

## Register mydlink Service Wizard: Step 2

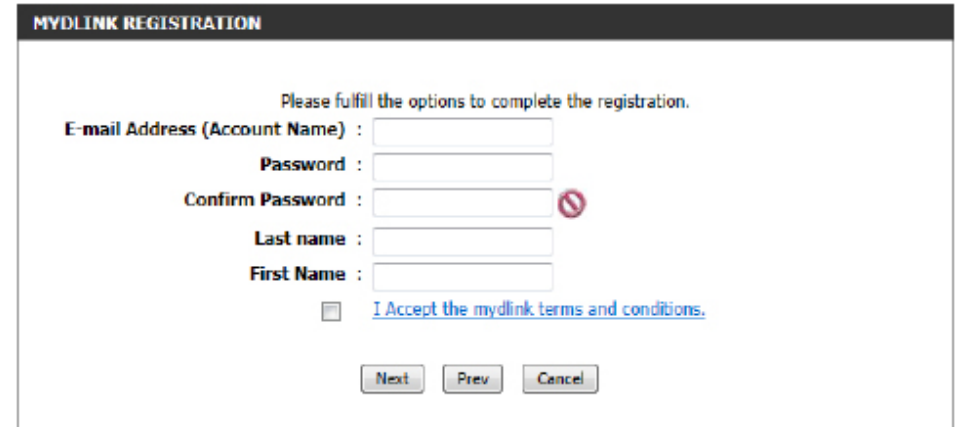
When registering a **new account**, the following page appears. The following parameters will be available for configuration:

- E-mail Address (Account Name):** Enter your e-mail address here. This e-mail address will also become your account name.
- Password:** Enter your preferred password choice here.
- Confirm Password:** Re-enter your preferred password choice here.
- Last Name:** Enter your last name here.
- First Name:** Enter your first name here.
- Accept terms and conditions:** Tick this option to accept the mydlink terms and conditions.

Click the **Next** button to proceed to the next step.

Click the **Prev** button to return to the previous step.

Click the **Cancel** button to discard the changes made and return to the main page.



The screenshot shows a web form titled "MYDLINK REGISTRATION" with a dark header. Below the header, it says "Please fulfill the options to complete the registration." The form contains the following fields and controls:

- E-mail Address (Account Name) :** A text input field.
- Password :** A text input field.
- Confirm Password :** A text input field with a red prohibition sign (a circle with a diagonal slash) to its right, indicating it is required.
- Last name :** A text input field.
- First Name :** A text input field.
- [I Accept the mydlink terms and conditions.](#)
- At the bottom, there are three buttons: **Next**, **Prev**, and **Cancel**.

When logging in with an **existing account**, the following page appears. The following parameters will be available for configuration:

- E-mail Address (Account Name):** Enter your e-mail address here. This e-mail address will also be your account name.
- Password:** Enter your preferred password choice here.

Click the **Login** button to login using these account details.

Click the **Prev** button to return to the previous step.

Click the **Cancel** button to discard the changes made and return to the main page.



The screenshot shows a web form titled "MYDLINK REGISTRATION" with a dark header. Below the header, it says "Please fulfill the options to complete the registration." The form contains the following fields and controls:

- E-mail Address (Account Name) :** A text input field.
- Password :** A text input field.
- At the bottom, there are three buttons: **Login**, **Prev**, and **Cancel**.

---

At any point during this wizard, we can change the preferred language used. To change the language, select the desired language option from the **Language** drop-down menu, found on the top right of this page.

### End of Wizard



# Advanced Virtual Server

This will allow you to open a single port. If you would like to open a range of ports, refer to the next page.

**Name:** Enter a name for the rule or select an application from the drop-down menu. Select an application and click << to populate the fields.

**IP Address:** Enter the IP address of the computer on your local network that you want to allow the incoming service to. If your computer is receiving an IP address automatically from the router (DHCP), your computer will be listed in the "Computer Name" drop-down menu. Select your computer and click <<.

**Private Port/ Public Port:** Enter the port that you want to open 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 Internet side, and the private port is the port being used by the application on the computer within your local network.

**Protocol Type:** Select **TCP**, **UDP**, or **Both** from the drop-down menu.

**Schedule:** The schedule of time when the Virtual Server Rule will be enabled. The schedule may be set to **Always**, which will allow the particular service to always be enabled. You can create your own times in the **Tools > Schedules** section.

**Inbound Filter:** Select **Allow All** (most common) or a created Inbound filter. You may create your own inbound filters in the **Advanced > Inbound Filter** page.

**VIRTUAL SERVER**

The Virtual Server option allows you to define a single public port on your router for redirection to an internal LAN IP Address and Private LAN port if required. This feature is useful for hosting online services such as FTP or Web Servers.

24 - VIRTUAL SERVERS LIST					
Remaining number of rules that can be created: 24					
			Port	Traffic Type	
<input type="checkbox"/>	Name	<< Application name ▾	Public Port	Protocol	Schedule
				Both ▾	Always ▾
	IP Address	<< Computer Name ▾	Private Port		Inbound Filter
					Allow All ▾
<input type="checkbox"/>	Name	<< Application name ▾	Public Port	Protocol	Schedule
				Both ▾	Always ▾
	IP Address	<< Computer Name ▾	Private Port		Inbound Filter
					Allow All ▾

## Port Forwarding

This will allow you to open a single port or a range of ports.

**Name:** Enter a name for the rule or select an application from the drop-down menu. Select an application and click << to populate the fields.

**IP Address:** Enter the IP address of the computer on your local network that you want to allow the incoming service to. If your computer is receiving an IP address automatically from the router (DHCP), you computer will be listed in the "Computer Name" drop-down menu. Select your computer and click <<.

**TCP/UDP:** Enter the TCP and/or UDP port or ports that you want to open. You can enter a single port or a range of ports. Separate ports with a comma.

Example: 24,1009,3000-4000

**Schedule:** The schedule of time when the Virtual Server Rule will be enabled. The schedule may be set to **Always**, which will allow the particular service to always be enabled. You can create your own times in the **Tools > Schedules** section.

**Inbound Filter:** Select **Allow All** (most common) or a created Inbound filter. You may create your own inbound filters in the **Advanced > Inbound Filter** page.

**PORT FORWARDING**

This option is used to open multiple ports or a range of ports in your router and redirect data through those ports to a single PC on your network. This feature allows you to enter ports in the format, Port Ranges (100-150), Individual Ports (80, 68, 888), or Mixed (1020-5000, 689). This option is only applicable to the INTERNET session.

**24 -- PORT FORWARDING RULES**

Remaining number of rules that can be created: 24

			Ports to Open	
<input type="checkbox"/>	Name <input type="text"/>	<< Application Name ▼	TCP <input type="text"/>	Schedule Always ▼
	IP Address <input type="text"/>	<< Computer Name ▼	UDP <input type="text"/>	Inbound Filter Allow All ▼
<input type="checkbox"/>	Name <input type="text"/>	<< Application Name ▼	TCP <input type="text"/>	Schedule Always ▼
	IP Address <input type="text"/>	<< Computer Name ▼	UDP <input type="text"/>	Inbound Filter Allow All ▼

## Application Rules

Some applications require multiple connections, such as Internet gaming, video conferencing, Internet telephony and others. These applications have difficulties working through NAT (Network Address Translation). Application Rules makes some of these applications work with the DIR-862L. If you need to run applications that require multiple connections, specify the port normally associated with an application in the "Trigger Port" field, select the protocol type as TCP or UDP, then enter the firewall (public) ports associated with the trigger port to open them for inbound traffic.

The DIR-862L provides some predefined applications in the table on the bottom of the web page. Select the application you want to use and enable it.

**Name:** Enter a name for the rule. You may select a pre-defined application from the drop-down menu and click <<.

**Trigger:** This is the port used to trigger the application. It can be either a single port or a range of ports.

**Traffic Type:** Select the protocol of the trigger port (TCP, UDP, or Both).

**Firewall:** This is the port number on the Internet side that will be used to access the application. You may define a single port or a range of ports. You can use a comma to add multiple ports or port ranges.

**Traffic Type:** Select the protocol of the firewall port (TCP, UDP, or Both).

**Schedule:** The schedule of time when the Application Rule will be enabled. The schedule may be set to **Always**, which will allow the particular service to always be enabled. You can create your own times in the **Tools > Schedules** section.

**APPLICATION RULES**

The Application Rules option is used to open single or multiple ports in your firewall when the router senses data sent to the Internet on an outgoing "Trigger" port or port range. Special Application rules apply to all computers on your internal network.

24 -- APPLICATION RULES					
Remaining number of rules that can be created: 24					
	Name	Application	Port	Traffic Type	Schedule
<input type="checkbox"/>	<input type="text"/>	<< Application Name ▾	Trigger <input type="text"/>	All ▾	Always ▾
			Firewall <input type="text"/>	All ▾	
<input type="checkbox"/>	<input type="text"/>	<< Application Name ▾	Trigger <input type="text"/>	All ▾	Always ▾
			Firewall <input type="text"/>	All ▾	

## QoS Engine

The QoS Engine option helps improve your network performance by prioritizing applications. By default the QoS Engine settings are disabled and application priority is not classified automatically. The QoS section contains a queuing mechanism, traffic shaping and classification. It supports two kinds of queuing mechanisms. Strict Priority Queue (SPQ) and Weighted Fair Queue (WFQ). SPQ will process traffic based on traffic priority. Queue1 has the highest priority and Queue4 has the lowest priority. WFQ will process traffic based on the queue weight. Users can configure each queue's weight. The sum of all the queue's weight must be 100. When surfing the Internet, the system will do traffic shaping based on the uplink and downlink speed. The classification rules can be used to classify traffic to different queues, then SPQ or WFQ will do QoS based on the queue's priority or weight.

The following parameters will be available for configuration:

**Enable QoS Engine:** This option is disabled by default. Enable this option for better performance and experience with online games and other interactive applications, such as VoIP.

**Automatic Uplink Speed:** The speed at which data can be transferred from the router to your Internet Service Provider (ISP). This is determined by your ISP. ISPs often define speed as a download/upload pair. For example, 1.5Mbps/284Kbps. Check this box to keep your uplink speed optimized. Otherwise, you may set an uplink speed of your own in **Manual Uplink Speed**.

**Checkbox:** Check this to enable an individual rule.

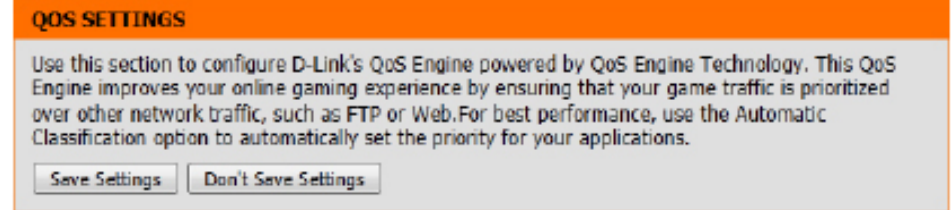
**Name:** Create a name for this rule.

**Priority:** Set the priority of the rule. 1 is the highest.

**Protocol:** Select the protocol the network traffic will be transmitted over.

**IP Range:** Select the IP range for the rule to be applied to. The **Local** range will apply to devices within your network, and the **Remote** range will apply to devices on the Internet.

**Port Range:** Select the ports for this rule to be applied to. Different applications will send traffic over different ports. An online game, email program, and video chat client will all likely use different ports.



## Network Filter

Use MAC (Media Access Control) Filters to allow or deny LAN (Local Area Network) computers by their MAC addresses from accessing the network. You can either manually add a MAC address or select the MAC address from the list of clients that are currently connected to the Broadband Router.

**Configure MAC Filtering:** Select **Turn MAC Filtering Off, Allow MAC addresses listed below**, or **Deny MAC addresses listed below** from the drop-down menu.

**MAC Address:** Enter the MAC address you would like to filter.

To find the MAC address on a computer, please refer to the *Networking Basics* section in this manual.

**DHCP Client:** Select a DHCP client from the drop-down menu and click << to copy that MAC Address.

**24 -- MAC FILTERING RULES**

Configure MAC Filtering below:  
 Turn MAC Filtering ON and ALLOW computers listed to access the network ▼

Remaining number of rules that can be created: **24**

	MAC Address		DHCP Client List	Schedule
<input type="checkbox"/>	<input type="text"/>	<<	Computer Name ▼	Always ▼ <input type="button" value="New Schedule"/>
<input type="checkbox"/>	<input type="text"/>	<<	Computer Name ▼	Always ▼ <input type="button" value="New Schedule"/>
<input type="checkbox"/>	<input type="text"/>	<<	Computer Name ▼	Always ▼ <input type="button" value="New Schedule"/>
<input type="checkbox"/>	<input type="text"/>	<<	Computer Name ▼	Always ▼ <input type="button" value="New Schedule"/>
<input type="checkbox"/>	<input type="text"/>	<<	Computer Name ▼	Always ▼ <input type="button" value="New Schedule"/>
<input type="checkbox"/>	<input type="text"/>	<<	Computer Name ▼	Always ▼ <input type="button" value="New Schedule"/>
<input type="checkbox"/>	<input type="text"/>	<<	Computer Name ▼	Always ▼ <input type="button" value="New Schedule"/>
<input type="checkbox"/>	<input type="text"/>	<<	Computer Name ▼	Always ▼ <input type="button" value="New Schedule"/>
<input type="checkbox"/>	<input type="text"/>	<<	Computer Name ▼	Always ▼ <input type="button" value="New Schedule"/>

# Access Control

The Access Control section allows you to control access in and out of your network. Use this feature as Parental Controls to only grant access to approved sites, limit web access based on time or dates, and/or block access from applications like P2P utilities or games.

**Add Policy:** Click the **Add Policy** button to start the Access Control Wizard.

## Access Control Wizard

Click **Next** to continue with the wizard.



Enter a name for the policy and then click **Next** to continue.

STEP 1: CHOOSE POLICY NAME

Choose a unique name for your policy.

Policy Name :

Select a schedule (e.g. **Always**) from the drop-down menu and then click **Next** to continue.

STEP 2: SELECT SCHEDULE

Choose a schedule to apply to this policy.

Details :

Enter the following information and then click **Next** to continue.

- **Address Type** - Select IP address, MAC address, or Other Machines.
- **IP Address** - Enter the IP address of the computer you want to apply the rule to.
- **Machine Address** - Enter the PC MAC address (i.e. 00:00.00.00.00).

STEP 3: SELECT MACHINE

Select the machine to which this policy applies.

Specify a machine with its IP or MAC address, or select "Other Machines" for machines that do not have a policy.

Address Type :  IP  MAC  Other Machines

IP Address :  <<

Machine Address :  <<

Machine
192.168.0.112

Select the filtering method and then click **Next** to continue.

STEP 4: SELECT FILTERING METHOD

Select the method for filtering.

Method :  Log Web Access Only  Block All Access  Block Some Access

Apply Web Filter :

Apply Advanced Port Filters :

Enter the rule:

**Enable** - Check to enable the rule.

**Name** - Enter a name for your rule.

**Dest IP Start** - Enter the starting IP address.

**Dest IP End** - Enter the ending IP address.

**Protocol** - Select the protocol.

**Dest Port Start** - Enter the starting port number.

**Dest Port End** - Enter the ending port number.

To enable web logging, click **Enable**.

Click **Save** to save the access control rule.

Your newly created policy will now show up under **Policy Table**.

Enable Policy	Machine	Filtering	Logged	Schedule		
<input checked="" type="checkbox"/>	dlink	192.168.0.106	Block Some Access	No	Always	

## Website Filters

Website Filters are used to allow you to set up a list of Web sites that can be viewed by multiple users through the network. To use this feature select to **Allow** or **Deny**, enter the domain or website and click **Save Settings**. You must also select **Apply Web Filter** under the *Access Control* section.

**Add Website** Select either **DENY computers access to ONLY Filtering Rule: these sites** or **ALLOW computers access to ONLY these sites**.

**Website URL/ Domain:** Enter the keywords or URLs that you want to allow or block. Click **Save Settings**.

40 -- WEBSITE FILTERING RULES

Configure Website Filter below:

DENY computers access to ONLY these sites ▼

Clear the list below...

Website URL/Domain	

# Inbound Filters

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

**Name:** Enter a name for the inbound filter rule.

**Action:** Select **Allow** or **Deny**.

**Enable:** Check to enable rule.

**Remote IP Start:** Enter the starting IP address. Enter 0.0.0.0 if you do not want to specify an IP range.

**Remote IP End:** Enter the ending IP address. Enter 255.255.255.255 if you do not want to specify an IP range.

**Add:** Click the **Add** button to apply your settings. You must click **Save Settings** at the top to save the settings.

**Inbound Filter Rules List:** This section will list any rules that are created. You may click the **Edit** icon to change the settings or enable/disable the rule, or click the **Delete** icon to remove the rule.

## INBOUND FILTER

The Inbound Filter option is an advanced method of controlling data received from the Internet. With this feature you can configure inbound data filtering rules that control data based on an IP address range.

Inbound Filters can be used for limiting access to a server on your network to a system or group of systems. Filter rules can be used with Virtual Server, Port Forwarding, or Remote Administration features.



### ADD INBOUND FILTER RULE

Name :

Action :

Remote IP Range	Enable	Remote IP Start	Remote IP End
<input type="text" value="0.0.0.0"/>	<input type="checkbox"/>	<input type="text" value="0.0.0.0"/>	<input type="text" value="255.255.255.255"/>
<input type="text" value="0.0.0.0"/>	<input type="checkbox"/>	<input type="text" value="0.0.0.0"/>	<input type="text" value="255.255.255.255"/>
<input type="text" value="0.0.0.0"/>	<input type="checkbox"/>	<input type="text" value="0.0.0.0"/>	<input type="text" value="255.255.255.255"/>
<input type="text" value="0.0.0.0"/>	<input type="checkbox"/>	<input type="text" value="0.0.0.0"/>	<input type="text" value="255.255.255.255"/>
<input type="text" value="0.0.0.0"/>	<input type="checkbox"/>	<input type="text" value="0.0.0.0"/>	<input type="text" value="255.255.255.255"/>
<input type="text" value="0.0.0.0"/>	<input type="checkbox"/>	<input type="text" value="0.0.0.0"/>	<input type="text" value="255.255.255.255"/>
<input type="text" value="0.0.0.0"/>	<input type="checkbox"/>	<input type="text" value="0.0.0.0"/>	<input type="text" value="255.255.255.255"/>
<input type="text" value="0.0.0.0"/>	<input type="checkbox"/>	<input type="text" value="0.0.0.0"/>	<input type="text" value="255.255.255.255"/>

### INBOUND FILTER RULES LIST

Name	Action	Remote IP Range		
Inbound1	allow	192.168.1.0-192.168.1.254		

# Firewall Settings

A firewall protects your network from the outside world. The DIR-862L offers a firewall type functionality. The SPI feature helps prevent cyber attacks. Sometimes you may want a computer exposed to the outside world for certain types of applications. If you choose to expose a computer, you can enable DMZ. DMZ is short for Demilitarized Zone. This option will expose the chosen computer completely to the outside world.

**Enable SPI:** SPI (Stateful Packet Inspection, also known as dynamic packet filtering) helps to prevent cyber attacks by tracking more states per session. It validates that the traffic passing through the session conforms to the protocol.

**Anti-Spoof Check:** Enable this feature to protect your network from certain kinds of “spoofing” attacks, where the attackers disguise their origin.

**DMZ IP Address:** Specify the IP address of the computer on the LAN that you want to have unrestricted Internet communication. If this computer obtains its IP address automatically using DHCP, be sure to make a static reservation on the **Setup > Network Settings** page so that the IP address of the DMZ machine does not change.

**PPTP:** Allows multiple machines on the LAN to connect to their corporate network using PPTP protocol.

**IPSEC (VPN):** Allows multiple VPN clients to connect to their corporate network using IPsec. Some VPN clients support traversal of IPsec through NAT. This ALG may interfere with the operation of such VPN clients. If you are having trouble connecting with your corporate network, try turning this ALG off. Please check with the system administrator of your corporate network whether your VPN client supports NAT traversal.

**RTSP:** Allows applications that uses Real Time Streaming Protocol to receive streaming media from the Internet. QuickTime and Real Player are some of the common applications using this protocol.

**SIP:** Allows devices and applications using VoIP (Voice over IP) to communicate across NAT. Some VoIP applications and devices have the ability to discover NAT devices and work around them. This ALG may interfere with the operation of such devices. If you are having trouble making VoIP calls, try turning this ALG off.

DIR-862L	SETUP	ADVANCED	TOOLS	STATUS	SUPPORT
VIRTUAL SERVER	<b>FIREWALL SETTINGS</b>				<b>Helpful Hints...</b> Enable the DMZ option only as a last resort. If you are having trouble using an application from a computer behind the router, first try opening ports associated with the application in the <b>Virtual Server</b> or <b>Port Forwarding</b> sections. <a href="#">More...</a>
PORT FORWARDING	The Firewall Settings allows you to set a single computer on your network outside of the router. <input type="button" value="Save Settings"/> <input type="button" value="Don't Save Settings"/>				
APPLICATION RULES	<b>ENABLE SPI</b>				
QOS ENGINE	Enable SPI: <input type="checkbox"/>				
NETWORK FILTER	<b>ANTI-SPOOF CHECKING</b>				
ACCESS CONTROL	Enable anti-spoof checking: <input type="checkbox"/>				
WEBSITE FILTER	<b>DMZ HOST</b>				
INBOUND FILTER	DMZ means "Demilitarized Zone." If an application has trouble working from behind the router, you can expose one computer to the Internet and run the application on that computer. <b>Note:</b> Putting a computer in the DMZ may expose that computer to a variety of security risks. Use of this option is only recommended as a last resort. Enable DMZ: <input type="checkbox"/> DMZ IP Address : 0.0.0.0 << Computer Name >>				
FIREWALL SETTINGS	<b>APPLICATION LEVEL GATEWAY (ALG) CONFIGURATION</b>				
ROUTING	PPTP : <input checked="" type="checkbox"/> L2TP : <input checked="" type="checkbox"/> IPsec (VPN) : <input checked="" type="checkbox"/> RTSP : <input checked="" type="checkbox"/> SIP : <input checked="" type="checkbox"/>				
ADVANCED WIRELESS					
WI-FI PROTECTED SETUP					
ADVANCED NETWORK					
GUEST ZONE					
IPv6 FIREWALL					
IPv6 ROUTING					

# Routing

The Routing option is an advanced method of customizing specific routes of data through your network.

**Name:** Enter a name for your route.

**Destination IP:** Enter the IP address of packets that will take this route.

**Netmask:** Enter the netmask of the route, please note that the octets must match your destination IP address.

**Gateway:** Enter your next hop gateway to be taken if this route is used.

**Metric:** The route metric is a value from 1 to 16 that indicates the cost of using this route. A value 1 is the lowest cost and 15 is the highest cost.

**Interface:** Select the interface that the IP packet must use to transit out of the router when this route is used.

The screenshot shows the D-Link DIR-862L web interface. The top navigation bar includes 'SETUP', 'ADVANCED', 'TOOLS', 'STATUS', and 'SUPPORT'. The 'ADVANCED' tab is selected, and the 'ROUTING' sub-tab is active. The main content area displays the 'ROUTING' configuration page, which includes a 'Save Settings' and 'Don't Save Settings' button. Below this is the 'ROUTE LIST' section, which shows a table of routes. The table has columns for 'Name', 'Destination IP', 'Metric', and 'Interface'. The 'Interface' column is set to 'WAN 0'. The 'Metric' column is set to '1'. The 'Destination IP' and 'Netmask' fields are empty. The 'Name' field is also empty. The 'Remaining number of rules that can be created: 32' is displayed above the table. The sidebar on the right contains 'Helpful Hints...' with the following information:

- Enable:** Specifies whether the entry will be enabled or disabled.
- Interface:** Specifies the interface -- WAN -- that the IP packet must use to transit out of the router, when this route is used.
- Destination IP:** The IP address of packets that will take this route.
- Netmask:** One bit in the mask specifies which bits of the IP address must match.
- Gateway:** The gateway IP address is the IP address of the router, if any, used to reach the specified destination.
- More...**

# Advanced Wireless

**Transmit Power:** Set the transmit power of the antennas.

**WLAN Partition:** This enables 802.11d operation. 802.11d is a wireless specification developed to allow implementation of wireless networks in countries that cannot use the 802.11 standard. This feature should only be enabled if you are in a country that requires it.

**WMM Enable:** WMM is QoS for your wireless network. This will improve the quality of video and voice applications for your wireless clients.

**HT20/40 Coexistence:** Enable this option to reduce interference from other wireless networks in your area. If the channel width is operating at 40MHz and there is another wireless network's channel over-lapping and causing interference, the router will automatically change to 20MHz.

**D-Link**

DIR-862L //

SETUP ADVANCED TOOLS STATUS SUPPORT

**ADVANCED WIRELESS**

If you are not familiar with these Advanced Wireless settings, please read the help section before attempting to modify these settings.

Save Settings Don't Save Settings

**ADVANCED WIRELESS SETTINGS**

Wireless Band : 2.4GHz  
 Transmit Power : High  
 WLAN Partition :   
 WMM Enable :   
 HT 20/40 MHz Coexistence :  Enable  Disable

**ADVANCED WIRELESS SETTINGS**

Wireless Band : 5GHz  
 Transmit Power : High  
 WLAN Partition :   
 WMM Enable :

**Helpful Hints ...**

It is recommended that you leave these parameters at their default values. Adjusting them could limit the performance of your wireless network.

Enabling WMM can help control latency and jitter when transmitting multimedia content over a wireless connection.

[More...](#)

## Wi-Fi Protected Setup (WPS)

Wi-Fi Protected Setup (WPS) System is a simplified method for securing your wireless network during the “Initial setup” as well as the “Add New Device” processes. The Wi-Fi Alliance (WFA) has certified it across different products as well as manufactures. The process is just as easy as pressing a button for the Push-Button Method or correctly entering an 8-digit code.

**Enable:** Enable/disable the Wi-Fi Protected Setup feature.

**Lock WPS-PIN Setup:** Tick this option to lock the configured PIN.

**PIN Settings:** A PIN is a unique number that can be used to add the router to an existing network or to create a new network. Only the Administrator (“admin” account) can change or reset the PIN.

**Current PIN:** Shows the current PIN.

**Reset PIN to Default:** Restore the default PIN of the router.

**Generate New PIN:** Create a random number that is a valid PIN. This becomes the router’s PIN. You can then copy this PIN to the user interface of the wireless client. This Wizard helps you add wireless devices to the wireless network.

**Add Wireless Station:** Starts a wizard which will display the wireless network settings to guide you through manual configuration, prompt you to enter the PIN for the device, or ask you to press the configuration button on the device. If the device supports Wi-Fi Protected Setup and has a configuration button, you can add it to the network by pressing the configuration button on the device and then the on the router within 120 seconds. The status LED on the router will flash three times if the device has been successfully added to the network.

There are several ways to add a wireless device to your network. A “registrar” controls access to the wireless network. A registrar only allows devices onto the wireless network if you have entered the PIN, or pressed a special Wi-Fi Protected Setup button on the device. The router acts as a registrar for the network, although other devices may act as a registrar as well.

**Note:** You may also press the physical WPS button on the device.

The screenshot shows the D-Link DIR-862L Advanced Wireless Setup page. The left sidebar contains a navigation menu with the following items: VIRTUAL SERVER, PORT FORWARDING, APPLICATION RULES, QOS ENGINE, NETWORK FILTER, ACCESS CONTROL, WEBSITE FILTER, INBOUND FILTER, FIREWALL SETTINGS, ROUTING, ADVANCED WIRELESS, WI-FI PROTECTED SETUP (highlighted), ADVANCED NETWORK, GUEST ZONE, IPV6 FIREWALL, and IPV6 ROUTING. The main content area is titled "WI-FI PROTECTED SETUP" and includes the following sections:

- WI-FI PROTECTED SETUP:** A description stating that WPS is used to easily add devices to a network using a PIN or button press. It includes "Save Settings" and "Don't Save Settings" buttons.
- WI-FI PROTECTED SETUP:** Configuration options for "Enable" (checked) and "Lock WPS-PIN Setup" (unchecked).
- PIN SETTINGS:** Shows the "Current PIN" as 59842750, with "Generate New PIN" and "Reset PIN to Default" buttons.
- ADD WIRELESS STATION:** Includes an "Add Wireless Device With WPS" button.

On the right side, there is a "Support" section with "Helpful Hints..." and "More..." links. The hints include: "Enable if other wireless devices you wish to include in the local network support Wi-Fi Protected Setup." and "Only 'Admin' account can change security settings." The "More..." link is also present.



# Advanced Network Settings

**Enable UPnP:** To use the Universal Plug and Play (UPnP™) feature click on **Enabled**. UPnP provides compatibility with networking equipment, software and peripherals.

**WAN Ping:** Checking the box will allow the DIR-862L to respond to pings. Unchecking the box may provide some extra security from hackers.

**WAN Port Speed:** You may set the port speed of the Internet port to 10 Mbps, 100 Mbps, or Auto (recommended).

**Enable Multicast Streams:** Check the box to allow multicast traffic to pass through the router from the Internet (IPv4).

**Enable IPV6 Multicast Streams:** Check the box to allow multicast traffic to pass through the router from the Internet (IPv6).

**D-Link**

DIR-862L //

SETUP   ADVANCED   TOOLS   STATUS   SUPPORT

**ADVANCED NETWORK**

If you are not familiar with these Advanced Network settings, please read the help section before attempting to modify these settings.

Save Settings   Don't Save Settings

**UPnP**

Universal Plug and Play (UPnP) supports peer-to-peer Plug and Play functionality for network devices.

Enable UPnP :

**WAN PING**

If you enable this feature, the WAN port of your router will respond to ping requests from the Internet that are sent to the WAN IP Address.

Enable WAN Ping Respond :

WAN Ping Inbound Filter :

Details :

**WAN PORT SPEED**

WAN Port Speed :

**MULTICAST STREAMS**

Enable Multicast Streams :

**IPv6 MULTICAST STREAMS**

Enable IPv6 Multicast Streams :

**Helpful Hints ...**

UPnP helps other UPnP LAN hosts interoperate with the router. Leave the UPnP option enabled as long as the LAN has other UPnP applications.

For added security, it is recommended that you disable the WAN Ping Respond option. Ping is often used by malicious Internet users to locate active networks or PCs.

The WAN speed is usually detected automatically. If you are having problems connecting to the WAN, try selecting the speed manually.

If you are having trouble receiving multicast streams from the Internet, make sure the Multicast Streams option is enabled.

[More...](#)

# Guest Zone

The Guest Zone feature will allow you to create temporary zones that can be used by guests to access the Internet. These zones will be separate from your main wireless network. You may configure different zones for the 2.4 GHz and 5 GHz wireless bands.

**Enable Guest Zone:** Check to enable the Guest Zone feature.

**Schedule:** The schedule of time when the Guest Zone will be active. The schedule may be set to **Always**, which will allow the particular service to always be enabled. You can create your own times in the **Tools > Schedules** section or click **Add New**.

**Wireless Network Name:** Enter a wireless network name (SSID) that is different from your main wireless network.

**Enable Routing Between Zones:** Check to allow network connectivity between the different zones created.

**Security Mode:** Select the type of security or encryption you would like to enable for the guest zone.

The screenshot displays the D-Link web interface for the DIR-862L router. The main navigation menu on the left includes: VIRTUAL SERVER, PORT FORWARDING, APPLICATION RULES, QOS ENGINE, NETWORK FILTER, ACCESS CONTROL, WEBSITE FILTER, INBOUND FILTER, FIREWALL SETTINGS, ROUTING, ADVANCED WIRELESS, WI-FI PROTECTED SETUP, ADVANCED NETWORK, GUEST ZONE (highlighted), IPV6 FIREWALL, and IPV6 ROUTING. The top navigation bar shows: SETUP, ADVANCED, TOOLS, STATUS, and SUPPORT. The 'GUEST ZONE' section is active, with a sub-header 'GUEST ZONE SELECTION'. It contains two configuration panels:

- 2.4GHz Band:**
  - Enable Guest Zone:
  - Schedule:  Always  Add New
  - Wireless Band: 2.4GHz Band
  - Wireless Network Name: dlink\_guest (Also called the SSID)
  - Enable Routing Between Zones:
- 5GHz Band:**
  - Enable Guest Zone:
  - Schedule:  Always  Add New
  - Wireless Band: 5GHz Band
  - Wireless Network Name: dlink\_media\_guest (Also called the SSID)
  - Enable Routing Between Zones:

On the right side, there is a 'Helpful Hints...' section with instructions on configuring guest zone settings and a 'More...' link.

# IPv6 Firewall

The DIR-862L's IPv6 Firewall feature allows you to configure which kind of IPv6 traffic is allowed to pass through the device. The DIR-862L's IPv6 Firewall functions in a similar way to the IP Filters feature.

**Enable Checkbox:** Check the box to enable the IPv6 firewall simple security.

**Configure IPv6 Firewall:** Select an action from the drop-down menu.

**Name:** Enter a name to identify the IPv6 firewall rule.

**Schedule:** Use the drop-down menu to select the time schedule that the IPv6 Firewall Rule will be enabled on. The schedule may be set to **Always**, which will allow the particular service to always be enabled. You can create your own times in the **Tools > Schedules** section.

**Source:** Use the **Source** drop-down menu to specify the interface that connects to the source IPv6 addresses of the firewall rule.

**IP Address Range:** Enter the source IPv6 address range in the adjacent **IP Address Range** field.

**Interface:** Use the **Interface** drop-down menu to specify the interface that connects to the destination IP addresses of the firewall rule.

**Protocol:** Select the protocol of the firewall port (**All**, **TCP**, **UDP**, or **ICMP**).

**Port Range:** Enter the first port of the range that will be used for the firewall rule in the first box and enter the last port in the field in the second box.

**D-Link**

DIR-862L // SETUP ADVANCED TOOLS STATUS SUPPORT

**IPv6 FIREWALL**

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

Save Settings Don't Save Settings

**IPv6 SIMPLE SECURITY**

Enable IPv6 Ingress Filtering:

Enable IPv6 Simple Security:

**IPv6 FIREWALL**

Configure IPv6 Firewall below:  
Turn IPv6 Firewall OFF

Remaining number of firewall rules that can be configured:

Name	Schedule	Source	Interface	IP Address Range	Protocol	Port Range
	Always				TCP	1 ~ 65535
	Always				TCP	1 ~ 65535

**Helpful Hints ...**

Check the **Application Name** drop down menu for a list of predefined server types. If you select one of the predefined server types, click the arrow button next to the drop down menu to fill out the corresponding field.

You can select a computer from the list of DHCP clients in the **Computer Name** drop down menu, or you can manually enter the IP address of the computer at which you would like to open the specified port.

Select a schedule for when the virtual server will be enabled. If you do not see the schedule you need in the list of schedules, go to the **Tools → Schedules** screen and create a new schedule.

Select a filter that restricts the Internet hosts that can access this virtual server to hosts that you trust. If you do not see the filter you need in the list of filters, go to the **Advanced → Inbound Filter** screen and create a new filter.

More...

# IPv6 Routing

This page allows you to specify custom routes that determine how data is moved around your network.

**Route List:** Check the box next to the route you wish to enable.

**Name:** Enter a specific name to identify this route.

**Destination IP/Prefix Length:** This is the IP address of the router used to reach the specified destination or enter the IPv6 address prefix length of the packets that will take this route.

**Metric:** Enter the metric value for this rule here.

**Interface:** Use the drop-down menu to specify if the IP packet must use the WAN or LAN interface to transit out of the Router.

**Gateway:** Enter the next hop that will be taken if this route is used.

**D-Link**

DIR-862L // SETUP ADVANCED TOOLS STATUS SUPPORT

**ROUTING**

This Routing page allows you to specify custom routes that determine how data is moved around your network.

Save Settings Don't Save Settings

**10 -- ROUTE LIST**

Name	Destination IPv6 / Prefix Length	Metric	Interface	Gateway
<input type="checkbox"/>	/	64	NULL	
<input type="checkbox"/>	/	64	NULL	
<input type="checkbox"/>	/		NULL	

**Helpful Hints...**

- Each route has a check box next to it, check this box if you want the route to be enabled.
- The name field allows you to specify a name for identification of this route, e.g. 'Network 2'
- The destination IPv6 address is the address of the host or network you wish to reach.
- The prefix length field identifies the portion of the destination IP in use.
- The gateway IP address is the IP address of the router, if any, used to reach the specified destination.
- [More...](#)

# Tools

## Admin

This page will allow you to change the Administrator and User passwords. You can also enable Remote Management. There are two accounts that can access the management interface through the web browser. The accounts are admin and user. Admin has read/write access while user has read-only access. User can only view the settings but cannot make any changes. Only the admin account has the ability to change both admin and user account passwords.

**Admin Password:** Enter a new password for the Administrator Login Name. The administrator can make changes to the settings.

**User Password:** Enter the new password for the User login. If you login as the User, you cannot change the settings (you can only view them).

**Gateway name:** Enter a name for your router.

**Enable Graphical Authentication:** Enables a challenge-response test to require users to type letters or numbers from a distorted image displayed on the screen to prevent online hackers and unauthorized users from gaining access to your router's network settings.

**Enable HTTPS Server:** Check to enable HTTPS to connect to the router securely. This means to connect to the router, you must enter **https://192.168.0.1** (for example) instead of **http://192.168.0.1**.

**Enable Remote Management:** Remote management allows the DIR-862L to be configured from the Internet by a web browser. A username/password is still required to access the Web Management interface.

**Remote Admin Port:** The port number used to access the DIR-862L is used in the URL. Example: **http://x.x.x.x:8080** whereas x.x.x.x is the Internet IP address of the DIR-862L and 8080 is the port used for the Web Management interface.

If you have enabled **HTTPS Server**, you must enter **https://** as part of the URL to access the router remotely.

**Remote Admin Inbound Filter:** This section will list any rules that are created. You may click the **Edit** icon to change the settings or enable/disable the rule, or click the **Delete** icon to remove the rule. **Details** will display the current status.

The screenshot shows the D-Link DIR-862L web management interface. The top navigation bar includes tabs for SETUP, ADVANCED, TOOLS, STATUS, and SUPPORT. The left sidebar lists various configuration sections: ADMIN, TIME, SYSLOG, EMAIL SETTINGS, SYSTEM, FIRMWARE, DYNAMIC DNS, SYSTEM CHECK, and SCHEDULES. The main content area is titled 'ADMINISTRATOR SETTINGS' and contains the following sections:

- ADMINISTRATOR SETTINGS:** A text box explaining that the 'admin' account can access the management interface and change passwords. Below this is a note stating that by default there is no password configured and it is recommended to create one. There are 'Save Settings' and 'Don't Save Settings' buttons.
- ADMIN PASSWORD:** A section with the instruction 'Please enter the same password into both boxes, for confirmation.' It contains two password input fields labeled 'Password' and 'Verify Password'.
- SYSTEM NAME:** A section with a 'Gateway Name' input field containing the text 'DIR-820L'.
- ADMINISTRATION:** A section with several checkboxes and input fields:
  - Enable Graphical Authentication:**
  - Enable HTTPS Server:**
  - Enable Remote Management:**
  - Remote Admin Port:** Input field with '8080' and a 'Use HTTPS' checkbox.
  - Remote Admin Inbound Filter:** A dropdown menu set to 'Allow All'.
  - Details:** Input field with 'Allow All'.

On the right side of the interface, there is a 'Helpful Hints ...' section with text about security recommendations for changing passwords and enabling remote management. A 'More...' link is also present.

# 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 Time Server. Daylight Saving can also be configured to automatically adjust the time when needed.

**Time:** Displays the current date and time of the router.

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

**Enable 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 Server:** NTP is short for Network Time Protocol. A NTP server will sync the time and date with your router. This will only connect to a server on the Internet, not a local server. Check the box to enable this feature.

**NTP Server Used:** Enter the IP address of a 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** to synch the date and time with the computer you are currently on.

The screenshot shows the D-Link web interface for the DIR-862L router. The main navigation bar includes ADMIN, TIME, SYSLOG, EMAIL SETTINGS, SYSTEM, FIRMWARE, DYNAMIC DNS, SYSTEM CHECK, and SCHEDULES. The current page is the TIME configuration page, which is divided into several sections:

- TIME:** A header section with a description: "The Time Configuration option allows you to configure, update, and maintain the correct time on the internal system clock. From this section you can set the time zone that you are in and set the NTP (Network Time Protocol) Server. Daylight Saving can also be configured to automatically adjust the time when needed." Below this are "Save Settings" and "Don't Save Settings" buttons.
- TIME CONFIGURATION:** This section displays the "Current Router Time" as "Fri Jan, 2, 1970 22:20:39". It includes a "Time Zone" dropdown menu set to "(GMT-08:00) Pacific Time (US/Canada), Tijuana". There is an "Enable Daylight Saving" checkbox which is currently unchecked. Below this are "Daylight Saving Dates" fields for "DST Start" and "DST End", each with dropdowns for Month, Week, Day of Week, and TIME.
- AUTOMATIC TIME CONFIGURATION:** This section contains an "Enable NTP Server" checkbox (unchecked) and an "NTP Server Used" field with a dropdown menu for selecting a server.
- SET THE DATE AND TIME MANUALLY:** This section provides fields for manually setting the date and time. The "Date And Time" field shows "Year: 2013", "Month: Feb", "Day: 6", "Hour: 02", "Minute: 19", "Second: 51", and "PM". A "Copy Your Computer's Time Settings" button is located below these fields.

On the right side of the interface, there is a "Support" section with "Helpful Hints..." and "More..." links.

# 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 web interface for the DIR-862L router. The top navigation bar includes 'DIR-862L', 'SETUP', 'ADVANCED', 'TOOLS', 'STATUS', and 'SUPPORT'. The left sidebar lists menu items: ADMIN, TIME, SYSLOG (selected), EMAIL SETTINGS, SYSTEM, FIRMWARE, DYNAMIC DNS, SYSTEM CHECK, and SCHEDULES. 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 'Save Settings' and 'Don't Save Settings' buttons. The 'SYSLOG SETTINGS' section is highlighted and contains the text 'Enable Logging To SysLog Server' with an unchecked checkbox, followed by 'Save Settings' and 'Don't Save Settings' buttons. On the right side, there is a 'Helpful Hints...' section with a bullet point: 'A System Logger (syslog) is a server that collects in one place the logs from different sources. If the LAN includes a syslog server, you can use this option to send the router's logs to that server.' and a 'More...' link.

# Email Settings

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

**Enable Email Notification:** When this option is enabled, router activity logs are emailed 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.

**SMTP Server Port:** Enter the SMTP port used on the server.

**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 to your account 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-862L web interface. The top navigation bar includes 'D-Link', 'DIR-862L', and tabs for 'SETUP', 'ADVANCED', 'TOOLS', 'STATUS', and 'SUPPORT'. The 'EMAIL SETTINGS' page is displayed, featuring a sidebar with menu items: ADMIN, TIME, SYSLOG, EMAIL SETTINGS (selected), SYSTEM, FIRMWARE, DYNAMIC DNS, SYSTEM CHECK, and SCHEDULES. The main content area is divided into four sections:

- EMAIL SETTINGS:** Contains a descriptive paragraph and two buttons: 'Save Settings' and 'Don't Save Settings'.
- EMAIL NOTIFICATION:** Includes a checkbox for 'Enable Email Notification'.
- EMAIL SETTINGS (Form):** Contains input fields for 'From Email Address', 'To Email Address', 'Email Subject', 'SMTP Server Address', 'SMTP Server Port' (with a value of 25), 'Enable Authentication' (checkbox), 'Account Name', 'Password', and 'Verify Password'. A 'Send Mail Now' button is located at the bottom right of this section.
- EMAIL LOG WHEN FULL OR ON SCHEDULE:** Includes checkboxes for 'On Log Full' and 'On Schedule', a 'Schedule' dropdown menu (set to 'Never'), and a 'Detail' input field. 'Save Settings' and 'Don't Save Settings' buttons are at the bottom.

A 'Helpful Hints...' sidebar on the right contains a bullet point: 'You may want to make the email settings similar to those of your email client program.' and a 'More...' link.



# System

This section allows you to manage the router's configuration settings, reboot the router, and 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've created.

**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. A file dialog will appear, allowing you to 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 **Choose File** option to find a previously saved file of configuration settings. Then, click the **Restore Configuration From File** 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.

The screenshot shows the D-Link web interface for the DIR-862L router. The top navigation bar includes tabs for SETUP, ADVANCED, TOOLS, STATUS, and SUPPORT. The left sidebar lists various configuration sections: ADMIN, TIME, SYSLOG, EMAIL SETTINGS, SYSTEM (highlighted), FIRMWARE, DYNAMIC DNS, SYSTEM CHECK, and SCHEDULES. The main content area is titled 'SYSTEM SETTINGS' and contains the following text and buttons:

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.

**Save Settings To Local Hard Drive:**

**Load Settings From Local Hard Drive:**  No file chosen

**Restore To Factory Default Settings:**   
Restore all Settings to the Factory Defaults

**Reboot The Device:**

The right sidebar, titled 'Helpful Hints ...', provides additional information: '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...'

# Firmware

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

**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.

**Upload:** Once you have a firmware update on your computer, use this option to browse for the file and then upload the information into the access point.

## Language Pack

You can change the language of the web UI by uploading available language packs.

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

The screenshot shows the D-Link DIR-862L web interface. The top navigation bar includes the D-Link logo and tabs for SETUP, ADVANCED, TOOLS, STATUS, and SUPPORT. The left sidebar lists various configuration options, with FIRMWARE highlighted. The main content area is titled 'FIRMWARE UPDATE' and contains the following information:

- FIRMWARE AND LANGUAGE PACK INFORMATION:**
  - Current Firmware Version: 1.00
  - Date: 2013/01/28
  - Current Language Pack Version: There is no language pack.
  - Check Online Now for Latest Firmware and Language pack 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.
  - 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:  No file chosen
  -
- LANGUAGE PACK UPGRADE:**
  - Upload:  No file chosen
  -

On the right side, there is a 'Helpful Hints' section with text about firmware updates and a 'More...' link.

# Dynamic DNS

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

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

**Server Address:** Select your DDNS provider from the drop-down menu or enter the DDNS server address.

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

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

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

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

**Status:** Displays the current connection status.

**IPv6:** You can also enable DDNS for usage over IPv6 in the same manner as above for IPv4.

**D-Link**

DIR-862L //

SETUP    ADVANCED    TOOLS    STATUS    SUPPORT

**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](http://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)

Save Settings    Don't Save Settings

**DYNAMIC DNS**

Enable Dynamic DNS :

Server Address :  <<

Select Dynamic DNS Server

Host Name :  (e.g. myhost.mydomain.net)

Username or Key :

Password or Key :

Verify Password or Key :

Timeout :  (hours)

Status : Disconnect

**DYNAMIC DNS FOR IPV6 HOSTS**

Enable :

IPv6 Address :  <<< Computer Name

Host Name :  (e.g. myhost.mydomain.net)

Save    Clear

**IPV6 DYNAMIC DNS LIST**

Enable	Host Name	IPv6 Address

**Helpful Hints ...**

To use this feature, you must first have a Dynamic DNS account from one of the providers in the drop down menu.

[More...](#)

# 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**.

**IPv6 Ping Test:** Enter the IPv6 address that you wish to Ping and click **Ping**.

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

The screenshot shows the D-Link DIR-862L web interface. The top navigation bar includes the D-Link logo and tabs for SETUP, ADVANCED, TOOLS, STATUS, and SUPPORT. The left sidebar lists various configuration options, with SYSTEM CHECK highlighted. The main content area is divided into three sections: PING TEST, IPV6 PING TEST, and PING RESULT. The PING TEST section contains a text box for 'Host Name or IP Address' and 'Ping' and 'Stop' buttons. The IPV6 PING TEST section contains a text box for 'Host Name or IPv6 Address' and 'Ping' and 'Stop' buttons. The PING RESULT section contains a text box with the instruction 'Enter a host name or IP address above and click 'Ping''. A 'Helpful Hints ...' section on the right provides additional information about the ping test.

**D-Link**

DIR-862L //

SETUP    ADVANCED    TOOLS    STATUS    SUPPORT

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

**PING TEST**

Ping Test sends "ping" packets to test a computer on the Internet.

**PING TEST**

Host Name or IP Address :  Ping Stop

**IPV6 PING TEST**

Host Name or IPv6 Address :  Ping Stop

**PING RESULT**

Enter a host name or IP address above and click 'Ping'

Helpful Hints ...

"Ping" checks whether a computer on the Internet is running and responding. Enter either the IP address of the target computer or enter its fully qualified domain name.

More...

WIRELESS

# Schedules

Schedules can be created for use with enforcing rules. For example, if you want to restrict web access to Mon-Fri from 3pm to 8pm, you could create a schedule selecting Mon, Tue, Wed, Thu, and Fri and enter a Start Time of 3pm and End Time of 8pm.

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

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

The screenshot shows the D-Link DIR-862L web interface. The top navigation bar includes 'SETUP', 'ADVANCED', 'TOOLS', 'STATUS', and 'SUPPORT'. The left sidebar lists various configuration categories: ADMIN, TIME, SYSLOG, EMAIL SETTINGS, SYSTEM, FIRMWARE, DYNAMIC DNS, SYSTEM CHECK, and SCHEDULES. The main content area is titled 'SCHEDULES' and contains the following text: 'The Schedule configuration option is used to manage schedule rules for various firewall and parental control features.' Below this text are two buttons: 'Save Settings' and 'Don't Save Settings'. The '10 - ADD SCHEDULE RULE' section includes a 'Name:' input field, a 'Day(s):' section with radio buttons for 'All Week' (selected) and 'Select Day(s)', and checkboxes for 'Sun', 'Mon', 'Tue', 'Wed', 'Thu', 'Fri', and 'Sat'. There is also an 'All Day - 24 hrs:' checkbox. The 'Time format:' is set to '12-hour'. The 'Start Time:' is '12:00 PM' and the 'End Time:' is '12:00 PM'. Below this is a 'SCHEDULE RULES LIST' table with columns for 'Name', 'Day(s)', and 'Time Frame'. The right sidebar contains 'Helpful Hints...' text explaining that schedules are used with other features and provides instructions on naming, saving, editing, and deleting schedules.

# Status

## Device Info

This page displays the current information for the DIR-862L. 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

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

**Wireless LAN1:** Displays the 2.4 GHz wireless MAC address and your wireless settings such as SSID and Channel.

**Wireless LAN2:** Displays the 5 GHz 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).

The screenshot shows the D-Link DIR-862L web interface. The main content area is titled "DEVICE INFORMATION" and contains the following sections:

- GENERAL:** Time: Sunday, January 02, 2011 12:45:08 AM; Firmware Version: 1.00, Tue, 16, Mar, 2010.
- WAN:** Connection Type: Dynamic IP (DHCP); Cable Status: Disconnected; Network Status: Disconnected (with Release and Renew buttons); Connection Up Time: N/A; MAC Address: 00:18:E7:95:70:A1; IP Address: 0.0.0.0; Subnet Mask: 0.0.0.0; Default Gateway: 0.0.0.0; Primary DNS Server: 0.0.0.0; Secondary DNS Server: 0.0.0.0; Advanced DNS: Disabled.
- LAN:** MAC Address: 00:18:E7:95:70:A0; IP Address: 192.168.0.1; Subnet Mask: 255.255.255.0; DHCP Server: Enabled.
- WIRELESS LAN1:** Wireless Band: 2.4GHz; Wireless Radio: Enable; 802.11 Mode: 802.11bgn; Channel Width: 20/40MHz; Channel: 2; Wi-Fi Protected Setup: Enabled/Not Configured. SSID List table:
 

Network Name (SSID)	Guest	MAC Address	Security Mode
dirk	No	00:18:E7:95:70:A0	Off
- WIRELESS LAN2:** Wireless Band: 5GHz Band; Wireless Radio: Enable; 802.11 Mode: 802.11n; Channel Width: 20/40MHz; Channel: 36; Wi-Fi Protected Setup: Enabled/Not Configured. SSID List table:
 

Network Name (SSID)	Guest	MAC Address	Security Mode
dirk_media	No	00:18:E7:95:70:A2	Off
- LAN COMPUTERS:** Table showing connected devices:
 

IP Address	Name (if any)	MAC
192.168.0.100	PM_test01	00:04:23:2C:51:A3
- IGMP MULTICAST MEMBERSHIPS:** Table with header: Multicast Group Address.

# Logs

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.

**Log Options:** You can select the types of messages that you want to display from the log. System Activity, Debug Information, Attacks, Dropped Packets, and Notice messages can be selected. Click **Apply Log Settings Now** to activate your settings.

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

**First Page:** Click to go to the first page.

**Last Page:** Click to go to the last page.

**Previous:** Click to go back one page.

**Next:** Click to go to the next page.

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

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

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

**D-Link**

DIR-862L

SETUP ADVANCED TOOLS STATUS SUPPORT

DEVICE INFO

LOGS

STATISTICS

INTERNET SESSIONS

ROUTING

WIRELESS

IPv6

IPv6 ROUTING

**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 internal syslog server support so you can send the log files to a computer on your network that is running a syslog utility.

**LOG OPTIONS**

**Log Options :**  System Activity  
 Debug Information  
 Attacks  
 Dropped Packets  
 Notice

Apply Log Settings Now

**LOG DETAILS**

First Page Last Page Previous Next

Refresh Clear Email Now Save Log

1/9

Time	Message
Jan 1 00:19:32	cron.err: crond[11725]: crond (busybox 1.12.1) started, log level 8
Jan 1 00:19:31	cron.err: crond[11673]: crond (busybox 1.12.1) started, log level 8
Jan 1 00:19:30	cron.err: crond[11557]: crond (busybox 1.12.1) started, log level 8
Jan 1 00:19:30	cron.err: crond[11349]: crond (busybox 1.12.1) started, log level 8
Jan 1 00:19:30	user.crit: kernel: Argh. No free space left for GC. nr_erasing_blocks is 0. nr_free_blocks is 0. (erasableempty: yes, erasingempty: yes, erasependingempty: yes)
Jan 1 00:00:24	user.info: kernel: br0: port 2(rA00_0) entering forwarding state
Jan 1 00:00:13	user.info: kernel: br0: port 2(rA00_0) entering learning state
Jan 1 00:00:13	user.info: kernel: br0: port 2(rA00_0) entering learning state
Jan 1 00:00:13	user.info: kernel: device rA00_0 entered promiscuous mode
Jan 1 00:00:13	user.warn: kernel: 0x1300 = 00064380

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...

WIRELESS

# Statistics

The screen below displays the **Traffic Statistics**. Here you can view the amount of packets that pass through the DIR-862L on both the WAN, LAN ports and the wireless segments. The traffic counter will reset if the device is rebooted.

The screenshot shows the D-Link DIR-862L web interface. The top navigation bar includes 'DIR-862L', 'SETUP', 'ADVANCED', 'TOOLS', 'STATUS', and 'SUPPORT'. The left sidebar lists various configuration options, with 'STATISTICS' selected. The main content area is titled 'TRAFFIC STATISTICS' and contains the following data:

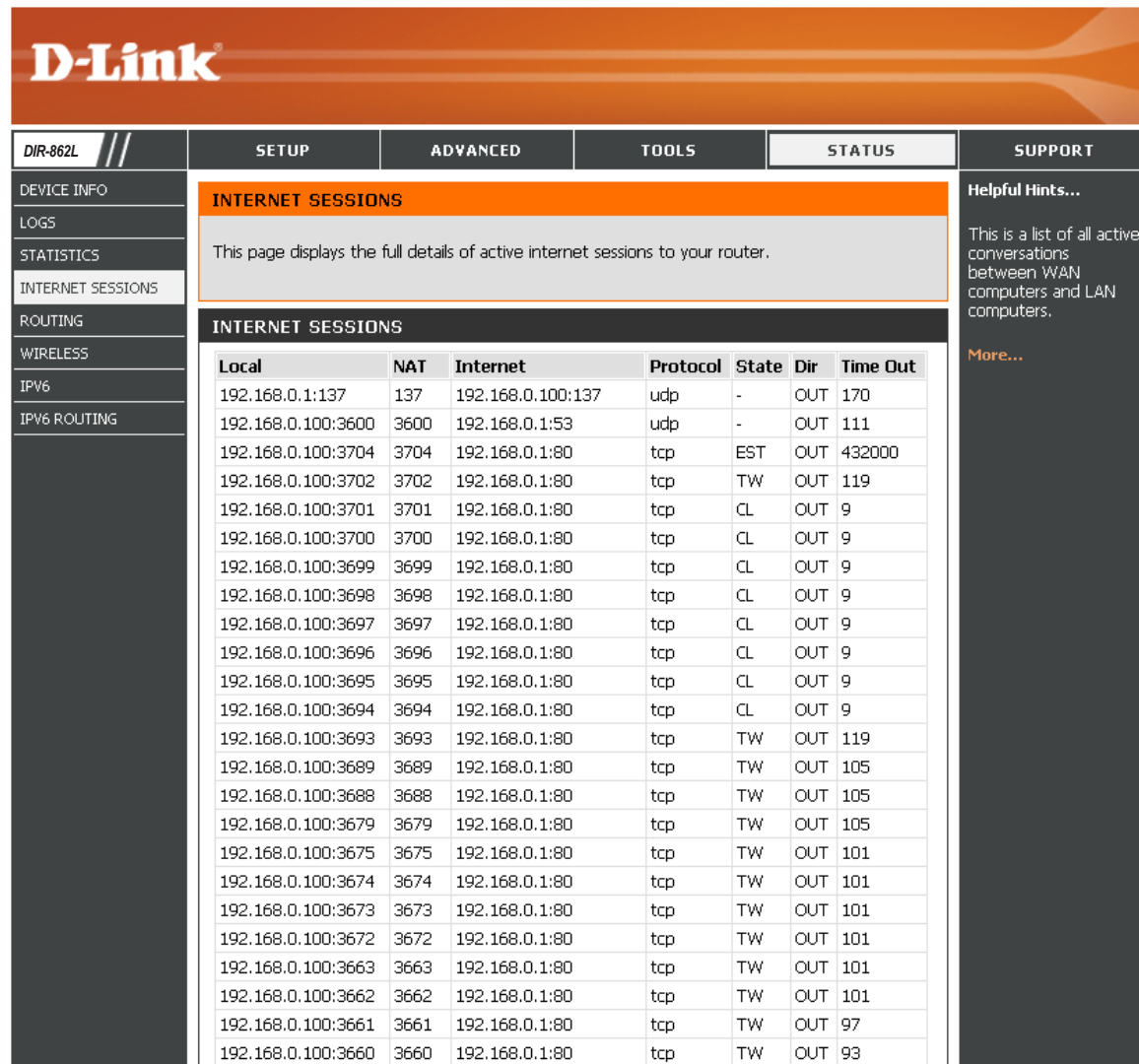
TRAFFIC STATISTICS	
Traffic Statistics display Receive and Transmit packets passing through your router.	
<input type="button" value="Refresh Statistics"/> <input type="button" value="Clear Statistics"/>	
LAN STATISTICS	
Sent : 133656	Received : 28232
TX Packets	RX Packets
Dropped : 0	Dropped : 0
Collisions : 0	Errors : 0
WAN STATISTICS	
Sent : 66	Received : 0
TX Packets	RX Packets
Dropped : 0	Dropped : 0
Collisions : 0	Errors : 0
WIRELESS STATISTICS	
Sent : 17694	Received : 484764
TX Packets	RX Packets
Dropped : 0	Dropped : 0
	Errors : 0
WIRELESS STATISTICS2	
Sent : 11865	Received : 7405
TX Packets	RX Packets
Dropped : 0	Dropped : 0
	Errors : 0

The right sidebar contains 'Helpful Hints...' and a 'More...' link. The bottom left corner of the interface displays 'WIRELESS'.



# 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.



**D-Link**

DIR-862L // SETUP ADVANCED TOOLS STATUS SUPPORT

DEVICE INFO  
LOGS  
STATISTICS  
INTERNET SESSIONS  
ROUTING  
WIRELESS  
IPV6  
IPV6 ROUTING

**INTERNET SESSIONS**

This page displays the full details of active internet sessions to your router.

**INTERNET SESSIONS**

Local	NAT	Internet	Protocol	State	Dir	Time Out
192.168.0.1:137	137	192.168.0.100:137	udp	-	OUT	170
192.168.0.100:3600	3600	192.168.0.1:53	udp	-	OUT	111
192.168.0.100:3704	3704	192.168.0.1:80	tcp	EST	OUT	432000
192.168.0.100:3702	3702	192.168.0.1:80	tcp	TW	OUT	119
192.168.0.100:3701	3701	192.168.0.1:80	tcp	CL	OUT	9
192.168.0.100:3700	3700	192.168.0.1:80	tcp	CL	OUT	9
192.168.0.100:3699	3699	192.168.0.1:80	tcp	CL	OUT	9
192.168.0.100:3698	3698	192.168.0.1:80	tcp	CL	OUT	9
192.168.0.100:3697	3697	192.168.0.1:80	tcp	CL	OUT	9
192.168.0.100:3696	3696	192.168.0.1:80	tcp	CL	OUT	9
192.168.0.100:3695	3695	192.168.0.1:80	tcp	CL	OUT	9
192.168.0.100:3694	3694	192.168.0.1:80	tcp	CL	OUT	9
192.168.0.100:3693	3693	192.168.0.1:80	tcp	TW	OUT	119
192.168.0.100:3689	3689	192.168.0.1:80	tcp	TW	OUT	105
192.168.0.100:3688	3688	192.168.0.1:80	tcp	TW	OUT	105
192.168.0.100:3679	3679	192.168.0.1:80	tcp	TW	OUT	105
192.168.0.100:3675	3675	192.168.0.1:80	tcp	TW	OUT	101
192.168.0.100:3674	3674	192.168.0.1:80	tcp	TW	OUT	101
192.168.0.100:3673	3673	192.168.0.1:80	tcp	TW	OUT	101
192.168.0.100:3672	3672	192.168.0.1:80	tcp	TW	OUT	101
192.168.0.100:3663	3663	192.168.0.1:80	tcp	TW	OUT	101
192.168.0.100:3662	3662	192.168.0.1:80	tcp	TW	OUT	101
192.168.0.100:3661	3661	192.168.0.1:80	tcp	TW	OUT	97
192.168.0.100:3660	3660	192.168.0.1:80	tcp	TW	OUT	93

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

# Routing

This page will display your current routing table.

The screenshot shows the D-Link DIR-862L web interface. The top navigation bar includes tabs for SETUP, ADVANCED, TOOLS, STATUS, and SUPPORT. The left sidebar contains a menu with options: DEVICE INFO, LOGS, STATISTICS, INTERNET SESSIONS, WIRELESS, ROUTING (selected), IPv6, and IPV6 ROUTING. The main content area is titled "ROUTING" and "Routing Table", with a sub-header "ROUTING TABLE". Below this is a table with the following data:

Destination	Gateway	Genmask	Metric	Iface	Creator
192.168.7.0	0.0.0.0	255.255.255.0	0	LAN	SYSTEM
192.168.0.0	0.0.0.0	255.255.255.0	0	LAN	SYSTEM
239.0.0.0	0.0.0.0	255.0.0.0	0	LAN	SYSTEM

On the right side of the interface, there is a "Helpful Hints..." section with the following text:

- This is a list of all routing rules on router.
- [More...](#)

The bottom of the page features a "WIRELESS" tab.

# 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-862L // SETUP ADVANCED TOOLS STATUS SUPPORT

DEVICE INFO  
LOGS  
STATISTICS  
INTERNET SESSIONS  
**WIRELESS**  
ROUTING  
IPv6  
IPv6 ROUTING

**CONNECTED WIRELESS CLIENT LIST**  
View the wireless clients that are connected to the router. (A client might linger in the list for a few minutes after an unexpected disconnect.)

**NUMBER OF WIRELESS CLIENTS - 2.4GHZ BAND : 0**

MAC Address	IP Address	Mode	Rate (Mbps)	Signal (%)

**NUMBER OF WIRELESS CLIENTS - 5GHZ BAND : 0**

MAC Address	IP Address	Mode	Rate (Mbps)	Signal (%)

**Helpful Hints...**

- This is a list of all wireless clients that are currently connected to your wireless router.
- [More...](#)

**WIRELESS**

# IPv6

The IPv6 page displays a summary of the Router's IPv6 settings and lists the IPv6 address and host name of any IPv6 clients.

D-Link					
DIR-862L	SETUP	ADVANCED	TOOLS	STATUS	SUPPORT
DEVICE INFO	<b>IPv6 NETWORK INFORMATION</b>				<b>Helpful Hints...</b> <ul style="list-style-type: none"> <li>All of your WAN and LAN connection details are displayed here.</li> <li><a href="#">More...</a></li> </ul>
LOGS	All of your Internet and network connection details are displayed on this page. The firmware version is also displayed here.				
STATISTICS	<b>IPv6 CONNECTION INFORMATION</b>				
INTERNET SESSIONS	<b>IPv6 Connection Type</b> : Link-Local <b>IPv6 Default Gateway</b> : None <b>LAN IPv6 Link-Local Address</b> : fe80::bef6:85ff:fed2:4a35 /64				
WIRELESS	<b>LAN IPv6 COMPUTERS</b>				
ROUTING	IPv6 Address		Name(if any)		
IPv6	<b>WIRELESS</b>				
IPv6 ROUTING					

# IPv6 Routing

This page displays the IPv6 routing details configured for your router.

The screenshot shows the D-Link DIR-862L web interface. The top navigation bar includes the D-Link logo and tabs for SETUP, ADVANCED, TOOLS, STATUS, and SUPPORT. The left sidebar contains a menu with options: DEVICE INFO, LOGS, STATISTICS, INTERNET SESSIONS, ROUTING, WIRELESS, IPV6, and IPv6 Routing. The main content area is titled "IPv6 ROUTING" and contains the following text:

**IPv6 Routing Table**

This page displays the routing details configured for your router.

**IPv6 ROUTING TABLE**

Destination IP	Gateway	Metric	Interface
----------------	---------	--------	-----------

The table is currently empty. The bottom of the page features the "WIRELESS" logo.

# Support

This page provides help and explanations for different sections of the firmware.

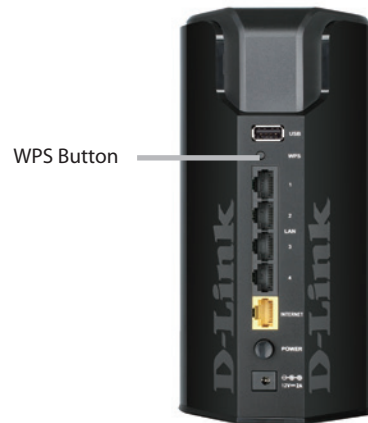
The screenshot displays the D-Link DIR-862L web interface. At the top, the D-Link logo is visible. Below it, a navigation bar contains tabs for SETUP, ADVANCED, TOOLS, STATUS, and SUPPORT. The SUPPORT tab is selected. On the left side, a vertical menu lists the main sections: MENU, SETUP, ADVANCED, TOOLS, and STATUS. The main content area is titled 'SUPPORT MENU' and contains a list of links: Setup, Advanced, Tools, and Status. Below this, there are four help sections: 'SETUP HELP' with links for Internet Connection, WAN, Wireless, Network Settings, Storage, IPv6, and mxdlink Settings; 'ADVANCED HELP' with links for Virtual Server, Port Forwarding, Application Rules, QoS Engine, Network Filter, Access Control, Website Filter, Inbound Filter, Firewall Settings, Routing, Advanced Wireless, Wi-Fi Protected Setup, Advanced Network, GUEST ZONE, IPv6 FIREWALL, and IPv6 Routing; 'TOOLS HELP' with links for Admin, TIME, Syslog, Email Settings, System, FIRMWARE, Dynamic DNS, System Check, and Schedules; and 'STATUS HELP' with links for Device Info, Logs, Statistics, Internet Sessions, Routing, Wireless, IPv6, and IPv6 Routing.

# Connect a Wireless Client to your Router

## WPS Button

The easiest and most secure way to connect your wireless devices to the router is WPS (Wi-Fi Protected Setup). Most wireless devices such as wireless adapters, media players, Blu-ray DVD players, wireless printers and cameras will have a WPS button (or a software utility with WPS) that you can press to connect to the DIR-862L router. Please refer to your user manual for the wireless device you want to connect to make sure you understand how to enable WPS. Once you know, follow the steps below:

**Step 1** - Press the WPS button on the DIR-862L for about 1 second. The Internet LED on the front will start to blink.



**Step 2** - Within 2 minutes, press the WPS button on your wireless client (or launch the software utility and start the WPS process).

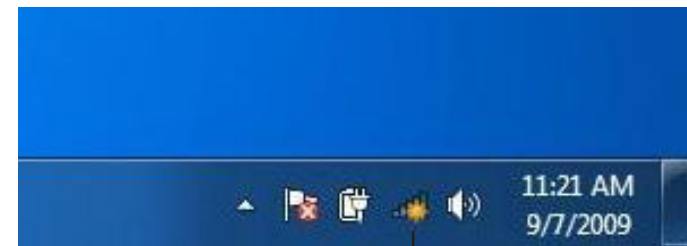
**Step 3** - Allow up to 1 minute to configure. Once the Internet light stops blinking, you will be connected and your wireless connection will be secure with WPA2.

# Windows® 7

## WPA/WPA2

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. Click on the wireless icon in your system tray (lower-right corner).



Wireless Icon

2. The utility will display any available wireless networks in your area.



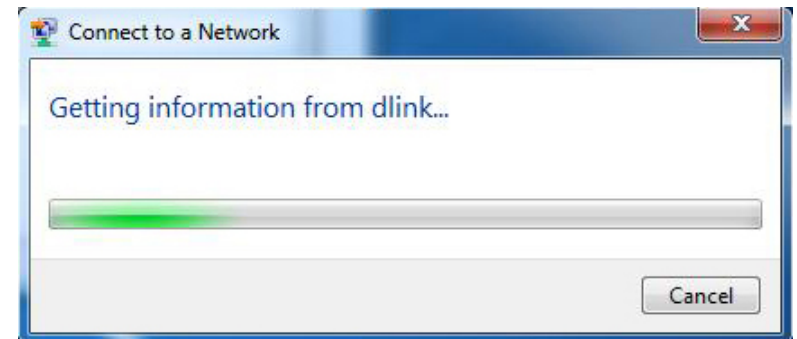


3. Highlight the wireless connection with Wi-Fi name (SSID) you would like to connect to and click the **Connect** button.

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

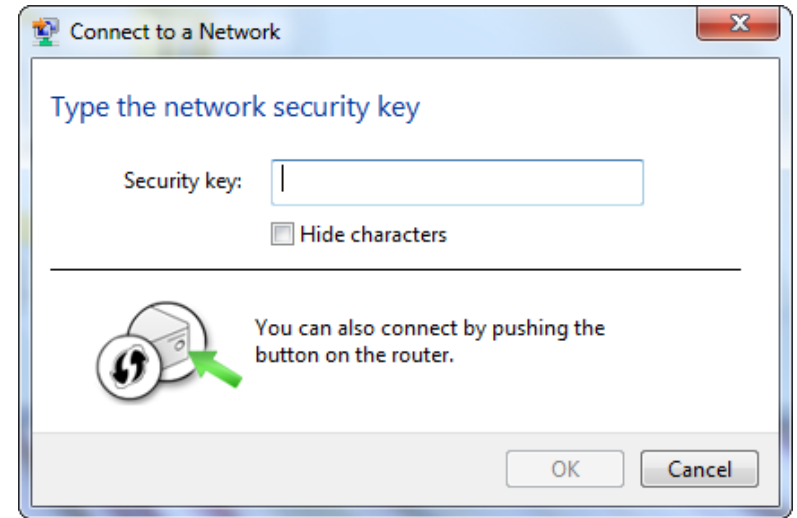


4. The following window appears while your computer tries to connect to the router.



5. Enter the same security key or passphrase (Wi-Fi password) that is on your router and click **Connect**. You can also connect by pushing the WPS button on the router.

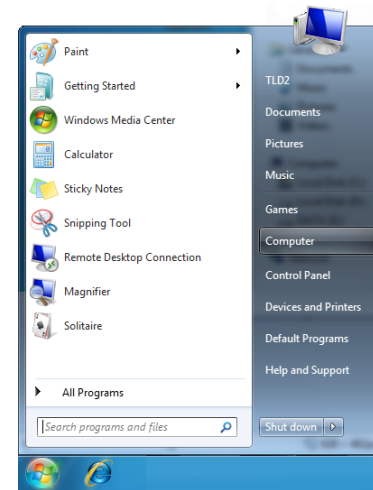
It may take 20-30 seconds to connect to the wireless network. If the connection fails, please verify that the security settings are correct. The key or passphrase must be exactly the same as on the wireless router.



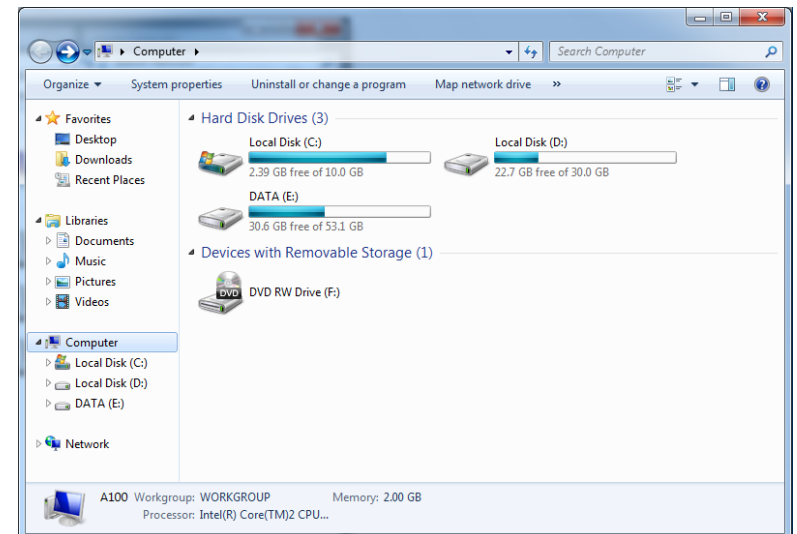
# WPS

The WPS feature of the DIR-862L can be configured using Windows® 7. Carry out the following steps to use Windows® 7 to configure the WPS feature:

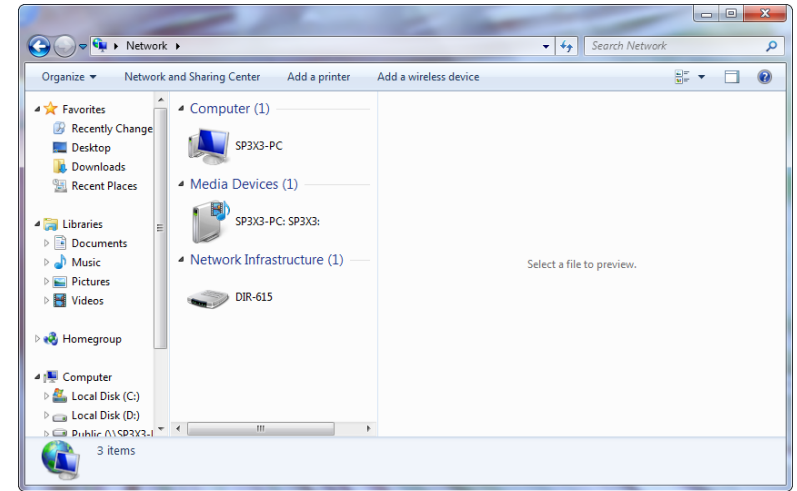
1. Click the **Start** button and select **Computer** from the Start menu.



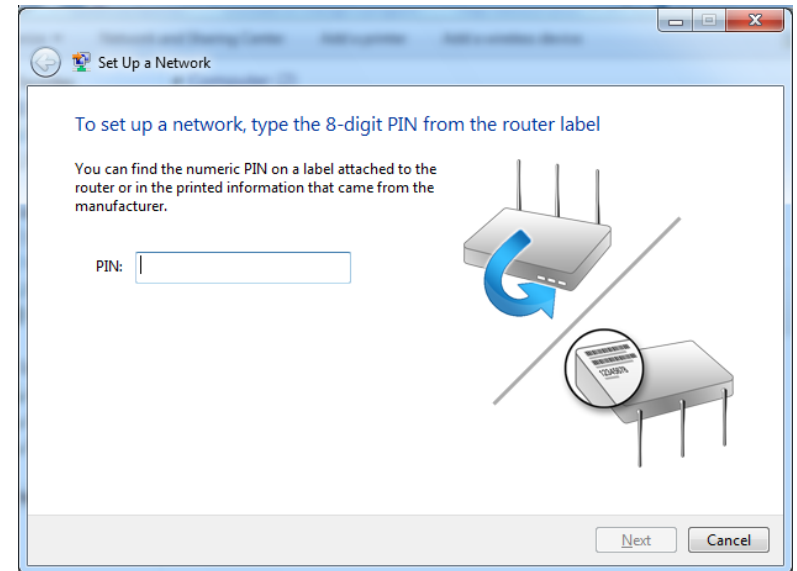
2. Click **Network** on the left side.



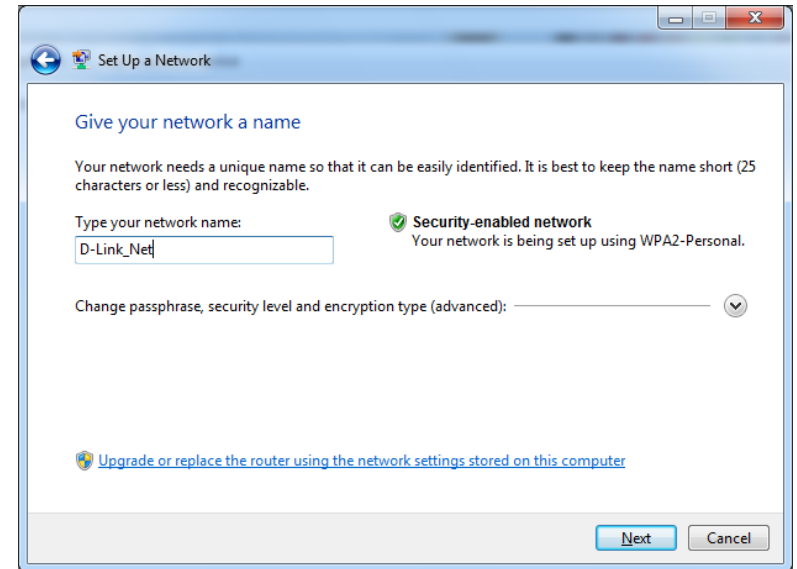
3. Double-click the DIR-862L.




4. Input the WPS PIN number (displayed in the WPS window on the Router's LCD screen or in the **Setup > Wireless Setup** menu in the Router's Web UI) and click **Next**.

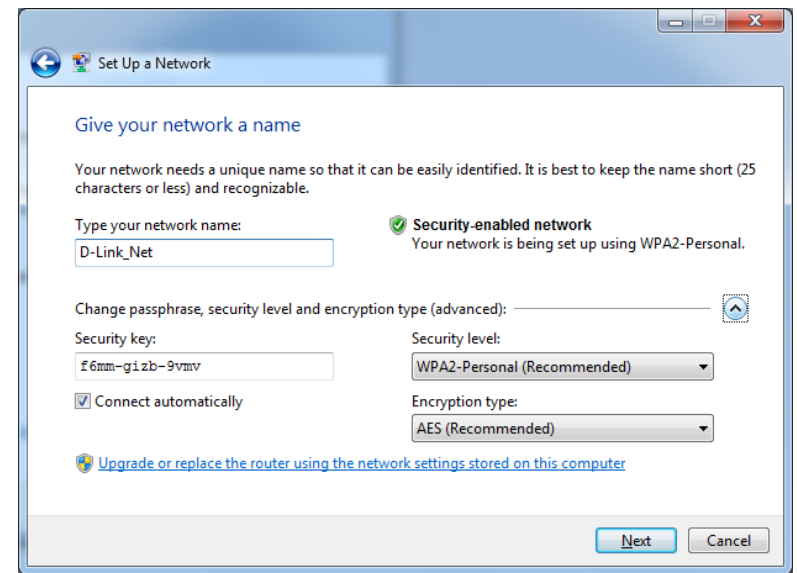


5. Type a name to identify the network.



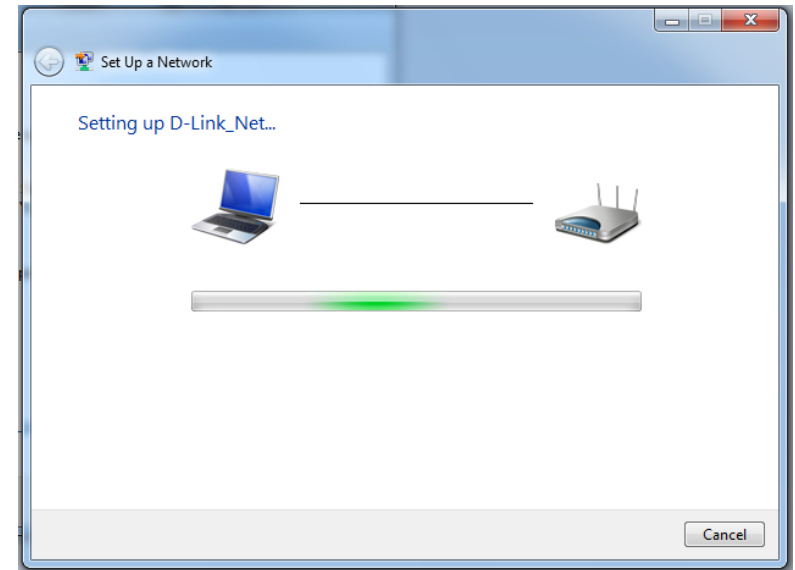
6. To configure advanced settings, click the  icon.

Click **Next** to continue.



7. The following window appears while the Router is being configured.

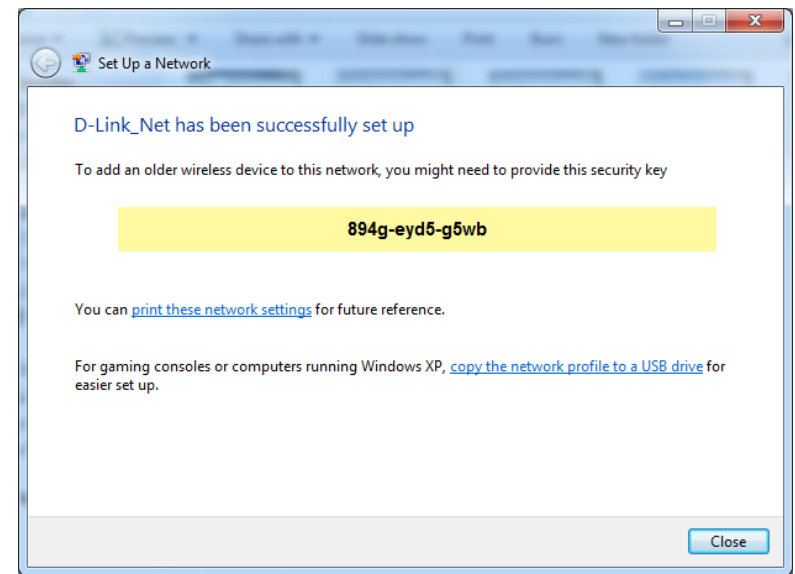
Wait for the configuration to complete.



8. The following window informs you that WPS on the router has been setup successfully.

Make a note of the security key as you may need to provide this security key if adding an older wireless device to the network in the future.

9. Click **Close** to complete WPS setup.



# Windows Vista®

Windows Vista® users may use the built-in wireless utility. If you are using another company's utility, 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.

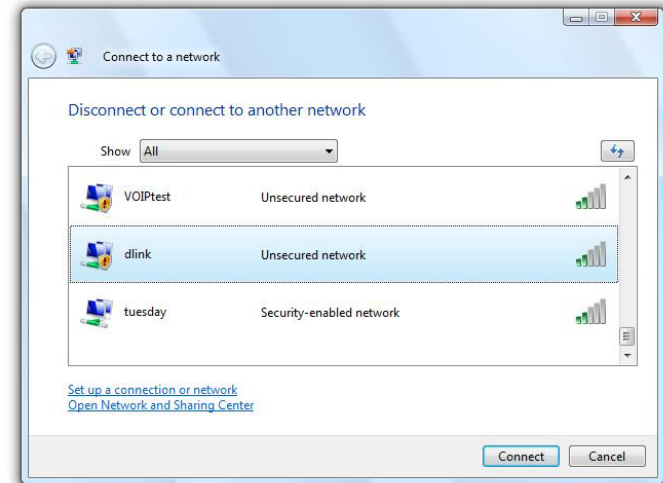
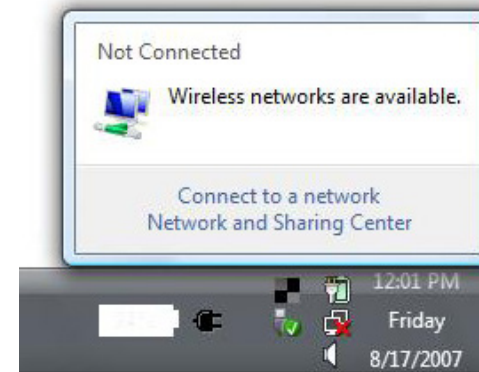
If you receive the **Wireless Networks Detected** bubble, click on the center of the bubble to access the utility.

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.

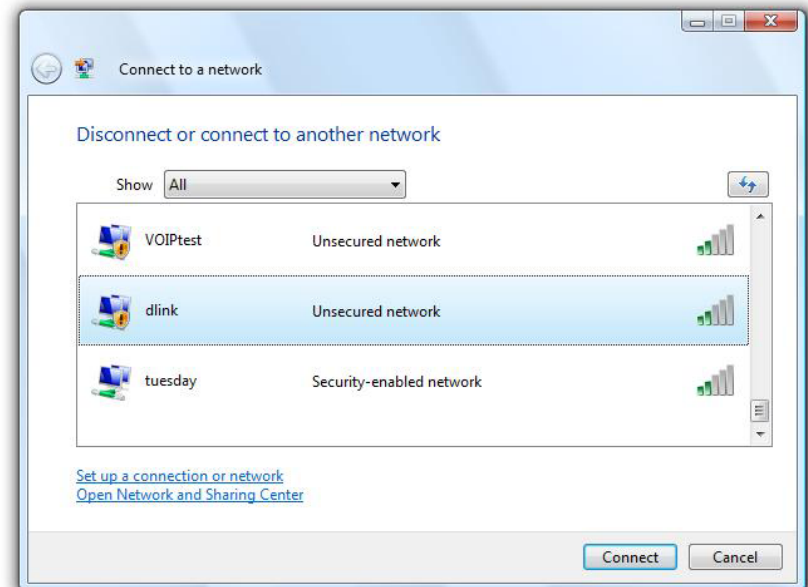
If you get a good signal but cannot access the Internet, check you TCP/IP settings for your wireless adapter. Refer to the **Networking Basics** section in this manual for more information.



## WPA/WPA2

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.

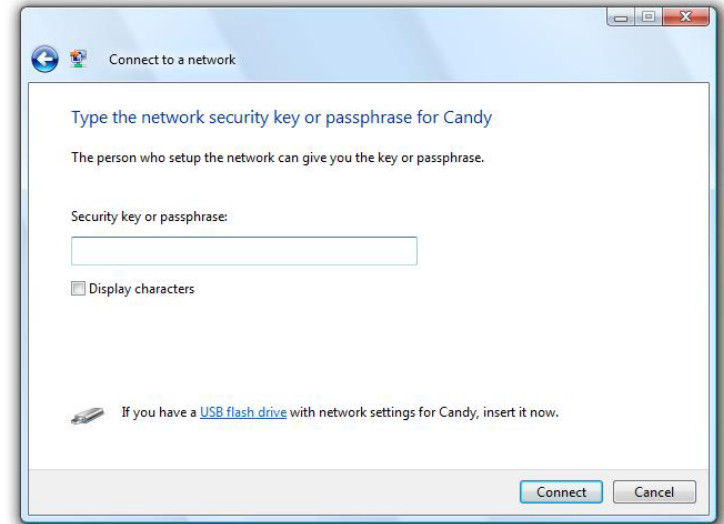
1. Open the Windows Vista® Wireless Utility by right-clicking on the wireless computer icon in your system tray (lower right corner of screen). Select **Connect to a network**.
2. Highlight the Wi-Fi name (SSID) you would like to connect to and click **Connect**.





3. Enter the same security key or passphrase (Wi-Fi password) 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.



## WPS/WCN 2.0

This router supports Wi-Fi protection, referred to as WCN 2.0 in Windows Vista®. The following instructions for setting this up depend 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.



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.

# 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, 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.

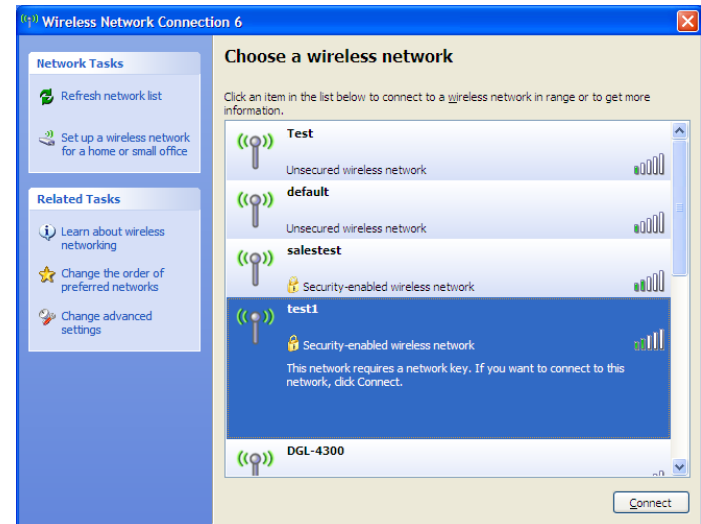
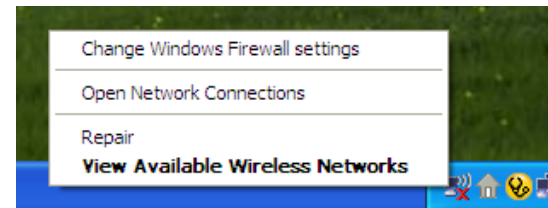
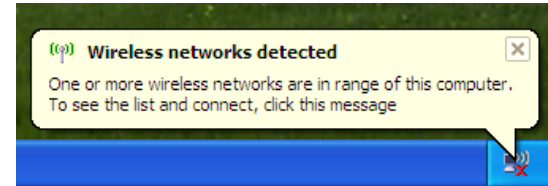
If you receive the **Wireless Networks Detected** bubble, click on the center of the bubble to access the utility.

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 Wi-Fi network (displayed using the SSID) and click the **Connect** button.

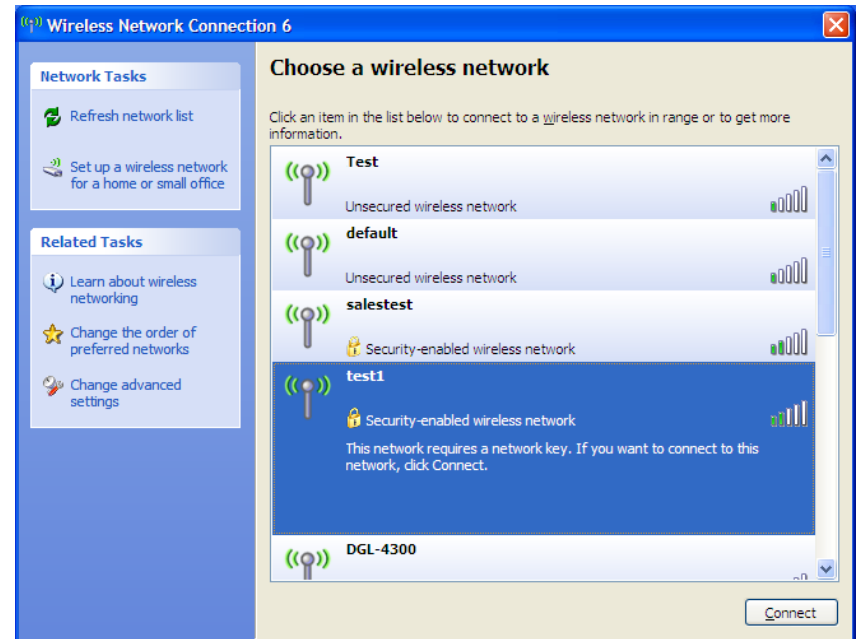
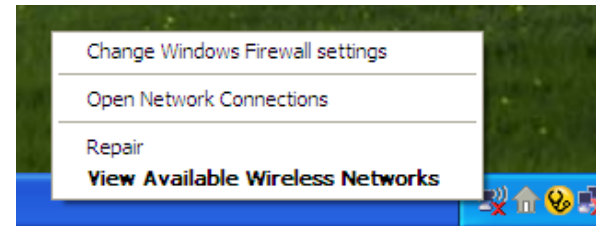
If you get a good signal but cannot access the Internet, check you TCP/IP settings for your wireless adapter. Refer to the **Networking Basics** section in this manual for more information.



## WPA/WPA2

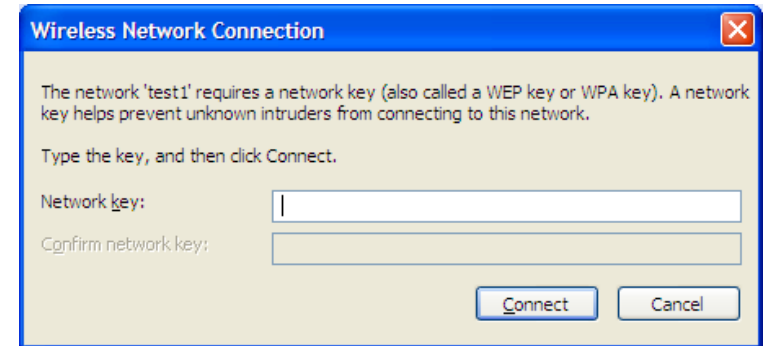
It is recommended to enable WPA on your wireless router or access point before configuring your wireless adapter. If you are joining an existing network, you will need to know the WPA key being used.

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 Wi-Fi network (SSID) you would like to connect to and click **Connect**.



3. The **Wireless Network Connection** box will appear. Enter the WPA-PSK Wi-Fi password 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 Wi-Fi password 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-862L. 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 nor do you 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:
  - Microsoft Internet Explorer® 7 and higher
  - Mozilla Firefox 3.5 and higher
  - Google™ Chrome 8 and higher
  - Apple Safari 4 and 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 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).

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, XP, Vista®, and 7 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.
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, let's 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?**

People use wireless or Wi-Fi technology as a way of connecting your computer to a 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?**

Overall, 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?**

Phones that connect wirelessly to a base station work like wireless does, using radio signals to transmit data from 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)**

Every local area network needs 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, 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)**

Range for Bluetooth (WPAN industry standard) is up to 30 feet away and eliminates the need for many cables.

Only WLAN has the speed and wireless operation range suitable for computers transmitting large amounts of data, but WPAN 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?**

Customers and employees, students and teachers, family members; everyone uses wireless. It has become so popular in recent years that almost everyone is using it. Whether it's for home or office, D-Link has a wireless solution for it.

### **Home**

- Kids won't trip over cables
- Email, surf, chat, game, etc...
- The only way to connect with new devices such as phones and tablets
- Freedom to move from room to room

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

- Instant access for visitors with guest networks
- Stay on top of everything at home as you would at the office
- Trim purchasing and maintenance costs associated with cables
- 32 or even more connections so everyone can get online

## **Where is wireless used?**

Wireless technology is expanding everywhere, not just at home or in the 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 connections in public places are usually called "hotspots".

Using a Wi-Fi enabled laptop, you can access a hotspot to connect to the Internet from remote locations like airports, hotels, coffee shops, libraries, restaurants, and convention centers.

A wireless network is easy to setup, but if you're installing one 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 and 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 will significantly reduce any interference that the appliances might cause since they operate on same frequency.

## Security

Don't let your 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.

# 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.

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 Wi-Fi enabled laptops. All the adapters must be in Ad-Hoc mode to communicate.

# Networking Basics

## Check your IP address

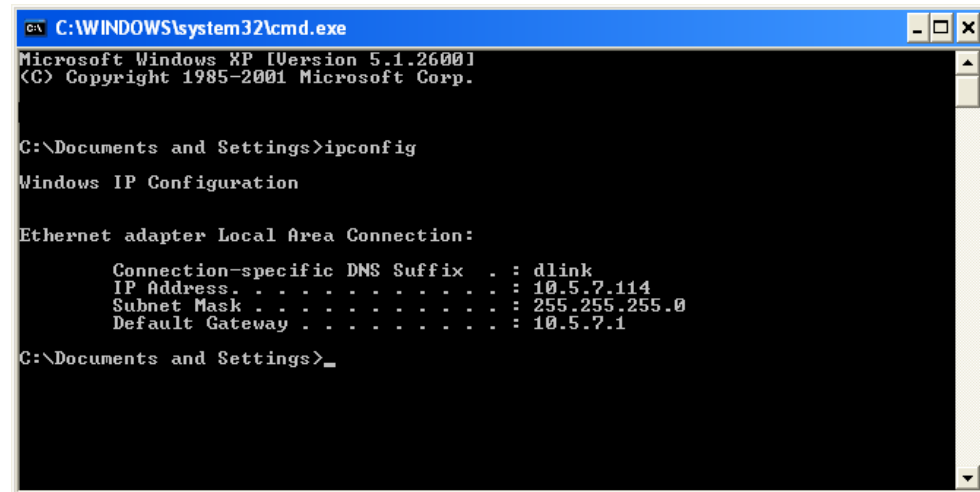
After you install your new D-Link adapter, by default, the TCP/IP settings should be set to obtain an IP address from a DHCP server (i.e. wireless router) automatically. To verify your IP address, please follow the steps below.

Click on **Start > Run**. In the run box type **cmd** and click **OK**. (Windows® 7/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.



```
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® 7 - Click on **Start > Control Panel > Network and Internet > Network and Sharing Center**.
- 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 network adapter and select **Properties**.

**Step 3**

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

**Step 4**

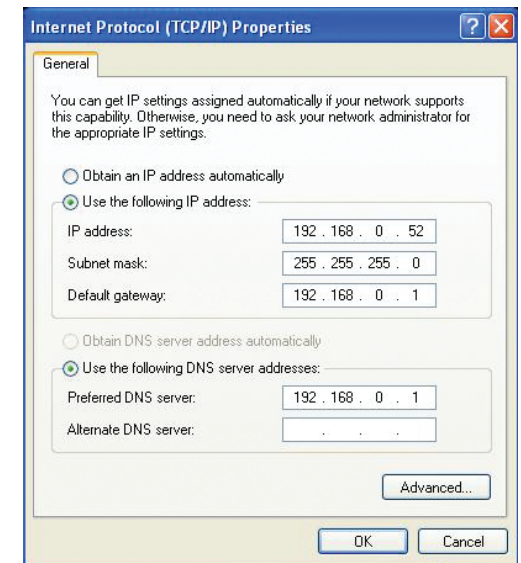
Click **Use the following IP address** and enter an IP address that is on the same subnet as your network or the LAN IP address on your router.

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 the Default Gateway the same as the LAN IP address of your router (e.g. 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

## Hardware Specifications

- LAN Interface: Four 10/100/1000 Gigabit LAN ports
- WAN Interface: 10/100/1000 Gigabit WAN port
- Wireless Interface (2.4 GHz): IEEE 802.11b/g/n
- Wireless Interface (5 GHz): IEEE 802.11a/n/ac
- USB Interface: USB 2.0 Compliant

## Operating Voltage

- Input: 100~240V ( $\pm 20\%$ ), 50~60Hz
- Output: DC12V, 2A

## Temperature

- Operating: 32 ~ 104°F (0 ~ 40°C)
- Non-Operating: -4 ~ 149°F (-20 ~ 65°C)

## Humidity

- Operating: 10% - 90% non-condensing
- Non-Operating: 5% - 95% non-condensing

## Standards

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

## Wireless Bandwidth Rate

- IEEE 802.11a: 54, 48, 36, 24, 18, 12, 9, and 6 Mbps
- IEEE 802.11b: 11, 5.5, 2, and 1 Mbps
- IEEE 802.11g: 54, 48, 36, 24, 18, 12, 9, and 6 Mbps
- IEEE 802.11n: 6.5 to 450 Mbps
- IEEE 802.11ac: 6.5 to 1299.9 Mbps

## Antenna Type

- Six Internal Antennas (Three 2.4 GHz Antennas, Three 5 GHz Antennas)

## Wireless Security

- 64/128bit WEP, WPA/WPA2-Personal, WPA/WPA2-Enterprise, WPS (PIN & PBC)
- FCC, IC
- Wi-Fi / WPS
- IPv6 Ready
- WIN 8

## Certifications

- FCC, IC
- cUL
- Wi-Fi / WPS
- IPv6 Ready
- WIN 8

## Federal Communication Commission Interference 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.

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.

This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter. Operations in the 5.15-5.25GHz band are restricted to indoor usage only.

### **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.

## Industry Canada Statement

This device complies with RSS-210 of the Industry Canada 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.

Ce dispositif est conforme à la norme CNR-210 d'Industrie Canada applicable aux appareils radio exempts de licence. Son fonctionnement est sujet aux deux conditions suivantes: (1) le dispositif ne doit pas produire de brouillage préjudiciable, et (2) ce dispositif doit accepter tout brouillage reçu, y compris un brouillage susceptible de provoquer un fonctionnement indésirable.

**Caution :**

- (i) the device for operation in the band 5150-5250 MHz is only for indoor use to reduce the potential for harmful interference to co-channel mobile satellite systems;
- (ii) high-power radars are allocated as primary users (i.e. priority users) of the bands 5250-5350 MHz and 5650-5850 MHz and that these radars could cause interference and/or damage to LE-LAN devices.

**Avertissement:**

- (i) les dispositifs fonctionnant dans la bande 5150-5250 MHz sont réservés uniquement pour une utilisation à l'intérieur afin de réduire les risques de brouillage préjudiciable aux systèmes de satellites mobiles utilisant les mêmes canaux;
- (ii) De plus, les utilisateurs devraient aussi être avisés que les utilisateurs de radars de haute puissance sont désignés utilisateurs principaux (c.-à-d., qu'ils ont la priorité) pour les bandes 5250-5350 MHz et 5650-5850 MHz et que ces radars pourraient causer du brouillage et/ou des dommages aux dispositifs LAN-EL.

**Radiation Exposure Statement:**

This equipment complies with IC 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.

**Déclaration d'exposition aux radiations:**

Cet équipement est conforme aux limites d'exposition aux rayonnements IC établies pour un environnement non contrôlé. Cet équipement doit être installé et utilisé avec un minimum de 20cm de distance entre la source de rayonnement et votre corps.