cancel Help

ActionName	Source	Destination	Protocol
<input checked="" type="checkbox"/> Allow Allow to Ping WAN port	WAN,*	LAN,192.168.0.1	ICMP,*
<input checked="" type="checkbox"/> Deny Default	**	LAN,192.168.0.1	**
<input checked="" type="checkbox"/> Allow Default	LAN,*	*,192.168.0.1	**

Leave the second box empty. Under Protocol, select **UDP**. In the port range boxes, enter **5060** in the first box and leave the second box empty.

Click **Always** or set a schedule.

Step 4 Click **Apply** and then **Continue**.

Step 5

Repeat steps 3 and 4 enter **ichat2** and open ports **16384-16403** (UDP).

D-Link Building Networks for People
AirPlus G+ High-Speed 2.4GHz Wireless VPN Router

Home **Advanced** Tools Status Help

Firewall Rules
Firewall Rules can be used to allow or deny traffic from passing through the DI-824VUP+.

Enabled Disabled

Name:

Action: Allow Deny

Interface: IP Start IP End Protocol Port Range

Source: WAN

Destination: LAN UDP

Schedule: Always
 From Time To
day to

Apply Cancel Help

ActionName	Source	Destination	Protocol
<input checked="" type="checkbox"/> Allow Allow to Ping WAN port	WAN,*	LAN,192.168.0.1	ICMP,*
<input checked="" type="checkbox"/> Deny Default	**	LAN,192.168.0.1	**
<input checked="" type="checkbox"/> Allow Default	LAN,*	*,192.168.0.1	**

Frequently Asked Questions (continued)

How do I set up my DI-824VUP to use iChat? -for Macintosh users- (continued)

For File Sharing:

Step 1 Click on **Advanced** and then **Virtual Server**.

Step 2 Check **Enabled** to activate entry.

Step 3 Enter a name for your virtual server entry (ichat3).

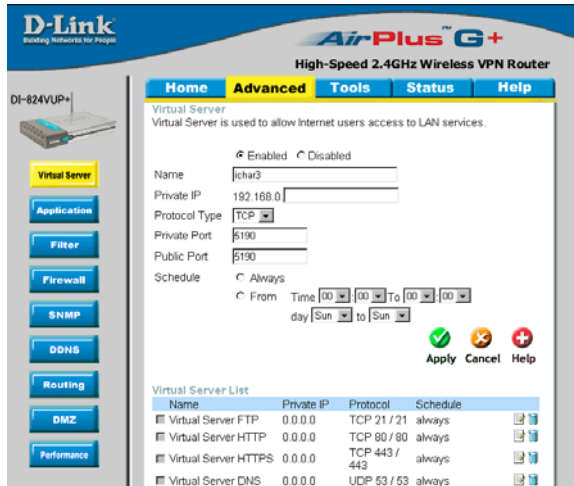
Step 4 Next to Private IP, enter the IP Address of the computer on your local network that you want to allow the incoming service to.

Step 5 Select **TCP** for Protocol Type.

Step 6 Enter **5190** next to Private Port and Public Port.

Step 7 Click **Always** or configure a schedule.

Step 8 Click **Apply** and then **Continue**.



If using Mac OS X Firewall, you may need to temporarily turn off the firewall in the Sharing preference pane on both computers.

To use the Mac OS X Firewall, you must open the same ports as in the router:

Step 1 Choose **Apple menu > System Preferences**.

Step 2 Choose **View > Sharing**.

Step 3 Click the **Firewall** tab.

Step 4 Click **New**.

Step 5 Choose **Other** from the Port Name pop-up menu.

Step 6 In the Port Number, Range or Series field, type in: **5060, 16384-16403**.

Step 7 In the Description field type in: **iChat AV**

Step 8 Click **OK**.

Frequently Asked Questions (continued)

How do I send or receive a file via iChat when the Mac OS X firewall is active? - for Macintosh users - Mac OS X 10.2 and later

The following information is from the online Macintosh AppleCare knowledge base:

“iChat cannot send or receive a file when the Mac OS X firewall is active in its default state. If you have opened the AIM port, you may be able to receive a file but not send them.

In its default state, the Mac OS X firewall blocks file transfers using iChat or America Online AIM software. If either the sender or receiver has turned on the Mac OS X firewall, the transfer may be blocked.

The simplest workaround is to temporarily turn off the firewall in the Sharing preference pane on both computers. This is required for the sender. However, the receiver may keep the firewall on if the AIM port is open. To open the AIM port:

Step 1 Choose Apple menu > System Preferences.

Step 2 Choose View > Sharing.

Step 3 Click the Firewall tab.

Step 4 Click New.

Step 5 Choose AOL IM from the Port Name pop-up menu. The number 5190 should already be filled in for you.

Step 6 Click OK.

If you do not want to turn off the firewall at the sending computer, a different file sharing service may be used instead of iChat. The types of file sharing available in Mac OS X are outlined in technical document 106461, "Mac OS X: File Sharing" in the *AppleCare Knowledge base* online.

Note: If you use a file sharing service when the firewall is turned on, be sure to click the Firewall tab and select the service you have chosen in the "Allow" list. If you do not do this, the firewall will also block the file sharing service. “

Frequently Asked Questions (continued)

What is NAT?

NAT stands for **Network Address Translator**. It is proposed and described in RFC-1631 and is used for solving the IP Address depletion problem. Each NAT box has a table consisting of pairs of local IP Addresses and globally unique addresses, by which the box can “translate” the local IP Addresses to global address and vice versa. Simply put, it is a method of connecting multiple computers to the Internet (or any other IP network) using one IP Address.

D-Link’s broadband routers (ie: DI-824VUP) support NAT. With proper configuration, multiple users can access the Internet using a single account via the NAT device.

For more information on RFC-1631: The IP Network Address Translator (NAT), visit <http://www.faqs.org/rfcs/rfc1631.html>

Contacting Technical Support

You can find the most recent software and user documentation on the D-Link website.

D-Link provides free technical support for customers within the United States for the duration of the warranty period on this product.

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

D-Link Technical Support over the Telephone:

(877) 453-5465

24 hours a day, seven days a week.

D-Link Technical Support over the Internet:

<http://support.dlink.com>

When contacting technical support, you will need the information below. (Please look on the back side of the unit.)

- *Serial number of the unit*
- *Model number or product name*
- *Software type and version number*

Warranty and Registration

Subject to the terms and conditions set forth herein, D-Link Systems, Inc. (“D-Link”) provides this Limited warranty for its product only to the person or entity that originally purchased the product from:

- D-Link or its authorized reseller or distributor and
- 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, addresses with an APO or FPO.

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

3-Year Limited Warranty for the Product(s) is defined as follows:

- Hardware (excluding power supplies and fans) Three (3) Years
- Power Supplies and Fans One (1) Year
- Spare parts and spare kits Ninety (90) days

D-Link’s sole obligation shall be to repair or replace the defective Hardware during the Warranty Period at no charge to the original owner or to refund at D-Link’s sole discretion. Such 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 in its sole discretion 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 from the date of original retail purchase. If a material defect is incapable of correction, or if D-Link determines in its sole discretion that it is not practical to repair or replace the defective Hardware, the 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 (“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 Warranty Period, the magnetic media on which D-Link delivers the Software will be free of physical defects. D-Link’s sole obligation shall be 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 at D-Link’s sole discretion. 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. Software will be warranted for the remainder of the original Warranty Period from the date of original retail purchase. 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 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.

- The original product owner must obtain a Return Material Authorization (“RMA”) number from the Authorized D-Link Service Office and, if requested, provide written proof of purchase of the product (such as a copy of the dated purchase invoice for the product) before the warranty service is provided.
- 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, with shipping charges prepaid. Expedited shipping is available if shipping charges are prepaid by the customer and upon request.

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: This limited warranty provided by D-Link does not cover: Products, if 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; 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. Repair by anyone other than D-Link or an Authorized D-Link Service Office will void this 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 NINETY (90) DAYS. 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 the product owner 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 manufacturers or 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. Contents are subject to change without prior notice. Copyright© 2002 by D-Link Corporation/D-Link Systems, Inc. All rights reserved.

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

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

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

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

The Manufacturer is not responsible for any radio or TV interference caused by unauthorized modifications to this equipment; such modifications could void the user's authority to operate the equipment.

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

IMPORTANT NOTE:

FCC Radiation Exposure Statement:

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. The antenna(s) used for this equipment must be installed to provide a separation distance of at least eight inches (20 cm) from all persons.

This transmitter must not be operated in conjunction with any other antenna.

Register online your D-Link product at <http://support.dlink.com/register/>