



# Manual

Version 1.2

DI-LB604  
**Load Balancing Router**

# Table of Contents

<b>Package Contents</b> .....	<b>4</b>
<b>Minimum System Requirements</b> .....	<b>4</b>
<b>Introduction</b> .....	<b>5</b>
<b>Features and Benefits</b> .....	<b>6</b>
<b>Hardware Overview</b> .....	<b>7</b>
Connections .....	7
LEDs.....	8
<b>Getting Started</b> .....	<b>9</b>
<b>Using the Configuration Menu</b> .....	<b>10</b>
Home.....	11
<i>Wizard</i> .....	11
<i>WAN</i> .....	12
Port Options.....	14
<i>LAN</i> .....	16
<i>DHCP</i> .....	16
DHCP Client List.....	17
Setting Static DHCP .....	18
<i>Load Balance</i> .....	19
<i>IPsec</i> .....	20
Advanced.....	25
<i>Host IP</i> .....	25
<i>Static Routing</i> .....	27
<i>Virtual Server</i> .....	28
<i>Applications</i> .....	29
<i>Multi-DMZ</i> .....	30
<i>Filters</i> .....	31
<i>QoS</i> .....	33
QoS Set Policy .....	34
<i>NAT</i> .....	35
Tools .....	37
<i>Admin</i> .....	37
<i>Time</i> .....	38
<i>System</i> .....	38
<i>Firmware</i> .....	39
<i>Email Alert</i> .....	40
<i>SNMP</i> .....	41

DDNS.....	42
UPnP .....	43
Misc.....	44
Status.....	46
Device Info.....	46
Log .....	47
Log Settings.....	47
Stats .....	49
NAT Status .....	51
NAT Connection List .....	52
<b>Troubleshooting .....</b>	<b>53</b>
<b>Technical Specifications .....</b>	<b>55</b>
<b>Frequently Asked Questions .....</b>	<b>57</b>
<b>Appendix.....</b>	<b>83</b>
Securing Your Network .....	83
Glossary .....	84
<b>Contacting Technical Support .....</b>	<b>92</b>
<b>Warranty .....</b>	<b>93</b>
<b>Registration .....</b>	<b>97</b>

# Package Contents

- DI-LB604 Load Balancing Router
- Cat. 5 Ethernet cable
- Power adapter (5.0V, 2A)
- CD-ROM with software and manual
- Quick installation guide



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

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

## Minimum System Requirements

- Ethernet-Based Cable or DSL Modem
- Computers with Windows, Macintosh, or Linux based operating systems with an installed Ethernet adapter and CD-ROM Drive
- Internet Explorer version 6.0 or Netscape Navigator version 7.0 and above



# Introduction

---

The D-Link Express EtherNetwork DI-LB604 is a 4-port Ethernet broadband router. The DI-LB604 enables users to quickly and easily share a high speed Internet connection. The D-Link DI-LB604 also incorporates many advanced features, commonly found in more expensive routers.

After completing the steps described in the quick installation guide you will have the ability to share a single Internet connection as well as sharing information and resources such as files and printers.

The DI-LB604 is compatible with most popular operating systems, including Macintosh, Linux and Windows, and can be integrated into an existing network. This Manual is designed to help you connect the D-Link Express EtherNetwork DI-LB604 to a high speed Internet connection and 4 Ethernet PC connections.

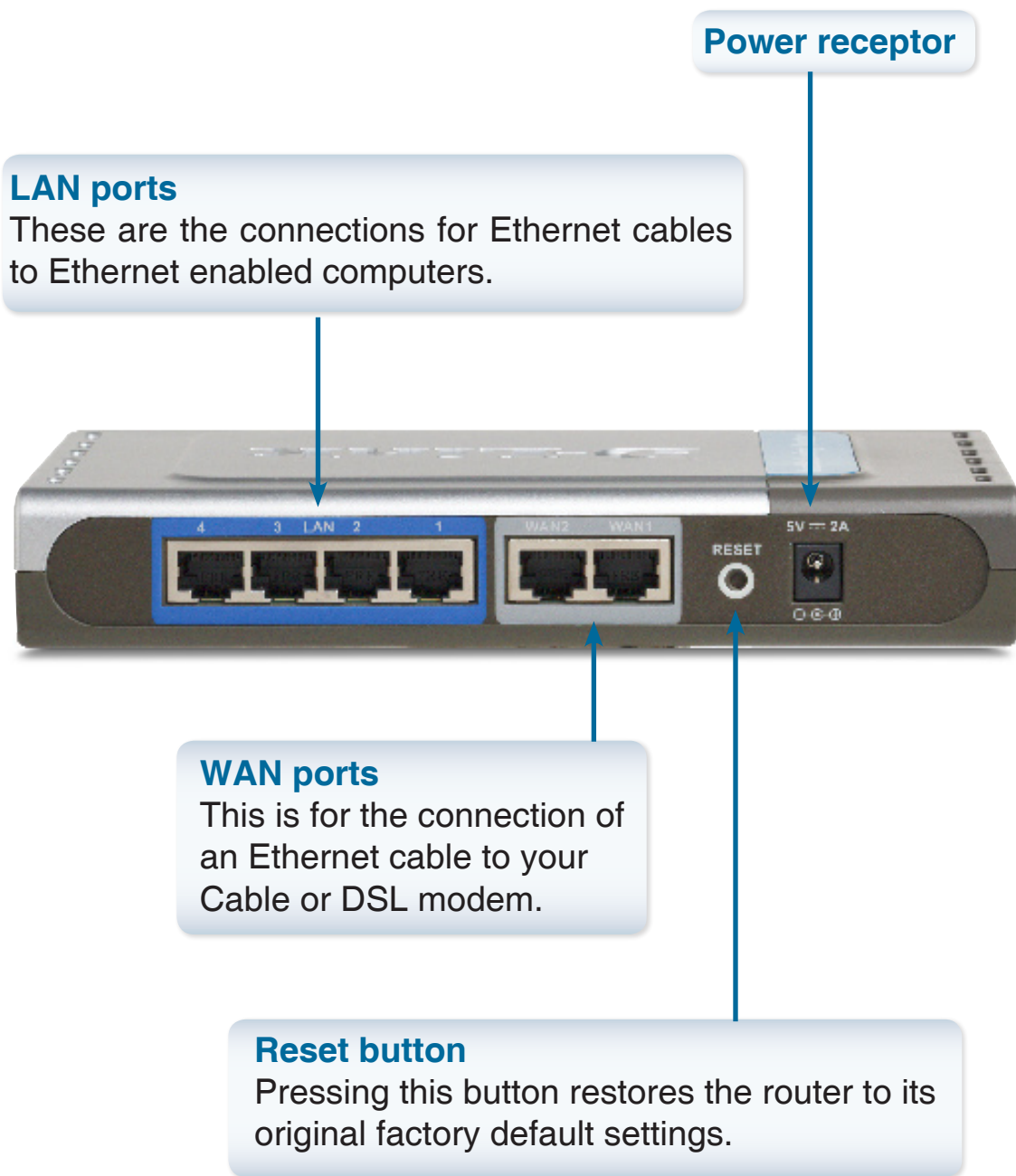
This manual provides a quick introduction to broadband router technology, firewalls, and local area networking. Please take a moment to read through this manual and get acquainted these various technologies.

# Features and Benefits

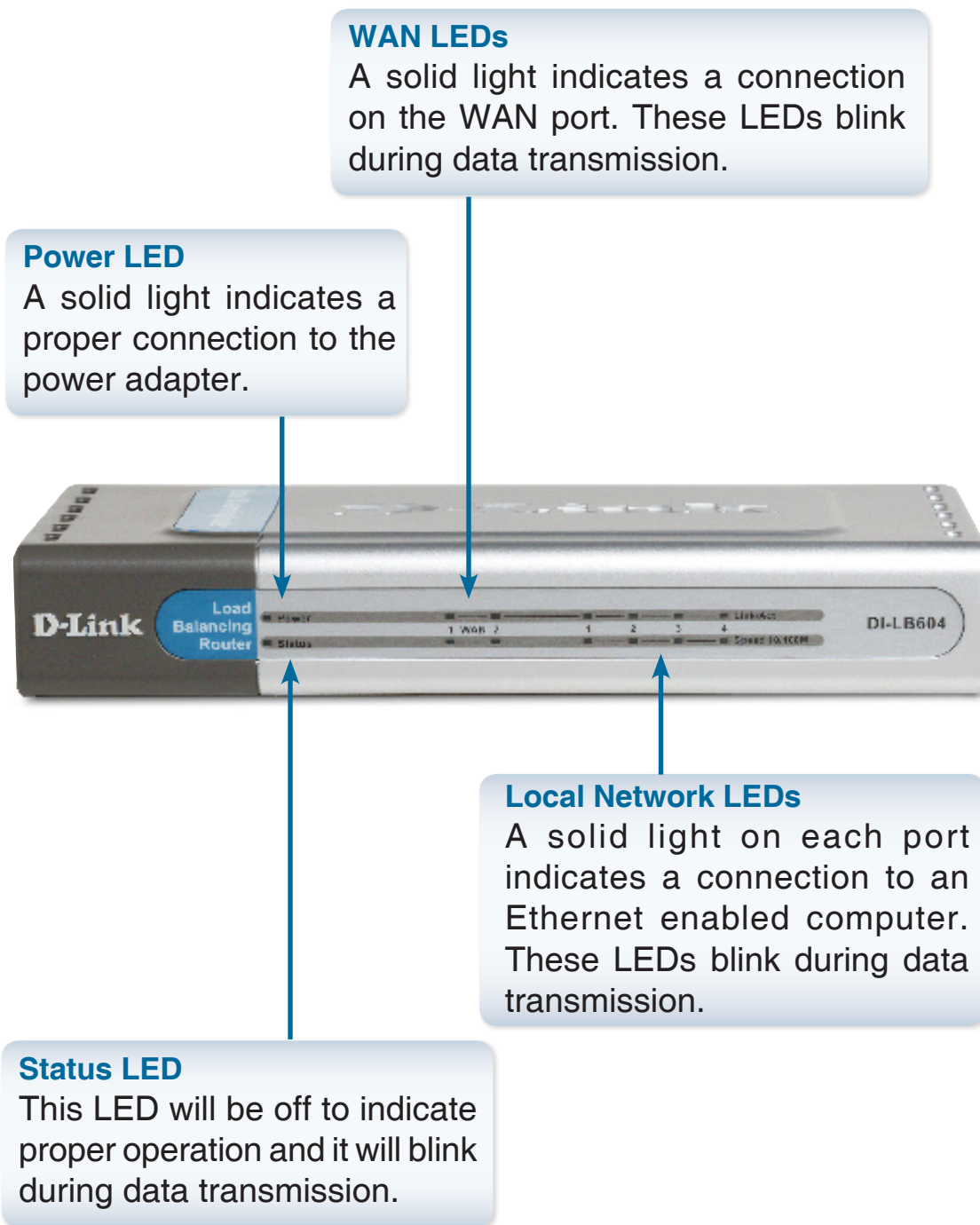
- Connects multiple computers to a broadband (cable or DSL) modem to share the Internet connection.
- Allows you to quickly and easily share an Internet connection with multiple computers and devices.
- Supports multiple and concurrent IPsec and PPTP pass-through sessions, so multiple users behind the DI-LB604 can access corporate networks through various VPN clients more securely.
- The web-based user interface displays a number of advanced network management features.
- Easily applied content filtering based on MAC Address, IP Address, URL and/or domain name.
- These filters can also be scheduled to be active on certain days or for a duration of hours or minutes.
- NAT allows you to share a single IP Address and protects you from outside intruders gaining access to your private network.
- All of the networked computers can retrieve TCP/IP settings automatically from the DI-LB604.
- The DI-LB604 is configurable through any network computer's web browser using Netscape or Internet Explorer.
- Allows you to assign different access rights for different users.
- Enables you to expose WWW, FTP and other services on your local area network (LAN) to be accessible to Internet users.
- When running special applications that require multiple connections, like Internet gaming, video conferencing, and Internet telephony, the DI-LB604 can detect the application type and open a multi-port tunnel for it.
- The demilitarized zone (DMZ) allows a networked computer to be fully exposed to the Internet. This function is used when the Special Application feature is insufficient to allow an application to function correctly.

# Hardware Overview

## Connections



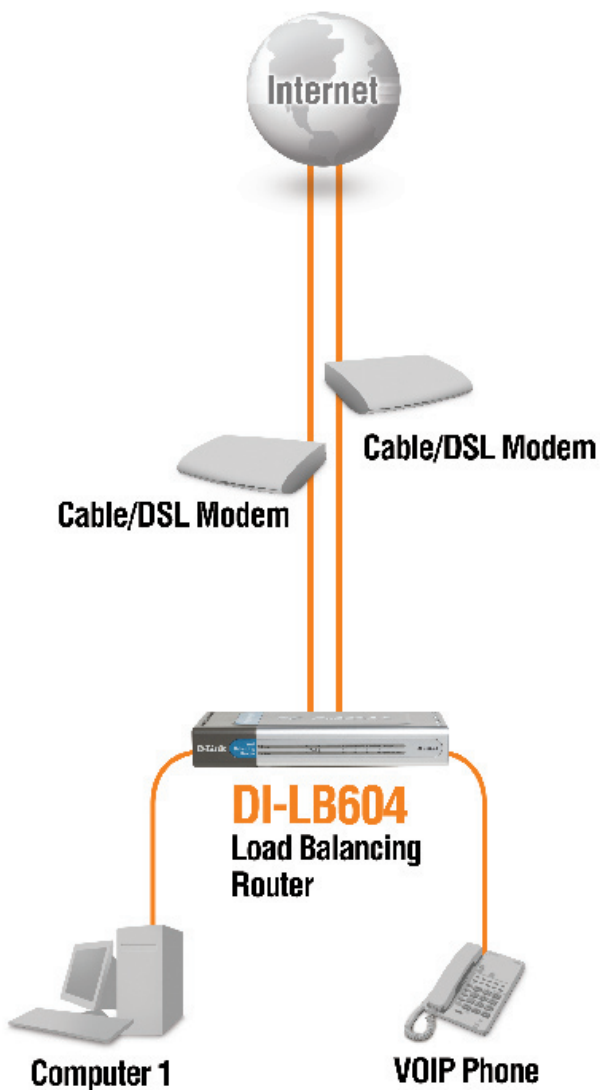
# LEDs





# Getting Started

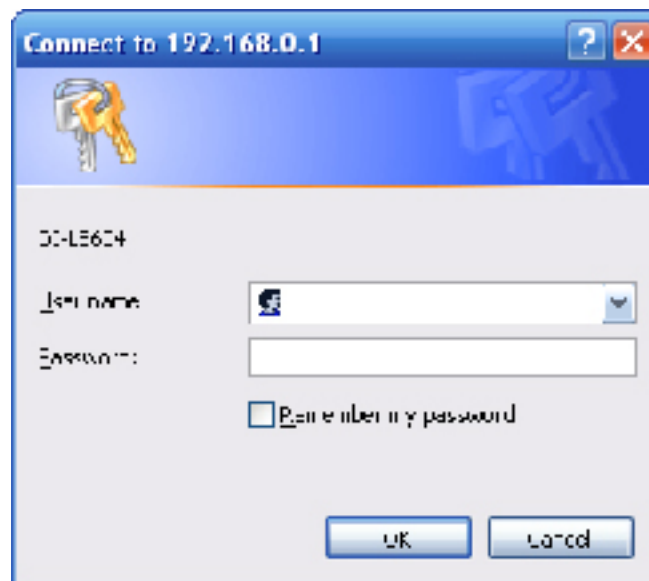
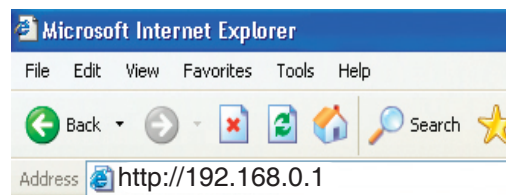
## Sample setup diagram:



# Using the Configuration Menu

When you want to configure your DI-LB604, you can access the configuration menu by opening a web-browser and typing in the IP address of the DI-LB604. The DI-LB604's default IP Address is 192.168.0.1

- Open a web browser.
- Type in the **IP address** of the router.



Note: If you have changed the default IP Address assigned to the DI-LB604, make sure to enter the correct IP address.

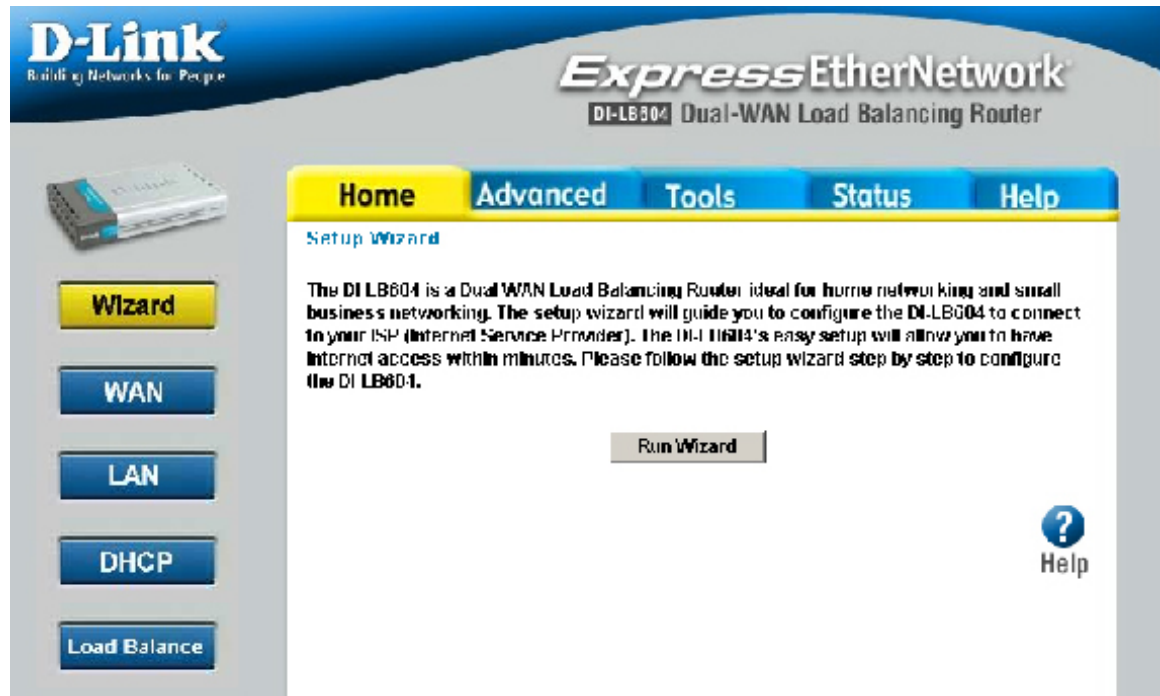
- Type "**admin**" for the User Name.
- Leave the **Password** blank.
- Click OK.

## Home

The Home tab provides the following configuration options: Wizard, WAN, LAN, DHCP, and Load Balance.

## Wizard

The Home>Wizard screen will appear. Please refer to the quick installation guide for more information regarding the setup wizard.



*Home > Wizard*

These buttons appear on most of the configuration screens in this section. Please click on the appropriate button at the bottom of each screen after you have made a configuration change.



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

# WAN

**Connection**

Interface:

Connect Mode:  Disable  Enable  Backup

Connect Type:

PPTP Connection:  Enable

Backup of: WAN2

**PPTP Dailup**

PPTP Server IP Address:

User Name:

Password:

Static IP Address:  (only for static ISP account)

PPTP MTU:  Bytes

**DNS (Optional for dynamic IP)**

Server 1:

Server 2:

Server 3:

**Optional**

Host Name:

Domain Name:

MAC Address:



Home > WAN

## Connection

**Connection Mode:**

There are three connection modes for each WAN port, Enable, Disable and Backup. Set to Disable if there is no modem connected to the WAN port. If both WAN ports are used, one is set to Enable and the other is set to Backup, the backup line will automatically be used when the other line is disconnected.

**Static IP:**

Select this if you want to specify a fixed IP address for the WAN port.

**Dynamic IP:**

Select this if you want the WAN port to get its IP address from a DHCP server.

**PPPoE:**


























Select this if you want the WAN port to get its IP address from a PPPoE server.

**PPTP Connection:**

To enable or disable PPTP connection on the WAN port.

**Backup of:**

To indicate which WAN port to be the backup of current port.

		
	<b>Address Information</b>	
	<b>Address Information:</b>	If you choose the connection type Static IP, then you have to fill in the information, IP address, Subnet Mask, and Gateway, provided by your ISP.
	<b>PPTP Dialup</b>	
	<b>Username / Password:</b>	These 2 fields must be completed if you are using PPPoE or PPTP dialup. If you are using PPTP dialup, remember you must select Static IP or Dynamic IP on Connection Type setup.
	<b>DNS</b>	
	<b>DNS (Domain Name Server):</b>	There are three entries available. It is necessary for those who are using static IP connected to the Internet. It is optional for those who are using dynamic IP or PPPoE.
	<b>Optional</b>	
	<b>Optional:</b>	If you still have trouble of connecting to the Internet, you may need to fill in this optional information. This information is most often used by Cable Modem services.
		
	<b>Host Name:</b>	The name of this device.
	<b>Domain Name:</b>	The specific name of this device on the Internet.
	<b>MAC Address:</b>	There is one default MAC Address for each WAN port of this device and it can be changed by user if necessary. (Cable Modem User may need this)
		
		
		
		
		
		
		
		
		
		
		
		

## Port Options

### Interface

WAN Port:

MTU:  Bytes

### Connection Health Check

Method: ICMP  HTTP  Traffic

Interval:  sec.

Alive Indicator:

### PPPoE/PPTP Connection

Auto Dialup:  Enable (Connection-on-demand)

Disconnect After Idle:  minutes (-1 Always-on)

Echo Time:  seconds

Echo Retry:  times

Go Back








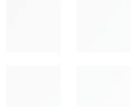

Home > WAN > Port Options

### Interface

- WAN Port:** Select the WAN port that you would like these port options to apply to.
- MTU:** The largest amount of data that can be transferred across a given physical network.

### Connection Health Check

- Connection Health Check:** There are three methods, **ICMP**, **HTTP** and **Traffic**, provided for device to check if WAN interfaces are connected to internet or not. A successful response of either method means that the connection is OK. If the chosen method fails, the connection is considered to be down.

	<p><b>Method:</b></p>	<p><b>ICMP:</b></p> <p>The health checking is performed by sending an ICMP echo request packet to the specific destination.</p> <p>The specific destination (“Alive Indicator”) could be either :</p> <ol style="list-style-type: none"> <li>1. if the input box is filled (NAME or IP address): the host is used.</li> <li>2. if the input box is left blank: gateway of wan interface will be used.</li> </ol> <p>If one ICMP echo reply packet from Alive Indicator or gateway is received, the connection is considered OK. If there are no response received after 4 tries, the connection is considered to be down.</p> <p><b>HTTP:</b></p> <p>The device gets a TCP connection with the Alive Indicator first. Then the device sends HTTP HEAD packet to the Alive Indicator. If any HTTP DATA from the Alive Indicator is received, the connection is considered OK. If there are no response received after 5 tries, the connection is considered to be down.</p> <p><b>Traffic:</b></p>
	<p><b>Interval:</b></p>	<p>The period to check if the WAN port is alive or not.</p>
	<p><b>Alive Indicator:</b></p>	<p>This is used for the ICMP or HTTP methods to determine if your Internet connection is active or not.(You can either fill-out the IP address or host name)</p>
<p><b>PPPoE / PPTP Connection</b></p>		
	<p><b>Auto Dialup:</b></p>	<p>To enable or disable auto dialup for a PPPoE/PPTP connection. If you decide not to use auto dialup or auto disconnect, then you have to connect/disconnect manually.</p>
	<p><b>Disconnect After Idle:</b></p>	<p>The amount of time the router will wait before it disconnects if there is no traffic on the connection. Enter -1 to keep the connection always alive. Enter 0 to enable ‘dial on demand by trigger’.</p>
	<p><b>EchoTime:</b></p>	<p>To determine how often an Echo request is sent to the PPPoE server. Normally, leave this setting as its default value.</p>
	<p><b>Echo Retry:</b></p>	<p>To determine the most times that the Echo request is allowed to be sent to the PPPoE server until getting a response. Normally, leave this setting as its default.</p>

# LAN

## LAN Settings

IP Address :

Subnet Mask :



Home > LAN

## LAN Settings

**IP Address:** This is the LAN IP address for this broadband router unit. Other computers on this LAN will see it as their gateway.

**Subnet Mask:** The subnet mask address must be the same as PCs on your LAN. The default subnet mask address is 255.255.255.0

# DHCP

DHCP Server :  Enable

Starting IP Address :

Ending IP Address :

Lease Time :  (min.)

DNS Server 1 IP for Client :

DNS Server 2 IP for Client :



Home > DHCP

## DHCP Server

**DHCP Server:** To activate DHCP Server function. If you have another DHCP server available on your network or your LAN IP are static, you should disable the DHCP Server function.

**Starting IP Address:** The Starting of the IP address range that will be leased to DHCP clients in device's LAN side.

**Ending IP Address:** The Ending of the IP address range that will be leased to DHCP clients in device's LAN side.



- Lease Time:** The amount of time for a DHCP server leased a IP address to a client.
- DNS Server 1 IP for Client:** The IP address of the first default DNS server for the client requesting DHCP.
- DNS Server 2 IP for Client:** The IP address of the second default DNS server for the client requesting DHCP.
- View DHCP List:** This button is linked to the page DHCP client List.
- Setting Static DHCP:** Click here to configure static DHCP.

## DHCP Client List

[DHCP Client List](#)



Host Name	IP Address	MAC Address	Type	Status	Time Left
simaste	192.168.1.7	00-11-09-2A-94-11	Dynamic	Lease:	15m:3s
mdk4sim	192.168.1.8	00-11-09-2A-94-12	Dynamic	Lease:	6m:3s
<b>DHCP Free Entry</b>					
27					

*Home > DHCP > View DHCP List*

### DHCP Client List Help

- DHCP Client List:** Lists the information about the hosts which have obtained an IP address from this router's DHCP server.

## Setting Static DHCP

### Static DHCP

Host Name :

MAC Address :

Reserved IP Address :

**Go Back**



### Static DHCP Client List

Name	MAC Address	Group	Reserved IP
------	-------------	-------	-------------

*Home > DHCP > Setting Static DHCP*

### Static DHCP

- Host Name:** This should be your computer name.
- MAC Address:** This is your computer's network adapter address. You can find this address by typing ipconfig /all under the command prompt mode of window NT /2000/XP, or winipcfg under window/95/98/Me's command prompt mode.
- Reserved IP Address:** The IP address you wish to assign to this host.

## Load Balance

### Load Balance Configuration

Enable:

Load Balance Base on: Bytes Tx + Rx

Loading Share: WAN 1 50 % WAN 2 50 %



### NAT Statistics

Interface	Status	Loading Share		Current Loading		
		Default	Current	Session	Byte	Packet
WAN 1	Disconnected	50 %	50 %	1	1	1
WAN 2	Disconnected	50 %	50 %	1	1	1

### Interface Statistics

Interface	Load Share	Overall Statistics		
		Received (KB)	Transmitted (KB)	Total (KB)
WAN 1	50 %	0 KB	0 KB	0 KB
WAN 2	50 %	0 KB	0 KB	0 KB



Home > Load Balance

### Load Balance Configuration

**Load Balance:** To determine how the traffic is shared among the WAN

**Enable:** This will allow you enable or disable the load balance

**Load Balance Base on:** Select the desired option to measure traffic.

**Loading Share:** Enter the desired percent of traffic load for each WAN port.

### NAT Statistics

**NAT Statistics:** The traffic statistics on NAT for WAN ports.

**Interface Statistics:** The traffic statistics on WAN ports.

# IPsec

**Tunnel List** -- Add New Policy --

---

**Tunnel Settings**

Tunnel Name

Tunnel State  Enable

Connection Type Static

WAN Binding WAN 1

---

**Local Net**

Local IP / Subnet  /

**Remote Net**

Remote IP / Subnet  /

**Remote Gateway**

Gateway IP / Domain

---

**Key Management**

Key Method AutoKey (IKE)

**Authentication**

Preshared Key

Local ID (Option) NONE

Remote ID (Option) NONE

---

**Action**

Continue Setup .. Delete

*Home > IPsec*

## Tunnel Settings

**Tunnel Name:**

Enter a name for the tunnel.

**Tunnel State:**

Check the box to enable tunnel state.

**Connection Type:**

Select Static or Dynamic from the drop-down menu.

**WAN Binding:**

Select WAN1 or WAN2 from the drop-down menu.

## Local Net

**Local IP/Subnet:**

Enter the local IP address and subnet for the local net.

**Remote Gateway/  
Client ID:**

Select an option from the drop-down menu. (Static only)

## Remote Net

**Remote IP/Subnet:**

Enter the remote IP address and subnet for the remote net.

## Remote Gateway

**Gateway IP/  
Domain:**

Enter the IP address of the remote gateway. (Static only)

**Remote Gateway/  
Client ID:**

Select IP address, domain name, or distinguished ID from the drop-down menu. Enter the value in the box. (Dynamic only)

**Key Management**

**Key Method:**

Select AutoKey (IKE) or Manual Key.

**Authentication**

**Preshared Key:**

Enter the preshared key. (AutoKey (IKE) only)

**Local ID (Option):**

Select an option from the drop-down menu. (Static only)

**Remote ID (Option):**

Select an option from the drop-down menu. (Static only)

After configuring the IPsec settings on this page, click on the Continue Setup button at the bottom of the page to go to the final page for IPsec settings. The final page will either show options for Manual Key or AutoKey, depending on what was selected (AutoKey is shown below; Manual Key follows).

**Phase 1**

Negotiation Type

DH Group

Encryption Method

Authentication Method

SA Lifetime  Seconds

**Phase 2**

Encapsulation Format

Encryption Method

Authentication Method

Perfect Forward Secrecy

Key Lifetime  
 In Time  Seconds  
 In Volume  Kbytes

**Advanced**

NetBIOS Broadcast  Enabled

NAT Traversal  Enabled

Auto Reconnected  Enabled

Passive Mode  Enabled

IKE Keep Alive (Ping)

**Action**



*Home > IPsec > Continue Setup (AutoKey (IKE) only)*

	<b>Phase 1</b>	
	<b>Negotiation Type:</b>	Select Main Mode or Aggressive Mode from the drop-down menu.
	<b>DH Group:</b>	Select a DH Group from the drop-down menu.
	<b>Encryption Method:</b>	Select DES or 3DES from the drop-down menu.
	<b>Authentication Method:</b>	Select MD5 or SHA1 from the drop-down menu.
	<b>SA Lifetime:</b>	Enter the SA lifetime in seconds.
	<b>Phase 2</b>	
	<b>Encapsulation Format:</b>	Select ESP or AH from the drop-down menu.
	<b>Encryption Method:</b>	Select NULL, DES, or 3DES from the drop-down menu.
	<b>Authentication Method:</b>	Select NULL, MD5, or SHA1 from the drop-down menu.
	<b>Perfect Forward Secrecy:</b>	Select No PFS or a DH Group from the drop-down menu.
	<b>Key Lifetime:</b>	Enter the Key lifetime in the fields for time and volume.
	<b>Advanced</b>	
	<b>NetBIOS Broadcast:</b>	Check the box to enable NetBIOS Broadcast.
	<b>NAT Traversal:</b>	Check the box to enable NAT Traversal.
	<b>Auto Reconnected:</b>	Check the box to enable Auto reconnect.
	<b>Passive Mode:</b>	Check the box to enable passive mode.
	<b>IKE Keep Alive (Ping):</b>	Enter the IP address for IKE keep alive (ping).
	<b>Action</b>	
	<b>Tunnel Test:</b>	Click the button to do a tunnel test.



**Manual Key Security Level**

Encapsulation Format

Encryption Method

Authentication Method

Encryption Key

Note : 8 ASCII Characters or 16 Hex Characters starting with 0x

Authentication Key

Note : 20 ASCII Characters or 40 Hex Characters starting with 0x

Inbound SPI

Note : Dec value or Hex value starting with 0x

Outbound SPI

Note : Dec value or Hex value starting with 0x

**Advanced**

NetBIOS Broadcast  Enabled

**Action**



*Home > IPsec > Continue Setup (Manual Key)*

**Manual Key Security Level**

<b>Encapsulation Format:</b>	Select AH or ESP from the drop-down menu.
<b>Encryption Method:</b>	Select NULL, DES, or 3DES from the drop-down menu.
<b>Authentication Method:</b>	Select NULL, MD5, or SHA1 from the drop-down menu.
<b>Encryption Key:</b>	Enter the encryption key.
<b>Authentication Key:</b>	Enter the authentication key.
<b>Inbound SPI:</b>	Enter a value for the Inbound SPI (Security Parameters Index).
<b>Outbound SPI:</b>	Enter a value for the Outbound SPI (Security Parameters Index).



**Advanced**

**NetBIOS  
Broadcast:**

Check the box to enable NetBIOS Broadcast.

**Action**

**Tunnel Test:**

Click the button to do a tunnel test.



# Advanced

The Advanced tab provides the following configuration options: Host IP, Static Routing, Virtual Server, Applications, Multi DMZ, Filters, QoS and NAT.

## Host IP

**Host Network Identity**

Host Name:

MAC Address: 00-00-00-00-00-00

Select Group: Data 1

Reserve in DHCP:  Enable

Reserved IP Address: 0.0.0

---

**Host Network Binding**

Binding WAN Port / Session:  Enable

Binding Method:  Strict Binding  Loose Binding

Select WAN Port: WAN 1

Select PPPoE Session: Session

**Host & Group List**

Name	MAC Address	Group	Reserved IP	Port/Session(PPPoE) Binding		
				Method	WAN	Seas.

*Advanced > Host IP*

### Host IP

**Host IP:**

The main purpose of this section is to define hosts on your LAN, and assign them to groups. Groups are used by the Access Filter and Block URL features. You can also bind multiple PPPoE sessions to individual hosts on the LAN.

### Host Network Identity

**Host Name:**

This should be your computer name.

**MAC Address:**

This is your computer's network adapter address. You can find this address by typing ipconfig /all under the command prompt mode of window NT /2000/XP, or winipcfg under window/95/98/Me's command prompt mode.

**Select Group:**

Select a group to assign the host to.

**Reserved IP Address:**

The IP address you wish to assign to this host.



**Host Network binding**

**Host Network binding:**

This is used only if you have multiple PPPoE sessions. Use this to ensure that a particular host always uses the same PPPoE session.

**Strict Binding:**

Only the bound interface is allowed to send packets for the specified host. If the bound interface is not available, no packet from the specified host can be sent.

**Loose Binding:**

In normal case, the packets from the specified host will be sent via the bound interface. If the bound interface is not available, the other interfaces are alternative.

**Host & Group List**

**Host & Group List:**

All the host entries you have made will be listed here.

# Static Routing

## Static Routing

**Network Address :**

**Netmask :**

**Gateway :**

**Interface :**

**Metric :**  (2~15)



## Routing List

Destination IP	Subnet Mask	Gateway	Interface	Metric	Type
----------------	-------------	---------	-----------	--------	------

*Advanced > Static Routing*

## Static Routing

### Static Routing:

If there is more than one router on a network, this Routing table must be configured because the router needs to know what packet goes to which router. A routing table entry is required for each LAN segment on the network.

### Network Address:

Network Address is the address of the destination network segment.

### Netmask:

The subnet mask used to select the bits from an IP Address that corresponds to the subnet.

### Gateway:

The IP router that the packets destined to the Network Address will be forwarded to.

### Interface:

The device's port that the packets destined to the Network Address will be passed through.

### Metric:

The number of routers that must be traversed to reach the destination network segment.

# Virtual Server

## Virtual Server

**Enable :**

**Server Name :**

**Private IP :**

**Protocol Type :**

**Private Port Range :**  ~

**Interface Binding :**

**Public Port Range :**  ~

**Allowed Remote IP :** From  To



### Virtual Server List

Name	Private IP	Protocol	Port Range	Binding	
<input type="checkbox"/> DNS	0.0.0.0	UDP	53~53/53~53	ALL	
<input type="checkbox"/> FINGER	0.0.0.0	UDP	79~79/79~79	ALL	

*Advanced > Virtual Server*

## Virtual Server

- Virtual Server:** This feature allows the servers (web server, mail server, FTP server, DNS, ... etc) on your LAN to be accessed from the Internet.
- Enable:** To activate or deactivate current entry.
- Server Name:** An unique name to identify the virtual server.
- Private IP:** Enter the IP address of the server on the device's LAN side. The hosts used as Virtual Servers should have a static IP address or a reserved IP address.
- Protocol Type:** Select the protocol (either TCP or UDP) used by the server software.
- Private Port Range:** The range of port numbers used by the server. If only one port number is used, fill the same number in both starting and ending fields.
- Interface Binding:** The WAN port that the virtual server is bound to.

**Public Port Range:** The range of port numbers for users in public to access the virtual server. If only one port number is used, fill the same number in both starting and ending fields.

**Allowed Remote IP:** The range of IP addresses that are allowed to access the virtual server.

## Applications

### Special Application

**Enable:**   
**Name:**   
**Trigger Port Range:**  0 ~  0  
**Trigger Type:**  TCP   
**Public Port Range:**  0 ~  0  
**Public Type:**  TCP



### Special Application List

Name	Trigger Port	Trigger Type	Public Port	Public Type
------	--------------	--------------	-------------	-------------

*Advanced > Applications*

### Special Application

**Special Application:** There are many special network applications that normally do not work behind a firewall. Due to network security considerations, only a few ports are open. Traffic using other ports is blocked. Here, you can choose to open other ports and allow the traffic which uses those ports.

### Special Application Configuration

**Special Application Configuration:** This section lets you enter the configuration data for the special application.

**Enable:** To activate or deactivate current entry.

**Name:** The name to identify the Special Application.

**Trigger Port Range:** The port number range to trigger the Special Application.

- Trigger Type:** The protocol to trigger the Special Application.
- Public Port Range:** The port range used in the connection from the Special Application server.
- Public Type:** The protocol used in the connection from the Special Application server.

**Special Application List**

- Special Application List:** Lists all the entries that have been created.

**Multi-DMZ**

**Multi DMZ Edit**

**Enable:**   
**WAN:** WAN 1   
**Name:**   
**DHCP:** DHCP  
**Private IP (LAN):** 0.0.0.0   
**Access Group:** Default   
**Direction:** Outgoing



**Multi DMZ List**

WAN	Name	Session / Public IP (WAN)	Private IP (LAN)	Access Group	Direction
-----	------	---------------------------	------------------	--------------	-----------

*Advanced > Multi DMZ*

**Multi DMZ**

- Multi DMZ (De-Militarized Zone):** This special function allows multiple Hosts on your LAN to be exposed to the Internet without any restrictions. This is useful for some network games, net meeting, or special applications. In order to enable these functions, you have to map one LAN IP address to one WAN IP address. However, because of the security risk, you should activate these functions only if they are necessary.
- Enable:** To activate or deactivate current DMZ entry.

- WAN:** The WAN port applied for current DMZ entry.
- Name:** To identify current DMZ entry.
- PPPoE Sess:** The PPPoE session that current DMZ entry is bound to.
- Private IP (LAN):** The IP address of the server in DMZ.
- Access Group:** To specify which Access Group will be applied. Each Access Group has its own access rules.
- Direction:** To specify that the Access Group will be applied in which way.

### Filters

#### Filters

- URL Blocking  Access Filter
- User-Defined Ports To Block

#### URL Blocking

Select Group :

URL List Type:

Index : 1

Enable :



#### List of Access Item

Index	URL / IP / Keyword On Web Site
-------	--------------------------------
















*Advanced > Filters*

#### URL Blocking

**URL Blocking:** If the URL, IP address or keyword entered here is found in the web page access packet from LAN users, the web page access will be blocked. You can have different restrictions for different groups. (Use the Host IP screen to assign Hosts to groups.)

#### Access Filters

**Access Filters:** To control the Internet access by LAN users.

	<b>Select One Group:</b>	The Group that current rule is applied to.
	<b>No Filtering:</b>	To allow all Internet access to LAN users.
	<b>Allow Selected Access only:</b>	To apply the rules defined in User-Defined Ports To Filter.
	<b>Block All Access:</b>	To prohibit all Internet access to LAN users.
	<b>Block Selected Items:</b>	To apply the rules defined in User-Defined Ports To Block.
	<b>ICMP Filters</b>	
	<b>ICMP Filters:</b>	To limit the ICMP activities initialized from LAN.
	<b>Block Selected Packet Types:</b>	To prohibit the selected types of ICMP packets from the LAN to be passed through the device.
	<b>Packet Types:</b>	The types of the ICMP packets that could be blocked.
	<b>User-defined Ports To Filter</b>	
	<b>User-defined Ports To Block:</b>	This lets you define custom ports to be filtered.
	<b>Enable:</b>	To activate or deactivate current rule.
	<b>Name:</b>	A unique name to identify current rule.
	<b>Protocol Type:</b>	The protocol to be blocked.
	<b>Port No. Range:</b>	The port number range to be blocked. (for TCP and UDP only ) If only one port number is used, enter the same port number in both fields.



# QoS

## QoS Features

Enable QoS:  Enable

Queuing Method:

## IP TOS(Type of Service) Features

Process TOS Field:  Enable

Overwrite Policy Priority:  Yes



*Advanced > QoS*

## QoS Setup

**Enable QoS:**

Users can choose to Enable QoS (Quality of Service). If set to “enable” QoS, the QoS will allow higher priority packets to pass through the device.

**Queuing Method:**

The methods for managing your queue. “Priority Queuing” is one of the first queuing variations to be widely implemented. This is based on the concept that certain types of traffic can be identified and shuffled to the front of the output queue so that some traffic is always transmitted ahead of other types of traffic.

**Process TOS Field:**

An 8 bits field in the IP packet header designed to contain values indicating how each packet should be handled in the network. If you choose “enable” then it will enable this function to process the IP Type of Service field.

**Overwrite Policy Priority:**

Choose “Yes” to enable the IP packet TOS field priority to overwrite the priority defined in the policy configuration.

## QoS Set Policy

### Policy Priority

**Policy Name:**   
**Local Address:** From  To   
**Remote Address:** From  To   
**Protocol Type:**   
**Source Port:** From  To   
**Destination Port:** From  To   
**Priority Queue:**



### Policy List

Policy Name	Source Address : Port	Destination Address : Port	Protocol	Queue
-------------	-----------------------	----------------------------	----------	-------

*Advanced > QoS > Set Policy*

Setting the QoS policy can assign received packets a higher/lower priority (based on your configuration) to pass through this device. You can define some policies which classify received packets based on local/remote IP addresses, ports and protocol type. This feature is useful when the WAN link is very busy or congested or when using special applications that need real time services such as Internet calling and video conference.

### QoS Policy

<b>Policy Name:</b>	The friendly name of a policy which is used to classify the received packets based on the following rules.
<b>Local/Remote Address:</b>	Specify a packet based on local/remote IP address. By default, the address is 0.0.0.0 which represents all IP Addresses. Port and Protocol Type define all packets for special applications.
<b>Protocol Type:</b>	This field is defined for which type of packet. It has some values such as IP, TCP and UDP.
<b>Source/Destination Port:</b>	Specify the port number ranges if TCP or UDP protocol is selected.
<b>Priority Queue:</b>	This device supports four queues. When a packet meets a policy rule requirement, it will be put into the responding queue. Otherwise it is assigned the lowest priority to pass through.

# NAT

## NAT Configuration

**NAT Routing :**  Enable

**TCP Timeout :**  seconds

**UDP Timeout :**  seconds

**TCP Window Limit :**  (0 for no limit)

**TCP MSS Limit :**  (0 for no change)

## non-Translation Port Range

State	Port Range	Timeout
<input checked="" type="checkbox"/> Enable	<input type="text" value="1025"/> ~ <input type="text" value="61439"/>	<input type="checkbox"/> Enable <input type="text" value="0"/> seconds
<input type="checkbox"/> Enable	<input type="text" value="0"/> ~ <input type="text" value="0"/>	<input type="checkbox"/> Enable <input type="text" value="0"/> seconds
<input type="checkbox"/> Enable	<input type="text" value="0"/> ~ <input type="text" value="0"/>	<input type="checkbox"/> Enable <input type="text" value="0"/> seconds
<input type="checkbox"/> Enable	<input type="text" value="0"/> ~ <input type="text" value="0"/>	<input type="checkbox"/> Enable <input type="text" value="0"/> seconds
<input type="checkbox"/> Enable	<input type="text" value="0"/> ~ <input type="text" value="0"/>	<input type="checkbox"/> Enable <input type="text" value="0"/> seconds

**Set NAT Alias**



*Advanced > Nat*

### NAT Configuration:

**NAT Routing:**

To enable or disable NAT routing by checking or unchecking the checkbox. If you disable NAT routing, this device will act as a Bridge or Static Router. Most features, including Load Balance, will be unavailable. If some packets whose port number cannot be translated for special applications, you must input value in port range for Disable Port Translation.

**TCP Timeout:**

During the time that TCP expects to receive the acknowledgement from the destination.

**UDP Timeout:**


During the time that UDP expects to receive the acknowledgement from the destination.

**TCP Window Limit:**

The maximum number of outstanding packets before TCP receiving an acknowledgement.

**TCP MSS Limit:**

The largest amount of data that can be transmitted in one TCP packet.

	<b>NAT Port Options</b>	
	<b>Port Range:</b>	The Source Port Number Range for TCP and UDP protocol.
	<b>Non-Port-Translation:</b>	To keep the source port number unchanged for TCP/UDP sessions on the specified Port Range. Some special applications do not allow the source port number to be translated.
	<b>Specific TCP / UDP Timeout:</b>	To define specific Timeout for TCP/UDP sessions on the specified Port Range.
	<b>Set NAT Alias</b>	
	<b>Set NAT Alias:</b>	The link to NAT Alias setting page.
	<b>NAT Alias:</b>	For each alias entry , the Wan IP acts as an alias IP of the host with Local Lan IP to internet via the specified WAN port for the specified Protocol packets. i.e. 1-1 NAT.
	<b>Enable:</b>	To activate or deactivate current entry.
	<b>Local Lan IP:</b>	The IP address of the host in LAN that wants to use the specific WAN IP as its source IP.
	<b>Wan IP:</b>	The IP address used as the source IP of the packets out from the specified host.
	<b>Protocol:</b>	The protocol that current rule is applied for.
	<b>WAN:</b>	The WAN port that current rule is applied for.
	<b>Back:</b>	The link to NAT Configuration page.

# Tools

The Tools tab provides the following options: Admin, Time, System, Firmware, Email Alert, SNMP, DDNS, UPNP and Misc.

## Admin

### Administrator Settings

Administrator (if Login Name is 'admin')

New Password:

Confirm Password:

### Remote Management

Remote Upgrade:  Enable

Remote Setup:  Enable

Allowed Remote IP:  ~

Access Port:



*Tools > Admin*

### Administrator Settings

**New Password /  
Confirm Password:**

This administrator password protects the configuration for this broadband router. It is recommended that you set a password to prevent other people change the router's configuration.

### Remote Management

**Remote Upgrade:**

To allow or disallow users to upgrade the firmware of the device through the web page remotely.

**Remote Setup:**

To allow or disallow users to setup the configuration of the device through the web page remotely.

**Allowed Remote  
IP:**

Only the requests from the hosts that its IP address is within the range of the Allowed Remote IP are allowed to Upgrade or Setup remotely.

**Access Port:**

The specific port number used for users to Upgrade or Setup the device remotely.

# Time

## Time

Local Time : Jan/01/2000 00:22:13

Time Zone : (GMT-12:00) Kwajalein

Default NTP Server 1 :

Default NTP Server 2 :

Default NTP Server 3 :

Set the Time : Year  Month  Day

Hour  Minute  Second



## NTP Configuration

### Time Zone:

To specify one time zone from the time zone list that lists all time differences between GMT and each local time zone.

### NTP Servers:

Up to 3 NTP servers can be used for the device to receive the time and date in Greenwich Mean Time (GMT), you can enter its IP or Domain address here.

# System

## System Setting

Save Settings To Local Hard Drive



## Load Settings

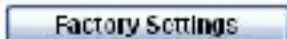
User Name : admin

Password :

Load Settings From Local Hard Drive

Restore To Factory Default Settings



Tools > System

**System Setting**

**Save Settings To Local Hard Drive:**

You can save current system configuration as a text file on a local hard disk, and then use the saved configuration file to upgrade another device later.

**Load Settings**

**Load Settings:**

You can Load the Settings through this web page.( If you are using remote Load, you have to enable "Remote Upgrade" and "Remote Setup" from the Admin page first).

**User Name / Password:**

Enter a password which will be used to login to the router.

**Load Settings From Local Hard Drive:**

Select the configuration file from local hard disk.

**Restore To Factory Default Settings:**

To restore the factory settings to system configuration.

**Firmware**

**Upgrade Firmware**

User Name : admin  
Password :

Upgrade Software From Local Hard Drive



*Tools > Firmware*

**Upgrade Firmware**

**Upgrade Firmware:**

You can upgrade new firmware through this web page.( If you are using remote upgrade, you have to enable "Remote Upgrade" and "Remote Setup" from the Admin page first).

**User Name / Password:**

The password will be authenticated for firmware upgrade.

**Upgrade Software From Local Hard Drive:**

Select the firmware file from local hard disk.

# Email Alert

## Global Settings: Notification on

**Email Alert Enable:**  Enable (Link Down)  
**Excessive Ping:**  Enable  
 MAX. Pings Before Notification:  Times/min.

## Email Alert Configuration

**Interface:** WAN 1  
**Email Server Address:**   
**User Name:**   
**Password:**   
**Sender Address:**   
**Recipient Address:**



## Email Alert Configuration List

Interface	Mail Server	User Name	
	Sender Addr.	Recipient Addr.	
WAN 1			
WAN 2			

*Tools > Email Alert*

## Global Settings Notification on

**Email Alert Enable:** To enable or disable the Email Alert in case that one of the WAN ports is disconnected.

**Excessive Ping:** This function is useful to prevent ICMP packets attacks, from WAN or LAN, on the device. It will drop the packets if the ping times are excessive the threshold value Max. Pings Before Notification. And it will send e-mail to notify the administrator if Email Alert is enabled.

## Email Alert Configuration

**Email Alert Configuration:** The purpose of email alert is when any of WAN ports is disconnected or malfunction, it will send an email message to inform of the recipient.

**Email (SMTP) Server Address:** The e-mail server address (ex. mail.yourdomain.com)

**User Name:** The user name of the e-mail address used for authentication.

**Password:** The password of the e-mail address used for authentication.

**Sender Address:** The email address of the sender.



**Recipient Address:** The email address of the receiver.

**Send Test E-mail:** Click this button will send a test e-mail in order to verify the settings are correct.

## SNMP

### System Information


**Contact Person :**

**Device Name :**


**Physical Location :**

### Community

**Community Name 1 :**

**Access Control 1 :**  

**Community Name 2 :**

**Access Control 2 :**  

### Trap Targets

**Target IP Address 1 :**  ( ex. xxx.xxx.xxx.xxx )

**Target IP Address 2 :**

**Target IP Address 3 :**



*Tools >SNMP*

### SNMP (Simple Network Management Protocol)

**SNMP:** This page only useful if you an SNMP program which you can use to access the Router and receive the trap alerts.

**System Information:** This is the system information which will identify this device.

**Community:** It is a relationship between an SNMP agent and a set of SNMP managers that defines authentication, access control, and proxy characteristics.

**Trap Targets:** Up to three IP address can be entered. Trap information will be sent to these addresses.

# DDNS

## Dynamic DNS Service

Service :

Server Name :

User Name :

Password :

Verify Password :

Domain Name :

## Additional Settings :

Enable Wildcard :

Enable Backup MX :

Mail Exchanger :

## WAN Port Binding



*Tools > DDNS*

## Dynamic DNS

### Dynamic DNS:

This is a technology that people can use to connect to your router using a domain name, instead of an IP address, even if you have a dynamic IP address from your ISP (instead of a static IP address).

## Dynamic DNS Service

### Service:

To specify the service provider.

### Server Name:

The name of the DDNS server.

### User Name:

The username to login to the DDNS server.

### Password:

The password to login to the DDNS server.

### Verify Password:

Re-enter the password to prevent the typing error.

### Domain Name:

The complete hostname to be updated.

## Additional Settings

### Enable Wildcard:

If enabled, all subdomains of your domain name maps to your current IP address. If disabled, no subdomains of your domain name have an IP address.

	<b>Enable Backup MX:</b>	Enable Backup to allow the use of Mail Exchanger.
	<b>Mail Exchanger:</b>	Define mail exchanger for the domain name. If omitted, the mail exchanger will be set to the domain name.
	<b>WAN Port Binding</b>	
	<b>WAN Port Binding:</b>	If bound on the WAN port, the domain name will be mapped to the IP address of the WAN port.
	<b>UPnP</b>	
	<b>UPnP Option</b>	
	<b>UPnP :</b> <input checked="" type="radio"/> Enable <input type="radio"/> Disable	
		<i>Tools &gt;UPnP</i>
	<b>UPnP Option</b>	
	<b>UPnP Option:</b>	With the UPnP (Universal Plug & Play) function, you can easily setup and configure an entire network, enable discovery and control of networked devices and services.
	<b>UPnP Port Mapping List:</b>	You can set the dynamic port mappings to Internet gateway via UPnP on Windows XP. This will allow you make a connection between applications and the defined device.

## Misc.

### External Filters Configuration

Block Selected ICMP Types

Packet Types:  Echo Request  Time-exceeded Request  
 Information Request  Address Mask Request

### DNS Loopback

Domain Name	Private IP	Domain Name	Private IP
<input type="text"/>	<input type="text" value="0.0.0.0"/>	<input type="text"/>	<input type="text" value="2.0.2.0"/>
<input type="text"/>	<input type="text" value="         "/>	<input type="text"/>	<input type="text" value="     "/>
<input type="text"/>	<input type="text" value="0.0.0.0"/>	<input type="text"/>	<input type="text" value="2.0.2.0"/>
<input type="text"/>	<input type="text" value="0.0.0.0"/>	<input type="text"/>	<input type="text" value="2.0.2.0"/>
<input type="text"/>	<input type="text" value="0.0.0.0"/>	<input type="text"/>	<input type="text" value="2.0.2.0"/>

### Application

System Restart:

IDENT Port:  Enable (Make it seem closed, not stealth)

SMTP Binding:  Enable

SMTP Binding Port:

IPSec Passthrough:  Enable  Max Tunnels

PPTP Passthrough:  Enable  Max Tunnels



Tools > Misc

### External Filters Configuration

**External Filters Configuration:**

To limit the packets passing through the device from WAN side to LAN side.

**IDENT Port:**

This port provides a means to determine the identity of a user on a particular TCP connection. By default, the device is stealth for this port. Enable to make this port closed, not stealth.

**Block Selected ICMP Types:**

To prohibit the selected types of ICMP packets from WAN to be passed through the device.

		<b>Packet Types:</b>	The types of the ICMP packets that could be blocked.
		<b>System Restart</b>	
		<b>System Restart:</b>	The link to the page to restart system.
		<b>DNS Loopback</b>	
		<b>DNS Loopback:</b>	If there is any domain in your private network. You can setup the mapping table of Domain Name & Private IP for DNS query.
		<b>Interface Binding</b>	
		<b>SMTP Binding:</b>	To determine if the SMTP packets are bound on the WAN port.
		<b>SMTP Binding Port:</b>	To specify the WAN port that your SMTP traffic is only transmitted on. It could be that you have two accounts from two different ISP. It is best to use only one.
		<b>IP Sec/PPTP:</b>	Enable this to allow UPN connections from PCs on the LAN to senders.
		<b>Set Protocol &amp; Port Binding</b>	
		<b>Set Protocol &amp; Port Binding:</b>	To determine if the SMTP packets are bound on the WAN port.
		<b>Protocol &amp; Port Binding</b>	
		<b>Protocol &amp; Port Binding:</b>	It is very like SMTP binding, but you must setup extra data like Protocol & Port Range. If all the checking items are met, the packet will be bound on the specified WAN port.
		<b>Enable:</b>	To activate or deactivate current rule.
		<b>Source IP:</b>	The IP address that the packet's source IP will be checked against.
		<b>Dest. IP / IP Address:</b>	The specific IP range that the packet's destination IP will be checked against. There are two forms of Dest. IP: If Subnet is selected, the fields IP Address and Subnet Mask need to be filled. If IP Range is selected, the fields From and To need to be filled.
		<b>Protocol:</b>	The protocol that the packet's protocol will be checked against.
		<b>Port Range:</b>	The specific port number range that the packet's destination port number will be checked against.
		<b>WAN:</b>	The specific WAN port that the packet will be bound on if all the checking items are met.
		<b>Back</b>	
		<b>Back:</b>	The link to the main page of Advanced Feature.

# Status

The Status tab provides the following options: Device Info, Log, and Stats.

## Device Info

**Device Information**

Firmware Version: Ver 2.0 Rel 10 Beta11 Built Date: Aug 30 2005

Interface	Connection Type	Status	MAC Address
WAN1	Ethernet	Connected	00:09:83:10:22:01
WAN2	PPPoE <input type="button" value="Connect"/>	Disconnected	00:09:83:10:22:02

Interface	IP Address	Subnet Mask	Gateway	DNS IP Address
WAN1	0.0.0.0	0.0.0.0	0.0.0.0	4.2.2.2
WAN2	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0

Interface	IP Address	Subnet Mask	MAC Address	DHCP Server
LAN	192.168.1.1	255.255.255.0	00:09:83:00:22:DE	Enable



*Status > Device Information*

### Device Information

#### Device Information:

This page describes the device's interfaces (WAN ports and LAN port) settings and status.

- Connect/Disconnect: Connect or disconnect PPPoE session immediately.
- Force Renew: Renew DHCP lease immediately.

# Log

[View Log](#)



Message Status: 0 messages send, 22 messages unsend

Time	Priority	Module	Messages
0 01:33:16	Info.	dhcp	Send DHCP ACK to LAN (00:11:09:2A:94:11).
0 01:33:16	Info.	dhcp	Receive DHCP Request from LAN (00:11:09:2A:94:11).

*Status > Log*

## View Log

### View Log:

The device keeps a running log of events and activities occurring on the device. The log will display up to 100 recent logs. Newer log activities will overwrite the older logs. When the device is rebooted, the logs are automatically cleared.

## Log Settings

### Syslog Delivery

Sending Out:  Enable

Keep Send Message:  Enable

	Enable	IP Address	Port (Default:514)	Log Priority Level
Syslog Server 1	<input type="checkbox"/>	0.0.0.0	514	Emerg.
Syslog Server 2	<input type="checkbox"/>	0.0.0.0	514	Emerg.
Syslog Server 3	<input type="checkbox"/>	0.0.0.0	514	Emerg.

### Log Priority for Modules

KERNEL	Info	MAIL	Info	AUTH	Emerg.	SYSDLOG	Info
SECURITY	Warning	NTP	Emerg.	AUDIT	Emerg.	PPPCE	Info
PPP	Info	PPPTF	Info	RF	Info	SLMP	Info
DRD	Info	LLD	Info	LLDP	Info	LDN	Info
UIFD	Info	MAIL	Emerg.	MAIL	Info		

*Status > Log > Log Settings*

## Syslog Delivery

### Sending Out:

If checked, device will send syslog messages to other machine (log servers). Note: Even you uncheck it, the system will generate log messages.

### Keep Sent Messages:

If checked, the sent messages will be kept on device, otherwise the sent message will be deleted.

### Syslog Servers:

- IP Address:

Up to 3 syslog servers can be used.

- Enable:

If checked, the log message will be sent to the server. You can disable or enable each server temporarily.

- Port:

If your syslog server does not use the default port (514), change it.

- Log Priority Level:

The messages are grouped into 8 priority levels, from Emergency to Debug. The lower level it is, the fewer messages it will generate. Emergency is the lowest priority level, and Debug is the highest one. So set priority to Debug will send all generated messages.

## Log Priority for Modules

### Log Priority for Modules:

This feature displays and controls current log priority for each module. For a module with different priorities, the different level of messages will be generated in Syslog. The lower level of log priority for module is, the more messages will be generated. DEBUG is the lowest level of log priority.

### Message Status:

Messages sent will be kept only when “Keep Sent Messages” checked. Currently we keep last 100 messages in RAM area, reboot or power-off will clear them.

- Clear All: Use this button to clear all unsent messages.

- Submit: It will validate the new settings.

- Reset: It will reserve current settings in flash.

- View Syslog: It will display current messages in Syslog.



# Stats

Statistics



## NAT Statistics

Interface	Status	Loading Share		Current Loading			Current Bandwidth	
		Default	Current	Session	Byte	Packet	Download	Upload
WAN 1	Disconnected	50 %	50 %	1	1	1	0 Bps	0 Bps
WAN 2	Disconnected	50 %	50 %	1	1	1	0 Bps	0 Bps

## Interface Statistics

Interface	Load Share	Overall Statistics		
		Received (KB)	Transmitted (KB)	Total (KB)
WAN 1	0 %	0 KB	0 KB	0 KB
WAN 2	0 %	0 KB	0 KB	0 KB

*Status > Statistics*

### Refresh

**Refresh:** Get the newest statistics data.

### Restart Counters

**Restart Counters:** Clear all the statistics counters to 0.

### Check NAT Detail:

The link to NAT Status page.

### NAT Statistics

**Connection Status:** Check if WAN1 and WAN2 ports are connected or disconnected.

### Default Loading Share:

Display the default traffic loading between WAN1 and WAN2 ports.

### Current Loading Share:

Display current traffic loading between WAN1 and WAN2 ports.

### Current Loading:

The number of sessions, Bytes and Packets currently being processed on each port.

### Current bandwidth:

Current Download and Upload speeds on each WAN port.



**Interface Statistics**

**Interface Statistics:**

**Load Share:**

**Overall Statistics:**

This section displays cumulative statistics.

Current traffic loading in percent, including the traffic for device itself, on each WAN port.

•Received:  
Current incoming traffic loading in KByte, including the traffic for device itself, on each WAN port.

•Transmitted:  
Current outgoing traffic loading in KByte, including the traffic for device itself, on each WAN port.

•Total:  
Current traffic loading in KByte, including the traffic for device itself, on each WAN port.

# NAT Status

NAT Status



Refresh

Go Back

## NAT Timeouts

TCP	300
UDP	120

## TCP Property

Max. Segment Size	0
Max. Windows Size	11

NAT Traffic	Local To Internet	Internet To Local
Bytes	-	-
Packets	-	-

## Connections

TCP	-
UDP	-
ICMP	-
Created	-
Deleted	-

View Connection List

## Errors

Checksum	-
Retries	-
Bad Packets	-

## Misc.

Total IP Packets	2257
Reserved Address	2

Status > Statistics > NAT Status

### NAT Status

**Refresh:**

Get the newest status information.

**View Connection List:**

The link to NAT Connection List page.

**NAT Timeouts:**

This displays the current timeout values for TCP and UDP connections.



- TCP Property:** This displays the MSS (Maximum Segment Size) and Maximum Windows size for TCP packets.
- NAT Traffic:** This section displays statistics for both outgoing (LAN to Internet) and Incoming (Internet to Local) traffic.
- Connections:** This displays the current number of active connections. For further details, click the View Connection list button.
- Errors:** Statistics are displayed for Checksum errors, number of retries, and number of bad packets.
- Misc:** This displays the total IP packets and reserved address.
- NAT Connection List:** To display the information and status of all the entries in NAT table.

## NAT Connection List

[NAT Connection List](#)



Index	Interface Protocol	State Destination Address	Wan Address Local Address	Idle	Packets Out/In
-------	-----------------------	------------------------------	------------------------------	------	-------------------

*Status > Statistics > NAT Status > View Connection List*

## Troubleshooting

This section provides solutions to problems that can occur during the installation and operation of the DI-LB604 router. We cover various aspects of the network setup, including the network adapters. Please read the following if you are having problems.

Note: It is recommended that you use an Ethernet connection to **configure the DI-LB604 router**.

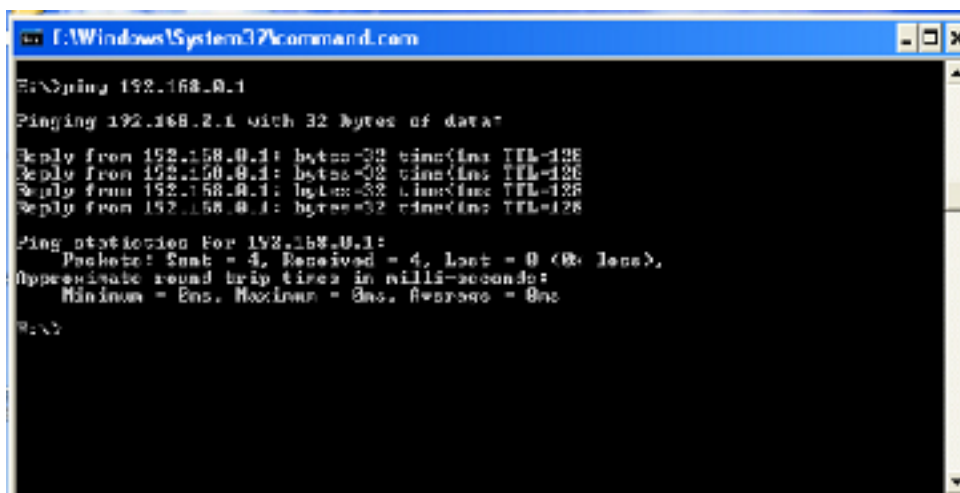
**The computer used to configure the DI-LB604 cannot access the Configuration menu.**

- Check that the **Ethernet LED** on the DI-LB604 is **ON**. If the **LED** is not **ON**, check that the cable for the Ethernet connection is securely inserted.
- Check that the Ethernet Adapter is working properly. Please see item 3 (**Check that the drivers for the network adapters are installed properly**) in this **Troubleshooting** section to check that the drivers are loaded properly.
- Check that the **IP Address** is in the same range and subnet as the DI-LB604. Please see **Checking the IP Address in Windows XP** in the **Networking Basics** section of this manual.

Note: The IP Address of the DI-LB604 is 192.168.0.1. All the computers on the network must have a unique IP Address in the same range, e.g. 192.168.0.x. Any computers that have identical IP Addresses will not be visible on the network. They must all have the same subnet mask, e.g. 255.255.255.0.

- Do a **Ping test** to make sure that the DI-LB604 is responding. Go to **Start>Run>Type Command>Type ping 192.168.0.1**. A successful ping will show four replies.

Note: If you have changed the default IP Address, make sure to ping the correct IP Address assigned to the DI-LB604.



```
F:\Windows\System32\cmd.exe
E:\>ping 192.168.0.1
Pinging 192.168.2.1 with 32 bytes of data:
Reply from 192.168.0.1: bytes=32 time=1ms TTL=128
Reply from 192.168.0.1: bytes=32 time=1ms TTL=128
Reply from 192.168.0.1: bytes=32 time=1ms TTL=128
Reply from 192.168.0.1: bytes=32 time=1ms TTL=128

Ping statistics for 192.168.0.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milliseconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
E:\>
```

To hard-reset the DI-LB604 to Factory Default Settings, please do the following:

- Locate the **Reset** button on the back of the DI-LB604.
- Use a paper clip to press the **Reset** button.
- Hold for about 10 seconds and then release.
- After the DI-LB604 reboots (this may take a few minutes) it will be reset to the factory **Default** settings.

### **Resetting the DI-LB604 to Factory Default Settings**

After you have tried other methods for troubleshooting your network, you may choose to **Reset** the DI-LB604 to the factory default settings.

# Technical Specifications

## VPN Pass Through/ Multi-Sessions

- PPTP
- IPSec

## VPN Security Support

- IKE Phase 1:
  - Cipher algorithm type key exchange: 3DES
  - Message digest for key exchange: MD5
  - Authentication method: Pre-shared key
  - DH group: 2
  - IKE SA lifetime: 120 min.
  - IKE negotiation mode: Main
- IKE Phase 2:
  - IPsec type: ESP
  - Cipher algorithm: 3DES
  - Method digest algorithm: MD5
  - Compression algorithm: None
  - IPsec tunnel lifetime: 120 min.
- VPN Encryption Policy:
  - Security association granularity per: Net
  - IPsec mode: IKE

## Device Management

- Web-based: Internet Explorer v6 or later; Netscape Navigator v7 or later; or other Java-enabled browsers
- DHCP Server and Client

## Advanced Firewall Features

- NAT with VPN Passthrough (Network Address Translation)
- MAC Filtering
- URL Filtering
- Scheduling

## Operating Temperature

- 32°F to 131°F (0°C to 55°C)

**Humidity:**

- 95% maximum (non-condensing)

**Safety and Emissions:**

- FCC

**LEDs:**

- Power
- Status
- LAN (10/100)
- WAN

**Physical Dimensions:**

- L = 7.56 inches (192mm)
- W = 4.65 inches (118mm)
- H = 1.22 inches (31mm)

**Power Input:**

- External power supply DC 5V, 3A

**Weight:**

- 10.8 oz. (0.3kg)

**Warranty:**

- 1 year



# Frequently Asked Questions

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

When entering the IP Address of the DI-LB604 (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 the web-based 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:

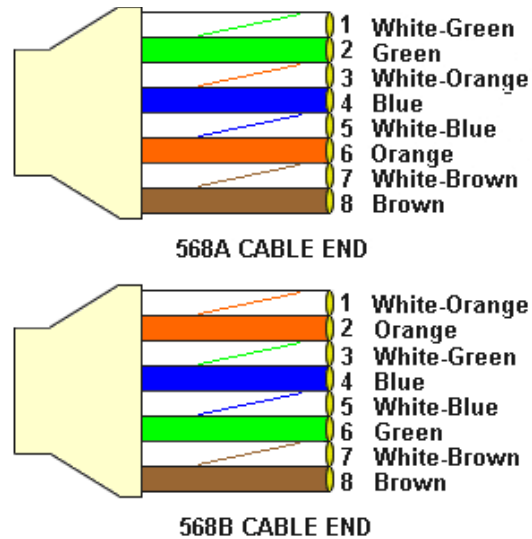
- Computer to Residential Gateway/Router
- Computer to Normal Port (hub/switch)
- Access Point to Normal Port (hub/switch)
- Print Server to Normal Port (hub/switch)
- Uplink Port to Normal Port (hub/switch)

Rule of Thumb:

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

### What'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 a straight-through cable from a crossover cable:**

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

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

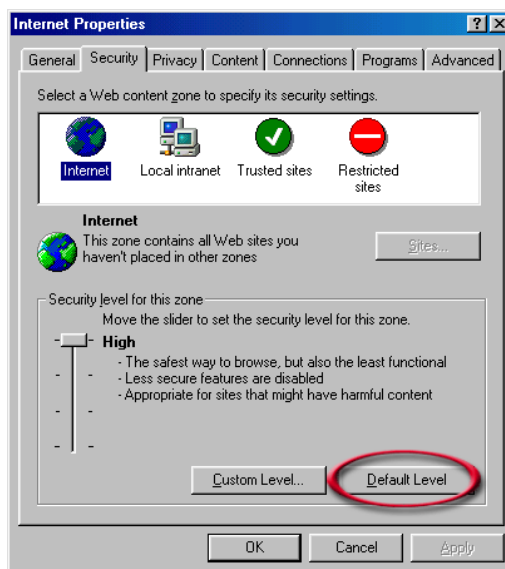
Hub/Switch uplink port to another Hub/Switch uplink port – Crossover

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

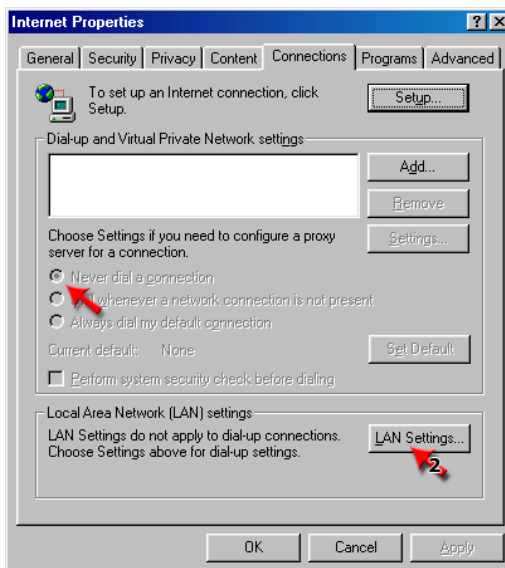
**Step 2:** Disable any Internet security software running on the computer. Software firewalls like Zone Alarm, Black Ice, Sygate, Norton Personal Firewall, etc. might block access to the configuration pages. Check the help files included with your firewall software for more information on disabling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

**Step 3:** Configure your Internet settings.

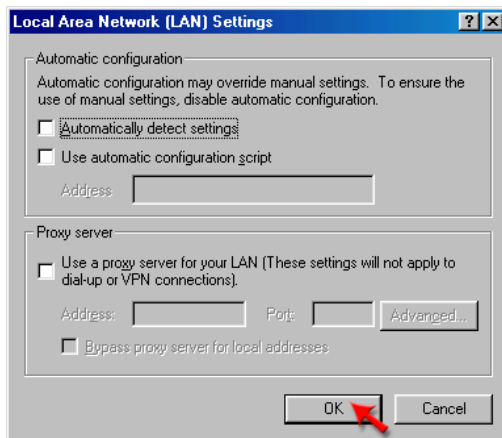
- Go to **Start>Settings>Control Panel**. Double click the **Internet Options** icon. From the **Security** tab, click the button to restore the settings to their defaults.



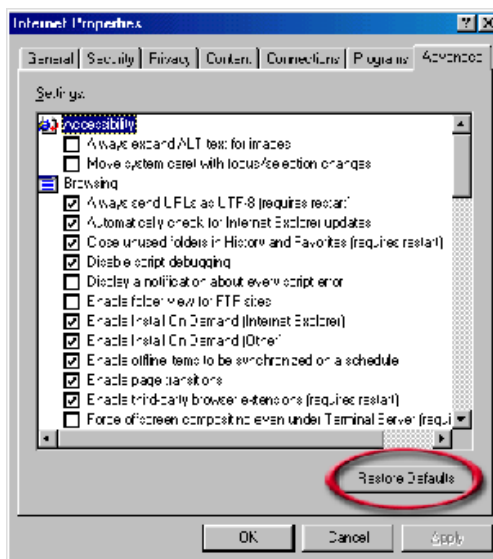
- Click to the **Connection** tab and set the dial-up option to **Never Dial a Connection**. Click the **LAN Settings** button.



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



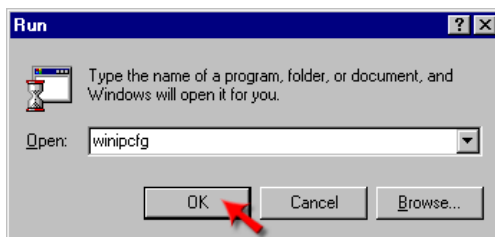
- Go to the **Advanced** tab and click the button to restore these settings to their defaults.
- Click **OK**. Go to the desktop and close any open windows.



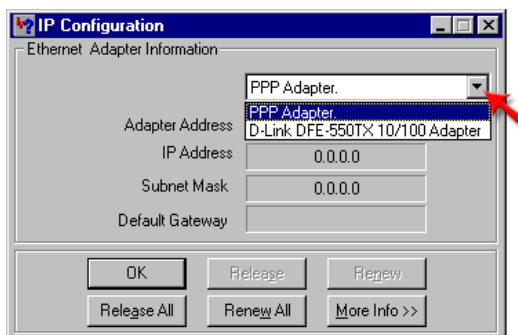
**Step 4:** Check your IP Address. Your computer must have an IP Address in the same range of the device you are attempting to configure. Most D-Link devices use the 192.168.0.X range.

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

- Click on **Start**, then click on **Run**.
- The Run Dialogue Box will appear. Type **wiipcfg** in the window as shown then click **OK**.



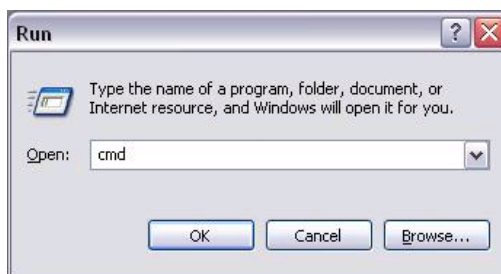
- The **IP Configuration** window will appear, displaying your **Ethernet Adapter Information**.
- Select your adapter from the drop down menu.
- If you do not see your adapter in the drop down menu, your adapter is not properly installed.



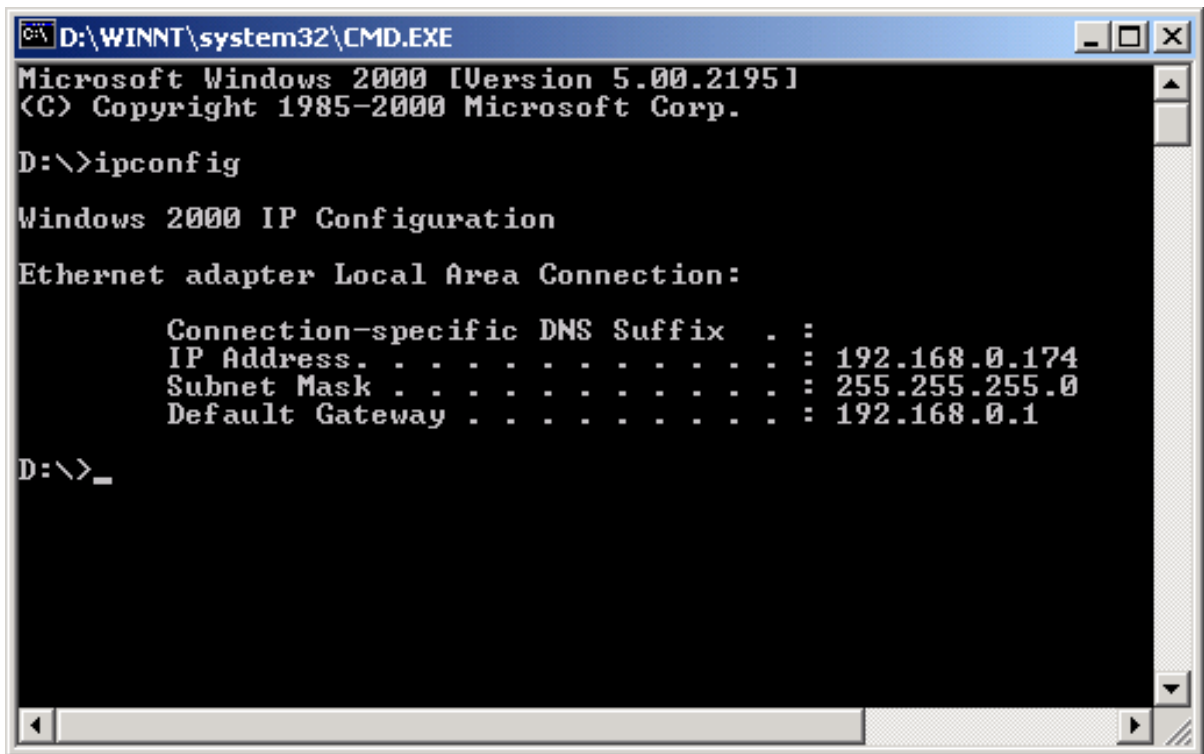
- After selecting your adapter, it will display your IP Address, subnet mask, and default gateway.
- Click **OK** to close the IP Configuration window.

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

- Click on **Start** and select **Run**.
- Type **cmd** then click **OK**.



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



```
D:\WINNT\system32\CMD.EXE
Microsoft Windows 2000 [Version 5.00.2195]
(C) Copyright 1985-2000 Microsoft Corp.

D:\>ipconfig

Windows 2000 IP Configuration

Ethernet adapter Local Area Connection:

    Connection-specific DNS Suffix  . :
    IP Address. . . . .               : 192.168.0.174
    Subnet Mask . . . . .             : 255.255.255.0
    Default Gateway . . . . .         : 192.168.0.1

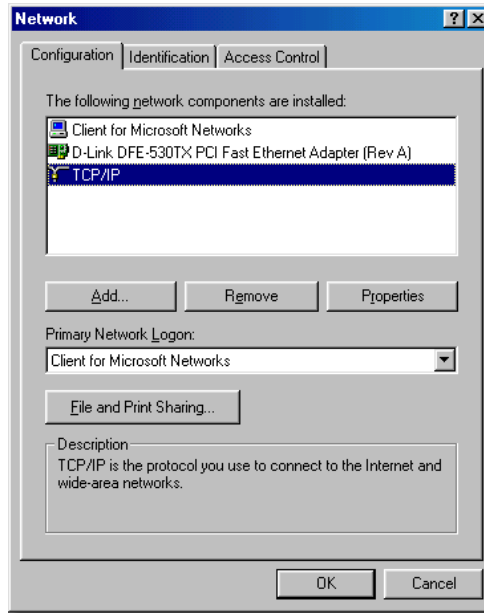
D:\>_
```

- Type **exit** to close the command prompt.

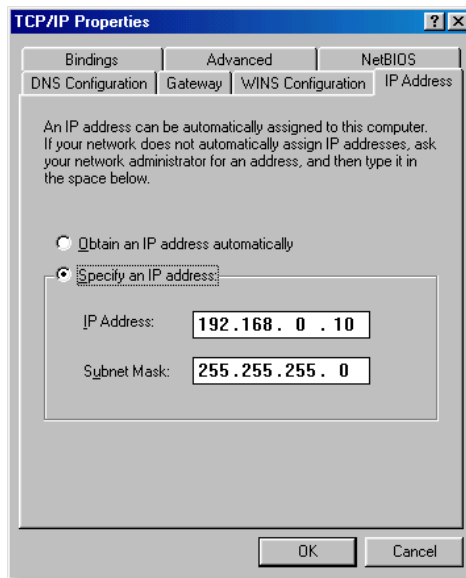
Make sure you take note of your computer's Default Gateway IP Address. The Default Gateway is the IP Address of the D-Link router. By default, it should be 192.168.0.1

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

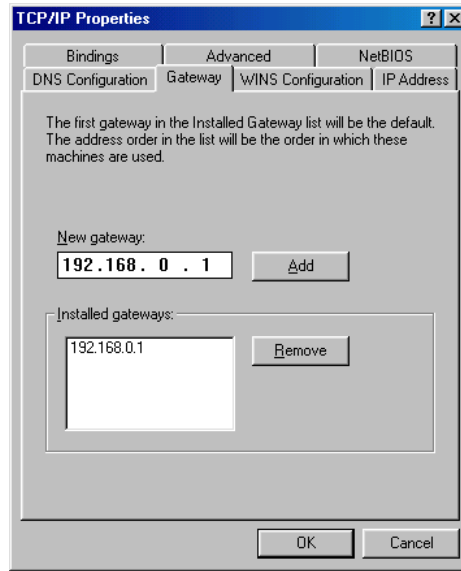
- From the desktop, right-click on the **Network Neighborhood** icon (Win ME - My Network Places) and select **Properties**.
- Highlight **TCP/IP** and click the **Properties** button. If you have more than 1 adapter, then there will be a TCP/IP "Binding" for each adapter. Highlight **TCP/IP > (your network adapter)** and then click **Properties**.



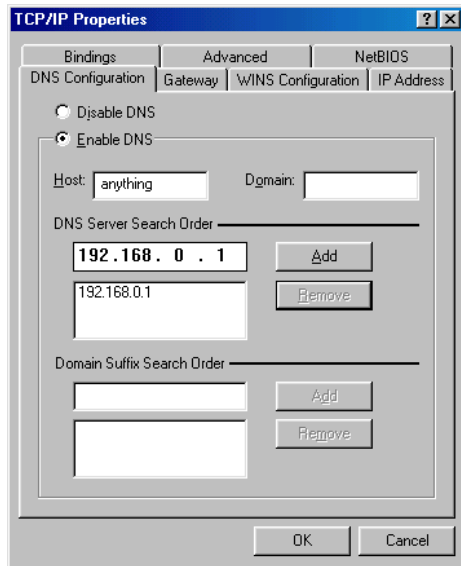
- Click **Specify an IP Address**.
- Enter in an IP Address that is on the same subnet as the LAN IP Address on your router. Example: If the router's LAN IP Address is 192.168.0.1, make your IP Address 192.168.0.X where X is between 2-99. Make sure that the number you choose is not in use on the network.



- Click on the **Gateway** tab.
- Enter the LAN IP Address of your router here (192.168.0.1).
- Click **Add** when finished.



- 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**.

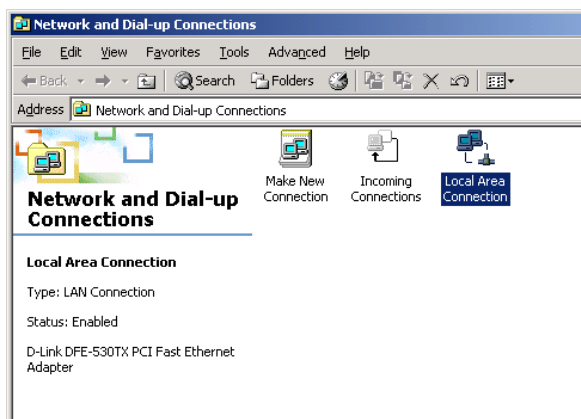


- Click **OK** twice.
- When prompted to reboot your computer, click **Yes**. After you reboot, the computer will now have a static, private IP Address.

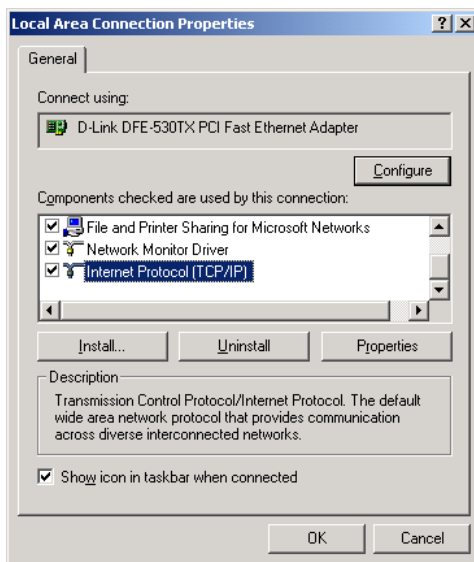


### How can I assign a Static IP Address in Windows 2000?

- Right-click on **My Network Places** and select **Properties**.
- Right-click on the **Local Area Connection** which represents your network card and select **Properties**.

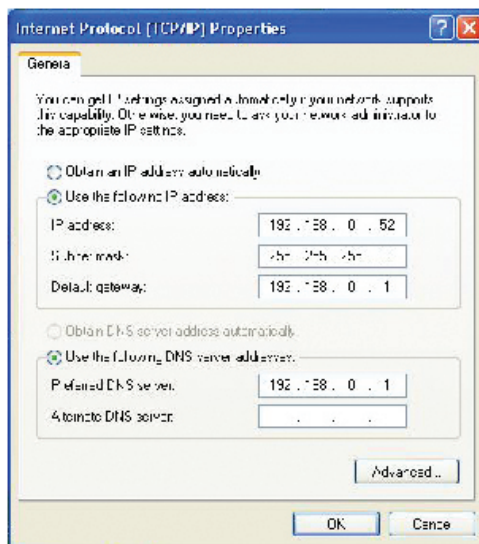


- Highlight **Internet Protocol (TCP/IP)** and click **Properties**.



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

- **The Secondary DNS** 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 XP?

- Click on **Start > Control Panel > Network and Internet Connections > Network connections**.
- See the second step for assigning a static IP address in Windows 2000 and continue from there.

**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 login page for the Web management. Follow instructions to login and complete the configuration.

## 2 How can I setup my router to work with a Cable modem connection?

### Dynamic Cable connection

(IE AT&T-BI, 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 on **Apply** and then **Continue** to save the changes.

#### WAN Settings

Please select the appropriate option to connect to your ISP.

- Dynamic IP Address Choose this option to obtain an IP address automatically from your ISP. (For most Cable modem users)
- Static IP Address Choose this option to set static IP information provided to you by your ISP.
- PPPoE Choose this option if your ISP uses PPPoE. (For most DSL users)
- Others PPTP, L2TP and BigPond Cable
  - PPTP (for Europe use only)
  - L2TP (for specific ISPs use only)
  - BigPond Cable (for Australia use only)

#### Dynamic IP Address

Host Name:

MAC Address:

(optional)

Primary DNS Server:

Secondary DNS Server:  (optional)

MTU:  MTU default = 1500

Apply Cancel Help

**Step 3:** Power cycle the cable modem and router.

Turn the cable modem off (first) . Turn the router off Leave them off for 2 minutes.\*\* Turn the cable modem on (first). Wait until you get a solid cable light on the cable modem. Turn the router on. Wait 30 seconds.

\*\* If you have a Motorola (Surf Board) modem, leave off for at least 5 minutes.

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

## Static Cable Connection

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

**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.

### WAN Settings

Please select the appropriate option to connect to your ISP.

- Dynamic IP Address Choose this option to obtain an IP address automatically from your ISP. (For most Cable Modem users)
- Static IP Address Choose this option to set static IP information provided to you by your ISP.
- PPTPoE Choose this option if your ISP uses PPPoE. (For most DSL users)
- Others PPTP, L2TP and BigPond Cable
  - PPTP (for Europe use only)
  - L2TP (for specific ISP use only)
  - BigPond Cable (for Australia use only)

### Static IP

IP Address:

Subnet Mask:

Default Gateway:

MAC Address:

(optional)

Primary DNS Server:

Secondary DNS Server:  (optional)

MTU:  (MTU default = 1500)

**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.

### **3 How can I setup my router to work with 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.

**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.

## **4 Can I use my D-Link Broadband Router to share my Internet connection provided by AOL DSL Plus?**

In most cases yes. AOL DSL+ 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

## **5 How do I open ports on my router?**

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.

### Virtual Server

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

Enabled  Disabled

**Name :**

**Private IP :**

**Protocol Type :**

**Private Port :**

**Public Port :**

**Firewall Rule :**

Details:

**Schedule :**

Details:

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

**Step 4:** Enter a name for your virtual server entry.

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

**Step 6:** Choose **Protocol Type** - either TCP or UDP.

**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.



## 6 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

## 7 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).*

**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** (nothing)

**Step 3:** Click the **Advanced** tab and then click on the **DMZ** button. Select **Enable** and type in the IP Address you found in 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.

### DMZ

DMZ (Demilitarized Zone) is used to allow a single computer on the LAN to be exposed to the Internet.

Enabled  Disabled

IP Address:

    
Apply Cancel Help

## 8 How do I open a range of ports on my DI-LB604 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.

### Firewall Rules

Firewall Rules can be used to allow or deny traffic from passing through the DI-724U.

**Name :**

**Action :**  Allow  Deny

**Source IP Range :**  to



### Firewall Rules List

Name	Action	Source IP Range
------	--------	-----------------

**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.

**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.

## 9 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 server at 192.168.0.7, then you need to specify the following virtual server mapping table:

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

## 10 How do I use *PC Anywhere* with my DI-LB604 router?

You will need to open 2 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.

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

Enabled  Disabled

Name:

Private IP:

Protocol Type:

Private Port:  --

Public Port:  --

Schedule:  Always

From Time:  :  :  To  :  :

Day:

Virtual Servers List			
Name	Private IP	Protocol	Schedule
pcanywhere2	172.17.8.100	TCP	Always

**Step 4:** The first entry will read as shown above.

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

**Step 6:** Create a second entry as shown below:

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

Enabled  Disabled

Name:

Private IP:

Protocol Type:

Private Port:  --

Public Port:  --

Schedule:  Always

From Time:  :  :  To  :  :

Day:

Virtual Servers List			
Name	Private IP	Protocol	Schedule
pcanywhere_	192.168.2.100	UDP	Always

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

**Step 8:** Run *PCAnywhere* from the remote site and use the WAN IP Address of the router, not your computer's IP Address.

## 11 How can I use *eDonkey* behind my D-Link Router?

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**.

### Firewall Rules

Firewall Rules can be used to allow or deny traffic from passing through the DI-724U.

**Name :**


**Action :**  Allow  Deny

**Source IP Range :**  to

    
Apply Cancel Help

### Firewall Rules List

Name	Action	Source IP Range
------	--------	-----------------



**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**.

## 12 How do I configure my router 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.

### Virtual Server

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

Enabled    Disabled

**Name :**

**Private IP :**

**Protocol Type :**

**Private Port :**

**Public Port :**

**Firewall Rule :**

Details:

**Schedule :**

Details:



  
 Apply Cancel Help

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



## 13 How do I configure my router to play Warcraft 3?

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

Warcraft 3 (Battlenet) uses port 6112.

**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 **TCP** for Protocol Type Enter **6112** for both Private Port and Public Port Click **Always** or set a schedule.

### Virtual Server

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

Enabled    Disabled

**Name :**

**Private IP :**

**Protocol Type :**

**Private Port :**




**Public Port :**

**Firewall Rule :**

Details:

**Schedule :**

Details:




  
**Apply Cancel Help**

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

Note: In order to host a Warcraft 3 game, you need to be able to accept both types of traffic on the computer that is running this game. To ensure this, please repeat steps 1-4 and this time make sure to select **UDP** for Protocol Type.

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.

## **14 How do I use NetMeeting with my D-Link Router?**

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>.

## **15 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. Basically, 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, including DI-LB604, support NAT. With proper configuration, multiple users can access the Internet using a single account via the NAT device.

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

# Appendix

## Securing Your Network

### 1. Change Admin Password

Changing the password to access your new router is the first step in securing your network. This can be done through the Wizard or on the Admin Page of the Tools tab. There is no password by default and hackers will know this when trying to access your network. Make sure that the password you choose is not commonly known or something that is easy to guess such as your last name or your pet's name. Try using a combination of letters and numbers to deter intruders from hacking into your network. Your private information should be kept private.

### 2. Change your SSID

### 3. Enable WEP and WPA

### 4. Change the default LAN IP address

Change the default LAN IP address from 192.168.0.1 to an alternate IP address. There are 3 ranges of IP addresses that have been reserved for use on Private Networks.

**10.0.0.0 - 10.255.255.255 (10.0.0.0/8)**

**172.16.0.0 - 172.31.255.255 (172.16.0.0/12)**

**192.168.0.0 - 192.168.255.255 (192.168.0.0/16)**

D-Link routers use 192.168.0.1 as their default LAN IP address. Choosing an alternate IP address lessens the probability of an intruders knowing what IP network your devices are on.

### 5. Set up MAC Filtering

Each networking device (router, network card, etc) on a network contains a unique hexadecimal number that identifies that specific product. This number is referred to as a MAC address. MAC filtering allows you to create a list of the MAC address of each device on your network and only allows these specific devices to associate with your network. With this feature enabled, devices attempting to connect to your network with a MAC address that is not in the list you created, will be denied access.

# Glossary

## A

**Access Control List** - ACL. Database of network devices that are allowed to access resources on the network.

**Access Point** - AP. Device that allows wireless clients to connect to it and access the network

**Ad-hoc network** - Peer-to-Peer network between wireless clients

**Address Resolution Protocol** - ARP. Used to map MAC addresses to IP addresses so that conversions can be made in both directions.

**ADSL** - Asymmetric Digital Subscriber Line

**Advanced Encryption Standard** - AES. Government encryption standard

**Alphanumeric** - Characters A-Z and 0-9

**Antenna** - Used to transmit and receive RF signals.

**AppleTalk** - A set of Local Area Network protocols developed by Apple for their computer systems

**AppleTalk Address Resolution Protocol** - AARP. Used to map the MAC addresses of Apple computers to their AppleTalk network addresses, so that conversions can be made in both directions.

**Application layer** - 7th Layer of the OSI model. Provides services to applications to ensure that they can communicate properly with other applications on a network.

**ASCII** - American Standard Code for Information Interchange. This system of characters is most commonly used for text files

**Attenuation** - The loss in strength of digital and analog signals. The loss is greater when the signal is being transmitted over long distances.

**Authentication** - To provide credentials, like a Password, in order to verify that the person or device is really who they are claiming to be

**Automatic Private IP Addressing** - APIPA. An IP address that a Windows computer will assign itself when it is configured to obtain an IP address automatically but no DHCP server is available on the network

## B

**Backward Compatible** - The ability for new devices to communicate and interact with older legacy devices to guarantee interoperability

**Bandwidth** - The maximum amount of bytes or bits per second that can be transmitted to and from a network device

**Basic Input/Output System** - BIOS. A program that the processor of a computer uses to startup the system once it is turned on

**Baud** - Data transmission speed

**Bit rate** - The amount of bits that pass in given amount of time

**bit/sec** - bits per second

**BOOTP** - Bootstrap Protocol. Allows for computers to be booted up and given an IP address with no user intervention

**Bottleneck** - A time during processes when something causes the process to slowdown or stop all together

**Broadband** - A wide band of frequencies available for transmitting data

**Broadcast** – Transmitting data in all directions at once

**Browser** – A program that allows you to access resources on the web and provides them to you graphically

## C

**Cable modem** – A device that allows you to connect a computer up to a coaxial cable and receive Internet access from your Cable provider

**CardBus** – A newer version of the PC Card or PCMCIA interface. It supports a 32-bit data path, DMA, and consumes less voltage

**Carrier Sense Multiple Access/Collision Avoidance** – CSMA/CA

**Carrier Sense Multiple Access/Collision Detect** – CSMA/CD

**CAT 5** – Category 5. Used for 10/100 Mbps or 1Gbps Ethernet connections

**Client** – A program or user that requests data from a server

**Collision** – When do two devices on the same Ethernet network try and transmit data at the exact same time.

**Cookie** – Information that is stored on the hard drive of your computer that holds your preferences to the site that gave your computer the cookie

**CSMA/CA** – Carrier Sense Multiple Access/Collision Avoidance

**CSMA/CD** – Carrier Sense Multiple Access/Collision Detection

## D

**Data** – Information that has been translated into binary do that it can be processed or moved to another device

**Data Encryption Standard** – Uses a randomly selected 56-bit key that must be known by both the sender and the receiver when information is exchanged

**Data-Link layer** – The second layer of the OSI model. Controls the movement of data on the physical link of a network

**Database** – Organizes information so that it can be managed updated, as well as easily accessed by users or applications

**DB-25** – A 25 pin male connector for attaching External modems or RS-232 serial devices

**DB-9** – A 9 pin connector for RS-232 connections

**dBd** - decibels related to dipole antenna

**dBi** - decibels relative to isotropic radiator

**dBm** - decibels relative to one milliwatt

**Decrypt** – To unscramble an encrypted message back into plain text

**Default** – A predetermined value or setting that is used by a program when no user input has been entered for this value or setting

**Demilitarized zone – DMZ.** A single computer or group of computers that can be accessed by both users on the Internet as well as users on the Local Network, but that is not protected by the same security as the Local Network.

**DHCP – Dynamic Host Configuration Protocol.** Used to automatically assign IP addresses from a predefined pool of addresses to computers or devices that requests them

**Digital certificate** – An electronic method of providing credentials to a server in order to have access to it or a network

**Direct Sequence Spread Spectrum** – DSSS. Modulation technique used by 802.11b wireless devices

**DNS – Domain Name System.** Translates Domain Names to IP addresses

**DOCSIS** – Data Over Cable Service Interface Specifications. The standard interface for cable modems

**Domain name** – A name that is associated with an IP address

**Download** – To send a request from one computer to another and have the file transmitted back to the requesting computer

**DSL** – Digital Subscriber Line. High bandwidth Internet connection over telephone lines

**Duplex** – Sending and Receiving data transmissions at the same time

**Dynamic DNS service** – DDNS is provided by companies to allow users with Dynamic IP addresses to obtain a Domain Name that will always be linked to their changing IP address. The IP address is updated by either client software running on a computer or by a router that supports DDNS, whenever the IP address changes.

**Dynamic IP address** – IP address that is assigned by a DHCP server and that may change. Cable Internet providers usually use this method to assign IP addresses to their customers.

## E

---

**EAP** – Extensible Authentication Protocol

**Email** – Electronic Mail is a computer-stored message that is transmitted over the Internet

**Encryption** – Converting data into cyphertext so that it cannot be easily read

**Enterprise** – Large organizations that use computers

**Ethernet** – The most widely used technology for Local Area Networks.

## F

---

**Fiber optic** – A way of sending data through light impulses over glass or plastic wire or fiber

**File server** – A computer on a network that stores data so that the other computers on the network can all access it

**File sharing** – Allowing data from computers on a network to be accessed by other computers on the network will different levels of access rights

**Firewall** – A device that protects resources of the Local Area Network from unauthorized users outside of the local network

**Firmware** – Programming that is inserted into a hardware device that tells it how to function

**Fragmentation** – Breaking up data into smaller pieces to make it easier to store

**FTP** – File Transfer Protocol. Easiest way to transfer files between computers on the Internet

**Full-duplex** – Sending and Receiving data at the same time

## G

---

**Gain** – The amount an amplifier boosts the wireless signal

**Gateway** – A device that connects your network to another, like the internet

**Gbps** – Gigabits per second

**Gigabit Ethernet** – Transmission technology that provides a data rate of 1 billion bits per second

**Graphical user interface** – GUI

---

## H

**H.323** – A standard that provides consistency of voice and video transmissions and compatibility for videoconferencing devices

**Half-duplex** – Data cannot be transmitted and received at the same time

**Hashing** – Transforming a string of characters into a shorter string with a predefined length

**Hexadecimal** – Characters 0-9 and A-F

**HomePNA** – Networking over telephone lines

**HomeRF** – Networking standard that combines 802.11b and DECT (digital Enhanced Cordless Telecommunication) that provides speeds up to 1.6 Mbps and a distance of 150 ft using a Frequency Hopping transmission method

**Hop** – The action of data packets being transmitted from one router to another

**Host** – Computer on a network

**HTTP** – Hypertext Transfer Protocol is used to transfer files from HTTP servers (web servers) to HTTP clients (web browsers)

**HTTPS** – HTTP over SSL is used to encrypt and decrypt HTTP transmissions

**Hub** – A networking device that connects multiple devices together

---

## I

**ICMP** – Internet Control Message Protocol

**IEEE** – Institute of Electrical and Electronics Engineers

**IETF** – Internet Engineering Task Force

**IGMP** – Internet Group Management Protocol is used to make sure that computers can report their multicast group membership to adjacent routers

**IIS** – Internet Information Server is a WEB server and FTP server provided by Microsoft

**IKE** – Internet Key Exchange is used to ensure security for VPN connections

**Infrastructure** – In terms of a wireless network, this is when wireless clients use an Access Point to gain access to the network

**Internet** – A system of worldwide networks which use TCP/IP to allow for resources to be accessed from computers around the world

**Internet Explorer** – A World Wide Web browser created and provided by Microsoft

**Internet Protocol** – The method of transferring data from one computer to another on the Internet

**Internet Protocol Security** – IPsec provides security at the packet processing layer of network communication

**Internet Service Provider** – An ISP provides access to the Internet to individuals or companies

**Interoperability** – The ability for products to interact with other products without much customer interaction

**Intranet** – A private network

**Intrusion Detection** – A type of security that scans a network to detect attacks coming from inside and outside of the network

**IP** – Internet Protocol

**IP address** – A 32-bit number, when talking about Internet Protocol Version 4, that identifies each computer that transmits data on the Internet or on an Intranet

**IPsec** – Internet Protocol Security

**IPv6** – Internet Protocol Version 6 uses 128-bit addresses and was developed to solve the problem that we face of running out of IP version 4 addresses

**IPX** – Internetwork Packet Exchange is a networking protocol developed by Novell to enable their Netware clients and servers to communicate

**ISP** – Internet Service Provider

## J

**Java** – A programming language used to create programs and applets for web pages

## K

**Kbps** – Kilobits per second

**Kbyte** - Kilobyte

**Kerberos** – A method of securing and authenticating requests for services on a network

## L

**LAN** – Local Area Network

**Latency** – The amount of time that it takes a packet to get from the one point to another on a network. Also referred to as delay

**LED** - Light Emitting Diode

**Legacy** – Older devices or technology

**Local Area Network** – A group of computers in a building that usually access files from a server

## M

**MAC address** – A unique hardware address for devices on a Local Area Network

**MDI** – Medium Dependent Interface is an Ethernet port for a connection to a straight-through cable

**MDIX** - Medium Dependent Interface Crossover, is an Ethernet port for a connection to a crossover cable

**Megabit** - Mb

**Megabyte** - MB

**Megabits per second** - Mbps

**MIB** – Management Information Base is a set of objects that can be managed by using SNMP

**MIMO** – Multiple-in Multiple-out

**Modem** – A device that Modulates digital signals from a computer to an analog signal in order to transmit the signal over phone lines. It also Demodulates the analog signals coming from the phone lines to digital signals for your computer

**MPPE** – Microsoft Point-to-Point Encryption is used to secure data transmissions over PPTP connections

**MTU** – Maximum Transmission Unit is the largest packet that can be transmitted on a packet-based network like the Internet



**Multicast** – Sending data from one device to many devices on a network

## N

**NAT** – Network Address Translation allows many private IP addresses to connect to the Internet, or another network, through one IP address

**NetBEUI** – NetBIOS Extended User Interface is a Local Area Network communication protocol. This is an updated version of NetBIOS

**NetBIOS** – Network Basic Input/Output System

**Netmask** – Determines what portion of an IP address designates the Network and which part designates the Host

**NetWare** – A Server Software developed by Novell

**Network Interface Card** – A card installed in a computer or built onto the motherboard that allows the computer to connect to a network

**Network layer** – The third layer of the OSI model which handles the routing of traffic on a network

**Network Time Protocol** – Used to synchronize the time of all the computers in a network

**NIC** – Network Interface Card

**NTP** – Network Time Protocol

## O

**OFDM** – Orthogonal Frequency-Division Multiplexing is the modulation technique for both 802.11a and 802.11g

**OSI** – Open Systems Interconnection is the reference model for how data should travel between two devices on a network

**OSPF** – Open Shortest Path First is a routing protocol that is used more than RIP in larger scale networks because only changes to the routing table are sent to all the other routers in the network as opposed to sending the entire routing table at a regular interval, which is how RIP functions

## P

**Password** - A sequence of characters that is used to authenticate requests to resources on a network

**Personal Area Network** – The interconnection of networking devices within a range of 10 meters

**Physical layer** – The first layer of the OSI model. Provides the hardware means of transmitting electrical signals on a data carrier

**PoE** – Power over Ethernet is the means of transmitting electricity over the unused pairs in a category 5 Ethernet cable

**POP 3** – Post Office Protocol 3 is used for receiving email

**PPP** – Point-to-Point Protocol is used for two computers to communicate with each over a serial interface, like a phone line

**PPPoE** – Point-to-Point Protocol over Ethernet is used to connect multiple computers to a remote server over Ethernet

**PPTP** – Point-to-Point Tunneling Protocol is used for creating VPN tunnels over the Internet between two networks

**Preamble** – Used to synchronize communication timing between devices on a network

## Q

---

**QoS** – Quality of Service

## R

---

**RADIUS** – Remote Authentication Dial-In User Service allows for remote users to dial into a central server and be authenticated in order to access resources on a network

**Rendezvous** – Apple's version of UPnP, which allows for devices on a network to discover each other and be connected without the need to configure any settings

**Repeater** – Retransmits the signal of an Access Point in order to extend it's coverage

**RIP** – Routing Information Protocol is used to synchronize the routing table of all the routers on a network

**RJ-11** – The most commonly used connection method for telephones

**RJ-45** - The most commonly used connection method for Ethernet

**RS-232C** – The interface for serial communication between computers and other related devices

**RSA** – Algorithm used for encryption and authentication

## S

---

**Samba** – A freeware program that allows for resources to be shared on a network. Mainly used in Unix based Operating Systems

**Server** – A computer on a network that provides services and resources to other computers on the network

**Session key** – An encryption and decryption key that is generated for every communication session between two computers

**Session layer** – The fifth layer of the OSI model which coordinates the connection and communication between applications on both ends

**Simple Mail Transfer Protocol** – Used for sending and receiving email

**Simple Network Management Protocol** – Governs the management and monitoring of network devices

**SMTP** – Simple Mail Transfer Protocol

**SNMP** – Simple Network Management Protocol

**SOHO** – Small Office/Home Office

**SPI** – Stateful Packet Inspection

**SSH** – Secure Shell is a command line interface that allows for secure connections to remote computers

**SSID** – Service Set Identifier is a name for a wireless network

**Stateful inspection** – A feature of a firewall that monitors outgoing and incoming traffic to make sure that only valid responses to outgoing requests for incoming packets are allowed to pass through the firewall

**Subnet mask** – Determines what portion of an IP address designates the Network and which part designates the Host

## T

---

**TCP** – Transmission Control Protocol

**TCP/IP** – Transmission Control Protocol/Internet Protocol

**TFTP** – Trivial File Transfer Protocol is a utility used for transferring files that is simpler to use than FTP but with less features

**Throughput** – The amount of data that can be transferred in a given time period

**Traceroute** – A utility displays the routes between you computer and specific destination

## U

---

**UDP** – User Datagram Protocol

**UNC** – Universal Naming Convention allows for shares on computers to be identified without having to know what storage device it's on

**Unicast** – Communication between a single sender and receiver

**Universal Plug and Play** – A standard that allows network devices to discover each other and configure themselves to be a part of the network

**UPnP** – Universal Plug and Play

**URL** – Uniform Resource Locator is a unique address for files accessible on the Internet

**UTP** – Unshielded Twisted Pair

## V

---

**Virtual LAN** -

**Virtual Private Network** – A secure tunnel over the Internet to connect remote offices or users to their company's network

**VLAN** – Virtual LAN

**Voice over IP** – Sending voice information over the Internet as opposed to the PSTN

**VoIP** – Voice over IP

## W

---

**Wake on LAN** – Allows you to power up a computer though it's Network Interface Card

**WAN** – Wide Area Network

**Web browser** – A utility that allows you to view content and interact with all of the information on the World Wide Web

**WEP** – Wired Equivalent Privacy is security for wireless networks that is supposed to be comparable to that of a wired network

**Wi-Fi** – Wireless Fidelity

**Wi-Fi Protected Access** – An updated version of security for wireless networks that provides authentication as well as encryption

**Wide Area Network** - A network spanning a large geographical area or consisting of more than one LAN.

**Wireless ISP** – A company that provides a broadband Internet connection over a wireless connection

**Wireless LAN** – Connecting to a Local Area Network over one of the 802.11 wireless standards

**WISP** – Wireless Internet Service Provider

**WLAN** – Wireless Local Area Network

## Y

---

**Yagi antenna** – A directional antenna used to concentrate wireless signals on a specific location

# Contacting Technical Support

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

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

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

## **Tech Support for customers within the United States:**

*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>

email: [support@dlink.com](mailto:support@dlink.com)

## **Tech Support for customers within Canada:**

*D-Link Technical Support over the Telephone:*

(800) 361-5265

Monday to Friday 7:30AM to 9:00PM EST

*D-Link Technical Support over the Internet:*

<http://support.dlink.ca>

email: [support@dlink.ca](mailto:support@dlink.ca)

When contacting technical support, please provide the following information:

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

# Warranty

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

- D-Link or its authorized reseller or distributor and
- Products purchased and delivered within the fifty states of the United States, the District of Columbia, U.S. Possessions or Protectorates, U.S. Military Installations, addresses with an APO or FPO.

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

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

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

D-Link's sole obligation shall be to repair or replace the defective Hardware during the Warranty Period at no charge to the original owner or to refund at D-Link's sole discretion. Such repair or replacement will be rendered by D-Link at an Authorized D-Link Service Office. The replacement Hardware need not be new or have an identical make, model or part. D-Link may in its sole discretion replace the defective Hardware (or any part thereof) with any reconditioned product that D-Link reasonably determines is substantially equivalent (or superior) in all material respects to the defective Hardware. Repaired or replacement Hardware will be warranted for the remainder of the original Warranty Period from the date of original retail purchase. If a material defect is incapable of correction, or if D-Link determines in its sole discretion that it is not practical to repair or replace the defective Hardware, the price paid by the original purchaser for the defective Hardware will be refunded by D-Link upon return to D-Link of the defective Hardware. All Hardware (or part thereof) that is replaced by D-Link, or for which the purchase price is refunded, shall become the property of D-Link upon replacement or refund.

**Limited Software Warranty:** D-Link warrants that the software portion of the product ("Software") will substantially conform to D-Link's then current functional specifications for the Software, as set forth in the applicable documentation, from the date of original retail purchase of the Software for a period of ninety (90) days ("Warranty Period"), provided that the Software is properly installed on approved hardware and operated as contemplated in its documentation. D-Link further warrants that, during the Warranty Period, the magnetic media on which D-Link delivers the Software will be free of physical defects. D-Link's sole obligation shall be to replace the non-conforming Software (or defective media) with software that substantially conforms to D-Link's functional specifications for the Software or to refund at D-Link's sole discretion. Except as otherwise agreed by D-Link in writing, the replacement Software is provided only to the original licensee, and is subject to the terms and conditions of the license granted by D-Link for the Software. Software will be warranted for the remainder of the original Warranty Period from the date or original retail purchase. If a material non-conformance is incapable of correction, or if D-Link determines in its sole discretion that it is not practical to replace the non-conforming Software, the price paid by the original licensee for the non-conforming Software will be refunded by D-Link; provided that the non-conforming Software (and all copies thereof) is first returned to D-Link. The license granted respecting any Software for which a refund is given automatically terminates.

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

Warranty as described herein, notwithstanding anything stated herein to the contrary.

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

- The customer must submit with the product as part of the claim a written description of the Hardware defect or Software nonconformance in sufficient detail to allow D-Link to confirm the same.
- The original product owner must obtain a Return Material Authorization (“RMA”) number from the Authorized D-Link Service Office and, if requested, provide written proof of purchase of the product (such as a copy of the dated purchase invoice for the product) before the warranty service is provided.
- After an RMA number is issued, the defective product must be packaged securely in the original or other suitable shipping package to ensure that it will not be damaged in transit, and the RMA number must be prominently marked on the outside of the package. Do not include any manuals or accessories in the shipping package. D-Link will only replace the defective portion of the Product and will not ship back any accessories.
- The customer is responsible for all in-bound shipping charges to D-Link. No Cash on Delivery (“COD”) is allowed. Products sent COD will either be rejected by D-Link or become the property of D-Link. Products shall be fully insured by the customer. D-Link will not be held responsible for any packages that are lost in transit to D-Link. The repaired or replaced packages will be shipped to the customer via UPS Ground or any common carrier selected by D-Link, with shipping charges prepaid. Expedited shipping is available if shipping charges are prepaid by the customer and upon request.
- Return Merchandise Ship-To Address

**USA:** 17595 Mt. Herrmann, Fountain Valley, CA 92708

**Canada:** 2180 Winston Park Drive, Oakville, ON, L6H 5W1 (Visit <http://www.dlink.ca> for detailed warranty information within Canada)

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

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

**Disclaimer of Other Warranties:** EXCEPT FOR THE LIMITED WARRANTY SPECIFIED HEREIN, THE PRODUCT IS PROVIDED “AS-IS” WITHOUT ANY WARRANTY OF ANY KIND WHATSOEVER INCLUDING, WITHOUT LIMITATION, ANY WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NON-INFRINGEMENT. IF ANY IMPLIED WARRANTY CANNOT BE DISCLAIMED IN ANY TERRITORY WHERE A PRODUCT IS SOLD, THE DURATION OF SUCH IMPLIED WARRANTY SHALL BE LIMITED TO NINETY (90) DAYS. EXCEPT AS EXPRESSLY COVERED UNDER THE LIMITED WARRANTY PROVIDED HEREIN, THE ENTIRE RISK AS TO THE QUALITY, SELECTION AND PERFORMANCE OF THE PRODUCT IS WITH THE PURCHASER OF THE PRODUCT.

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

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

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

Copyright Statement: **No part of this publication or documentation accompanying this Product may be reproduced in any form or by any means or used to make any derivative such as translation, transformation, or adaptation without permission from D-Link Corporation/D-Link Systems, Inc., as stipulated by the United States Copyright Act of 1976. Contents are subject to change without prior notice. Copyright® 2002 by D-Link Corporation/D-Link Systems, Inc. All rights reserved.**

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

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

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

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

**FCC Caution:**

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

**IMPORTANT NOTE:****FCC Radiation Exposure Statement:**

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 20cm between the radiator & your body. To maintain compliance with FCC RF exposure compliance requirements, please avoid direct contact to the transmitting antenna during transmitting.

This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

D-Link declares that the DI-LB604 (FCC ID: KA2DI634MA1) is limited in CH1~CH11 by specified firmware controlled in the USA.

**For detailed warranty outside the United States, please contact corresponding local D-Link office.**



# Registration



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

03/10/2008