D-Link *Air*Plus *G* DI-824VUP

High-Speed Enhanced 2.4 GHz Wireless VPN Router

Manual



Contents

Package Contents	3
Introduction	4
Wireless Basics	6
Getting Started	9
Using the Configuration Menu	11
Installing the Print Server Software	65
Configuring on Windows 98se/Me Platforms	67
Networking Basics	69
Reset to Factory Default Settings	
Reset to Factory Default Settings	
Reset to Factory Default Settings Technical Specifications Frequently Asked Questions	
Reset to Factory Default Settings Technical Specifications Frequently Asked Questions Contacting Technical Support	
Reset to Factory Default Settings Technical Specifications Frequently Asked Questions Contacting Technical Support Warranty	

Package Contents

Contents of Package:

- D-Link AirPlus G DI-824VUP High-Speed Enhanced 2.4GHz Wireless VPN Router
- Power Adapter 5V DC / 2.5A
- Manual on CD
- Quick Installation Guide

D-Link

Note: Using a power supply with a different voltage rating than the one included with the DI-824VUP will cause damage and void the warranty for this product.

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

System Requirements For Configuration:

- Ethernet-Based Cable or DSL Modem
- Computer with Windows, Macintosh, or Linux-based operating system with an installed Ethernet adapter
- Internet Explorer version 6.0 or Netscape Navigator version 6.0 and above, with JavaScript enabled

DI-824VU

Introduction

The D-Link *Air*Plus *G* DI-824VUP Wireless VPN Router is an 802.11g high performance, wireless router with two printer ports, one parallel and one USB. It is an ideal way to extend the reach and number of computers connected to your wireless network.

Unlike most 802.11g routers, the DI-824VUP is capable of data transfer speeds up to 54 Mbps* (compared to the standard 11 Mbps) when used with other D-Link *Air*Plus *G* products such as the DWL-G650 and DWL-G520 Wireless Adapters.

After completing the steps outlined in the *Quick Installation Guide* (included in your package) you will have the ability to share information and resources, as well as share a printer wirelessly on your network.

The DI-824VUP is compatible with most popular operating systems, including Macintosh, Linux and Windows, and can be integrated into a large network. This Manual is designed to help you connect the Router and D-Link *Air*Plus 2.4GHz Wireless Adapters into a network in Infrastructure mode. *Please take a look at the Getting Started section in this manual to see an example of an Infrastructure network using the* DI-824VUP.

^{*}Maximum wireless signal rate based on IEEE Standard 802.11g specifications. Actual data throughput will vary. Network conditions and environmental factors, including volume of network traffic, building materials and construction, and network overhead lower actual data throughput rate.

Connections



Features & Benefits

- Connects multiple computers to an Ethernet Broadband (Cable or DSL) modem to share the Internet connection
- Supports VPN pass-through, providing added security
- Advanced Firewall features for added network security
- DHCP server support enables all networked computers to automatically receive IP addresses
- Wireless connection of up to 54Mbps
- Web-based interface for Management
- Access Control to manage users on the network
- Maximum reliability, throughput and connectivity with automatic data rate switching
- Stronger network security with 256-bit encryption
- Printer port enables connection to a network printer
- WAN and LAN ports auto detect cable types (straight-through or cross-over)
 - UPnP supported



Note: Please refer to the *Resetting the DI-824VUP to the Factory Defualt Settings* section in this manual for instructions on how to use the Reset button.

LEDS

LED stands for Light-Emitting Diode. The **DI-824VUP** has the following LEDs as described below:

LED	LED Activity
Power	A steady light indicates a connection to a power source
WAN	A solid light indicates connection on the WAN port. This LED blinks during data transmission
Status	Flashes once per second to indicate the unit is working properly
СОМ	A steady light indicates a connection to a back-up dial-up modem.
USB	A steady light indicates a connection to a USB printer.
LPT	A steady light indicates a connection to a parallel printer port
WLAN	A blinking light indicates that the wireless segment is ready. This LED blinks during wireless data transmission.
LOCAL NETWORK (Ports 1-4)	A solid light indicates a connection to an Ethernet-enabled computer on ports 1-4. This LED blinks during data transmission.

Wireless Basics

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

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

Wireless Basics

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

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

People use wireless LAN technology for many different purposes:

Mobility - Productivity increases when people have access to data in any location within the operating range of the WLAN. Management decisions based on real-time information can significantly improve worker efficiency.

Low Implementation Costs – WLANs (Wireless Local Area Networks) are easy to set up, manage, change, and relocate. Networks that frequently change, both physically and logically, can benefit from WLANs ease of implementation. WLANs can operate in locations where installation of wiring may be impractical.

Installation Speed and Simplicity - Installing a wireless LAN system can be fast, easy, and can eliminate the need to pull cable through walls and ceilings.

Network Expansion - Wireless technology allows the network to go where wires cannot.

Scalability – Wireless Local Area Networks (WLANs) can be configured in a variety of topologies to meet the needs of specific applications or existing infrastructure. Configurations are easily changed and range from peer-to-peer networks suitable for a small number of users to larger infrastructure networks to accommodate hundreds or thousands of users, depending on the number of wireless devices deployed.

Wireless Basics

The DI-824VUP is compatible with other **D-Link AirPlus G** 802.11g products, which include:

- Enhanced 2.4GHz Wireless Cardbus Adapters used with laptop computers (DWL-G650)
- Enhanced 2.4GHz Wireless PCI cards used with desktop computers (DWL-G520)

Standards-Based Technology

Based on the IEEE **802.11g** standard, the DI-824VUP is interoperable with existing compatible 2.4GHz wireless technology with data transfer speeds of up to 54Mbps (with the D-Link *Air*Plus *G* family of wireless devices,) as well as standard 802.11b technology (the D-Link *Air* family of wireless devices), with speeds of up to 11Mbps.

Installation Considerations

The D-Link *Air*Plus *G* DI-824VUP lets you access your network, using a wireless connection, from virtually anywhere. Keep in mind, however, that the number, thickness, and location of walls, ceilings, or other objects that the wireless signals must pass through may limit the range. Typical ranges vary depending on the types of materials and background RF (radio frequency) noise in your home or business. The key to maximizing wireless range is to follow these basic guidelines:

- Keep the number of walls and ceilings between the DI-824VUP and your receiving device (e.g., the DWL-G650) to a minimum-each wall or ceiling can reduce your D-Link *Air*Plus wireless product's range from 3-90 feet (1-30 meters.) Position your receiving devices so that the number of walls or ceilings is minimized.
- 2. Be aware of the direct line between routers and computers. A wall that is 1.5 feet thick (.5 meters), at a 45-degree angle appears to be almost 3 feet (1 meter) thick. At a 2-degree angle it looks over 42 feet (14 meters) thick! Try to make sure that devices are positioned so that the signal will travel straight through a wall or ceiling for better reception.
- 3. Building Materials make a difference a solid metal door or aluminum studs may have a negative effect on range. Try to position wireless devices and computers with wireless adapters so that the signal passes through drywall or open doorways and not other materials.
- 4. Keep your product away (at least 3-6 feet or 1-2 meters) from electrical devices or appliances that generate RF noise.

Getting Started

With its default settings, the DI-824VUP will connect with other D-Link *Air* or *Air*Plus products, right out of the box.

With a single IP Address from your Broadband Internet Service provider you can share the Internet with all the computers on your local network, without sacrificing speed or security, using D-Link *Air* networking products.

IP ADDRESS

Note: If you are using a DHCP-capable router in your network setup, such as the DI-824VUP, you will not need to assign a static IP Address.

If you need to assign IP Addresses to the computers on the network, please remember that the **IP Address for each computer must be in the same IP Address range as all the computers in the network**, and the Subnet Mask must be exactly the same for all the computers in the network.

For example: If the first computer is assigned an IP Address of 192.168.0.2 with a Subnet Mask of 255.255.255.0, then the second computer can be assigned an IP Address of 192.168.0.3 with a Subnet Mask of 255.255.255.0, etc.

IMPORTANT: If computers or other devices are assigned the same IP Address, one or more of the devices may not function properly on the network.

An **Infrastructure** wireless network contains an Access Point. The **Infrastructure Network** example, shown here, contains the following D-Link network devices:

A wireless Broadband Router -D-Link AirPlus G DI-824VUP A laptop computer with a wireless adapter -D-Link AirPlus G DWL-G650 A desktop computer with a wireless adapter -D-Link AirPlus G DWL-G520 A Cable modem -D-Link DCM-201

Getting Started



Please remember that **D-Link AirPlus** wireless devices are pre-configured to connect together, right out of the box, with their default settings.

For a typical wireless setup at home (as shown above), please do the following:



You will need broadband Internet access (a Cable or DSL subscription line into your home or office).



Consult with your Cable or DSL provider for proper installation of the modem.



Connect the Cable or DSL modem to the DI-824VUP wireless broadband router (See the Quick Installation Guide included with the DI-824VUP.)



If you are connecting a desktop computer to your network, you can install the D-Link *Air*Plus *G* DWL-G520 wireless PCI adapter into an available PCI slot. (See the Quick Installation Guide included with the DWL-G520.)



If you are connecting a laptop computer to your network, install the drivers for the wireless cardbus adapter (e.g., D-Link *Air*Plus *G* DWL-G650) into a laptop computer.(See the Quick Installation Guide included with the DWL-G650.) (See the Quick Installation Guide included with the DWL-650+.)



Connect your printer to the printer port on the DI-824VUP. Please refer to the quick installation guide for loading the print server software.

Whenever you want to configure your network or the DI-824VUP, you can access the Configuration Menu by opening the web-browser and typing in the IP Address of the DI-824VUP. The DI-824VUP default IP Address is shown below:

- Open the web browser
 - Type in the IP Address of the DI-824VUP



Note: if you have changed the default IP Address assigned to the DI-824VUP, make sure to enter the correct IP Address.

The factory default User name is admin and the default **Password** is blank (empty). It is recommended that you change the admin password for security purposes. Please refer to **Tools > Admin** to change the admin password.

Home > Wizard





The Home>Wizard screen will appear. Please refer to the Quick Installation Guide for more information regarding the Setup Wizard.



Clicking **Apply** will save changes made to the page.



Clicking **Cancel** will clear changes made to the page.



Clicking **Help** will bring up helpful information regarding the page.



Clicking **Restart** will restart the router. (Necessary for some changes.)

Restart

Home > Wireless

		High-Speed	Plus 2.4GHz Wirele	G SS VPN Ro
Home	Advanced	Tools	Status	Hel
Wireless Setti These are the w	ngs ireless settings for th	e AP(Access Poinț) portion.	
Network ID(SSI	D) default			
Channel	6 🛩			
WEP	○ Enat	led 💿 Disabled		
WEP Encryption	64 Bit	~		
WE	P Key 1 💿			
	Key 2 🔘			
	Key 3 🔘			
	Key 4 🔘			
802.1X Setting	ß			
	C Enabled	Disabled		
Encryption Key	Length Length 🔘 (64 bits 🔿 128 bits	○ 256 bits	
	Lifetime 5 M	inutes 💌		
RADIUS Server	1 IP			
	Port			
	Shared Sech	et		
				63
			Apply	Cancel H

SSID

default is the default setting. All devices on the network must share the same SSID. If you change the default setting, the SSID may be up to 32 characters long.

- **Channel 6** is the default channel. All devices on the network must share the same channel.
- WEP Click Enabled or Disabled (default).
- WEP Encryption Select the level of encryption desired: 64, 128, or 256-bit.
 - 64-bit Requires 10 digits
 - **128-bit** Requires 26 digits
 - 256-bit Requires 58 digits

Keys 1-4

Input up to 4 WEP keys using Hexadecimal format; select the one you wish to use.

Hexadecimal digits consist of the numbers 0-9 and the letters A-F.



WEP (*Wired Equivalent Privacy*) If you enable encryption on the DI-824VUP, make sure to also enable encryption on all 802.11b and 802.11g wireless clients, or wireless connection will not be established.

Home > Wireless (Continued)

Hom	e Adva	nced	Tools	Status	Hel
Wireless 9 These are t	iettings he wireless setti	ngs for the AP	Access Point)	portion.	
Network ID	(88ID)	detault			
ard Channel		6 🛩			
WEP		CEnabled	Disabled		
WEP Encry	ption	64 Bit 👻			
	WEP Key 1 ③				
	Key 2 〇				
	Key 3 O				
	Key 4 O				
002.1X Se	ttings				
	0	Enabled @D	balled		
Encryption	Key Length Len	ath () 64 bit	s O 128 bits	O 256 bits	
	Life	time S Minute	*		
RADIUS SI	rver1 IP	2010. No. 1	-	1	
	Por	6			
	Sha	red Secret			
			-		

The 802.1x is an authentication method which is designed to 802.1x compliment the existing WEP encryption. During the authentication process, the server verifies the identity of the client attempting to connect to the network. With the proper client account and encryption key, access to the network is granted. Unfamiliar encryption key or clients are denied from accessing the wireless network. This feature will help safe guard a Local Area Network (LAN) from unwanted visitors.

> To take the full advantage of the 802.1x in DI-824VUP, all of the wireless devices on your network must be 802.1x compatible and must have the 802.1x feature enabled to communicate with the router. (Note: Windows 2000 users will find a few downloads to enable 802.1x clients on the Microsoft website.)

Encryption Key Selection for Encryption Key

- 64 bits This will generate a 10 digit Dynamic Key value for encryption.
- 128 bits This will generate a 26 digit Dynamic Key value _ for encryption.
- 256bits This will generate a 58 digit Dynamic Key value for encryption.
- Lifetime Select the period of time before a new Dynamic Key is generated.

RADIUS Server Enter the IP address and port number of the RADIUS server that will be used as the 802.1x authenticator. Enter the secret key that has also been entered into the RADIUS server's configuration.

* Dynamic Keying is a technique for changing the WEP Key used between the supplicant (wireless client) and the access point.

Home > WAN



Choose WAN Type

WAN stands for *Wide Area Network*. In this case WAN represents the mode in which your ISP connects to the Internet. If you are uncertain, please ask your ISP which of the following represents your connection mode to the Internet:

Dynamic IP Address	Obtain an IP address from your ISP automatically (mainly for Cable users).
Static IP Address	Your ISP assigns you a Static IP Address.
PPP over Ethernet	Some ISPs require the use of PPPoE to connect to their services (mainly for DSL users).
Dial-up Network	Dial-up users can select this option to connect to their ISP through an analog dial-up modem if broadband connectivity is unavailable.
Others	
РРТР	For use in Europe only.
Big Pond Cable	For use in Australia only.

Home > WAN > Dynamic IP Address

Home 🗛	Ivanced Tools Status Hel
WAN Settings Please select the appl	priate option to connect to your ISP.
Oynamic IP Addr	ss Choose this option to obtain an IP address automatically from your ISP. (For most Cable modern 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 DS users)
🔿 Dial-up Network	To surf the Internet via PSTN/ISDN.
O Others	PPTP and BigPond Cable.
Dynamic IP Addres	
Host Name	(Optional)
MAC Address	00 - 80 - C8 - C2 - BD - 44
Primary DNS Address	0.0.0.0
Secondary DNS Addre	ss 0.0.0.0
MTU	1500
Auto-reconnect	Enabled O Disabled
Auto-backup	C Enabled Disabled

Most Cable modem users will select this option to obtain an IP Address automatically from their ISP (Internet Service Provider).

Host Name	This is optional, but may be required by some ISPs. The host name is the device name of the Router.
Renew IP Forever	Enable this feature to allow the router to automatically reconnect to the ISP if the connection drops.
MAC Address	The default MAC Address is set to the WAN's physical interface MAC address on the Router.
Clone MAC Address	This feature will copy the MAC address of the Ethernet card from the computer that is logged into the router, and replace the WAN MAC address of the Router with this Ethernet card MAC address. It is not recommended that you change the default MAC address unless required by your ISP.

Home > WAN > Static IP Address

D-Link Building Networks for People		Air Plus G
		High-Speed 2.4GHz Wireless VPN Router
	Home Advar	nced Tools Status Help
JI-624V0P	WAN Settings Please select the appropriate	option to connect to your ISP.
	O Dynamic IP Address	Choose this option to obtain an IP address automatically from your ISP. (For most Cable modem users)
Wizard	Static IP Address	Choose this option to set static IP information provided to you by your ISP.
Wireless	PPPoE	Choose this option if your ISP uses PPPoE. (For most DSL users)
	🔘 Dial-up Network	To surf the Internet via PSTN/ISDN.
WAN	O Others	PPTP and BigPond Cable.
(management)	Static IP Address	
LAN	IP Address	0.0.0.0
DHCP	Subnet Mask	255.255.255.0
	ISP Gateway Address	0.0.0.0
VPN	Primary DNS Address	0.0.0.0
	Secondary DNS Address	0.0.0.0
	MTU	1500
	Auto-backup	C Enabled O Disabled

If you use a Static IP Address, you will input information here that your ISP has provided to you.

WAN IP Address	Input the IP Address provided by your ISP.
WAN Subnet Mask	Input the Subnet Mask provided by your ISP.
WAN Gateway	Input the Gateway address provided by your ISP.
Primary DNS	Input the primary DNS address provided by your ISP.
Secondary DNS	(Optional) Input the Secondary DNS address provided by your ISP.
MTU	<i>Maximum Transmission Unit</i> ; default is 1500; you may need to change the MTU to conform to your ISP.
Auto-backup	Enabling this feature will connect your router to the Internet using a dial-up service if your broadband connection becomes unavailable. A subscription to a dial-up service is required for the auto-backup to work.

Home > WAN > PPPoE

Most DSL users will select this option to obtain an IP address automatically from their ISP through the use of PPPoE.

Home Adva	anced	Tools	Status	Help
WAN Settings Please select the appropria	de option to co	innect to your IS	P.	
O Dynamic IP Address	Choose	e this option to o	btain an IP address a 4 Cable modern user	utomatically
Static IP Address	Choose	this option to s	et static IP information	n provided to
PPPoE	Choose	this option if yo	ur ISP uses PPPoE	For most DSL
O Dial-up Network	To surf	the Internet via I	STNISDN.	
O Others	РРТР а	nd BigPond Cal	ble.	
PPP ever Ethernet				
	⊙ Dyn	amic PPPoE C	Static PPPoE	
User Name				
Password				
Retype Password				
Service Name			(Optional)	
IP Address	0.0.0.0			
Primary DNS Address	0000			
Secondary DNS Address	0.0 7 7			
Maximum Idle Time	0	Minutes		
MTU	1492	1		
Auto-reconnect	() Ena	bled O Disabl	ed	
			0.041	

User Name	Your PPPoE username provided by your ISP.
Password	Your PPPoE password provided by your ISP.
Service Name	(Optional) Check with your ISP for more information if they require the use of service name.
IP Address	(Optional) Enter in the IP Address if you are assigned a static PPPoE address.
Primary DNS	You will get the DNS IP automatically from your ISP but you may enter a specific DNS address that you want to use instead.
Secondary DNS	(Optional) Input the secondary DNS address.
Maximum Idle Time	Enter a maximum idle time during which Internet connection is maintained during inactivity. To disable this feature, enable <i>Auto-reconnect</i> .
MTU	<i>Maximum Transmission Unit</i> ; default is 1492; you may need to change the MTU to conform to your ISP.
Auto-reconnect	If enabled, the Broadband Router will automatically connect to your ISP after your system is restarted or if the connection is dropped.
Auto-backup	Enabling this feature will connect your router to the Internet using a dial-up service if your broadband connection becomes unavailable. A subscription to a dial-up service is required for the auto-backup to work.

Home > WAN > Dial-up Network

Most Dial-up users will select this option to connect to their ISP through an analog dial-up modem. This feature can be used as a back-up when your broadband connectivity is unavailable.

	н	gh-Speed 2	Plus (2.4GHz Wireles	📑 is VPN Ro
Home	Advanced	Tools	Status	Hel
WAN Settings Please select the ap	ppropriate option to c	innect to your IS	P.	
 Dynamic IP Ad 	idress Choos from yo	e this option to o ur ISP. (For mo	obtain an IP address st Cable modem use	automatically rs)
Static IP Addre	ess Choos you by	e this option to s our ISP.	set static IP informatio	on provided to
O PPPoE	Choos users)	e this option if y	our ISP uses PPPoE.	(For most DS
 Dial-up Netwo 	rk To sur	the Internet via	PSTN/ISDN.	
 Others 	PPTP :	nd BigPond Ca	ble.	
Dial-up Network				
Dial-up Telephone				
Dial-up Account				
Dial-up Password	•••••			
Retype Password	•••••			
Primary DNS	0.0.0.0			
Secondary DNS	0.0.0.0			
Assigned IP Addres	ss 0.0.0.0	(0	ptional)	
Extra Settings				
Maximum Idle Time	9 0	Minutes		
Baud Rate	57600	bps		
Disable auto-dial	OEn	ibled 💿 Disab	led	
Auto-reconnect	• En	bled ODisab	led	

Dial-up Telephone Telephone number to connect to your ISP **Dial-up Account** Username provided by your ISP **Dial-up Password** Password provided by your ISP If the settings are configured as "0.0.0.0," they will be Primary DNS/ automatically assigned upon connection. Seconday DNS Assigned (Optional) Enter in the IP Address if you are assigned a static PPPoF address **IP Address** This setting is used to optimize the communication Extra Settings quality between the ISP and your analog dial-up modem. (Initialization string) - optional. Maximum Idle Time Enter a maximum idle time during which Internet connection is maintained during inactivity. To disable this feature. enable Auto-reconnect. **Baud Rate** The communication speed between the DI-824VUP and your modem. Auto-reconnect If enabled, the Broadband Router will automatically connect to your ISP after your system is restarted or if the connection is dropped.

Home > WAN > Others > PPTP



Point-to-Point Tunneling Protocol (PPTP) is a WAN connection used in Europe.

My IP Address	Enter the IP Address.
My Subnet Mask	Enter the Subnet Mask.
Server IP Address	Enter the Server IP Address.
PPTP Account	Enter the PPTP account name.
PPTP Password	Enter the PPTP password.
Connection ID	(Optional) Enter the connection ID if required by your ISP.
Maximum Idle Time	Enter a maximum idle time during which Internet connection is maintained during inactivity. To disable this feature, enable <i>Auto-reconnect</i> .
Auto-reconnect	If enabled, the Broadband Router will automatically connect to your ISP after your system is restarted or if the connection is dropped.
Auto-backup	Enabling this feature will connect your router to the Internet using a dial-up service if your broadband connection becomes unavailable. A subscription to a dial-up service is required for the auto-backup to work.

Home > WAN > Others > BigPond Cable

Link			Air	Plus G	
			High-Speed 2	.4GHz Wireless VPN Ro	oute
	Home	Advance	d Tools	Status Hel	р
	WAN Settings Please select the	e appropriate optic	on to connect to your ISI	5 ≦%	
	🔿 Dynamic IP	Address 1	Choose this option to o from your ISP. (For mos	btain an IP address automatically t Cable modem users)	
zard	O Static IP Ad	dress	Choose this option to s you by your ISP.	et static IP information provided to	
55	O PPPoE		Choose this option if yo users)	ur ISP uses PPPoE. (For most DS	L
	🔘 Dial-up Net	work	To surf the Internet via F	STN/ISDN.	
	 Others 		PPTP and BigPond Cal	ole.	
	O PPTP		(for Europe use only)		
	💿 BigPond	i Cable	(for Australia use only)		
	Dynamic IP Ac	Idress for BigP	ond		
	User Name	[
	Password		•••••		
	Retype Passwor	d	•••••		
	Login Server IP	[(Optional)	
	Auto-reconnect		Enabled ODisable	ed	
	Auto-backup		O Enabled O Disable	he	

Dynamic IP Address for BigPond is a WAN connection used in Australia.

User Name	Enter in the user name for the BigPond account.
Password	Enter the password for the BigPond account.
Login Server IP	(Optional) Enter the Login Server IP if required.
Auto-reconnect	If enabled, the Broadband Router will automatically connect to your ISP after your system is restarted or if the connection is dropped.
Auto-backup	Enabling this feature will connect your router to the Internet using a dial-up service if your broadband connection becomes unavailable. A subscription to a dial-up service is required for the auto-backup to work.

Home > LAN

D-Link Building Networks for People		н	Air igh-Speed 2	Plus .4GHz Wirele	G ess VPN	Route
824VUP	Home	Advanced	Tools	Status	Н	elp
	LAN Settings The IP address of	of the DI-824VUP.				
	IP Address	192.16	8.0.1			
Wizard	Subnet Mask	255.25	5.255.0			
	Domain Name]	
Wireless				0	8	0
WAN				Apply	Cancel	Help
LAN						
DHCP						
VPN						

LAN is short for Local Area Network. This is considered your internal network. These are the IP settings of the LAN interface for the DI-824VUP. These settings may be referred to as Private settings. You may change the LAN IP address if needed. The LAN IP address is private to your internal network and cannot be seen on the Internet.

IP Address	The IP address of the LAN interface. The default IP address is: 192.168.0.1 .
Subnet Mask	The subnet mask of the LAN interface. The default subnet mask is 255.255.255.0 .
Domain Name	(Optional) The name of your local domain.

Home > DHCP

r People			AirP	lus (G
-		Hi	gh-Speed 2.4GH	tz Wireles	s VPN Rout
	Home	Advanced	Tools S	Status	Help
ſ	DHCP Server The DI-824VUP of	can be setup as a DHCP	Server to distribute IP	addresses to	the LAN network.
	DHCP Server	🖲 Ens	abled 🔿 Disabled		
	Starting IP Addre	ess 192.16	8.0.100		
	Ending IP Addre	ss 192.16	8.0.199		
	Lease Time	1 WEEK	< 💌		
	IP Address 19 MAC Address DHCP Client	32.168.0.	Clone)	
				🕥 Apply (沒 🔂 Cancel Help
	Static DHCP CI	lients List	Mac adda		
	rvame	IF Address	MAC Addre	199	
	Dynamic DHCP	Clients List	MAC Address	-	units of Time a
	mustiname	102.160.0.110	MAG Address	an T	ue Sep 30

DHCP stands for *Dynamic Host Control Protocol*. The DI-824VUP has a built-in DHCP server. The DHCP Server will automatically assign an IP address to the computers on the LAN/private network. Be sure to set your computers to be DHCP clients by setting their TCP/IP settings to "Obtain an IP Address Automatically." When you turn your computers on, they will automatically load the proper TCP/IP settings provided by the DI-824VUP. The DHCP Server will automatically allocate an unused IP address from the IP address pool to the requesting computer. You must specify the starting and ending address of the IP address pool.

DHCP Server Enable or disable the DHCP service.

Starting IP Address The starting IP address for the DHCP server's IP assignment.

- Ending IP Address The ending IP address for the DHCP server's IP assignment.
- **Lease Time** The length of time for the DHCP lease.
- **Static DHCP** Used to allow the DHCP server to assign the same IP adress to a specific MAC address. Enter the name, IP address, and MAC address into the fields. Select which DHCP client to clone.
- DHCP Clients List Lists the DHCP clients connected to the DI-824VUP. Click **Refresh** to update the list. The table will show the Host Name, IP Address, and MAC Address of the DHCP client computer.

Using the Configuration Menu Home > VPN Settings

VPN Settings are settings that are used to create virtual private tunnels to remote VPN gateways. The tunnel technology supports data confidentiality, data origin, authentication, and data integrity of network information by utilizing encapsulation protocols, encryption algorithms, and hashing algorithms.

	Air High-Speed 2	
Advanced	d Tools	Status He
js		
ltem		Setting
	🗌 Enable	
adcast	🔲 Enable	
oftunnels	0	
Tunnel Name		Method
		IKE 🖌 More
		IKE 🖌 More
		IKE 🖌 More
	1	IKE 🖌 More
	1	IKE V More
	Advanced F Item adcast Tunnel Name 	

VPN	Click Enable to enable VPN tunnels. When you are not using the VPN feature, it is best to keep VPN disabled.
NetBIOS broadcast	Enable this to allow NetBIOS braodcast over the VPN tunnels.
Max. number of tunnels	Select the maximum number of allowable tunnels.
Tunnel Name	Create a name for the tunnel.
Method	IPSec VPN supports two kinds of key-obtained methods: manual key and automatic key exchange. Manual key approach indicates that the two endpoint VPN gateways require setting up authentication and encryption key by the Administrator manually. However, IKE approach will perform automatic Internet key exchange. Admins of both endpoint gateways will only need to set the same pre-shared key.
More	For more in depth configuration to adjust manual key or IKE method settings, click More.

Home > VPN Settings > Tunnel > Method >IKE

D -Link	AirPlus				
Building Networks for People		High-Speed 2.4	4GHz Wireless VP	N Router	
	Home Ad	vanced Tools	Status	Help	
DI-824VUP	VPN Settings - Tun	nnel 1	Setting		
Wizard Wiretess WAN LAN DHCP VPN	Tunnel Name Aggressive Mode Local Subnet Local Netmask Remote Subnet Remote Netmask Remote Gateway Preshare Key IKE Proposal index IPSec Proposal index	Enable 0.0.0 0.0.0 0.0.0 0.0.0 0.0.0 Select IKE F Select IPSe	Setting Proposal		
Tunnel Name	Current tunne	el name.	9 9 8	0	
Aggressive Mode	Enabling this mode will accelerate establishing tunnel, b the device will have less security.				
Local Subnet	The subnet of the VPN gateway's local network. It can be host, a partial subnet or a whole subnet.				
Local Netmask	Enter the Subnet Mask for the Local Network of the rout				
Remote Subnet	The subnet o can be a hos	of the remote VF t, a partial subn	N gateway's et, or a who	s local ne le subne	
Remote Netmask	The Subnet Mask of the remote VPN gateway's Local Network.				
Remote Gateway	The WAN IP address of remote VPN gateway.				
Preshared Key	The first key th gateways for r key must be th	hat supports IKE negotiating furthe he same for both	mechanism er security ke endpoint ga	of both V ys. The p teways.	
IKE Proposal index	Click the butto and select fro	on to setup a set om the set of IK	of frequent- E proposals	used IKE for the tu	
IPSec Proposal index	Click the bu proposals and tunnel.	tton to setup a d select from the	a set of fre e set of IPSe	quent-us ec propos	

Home > VPN Settings > Tunnel > Method > IKE > Select IKE Proposal

VPR Settings Dynamic VPN Tunnel Set IKE Proposal Rem Setting INE Proposal index Encry- ID Proposal Name DH Group ID Proposal Name DH Group I Group 1 with algorithm Life Time Life Time Life Time Unit I Group 1 with algorithm Sec. with algorithm	Home	Advance	d Tools	s Sta	tus	Help
Item Setting IFE Proposal Name Emory - ID Proposal Name ID Proposal Name III Group 1 willion III Group 1 willion IIII Group 1 willion IIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIII	VPN Settings	Dynamic VPN	Tunnel - Set IKE	Proposal		
IFE Proposal index Empty- Remove ID Proposal Name DH Oroup Encrypt algorithm Auth algorithm Life Time Unit 1 Oroup 1 3065 × SHA1 × 0 Sec. × 2 Oroup 1 3065 × SHA1 × 0 Sec. × 3 Oroup 1 3065 × SHA1 × 0 Sec. × 4 Oroup 1 3065 × SHA1 × 0 Sec. × 6 Oroup 1 3065 × SHA1 × 0 Sec. × 0 Oroup 1 3065 × SHA1 × 0 Sec. × 9 Oroup 1 3065 × SHA1 × 0 Sec. ×		tem		Settin	g	
Concept of Sector	IKE Proposal inc	iex	- Empty -			
D Proposal Name DH Group 1 Encrypt algorithm Life Time Life Time Unit 1 Group 1 3065 v 9444 v 0 Sec. v 2 Group 1 v 3065 v 9444 v 0 Sec. v 3 Group 1 v 3065 v 9441 v 0 Sec. v 4 Group 1 v 3065 v 9441 v 0 Sec. v 5 Group 1 v 3065 v 9441 v 0 Sec. v 6 Group 1 v 3065 v 9441 v 0 Sec. v 7 Group 1 v 3065 v 9441 v 0 Sec. v 8 Group 1 v 3065 v 9441 v 0 Sec. v 9 Group 1 v 3065 v 9441 v 0 Sec. v				Renove		
D Proposal Name DH Group Encropt algorithm Auth algorithm Life Time Life Time <thlife th="" time<=""></thlife>			<u> </u>	Henere		
1 Oroup 1 3665 vr SHA1 vr 0 Sec. vr 2 Oroup 1 vr XC5 vr SHA1 vr 0 Sec. vr 3 Oroup 1 vr XC5 vr SHA1 vr 0 Sec. vr 4 Oroup 1 vr XC5 vr SHA1 vr 0 Sec. vr 5 Oroup 1 vr SEE vr SHA1 vr 0 Sec. vr 6 Oroup 1 vr SEE vr SHA1 vr 0 Sec. vr 6 Oroup 1 vr SEE vr SHA1 vr 0 Sec. vr 9 Oroup 1 vr SEE vr SHA1 vr 0 Sec. vr 9 Oroup 1 vr SEE vr SHA1 vr 0 Sec. vr	55 ID Proposal Na	me DH Group	Encrypt algorithm	Auth algorithm	Life Time	Life Time Unit
2 Group 1 w 3065 w SPA1 w 0 Sec. w 3 Group 1 w 3055 w SPA1 w 0 Sec. w 4 Group 1 w 3055 w SPA1 w 0 Sec. w 5 Group 1 w 3055 w SPA1 w 0 Sec. w 6 Group 1 w 3055 w SPA1 w 0 Sec. w 7 Group 1 w 3055 w SPA1 w 0 Sec. w 8 Group 1 w 3055 w SPA1 w 0 Sec. w 9 Group 1 w 3055 w SPA1 w 0 Sec. w	1	Group 1 💌	30ES 💌	SHA1 💙	0	Sec. 💌
3 Group 1 w 20ES w SHA1 w 0 Sac. w 4 Group 1 w 30ES w SHA1 w 0 Sac. w 5 Group 1 w 30ES w SHA1 w 0 Sac. w 6 Group 1 w 30ES w SHA1 w 0 Sac. w 7 Group 1 w 30ES w SHA1 w 0 Sac. w 8 Group 1 w 30ES w SHA1 w 0 Sac. w 9 Group 1 w 30ES w SHA1 w 0 Sac. w	2	Group 1 👻	30ES 💌	SHA1 😪	0	Sec. 💌
4 Oroup 1 w 2065 v SHA1 w 0 Sec. w 5 Oroup 1 w 2065 v SHA1 w 0 Sec. w 6 Oroup 1 w 2065 v SHA1 w 0 Sec. w 7 Oroup 1 w 2065 v SHA1 w 0 Sec. w 8 Oroup 1 w 2065 v SHA1 w 0 Sec. w 9 Oroup 1 w 2065 v SHA1 w 0 Sec. w	3	Group 1 💌	3DES 💌	SHA1 💌	0	Sec. 💌
5 Group 1 v 3065 v 5HA1 v 0 Sec. v 6 Group 1 v 3065 v 5HA1 v 0 Sec. v 7 Group 1 v 3065 v 5HA1 v 0 Sec. v 0 Group 1 v 3065 v 5HA1 v 0 Sec. v 0 Group 1 v 3065 v SHA1 v 0 Sec. v 9 Group 1 v 3065 v SHA1 v 0 Sec. v	4	Oroup 1 💌	3DES 💌	SHA1 🛩	0	Sec. 💙
6 Group 1 v S0ES v SH41 v 0 Sec. v 7 Group 1 v S0ES v SH41 v 0 Sec. v 8 Group 1 v S0ES v SH41 v 0 Sec. v 9 Group 1 v S0ES v SH41 v 0 Sec. v	5	Oroup 1 😽	3DES 🛩	SHA1 😽	0	Sec. 💌
7 Oroup 1 v 3005 v SHA1 v 0 Sec. v 8 Oroup 1 v 3005 v SHA1 v 0 Sec. v 9 Oroup 1 v 3005 v SHA1 v 0 Sec. v	6	Group 1 💌	30ES 💌	SHA1 🛩	0	Sec. 💌
8 Group 1 v 3055 v SHA1 v 0 Sec. v 9 Group 1 v 3055 v SHA1 v 0 Sec. v	7	Group 1 💌	30ES 💌	SHA1 🛩	0	Sec. 💌
9 Group 1 🖌 30ES 🖌 SHA1 🖌 0 Sec. 🗸	8	Group 1 💌	30ES 💌	SHA1 ¥	0	Sec. 💌
	9	Group 1 💌	3DES 💌	SHA1 💌	0	Sec. 👻
10 Oroup 1 🛩 3065 🛩 SHA1 🛩 0 Sec. 🛩	10	Oroup 1 👻	30ES 💌	SHA1 🛩	0	Sec. 👻
		Proposal ID -	select one 💌	Add to Proposa	lindex	

IKE Proposal index	A list of selected proposal indexes from the IKE proposal pool
	listed below.

Proposal Name This is the name used to classify the IKE proposal.

DH Group There are three groups that can be selected: group 1 (MODP768), group 2 (MODP1024), and group 5 (MODP1536).

Encrypt algorithm There are two algorithms that can be selected: 3DES and DES.

Auth algorithm There are two algorithms that can be selected: SHA1 and MD5.

Home > VPN Settings > Tunnel > Method > IKE > Select IKE Proposal Continued...

VPN Settings	Advance Dynamic VPN	ad Tool	s Sta	tus	Hel
-	Rem		Setti	ng	
IKE Proposal in	dex	- Empty -			
			Renove		
ID Proposal Na	me DH Group	Encrypt algorithm	Auth algorithm	Life Tim	e Life Time I
1	Group 1 👻	30ES 💌	SHA1 🖤	0	Sec.
2	Group 1 👻	30ES 💌	SHA1 👻	0	Sec.
3	Group 1 👻	3DES 💌	SHA1 ¥	0	Sec.
4	Group 1 👻	3DES 💌	SHA1 🛩	0	Sec.
5	Oroup 1 👻	30ES 🛩	SHA1 😽	0	Sec.
6	Group 1 💌	30ES 💙	SHA1 💌	0	Sec.
7	Group 1 💌	3065 💌	SHA1 💌	0	Sec. 💌
8	Group 1 💌	30ES 💌	SHA1 💌	0	Sec. N
9	Group 1 👻	3DES 💌	SHA1 👻	0	Sec.
10	Oroup 1 👻	30ES 👻	SHA1 👻	0	Sec. Y
	Proposal ID -	- select one 💌 [Add to Proposi	al index	

Life Time	Enter in the life time value.
Life Time Unit	There are two units that can be selected: second and KB.
Proposal ID	The identifier of IKE proposal can be chosen for adding the corresponding proposal to the dedicated tunnel.
Add to	Click it to add the chosen proposal indicated by proposal ID to IKE Proposal index list.

Home > VPN Settings > Tunnel > Method > IKE > Select IPSEC Proposal

Ho	me 🛕	dvance	ed Tool:	s Sta	tus	Help
VPN Se	ttings - Dyn	amic VPN	Tunnel - Set IKE	Proposal		
	Rem			Setti	la la	
IKE Prop	osal index		- Empty -			
				Renove		
ID Prop	osal Name 1	DH Group	Encrypt algorithm	Auth algorithm	Life Time	Life Time Un
1		Group 1 💌	3065 💌	SHA1 💌	0	Sec. 💌
2		Group 1 👻	SDES 🛩	SHA1 🛩	0	Sec. 🛩
3		Group 1 🛩	DES 🛩	SHA1 💌	0	Sec. 🤟
4		Group 1 💌	3065 💌	SHA1 💌	0	Sec. 💌
5		Group 1 💌	3DES 💌	SHA1 💌	0	Sec. 💌
6		Group 1 💌	30ES 💌	SHA1 💌	0	Sec. 💌
7		Group 1 💌	30ES 💌	SHA1 💌	0	Sec. M
8		Group 1 💌	30ES 💌	SHA1 💌	0	Sec. 💌
9		Group 1 👻	30ES 💌	SHA1 💌	0	Sec. 💌
10		Group 1 💌	30ES 🛩	SHA1 💌	0	Sec. 💌
	Pr	roposal ID -	- select one 👻	Add to Proposi	l index	

IPSec Proposal index	A list of selected proposal indexes from the IPSec proposal pool listed below.
Proposal Name	This is the name used to classify the IPSec Proposal
DH Group	There are three groups that can be selected: group 1 (MODP768), group 2 (MODP1024), and group 5 (MODP1536).
Encap protocol	There are two protocols that can be selected: ESP and AH.
Encrypt algorithm	There are two algorithms that can be selected: 3DES and DES.
Auth algorithm	There are three algorithms that can be selected: SHA1, MD5, and None.

Home > VPN Settings > Tunnel > Method > IKE > Select IPSEC Proposal Continued...

VPR Settings Dynamic VPR Tunnel Setting Rem Setting RE Proposal Index Encryst algorithm Aufin algorithm D Proposal Name DH Group Encryst algorithm D Proposal Name DH Group Encryst algorithm 1 Group 1 w 3665 w SHA1 w 0 2 Group 1 w 3665 w SHA1 w 0 3 Group 1 w 3665 w SHA1 w 0 4 Group 1 w 3665 w SHA1 w 0 5 Group 1 w 3665 w SHA1 w 0 6 Group 1 w 3665 w SHA1 w 0 6 Group 1 w 3665 w SHA1 w 0 6 Group 1 w 3665 w SHA1 w 0 9 Group 1 w 3665 w SHA1 w 0 9 Group 1 w 3665 w SHA1 w 0 9 Group 1 w 3665 w SHA1 w 0 9 Group 1 w 3665 w SHA1 w 0 9 Group 1 w 3665 w SHA1 w 0 9 Group 1 w 3665 w SHA1 w 0 9 Group 1 w 3665 w		Home	Advanc	ed Tools	s Sta	tus	Help
Rem Setting B/E Proposal Index Empty- Remove D Proposal Name Encrypt algorithm Auth algorithm Life Time Unit 1 Group 1 3065 × SHA1 × 0 Soc × 2 Group 1 3065 × SHA1 × 0 Soc × 3 Group 1 3065 × SHA1 × 0 Soc × 4 Group 1 3065 × SHA1 × 0 Soc × 5 Group 1 3065 × SHA1 × 0 Soc × 6 Group 1 3065 × SHA1 × 0 Soc × 6 Group 1 3065 × SHA1 × 0 Soc × 7 Group 1 3065 × SHA1 × 0 Soc × 9 Group 1 × 3065 × SHA1 × 0 Soc × 9 Group 1 × 3065 × SHA1 × 0 Soc × 10 Group 1 × 3065 × SHA1 × 0 Soc × 9	-	VPN Settings Dy	namic VPN	Tunnel - Set IKE	Proposal		
Inter Proposal Name DH Group Encrypt Algorithm Auth algorithm Life Time Unit 1 Group 1 w 565 w SHAI w 0 Soc w 2 Group 1 w 3655 w SHAI w 0 Soc w 3 Group 1 w 3655 w SHAI w 0 Soc w 4 Group 1 w 3655 w SHAI w 0 Soc w 5 Group 1 w 3655 w SHAI w 0 Soc w 6 Group 1 w 3655 w SHAI w 0 Soc w 6 Group 1 w 3655 w SHAI w 0 Soc w 0 Group 1 w 3655 w SHAI w 0 Soc w 10 Group 1 w 3655 w SHAI w 0 Soc w 10 Group 1 w 3655 w SHAI w 0 Soc w 10 Group 1 w 3655 w SHAI w 0 Soc w 10 Group 1 w 3655 w SHAI w 0 Soc w		Iter	n	-	Settin	la 🛛	
Remove D Proposal Name DH Group Encrypt algorithm Auth algorithm Life Time Unit 1 Oroup 1 3065 v SHAI v 0 Soc v 2 Oroup 1 v 3065 v SHAI v 0 Soc v 3 Oroup 1 v 3065 v SHAI v 0 Soc v 4 Oroup 1 v 3065 v SHAI v 0 Soc v 5 Oroup 1 v 3065 v SHAI v 0 Soc v 6 Oroup 1 v 3065 v SHAI v 0 Soc v 7 Oroup 1 v 3065 v SHAI v 0 Soc v 9 Oroup 1 v 3065 v SHAI v 0 Soc v 9 Oroup 1 v 3065 v SHAI v 0 Soc v 9 Oroup 1 v 3065 v SHAI v 0 Soc v 9 Oroup 1 v 3065 v SHAI v 0 Soc v 10 Oroup 1 v 3065 v SHAI v		ike Proposal index		- Empty -			
D Proposal Name DH Group Encryst algorithm Aufh algorithm Life Time Life Time Unit 1 Group 1 w 3065 w SHA1 w 0 Soc w 2 Group 1 w 3065 w SHA1 w 0 Soc w 3 Group 1 w 3065 w SHA1 w 0 Soc w 4 Group 1 w 3065 w SHA1 w 0 Soc w 5 Group 1 w 3065 w SHA1 w 0 Soc w 6 Group 1 w 3065 w SHA1 w 0 Soc w 7 Group 1 w 3065 w SHA1 w 0 Soc w 0 Group 1 w 3055 w SHA1 w 0 Soc w 0 Group 1 w 3055 w SHA1 w 0 Soc w 9 Droup 1 w 3055 w SHA1 w 0 Soc w 10 Group 1 w 3055 w SHA1 w 0 Soc w 10 Group 1 w 3055 w SHA1 w 0 <td< td=""><td></td><td></td><td></td><td></td><td>Remove</td><td></td><td></td></td<>					Remove		
D Proposal Name DH Group Encrypt algorithm, Auth algorithm Life Time Unit 1 Oroup 1 3065 v SHA1 v 0 Soc v 2 Oroup 1 v 3065 v SHA1 v 0 Soc v 3 Oroup 1 v 3065 v SHA1 v 0 Soc v 4 Oroup 1 v 3065 v SHA1 v 0 Soc v 5 Oroup 1 v 3065 v SHA1 v 0 Soc v 6 Oroup 1 v 3065 v SHA1 v 0 Soc v 6 Oroup 1 v 3065 v SHA1 v 0 Soc v 7 Oroup 1 v 3065 v SHA1 v 0 Soc v 8 Oroup 1 v 3065 v SHA1 v 0 Soc v 10 Oroup 1 v 3065 v SHA1 v 0 Soc v 10 Oroup 1 v 3065 v SHA1 v 0 Soc v 10 Oroup 1 v 3065 v SHA1 v 0 Soc v <							
1 Group 1 XEEs SHAI 0 Sec. v 2 Group 1 XEEs SHAI 0 Sec. v 3 Group 1 XEEs SHAI 0 Sec. v 4 Group 1 XEEs SHAI 0 Sec. v 5 Group 1 XEEs SHAI 0 Sec. v 6 Group 1 XEEs SHAI 0 Sec. v 7 Group 1 XEEs SHAI 0 Sec. v 8 Group 1 XEEs SHAI 0 Sec. v 9 Group 1 XEES SHAI 0 Sec. v 9 Group 1 XEES SHAI 0 Sec. v 9 Group 1 XEES SHAI 0 Sec. v 10 Group 1 XEES SHAI 0 Sec. v 10 <t< td=""><td></td><td>ID Proposal Name</td><td>DH Group</td><td>Encrypt algorithm</td><td>Auth algorithm</td><td>Life Time</td><td>Life Time Uni</td></t<>		ID Proposal Name	DH Group	Encrypt algorithm	Auth algorithm	Life Time	Life Time Uni
2 Droup 1 v 3055 v SHA1 v 0 Soc. v 3 Oroup 1 v 3055 v SHA1 v 0 Soc. v 4 Oroup 1 v 3055 v SHA1 v 0 Soc. v 5 Oroup 1 v 3055 v SHA1 v 0 Soc. v 6 Oroup 1 v 3055 v SHA1 v 0 Soc. v 7 Oroup 1 v 3055 v SHA1 v 0 Soc. v 8 Oroup 1 v 3055 v SHA1 v 0 Soc. v 9 Oroup 1 v 3055 v SHA1 v 0 Soc. v 9 Oroup 1 v 3055 v SHA1 v 0 Soc. v 9 Oroup 1 v 3055 v SHA1 v 0 Soc. v 10 Oroup 1 v 3055 v SHA1 v 0 Soc. v 9 Oroup 1 v 3055 v SHA1 v 0 Soc. v 10 Oroup 1 v 3055 v SHA1 v 0 Soc. v		1	Group 1 🛩	3DES 💌	SHA1 💌	0	Sec. 💌
3 Oroup 1 3055 SHA1 0 Sec. 4 4 Oroup 1 3055 SHA1 0 Sec. 4 5 Oroup 1 3055 SHA1 0 Sec. 4 6 Oroup 1 3055 SHA1 0 Sec. 4 7 Oroup 1 2055 SHA1 0 Sec. 4 8 Oroup 1 2055 SHA1 0 Sec. 4 9 Oroup 1 3055 SHA1 0 Sec. 4 9 Oroup 1 3055 SHA1 0 Sec. 4 10 Oroup 1 3055 SHA1 0 Sec. 4 9 Oroup 1 3055 SHA1 0 Sec. 4 10 Oroup 1 3055 SHA1 0 Sec. 4		2	Group 1 💌	3065 💌	SHA1 💌	0	Sec. 💌
4 Oroup 1 v 265 v SHA1 v 0 Sec. v 5 Oroup 1 v 265 v SHA1 v 0 Sec. v 6 Oroup 1 v 265 v SHA1 v 0 Sec. v 7 Oroup 1 v 265 v SHA1 v 0 Sec. v 8 Oroup 1 v 265 v SHA1 v 0 Sec. v 9 Oroup 1 v 265 v SHA1 v 0 Sec. v 9 Oroup 1 v 265 v SHA1 v 0 Sec. v 10 Oroup 1 v 265 v SHA1 v 0 Sec. v 10 Oroup 1 v 265 v SHA1 v 0 Sec. v 10 Oroup 1 v 265 v SHA1 v 0 Sec. v	11	3	Group 1 💙	3DES 💙	SHA1 💌	0	Sec. 💌
5 Group 1 v 2025 v SHA1 v 0 Sec. v 6 Group 1 v 2025 v SHA1 v 0 Sec. v 7 Group 1 v 2025 v SHA1 v 0 Sec. v 0 Group 1 v 2025 v SHA1 v 0 Sec. v 0 Group 1 v 2025 v SHA1 v 0 Sec. v 10 Group 1 v 2025 v SHA1 v 0 Sec. v 10 Group 1 v 2025 v SHA1 v 0 Sec. v Proposal (D seled ore - v Ad019 Proposal Index V		4	Group 1 👻	3DES 💌	SHA1 💌	0	Sec. 💌
6 Oroup 1 3055 v SHA1 w 0 Sec. w 7 Oroup 1 3055 v SHA1 w 0 Sec. w 8 Oroup 1 3055 v SHA1 w 0 Sec. w 9 Oroup 1 v 3055 v SHA1 w 0 Sec. w 10 Oroup 1 v 3055 v SHA1 w 0 Sec. w Proposal (0 Sec. v SHA1 w 0 Sec. w		5	Group 1 👻	3DES 🛩	SHA1 🛩	0	Sec. 💌
7 Oroup1 v 30ES v \$RIA1 v 0 \$sec. v 8 Oroup1 v 30ES v \$RIA1 v 0 \$sec. v 9 Oroup1 v 30ES v \$RIA1 v 0 \$sec. v 10 Oroup1 v 30ES v \$SHA1 v 0 \$sec. v 9 Oroup1 v 30ES v \$SHA1 v 0 \$sec. v 10 Oroup1 v 30ES v \$SHA1 v 0 \$sec. v Proposal (D - select one - v Add10 Proposal index \$sec. v		6	Group 1 🛩	JDES 🛩	SHA1 🛩	0	Sec. 🛩
8 Oroup 1 3055 \$141 0 Sec. 9 9 Oroup 1 3055 \$141 0 Sec. 9 10 Oroup 1 3055 \$141 0 Sec. 9 10 Oroup 1 3055 \$141 0 Sec. 9 Proposal ID -select one v A0010 Proposal Index 10		7	Group 1 👻	DES 👻	SHA1 💌	0	Sec. 💌
		8	Group 1 👻	DES 💌	SHA1 💌	0	Sec. 💌
10 Croup1 v 3065 v 5HA1 v 0 Sec. v Proposal ID select one v Add1c Proposal index		9	Croup 1 💌	3065 V	SHA1 💌	0	Sec. V
Proposal ID select one V Add to Proposal Index		10	Group 1 💌	3DES 💌	SHA1 🐱	0	Sec. V
Proposal ID - select one V Add to Proposal index							
		3	Proposal ID	select one 💌 [Add to Propose	l index	
					9	S	30

Life Time	Enter in a life time value.
Life Time Unit	There are two units that can be selected: second and KB.
Proposal ID	The identifier of IPSec proposal can be chosen for adding the corresponding proposal to the dedicated tunnel.
Add to	Click it to add the chosen proposal indicated by proposal ID to IPSec Proposal index list.

Home > VPN Settings > Tunnel > Manual

Link Networks for People		Air	Plus [®] C	
	Home Adva	nced Tools	Status	Hel
	VPN Settings - Tunnel	11		
	ltem		Setting	
	Tunnel Name		1	
	Aggressive Mode	Enable		
	Local Subnet	0.0.0	1	
	Local Netmask	0.0.0.0	1	
	Remote Subnet	0.0.0.0		
	Remote Netmask	0.0.0.0		
	Remote Gateway			Î.
	Method	MANUAL		
	Local SPI	0×0000		
	Remote SPI	0x0000	1	
L	Encapsulation Protocol	ESP -		
	Encryption Algorithm	3DES 💌		
	Encryption Key (For ESP Only)		(for 3DES)	ONLY) ONLY)
	Authentication Algorithm	NONE -		A.
	Authentication Key			

Tunnel Name	Current tunnel name.
Aggressive Mode	Enabling this mode will accelerate establishing tunnel, but the device will have less security.
Local Subnet	The subnet of the VPN gateway's local network. It can be a host, a partial subnet, or a whole subnet.
Local Netmask	Enter the Subnet Mask for the Local Network of the router.
Remote Subnet	The subnet of the remote VPN gateway's local network. Enter in a valid Netmask IP address of the remote router.
Remote Netmask	The Subnet Mask of the remote VPN gateway's Local Network.
Remote Gateway	The WAN IP address of remote VPN gateway.
Method	The set of rules applied when connecting to the VPN gateway
Local SPI	The value of the local SPI should be set in hex format.
Remote SPI	The value of the remote SPI should be set in hex format.

Home > VPN Settings > Tunnel > Manual Continued...

irks for People			AirF	lus C	
1	Home	H Advanced	gn-Speed 2.4 Tools	GHZ Wireless Status	VPN Ro Helj
	VPN Settings -	Tunnel 1			
-	lte	m		Setting	
	Tunnel Name			1	
	Aggressive Mod	в	Enable		
	Local Subnet		0.0.0	1	
	Local Netmask		0.0.0.0		
	Remote Subnet		0.0.0.0		
	Remote Netmas	k	0.0.0.0		
	Remote Gatewa	У			
	Method		MANUAL		
	Local SPI		0x0000		
	Remote SPI		0x0000	1	
	Encapsulation F	rotocol	ESP 💌		
	Encryption Algor	ithm	3DES 💌		
	Encryption Key				
	(For ESP Only)			(for 3DES	ONLY)
				(for 3DES	ONLY)
	Authentication A	lgorithm	NONE -		
	Authentication K	еу			

Encapsulation Protocol	There are two protocols that can be selected: ESP and AH.
Encryption Algorithm	There are two algorithms that can be selected: 3DES and DES.
Encryption Key	For DES, the encryption key is 8 bytes (16 Char.). For 3DES, the encryption key is 24 bytes (48 Char.).
Authentication Algorithm	There are two algorithms that can be selected: SHA1 and MD5.
Authentication Key	For MD5, the authentication algorithm is16 bytes (32 Char.).For SHA1, the authentication algorithm is 20 bytes.(40 Char.).
Life Time	Enter in the life time value.
Life Time Unit	There are two units that can be selected: Second and KB.

Using the Configuration Menu Home > VPN Settings > Dynamic VPN Tunnel

D-Link		AirPlus G
		High-Speed 2.4GHz Wireless VPN Router
	Home Adva	nced Tools Status Help
2400	VPN Settings - Dynamic \	/PN Tunnel
- Co	Item	Setting
	Tunnel Name	
Wizard	Dynamic VPN	Enable
	Local Subnet	0.0.0.0
Wireless	Local Netmask	0.0.0.0
	Preshare Key	
WAN	IKE Proposal index	Select IKE Proposal
	IPSec Proposal index	Select IPSec Proposal
LAN		
		3 3 🕄
DHCP		Back Apply Cancel Help
VPN		

VPN Settings - IKE There are three parts that are necessary to setup the configuration of IKE for the dedicated tunnel: basic setup, IKE proposal setup, and IPSec proposal setup. Basic setup includes the setting of following items: local subnet, local netmask, remote subnet, remote netmask, remote gateway, and pre-shared key. The tunnel name is derived from the previous page of VPN setting. IKE proposal setup includes the setting of a set of frequent-used IKE proposals and selecting from the set of IKE proposals.

Tunnel NameCurrent tunnel name.

Dynamic VPN This feature works with a VPN software client so the DI-824VUP does not need to know the IP address of the remote clients.

Aggressive Mode Enabling this mode will accelerate establishing the tunnel, but the device will have less security.

Local Subnet The subnet of the VPN gateway's local network. It can be a host, a partial subnet, or a whole subnet.

Local Netmask The netmask of the VPN gateway's local network.

Home > VPN Settings > Dynamic VPN Tunnel Continued...

Link tworks for People			A	Plu	G	
		H	ligh-Speed	2.4GHz Wi	reless V	PN Route
	Home	Advanced	Tools	Stat	IS	Help
	VPN Settings - I	Dynamic VPN Tunr	el			
	h	tem		Setting		
	Tunnel Name					
	Dynamic VPN		🔲 Enable			
	Local Subnet		0.0.0.0			
	Local Netmask		0.0.0.0			
	Preshare Key					
	IKE Proposal ind	ex	Select IKE Pro	posal		
	IPSec Proposal in	ndex	Select IPSec I	Proposal		
				G (b 🙆	
				Back Ap	ply Can	cel Help
				10 CT 40	•	

Preshared Key

The first key that supports IKE mechanism of both VPN gateways for negotiating further security keys. The pre-shared key must be the same for both endpoint gateways.

IKE Proposal index Click the button to setup a set of frequent-used IKE proposals and select from the set of IKE proposals for the dedicated tunnel.

IPSec Proposal Click the button to setup a set of frequent-used IPSec proposals and select from the set of IPSec proposals for the dedicated tunnel.

Using the Configuration Menu Home > VPN Settings > Dynamic VPN Tunnel > Set IKE Proposal

D -Link			
Building Networks for People		High-Speed 2.4GHz Wireless	VPN Router
	Home Advanced	Tools Status	Help
DI-824VOP	VPN Settings - Dynamic VPN Tur	nnel - Set IKE Proposal	
- Comment	Item IKE Proposal index	Setting	
Wizard		Remove	
Wireless	ID Proposal Name DH Group Er	ncrypt algorithm Auth algorithm Life Time	Life Time Unit
WAN	1 Group 1 🗸	3DES V SHA1 V 0	Sec. 🛩
	2 Group 1 🔮	3DES V SHA1 V 0	Sec. V
LAN	4 Group 1 👻	3DES V SHA1 V 0	Sec. 💌
DHCP	5 Group 1 💌	3DES V SHA1 V 0	Sec. 🛩
VPN	6 Group 1 ¥	3DES V SHA1 V 0	Sec. V
	8 Group 1 💌	3DES V SHA1 V 0	Sec. 💌
	9 Group 1 💌	3DES V SHA1 V 0	Sec. 💌
	10 Group 1 🝸	3DES V SHA1 V 0	Sec. 🚩
	Proposal ID se	elect one 👻 Add to Proposal index	
		🌍 🥩 🌔 Back Apply Ca	3 🛟 ancel Help
IKE Proposal index	A list of selected p pool listed below.	proposal indexes fr	rom the
Proposal Name	It indicates which	IKE proposal to be	e focuse
DH Group	There are three gr 1 (MODP768), gro (MODP1536).	roups that can be soup 2 (MODP1024	selectec), and g
Encrypt algorithm	There are two algo	prithms that can be s	selected:
Auth algorithm	There are two algo	prithms that can be s	selected:

Home > VPN Settings > Dynamic VPN Tunnel > Set IKE Proposal Continued...

	Home	Advance	d Tools	Stat	tus	Help
anter a	/PN Settings	- Dynamic VPN T	unnel - Set IKE I	Proposal		
		Item		Settin	g	
	IKE Proposal in	idex	- Empty -			
rd				Barraus		
				Remove		
less	D Proposal Na	ame DH Group E	Encrypt algorithm	Auth algorithm	Life Time	Life Time Unit
	1	Group 1 💌	3DES 🐱	SHA1 💌	0	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. 🗸

Life Time Enter in the life time value.

Life Time Unit There are two units that can be selected: second and KB.

Proposal ID The identifier of IKE proposal can be chosen for adding the corresponding proposal to the dedicated tunnel.

Add to Click it to add the chosen proposal indicated by proposal ID to IKE Proposal index list.

Home > VPN Settings > Dynamic VPN Tunnel > Set IPSEC Proposal

	and a second
VPN Settings - Dynamic VPN Tunnel - Set IPSEC Proposal	
Item Setting	
IPSec Proposal index - Empty -	
Remove	
Proposal Did Group Encap Encrypt Auth Lit	fe Life Tir
Name protocol algorithm algorithm Ti	me Unit
1 None V ESP V 3DES V None V 0	Sec.
2 None V ESP V 3DES V None V 0	Sec.
3 None Y ESP Y 3DES V None V 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 V ESP V 3DES V None V 0	Sec.

IPSec Proposal index	A list of selected proposal indexes from the IPSec proposal pool listed below.
Proposal Name	This is the name used to classify the IPSec proposal.
DH Group	There are three groups that can be selected: group 1 (MODP768), group 2 (MODP1024), and group 5 (MODP1536).
Encap protocol	There are two protocols that can be selected: ESP and AH.
Encrypt algorithm	There are two algorithms that can be selected: 3DES and DES.
Auth algorithm	There are three algorithms that can be selected: SHA1, MD5, and None.

Home > VPN Settings > Dynamic VPN Tunnel > Set IPSEC Proposal Continued...

	Home	Advanc	ed	Tools	Statu	5	Help
~	VPN Settings -	Dynamic VPN	l Tunnel -	Set IPSEC P	roposal		
-		ltem			Setting		
L	IPSec Proposal	index	- Emp	ty -			
L				Remo	ive		
			L				
	ID Proposal	DH Group	Encap	Encrypt	Auth	Life	Life Time
	1	None 🗸	ESP V	3DES V	None V	0	Sec. V
	2	None 💌	ESP 🗸	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. 🚩
		Bronocal ID	select one	V Add to	Bronocal in	lov	
		Proposal ID	select one	🗸 Add to	Proposal ine	lex	

Life Time Enter in a life time value.

Life Time Unit There are two units that can be selected: second and KB.

Proposal IDThe identifier of IPSec proposal can be chosen for adding
the corresponding proposal to the dedicated tunnel.

Add to Click it to add the chosen proposal indicated by proposal ID to IPSec Proposal index list.
Using the Configuration Menu Home > VPN Settings > L2TP Server Setting

	н	ligh-Speed 2	4GHz W	ireless \	VPN Rout
Home	Advanced	Tools	Stat	us	Help
L2TP Server					
	Item		Setting	l).	
L2TP Server	1	Enable			
Virtual IP of L2T	P Server	10 0 1	.1		
Authentication F	Protocol	● PAP ○ CHAP	O MSCHAP		
		Tunnel Setting			
Tunnel Name					
User Name					
Password					
			G (0 6	3 0
			Back Ap	oply Car	ncel Help
	Lloorblomo	Paceword			

Click to enable the L2TP Server function.
Enter your Virtual IP address to access the L2TP server.
Select one of the following authentication protocols: PAP, CHAP, or MSCHAP.
Current tunnel name.
Enter in the username for the L2TP account.
Enter in the password for the L2TP account.

Using the Configuration Menu Home > VPN Settings > PPTP Server Setting

People		Hig	A h-Speed	i 2.4GHz	US Wirele	G ss VPN	Rou
Ho	me Adv	/anced	Tools	S	atus) F	elp
PPTP S	erver						
1	Item			Se	etting		
PPTP Se	rver		Enable				
Virtual IP	of PPTP Server	10	. 0	.0	1		
Authentic	ation Protocol	۲	PAP Och	AP 🔿 MSC	HAP		
		Tu	nnel Settin	1			
Tunnel N	lame						
User Na	me 🗌						
Passwor	d		1				
			-	0		62	0
				Bask	Annha	Ganad	U.ala
				Dack	Арріу	cancel	netp

Click to enable the PPTP Server function.

Enter your Virtual IP address to access the PPTP server.

Select one of the following authentication protocols: PAP, CHAP, or MSCHAP.

Tunnel Name Current tunnel name.

User Name Enter in the username for the PPTP account.

Password Enter in the password for the PPTP account.

Virtual IP of Er PPTP Server Authentication Sa Protocol C

Enable PPTP

Server

Advanced > Virtual Server

D-Link ang Networks for People		_	High	AirP	lus Iz Wirele		Route
24VUP	Home Virtual Server	Advan			Status		lelp
Virtual Server Application Filter Firewall SNMP DDNS	Name Private IP Protocol Type Private Port Public Port Schedule	 ○ Enable 192.168.0. TCP ♥ O Always ○ From 	d Obisable	d 	₹ <u>00 ¥</u> Øply	Cancel	G Help
Routing	Virtual Server Name	_ist FTP	Private IP 0.0.0.0	Protocol TCP 21 / 21	Schedule always		211
DMZ	Virtual Server Virtual Server Virtual Server	HTTP HTTPS DNS	0.0.0.0 0.0.0.0 0.0.0.0	TCP 80/80 TCP 443/443 UDP 53/53	always always always		
	Virtual Server	SMTP POP3	0.0.0.0 0 0 0 0	TCP 25/25 TCP 110/110	always always		

The DI-824VUP can be configured as a virtual server so that remote users accessing Web or FTP services via the public IP address can be automatically redirected to local servers in the LAN (Local Area Network).

The DI-824VUP firewall feature filters out unrecognized packets to protect your LAN network so all computers networked with the DI-824VUP are invisible to the outside world. If you wish, you can make some of the LAN computers accessible from the Internet by enabling *Virtual Server*. Depending on the requested service, the DI-824VUP redirects the external service request to the appropriate server within the LAN network.

Name	The name referencing the virtual service.
Private IP	The server computer in the LAN network that will be providing the virtual services.
Protocol Type	The protocol used for the virtual service.
Private Port	The port number of the service used by the Private IP com-
Public Port	The port number on the WAN side that will be used to access the virtual service.
Schedule	Select Always , or choose From and enter the time period during which the virtual service will be available.

Advanced > Application

ding Networks for People		н	AirPlus igh-Speed 2.4GHz Wireles	G ss VPN Router
	Home	Advanced	Tools Status	Help
AVOP	Special Application	on s used to run applica	ations that require multiple connectio	ins.
		🔿 Enabled 🔿 Dis	abled	
Virtual Server	Name			
	Trigger Port	-		
Application	Trigger Type	TCP 🔽		
	Public Ports			
Filter	Public Type	TCP 🔽		
		Reador		
Firewall	Special Applicatio	on List	Apply	😧 🛟 Cancel Help
Firewall	Special Application	on List Trigger 6112	Public Port 6112	Cancel Help
Firewall SNMP DDNS	Special Application	on List Trigger 6112 7175	Public Port 6112 51200-51201,51210	Cancel Help
Firewall SNMP DDNS	Special Applicatio Name Battle.net Dialpad ICU II	on List Trigger 6112 7175 2019	Public Port 6112 51200-51201,51210 2000-2038,2050- 2051,2069,2085,3010-3030	Cancel Help
Firewall SNMP DDNS Routing	Special Application Name Battle.net Dialpad ICU II Zone Zone	Di List Trigger 6112 7175 2019 47624	Public Port 6112 51200-51201,51210 2000-2038,2050- 2051,2069,2085,3010-3030 2300-2400,28800-29000	Source Image: Cancel Help Image: Cancel Image: Cancel Image: Cancel Image: Cancel
Firewall SNMP DDNS Routing DMZ	Special Application Name Battle.net Dialpad ICU II MSN Gaming Zone PC-to-Phone	Dist Trigger 6112 7175 2019 47624 12053	Public Port 6112 51200-51201,51210 2000-2038,2050- 2009,2088,2085,3010-3030 2300-2400,28800-29000 12120,12122,24150-24220	Cancel Help
Firewall SNMP DDNS Routing DMZ	Special Applicatio Name Battle.net Dialpad ICU II MSN Gaming Zone Pc-to-Phone Quick Time	on List Trigger 6112 7175 2019 47624 12053 554	Public Port 6112 51200-51201,51210 2000-2038,2050- 2051,2069,2085,3010-3030 2300-2400,28800-29000 12120,12122,24150-24220 6970-6999	Cancel Help

Some applications require multiple connections, such as Internet gaming, video conferencing, Internet telephony, and others. These applications have difficulties working through NAT (Network Address Translation). *Special Applications* makes some of these applications work with the DI-824VUP. If you need to run applications that require multiple connections, specify the port normally associated with an application in the **Trigger** field, then enter the public ports associated with the trigger port into the **Incoming Ports** field.

At the bottom of the screen, there are already defined special applications. To use them, select them from the list by clicking a check mark next to the application name. Users may configure the special applications by clicking the Edit icon next to the application. If the mechanism of Special Applications fails to make an application work, try using DMZ host instead.

Note! Only one PC can use each Special Application tunnel.

- Enabled Select to activate the policy.
- **Trigger Port** This is the port used to trigger the application. It can be either a single port or a range of ports.
- **Public Ports** This is the port number on the WAN side that will be used to access the application. You may define a single port or a range of ports. You can use a comma to add multiple ports or port ranges.

Using the Configuration Menu Advanced > Filter > IP Filter

Use IP (Internet Protocol) filters to allow or deny computers access to the Internet based on their IP address.



IP Filter

Use IP Filters to deny LAN IP addresses access to the internet.

Enabled or Disabled

Click **Enabled** to apply the filter policy or click **Disabled** to enter an inactive filter policy. (You can reactivate the policy later.)

IP Address

Enter in the IP address range of the computers that you want the policy to apply to. If it is only a single computer that you want the policy applied to, then enter the IP address of that computer in the Start Source IP and leave the End Source IP blank.

Port Range

Enter in the port range of the TCP/UDP ports that you want the policy to apply to. If it is only a single port that you want the policy applied to, then enter the port number in the Start Port field and leave the End Port field blank. If you want to use all the ports, you can leave the port range empty.

Protocol

Select TCP or UDP as the protocol type.

Schedule

Select **Always**, or choose **From** and enter the time period during which the IP filter policy will be in effect.

Advanced > Filter > MAC Filters

	Home	Advanced	Tools	Status	Hel
	Filter				
	Filters are used t	o allow or deny LAN use	ers from accessing	the Internet.	
and Cal	OIPFIlters	O URL BIOCKING			
	MAC Filters	O Domain Blocking			
ual Server	MAC Filters				
1	Use MAC addres	s to allow or deny comp	uters access to th	e network.	
plication	Disabled M	å∩ Filters			
Filter		computers with MAC ad	dress listed below	to access the net	beork
ritter	Only demy of	omputers with MAC add	Iress listed below	to access the net	work
		ompaters with wro add	incos instea below	to access the net	work
rewaii	Name				
PALMO	MAC Address			1	
SNMP	DHCP Client	select one		lone	
	Brief Chem	Select one			
DDNS				V	U
				Apply	Cancel He
buting	MAC Eller Line				
	Name	MAC Addres	s		

MAC (Media Access Control) Filters are used to allow or deny LAN (Local Area Network) computers from accessing the Internet and network by their MAC address.

At the bottom of the screen, there is a list of MAC addresses from the DHCP client computers connected to the DI-824VUP. To use them, select one from the drop down list. Next click the "Clone" button. Then click the "Apply" button and the DI-824VUP will fill in the appropriate information to the list.

Disabled MAC Filter

Select this option if you do not want to use MAC filters.

Only allow computers with MAC address listed below to access the network

Select this option to only allow computers that are in the list to access the network and Internet. All other computers will be denied access to the network and Internet.

Only deny computers with MAC address listed below to access the network

Select this option to only deny computers that are in the list to access the network and Internet. All other computers will be allowed access to the network and Internet.

MAC Address

Enter the MAC Address of the client that will be filtered.

Using the Configuration Menu Advanced > Filter > URL Blocking



Use URL Blocking to deny LAN computers from accessing specific web sites by its URL. A URL is a specially formatted text string that defines a location on the Internet. If any part of the URL contains the blocked word, the site will not be accessible and the web page will not display.

Disabled URL Blocking

Select this option if you do not want to use URL Blocking.

Advanced > Filter > Domain Blocking



Use Domain Blocking to allow or deny computers access to specific Internet domains whether it is through www, ftp, snmp, etc.

Disabled Domain Blocking

Select this option if you do not want to use Domain Blocking.

Allow users to access all domains except "Blocked Domains"

Select this option to deny users to access the specified Internet domains listed below. Users will be allowed access to all other Internet domains.

Deny users to access all domains except "Permitted Domains"

Select this option to allow users to access the specified Internet domains listed below. Users will be denied access to all other Internet domains.

Using the Configuration Menu Advanced > Firewall

	Home	Advan	ced Too	ols Statu	is He	lp
	Firewall Rule	les s can be used to a	llow or deny traffic	from passing through	i the DI-824VUP.	
		🔿 Enabled 🔘	Disabled			
ual Server	Name					
	Action	O Allow O De	ny			
ication		Interface IP St	art IPE	nd Protoco	I Port Range	
_	Source	* 🗸				
	Destination	* 🗸		TCP N		
	Schedule	 Always 				
		O From	Time 00 💌 0	0 💙 To 00 💙 00 💙		
			day Sun 💌 to	Sun 💌		
MP				C) 🙆 (
				Apr	oly Cancel H	lelp
	Firewall Ru Action Na	les List me	Source	Destination	Protocol	
	Allow Allo	ow to Ping WAN po	ort WAN,*	LAN,192.168.0.1	ICMP,*	1
1	Deny De	fault	**	LAN,-	77 E	1
۷				192.168.0.1	•• IT	16

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

Enabled or Disabled

Click **Enabled** to apply the filter policy or click **Disabled** to enter an inactive filter policy (You can reactivate the policy later).

Name

Enter the name of the Firewall Rule.

Action

Select Allow or Deny to allow or deny traffic to pass through the DI-824VUP.

Source

Choose between a LAN or WAN source. An asterisk signifies the selection of both sources.

IP Start

The starting IP address for the filter policy. Leaving the field blank selects all IPs.

IP End

The ending IP address for the filter policy. Leaving the field blank selects all IPs.

Destination

Choose between a LAN or WAN destination. An asterisk signifies the selection of both destinations.

Using the Configuration Menu Advanced > Firewall Continued

etworks for People	-		High-Sp	AirPlu beed 2.4GHz V	IS (Vireles	G s VPN Rout
	Home	Advance	d To	ols Sta	tus	Help
Fi	rewall Rules rewall Rules ca	an be used to allow	r or deny traffi	c from passing thro	ugh the D	I-824VUP.
	ame 🗌)Enabled ()Dis	abled			
A	ction (
	In	terface IP Start	IP E	ind Prot	ocol Po	ort Range
S S	ource 🔹	~				
– D	estination 🔹	~		TCF	~	-
S	chedule	O Always				
		○ From T	ime 00 💌 : 0	10 🔽 To 00 👻 : 00) 🕶	
		d	ay Sun 💌 to	Sun 💌		
						63
					Apply (Cancel Help
						100 (100) (100)
i i Fi	rewall Rules	List	Source	Dectination	Protoc	ol
	Allow Allow1	to Ping WAN port	WAN,*	LAN,192.168.	0.1 ICMP.	* 🛛 🕅
	Denv Defau	It	**	LAN,-	**	
			LANI*	192.168.0.1	**	
	Allow Defou					

IP Address

Enter in the IP address range of the computers that you want the policy to apply to. If it is only a single computer that you want the policy applied to, then enter the IP address of that computer in the Start Source IP and leave the End Source IP blank.

Protocol

Select one of the following protocols: TCP, UDP, or ICMP.

Port Range

Enter in the port range of the TCP/UDP ports that you want the policy to apply to. If it is only a single port that you want the policy applied to, then enter the port number in the Start Port field and leave the End Port field blank. If you want to use all the ports, you can leave the port range empty.

Schedule

Select **Always**, or choose **From** and enter the time period during which the virtual service will be available.

Using the Configuration Menu Advanced > SNMP

D-Link Building Networks for People		н	Air igh-Speed 2.4	Plus C	VPN Router
01-824VUP	Home	Advanced	Tools	Status	Help
	SNMP Use Simple Netw	ork Management Proto	col(SNMP) for DI-82	4VUP managemer	it purposes.
	SNMP Local	💽 Ena	bled 🔿 Disabled		
Virtual Server	SNMP Remote	🔘 Ena	bled 💿 Disabled		
	Get Community	public			
Application	Set Community	private			
	IP 1				
Filter	IP 2				
	IP 3				
Firewall	IP 4				
SNMP	SNMP Version	Ovi	⊃V2¢		
DDNS				Mapply Ca	ancel Help
Routing					
DMZ					
Performance					

SNMP (Simple Network Management Protocol) is a widely used network monitoring and control protocol that reports activity on each network device to the administrator of the network. SNMP can be used to monitor traffic and statistics of the DI-824VUP. The DI-824VUP supports SNMP v1 or v2c.

Enable SNMP	(Simple Network Management Protocol.)
Local	LAN (Local Area Network).
Remote	WAN (Wide Area Network).
Get Community	Enter the password public in this field to allow "Read only" access to network administration using SNMP. You can view the network, but no configuration is possible wth this setting.
Set Community	Enter the password private in this field to gain "Read and Write" access to the network using SNMP software. The administrator can configure the network with this setting.
SNMP v1	Simple Network Management Protocol (SNMP) is an application layer protocol that facilitates the exchange of management information between nework devices.
SNMP v2	Enhanced version of SNMP v1 with additional protocol operations such as UDP, IP, CLNS, DDP, and IPX.

Advanced > DDNS

D-Link Building Networks for People		н	Air gh-Speed 2.	Plus (4GHz Wireless	S VPN Router
	Home	Advanced	Tools	Status	Help
	Dynamic DNS Use Dynamic DN	S if you want to use you	r DDNS account.		
	DDNS	Oisable	d 🔿 Enabled		
Virtual Server	Provider	DynDNS.org	(Dynamic) 🔽		
	Host Name				
Application	Username / E-m:	ail			
Filter	Password / Key				
Firewall				V Apply C	🎝 🔂
Routing					
DMZ Performance					

DDNS (Dynamic Domain Name System) keeps dynamic IP addresses (*e.g.*, IP addresses assigned by a DHCP capable router or server) linked to a domain name. Users who have a Dynamic DNS account may use this feature on the DI-824VUP.

DDNS	When an IP address is automatically assigned by a DHCP server, DDNS automatically updates the DNS server. Select Disabled or Enabled .
Provider	Select from the pull-down menu.
Host Name	Enter the Host name.
Username/Email	Enter the username or email address.
Password/Key	Enter the password or key.

Using the Configuration Menu Advanced > Routing

Static routes can be added if you require specific routes within your internal network. These routes will not apply to the WAN (Internet) network.



Dynamic Routing	Dynamic Routing Settings allow the VPN Router to route IP packets to another network automatically. The RIP protocol is applied, and broadcasts the routing information to other routers on the network regularly. By default, it is set to disable. Check to enable (RIPv1/RIPv2)
	protocol.
RIP v1	Protocol in which the IP address is routed through the internet.
RIP v2	Enhanced version of RIP v1with added features such as Authentication, Routing Domain, Next Hop Fowarding, and Subnet-mask Exchange.
Destination	Enter in the IP of the specified network that you want to access using the static route.
Subnet Mask	Enter in the subnet mask to be used for the specified net work.
Gateway	Enter in the gateway IP address to the specified network.
Нор	Enter in the amount of hops it will take to the specified network.
Enable	Select this option for the specified static route to take effect.

Hop Count - In a transmission path, each link is terminated at a network device such as a router or gateway. The number of hops equals the number of routers or gateways that data must pass through before reaching the destination.

Advanced > DMZ

D-Link Building Networks for People		н	Air igh-Speed 2	Plus C .4GHz Wireless	VPN Router
I-824VUP	Home	Advanced	Tools	Status	Help
	DMZ DMZ(Demilitariz the Internet.	ed Zone) is used to all	ow a single com	puter on the LAN to b	e exposed to
Virtual Server	IP Address	○ Enabled	abled		
Application				🥥 🌔	3 🗘
Filter				Apply Ca	ncel Help
Firewall					
SNMP					
DDNS					
Routing					
DMZ					
Performance					

If you have a computer that cannot run Internet applications properly from behind the DI-824VUP, then you can allow that computer to have unrestricted Internet access. Enter the IP address of that computer as a DMZ (Demilitarized Zone) host with unrestricted Internet access. Adding a client to the DMZ may expose that computer to a variety of security risks; so only use this option as a last resort.

Advanced > Performance

Link etworks for People		н	Air ligh-Speed 2	Plus C .4GHz Wireless	VPN Route
	Home	Advanced	Tools	Status	Help
	Wireless Perform These are the Wirel	ance ess Performance fea	atures for the AP(A	Access Point) portion.	
	Beacon Interval	100 (msei	c, range:1~1000, c	default: 100)	
	DTIM Interval	3 (ran <u>c</u>	je: 1~65535, defa	ult: 3)	
	TX Rates	Auto 🚩 (Mbps))		
	Wireless Mode	💿 mixed mode	e 🔘 G mode		
	Authentication Type	🔿 Open Syster	m 🔿 Shared Key	🖲 Both	
	SSID broadcast	🖲 Enable 🔘 🛛	Disable		
	8X	💿 Enable 🔿	Disable		
				🚫 🌔 Apply Ca	3 🔂 Incel Help

- **Beacon Interval** Beacons are packets sent by an Access Point to synchronize a wireless network. Specify a value. **100** is the default setting and is recommended.
- **DTIM interval** (Delivery Traffic Indication Message) **3** is the default setting. A DTIM is a countdown informing clients of the next window for listening to broadcast and multicast messages.
- **TX Rates** Select the data rate. Default is **Auto**.
- Wireless Mode Select either mix mode or G mode.
 - **Mixed Mode** The DI-824VUP will use either B or G mode depending on which mode has a stronger frequency.
 - **G Mode** The DI-824VUP will only use G mode.

Advanced > Performance (Continued)



Authentication Select Open system, Shared Key or Both.

- **Open System** The DI-824VUP will be visible to all devices on the network. This is the default setting.
- Shared Key In this mode, in order to access the DI-824VUP on the network, the device must have the same encryption as the router in order to communicate.
- Both In this mode, all devices on the network can access the DI-824VUP.
- **SSID Broadcast Enable** is the default setting. Choose **Enable** to broadcast the SSID across the network. All devices on a network must share the same SSID (Service Set Identifier) to establish communication. Choose **Disable** if you do not wish to broadcast the SSID over the network.
- 8x Enable 8X Mode on the wireless client and the DI-824VUP to increase data transmission speed. 8X Mode will only work with wireless devices that also support 8X Mode.

Using the Configuration Menu Tools > Admin

D-Link Building Networks for People		н	gh-Speed 2.	Plus (4GHz Wireless	S VPN Router
DI-824VUP Admin Time System Firmware Misc	Home Administrators of Administrator (11 R User (The Login R Remote Manag Let administrator	Advanced Settings an change their login pa he Login Name is "adm New Password • teconfirm Password • tec	Tools ssword. n") task from remote	Status	Help

You can change the administrator and user passwords here. It is recommended that you change the administrator password from the default setting. The default password is blank (nothing).

Password	To change the administrator or user password, enter the new password twice to confirm.
Remote Management	Remote Management allows the device to be configured through the WAN (Wide Area Network) port from the Internet using a web browser. A username and password is still required to access the browser-based management interface.
IP Address	Internet IP Address of the computer that has access to the DI-824VUP. If the IP Address is set to 0.0.0.0, this allows all Internet IP addresses to access the DI-824VUP.
Port	The port number used to access the DI-824VUP. Example:http:// <u>x.x.x.x8080</u> , where x.x.x.x. is the WAN IP address of the DI-824VUP and 8080 is the port used for the Web Management interface.

Tools > Time

me Adv	vanced	5 opeen			
		Tools	Status	H	elp
DI-824VUP syster vice Time : Tue Se able NTP	m time. ep 30 00:52:31 2	2003			
fault NTP Server ne Zone	(GMT-08:00)Pacit	fic Time (US & Cana	da)	(Optional)	*
t Device Date and ar: 2003 💌 Mor	l Time nth: Sep 💌 Da	ay: 30 💌			
ur: 00 💌 Minuti	e: 00 💌 Seco	nd: 00 💌		-	~
			V Apply	Cancel	🕞 Help
va fin ta	ice Time : Tue S Ible NTP ault NTP Server le Zone Device Date and r: 2003 V Mor Jr: 00 V Minut	ice Time : Tue Sep 30 00:52:31 2 ible NTP ault NTP Server ie Zone (GMT-08:00)Paci Device Date and Time rr. 2003 V Month: Sep V Da Jrr. 00 V Minute: 00 V Seco	ice Time : Tue Sep 30 00:52:31 2003 ible NTP ault NTP Server ie Zone Device Date and Time r: 2003 V Month: Sep V Day: 30 V Jr: 00 V Minute: 00 V Second: 00 V	ice Time : Tue Sep 30 00:52:31 2003 ible NTP ault NTP Server ie Zone (GMT-08:00)Pacific Time (US & Canada) Device Date and Time r: 2003 V Month: Sep V Day: 30 V ur: 00 V Minute: 00 V Second: 00 V Apply	ice Time : Tue Sep 30 00:52:31 2003 ible NTP ault NTP Server (Optional) ie Zone (GMT-08:00)Pacific Time (US & Canada) Device Date and Time r: 2003 V Month: Sep V Day: 30 V ur: 00 V Minute: 00 V Second: 00 V Apply Cancel

You will need to set the time zone corresponding to your location. The time can be set manually or the device can connect to a NTP (Network Time Protocol) server to retrieve the time.

Enable NTP

(Network Time Protocol). Select to synchronize the time on the DI-824VUP to an NTP server.

Set Device Date and Time

You can manually set the time on your network here.

NTP is short for **N**etwork **T**ime **P**rotocol, an Internet standard protocol that assures accurate synchronization to the millisecond of computer clock times in a network of computers.

Tools > System



The current system settings can be saved as a file onto the local hard drive. The saved file or any other saved setting file created by the DI-824VUP can be uploaded into the unit. To reload a system settings file, click on "Browse" to search the local hard drive for the file to be used. The device can also be reset back to factory default settings by clicking on "Reset to Default" button. Use the restore feature only if necessary. This will erase previously saved settings for the unit. Make sure to save your system settings before doing a factory restore.

Save Settings to Local Hard Drive	Click Save to save the current settings to the local Hard Drive.
Load Settings from Local Hard Drive	Click Browse to find the settings file, then click Load .
Restore to Factory Default Settings	Click Reset to Default to restore the factory default settings.

Tools > Firmware



You can upgrade the firmware of the device using this tool. Make sure that the firmware you want to use is saved on the local hard drive of the computer. Click on "Browse" to search the local hard drive for the firmware to be used for the update. Upgrading the firmware will change the system settings of the router back to the default mode. It is recommended that you save your system settings before doing a firmware upgrade. Please check the D-Link support site for firmware updates at http://support.dlink.com.

Browse

After you have downloaded the new firmware, click **Browse** in this window to locate the firmware update on your hard drive. Click **Apply** to complete the firmware upgrade.



Note! Do not power off the unit when it is being upgraded. When the upgrade is complete, the unit will be restarted automatically.

Tools > Misc



Ping TestIn the open box, enter in a URL (i.e., www.dlink.com) or an IP
address and click on Ping to test your internet connection.

Restart Device Click Reboot to restart the unit.

Block WAN Ping Click **Enable** to block the WAN ping. Computers on the Internet will not get a reply back from the DI-824VUP when it is being "ping"ed. This may help to increase security.

SPI Mode When this feature is enabled, the router will record the packet information passed through the router such as IP address, port address, ACK, SEQ number, and so on. The router will also check every incoming packet to detect if it is valid.

DoS When DoS is enabled, the router will prevent Denial of Service attacks on all computers connected to the DI-824VUP.

Tools > Misc (Continued)



UPnP UPnP is short for Universal Plug and Play which is a networking architecture that provides compatibility among networking equipment, software, and peripherals. The DI-824VUP is a UPnP enabled router and will only work with other UPnP devices/ softwares. If you do not want to use the UPnP Functionality, it can be disabled by selecting "Disabled".

VPN Pass-Through Through Thro

Non-standard FTP port If an FTP server you want to access is not using the standard port 21, then enter in the port number that the FTP server is using instead.

Status > Device Info

k				
ple		Air	Plus (۲
		High-Speed 2.4	GHz Wireles	s VPN Rou
Ho	me Advanced	Tools	Status	Help
Device	e Information			
	Firmware V	ersion: 1.00, Tue, Sep	30 2003	
LAN				
	MAC Address	00-80-C8-23-5C-9F		
	IP Address	192.168.0.1		
	Subnet Mask	255.255.255.0		
	DHCP Server	Enabled		
WAN	MACAdda	00.00.00.00.60.05		
	MAC Address	DU-80-C8-23-5C-9E		
	Connection	DHCP Connecting	DHCP Release	
	Remaining Lease Time	00:00:00		
	IP Address	0.0.0.0		
	Subnet Mask	0.0.0.0		
	Gateway	0.0.0.0		
	Domain Name Server	0.0.0.0		
Wirele	SS			
	MAC Address	00-80-C8-23-5C-9F		
	ESSID	default		
	WEP	Disable		
	Channel	6		
Periph	eral			
	Printer(DB25)	Not ready		
	Printer(USB0)	Not ready		
Device	Time: Tue Sep 30 00:56:43 20(03		
				C
				He

This screen displays information about the DI-824VUP such as WAN, LAN, and Wireless status.

DHCP Renew	Use this button to reconnect to your ISP, if your WAN connection is set up for DHCP.
DHCP Release	Use this button to disconnect from your ISP, if your WAN connection is set up for DHCP.

Using the Configuration Menu Status > Log

D-Link Inding Networks for People		н	Air igh-Speed 2.	Plus C	S VPN Rout
24VUP	Home	Advanced	Tools	Status	Help
	View Log View Log displa features.	ys the activities occurrin	g on the DI-824VU	P. Click on Log Settir	ngs for advance
Device Info	First Page	Last Page Previous	Next Clear L	og Settings	0
Log	Page 1/1				Help
State	WAN Type: Dyn Display time: Tu	amic IP Address (1.00) Je Sep 30 00:57:41 2003	3		
Wireless					

This screen displays activities occurring on the DI-824VUP.

First Page	Click First Page to go to the first page of the log.
Last Page	Click Last Page to go to the last page of the log.
Previous	Click Previous to go to the previous page of the log.
Next	Click Next to go to the next page of the log.
Clear	Click Clear to clear the entire log.
Log Settings	Click for advanced features (see next page).

Using the Configuration Menu Status > Log > Log Settings

D-Link Building Networks for People	AirPlus G
	High-Speed 2.4GHz Wireless VPN Router
324VUP	Home Advanced Tools Status Help Log Settings Logs can be saved by sending it to an admin email address or to a syslog server.
Device Info	E-mail Alert SMTP Server / IP Address Email Address E-mail Subject Syston
Stats Wireless	Syslog Server IP Address 192.168.0. O Enabled O Disabled Log Type V System Activity V Debug Information V Attacks V Dropped Packets V Notice
	🧭 😣 🔂 Apply Cancel Help

E-Mail Alert The DI-824VUP can be set up to send the log files to a specific email address.

SMTP Server IP Enter in the IP address of the mail server.

Email Address Enter in the email address of the recipient who will receive the email log.

Send Mail Now Click to send mail immediately.

IP Address of the Syslog Server Enter in the IP address of a syslog server within the network. Click Enable to activate the policy. The DI-824VUP will send all of it's logs to the specified syslog server.

Log Type Select the types of activity to log. By default, all values are selected.

Status > Stats

High-Speed 2.4GHz Wireless VPN Ro Home Advanced Tools Status Help Traffic Statistics Traffic Statistics display Receive and Transmit packets passing through the DI-824VUP. Refresh Reset Reset Refresh Reset Refresh Refresh Refr	opie		AirPlus	G
Home Advanced Tools Status Hell Traffic Statistics Traffic Statistics display Receive and Transmit packets passing through the DI-824VUP. Refresh Receive Transmit packets passing through the DI-824VUP. Refresh Reset Receive Transmit packets passing through the DI-824VUP. WAN 0 Packets 116 Packets Hell Minister 1290 Packets 1371 Packets Hell Minister 1290 Packets 1371 Packets Hell		H	igh-Speed 2.4GHz Wirele	ss VPN Rout
	Home	Advanced	Tools Status	Help
Receive Transmit WAN 0 Packets 116 Packets LAN 1290 Packets 1371 Packets Mitrolece 218 Packets 211 Packets	Traffic Statis Traffic Statis	tistics tics display Receive and Tr: Reset	ansmit packets passing through the	DI-824VUP.
WAN 0 Packets 116 Packets LAN 1290 Packets 1371 Packets Windows 215 Packets 211 Packets		Receive	Transmit	Help
VVII eless 213 Fathels 311 Fathels	WAN LAN Wireless	0 Packets 1290 Packets 215 Packets	116 Packets 1371 Packets 311 Packets	

In the Stats section, traffic statistics are displayed.

Refresh	This will update the page.
Reset	This will reset the packet counter to zero.
WAN	Displays Received / Transmitted packets from the WAN port.
LAN	Displays Received / Transmitted packets from the LAN port.

Status > Wireless

D-Link Building Networks for People		Air	Plus C	
	H H	ligh-Speed 2.	4GHz Wireless	VPN Router
0.024/0.0	Home Advanced	Tools	Status	Help
Device Info	Connected Wireless Client List The Wireless Client table below display Refresh	s Wireless clients (Connected to the AP	(Access Point). CD Help
Log	Connected Time		MAC Address	
Stats Wireless	Tue Sep 30 00:56:34 2003	00-40-05-1	C5-BA-76	

This screen displays the connection time and the MAC Address of the connected wireless clients. Click on **Refresh** for the most recent information.

Help



This screen displays the complete **Help** menu. For help at anytime, click the **Help** tab in the Configuration menu.

Installing the Print Server Software

Insert the installation CD-ROM into the CD-ROM drive. The following window will be shown automatically. If it is not, please run "autorun.exe" on the CD-ROM.



Installing the Print Server Software (continued)



Configuring on Windows 98se/Me Platforms

After you finish the software installation procedure, your computer will be capable of network printing provided by the DI-824VUP. For convenience, we call the printer connected to the printer port of the DI-824VUP a printer server. On a Windows 95/98 platform, open the Printers window in the My Computer menu.

Now, you can configure the the DI-824VUP:

Find out the corresponding printer, for example, the HP Right click on that icon, an Properties.

The following screen appea



print server of	HP LaserJet 6L (PCL) Properties
g icon of your LaserJet 6L . Id then select	General Details Sharing Paper Print Quality Fonts Device Options W HP Laseulet 6L (PCL) Comment Separator page [none] Browse
ars:	Print Test Page
	HP LasenJet 2200 Series PCL 6 Properties
All-in-1)" Print To er Driver ect driver	Details Det Management Image: Constraint of the following got: Print to the following got: PRIT (Part Server) Image: Constraint of the following got: Print (print Server) Image: Constraint of the following give: Print (print Server) Image: Constraint of the following give: Print (print Server) Image: Constraint of the following give: Print (print) Image: Constraint of the following give: Capture Printer Port. Egd Capture. Tymood settings: To seconds Transmission gety: F5 Scool Sattings: Pott Settings

Click on the Details tab

Choose the "PRTmate: (A from the list attached at the item. Be sure that the Print item is configured to the corr of your printer server.

Click Port Settings

Choose your printer interface.



×

OK

Help

Configuring on Windows 2000/XP Platforms

	🐝 HP LaserJet GL Properties 🛛 🖬 🛛
Click Port	Consul State Ports Idvanced Security Device Settings IP LaseJet 6L
The configuration procedure for a Windows 2000/XP platform is similar to that of Windows 95/98 except the screen of printer <i>Properties</i> .	Pink to the following port(s). Documents will park to the first free checked part. Port Description Printer COM1: Serial Port COM2 Serial Port COM3 Serial Port COM4: Serial Port COM4: Serial Port COM4: Serial Port PhtTimate Local Port Image: Compare Port. Image: Compare Port. Add Port Delete Port Configure Port
Click Configure Port	Enable bidirectional support Epable printer pooling OK Cancel 2009
Choose your printer interface. Type in the IP address of the DI-824VUP.	Printer Position
Click OK	192.168.0.1

(Note: Screen shots are taken in Windows 2000, similar screens will appear in Windows XP.)

Using the Network Setup Wizard in Windows XP

In this section you will learn how to establish a network at home or work, using **Microsoft Windows XP.**

Note: Please refer to websites such as <u>http://www.homenethelp.com</u> and <u>http://www.microsoft.com/windows2000</u> for information about networking computers using Windows 2000, ME or 98.

Go to Start > Control Panel > Network Connections Select Set up a home or small office network



When this screen appears, Click Next.

Please follow all the instructions in this window:



Click Next.

In the following window, select the best description of your computer. If your computer connects to the internet through a gateway/router, select the second option as shown.



Click Next.

Enter a Computer description and a Computer name (optional).



Click Next.

Enter a **Workgroup** name. All computers on your network should have the same **Workgroup** name.



Click Next.

Please wait while the Network Setup Wizard applies the changes.



When the changes are complete, click Next.

Please wait while the **Network Setup Wizard** configures the computer. This may take a few minutes.


Networking Basics

In the window below, select the option that fits your needs. In this example, **Create a Network Setup Disk** has been selected. You will run this disk on each of the computers on your network. Click **Next**.

Network Setup Wizard
You're almost done
You need to run the Network Setup Wizard once on each of the computers on your network. To run the wizard on computers that are not running Windows XP, you can use the Windows XP CD or a Network Setup Disk.
What do you want to do?
⊙ Create a Network Setup Disk
◯ <u>U</u> se the Network Setup Disk I already have
O Use my Windows XP CD
O Just finish the wizard; I don't need to run the wizard on other computers
< <u>B</u> ack Next > Cancel

Insert a disk into the Floppy Disk Drive, in this case drive A.



Networking Basics

Copying	
Please wait while the wizard copies files	
(Cancel

Please read the information under **Here's how** in the screen below. After you complete the **Network Setup Wizard** you will use the **Network Setup Disk** to run the **Network Setup Wizard** once on each of the computers on your network. To continue click **Next**.

Network Setup Wizard
To run the wizard with the Network Setup Disk
Complete the wizard and restart this computer. Then, use the Network Setup Disk to run the Network Setup Wizard once on each of the other computers on your network. Here's how: 1. Insert the Network Setup Disk into the next computer you want to network. 2. Open My Computer and then open the Network Setup Disk. 3. Double-click "netsetup."
< <u>Back</u> <u>Next</u> Cancel

Networking Basics

Please read the information on this screen, then click **Finish** to complete the **Network Setup Wizard**.

Network Setup Wizard		
	Completing the Network Setup Wizard	
	You have successfully set up this computer for home or small office networking.	
出了个	For help with home or small office networking, see the following topics in Help and Support Center:	
	Using the Shared Documents folder Sharing files and folders	
	 <u>Sharing files and folders</u> <u>Sharing files and folders</u> To see other computers on your network, click Start, and then click My Network Places. 	
	To close this wizard, click Finish.	
	< <u>B</u> ack Finish Cancel	

The new settings will take effect when you restart the computer. Click **Yes** to restart the computer.

System 9	Settings Change 🛛 🔀
2	You must restart your computer before the new settings will take effect. Do you want to restart your computer now?
	Yes No

You have completed configuring this computer. Next, you will need to run the **Network Setup Disk** on all the other computers on your network. After running the **Network Setup Disk** on all your computers, your new wireless network will be ready to use.

Networking Basics Naming your Computer

To name your computer, please follow these directions: In Windows XP:

- Click Start (in the lower left corner of the screen).
- **Right-click** on **My Computer**.
- Select Properties and click.



- Select the Computer Name Tab in the System Properties window.
- You may enter a Computer Description if you wish; this field is optional.
- To rename the computer and join a domain, Click **Change**.



Networking Basics Naming your Computer

In this window, enter the Computer name.	Computer Name Changes
Select Workgroup and enter the name of the Workgroup.	You can change the name and the membership of this computer. Changes may affect access to network resources.
	Office
network must have the same Workgroup name.	Full computer name: Office
Click OK.	Member of Domain: Workgroup: Accounting OK Cancel

Checking the IP Address in Windows XP

The wireless adapter-equipped computers in your network must be in the same IP Address range (see Getting Started in this manual for a definition of IP Address Range). To check on the IP Address of the adapter, please do the following:

Right-click on the Local Area Connection icon in the task bar	Disable Status Repair	
	View Available Wireless Networks	
	Open Network Connections	
Click on Status.		3:05 PM

Networking Basics Checking the IP Address in <u>Windows XP</u>

This window will appear.		tus 🛛 ? 🔀
Click the Support tab.	General Support Internet Protocol (TCP/IP) Address Type: Address: 1 Subnet Mask: 2 Default Gateway:	ned by DHCP 192.168.0.114 255.255.255.0 192.168.0.1 Details
Click Close.	Regair	<u><u>C</u>lose</u>

Assigning a Static IP Address in Windows XP/2000

Note: Residential Gateways/Broadband Routers will automatically assign IP Addresses to the computers on the network, using DHCP (Dynamic Host Configuration Protocol) technology. If you are using a DHCP-capable Gateway/ Router you will not need to assign Static IP Addresses.

If you are not using a DHCP capable Gateway/Router, or you need to assign a Static IP Address, please follow these instructions:

Go to Start .	Tour Windows XP	Control Panel
Double-click on Control Panel.	Files and Settings Transfer Wizard	 Help and Support Search Run
	2 🛃 start	P Log Off 🚺 Turn Off Computer

Networking Basics Assigning a Static IP Address in <u>Windows XP/2000</u>

Double-click on **Network** Connections.



 Single-click on Properties.





Networking Basics Assigning a Static IP Address in <u>Windows XP/2000</u>

- Click on Internet Protocol (TCP/IP).
- Click Properties.

- Input your IP address and subnet mask. (The IP Addresses on your network must be within the same range. For example, if one computer has an IP Address of 192.168.0.2, the other computers should have IP Addresses that are sequential, like 192.168.0.3 and 192.168.0.4. The subnet mask must be the same for all the computers on the network.)
- Input your DNS server addresses. (Note: If you are entering a DNS server, you must enter the IP Address of the Default Gateway.)

The DNS server information will be supplied by your ISP (Internet Service Provider).

Local Area Connection 7 Properties ? General Advanced Connect using: D-Link DWL-A650 Configure. This connection uses the following items: Client for Microsoft Networks 🗹 🚚 File and Printer Sharing for Microsoft Networks 🗹 🚚 QoS Packet Scheduler Internet Protocol (TCP/IP) Install. Uninstall Properties Description Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks. Show icon in notification area when connected ΟK Cancel

Internet Protocol (TCP/IP) Prope	rties ? 🔀
General	
You can get IP settings assigned autor this capability. Otherwise, you need to a the appropriate IP settings.	natically if your network supports ask your network administrator for
O Obtain an IP address automatical	y
Use the following IP address:	
IP address:	192.168.0.2
S <u>u</u> bnet mask:	255.255.255.0
Default gateway:	· · ·
O Obtain DNS server address auton	natically
O Use the following DNS server add	Iresses:
Preferred DNS server:	· · · · · · ·
Alternate DNS server:	· · ·
	Advanced
	OK Cancel

Networking Basics Assigning a Static IP Address with <u>Macintosh OSX</u>

- Go to the Apple Menu and select System Preferences.
- Click on Network.

- Select Built-in Ethernet in the Show pull-down menu.
- Select Manually in the Configure pull-down menu.



(*******	Location: Automatic	
ow: Built-in Ether	v Manually	oxies
Configure	Manually using DHCP Using DHCP Using BootP	Router
IP Address: Subnet Mask:	(Provided by DHCP Server) 255.255.255.0	
Router:	192.168,0.1	Search Domains (Optional)
DHCP Client ID:	(Optional)	
Ethernet Address:		Example: apple.com, earthlink ner

- Input the Static IP Address, the Subnet Mask and the Router IP Address in the appropriate fields.
- Click **Apply Now**.

000		Netw	vork	C
i 🛋		S ()		
Show All	Displays Soun	d Network Startup Dis	k	
		Location: Automa	tic 😝	
Show:	Built-in Etherr	iet	÷	
	ſ	TCP/IP PPPoE A	AppleTalk Proxies	_
	Configure:	Manually	*	
			Domain Name Servers (Optional)	
	IP Address:	192.168.0.2		
9	Subnet Mask:	255.255.255.0		
	Router:	192.168.0.1	Search Domains (Optional)	
			Example: apple.com, earthlink.net	
Ether	net Address:	00:09:93:75:de:5a		

Networking Basics Selecting a Dynamic IP Address with <u>Macintosh OSX</u>

- Go to the Apple Menu and select System Preferences.
- Click on Network.



- Select Built-in Ethernet in the Show pull-down menu.
- Select Using DHCP in the Configure pull-down menu.

	Location: Automatic	•
w: Built-in Ethen	net 🚺	
	Manually Manually using DHCI	roxies
Configure	✓ Using DHCP	
-	Using BootP	www.ame Servers (Optional)
IP Address:	(Provided by DHCP Server)	
Subnet Mask:	255.255.255.0	
Router:	192.168.0.1	Search Domains (Optional)
DHCP Client ID:	(Optional)	
Ethernet Address:		Example: apple.com, earthlink.net

- Click Apply Now.
- The IP Address, Subnet mask, and the Router's IP Address will appear in a few seconds.

000		Netw	ork	C
	I	6 🙆		
SUOM MI	Displays 300	Location: Automat	tic 🔹	
Show:	Built-in Ether	net		
	1	TCP/IP PPPOE A	ppleTalk Proxies	_
	Configure:	Using DHCP	(F)	
			Domain Name Servers (Optional)	
	IP Address:	192.168.0.160 (Provided by DHCP Server	0	
	Subnet Mask:	255.255.255.0		
ιι	Router:	192.168.0.1	Search Domains (Optional)	
DH	ICP Client ID:			
Ether	met Address:	(Optional) 00:06:96:79:de:5a	Example: apple.com, earthlink.net	
(i) Cik	k the lock to s	prevent further changes.	Apply Now	

Networking Basics Checking the Wireless Connection by <u>Pinging in Windows XP and 2000</u>

Go to Start > Run > type cmd. A window similar to this one will appear. Type ping xxx.xxx. xxx, where xxx is the IP Address of the Wireless Router or Access Point. A good wireless connection will show four replies from the Wireless Router or Access Point, as shown.



Checking the Wireless Connection by Pinging in Windows Me and 98

Go to Start > Run > type command. A window similar to this will appear. Type ping xxx.xxx. xxx.xxx where xxx is the IP Address of the Wireless Router or Access Point. A good wireless connection will show four replies from the wireless router or access point, as shown.



Networking Basics Adding and Sharing Printers in <u>Windows XP</u>

After you have run the **Network Setup Wizard** on all the computers in your network (please see the **Network Setup Wizard** section at the beginning of **Networking Basics**), you can use the **Add Printer Wizard** to add or share a printer on your network.

Whether you want to add a **local printer** (a printer connected directly to one computer), share an **LPR printer** (a printer connected to a print server), or share a **network printer** (a printer connected to your network through a Gateway/Router), use the **Add Printer Wizard**. Please follow the directions below:

First, make sure that you have run the <u>Network Setup Wizard</u> on all of the computers on your network.

On the following pages, we will show you these 3 ways to use the **Add Printer Wizard**:

- 1. Adding a local printer
- 2. Sharing an network printer
- 3. Sharing an LPR printer

(Other Networking Tasks)

For help with other tasks, that we have not covered here, in home or small office networking, see Using the Shared Documents folder and Sharing files and folders in the Help and Support Center in Microsoft Windows XP.

Networking Basics Adding a local printer (a printer connected directly to a computer)

A printer that is not shared on the network and is connected directly to one computer is called a **local printer**. If you do not need to share your printer on a network, follow these directions to add the printer to one computer.







- Select Local printer attached to this computer.
- (Deselect Automatically detect and install my Plug and Play printer if it has been selected.)
- Add Printer Wizard

 Local or Network Printer

 The wizard needs to know which type of printer to set up.

 Select the option that describes the printer you want to use:

 ① Local printer attached to this computer
 ① Automatically detect and install my Plug and Play printer
 ① A ngtwork printer, or a printer attached to another computer
 ① In set up a network printer that is not attached to a print server,
 use the "Local printer" option.



- Click Next.
- Select Use the following port:
- From the pull-down menu select the correct port for your printer.

(Most computers use the **LPT1:** port, as shown in the illustration.)



- Select and highlight the correct driver for your printer.
 - Click Next.

(If the correct driver is not displayed, insert the CD or floppy disk that came with your printer and click **Have Disk**.)

At this screen, you can change the name of the printer (optional).



Click Next.

Click Next.

Select Yes, to print a test page. A successful printing will confirm that you have chosen the correct driver.



< Back

Next >

Cancel

This screen gives you information about your printer.



Click Finish.

When the test page has printed,



Click OK.

Go to Start > Printers and Faxes.

A successful installation will display the printer icon as shown at right.

You have successfully added a local printer.



Sharing a network printer

After you have run the **Network Setup Wizard** on all the computers on your network, you can run the **Add Printer Wizard** on all the computers on your network. Please follow these directions to use the **Add Printer Wizard** to share a printer on your network:





Networking Basics *Sharing a network printer*





Click Next.

Select Network Printer.

Click Next.

Add Printer Wizard
Local or Network Printer The wizard needs to know which type of printer to set up.
Select the option that describes the printer you want to use:
Automatically detect and install my Plug and Play printer
To set up a network printer that is not attached to a print server, use the "Local printer" option.
< <u>B</u> ack <u>N</u> ext > Cancel

Networking Basics *Sharing a network printer*

Select Browse for a printer.

Add Printer Wizard		
Specify a Printer If you don't know the name or address of the printer, you can search for a printer that meets your needs.		
What printer do you want to connect to? Browse for a printer Connect to this printer (or to browse for a printer, select this option and click. Next): Name. Example: \\server\printer		
Connect to a printer on the Internet or on a home or office network: URL: Example: http://server/printers/myprinter/.printer		
< Back Next > Cancel		

Select the printer you
would like to share.

Click Next.

Click Next.

Add Printe	er Wizard		
Browse Whe	for Printer en the list of printers appears, sele	act the one you want to use.	Ŷ
Printer: Shared	MQC3MP DeskJet 500 printers: ficrosoft Windows Network DUNK J IQC2 J IQC2 J HPDeskJe	HP DeskJet 500	
Printe Com State	r information ment: us: Ready	Documents waiting:	0
		< <u>B</u> ack <u>N</u> ext>	Cancel





Networking Basics Sharing a network printer

- To check for proper installation:
- Go to Start > Printers and Faxes.



The printer icon will appear at right, indicating proper installation.

You have completed adding the printer.

To share this printer on your network:

- Remember the **printer name**.
- Run the Add Printer Wizard on all the computers on your network.
- Make sure you have already run the Network Setup Wizard on all the network computers.

After you run the **Add Printer Wizard** on all the computers in the network, you can share the printer.



To share an **LPR printer** (using a print server,) you will need a Print Server such as the **DP-101P+**. Please make sure that you have run the **Network Setup Wizard** on all the computers on your network. To share an **LPR printer**, please follow these directions:





Click Next.

Please read the

screen.

instructions on this

- Select Create a new port.
- From the pull-down menu, select Standard TCP/IP
 Port, as shown.

Add Printer Wizard			
Select a Printer Port Computers communicate with printers through ports.			
Select the port you want your printer to use. If the port is not listed, you can create a new port.			
OUse the following port:	LPT1: (Recommended Printer Port)	M	
Note: Most computers of The connector for this p	use the LPTT port to communicate with a low sort should look something like this:	cal printer.	
Type of port:	Standard TCP/IP Port	Cancel	



- Click **Next**.
- Enter the Printer IP Address and the Port Name, as shown.

Add Standard TCP/IP Printer Port Wizard		
1	Add Port For which device do you want to	o add a pot?
	Enter the Printer Name or IP add	fress, and a port name for the desired device.
	Printer Name or IP Address:	192.170.0.20
	Port Name:	IP_192.170.0.20
		< <u>Back</u> <u>N</u> ext > Cancel



	Add Standard TCP/IP Printer Port Wizard 🛛 🔀		
_	Additional Port Information Required The device could not be identified.		
 In this screen, select Custom. 	The detected device is of unknown type. Be sure that: 1. The device is properly configured. 2. The address on the previous page is correct. Either correct the address and perform another search on the network by returning to the previous wizard page or select the device type if you are sure the address is correct.		
Click Settings.	Device Type Standard Generic Network Card Gustom Sgttings < Back Next> Cancel		
	Configure Standard TCD//D Destablesites		
	Part Satinga		
Enter the Port Name and the	Port Name: IP_192.170.0.20		
Printer Name	Printer Name or IP Address: 192.170.0.20		
or I P Addross	Protocol		
IF Address.			
Select LPR.	Port Number: 9100		
Enter a	LPR Settings		
Queue	Queue Name: Ip		
Name (if your Print-Server/	LPR Byte Counting Enabled		
Name (if your Print-Server/ Gateway has more than	LPR Byte Counting Enabled SNMP Status Enabled		
Name (if your Print-Server/ Gateway has more than one port,	LPR Byte Counting Enabled SNMP Status Enabled Community Name: public		
Name (if your Print-Server/ Gateway has more than one port, you will need a Queue name).	LPR Byte Counting Enabled SNMP Status Enabled Gommunity Name: public SNMP Device Index: 1		
Name (if your Print-Server/ Gateway has more than one port, you will need a Queue name).	LPR Byte Counting Enabled SNMP Status Enabled Gommunity Name: public SNMP Device Index: 1 OK Cancel		

 This screen will show you information about your printer.



Click Finish.

- Select the printer you are adding from the list of Printers.
- Insert the printer driver disk that came with your printer.
- Click Have Disk.



If the printer driver is already installed, do the following:

Select Keep existing driver.





Add Printer Wizard You can rename your printer if Name Your Printer You must assign a name to this printer you choose. It is optional. Type a name for this printer. Because some programs do not support printer and server name combinations of more than 31 characters, it is best to keep the name as short as nossible Please remember the name Printer name of your printer. You will need HP DeskJet 500 this information when you use the Add Printer Wizard on the other computers on your network.

Click Next.

Select **Yes**, to print a test page.



Click Next

This screen will display information about your printer.

- Click Finish to complete the addition of the printer.
- Please run the Add Printer Wizard on all the computers on your network in order to share the printer.



Note: You must run the **Network Setup Wizard** on all the computers on your network before you run the **Add Printer Wizard**.

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."

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



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



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 facotry defaults.

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



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 winipcfg 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.

P Configuration	_
	PPP Adapter.
Adapter Address IP Address	PPP Adapter. D-Link DFE-550TX 10/100 Adapter 0.0.0.0
Subnet Mask Default Gateway	0.0.0.0
OK Re Release All Re	new All More Info >>

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

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.

Run		? 🔀
	Type the name of a program, folder, document, or Internet resource, and Windows will open it for you	J.
<u>O</u> pen:	cmd	~

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.

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.



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. <u>Example</u>: 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).

Internet Protocol (TCP/IP) Propert	ies 🙎 🕺	
General		
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.		
O Obtain an IP address automatic	ally	
─● Use the following IP address: -		
IP address:	192.168.0.65	
S <u>u</u> bnet mask:	255 . 255 . 255 . 0	
Default gateway:	192.168.0.1	
C Obtain DNS server address aut	omatically	
Use the following DNS server a	ddresses:	
Preferred DNS server:	192.168.0.1	
Alternate DNS server:	4 . 2 . 2 . 2	
	Advanced	
	OK Cancel	

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 Neigborhood** 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**.

Network	?×
Configuration Identification Access Control	
The following network components are installed:	
	- 11
Lient for Microsoft Networks D.1 ink DEE 530TX PCI East Ethernet Adapter (Rev A)	
	- 11
	- II
Add Remove Properties	
Primary Network Logon:	
Client for Microsoft Networks	-
Eile and Print Sharing	
- Description	- II
TCP/IP is the protocol you use to connect to the Internet an	d
wide-area networks.	
OK Car	icel

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. <u>Example</u>: 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



ICP/IP Properties				1	×
Bindings DNS Configuration	Ad- Gateway	wins Co	 onliguestic	NetBIOS n IPAddres	
The first gateway The address orde machines are use	in the Install (in the list w d	ed Gatewa II be the or	y list will b der in whi	e the default. ch these	
<u>N</u> ew gateway 192.168.	0.1] [dd		
	ψe.	Be	nove		
			OK	Cancel	J

Bindings	Advanced	NetBIOS
NS Configuration G	atemay WINS Conf	iguation IP Address
C Djsable DNS		
@ Enable DNS		
Host: anything	Dgmain [
DNS Server Search	Order	
192.168.	0.1	Add
192.168.0.1		errove.
Domain Suffix Sear	ch Order	
		233
	107	turet.

web management. Follow instructions to log in and complete the configuration.

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.

Connect to 19	2.168.0.1
DI-824VUP User name:	🖸 admin 💌
Password:	Remember my password
	OK Cancel

Home Adv	anced Tools Status He
WAN Settings Please select the appropr	iate option to connect to your ISP.
 Dynamic IP Address 	Choose this option to obtain an IP address automaticall from your ISP. (For most Cable modem users)
Static IP Address	Choose this option to set static IP information provided t you by your ISP.
○ PPPoE	Choose this option if your ISP uses PPPoE. (For most D users)
 Dial-up Network 	To surf the Internet via PSTN/ISDN.
O Others	PPTP and BigPond Cable.
Dynamic IP Address	
Host Name	(Optional)
MAC Address	00 - 80 - C8 - C2 - BD - 44
	Clone MAC Address
Primary DNS Address	0.0.0.0
Secondary DNS Address	0.0.0.0
MTU	1500
Auto-reconnect	Enabled O Disabled
Auto-backup	C Enabled Disabled
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-201modem, 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

DL8

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.

Home	Advand	ced	Tools	Status	He
WAN Settings Please select the	e appropriate o	ption to co	nnect to your IS	Р.	
O Dynamic IF	Address	Choose from you	this option to o ut ISP. (For mos	otain an IP address It Cable modern use	automatically rs)
Static IP Ad	dress	Choose	this option to s	et static IP information	on provided to
O PPPoE		Choose	this option if yo	ur ISP uses PPPoE.	(For most D
O Dial-up Ne	Work	To surf	the Internet via I	PSTN/SDN.	
O Others		PPTP a	nd BigPond Cal	ble.	
Static IP Addr	0125				
IP Address		0.0.0.0			
Subnet Mask		255.255	255.0		
ISP Gateway Ad	dress	0.0.0.0			
Primary DNS Ad	Idress	0.0.0.0			
Secondary DNS	Address	0.0.0.0			
NTU		1500	1		
Auto-backup		OFIN	bled Disabl	ad	

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 Enternet 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.

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.

How do I establish a VPN connection between two DI-824VUP Routers?

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.

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



How do I establish a VPN connection between two DI-824VUP Routers? (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.



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.



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.



How do I establish a VPN connection between two DI-824VUP Routers? (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.

н	ome	Advanced	I Too	la Sta	tus	Help
MPN S	Settings - Tr	urosel 1 - Set IR	F Proposal			
-	Re			Sett	-	
IKE Pr	roposal index		- Empty -			
				(Denner 1		
				[institute]		
ID PR	oposal Name	DH Group E	ncrypt algorith	m Auth algorithm	Life Tim	e Life Time Un
1.8	E Proposal	Oroup I 👻	soes 👻	SHA1 👻	0	Sec. 🛩
2		Orbup 2	JORS M	SHA1 🛩	0	Sec. 💌
3		Oroup 5	3065 🛩	SHAT 唑	0	Sec. w
4 [Oroup 1 🐱	3065 🕶	101A1 M	0	Sec. V
5		Oroup 1 💌	soes 🛒	SPIA1	0	Sec. 🛩
6		Group 1 🐱	aces 👻	SHA1 🛩	8	Sec. V
7		Group 1 🐱	3065 🛩	SHAT -	0	Sec. W
0		Orough 1 🐱	3000 V	0HA1 🛩	0	5ee
		Oroup 1	aces 🛩	SHA1	0	Sec. V
10		Group 1 😒	THE REAL PROPERTY.	THAT W	0	Sec. V

How do I establish a VPN connection between two DI-824VUP Routers? (continued)

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

	Home	Advance	d Tools	Sta	tus	He
N	PN Settings -	Tunnel 1 - Set R	KE Proposal			
1		tem		Setti	ng	
1	E Proposal ind	iex.	- Enpty -			
				Remove		
11.5	Descent bio	This Case of	a contained a loss of the second	A shares and a start of the sta	Con The	a Line Time
ŝ	1 bot Proposal	Ormen 1 . W	Tes v	SHA1 W	0	Sec.
	The Proposed	010401	3.65	41911	•	en.
	-	Group 1	D45	3P941 🖤	ų	346.
	3	Group 1 💙	3062 💌	SHA1 🗸	0	Sec.
	4	Group 1 🛩	xes 💌	SHA1 💌	0	Sec.
3	5	Group 1 💌	xes 💌	SHA1 💌	0	Sec.
Э	6	Group 1 😒	3065 💌	SHA1 W	0	Sec.
	,	Group 1 👻	ices w	SHA1 ¥	0	Sec.
1	0	Group 1 🛩	xes v	SHAT Y	0	Sec.
		Conn 1 w	wee w	Chi44 m	6	Car
	·	Oroup's (*	3.45	37941	0	980.

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

н	ome	Advanced	d Tools	s Sta	ntus	H
VPN	Settings - 1	funnel 1 - Set If	E Proposal			
		em	-	Set	ling	
REP	roposal inde	BK .	- Engly -			
				Resove		
1.000				Recourses		
ID P	oposal Nam	e DH Group E	ncrypt algorithm	Auth algorithm	n Life Tim	e Life Tin
1.2.2	RE Proposal	Oroup 1 👻	ates 🛩	SHAT S	0	Sec.
- 4 L		Oroup 1 💌	30E2 💌	MDS	0	Sec.
3		Group 1 🛩	xes 💌	SHA1 🛩	0	Sec
. 4		Group 1 😁	oces 🛩	SHA1 🛩	0	Sec.
5 [Group 1 🛩	30ES 🛩	SHA1 🛩	0	Sec.
6		Group 1 💌	3062 💌	SHA1 😪	0	Sec.
1		Oroup 1 🐱	xes 🖌	SHA1 🖌	0	Sec.
8		Oroup 1 🛩	stes 🛩	SHA1	0	Sec.
9		Oroup 1 🛩	sces 🛩	SHA1 -	0	Sec.
10		Organ 1 M	3085 -	SHA1 W	0	Sec

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

	Home	Advanced	Tool	s Sta	atus	He	ł
VE	N Settings -	Tunnel 1 - Set IK	E Proposal				
1.0	,	tem		Set	ting		
90	E Proposal ind	ex	- Ensty -				
				(Burner)			
			-	[nemove]			
ID	Proposal Nar	ne DH Group E	ncrypt algorithm	n Auth algorithe	n. Life Time	Life Tim	e.t
1	INE Proposal	Group 1 💌	3085 💌	SHA1 ¥	2000	Sec.	3
2		Group 1 🐱	30ES 👻	SHA1 9	0	*2-Ae	
3	1	Oroup 1 🛩	xes 💌	SHAT 🛩	0	Sec	2
4		Oroup 1 💌	xes 🛩	SHA1 🛩	0	Sec.	3
5		Group 1 🐱	xxes 🐱	SHA1 M	0	Sec.	×
6		Group 1 🛩	xes 🛩	5HA1 ¥	0	Sec.	
7		Group 1 🛩	30ES 🛩	SHA1 👻	0	Sec.	3
8	1	Group 1 💌	30ES 💌	SHA1 M	0	Sec.	
9		Oroup 1 💌	xes 👻	SHA1 👻	0	Sec.	a de
10	é li	Group 1 😽	xxes 🛩	SHA1 W	0	Sec.	

How do I establish a VPN connection between two DI-824VUP Routers? (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.

	Home	Advance	d Tools	Sta	tus	Help
VP	N Settings - To	nnel 1 - Set I	CE Proposal			
1.1	Ree	n		Settle	g	
IKE	Proposal index		HE Proposal	1		
				Renove		
				(
ID.	Proposal Name	DH Group	Encrypt algorithm	Auth algorithm	Life Time	Life Time Un
1	RE Proposal	Oroup 1 👻	3065 👻	SHA1 ¥	2800	Sec. 💌
2		Group 1 👻	3065 💌	SHA1 👻	0	Sec. 🛩
э		Group 1 🐱	3065 💌	SHA1 💌	0	Sec. 💌
4		Group 1 💌	3065 💌	SHA1 💌	0	Sec. 💌
5		Group 1 👻	30ES 💌	SHA1 😽	0	Sec. 🛩
6		Oroup 1 🛩	3065 🛩	SHA1 ~	0	Sec. 🛩
7		Oroup 1 💌	3065 💌	SHAT 🛩	0	Sec. 💌
9		Group 1 💌	3065 💌	SHA1 ¥	0	Sec. 🛩
9		Group 1 🛩	3045 M	SHA1 ¥	0	Sec. 🛩
10		Group 1 💌	3065 💌	SHA1 V	0	Sec. 💌
1.11		designed and the	2 13501211		<u> </u>	
	4	Proposal ID 1	× (/	ad to Proposa	index .	

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

D-Link	Air Plus [®] G
	High-Speed 2.4GHz Wireless VPN Router
	The device is restarting
	Continue

Step 16 Click on Select IPSec Proposal.



How do I establish a VPN connection between two DI-824VUP Routers? (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.

Home	Advan	ced	Tool	s	Sta	itu	5	He
VPN Settings	-Tunnel 1 - S	at IPSE	Proposi	d .				
1	Rem				Sett	ing		
IPSec Proposi	d index	F	Ensty -					
				_	_			
				Rete	we			
- Proposal	20021001	Fotan	Ente	ent .	Auth		1.05	Life T
ID Name	DH Group	protoco	algor	thm	algorit	m	Time	Unit
1 IPSec Propo	sal None S	ESP	✓ 30	es 🛩	None	×	Q.	Sec
2	Group 1	ESP	 ✓ 30 	es 🛩	None	۲	0	Sec
3	Oroup 2 Oroup 5	ESP	~ 30	cs 🛩	None	¥	0	Sec
4	None	ESP	~ 30	CS 🛩	None	*	0	Sec
5	None	ESP	✓ 30	es 💌	None	۷	0	Sec
6	None	ESP	 ⇒ 30 	es v	None	~	0	Sec.
7	None	ESP	¥ 30	es v	None	¥	0	Sec.
8	None S	ESP	v 30	es 🐱	None	v	0	Sec
9	None	ESP	× 30	es .~	None	×	0	Sec.
10	None	PSP	-	rs v	None	×	0	Sec

Step 18 Select ESP or AH as the Encapsulation Protocol.

	Home	Adva	inc	ed '	Tools	Statu	5	Help
VE	N Sottings - T	unnel 1	- Se	HIPSEC P	rop-ns-al			
		BID				Setting		
P	Sec Proposal in	dex		- Erre	xty -			
					(Burk			
					Lineak	me		
D	Proposal	DH Gro	op	Encap	Encrypt	Auth	Life	Life Time
1	PSec Proposal	None	~		agomm apes v	None V	a	Sec. V
5	-	None		CSP	SDES V	Nove w	0	Sec. V
3		None	¥	ESP ¥	3065 ¥	Non Y	0	Sec. V
- 4		None	v	ESP 💌	ades M	None 🛩	0	Sec. V
5	-	None	×	ESP 💌	3065 V	None 💌	0	Sec. v
6	-	None	¥	ESP 🛩	soes 🖌	None 🤟	0	Sec. V
7	-	None	۷	ESP 🛩	3DES ¥	None 🛩	0	Sec. V
0		None	~	ESP 🛩	3065 🛩	None 💌	0	Sec
9		None	v	ESP 💌	3065 ¥	None 💌	0	Sec. ¥
10	-	None	¥	ESP 👻	soes 🛩	None 💌	0	Sec.

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

	Home	Advan	ced	Tools	Statu	8	Help
VP	N Settings - T	unnel 1 - S	ut IPSEC I	ropusal			
	R	m			Setting		
IPS	ec Proposal In	dex	-64	AqA =			
				Renk	ove		
ID	Proposal	DH Group	Encap	Encrypt	Auth	Life	Life Time
1	PSec Proposel	None 💌	ESP *	3065 -	None V	0	Sec. N
2		None	ESP 🛩	DES	None 🛩	0	Sec.
э		None v	ESP 💌	3065 M	None 🛩	0	Sec.
4		None 💌	ESP 👻	3065 💌	None 💌	0	Sec.
6		None 👻	ESP 💌	3065 👻	None 🌱	0	Sec.
8		None	ESP 🛩	1065 🛩	None 🛩	0	Sec.
7		None 💌	ESP 💌	3065 💌	None 🛩	0	Sec.
8		None 👻	ESP 💌	3065 👻	None 👻	a	Sec.
9		None	ESP 🛩	3085 🛩	None 💌	0	Sec.
10		None M	ESP 💌	3085 V	None 💌	0	Sec.

How do I establish a VPN connection between two DI-824VUP Routers? (continued)

D-Link

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.

	nome	Advanc	ed	Tools	Statu	s Hela
31-824VUP	VPN Settland -	Tunnel 1 - Se	t IPSEC P	first day	Grand	
100		1000				
E	PSer Prosonal	ndex	-		Setting	
(Internet in the second	- sect republic		- 114			
annara -				Reno	ve .	
Wireless	Deserved		Engan	Escard	6.4%	In Int
	ID Name	DH Group	protocol	algorithm	algorithm	Time Unit
WAN	1 PSec Propose	il None 💌	ESP 😽	30ES 💌	None 🛩	0 Sec.
(Internet in the second se	2	None 🛩	ESP 💌	3065 💌	MD6	0 Sec.
LAN	3	None 🛩	ESP ¥	3065 M	and a second	0 Sec. 1
DHCP		None w	ESP M	3065 M	None V	0 Sec.
		None V	FOP W	3065	Nore of	0 500
VPN	7	None V	ETP V	XES V	None W	0 Sec.
		None 👻	ESP 🛩	xes 🛩	None 🛩	0 Sec.
	9	None 🛩	ESP 🛩	xes 🛩	None 🛩	0 Sec.
	10	None 👻	ESP 💌	3065 🛩	None 🛩	0 Sec.
		Proposal ID	- select one	(A0010	Proposal inc	dex
					_	
D-Link				Ain	Dive	C
			High	Snood 2	CH-Wie	Jose VDN Ro
1	Home	Advance	ringi	Loolo	States	NOS VEN RO
824VUP	MOMe Sulface	Advance	A IDSIC D	10015	Statu	s neg
	ALL ASSAULTS	10000011-30	an secon	all and a second		
-	IPSac Proposal	tem	-		Setting	
and the second second	in Get in reporter in		- 176	KY -		
WIZARG				Feno	10	
Wireless	- Proposal	100	Foran	Encont	Auth	Life Life Time
	ID Name	DH Group	protocol	algorithm	algorithm	Time Unit
WAN	1 PSec Propose	i None 💌	ESP 👻	30ES 🛩	None 💌	0 Sec. N
LAN		None 💌	ESP W	3062	None 💌	0 KB
		None w	BCD W	1005	None w	0 Sec 1
DHCP	4	None 💌	ESP 💌	soes 💌	None M	0 Sec. N
DHCP	5	None 🛩	859 ¥	3085 ¥	None 💌	0 Sec. 1
DHCP VPN	4 5 6 7	None 🛩 None 🛩	ESP ¥ ESP ¥ ESP ¥	3085 ¥ 3085 ¥ 3085 ¥	None 🛩	0 Sec. 0 0 Sec. 0 0 Sec. 0
DHCP	4 5 6 7 8	None 🛩 None 🛩 None 🛩	ESP ¥ ESP ¥ ESP ¥ ESP ¥	3065 ¥ 3065 ¥ 3065 ¥ 3065 ¥	None V None V None V	0 Sec. 0 0 Sec. 0 0 Sec. 0
DHCP VPN	4 5 7 8 9	None V None V None V None V	ESP ¥ ESP ¥ ESP ¥ ESP ¥	3065 ¥ 3065 ¥ 3065 ¥ 3065 ¥ 3065 ¥	None V None V None V None V	0 Sec. 0 0 Sec. 0 0 Sec. 0 0 Sec. 0 0 Sec. 0
OHCP VPN	4 5 7 8 9 10	None V None V None V None V None V	ESP ¥ ESP ¥ ESP ¥ ESP ¥ ESP ¥	3065 ¥ 3065 ¥ 3065 ¥ 3065 ¥ 3065 ¥ 3065 ¥	None V None V None V None V None V	0 Sec. 0 0 Sec. 0 0 Sec. 0 0 Sec. 0 0 Sec. 0 0 Sec. 0
UHCP VPN	4 5 7 8 9 10	None V None V None V None V None V	ESP ¥ ESP ¥ ESP ¥ ESP ¥ ESP ¥ ESP ¥	2065 ¥ 3065 ¥ 3065 ¥ 3065 ¥ 3065 ¥ 3065 ¥	None V None V None V None V	0 Sec. 0 0 Sec. 0 0 Sec. 0 0 Sec. 0 0 Sec. 0 0 Sec. 0
DHCP VPN	4 5 7 8 9 10	None V None V None V None V None V None V	ESP ¥ ESP ¥ ESP ¥ ESP ¥ ESP ¥ ESP ¥	3065 ¥ 3065 ¥ 3065 ¥ 3065 ¥ 3065 ¥ 3065 ¥	None V None V None V None V None V None V	0 Sec. 0 0 Sec. 0 0 Sec. 0 0 Sec. 0 0 Sec. 0 0 Sec. 0 0 Sec. 0
DHCP VPN	4 5 6 7 8 9 10	None V None V None V None V None V None V	ESP V ESP V ESP V ESP V ESP V	3065 ¥ 3065 ¥ 3065 ¥ 3065 ¥ 3065 ¥ 3065 ¥	None V None V None V None V None V None V	0 Sec. 0 0 Sec. 0 0 Sec. 0 0 Sec. 0 0 Sec. 0 0 Sec. 0 0 Sec. 0
DHCP VPN	4	None V None V None V None V None V Proposal ID	ESP V ESP V ESP V ESP V ESP V ESP V	3065 ¥ 3065 ¥ 3065 ¥ 3065 ¥ 3065 ¥ 3065 ¥	Nore V Nore V Nore V Nore V Nore V Proposal Inc	0 Sec. 0 0 S
UPP	4	None V None V None V None V None V Proposal ID	ESP V ESP V ESP V ESP V ESP V ESP V High	3065 ¥ 3065 ¥	Nore V Nore V Nore V Nore V Nore V Proposal Ind	0 Sec 0 0 Sec
DHEF VPN	46678910	Nove	ESP v ESP v ESP v ESP v ESP v ESP v High	XES * Addite Addite Addite Addite	Nore V Nore V No	0 Sec. 0 0 Sec.
D-Link	4	None V None V None V None V None V Propessil ID	ESP V ESP V ESP V ESP V ESP V ESP V ESP V High	305 V 305 V 30	Nore V Nore V No	0 Sec. 0 0 Sec. 0 0 Sec. 0 0 Sec. 0 0 Sec. 0 0 Sec. 0 1 Sec.
URUE VPN	4 5 6 7 8 9 10 10 10 10 10 10 10 10 10 10 10 10 10	None W None W None W None W None W Proposal ID Advance Tonnel 1 - Se	ESP v ESP v ESP v ESP v ESP v ESP v ESP v High	305 V 305 V 30	Inne V Inne Inne Inne Inne Inne Inne Inne Inne	0 Sec. 0 0 Sec.
UPN VPN	4	None W None W None W None W None W None W Proposal IO Proposal IO	ESP V ESP V ESP V ESP V ESP V ESP V ESP V High	X05 V X65 V	Inne V Inne Inne Inne Inne Inne Inne Inne Inne	0 5ec 7 0 5ec 7 0 5ec 7 0 5ec 7 1 5
	4 5 6 7 8 9 10 10 10 10 10 10 10 10 10 10 10 10 10	None W None W None W None W None W None W Proposal ID Proposal ID	ESP v ESP v ESP v ESP v ESP v ESP v ESP v High	X05 V X65 V	Nove V Nove V No	0 56 7 0 56 7
	4 5 6 7 7 8 7 7 7 9 7 10 10 10 10 10 10 10 10 10 10 10 10 10	None W None W No	ESP v ESP v ESP v ESP v ESP v ESP v High	X05 V X05 V	Nove V Nove V No	0 Be 0 0
	4 5 6 7 8 9 10 10 10 10 10 10 10 10 10 10	Nove	ESP v ESP v	X05 V X05 V	Itone V Itone V Ito	0 Bec 1 0 Bec 1 0 Bec 1 0 Bec 1 0 Bec 1 0 Bec 1 1 B
	4 5 6 7 7 8 9 10 10 10 10 10 10 10 10 10 10 10 10 10	None W None W None W None W None W None W Proposal ID Advance Tomat 1 - Se tem ndex	ESP v ESP v	xes v xes v	Itore V Itore	0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
	4 5 6 7 8 9 10 7 8 9 10 7 8 9 10 7 9 9 10 7 9 9 9 10 7 9 9 10 7 9 9 10 7 9 9 9 10 7 9 9 9 10 7 9 9 9 10 9 7 9 9 10 9 7 9 9 10 9 9 10 9 10	Advanc	ESP v ESP v	xes v xes v xe	Intre V Intre	0 96: 9 0 9
	4 5 6 7 7 8 9 9 10 10 10 10 10 10 10 10 10 10 10 10 10	Acce of the second seco	EP v ESP v E	SOES V SOES V SO	Inore V Inore Inore Ino	0 56: 1 0 5
	4 5 6 7 7 8 8 9 10 10 10 10 10 10 10 10 10 10 10 10 10	Aone w None w	ED V ED V ED V ED V ED V ED V ED V ED V	XES V	Inore V Inore Inore Ino	0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
DHCP VPN	4	None W None W None W None W None W Proposal ID Proposal ID Informer None W None W None W None W	EP v EP v EP v EP v EP v EP v EP v EP v Field Field Field EFread Field EFread EF	XES V XES V XES V XES V XES V XES V XES V XES V Adde Popolal Proposition XES V XES V	Incre v Incre	0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
DHCP VPN	4 5 6 7 7 8 8 9 9 10 10 10 10 10 10 10 10 10 10 10 10 10	None W	EP v EP v EP v EP v EP v EP v EP v EP v	XES V	Rane vi Rane vi	0 000 00000000000000000000000000000000
	4 5 5 6 7 7 8 8 9 10 7 8 9 10 7 9 10 7 9 10 7 9 10 7 1 9 10 7 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	Bone w	EP v EP v	ICES V ICES V IC	Rure V Rure V Rure V Rure V Rure V Rure V Statistic Statistic Rure V Statistic Rure Rure V Statistic Rure Rure V	0 56: 1 0 56: 1 1 1 1 1 1 1 1 1 1 1 1 1 1

AirPlus G

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.

How do I establish a VPN connection between two DI-824VUP Routers? (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 establish a VPN connection between my DI-824VUP and 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 19	2.168.0.1
R	
DI-824VUP User name:	😰 admin 💌
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.

How can establish a VPN connection between my DI-824VUP and 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.



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



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.



How can establish a VPN connection between my DI-824VUP and 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.



	Home	Advanced	I Tool	s Sta	tus	Hel
N VI	N Settings -	Tunnel 1 - Set III	E Proposal			
	1	tem		Setti	a	
IK	E Proposal inc	lex	- Empty -			
				(Participa)		
				Memove		
ID	Proposal Na	me DH Group E	incrypt algorithm	Auth algorithm	Life Time	e Life Time l
1	INE Proposal	Oroup 1 😽	3065 🛩	SHAT 🜱	2800	Sec. N
2		Group 1 🛩	3085 🛩	SHA1 🛩	0	Dec.
1.2		Group 1 💌	30ES 💌	SHA1 💌	0	Sec.
4	i E	Group 1 💌	3085 💌	SHA1 💌	0	Sec.
5		Oroup 1 💌	3065 🛩	SHA1 🛩	0	Sec.
6		Group 1 👻	308S 👻	SHA1 👻	0	Sec.
7	20	Group t 💌	3065 🛩	SHA1 💌	0	Sec.
	6	Group 1 💌	30ES 😽	SHA1 💌	0	Sec.
9	6	Group 1 💌	30ES 💌	SHA1 💌	0	Sec.
10	1	Oroup 1 🛩	3065 ¥	SHA1 🛩	0	Sec.

How can establish a VPN connection between my DI-824VUP and 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.

Setting	
Setting	
[Retrine]	
(interest of the second secon	
Auth algorithm Life Time	e Life Time Ur
SHA1 🛩 2800	Sec. 👻
SHA1 💌 0	Sec. 🛩
SHA1 💌 0	Sec. 🛩
SHA1 💌 0	Sec. 💌
SHA1 😽 0	Sec. 🛩
SHA1 🛩 0	Sec. 🛩
SHAT 🛩 0	Sec. 💌
SHA1 🛩 0	Sec. 🛩
SHA1 🛩 0	Sec. 🛩
SHA1 💌 0	Sec. 🗸
	SHAT 2000 SHAT 2000 SHAT 0 SHAT 0

Step 13 The device will restart. Click on the 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.

D-Link	Air Plus [®] G
	High-Speed 2.4GHz Wireless VPN Router
	The device is restarting



How can establish a VPN connection between my DI-824VUP and a DI-804V or DI-804HV Router? (continued)

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

man	Home	Advan	ced		Tools	Sta	atu	5	Help
-824VUP	VPN Setting	s - Tunnel 1 - S	at IPSI	IÇ P	roposal				
C.	-	Rem				Set	ting		
	IPSec Propos	al index		- Dry	dγ÷				
Wizard					Re	-			
(manual d				_	(
Wireless	ID Proposal Name	DH Oroup	Encap	10:	Encrypt algorithm	Auth	hm	Life Time	Life Time Unit
WAN	1 IPSec Prop	osal None N	ESP	v	30ES	None	~	0	Sec. V
	2	None	89	~	Des	None		0	Sec. v
LAN	3	None	657	~	stes .	None	~	Q	Sec. 💌
(management)	4	None	857	*	xes .	None	.*	0	Sec. ¥
DHCP	5	None	854	*	3065	None	¥	0	Sec. V
VAN	6	None	ESP	~	30ES	None	*	0	Sec. w
	7	None	ESP	*	3065	None	*	0	Sec. v
		None	ESF	×	3065	None	*	0	Sec. v
	9	None	EST	v	30E5	None	v	0	Sec. V
	10	Non	etz	~	3045	None		0	Eac. W

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.

Offest Settings - Landa 1 - Setting Setting Setting Manual Picc Proposal Picc Proposal Pisse Proposal OH Orsup Encal Setting Pisse Proposal OH Orsup Encal Setting Pisse Proposal OH Orsup Encal Setting Pisse Proposal OH Orsup Encal Encryst Auth Life Life Name O OF Set Encryst None ¥ O OF Set None ¥ O OF Set A None ¥ O OF Set None ¥ O Set None ¥ O Set B None ¥ O OF Set None ¥ O Set None ¥ O Set
Rem Setting IPSec Proposal Index PSec Proposal D Proposal Index PSec Proposal D Proposal Index PSec Proposal 1 PSec Proposal Name 2 Name 3 Name 3 Name 5 Name 6 Name 6 Name
D Proposal Name DH Group Encap Encap Encap Signifier Encap Signifier <thencap Signifier <thencap< td=""></thencap<></thencap
Premove Premove D Placenal DH Group End all End all All Mill Image Units 1 PSec Presone None Image ESP 2005 None 0 Dispersive 2 None Image ESP 2055 None 0 Dispersive 3 None ESP 2055 None 0 Sec 4 None ESP 2055 None 0 Sec Sec 5 None ESP 2055 None 0 Sec
D Proposal Name D+1 Groups patience Encape approximation Encape approximation Auth approximation Lfm
1 PSic Popose Row V ESP 2055 None 0 2000 Row 0 So So Now 0 Row 0 Row 0 So So Now 0 So So Now 0 So So So So Now 0 So So So Now 0 So So So
2 None EEP 20ES None 0 Mage 3 None W EEP 20ES W None Ø Eee 4 None W EEP 20ES None Ø Eee 5 None W EEP 20ES None Ø Eee 6 None V EEP 20ES None Ø Eee
3 None V ESP 3065 None 0 Sec 4 None V ESP 3065 None 0 Sec 5 None V ESP 3065 None 0 Sec 6 None V ESP 3055 None 0 Sec
4 None CESP 3DES None 0 Sec 5 None ESP 3DES None 0 Sec 6 None ESP 3DES None 0 Sec
5 None v ESP v 3055 v None v 0 Sec
6 None V ESP V 2005 V None V 0 Sec
7 None 🛩 ESP 🛩 30ES 🛩 None 🛩 0 Sec
8 None V ESP V 30ES V None V 0 Sec
9 None 💙 ESP 🛩 30ES 🛩 None 🛩 0 Sec
10 None 👻 ESP 💟 3065 💌 None 👻 0 Sec
Dronosal ID 1 Add to Dronosal index
Proposal ID 1 Proposal index

E	He	m					Sett	ing		
IP	Sec Proposal in	dex			PSec	: Proposal	Remove)		
ID	Proposal Name	DH Gr	up	Encap	ol	Encrypt algorithm	Auth	m	Life Time	Life Time Unit
1	PSec Proposal	None	~	ESP	¥	3065 ×	None	*	0	Sec. Y
2		None		ESP	4	30ES 🗸	None	٠	0	Sec. V
3		None	۷	ESP	¥	30es 👻	None	٧.	0	Sec. ¥
4		None	~	85P	*	3085 👻	None	٠	0	Sec. v
5		None		ESP	۷	30ES 💌	None	٧	0	Sec. V
6		None	~	£5P	2	30ES 💌	None	*	0	Sec. 🛩
7		None	Y	ISP	v	308S 💙	None	۷	8	Sec. Y
8		None	×	ESP	۷	30ES 💌	None	v	0	Sec. V
9		None	۲	ESP	٠	3065 💌	None	۲	0	Sec. 🛩
10		None		85P	¥	3065 ¥	None	٣	0	Sec. V

How can establish a VPN connection between my DI-824VUP and a DI-804V or DI-804HV Router? (continued)

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

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.

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.



D-Link				VPN Rout	er 🕕	-804V
	DEVICE INFORMATION	DEVICE STATUS	BASIC SETUP	ADVANCED SETTINGS	SYSTEM TOOLS	HELP
Main menu	VPN SETTI	NGS				
TIME SETTINGS	Constitution	N	No.			
DEVICE IP SETTINGS	Connection	Name	INGM AND			
CABLE/DSL ISP SETTINGS	Enable	Connection Name	Local IPSEC II	D Remote	IPSEC ID	ommand
ISP ADDITIONAL SETTINGS						
MODEM						
VPN SETTINGS				< BACK	NEXT >	
SAVE & RESTART						
Copyright © 2000						

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

How can establish a VPN connection between my DI-824VUP and 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.

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

To configure the DI-804HV 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	2.168.0.1
R	
DI-824VUP User name: Password:	🖸 admin 💌
	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.

How can establish a VPN connection between my DI-824VUP and 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.



Step 4 In the Local Subnet and Local Netmask fields enter the network identifier for DI-804HV's LAN and the corresponding subnet mask.

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





How can establish a VPN connection between my DI-824VUP and a DI-804V or DI-804HV Router? (continued)

Step 6 In the Remote Gateway field enter the WAN IP address of the remote DI-804V and in the Preshared Key field, enter a key which must be exactly the same as the Preshared Key that is configured on the DI-804V.



Step 7 Click Apply 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 drop down 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.

-Link ng Networks for People	DI-804HV Broadband Hardware VPN Router								
	Home	Advanced	Tools	s Stat	tus	Help			
	VPN Settings - 1	Funnel 1 - Set IKE	Proposal						
2	R	em	Setting						
Ť.	IKE Proposal inde	өх	- Empty -						
Wizard				Remove					
WAN	ID Proposal Nam	ne DH Group En	crypt algorithm	Auth algorithm	Life Time	Life Time Unit			
	1 KE Proposal	Group 2 💌	3DES 💌	SHA1 💌	28800	Sec. 💌			
LAN	2	Group 1 💌	30ES 💌	SHA1 -	0	Sec. 💌			
	3	Group 1 💌	3DES 💌	SHA1 ·	0	Sec. 💌			
DHCP	4	Group 1 💌	3DES 💌	SHA1 ¥	0	Sec. 💌			
VAL	5	Group 1 💌	30ES 💌	SHA1 V	0	Sec. 💌			
100	6	Group 1 💌	3DES V	SHA1 ¥	0	Sec. ·			
	7	Group 1 💌	3DES -	SHA1	0	Sec. ·			
	8	Group 1 💌	3DES -	SHA1	0	Sec. ·			
	9	Group 1 💌	3DES V	SHA1 ¥	0	Sec. ·			
	10	Group 1 💌	30ES •	SHA1 ¥	0	Sec. ·			
		Proposal ID Sei	ect one 💌 📝	Add to Proposal	index				

How can establish a VPN connection between my DI-824VUP and a DI-804V or DI-804HV Router? (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 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.

Step 14 Select ESP as the Encapsulation Protocol.

D-Link	DI-804HV Broadband Hardware VPN Router							
	Home	Advanced	Tools	Status	Help			
	VPN Settings -	Tunnel 1 - Set IKE I	Proposal					
- and		Item	Setting					
	IKE Proposal in	dex	IKE Proposal					
Wizard				Remove				
WAN	ID Proposal Na	ime DH Group Encr	ypt algorithm Au	th algorithm Life	Time Life Time Unit			
	1 KE Proposal	Group 2 💌	3DES 💌	SHA1 💌 288	00 Sec. 💌			
LAN	2	Group 1 💌	3DES 💌	SHA1 V 0	Sec. 💌			
DHCP	3	Group 1 💌	3DES 💌	SHA1 • 0	Sec. •			
	4	Group 1 💌	3DES 💌	SHA1 💌 0	Sec. 💌			
VPN	5	Group 1 💌	3DES 💌	SHA1 💌 0	Sec. 💌			
	6	Group 1 💌	3DES 💌	SHA1 V	Sec. 💌			
	7	Group 1 💌	30ES 💌	SHA1 V 0	Sec. 💌			
	8	Group 1 💌	3DES 💌	SHA1 💌 0	Sec. 💌			
	9	Group 1 💌	30ES 💌	SHA1 • 0	Sec. 💌			
	10	Group 1 💌	30ES 💌	SHA1 V 0	Sec. 💌			
		Proposal ID	▼ Add	Proposal inde	×			

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

Step 16 Enter a Lifetime value of 3600 and then select Sec. as the unit for the lifetime value.

vorks for People	DI-804HV Broadband Hardware VPN Router							
1	Home	Advance	d	Tools	Statu	s	Help	
l	VPN Settings	Tunnel 1 - Set	IPSEC P	roposal				
		Item			Setting			
	IPSec Proposal	index	- Em	Remo	ve			
	ID Proposal Name	DH Group E	ncap rotocol	Encrypt algorithm	Auth algorithm	Life Time	Life Time Unit	
	1 PSec Propos	al None 💌	ESP 💌	3DES 💌	MDS 💌	3600	Sec.	
	2	None 💌	ESP 💌	3DES 💌	None 💌	0	Sec.	
L	3	None 💌	ESP 💌	3DES 💌	None 💌	0	Sec.	
	4	None 💌	ESP 💌	3DES 💌	None 💌	0	Sec.	
L	5	None 💌	ESP 💌	3DES 💌	None 💌	0	Sec.	
L	6	None 💌	ESP 💌	3DES 💌	None 💌	0	Sec. •	
l	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. 💌	

How can establish a VPN connection between my DI-824VUP and a DI-804V or DI-804HV Router? (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.

K.			Broa	DI-	BO4HV ardware \	/PN R	outer
T	Home	Advan	ed	Tools	Statu	s	Help
V	PN Settings - T	'unnel 1 - S	et IPSEC P	roposal			
	H.	em			Setting		
IF	Sec Proposal in	dex	PSe	c Proposal			
				. I.	Parren		
					Nemore		
10	Proposal Name	DH Group	Encap protocol	Encrypt algorithm	Auth algorithm	Life Time	Life Time Unit
1	PSec Proposal	None 💌	ESP 💌	3DES 💌	MDS 💌	3600	Sec. 💌
2		None 💌	ESP 💌	30ES 💌	None 💌	0	Sec.
3		None 💌	ESP 💌	30ES 💌	None 💌	0	Sec.
4		None 💌	ESP 💌	3DES 💌	None 💌	0	Sec.
6		None 💌	ESP 💌	3DES 💌	None 💌	0	Sec. 💌
e		None 💌	ESP 💌	30ES 💌	None 💌	0	Sec. 💌
7		None 💌	ESP 💌	3DES 💌	None 💌	0	Sec. 💌
8		None 💌	ESP 💌	3DES 💌	None 💌	0	Sec. 💌
9		None 💌	ESP 💌	30ES 💌	None 💌	0	Sec. 💌
	0	None 💌	ESP 💌	3DES 💌	None 💌	0	Sec. 💌

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.

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

D:\>ipconfig
Windows 2000 IP Configuration
Ethernet adapter Local Area Connection 10:
Connection-specific DNS Suffix .: IP Address
D:>>ping 192.168.0.100
Pinging 192.168.0.100 with 32 bytes of data:
Reply fron 192.168.0.100: bytes=32 time=10ms TTL=126 Reply fron 192.168.0.100: bytes=32 time<10ms TTL=126 Reply fron 192.168.0.100: bytes=32 time<10ms TTL=126 Reply fron 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), Approxinate round trip times in milli-seconds: Minimum = 0ms, Maximum = 10ms, Average = 2ms

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 establish a VPN connection between my DI-824VUP and 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.

How can I establish a VPN connection between my DI-824VUP and a DFL-300 Firewall? (continued)

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



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

Home	Advanced	Tools	Status	Help
VPN Settings	-Tunnel 1			
1	Rem		Setting	
Tunnel Name		New VPN		
Aggressive Mo	ide	Enable		
Local Subnet		192.168.0.0		
Local Netmas	k .	255 255 255 0		
Remote Subn	et	0.0.00		
Remote Netm	ask	0.0.0.0		
Remote Gatev	vay			
Preshare Key				
IKE Proposal	ndex	Select INE Prop	Manager and Manager	
IPSec Proposi	al index	Select PSec P	voposel.	

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.



How can I establish a VPN connection between my DI-824VUP and 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.

Ho	me	Advanced	Tools	Status	He
VPN Se	ttings -	Tinnel 1			
		lem		Setting	
Tunnel	Name		New VPN		
Aggress	ive Mode		Enable		
Local S	ubnet		192168.0.0		
Local N	etmask		255 255 255 0		
Remote	Subnet		192.168.2.0		
Remote	Netmasi	ĸ	255 255 255 0		
Remote	Gablewile		20 20 20 20	1	
Presha	e Key		1234567		
IKE Pro	posal ind	ex	Select INE Prop	osel	
IPSec P	roposal i	ndex	Select PSec P	opeeal	

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.

	Hom	e	Advanc	ed	Too	ds		Sta	tus	He	elp
	VPN Settle	igs - Tu	nnel 1 - Set	IKE Pro	possi						
1	1	ter	n					Settie	4		
	IKE Propos	al index		- 64	str-						
						100					
				- L.		10	enove.				
	ID Proposi	al Name	DH Group	Encrypt	Ngoritt	tm:/	with algo	rithm	Life Time	Life Tim	e Ur
	1 HE Pro	iecoq	Oroup 1 💌	306	s v		SHAT	۷	2800	Sec.	٧
	2		Group 1 🐱	306	s 👻		SHAT	*	0	*2v/te	
	3		Oroup 1 🐱	306	s 👻		SHAT	*	0	Sec.	*
	4		Oroup 1 👻	306	5.Y		SHAT	4	0	Sec.	۲
	5		Oroup 1 🐱	306	s v		SHAT	•	0	Sec.	۷
	6		Group 1 🐱	306	s •		SHAT	~	0	Sec.	*
	7		Group 1 🛩	306	5 *		SHAT	*	0	Sec.	¥
	8		Oroup 1 💌	308	5 7		SHAT	~	0	Sec	٧
	9		Oroup 1 💌	306	5.4		SHAT	4	0	Sec.	4
н.	10		Oroup 1 🛩	306	5 4		SHAT	*	0	Sec.	¥

How can I establish a VPN connection between my DI-824VUP and 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.

Home	Advanced	Tools	Status	Hel
=	- Linniet 1 - Set in	c Proposal		
IKE Proposal in	ndex	KE Proposal	Setting	
			Renove	
ID Proposal N	ame DH Group E	ncrypt algorithm	Auth algorithm Life Tim	e Life Time
1 PE Propos	el Group 1 🕊	3DES 🛩	SHA1 ¥ 2800	Sec.
2	Oroup 1 👻	308S 💌	SHAT 💌 0	Sec.
3	Group 1 💌	3065 🛩	SHA1 💌 0	Sec.
4	Group 1 💌	3065 💌	SHA1 V 0	Sec.
5	Group 1 👻	30E5 💌	SHA1 😽 0	Sec.
6	Oroup 1 🛩	3065 🛩	SHA1 👻 0	Sec.
1	Oroup 1 💌	3DES 💌	SHAT 👻 0	Sec.
0	Group 1 💌	30ES 💌	SHA1 👻 0	Sec.
9	Group 1 😁	3085 M	SHA1 🛩 0	Sec.
10	Group 1 👻	3065 🛩	SHA1 💌 0	Sec.
	Descended 1	20	Millio Property in Ann	

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 unit for the lifetime value.

	Home	Advance	d Too	ls Sta	tus	He	Þ
VP	N Settings -	Tunnel 1 - Set D	CE Proposal				
	,	tem		Sett	ng		
IKE	Proposal ind	θ.r.	-Enety -	1			
				(Press			
				[month			
ID.	Proposal Nan	ne DH Group	incryst algorith	m Auth algorithm	Life Time	Life Time	U
1	IKE Proposal	Group 1 🛩	3065 🛩	MDG 🛩	20000	Sec.	÷
2		Group 1 🛩	30ES 🛩	SHA1 MDS	0	Sec.	÷
3	1	Group 1 💌	SDES 🛩	SHA1 🛩	0	Sec.	Y
1.4	0	Group 1 🛩	soes 💌	SHA1 🛩	0	Sec.	÷
5	1	Group 1 😒	3065 🐱	SHA1 V	0	Sec.	Y
6		Group 1 🜳	3065 👻	SHA1 ¥	D	Sec.	÷
1	0	Group 1 🛩	3DES 🐱	SHA1 💌	0	Sec.	÷
8		Oroup 1 🛩	SDES 👻	SHA1 💌	0	Sec.	÷
9		Oroup 1 😁	SDES 👻	SHA1 M	0	Sec.	۲
10		Group 1 🛩	3065 V	SHA1 -	0	Sec.	4

How can I establish a VPN connection between my DI-824VUP and 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.

D-Link	Air Plus [®] G
	High-Speed 2.4GHz Wireless VPN Route
	The device is restarting
	Continue

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.





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.

How can I establish a VPN connection between my DI-824VUP and a DFL-300 Firewall? (continued)

a a	
nk	Office Firewall
n VPN Auto Keyed Tunnel	
Name	NewVFN
From Source @ Inter	nal C DMZ
Subnet / Mask	192.168.1.0 / 255.255.255.0
To Destination	• • • • •
Remote Gateway F	Fixed IP 10.10.10.10
Subnet / Mask	192 168.0.0 / 255 255 255 0
C Remote Gateway -	Amamic IP
Subnet / Mask	0.235,235,235
C Remete Cleast File	ad ID as Domenia ID
Authentication Method	Deshare w
Prochased Karr	Preside A
Presnared Key	123466
Encapsulation	- Alexandra - Alexan
Data Encryption + Al Authoritication Only	uthentication
C Authentication Only	
Perfect Forward Secret	ay and a second s
IPSec Lifetime	28800 Seconds
	OK Carcel

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.

		0 11	0011	3															
Etherne	et ad	apte	r Lo	cal	Ĥı	rea	Co	nn	ec	tio	n 1	10							
	Con	nect	ion-:	spe	cif	fic	D١	IS	Su	ffi	×								
	IP Cb	Addr	ess.											19	2.	16	8.	1.1	2 0
	Def	ault	Gate	eva									-	19	2	16	8.	1.1	1.0
						- L. 1	29	h	1.0.1	- 0	f	lat							
Pinging	r 192	-168	-И-11																
Pinging	y 192	.168	.0.1	99	w10	. n	36	na						١.		_	~		
Pinging Reply i Reply i	y 192 from	.168 192.	168.0	80 8.1 8.1	00: 00:	bi bi	yte		32	ti	ne	=1(des:		ŢI	,=1 .=1	26		
Pinging Reply f Reply f Reply f	y 192 fron fron fron	.168 192. 192. 192.	168.0 168.0 168.0	8.1 8.1 8.1	00: 00: 00:	: b : b : b	yte yte yte		32 32 32	ti ti	ne ne	=1((1)	des des		TI TI TI	,=1 ,=1 ,=1	26 26 26		
Pinging Reply f Reply f Reply f Reply f	y 192 fron fron fron fron fron	.168 192. 192. 192. 192.	168.0 168.0 168.0 168.0	9.1 9.1 9.1 9.1	00 00 00 00	: b: : b: : b: : b: : b:	yte yte yte yte	109 18= 18= 18=	32 32 32 32 32	ti ti ti	ne ne ne	=1) (1) (1) (1)	des des des		TI TI TI	,=1 ,=1 ,=1 ,=1	26 26 26 26		
Pinging Reply f Reply f Reply f Reply f Reply f	y 192 fron fron fron fron tatis	.168 192. 192. 192. 192. tics	168.0 168.0 168.0 168.0 168.0	0.1 0.1 0.1 0.1 0.1	00: 00: 00: 00:	: b : b : b : b : b : b	yte yte yte yte	109 109 109 109	32 32 32 32 32	ti ti ti	ne ne ne	=1((1) (1) (1)	des des des des		TI TI TI	,=1 ,=1 ,=1	26 26 26		

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

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.

Home	Adva	nced 🗾	Tools	Status	1 8	lelp
Virtual Server Virtual Server is	used to allow	Internet users	access to LAN ser	vices.		
	OEnable	ad ODisable	bd			
Name						
Private IP	192.168.0	{}	2			
Protocol Type	TCP 👻					
Private Port	() ()					
Public Port						
Schedule	O Alway					
	O From	Time 00	- 00 - To 00 -	- 00		
	C main	day Sun	v to Sun v			
		Gal) [0	63	C
				Apply	Cancel	Help
Virtual Server	List					
Name		Private IP	Protocol	Schedule		
Virtual Serve	IT FTP	0.0.0.0	TCP 21/21	always		31
Virtual Serve	r HTTP	0.0.0.0	TCP 80/80	always		31
Virtual Serve	IT HTTPS	0.0.0.0	TCP 443/443	always		31
Virtual Serve	r DNS	0.0.0.0	UDP 53753	always		21
Virtual Serve	r SMTP	0.0.0.0	TCP 25/25	always		30

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.

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).

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).

Connect to 19	2.168.0.1
R	
DI-824VUP	
User name:	😰 admin 🔛
Password:	
	Remember my password
	OK Cancel

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.



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.

D-Link admg Networks for People	High-Speed 2.4GHz Wireless VPN Route						
	Home	Advance	d Too	ols Sta	tus	Help	
2400	Firewall Rules Firewall Rules ca	n be used to allow	v or deny traffic abled	from passing throu	igh the DI-824	IVUP.	
Virtual Server	Name						
The second	Action	Allow ODeny					
Application	Int	terface IP Start	IP E	nd Prote	ocol Port Ra	ange	
	Source *	~					
Filter	Destination *	~		TCP	~]-	
	Schedule	Always					
Firewall		◯ From T	ime 00 💌 0	00 🗸 To 00 🖌 00	~		
		d	ay Sun 💌 to	Sun 👻			
SNMP					🔗 🔗	0	
				,	oply Can	rel Help	
DDNS				,	opply can	let netp	
	Firewall Rules	List					
Routing	Action Name		Source	Destination	Protocol	F 1 63	
	Allow Allow t	o Ping WAN port	WAN,*	LAN,192.168.0).1 ICMP,*	L 1	
DMZ	🗌 Deny Defaul	t	**	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.

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	Х
80	192.168.0.6	Х
1723	192.168.0.7	Х

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**.

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

Step 6 Create a second entry as shown here:

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

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



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.



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.

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

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**

in i	Home	Advan	ced 🗾	ools	Status	Help
	Virtual Server Virtual Server i	r is used to al	llow Internet	users access t	to LAN service	s.
		C Enable	ed C Disabl	ed		
ver	Name	SOCOM				
	Private IP	192.168.0	100			
	Protocol Type	TCP .				
	Private Port	6869	_			
	Public Port	6869				
	Schedule	Alway	'S			
		C From	Time 00	• 00 • To 0	• 00 • 00	
MP			day Sun	🔹 to Sun 💌		
					🍼 🌔	3 🗘
					Apply Ca	ncel Help
	Mintural Control	el int				
9		L F12F				
	Name		Private IP	Protocol	Schedule	
	Name Virtual Serv	ver FTP	Private IP 0.0.0.0	Protocol TCP 21 / 21	Schedule always	
	Name Virtual Serv Virtual Serv	ver FTP ver HTTP	Private IP 0.0.0.0 0.0.0.0	Protocol TCP 21 / 21 TCP 80 / 80	Schedule always always	21
	Name Virtual Serv Virtual Serv Virtual Serv	ver FTP ver HTTP ver HTTPS	Private IP 0.0.0.0 0.0.0.0 0.0.0.0	Protocol TCP 21 / 21 TCP 80 / 80 TCP 443 /	Schedule always always always	

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**.
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

H	lome	Advan	iced 🗧	Tools	Status	1 6	telp
Virtua	al Server Server is i	used to allow I	internet user	s access to LAN se	nvices.		
		Enable	d ODisab	led			
Nam	0	gamespy	1				
Priva	te IP	192.168.0.	100				
Proto	col Type	Both 💌					
Priva	te Port	3783					
Publi	c Port	3783					
			<u>.</u>				
ocine	oble	 Always Conversion 					
		O Prom	and Sin	* 10 Cm *			
			Gay Jul	Collin Source		1	-
					v	2	U
					Apply	Cancel	Help
Vien	al Servier	List					
N	lame		Private IP	Protocol	Schedule		
OV	Intual Serve	FTP	0.0.0.0	TCP 21/21	always		
ΠV	Intual Serve	HTTP	0.0.0.0	TCP 90/90	always		
OV.	Intual Serve	HTTPS	0.0.0.0	TCP 443/44	3 always		
OV	Intual Serve	r DNB	0.0.0.0	UDP 53753	always		
1000		OLATE.	0000	100 26/26			13-14

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.

Click Apply and then continue.



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.

	Home	Advanc	rlign-	ople	Status	ISS VPN	Rou
90	Virtual Server Virtual Server is u	used to allow int	ternet users a	ccess to LAN ser	vices.		eip
ual Server	Name	 Enabled kazaa 	O Disabled				
	Private IP	192.168.0.1	00				
dication	Protocol Type	TCP 💌					
	Private Port	6859					
Filter	Public Port	6859					
	Schedule	Abways					
rewall		O From	Time 00 💌	00 V To 00 V	. 00 .		
			day Sun 💌	to Sun 💌			
DDNS				177 Assessive and the	S Apply	Cancel	C
	Virtual Server	List					
suting	Name		Private IP	Protocol	Schedule		-
and the second	Virtual Server	r FTP	0.0.0.0	TCP 21/21	always		2
		1.1.1.1.1.1.1.1	10.00	and a second second second			
z	Virtual Server	THTTP	0.0.0.0	TCP 80/80	always		
	Virtual Server	rHTTP rHTTPS	0.0.0.0 0.0.0.0	TCP 80/80 TCP 443/443	always		

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

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

To hose 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 you 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.

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.

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.



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).

Home	Advance	d Tools	Status	Help
Firewall R	ules es can be used to allo	w or deny traffic fro	m passing through th	e DI-824VUP.
	Enabled O Dis	sabled		
Name	ichat2	1		
Action	Allow O Derw			
	Interface IP Start	IP End	Protocol	Port Range
Source	WAN 👻 192.168	.0.100		
Destination	LAN 👻		TCP 👻	
Schedule	Always			
	O From 1	lime 00 💌 00	To 00 ¥ 00 ¥	
		tay Sun v to S	n ×	
			C A	0 0
			Apply	Cancel neip
Firewall R	ules List			
Action N	ame	Source	Destination Pro	stocol
Allow A	low to Ping WAN port	WAN,*	LAN, 192.168.0.1 ICH	AP,*
Deny D	efault		192 168.0.1	131
	1210-2			136

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

D-Link

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.

		High-	Speed 2.4G	iHz Wirele	ss VPN	Rou
Home	Advanc	ed 🔤	ools	Status		leip
Virtual Server is a Name Private IP Protocol Type	Enabled ichat3 192.168.0 TCP	O Disabled	cess to LAN se	rvices.		
Private Port Public Port Schedule	5190 5190 O Always	1				
	O From	Time 00 🤟 day Sun 💌	00 ¥ To 00 to Sun ¥		Cancel	C
Virtual Server	List					
Name	p	rivate IP	Protocol	Schedule		
Virtual Serve	rFTP 0	0.0.0	TCP 21/21	always		3
Virtual Serve	HTTP 0	0.0.0	TCP 80/80	always		
Virtual Serve	rHTTPS 0	0.0.0	TCP 443/443	ahways		
Virtual Serve	DNB 0	0.0.0	UDP 53/53	always		
						104

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

Stsp 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.

How do I send or receive a file via iChat when the Mac OSX 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. "

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 <u>http://www.faqs.org/rfcs/rfc1631.html</u>

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