

## Time Settings

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

**Time Zone:** Select the Time Zone from the drop-down menu.

**Daylight Saving:** To select Daylight Saving time manually, select enabled or disabled, and enter a start date and an end date for daylight saving time.

**Enable NTP** NTP is short for Network Time Protocol. NTP **Server:** synchronizes computer clock times in a network of computers. Check this box to use a NTP server. This will only connect to a server on the Internet, not a local server.

**NTP Server Used:** Enter the NTP server or select one from the drop-down menu.

**Manual:** To manually input the time, enter the values in these fields for the Year, Month, Day, Hour, Minute, and Second and then click **Set Time**. You can also click **Copy Your Computer's Time Settings**.

**D-Link**

DIR-628

ADMIN TIME SYSLOG EMAIL\_SETTINGS SYSTEM FIRMWARE DYNAMIC DNS SYSTEM CHECK SCHEDULES

**TIME**

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

Save Settings Don't Save Settings

**TIME CONFIGURATION**

Current Router Time : Saturday, January 31, 2004 11:58:11 AM

Time Zone : (GMT-08:00) Pacific Time (US/Canada), Tijuana

Enable Daylight Saving :

Daylight Saving Offset : +1:00

Daylight Saving Dates : DST Start Apr 1st DST End Oct 5th Day of Week Time 2 am

**AUTOMATIC TIME CONFIGURATION**

Enable NTP Server :

NTP Server Used : florida.ath.cx << Select NTP Server

**SET THE DATE AND TIME MANUALLY**

Date And Time : Year 2004 Month Jan Day 31 Hour 11 Minute 57 Second 27 AM

Copy Your Computer's Time Settings

**WIRELESS**

Helpful Hints...  
Good timekeeping is important for accurate logs and scheduled firewall rules.  
More...

# SysLog

The Broadband Router keeps a running log of events and activities occurring on the Router. You may send these logs to a SysLog server on your network.

**Enable Logging to SysLog Server:** Check this box to send the router logs to a SysLog Server.

**SysLog Server IP Address:** The address of the SysLog server that will be used to send the logs. You may also select your computer from the drop-down menu (only if receiving an IP address from the router via DHCP).

The screenshot shows the D-Link router configuration interface. At the top, there is a navigation bar with tabs for ADMIN, TIME, SYSLOG, EMAIL SETTINGS, SYSTEM, FIRMWARE, DYNAMIC DNS, SYSTEM CHECK, SCHEDULES, and WIRELESS. The SYSLOG tab is selected. Below the navigation bar, there are sections for SETUP, ADVANCED, TOOLS, and STATUS. The main content area is titled 'SYSLOG' and contains the following text: 'The SysLog options allow you to send log information to a SysLog Server.' Below this text are two buttons: 'Save Settings' and 'Don't Save Settings'. Underneath, there is a section titled 'SYSLOG SETTINGS' with a checkbox for 'Enable Logging To SysLog Server' which is checked. Below the checkbox is a text field for 'Syslog Server IP Address' containing '0.0.0.0' and a dropdown menu for 'Computer Name' with a downward arrow. At the bottom right of the main content area, there is a 'Helpful Hints...' section with text explaining that a System Logger (syslog) is a server that collects logs from different sources and that the LAN includes a syslog server. It also mentions that you can use this option to send the router's logs to that server, with a 'More...' link.

## Email Settings

The Email feature can be used to send the system log files, router alert messages, and firmware update notification to your email address.

**Enable Email Notification:** When this option is enabled, router activity logs are e-mailed to a designated email address.

**From Email Address:** This email address will appear as the sender when you receive a log file or firmware upgrade notification via email.

**To Email Address:** Enter the email address where you want the email sent.

**SMTP Server Address:** Enter the SMTP server address for sending email. If your SMTP server requires authentication, select this option.

**Enable Authentication:** Check this box if your SMTP server requires authentication.

**Account Name:** Enter your account for sending email.

**Password:** Enter the password associated with the account. Re-type the password associated with the account.

**On Log Full:** When this option is selected, logs will be sent via email when the log is full.

**On Schedule:** Selecting this option will send the logs via email according to schedule.

**Schedule:** This option is enabled when On Schedule is selected. You can select a schedule from the list of defined schedules. To create a schedule, go to **Tools > Schedules**.

The screenshot shows the D-Link DIR-628 Web Management Interface. The top navigation bar includes 'ADMIN', 'TIME', 'SYSLOG', 'EMAIL SETTINGS', 'SYSTEM', 'FIRMWARE', 'DYNAMIC DNS', 'SYSTEM CHECK', and 'SCHEDULES'. The 'EMAIL SETTINGS' page is displayed, featuring a 'D-Link' logo and a 'SUPPORT' link. The main content area is divided into three sections:

- EMAIL SETTINGS:** Contains a description: "The Email feature can be used to send the system log files, router alert messages, and firmware update notification to your email address." Below this are 'Save Settings' and 'Don't Save Settings' buttons.
- ENABLE:** Contains a checkbox for 'Enable Email Notification'.
- EMAIL LOG WHEN FULL OR ON SCHEDULE:** Contains checkboxes for 'On Log Full' and 'On Schedule', a 'Schedule' dropdown menu (set to 'Never'), and a 'Details' field.

At the bottom of the page, there is a 'WIRELESS' section.

# System Settings

**Save Settings to Local Hard Drive:** Use this option to save the current router configuration settings to a file on the hard disk of the computer you are using. First, click the Save button. You will then see a file dialog, where you can select a location and file name for the settings.

**Load Settings from Local Hard Drive:** Use this option to load previously saved router configuration settings. First, use the Drive: Browse control to find a previously save file of configuration settings. Then, click the Load button to transfer those settings to the router.

**Restore to Factory Default Settings:** This option will restore all configuration settings back to the settings that were in effect at the time the router was shipped from the factory. Any settings that have not been saved will be lost, including any rules that you have created. If you want to save the current router configuration settings, use the Save button above.

**Reboot Device:** Click to reboot the router.

**DIR-628** // **ADMIN** **TIME** **SYSLOG** **EMAIL SETTINGS** **SYSTEM** **FIRMWARE** **DYNAMIC DNS** **SYSTEM CHECK** **SCHEDULES** **WIRELESS**

**SYSTEM SETTINGS**

The System Settings section allows you to reboot the device, or restore the router to the factory default settings. Restoring the unit to the factory default settings will erase all settings, including any rules that you have created.

The current system settings can be saved as a file onto the local hard drive. The saved file or any other saved setting file created by device can be uploaded into the unit.

**SYSTEM SETTINGS**

**Save To Local Hard Drive:**

**Load From Local Hard Drive:**

**Restore To Factory Default:**   
 Restore all settings to the factory defaults.

**Reboot The Device:**

**Helpful Hints...**

Once your router is configured the way you want it, you can save the configuration settings to a configuration file.

You might need this file so that you can load your configuration later in the event that the router's default settings are restored.

To save the configuration, click the **Save Configuration** button.

[More...](#)

## Update Firmware

You can upgrade the firmware of the Router here. Make sure the firmware you want to use is on the local hard drive of the computer. Click on **Browse** to locate the firmware file to be used for the update. Please check the D-Link support site for firmware updates at <http://support.dlink.com>. You can download firmware upgrades to your hard drive from the D-Link support site.

**Firmware** Click on **Check Online Now for Latest Firmware Upgrade: Version** to find out if there is an updated firmware; if so, download the new firmware to your hard drive.

**Browse:** After you have downloaded the new firmware, click **Browse** to locate the firmware update on your hard drive. Click **Upload** to complete the firmware upgrade.

**Notifications** Check **Automatically Check Online for Latest Firmware Version** to have the router check automatically to see if there is a new firmware upgrade.

Check **Email Notification of Newer Firmware Version** to have the router send an email when there is a new firmware available.

**D-Link**

DIR-628 // SETUP ADVANCED TOOLS STATUS SUPPORT

**FIRMWARE**

There may be new firmware for your DIR-628 to improve functionality and performance. To upgrade the firmware, locate the upgrade file on the local hard drive with the Browse button. Once you have found the file to be used, click the Upload button below to start the firmware upgrade.

Save Settings Don't Save Settings

**FIRMWARE INFORMATION**

Current Firmware Version : 1.00  
Current Firmware Date : 2008/03/12  
Check Online Now for Latest Firmware Version :

**FIRMWARE UPGRADE**

**Note:** Some firmware upgrades reset the configuration options to the factory defaults. Before performing an upgrade, be sure to save the current configuration from the [Tools](#) → [System](#) screen.

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

Upload :

**FIRMWARE UPGRADE NOTIFICATION OPTIONS**

Automatically Check Online for Latest Firmware Version :   
Email Notification of Newer Firmware Version :

**WIRELESS**

**Helpful Hints...**

Firmware updates are released periodically to improve the functionality of your router and to add features. If you run into a problem with a specific feature of the router, check if updated firmware is available for your router.

[More...](#)

## DDNS

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

**DDNS:** Dynamic Domain Name System is a method of keeping a domain name linked to a changing IP Address. Check the box to enable DDNS.

**Server Address:** Choose your DDNS provider from the drop down menu.

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

**Username or Key:** Enter the Username for your DDNS account.

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

**Timeout:** Enter a time (in hours).

**Status:** Displays the current status - Connected or Disconnected.

The screenshot shows the D-Link configuration interface for DDNS. The top navigation bar includes 'DIR-628', 'ADMIN', 'TIME', 'SYSLOG', 'EMAIL\_SETTINGS', 'SYSTEM', 'FIRMWARE', 'DYNAMIC DNS', 'SYSTEM CHECK', and 'SCHEDULES'. The 'DYNAMIC DNS' section is highlighted in orange and contains the following text:

**DYNAMIC DNS**  
The DDNS feature allows you to host a server (Web, FTP, Game Server, etc...) using a domain name that you have purchased (www.whateveryournameis.com) with your dynamically assigned IP address. Most broadband Internet Service Providers assign dynamic (changing) IP addresses. Using a DDNS service provider, your friends can enter your host name to connect to your game server no matter what your IP address is.  
Sign up for D-Link's Free DDNS service at [www.DLinkDDNS.com](http://www.DLinkDDNS.com).

Buttons: Save Settings, Don't Save Settings

**DYNAMIC DNS**  
Enable Dynamic DNS:

Server Address:  [Select Dynamic DNS Server]  
Host Name:  (e.g.: me.mydomain.net)  
Username or Key:   
Password or Key:   
Verify Password or Key:   
Timeout: 576 (hours)  
Status: Disconnect

At the bottom of the page, the 'WIRELESS' section is visible.

# System Check

**Ping Test:** The Ping Test is used to send Ping packets to test if a computer is on the Internet. Enter the IP Address that you wish to Ping, and click **Ping**.

**Ping Results:** The results of your ping attempts will be displayed here.



# Schedules

**Name:** Enter a name for your new schedule.

**Days:** Select a day, a range of days, or All Week to include every day.

**Time:** Check **All Day - 24hrs** or enter a start and end time for your schedule.

**Save:** Click **Save** to save your schedule. You must click **Save Settings** at the top for your schedules to go into effect.

**Schedule Rules List:** The list of schedules will be listed here. Click the **Edit** icon to make changes or click the **Delete** icon to remove the schedule.

**D-Link**

DIR-628

ADMIN  
TIME  
SYSLOG  
EMAIL SETTINGS  
SYSTEM  
FIRMWARE  
DYNAMIC DNS  
SYSTEM CHECK  
SCHEDULES

**SETUP** **ADVANCED** **TOOLS** **STATUS** **SUPPORT**

**SCHEDULES**

The Schedule configuration option is used to manage schedule rules for various firewall and parental control features.

**Helpful Hints...**

Schedules are used with a number of other features to define when those features are in effect.

Give each schedule a name that is meaningful to you. For example, a schedule for Monday through Friday from 3:00pm to 9:00pm, might be called "After School".

Click **Save** to add a completed schedule to the list below.

Click the **Edit** icon to change an existing schedule.

Click the **Delete** icon to permanently delete a schedule.

**More...**

**ADD SCHEDULE RULE**

Name :

Day(s) :  All Week  Select Day(s)

Sun  Mon  Tue  Wed  Thu  Fri  Sat

**All Day - 24 hrs** :

Start Time : 12 : 0 AM (hour:minute, 12 hour time)

End Time : 12 : 0 AM (hour:minute, 12 hour time)

**SCHEDULE RULES LIST**

Name	Day(s)	Time Frame
<input type="text"/>	<input type="text"/>	<input type="text"/>

**WIRELESS**



## Device Information

This page displays the current information for the DIR-628. It will display the LAN, WAN (Internet), and Wireless information.

If your Internet connection is set up for a Dynamic IP address then a **Release** button and a **Renew** button will be displayed. Use **Release** to disconnect from your ISP and use **Renew** to connect to your ISP.

If your Internet connection is set up for PPPoE, a **Connect** button and a **Disconnect** button will be displayed. Use **Disconnect** to drop the PPPoE connection and use **Connect** to establish the PPPoE connection.

**General:** Displays the router's time and firmware version.

**WAN:** Displays the MAC address and the public IP settings for the router.

**LAN:** Displays the MAC address and the private (local) IP settings for the router.

**Wireless LAN:** Displays the wireless MAC address and your wireless settings such as SSID and Channel.

**LAN Computers:** Displays computers and devices that are connected to the router via Ethernet and that are receiving an IP address assigned by the router (DHCP).

DIR-628	SETUP	ADVANCED	TOOLS	STATUS	SUPPORT
DEVICE INFO	<b>DEVICE INFORMATION</b>				Helpful links...
LOGS	All of our links & tool network connection details are displayed on this page. The Firmware version is also displayed here.				MAC (LAN) and LAN connection details are displayed here.
STATISTICS					
INTERNET SETTINGS					
WIRELESS					
<b>GENERAL</b>					
Time : Saturday, January 21, 2006 12:00:28 PM					
Firmware Version : 1.00_2006102712					
<b>WAN</b>					
Connection Type : DHCP Client					
QoS Engine : Active					
Cable Status : Connected					
Network Status : Established					
Connection Up Time : 2 Days, 21:28:15					
MAC Address : 00:03:5d:00:01:23					
IP Address : 192.168.0.10					
Subnet Mask : 255.255.255.0					
Default Gateway : 192.168.0.1					
Primary DNS Server : 192.152.0.11					
Secondary DNS Server : 67.130.140.2					
<b>LAN</b>					
MAC Address : 00:03:5d:00:01:24					
IP Address : 192.168.0.1					
Subnet Mask : 255.255.255.0					
DHCP Server : Enabled					
<b>WIRELESS LAN</b>					
Wireless Radio : Enabled					
MAC Address : 00:1E:58:20:00:02					
Network Name (SSID) : GIGaset					
Channel : 36					
Security Mode : WEP					
WEP Protected Setup : Enabled/Configured					
<b>LAN COMPUTERS</b>					
IP Address Name (if any) MAC					
192.168.0.197 PHLab16 00:0c:f1:fe:ec:d					
192.168.0.199 PHLab15 00:16:17:48:b2:9					

# Log

The router automatically logs (records) events of possible interest in its internal memory. If there isn't enough internal memory for all events, logs of older events are deleted but logs of the latest events are retained. The Logs option allows you to view the router logs. You can define what types of events you want to view and the level of the events to view. This router also has external Syslog Server support so you can send the log files to a computer on your network that is running a Syslog utility.

**What to View:** You can select the types of messages that you want to display from the log. **Firewall & Security**, **System**, and **Router Status** messages can be selected.

**View Levels:** There are three levels of message importance: **Informational**, **Warning**, and **Critical**. Select the levels that you want displayed in the log.

**Apply Log Settings:** Will filter the log results so that only the selected options appear.

**Refresh:** Updates the log details on the screen so it displays any recent activity.

**Clear:** Clears all of the log contents.

**Email Now:** This option will send a copy of the router log to the email address configured in the Tools > Email screen.

**Save Log:** This option will save the router to a log file on your computer.

**D-Link**

DIR-628

DEVICE INFO

LOGS

STATISTICS

INTERNET SESSIONS

WIRELESS

SETUP

ADVANCED

TOOLS

STATUS

SUPPORT

**LOGS**

Use this option to view the router logs. You can define what types of events you want to view and the event levels to view. This router also has external syslog server support so you can send the log files to a computer on your network that is running a syslog utility.

**LOG OPTIONS**

What to View :  Firewall & Security  System  Router Status

View Levels :  Critical  Warning  Informational

Apply Log Settings Now

**LOG DETAILS**

Refresh Clear Email Now Save Log

281 Log Entries:

Priority	Time	Message
[WARN]	Sat Jan 31 12:05:37 2004	Blocked packet from 192.168.69.101 to 192.168.69.101 (LAND Attack)
[INFO]	Sat Jan 31 12:01:02 2004	Above message repeated 25 times
[INFO]	Sat Jan 31 12:00:08 2004	Blocked incoming TCP packet from 64.4.23.60-443 to 192.168.69.101-49567 as RST:ACK received but there is no active connection
[WARN]	Sat Jan 31 11:56:36 2004	Blocked packet from 192.168.69.101 to 192.168.69.101 (LAND Attack)
[INFO]	Sat Jan 31 11:47:32 2004	Above message repeated 38 times
[INFO]	Sat Jan 31 11:43:56 2004	Blocked incoming TCP packet from 63.111.24.33-80 to 192.168.69.101-1202 as SYN:ACK received but there is no active connection
[WARN]	Sat Jan 31 11:43:06 2004	Blocked packet from 192.168.69.101 to 192.168.69.101 (LAND Attack)

Helpful Hints...  
Check the log frequently to detect unauthorized network usage.  
You can also have the log mailed to you periodically. Refer to [Tools](#) → [Email](#).  
[More...](#)

# Stats

The screen below displays the Traffic Statistics. Here you can view the amount of packets that pass through the DIR-628 on both the WAN and the LAN ports. The traffic counter will reset if the device is rebooted.

DIR-628	SETUP	ADVANCED	TOOLS	STATUS	SUPPORT
<p><b>TRAFFIC STATISTICS</b></p> <p>Traffic Statistics display Receive and Transmit packets passing through your router.</p> <p>Refresh Statistics <input type="button" value="Clear Statistics"/></p>					
<p><b>LAN STATISTICS</b></p> <p>Sent : 2495888      Received : 2922256</p> <p>TX Packets Dropped : 0      RX Packets Dropped : 0</p> <p>Collisions : 0      Errors : 0</p>					
<p><b>WAN STATISTICS</b></p> <p>Sent : 39193      Received : 53732</p> <p>TX Packets Dropped : 0      RX Packets Dropped : 0</p> <p>Collisions : 0      Errors : 0</p>					
<p><b>WIRELESS STATISTICS</b></p> <p>Sent : 428553      Received : 195327</p> <p>TX Packets Dropped : 0      RX Packets Dropped : 0</p> <p>Errors : 16</p>					
<p><b>Helpful Hints...</b></p> <p>This is a summary of the number of packets that have passed between the WAN and the LAN since the router was last initialized.</p> <p><a href="#">More...</a></p>					

## Internet Sessions

The Internet Sessions page displays full details of active Internet sessions through your router. An Internet session is a conversation between a program or application on a LAN-side computer and a program or application on a WAN-side computer.

**Local:** The IP address and, where appropriate, port number of the local application.

**NAT:** The port number of the LAN-side application as viewed by the WAN-side application.

**Internet:** The IP address and, where appropriate, port number of the application on the Internet.

**Protocol:** The communications protocol used for the conversation.

**State:** State for sessions that use the TCP protocol:

**NO: None** -- This entry is used as a placeholder for a future connection that may occur.  
**SS: SYN Sent** -- One of the systems is attempting to start a connection.

**EST: Established** -- the connection is passing data.

**FW: FIN Wait** -- The client system has requested that the connection be stopped.

**CW: Close Wait** -- The server system has requested that the connection be stopped.

**TW: Time Wait** -- Waiting for a short time while a connection that was in FIN Wait is fully closed.

**LA: Last ACK** -- Waiting for a short time while a connection that was in Close Wait is fully closed.

**CL: Closed** -- The connection is no longer active but the session is being tracked in case there are any retransmitted packets still pending.

The screenshot shows the D-Link DIR-628 Internet Sessions page. The main content is a table of active internet sessions. The table has the following columns: Local, NAT, Internet, Protocol, State, Dir, Priority, and Time Out. The data rows show various IP addresses and port numbers for local and NAT, with corresponding Internet IP addresses and port numbers, protocols (TCP or UDP), states (SS, -), and time out values (128, 238, 293, 283, 279, 278, 226, 273, 221, 221, 272, 269, 265, 258, 254).

Local	NAT	Internet	Protocol	State	Dir	Priority	Time Out
192.168.0.197:50597	50597	66.199.250.170:8911	TCP	SS	Out	128	238
192.168.0.197:50596	50596	72.51.37.237:8899	TCP	SS	Out	128	238
192.168.0.197:50595	50595	219.239.90.172:28221	TCP	SS	Out	128	238
192.168.0.197:50594	50594	80.252.110.146:4661	TCP	SS	Out	128	238
192.168.0.197:41787	41787	80.239.200.102:3004	UDP	-	Out	128	293
192.168.0.197:41787	41787	80.239.200.104:3004	UDP	-	Out	128	283
192.168.0.197:41787	41787	222.186.190.39:4073	UDP	-	Out	128	279
192.168.0.197:41787	41787	80.239.200.109:3004	UDP	-	Out	128	278
192.168.0.197:50591	50591	60.28.197.35:28221	TCP	SS	Out	128	226
192.168.0.197:41787	41787	72.51.37.107:9127	UDP	-	Out	128	273
192.168.0.197:50589	50589	72.51.37.237:8899	TCP	SS	Out	128	221
192.168.0.197:50590	50590	66.199.250.170:8911	TCP	SS	Out	128	221
192.168.0.197:50587	50587	80.252.110.146:4661	TCP	SS	Out	128	221
192.168.0.197:50588	50588	219.239.90.172:28221	TCP	SS	Out	128	221
192.168.0.197:41787	41787	62.241.53.4:4246	UDP	-	Out	128	272
192.168.0.197:41787	41787	62.241.53.2:4246	UDP	-	Out	128	269
192.168.0.197:41787	41787	80.239.200.99:3004	UDP	-	Out	128	265
192.168.0.197:41787	41787	80.239.200.103:3004	UDP	-	Out	128	258
192.168.0.197:41787	41787	62.241.53.16:4246	UDP	-	Out	128	254

Helpful Hints...  
 This is a list of all active conversations between WAN computers and LAN computers.  
[More...](#)

**Dir:** The direction of initiation of the conversation:

**Out** - Initiated from LAN to WAN.

**In** - Initiated from WAN to LAN.

**Priority:** The preference given to outbound packets of this conversation by the QoS Engine logic. Smaller numbers represent higher priority.

**Time Out:** The number of seconds of idle time until the router considers the session terminated. The initial value of Time Out depends on the type and state of the connection.

**300 seconds** - UDP connections.

**240 seconds** - Reset or closed TCP connections. The connection does not close instantly so that lingering packets can pass or the connection can be re-established.

**7800 seconds** - Established or closing TCP connections.

# Wireless

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

**D-Link**

DIR-628

SETUP ADVANCED TOOLS STATUS SUPPORT

**WIRELESS**

**Associated Wireless Client List**

Use this option to view the wireless clients that are connected to your wireless router.

**NUMBER OF WIRELESS CLIENTS : 1**

MAC Address	IP Address	Mode	Rate	Signal(%)
00:03:2F:11:23:28	192.168.0.127	11g	54	100

**Helpful Hints...**

This is a list of all wireless clients that are currently connected to your wireless router.

[More...](#)

**WIRELESS**

# Support

<b>D-Link</b>					
<b>DIR-628</b>	<b>SETUP</b>	<b>ADVANCED</b>	<b>TOOLS</b>	<b>STATUS</b>	<b>SUPPORT</b>
MENU	<b>SUPPORT MENU</b>				
SETUP	<ul style="list-style-type: none"> <li>• <a href="#">Setup</a></li> <li>• <a href="#">Advanced</a></li> <li>• <a href="#">Tools</a></li> <li>• <a href="#">Status</a></li> </ul>				
ADVANCED					
TOOLS					
STATUS					
<b>SETUP HELP</b>					
<ul style="list-style-type: none"> <li>• <a href="#">Internet Connection</a></li> <li>• <a href="#">WAN</a></li> <li>• <a href="#">Wireless</a></li> <li>• <a href="#">Network Settings</a></li> </ul>					
<b>ADVANCED HELP</b>					
<ul style="list-style-type: none"> <li>• <a href="#">Virtual Server</a></li> <li>• <a href="#">Port Forwarding</a></li> <li>• <a href="#">Application Rules</a></li> <li>• <a href="#">DOS Engine</a></li> <li>• <a href="#">Access Control</a></li> <li>• <a href="#">Website Filter</a></li> <li>• <a href="#">Network Filter</a></li> <li>• <a href="#">Firewall Settings</a></li> <li>• <a href="#">Inbound Filter</a></li> <li>• <a href="#">Advanced Wireless</a></li> <li>• <a href="#">Wi-Fi Protected Setup</a></li> <li>• <a href="#">Advanced Network</a></li> </ul>					
<b>TOOLS HELP</b>					
<ul style="list-style-type: none"> <li>• <a href="#">Admin</a></li> <li>• <a href="#">Time</a></li> <li>• <a href="#">Syslog</a></li> <li>• <a href="#">Email Settings</a></li> <li>• <a href="#">System</a></li> <li>• <a href="#">Firmware</a></li> <li>• <a href="#">Dynamic DNS</a></li> <li>• <a href="#">System Check</a></li> <li>• <a href="#">Schedules</a></li> </ul>					
<b>STATUS HELP</b>					
<ul style="list-style-type: none"> <li>• <a href="#">Device Info</a></li> <li>• <a href="#">Wireless</a></li> <li>• <a href="#">Logs</a></li> <li>• <a href="#">Statistics</a></li> <li>• <a href="#">Internet Sessions</a></li> </ul>					
<b>WIRELESS</b>					

# Wireless Security

This section will show you the different levels of security you can use to protect your data from intruders. The DIR-655 offers the following types of security:

- WPA2 (Wi-Fi Protected Access 2)
- WPA (Wi-Fi Protected Access)
- WPA2-PSK (Pre-Shared Key)
- WPA-PSK (Pre-Shared Key)

## What is WPA?

WPA, or Wi-Fi Protected Access, is a Wi-Fi standard that was designed to improve the security features of WEP (Wired Equivalent Privacy).

The 2 major improvements over WEP:

- Improved data encryption through the Temporal Key Integrity Protocol (TKIP). TKIP scrambles the keys using a hashing algorithm and, by adding an integrity-checking feature, ensures that the keys haven't been tampered with. WPA2 is based on 802.11i and uses Advanced Encryption Standard (AES) instead of TKIP.
- User authentication, which is generally missing in WEP, through the extensible authentication protocol (EAP). WEP regulates access to a wireless network based on a computer's hardware-specific MAC address, which is relatively simple to be sniffed out and stolen. EAP is built on a more secure public-key encryption system to ensure that only authorized network users can access the network.

WPA-PSK/WPA2-PSK uses a passphrase or key to authenticate your wireless connection. The key is an alpha-numeric password between 8 and 63 characters long. The password can include symbols (!?\*&\_) and spaces. This key must be the exact same key entered on your wireless router or access point.

WPA/WPA2 incorporates user authentication through the Extensible Authentication Protocol (EAP). EAP is built on a more secure public key encryption system to ensure that only authorized network users can access the network.



# Wireless Security Setup Wizard

To run the security wizard, click on Setup at the top and then click **Launch Wireless Security Setup Wizard**.



Type your desired wireless network name (SSID).

**Automatically:** Select this option to automatically generate the router's network key and click **Next**.

**Manually:** Select this option to manually enter your network key and click **Next**.

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

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

Network Name (SSID) : dir628a1

- Automatically assign a network key (Recommended)

To prevent outsiders from accessing your network, the router will automatically assign a security (also called WEP or WPA key) to your network.

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

- Use WPA encryption instead of WEP (WPA is stronger than WEP and all D-Link wireless client adapters support WPA)

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

Prev Next Cancel Save

If you selected **Automatically**, the summary window will display your settings. Write down the security key and enter this on your wireless clients. Click **Save** to save your settings.

**SETUP COMPLETE!**

Below is a detailed summary of your wireless security settings. Please print this page out, or write the information on a piece of paper, so you can configure the correct settings on your wireless client adapters.

Wireless Network Name : dir628a1  
(SSID) :

Security Mode : Auto (WPA or WPA2) - Personal  
Cipher Type : TKIP and AES  
Pre-Shared Key : 21b2e5486fa27a749b051e4c457212231e8597ea9effc179d63faae60a066a

Prev Next Cancel Save

If you selected **Manually**, the following screen will appear.

**STEP 2: SET YOUR WIRELESS SECURITY PASSWORD**

You have selected your security level - you will need to set a wireless security password.

The WPA (Wi-Fi Protected Access) key must meet one of following guidelines:

- Between 8 and 64 characters (A longer WPA key is more secure than a short one)
- Exactly 64 characters using 0-9 and A-F

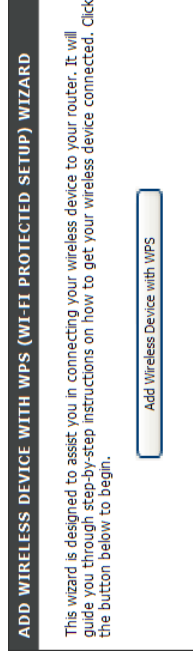
Wireless Security Password :

Note: You will need to enter the same password as keys in this step into your wireless clients in order to enable proper wireless communication.

Prev Next Cancel Save

## Add Wireless Device with WPS Wizard

From the **Basic** > **Wizard** screen, click **Add Wireless Device with WPS**.



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

If you select **Manual**, a settings summary screen will appear. Write down the security key and enter this on your wireless clients.



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

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



# Configure WPA-Personal (PSK)

It is recommended to enable encryption on your wireless router before your wireless network adapters. Please establish wireless connectivity before enabling encryption. Your wireless signal may degrade when enabling encryption due to the added overhead.

1. Log into the web-based configuration by opening a web browser and entering the IP address of the router (192.168.0.1). Click on **Setup** and then click **Wireless Settings** on the left side.
2. Next to **Security Mode**, select **WPA-Personal**.
3. Next to **WPA Mode**, select **Auto**, **WPA2 Only**, or **WPA Only**. Use **Auto** if you have wireless clients using both WPA and WPA2.
4. Next to **Cypher Type**, select **TKIP and AES**, **TKIP**, or **AES**.
5. Next to **Group Key Update Interval**, enter the amount of time before the group key used for broadcast and multicast data is changed (3600 is default).

**WIRELESS SECURITY MODE**

To protect your privacy you can configure wireless security features. This device supports two wireless security modes including: WPA-Personal, and WPA-Enterprise. WPA provides a higher level of security. WPA-Personal does not require an authentication server. The WPA-Enterprise option requires an external RADIUS server.

Security Mode: WPA-Personal

---

**WPA**

WPA requires stations to use high grade encryption and authentication. For legacy compatibility, use **WPA** or **WPA2** mode. This mode uses WPA for legacy clients while maintaining higher security with stations that are WPA2 capable. The strongest cipher that the client supports will be used. For best security, use **WPA2 Only** mode. In this mode, legacy stations are not allowed access with WPA security. The AES cipher will be used across the wireless network to ensure best security.

WPA Mode: Auto (WPA or WPA2)

Cipher Type: TKIP and AES

Group Key Update Interval: 3600 (seconds)

---

**PRE-SHARED KEY**

Pre-Shared Key: ••••••••

6. Next to **Pre-Shared Key**, enter a key (passphrase). The key is entered as a pass-phrase in ASCII format at both ends of the wireless connection. The pass-phrase must be between 8-63 characters.
7. Click **Save Settings** to save your settings. If you are configuring the router with a wireless adapter, you will lose connectivity until you enable WPA-PSK on your adapter and enter the same passphrase as you did on the router.

# Configure WPA-Enterprise (RADIUS)

It is recommended to enable encryption on your wireless router before your wireless network adapters. Please establish wireless connectivity before enabling encryption. Your wireless signal may degrade when enabling encryption due to the added overhead.

1. Log into the web-based configuration by opening a web browser and entering the IP address of the router (192.168.0.1). Click on **Setup** and then click **Wireless Settings** on the left side.
2. Next to **Security Mode**, select **WPA-Enterprise**.
3. Next to **WPA Mode**, select **Auto**, **WPA2 Only**, or **WPA Only**. Use **Auto** if you have wireless clients using both WPA and WPA2.
4. Next to **Cypher Type**, select **TKIP and AES**, **TKIP**, or **AES**.
5. Next to **Group Key Update Interval**, enter the amount of time before the group key used for broadcast and multicast data is changed (3600 is default).
6. Next to **Authentication Timeout**, enter the amount of time before a client is required to re-authenticate (60 minutes is default).
7. Next to **RADIUS Server IP Address** enter the IP Address of your RADIUS server.

**WIRELESS SECURITY MODE**

To protect your privacy you can configure wireless security features. This device supports two wireless security modes including: WPA-Personal and WPA-Enterprise. WPA provides a higher level of security. WPA-Personal does not require an authentication server. The WPA-Enterprise option requires an external RADIUS server.

**Security Mode :** WPA-Enterprise

---

**WPA**

WPA requires stations to use high grade encryption and authentication. For legacy compatibility, use **WPA** or **WPA2** mode. This mode uses WPA for legacy clients while maintaining higher security with stations that are WPA2 capable. The strongest cipher that the client supports will be used. For best security, use **WPA2 Only** mode. In this mode, legacy stations are not allowed access with WPA security. The AES cipher will be used across the wireless network to ensure best security.

**WPA Mode :** Auto (WPA or WPA2)

**Cipher Type :** TKIP and AES

**Group Key Update Interval :** 3600 (seconds)

---

**EAP (802.1X)**

When WPA enterprise is enabled, the router uses EAP (802.1x) to authenticate clients via a remote RADIUS server.

**Authentication Timeout :** 60 (minutes)

**RADIUS server IP Address :** 0.0.0.0

**RADIUS server Port :** 1812

**RADIUS server Shared Secret :** radius\_shared

**MAC Address Authentication :**

[Advanced >>](#)

8. Next to *RADIUS Server Port*, enter the port you are using with your RADIUS server. 1812 is the default port.

9. Next to *RADIUS Server Shared Secret*, enter the security key.

10. If the *MAC Address Authentication* box is selected then the user will need to connect from the same computer whenever logging into the wireless network.

11. Click **Advanced** to enter settings for a secondary RADIUS Server.

12. Click **Apply Settings** to save your settings.

**EAP (802.1X)**

When WPA enterprise is enabled, the router uses EAP (802.1x) to authenticate clients via a remote RADIUS server.

Authentication Timeout :	60 (minutes)
RADIUS server IP Address :	0.0.0.0
RADIUS server Port :	1812
RADIUS server Shared Secret :	radius_shared
MAC Address Authentication :	<input checked="" type="checkbox"/>

<< **Advanced**

Optional backup RADIUS server :

Second RADIUS server IP Address :	0.0.0.0
Second RADIUS server Port :	1812
Second RADIUS server Shared Secret :	radius_shared
Second MAC Address Authentication :	<input checked="" type="checkbox"/>

# Connect to a Wireless Network

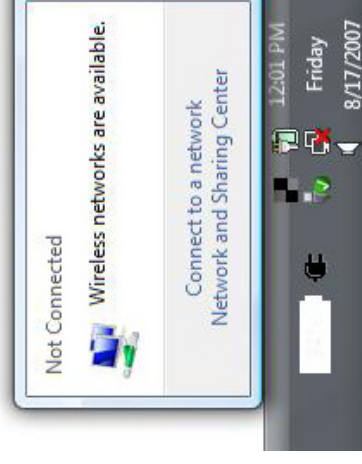
## Using Windows Vista®

Windows Vista® users may use the built-in wireless utility. If you are using another company's utility or Windows® 2000, please refer to the user manual of your wireless adapter for help with connecting to a wireless network. Most utilities will have a "site survey" option similar to the Windows Vista® utility as seen below.

If you receive the **Wireless Networks Detected** bubble, click on the center of the bubble to access the utility.

or

Right-click on the wireless computer icon in your system tray (lower-right corner next to the time). Select **Connect to a network**.



The utility will display any available wireless networks in your area. Click on a network (displayed using the SSID) and click the **Connect** button.

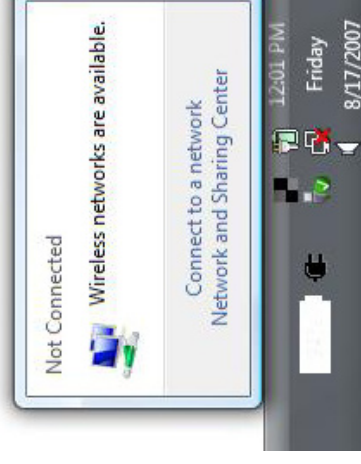
If you get a good signal but cannot access the Internet, check you TCP/IP settings for your wireless adapter. Refer to the **Networking Basics** section in this manual for more information.



# Configure Wireless Security

It is recommended to enable wireless security (WPA/WPA2) on your wireless router or access point before configuring your wireless adapter. If you are joining an existing network, you will need to know the security key or passphrase being used.

1. Open the Windows Vista® Wireless Utility by right-clicking on the wireless computer icon in your system tray (lower right corner of screen). Select **Connect to a network**.



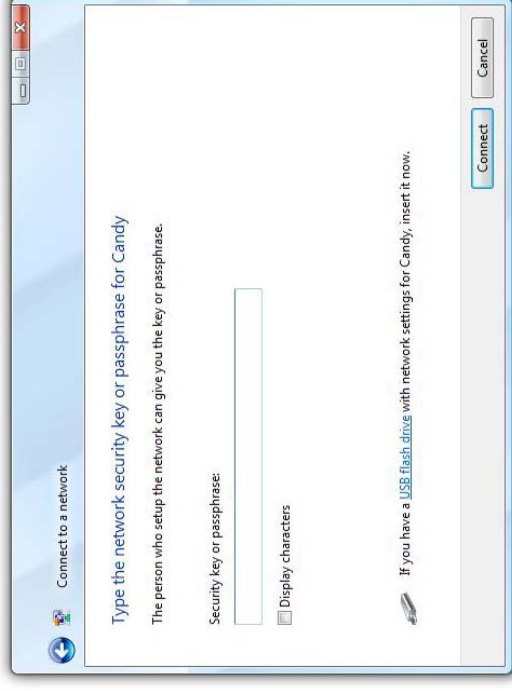
2. Highlight the wireless network (SSID) you would like to connect to and click **Connect**.





**3. Enter the same security key or passphrase that is on your router and click **Connect**.**

It may take 20-30 seconds to connect to the wireless network. If the connection fails, please verify that the security settings are correct. The key or passphrase must be exactly the same as on the wireless router.



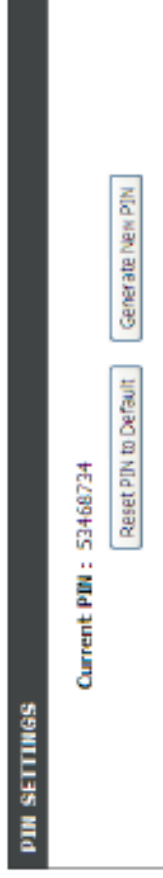
## Connect Using WCN 2.0 in Windows Vista®

The router supports Wi-Fi protection, referred to as WCN 2.0 in Windows Vista®. The following instructions for setting this up depends on whether you are using Windows Vista® to configure the router or third party software.

When you first set up the router, Wi-Fi protection is disabled and unconfigured. To enjoy the benefits of Wi-Fi protection, the router must be both enabled and configured. There are three basic methods to accomplish this: use Windows Vista's built-in support for WCN 2.0, use software provided by a third party, or manually configure.

If you are running Windows Vista®, log into the router and click the **Enable** checkbox in the **Basic** > **Wireless** section. Use the Current PIN that is displayed on the **Advanced** > **Wi-Fi Protected Setup** section or choose to click the **Generate New PIN** button or **Reset PIN to Default** button.

For additional information, please refer to page 46.



If you are using third party software to set up Wi-Fi Protection, carefully follow the directions. When you are finished, proceed to the next section to set up the newly-configured router.

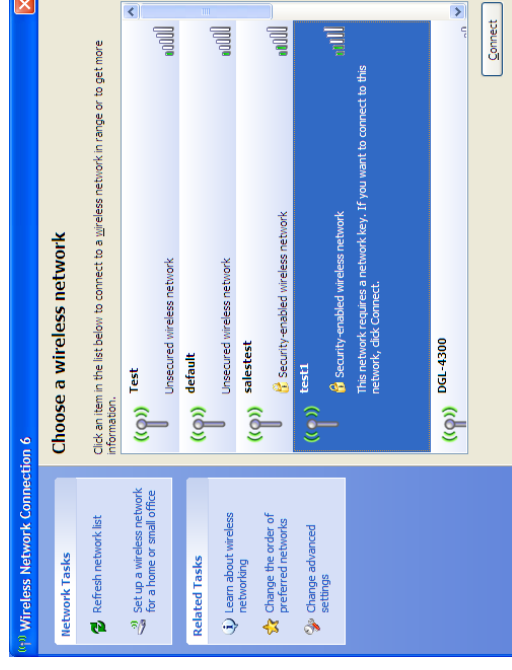
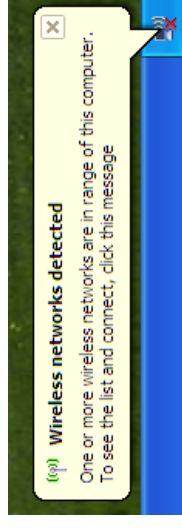
# Connect to a Wireless Network Using Windows® XP

Windows® XP users may use the built-in wireless utility (Zero Configuration Utility). The following instructions are for Service Pack 2 users. If you are using another company's utility or Windows® 2000, please refer to the user manual of your wireless adapter for help with connecting to a wireless network. Most utilities will have a "site survey" option similar to the Windows® XP utility as seen below.

If you receive the **Wireless Networks Detected** bubble, click on the center of the bubble to access the utility.

or

Right-click on the wireless computer icon in your system tray (lower-right corner next to the time). Select **View Available Wireless Networks**.



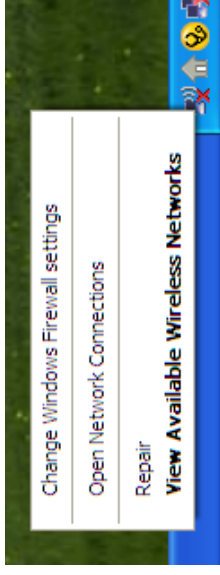
The utility will display any available wireless networks in your area. Click on a network (displayed using the SSID) and click the **Connect** button.

If you get a good signal but cannot access the Internet, check you TCP/IP settings for your wireless adapter. Refer to the **Networking Basics** section in this manual for more information.

# Configure WPA-PSK

It is recommended to enable encryption on your wireless router or access point before configuring your wireless adapter. If you are joining an existing network, you will need to know the passphrase being used.

1. Open the Windows® XP Wireless Utility by right-clicking on the wireless computer icon in your system tray (lower-right corner of screen). Select **View Available Wireless Networks**.

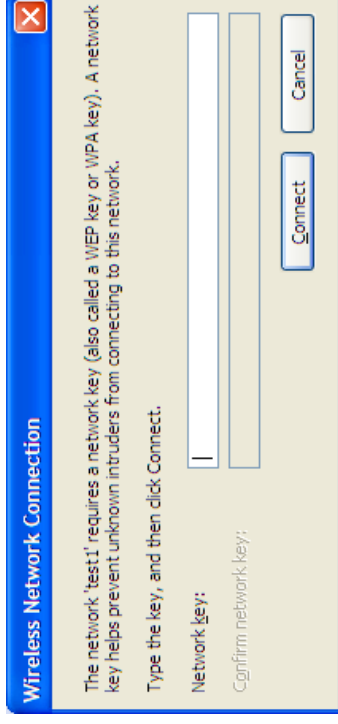


2. Highlight the wireless network (SSID) you would like to connect to and click **Connect**.



3. The **Wireless Network Connection** box will appear. Enter the WPA-PSK passphrase and click **Connect**.

It may take 20-30 seconds to connect to the wireless network. If the connection fails, please verify that the WPA-PSK settings are correct. The WPA-PSK passphrase must be exactly the same as on the wireless router.



# Troubleshooting

This chapter provides solutions to problems that can occur during the installation and operation of the DIR-628. Read the following descriptions if you are having problems. (The examples below are illustrated in Windows® XP. If you have a different operating system, the screenshots on your computer will look similar to the following examples.)

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

When entering the IP address of the D-Link router (192.168.0.1 for example), you are not connecting to a website on the Internet or have to be connected to the Internet. The device has the utility built-in to a ROM chip in the device itself. Your computer must be on the same IP subnet to connect to the web-based utility.

- Make sure you have an updated Java-enabled web browser. We recommend the following:
  - Internet Explorer 6.0 or higher
  - Netscape 8 or higher
  - Mozilla 1.7.12 (5.0) or higher
  - Opera 8.5 or higher
  - Safari 1.2 or higher (with Java 1.3.1 or higher)
  - Camino 0.8.4 or higher
  - Firefox 1.5 or higher
- Verify physical connectivity by checking for solid link lights on the device. If you do not get a solid link light, try using a different cable or connect to a different port on the device if possible. If the computer is turned off, the link light may not be on.
- Disable any Internet security software running on the computer. Software firewalls such as Zone Alarm, Black Ice, Sygate, Norton Personal Firewall, and Windows® XP firewall may block access to the configuration pages. Check the help files included with your firewall software for more information on disabling or configuring it.

• Configure your Internet settings:

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

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

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

To reset the router, locate the reset button (hole) on the rear panel of the unit. With the router powered on, use a paperclip to hold the button down for 10 seconds. Release the button and the router will go through its reboot process. Wait about 30 seconds to access the router. The default IP address is 192.168.0.1. When logging in, the username is **admin** and leave the password box empty.

### 3. Why can't I connect to certain sites or send and receive emails when connecting through my router?

If you are having a problem sending or receiving email, or connecting to secure sites such as eBay, banking sites, and Hotmail, we suggest lowering the MTU in increments of ten (Ex. 1492, 1482, 1472, etc).

**Note: AOL DSL+ users must use MTU of 1400.**

To find the proper MTU Size, you'll have to do a special ping of the destination you're trying to go to. A destination could be another computer, or a URL.

- Click on **Start** and then click **Run**.
- Windows® 95, 98, and Me users type in **command** (Windows® NT, 2000, and XP users type in **cmd**) and press **Enter** (or click **OK**).
- Once the window opens, you'll need to do a special ping. Use the following syntax:

**ping [url] [-f] [-l] [MTU value]**

**Example: ping yahoo.com -f -l 1472**

```
C:\>ping yahoo.com -f -l 1482
Pinging yahoo.com [66.94.234.13] with 1482 bytes of data:
Packet needs to be fragmented but DF set.
Packet needs to be fragmented but DF set.
Packet needs to be fragmented but DF set.
Ping statistics for 66.94.234.13:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
C:\>ping yahoo.com -f -l 1472
Pinging yahoo.com [66.94.234.13] with 1472 bytes of data:
Reply from 66.94.234.13: bytes=1472 time=93ms TTL=52
Reply from 66.94.234.13: bytes=1472 time=109ms TTL=52
Reply from 66.94.234.13: bytes=1472 time=125ms TTL=52
Reply from 66.94.234.13: bytes=1472 time=203ms TTL=52
Ping statistics for 66.94.234.13:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 93ms, Maximum = 203ms, Average = 132ms
C:\>
```



You should start at 1472 and work your way down by 10 each time. Once you get a reply, go up by 2 until you get a fragmented packet. Take that value and add 28 to the value to account for the various TCP/IP headers. For example, lets say that 1452 was the proper value, the actual MTU size would be 1480, which is the optimum for the network we're working with ( $1452+28=1480$ ).

Once you find your MTU, you can now configure your router with the proper MTU size.

To change the MTU rate on your router follow the steps below:

- Open your browser, enter the IP address of your router (192.168.0.1) and click **OK**.
- Enter your username (admin) and password (blank by default). Click **OK** to enter the web configuration page for the device.
- Click on **Setup** and then click **Manual Configure**.
- To change the MTU enter the number in the MTU field and click **Save Settings** to save your settings.
- Test your email. If changing the MTU does not resolve the problem, continue changing the MTU in increments of ten.

# Wireless Basics

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

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

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

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

## **What is Wireless?**

Wireless or Wi-Fi technology is another way of connecting your computer to the network without using wires. Wi-Fi uses radio frequency to connect wirelessly, so you have the freedom to connect computers anywhere in your home or office network.

## **Why D-Link Wireless?**

D-Link is the worldwide leader and award winning designer, developer, and manufacturer of networking products. D-Link delivers the performance you need at a price you can afford. D-Link has all the products you need to build your network.

## **How does wireless work?**

Wireless works similar to how cordless phone work, through radio signals to transmit data from one point A to point B. But wireless technology has restrictions as to how you can access the network. You must be within the wireless network range area to be able to connect your computer. There are two different types of wireless networks Wireless Local Area Network (WLAN), and Wireless Personal Area Network (WPAN).

## **Wireless Local Area Network (WLAN)**

In a wireless local area network, a device called an Access Point (AP) connects computers to the network. The access point has a small antenna attached to it, which allows it to transmit data back and forth over radio signals. With an indoor access point as seen in the picture, the signal can travel up to 300 feet. With an outdoor access point the signal can reach out up to 30 miles to serve places like manufacturing plants, industrial locations, college and high school campuses, airports, golf courses, and many other outdoor venues.

## **Wireless Personal Area Network (WPAN)**

Bluetooth is the industry standard wireless technology used for WPAN. Bluetooth devices in WPAN operate in a range up to 30 feet away.

Compared to WLAN the speed and wireless operation range are both less than WLAN, but in return it doesn't use nearly as much power which makes it ideal for personal devices, such as mobile phones, PDAs, headphones, laptops, speakers, and other devices that operate on batteries.

## **Who uses wireless?**

Wireless technology has become so popular in recent years that almost everyone is using it, whether it's for home, office, business, D-Link has a wireless solution for it.

### **Home**

- Gives everyone at home broadband access
- Surf the web, check email, instant message, and etc
- Gets rid of the cables around the house
- Simple and easy to use

### **Small Office and Home Office**

- Stay on top of everything at home as you would at office
- Remotely access your office network from home
- Share Internet connection and printer with multiple computers
- No need to dedicate office space

## **Where is wireless used?**

Wireless technology is expanding everywhere not just at home or office. People like the freedom of mobility and it's becoming so popular that more and more public facilities now provide wireless access to attract people. The wireless connection in public places is usually called "hotspots".

Using a D-Link Cardbus Adapter with your laptop, you can access the hotspot to connect to Internet from remote locations like: Airports, Hotels, Coffee Shops, Libraries, Restaurants, and Convention Centers.

Wireless network is easy to setup, but if you're installing it for the first time it could be quite a task not knowing where to start. That's why we've put together a few setup steps and tips to help you through the process of setting up a wireless network.

## **Tips**

Here are a few things to keep in mind, when you install a wireless network.

### **Centralize your router or Access Point**

Make sure you place the router/access point in a centralized location within your network for the best performance. Try to place the router/access point as high as possible in the room, so the signal gets dispersed throughout your home. If you have a two-story home, you may need a repeater to boost the signal to extend the range.

### **Eliminate Interference**

Place home appliances such as cordless telephones, microwaves, and televisions as far away as possible from the router/access point. This would significantly reduce any interference that the appliances might cause since they operate on same frequency.

## Security

Don't let you next-door neighbors or intruders connect to your wireless network. Secure your wireless network by turning on the WPA or WEP security feature on the router. Refer to product manual for detail information on how to set it up.

# Wireless Modes

There are basically two modes of networking:

- **Infrastructure** – All wireless clients will connect to an access point or wireless router.
- **Ad-Hoc** – Directly connecting to another computer, for peer-to-peer communication, using wireless network adapters on each computer, such as two or more DIR-628 wireless network Cardbus adapters.

An Infrastructure network contains an Access Point or wireless router. All the wireless devices, or clients, will connect to the wireless router or access point.

An Ad-Hoc network contains only clients, such as laptops with wireless cardbus adapters. All the adapters must be in Ad-Hoc mode to communicate.

# Networking Basics

## Check your IP address

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

Click on **Start** > **Run**. In the run box type **cmd** and click **OK**. (Windows Vista® users type **cmd** in the **Start Search** box.)

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

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

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

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



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

C:\Documents and Settings>ipconfig
Windows IP Configuration

Ethernet adapter Local Area Connection:

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

C:\Documents and Settings>
```

## Statically Assign an IP address

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

### Step 1

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

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

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

### Step 2

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

### Step 3

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

### Step 4

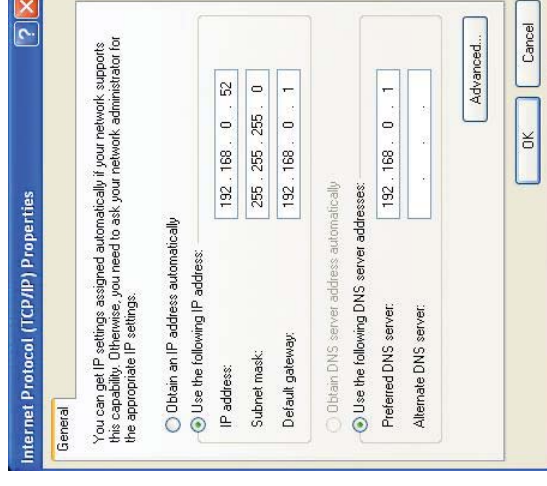
Click **Use the following IP address** and enter an IP address that is on the same subnet as your network or the LAN IP address on your router.

**Example:** If the router's LAN IP address is 192.168.0.1, make your IP address 192.168.0.X where X is a number between 2 and 99. Make sure that the number you choose is not in use on the network. Set Default Gateway the same as the LAN IP address of your router (192.168.0.1).

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

### Step 5

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





# Technical Specifications

## Standards

- IEEE 802.11n (draft)
- IEEE 802.11g
- IEEE 802.11a
- IEEE 802.3
- IEEE 802.3u

## Security

- WPA-Personal
- WPA2-Personal
- WPA-Enterprise
- WPA2-Enterprise

## Frequency Range

- 2.4GHz to 2.483GHz (802.11n/g)
- 5.15GHz to 5.25GHz (802.11a)
- 5.725GHz to 5.85GHz (802.11a)

## External Antenna Type

- Two (2) detachable reverse SMA Antennas

## LEDs

- Power
- WLAN
- Internet
- LAN (10/100)
- Status
- USB

## Operating Temperature

- 32°F to 131°F ( 0°C to 55°C)

## Humidity

- 95% maximum (non-condensing)

## Safety & Emissions

- FCC
- CE
- IC

## Dimensions

- L = 7.6 inches
- W = 4.6 inches
- H = 1.2inches

## Warranty

- 1 Year limited

\* Maximum wireless signal rate derived from IEEE Standard 802.11a, 802.11g and Draft 802.11n specifications. Actual data throughput will vary. Network conditions and environmental factors, including volume of network traffic, building materials and construction, and network overhead, lower actual data throughput rate. Environmental factors will adversely affect wireless signal range.

# Contacting Technical Support

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

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

- Model number of the product (e.g. DIR-628)
- Hardware Revision (located on the label on the bottom of the router (e.g. rev A1))
- Serial Number (s/n number located on the label on the bottom of the router).

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

## For customers within the United States:

**Phone Support:**  
(877) 453-5465

**Internet Support:**  
<http://support.dlink.com>

## For customers within Canada:

**Phone Support:**  
(800) 361-5265

**Internet Support:**  
<http://support.dlink.com>

# Warranty

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

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

## Limited Warranty:

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

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

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

### **Limited Software Warranty:**

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

### **Non-Applicability of Warranty:**

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

### **Submitting A Claim:**

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

- The customer must submit with the product as part of the claim a written description of the Hardware defect or Software nonconformance in sufficient detail to allow DLink to confirm the same, along with proof of purchase of the product (such as a copy of the dated purchase invoice for the product) if the product is not registered.
- The customer must obtain a Case ID Number from D-Link Technical Support at 1-877-453-5465, who will attempt to assist the customer in resolving any suspected defects with the product. If the product is considered defective, the customer must obtain a Return Material Authorization (“RMA”) number by completing the RMA form and entering the assigned Case ID Number at <https://rma.dlink.com/>.

- After an RMA number is issued, the defective product must be packaged securely in the original or other suitable shipping package to ensure that it will not be damaged in transit, and the RMA number must be prominently marked on the outside of the package. Do not include any manuals or accessories in the shipping package. DLink will only replace the defective portion of the product and will not ship back any accessories.
- The customer is responsible for all in-bound shipping charges to D-Link. No Cash on Delivery (“COD”) is allowed. Products sent COD will either be rejected by D-Link or become the property of D-Link. Products shall be fully insured by the customer and shipped to D-Link Systems, Inc., 17595 Mt. Herrmann, Fountain Valley, CA 92708. D-Link will not be held responsible for any packages that are lost in transit to D-Link. The repaired or replaced packages will be shipped to the customer via UPS Ground or any common carrier selected by D-Link. Return shipping charges shall be prepaid by D-Link if you use an address in the United States, otherwise we will ship the product to you freight collect. Expedited shipping is available upon request and provided shipping charges are prepaid by the customer. D-Link may reject or return any product that is not packaged and shipped in strict compliance with the foregoing requirements, or for which an RMA number is not visible from the outside of the package. The product owner agrees to pay D-Link’s reasonable handling and return shipping charges for any product that is not packaged and shipped in accordance with the foregoing requirements, or that is determined by D-Link not to be defective or non-conforming.

### **What Is Not Covered:**

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

While necessary maintenance or repairs on your Product can be performed by any company, we recommend that you use only an Authorized D-Link Service Office. Improper or incorrectly performed maintenance or repair voids this Limited Warranty.

### **Disclaimer of Other Warranties:**

EXCEPT FOR THE LIMITED WARRANTY SPECIFIED HEREIN, THE PRODUCT IS PROVIDED “AS-IS” WITHOUT ANY WARRANTY OF ANY KIND WHATSOEVER INCLUDING, WITHOUT LIMITATION, ANY WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT.

IF ANY IMPLIED WARRANTY CANNOT BE DISCLAIMED IN ANY TERRITORY WHERE A PRODUCT IS SOLD, THE DURATION OF SUCH IMPLIED WARRANTY SHALL BE LIMITED TO THE DURATION OF THE APPLICABLE WARRANTY PERIOD SET FORTH ABOVE. EXCEPT AS EXPRESSLY COVERED UNDER THE LIMITED WARRANTY PROVIDED HEREIN, THE ENTIRE RISK AS TO THE QUALITY, SELECTION AND PERFORMANCE OF THE PRODUCT IS WITH THE PURCHASER OF THE PRODUCT.

**Limitation of Liability:**

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

**Governing Law:**

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

**Trademarks:**

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

**Copyright Statement:**

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

Copyright ©2008 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 communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one of the following measures:

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

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

### **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.

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions:

- (1) This device may not cause harmful interference, and
- (2) this device must accept any interference received, including interference that may cause undesired operation.

### **IMPORTANT NOTE:**

#### **FCC Radiation Exposure Statement:**

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. 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. If this device is going to be operated in 5.15 ~ 5.25GHz frequency range, then it is restricted in indoor environment only.

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

The availability of some specific channels and/or operational frequency bands are country dependent and are firmware programmed at the factory to match the intended destination. The firmware setting is not accessible by the end user.

We declare that the product is limited in CH1 ~CH11 by specified firmware controlled in the USA.

### **IC statement**

Operation is subject to the following two conditions:

- 1) This device may not cause interference and
- 2) This device must accept any interference, including interference that may cause undesired operation of the device.

This device has been designed to operate with an antenna having a maximum gain of 2 dBi. Antenna having a higher gain is strictly prohibited per regulations of Industry Canada. The required antenna impedance is 50 ohms.

### **IMPORTANT NOTE:**

#### **IC Radiation Exposure Statement:**

This equipment complies with IC radiation exposure limits set forth for an uncontrolled environment. End users must follow the specific operating instructions for satisfying RF exposure compliance. This equipment should be installed and operated with minimum distance 20cm between the radiator & your body.

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

- (i) the device for the band 5150-5250 MHz is only for indoor usage to reduce potential for harmful interference to co-channel mobile satellite systems;
- (ii) the maximum antenna gain (2dBi) permitted (for devices in the band 5725-5825 MHz) to comply with the e.i.r.p. limits specified for point-to-point and non point-to-point operation as appropriate, as stated in section A9.2(3).

In addition, users should also be cautioned to take note that high-power radars are allocated as primary users (meaning they have priority) of the bands 5250-5350 MHz and 5650-5850 MHz and these radars could cause interference and/or damage to LE-LAN devices.

#### **Règlement d'Industry Canada**

Les conditions de fonctionnement sont sujettes à deux conditions:

- 1) Ce périphérique ne doit pas causer d'interférence et.
- 2) Ce périphérique doit accepter toute interférence, y compris les interférences pouvant perturber le bon fonctionnement de ce périphérique.

The Class [B] digital apparatus meets all requirements of the Canadian Interference-Causing Equipment Regulation.

Cet appareil numérique de la class [B] respecte toutes les exigences du Règlement sur le matériel brouilleur du Canada.



# Registration



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

Version 1.2  
May 20, 2008