

## SD Card

This page allows you to browse and manage the recorded files on an SD card which is inserted into the camera.

A list of files stored on the inserted SD card is displayed. By selecting the check box, you can selectively delete video or images. If you want to erase the SD card or if it is a new one, click **Format SD Card**.

**Note:** Format SD Card will erase all the contents of the SD card.

Product: DCS-942L Firmware version: 1.00

**D-Link**

DCS-942L // LIVE VIDEO SETUP MAINTENANCE STATUS HELP

Setup Wizard  
Network  
Wireless Setup  
Dynamic DNS  
Image Setup  
Audio and Video  
Time and Date  
Video Clip  
Snapshot  
Motion Detection  
SD Card  
Logout

**SD CARD**  
Here you could browse and manage the record files which stored in SD Card.

**SD CARD**  
SD Card [DCS-942L /](#) SD Status : Invalid  
Files per Page: 5 [Refresh](#) Pages: 0 of  
 Delete 

| Name | Size |
|------|------|
|------|------|

  
 Total : KB, Used : KB, Free : KB

**Helpful Hints..**  
Click this icon to automatically format the SD Card and create "Video" folder.

**SURVEILLANCE**

# Maintenance Admin

This section allows you to change the administrator's password and configure the server settings for your camera. You can also manage the user account(s) that access to your camera.

**Admin Password Setting:** To change your password, enter your current password and then enter the new one in the **New Password** and **Confirm New Password** fields.

**Add User Account:** Create a new user for accessing the video image. Enter the user name, password, and password confirmation, and click **Add**. A maximum of 8 user accounts can be added into the user list.

**User List:** Select a user from the drop-down menu and click **Delete** to remove the user account from having access to the camera images.

**RTSP Authentication:** Enable user validation for RTSP streaming.

**HTTP Authentication:** Enable user validation for HTTP streaming.

**Snapshot URL Authentication:** Select **Enable** to allow access to the current camera snapshot via the web address indicated.

**Camera Name:** Specify a name for your camera.

**OSD:** In the **Label** field, you may enter a name to display on the image and check a box to put the current time on the image also.

**LED Light:** Select **Normal** to enable the LED on the front of the device, or select off to disable the LED. It can also be set to flicker on and off.

Product: DCS-942L Firmware version: 1.00

**D-Link**

DCS-942L // LIVE VIDEO SETUP MAINTENANCE STATUS HELP

Admin System Firmware Upgrade Logout

**ADMIN**

Here you can change the administrator's password for your account as well as add and/or delete user account(s). You can also configure a unique name for your camera, and enable its OSD (On-Screen Display) feature in order to display camera name and time stamp for both live video and recordings of your camera.

**ADMIN PASSWORD SETTING**

Old Password  30 characters maximum

New Password  30 characters maximum

Confirm New Password

**ADD USER ACCOUNT**

User Name  30 characters maximum

New Password  30 characters maximum

Confirm New Password

20 users maximum

**USER LIST**

User Name -- User list --

**AUTHENTICATION**

RTSP Authentication

HTTP Authentication

Snapshot URL Authentication (<http://192.168.0.101/image/jpeg.cgi>)

**DEVICE SETTING**

Camera Name  DCS-942L 36 characters maximum

OSD

Label  DCS-942L 30 characters maximum

Time Stamp

LED light  Power/Link

**Helpful Hints..**

For security purposes, it is recommended to change the password for your administrator account. Be sure to write down the new password to avoid having to reset the camera in the event that it is forgotten.

**User Account**  
User account is given to an user a privilege to login into Live View page and use functions in the page.

**RTSP Authentication**  
Enable user validation for RTSP streaming.

**HTTP Authentication**  
Enable user validation for HTTP streaming.

**Snapshot URL Authentication**  
Enable user validation for Snapshot URL.

**OSD**  
Enable OSD, the camera name and time will be displayed on the video screen.

**LED light Power/Link**  
Normal LED blinking depending on power and linkage status.  
**Off**  
Always turn off LED.  
**Flicker**  
Always flicking LED.

SURVEILLANCE

## System

This section allows you to save and restore your configuration, restore the factory settings, and/or restart the camera.

The screenshot displays the web interface for a D-Link DCS-942L camera. At the top, it shows 'Product: DCS-942L' and 'Firmware version: 1.00'. The D-Link logo is prominently displayed in an orange banner. Below this is a navigation menu with tabs for 'LIVE VIDEO', 'SETUP', 'MAINTENANCE', 'STATUS', and 'HELP'. The 'SYSTEM' page is active, showing options to 'Save To Local Hard Drive', 'Load From Local Hard Drive', 'Restore To Factory Defaults', and 'Reboot Device'. A 'Helpful Hints..' section on the right provides instructions on restoring factory settings.

| DCS-942L         | LIVE VIDEO  | SETUP                    | MAINTENANCE        | STATUS | HELP   |
|------------------|---|--------------------------|--------------------|--------|--|
| Admin            | <b>SYSTEM</b>   |                          |                    |        | <b>Helpful Hints..</b><br>After the factory's default settings have been restored, use the installation wizard software provided with your camera to search and connect to the camera. |
| System           | Here you may backup, restore, and reboot your camera. |                          |                    |        |  |
| Firmware Upgrade | <b>SYSTEM</b>   |                          |                    |        |  |
| Logout           | Save To Local Hard Drive                              | Save Configuration       |                    |        |  |
|                  | Load From Local Hard Drive                            | Browse..                 | Load Configuration |        |  |
|                  | Restore To Factory Defaults                           | Restore Factory Defaults |                    |        |  |
|                  | Reboot Device   | Reboot Device            |                    |        |  |

**SURVEILLANCE**

## Firmware Upgrade

Your current firmware version and date will be displayed on your screen. You may go to the D-Link Support Page to check for the latest firmware versions available.

To upgrade the firmware on your DCS-942L, please download and save the latest firmware version from the D-Link Support Page to your local hard drive. Locate the file on your local hard drive by using the **Browse** button. Then, click the **Upload** button to start the firmware upgrade.

The screenshot shows the D-Link web interface for a DCS-942L camera. The top navigation bar includes 'LIVE VIDEO', 'SETUP', 'MAINTENANCE', 'STATUS', and 'HELP'. The 'MAINTENANCE' tab is selected. The main content area is titled 'FIRMWARE UPGRADE' and contains the following text:

A new firmware upgrade may be available for your camera. It is recommended to keep your camera firmware up-to-date to maintain and improve the functionality and performance of your internet camera. Click here [D-Link Support Page](#) to check for the latest firmware version available.

To upgrade the firmware on your IP camera, please download and save the latest firmware version from the D-Link Support Page to your local hard drive. Locate the file on your local hard drive by clicking the Browse button. Once you have found and opened the file using the browse button, click the **Upload** button to start the firmware upgrade.

Below the text is a section titled 'FIRMWARE INFORMATION' with the following details:

|                            |            |
|----------------------------|------------|
| Current Firmware Version : | 1.00       |
| Current Firmware Date :    | 2010-04-29 |

At the bottom of the main content area is another 'FIRMWARE UPGRADE' section with a file upload form:

File Path :

The right sidebar contains 'Helpful Hints..' with the following text:

Firmware updates are released periodically to improve the functionality of your IP camera and also to add new features. If you run into a problem with a specific feature of the IP camera, check our support site by clicking [here](#) and see if updated firmware is available for your IP camera.

# Status

## Device Info

This section displays detailed information about your device and network settings.

Product: DCS-942L Firmware version: 1.00

**D-Link**

DCS-942L // LIVE VIDEO SETUP MAINTENANCE **STATUS** HELP

Device Info

Log

Logout

**DEVICE INFO**

All of your network connection details are displayed on this page. The firmware version is also displayed here.

**Helpful Hints..**

This page displays all the information about the camera and network settings.

**INFORMATION**

|                       |                             |
|-----------------------|-----------------------------|
| Camera Name           | DCS-942L                    |
| Time & Date           | Sat Jan 1 05:29:03 2011 DST |
| Firmware Version      | 1.00                        |
| Firmware Build Number | 0506                        |
| MAC Address           | 1C:AF:F7:74:AA:01           |
| IPv4 Address          | 192.168.0.101               |
| IPv4 Subnet Mask      | 255.255.255.0               |
| IPv4 Default Gateway  | 192.168.0.1                 |
| IPv4 Primary DNS      | 192.168.0.1                 |
| IPv4 Secondary DNS    |                             |
| PPPoE Status          | Disable                     |
| DDNS Status           | Disable                     |

**SURVEILLANCE**

# Log

The system log records camera events that have occurred.

The screenshot shows the D-Link DCS-942L web interface. At the top, it displays 'Product: DCS-942L' and 'Firmware version: 1.00'. The D-Link logo is prominently featured. Below the logo is a navigation menu with tabs for 'DCS-942L', 'LIVE VIDEO', 'SETUP', 'MAINTENANCE', 'STATUS', and 'HELP'. The 'Log' page is active, showing a sidebar with 'Device Info', 'Log', and 'Logout' options. The main content area is divided into two sections: 'SYSTEM LOG' and 'CURRENT LOG'. The 'SYSTEM LOG' section contains the text: 'The system log records camera events that have occurred.' The 'CURRENT LOG' section lists four entries: '2011-01-01 00:02:48 admin is streaming video.', '2011-01-01 00:02:48 admin is streaming video.', '2011-01-01 02:40:50 admin is streaming video.', and '2011-01-01 02:40:56 admin is streaming video.'. Below the current log entries are 'Clear' and 'Download' buttons. On the right side, a 'Helpful Hints..' section provides instructions: 'You can save the log to your local hard drive by clicking the Download button, and you can clear the log by clicking on the Clear button.' The bottom of the interface features a 'SURVEILLANCE' banner.

# Wireless Security

This section will show you the different levels of security you can use to protect your data from intruders.

The DCS-942L offers the following types of security:

- WPA-PSK (Pre-Shared Key)
- WEP (Wired Equivalent Privacy)

## What is WEP?

WEP stands for Wired Equivalent Privacy. It is based on the IEEE 802.11 standard and uses the RC4 encryption algorithm. WEP provides security by encrypting data over your wireless network so that it is protected as it is transmitted from one wireless device to another.

To gain access to a WEP network, you must know the key. The key is a string of characters that you create. When using WEP, you must determine the level of encryption. The type of encryption determines the key length. 128-bit encryption requires a longer key than 64-bit encryption. Keys are defined by entering in a string in HEX (hexadecimal - using characters 0-9, A-F) or ASCII (American Standard Code for Information Interchange – alphanumeric characters) format. ASCII format is provided so you can enter a string that is easier to remember. The ASCII string is converted to HEX for use over the network. Four keys can be defined so that you can change keys easily.

# What is WPA?

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

The 2 major improvements over WEP:

Improved data encryption through the Temporal Key Integrity Protocol (TKIP). TKIP scrambles the keys using a hashing algorithm and, by adding an integrity-checking feature, ensures that the keys haven't been tampered with. WPA2 is based on 802.11i and uses Advanced Encryption Standard instead of TKIP.

User authentication, which is generally missing in WEP, through the extensible authentication protocol (EAP). WEP regulates access to a wireless network based on a computer's hardware-specific MAC address, which is relatively simple to be sniffed out and stolen. EAP is built on a more secure public-key encryption system to ensure that only authorized network users can access the network.

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



## Configuring the DCS-942L with a Router

D-Link's DCS-942L is a versatile and cost effective Network Camera offering both video and audio monitoring. It can also serve as a powerful surveillance system in security applications. The DCS-942L can be used with any wired or 802.11n/g wireless router. This section explains how to view the camera from either the Internet or from inside your internal network.

Components Needed:

- 1 DCS-942L Network Camera
- 1 Ethernet Cable
- A Wired or Wireless router such as the D-Link DIR-655 Wireless Router
- Ethernet based PC for system configuration

### Setting up the DCS-942L for Use Behind a Router

Installing a DCS-942L Network Camera on your network is an easy 4–step procedure:

1. Assign a local IP address to your network camera.
2. View the network camera using your Internet Explorer web browser.
3. Access the router with your web browser.
4. Open virtual server ports to enable remote image viewing.

**Note:** *These are manual steps; however, if you decide to use the wizard, it will perform every step automatically.*

This section is designed to walk you through the setup process for installing your camera behind a router and enable remote video viewing. For the basic setup of the DCS-942L, follow the steps outlined in the Quick Install Guide.

After you have completed the setup of the DCS-942L outlined in the Quick Installation Guide you will have an operating camera that has an assigned IP Address. Because you are using a router to share the Internet with one or more PCs, the IP Address assigned to the Network Camera will be a local IP Address. This allows viewing within your Local Area Network (LAN) until the router is configured to allow remote viewing of the camera over the Internet.

## 1. Assign a Local IP Address to Your Camera

Run the setup wizard from the CD included with the DCS-942L. Follow the steps in the Quick Install Guide to configure the DCS-942L. The camera will be assigned a local IP Address that allows it to be recognized by the router. Write down this IP Address for future reference.

## 2. View the Network Camera Using Your Internet Explorer Web Browser

Run your Internet Explorer Web browser. In the address bar, type in the IP Address that was assigned to the Network Camera by the DCC program. The DCS-942L Live Video Page appears with a window displaying live video from the camera. You are able to view this screen from any PC running Internet Explorer on your LAN.

Click on the **Setup** button on the left side of the display. Scroll to the bottom of the Network Setup page to display the ports used by HTTP and Streaming audio and video.

| DIR-655           | SETUP  | ADVANCED | TOOLS | STATUS | SUPPORT  |
|-------------------|--|----------|-------|--------|--|
| DEVICE INFO       | <b>DEVICE INFORMATION</b>  |          |       |        | Helpful Hints...   |
| LOGS              | All of your Internet and network connection details are displayed on this page. The firmware version is also displayed here.   |          |       |        | All of your WAN and LAN connection details are displayed here. |
| STATISTICS        | <b>GENERAL</b>   |          |       |        | More...  |
| INTERNET SESSIONS | Time : 2007/10/10 PM 10:10:33<br>Firmware Version : 1.02, 2006/10/13   |          |       |        |  |
| WIRELESS          | <b>WAN</b>   |          |       |        |  |
| WISH SESSIONS     | Connection Type : DHCP Client<br>QoS Engine : Active<br>Cable Status : connected<br>Network Status : connected<br>Connection Up Time : N/A<br><input type="button" value="Renew"/> <input type="button" value="Release"/><br>MAC Address : 00:19:5B:03:04:E9<br>IP Address : 210.21.33.48<br>Subnet Mask : 255.255.255.248<br>Default Gateway : 210.21.33.254<br>Primary DNS Server : 168.95.1.1<br>Secondary DNS Server : 0.0.0.0 |          |       |        |  |
|                   | <b>LAN</b>   |          |       |        |  |
|                   | MAC Address : 00:19:5B:03:04:E8<br>IP Address : 192.168.0.1<br>Subnet Mask : 255.255.255.0<br>DHCP Server : Enabled  |          |       |        |  |
|                   | <b>WIRELESS LAN</b>  |          |       |        |  |
|                   | Wireless Radio : Enabled<br>WISH : Active<br>MAC Address : 00:19:5B:03:04:E8<br>Network Name (SSID) : dlink<br>Channel : 4<br>Security Mode : Disabled<br>Wi-Fi Protected Setup : Enabled/Not Configured   |          |       |        |  |

The **Setup > Network** page displays the port settings for your camera. If necessary, these ports can be changed if they are already in use by other devices (e.g. in a multiple camera environment).

**Note:** Both the HTTP port and RTSP port are required to be opened for the DCS-942L.

Product: DCS-942L Firmware version: 1.00

---

# D-Link

| DCS-942L  | LIVE VIDEO  | SETUP | MAINTENANCE | STATUS | HELP   |
|---|---|-------|-------------|--------|--|
| <ul style="list-style-type: none"> <li>Setup Wizard</li> <li><b>Network</b></li> <li>Wireless Setup</li> <li>Dynamic DNS</li> <li>Image Setup</li> <li>Audio and Video</li> <li>Time and Date</li> <li>Video Clip</li> <li>Snapshot</li> <li>Motion Detection</li> <li>SD Card</li> <li>Logout</li> </ul> | <div style="background-color: #f4a460; padding: 5px; border: 1px solid #ccc;"> <p><b>NETWORK</b></p> <p>You can configure your LAN and Internet settings here.</p> <p style="text-align: center;"> <input type="button" value="Save Settings"/> <input type="button" value="Don't Save Settings"/> </p> </div> <div style="background-color: #333; color: white; padding: 5px; border: 1px solid #ccc;"> <p><b>LAN SETTINGS</b></p> <p><b>LAN SETTINGS</b></p> <p> <input type="radio"/> Automatic IP Address<br/> <input checked="" type="radio"/> Static IP Address                 </p> <p>IPv4 Address <input type="text" value="192.168.0.20"/></p> <p>Subnet Mask <input type="text" value="255.255.255.0"/></p> <p>Default Gateway (Router) <input type="text" value="192.168.0.1"/></p> <p>Optional Primary DNS <input type="text"/></p> <p>Optional Secondary DNS <input type="text"/></p> <p><input checked="" type="checkbox"/> PPPoE</p> <p>User Name <input type="text"/></p> <p>Password <input type="text"/></p> <p>Confirm Password <input type="text"/></p> <p>Status <span style="float: right;">Disabled</span></p> <p><b>PORT SETTINGS</b></p> <p>HTTP Port <input type="text" value="80"/></p> <p>RTSP Port <input type="text" value="554"/></p> <p><b>UPnP</b></p> <p><input checked="" type="checkbox"/> UPnP</p> <p><input checked="" type="checkbox"/> UPnP Port Forward</p> <p>External HTTP <input type="text" value="80"/></p> <p>External RTSP <input type="text" value="554"/></p> <p><b>Apple</b></p> <p><input checked="" type="checkbox"/> Bonjour</p> <p style="text-align: center;"> <input type="button" value="Save Settings"/> <input type="button" value="Don't Save Settings"/> </p> </div> |       |             |        | <p><b>Helpful Hints..</b></p> <p>Select if you are running a DHCP server on your network and would like an IP address assigned to your camera automatically.</p> <p><b>HTTP Port</b><br/>Allocate the port of camera to allow you to connect via a standard web browser.</p> <p><b>RTSP Port</b><br/>Allocate the port of camera to allow you to connect by using QuickTime or streaming mobile devices.</p> <p><b>UPnP</b><br/>Enable UPnP will allow you to discover camera as an UPnP device in the network.</p> <p><b>Bonjour</b><br/>Enable Bonjour will allow you to discover camera with an Apple computer.</p> |

SURVEILLANCE

## Router Set-Up and Installation

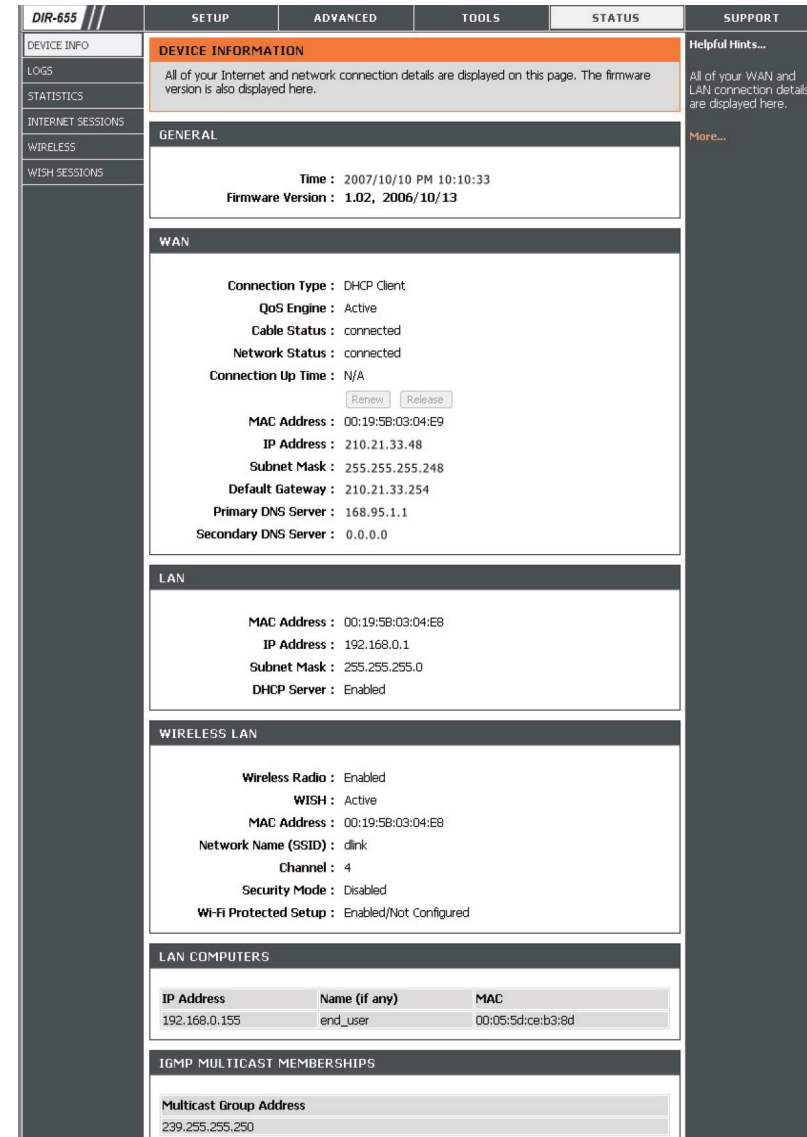
The following steps generally apply to any router that you have on your network. The D-Link DIR-655 is used as an example to clarify the configuration process. Configure the initial settings of the DIR-655 by following the steps outlined in the DIR-655 Quick Installation Guide.

### 3. Access the Router with Your Web Browser

If you have cable or DSL Internet service, you will most likely have a dynamically assigned WAN IP Address. 'Dynamic' means that your router's WAN IP address can change from time to time depending on your ISP. A dynamic WAN IP Address identifies your router on the public network and allows it to access the Internet. To find out what your router's WAN IP Address is, go to the Status menu on your router and locate the WAN information for your router (as shown on the next page). The WAN IP Address will be listed. This will be the address that you will need to type in your Web browser to view your camera over the Internet.

Your WAN IP Address will be listed on the router's

**Status > Device** Info page.



| IP Address    | Name (if any) | MAC               |
|---------------|---------------|-------------------|
| 192.168.0.155 | end_user      | 00:05:5d:ce:b3:8d |

**Note:** Because a dynamic WAN IP can change from time to time depending on your ISP, you may want to obtain a Static IP address from your ISP. A Static IP address is a fixed IP address that will not change over time and will be more convenient for you to use to access your camera from a remote location. The Static IP Address will also allow you to access your camera attached to your router over the Internet.

### 4. Open Virtual Server Ports to Enable Remote Image Viewing

The firewall security features built into the DIR-655 router prevent users from accessing the video from the DCS-942L over the Internet. The router connects to the Internet over a series of numbered ports. The ports normally used by the DCS-942L are blocked from access over the Internet. Therefore, these ports need to be made accessible over the Internet. This is accomplished using the Virtual Server function on the DIR-655 router. The Virtual Server ports used by the camera must be opened through the router for remote access to your camera. Virtual Server is accessed by clicking on the **Advanced** tab of the router screen.

Follow these steps to configure your router's Virtual Server settings:

1. Click **Enabled**.
2. Enter a different name for each entry.
3. Enter your camera's local IP Address (e.g., 192.168.0.120) in the Private IP field.
4. Select TCP for HTTP port, both (TCP and UDP) for RTSP and both (TCP and UDP) for 5556 - 5559 ports.
5. If you are using the default camera port settings, enter 80 into the Public and Private Port section, click **Apply**.
6. Scheduling should be set to Always so that the camera images can be accessed at any time.

Repeat the above steps adding the port 554 to both the Public and Private Port sections. A check mark appearing before the entry name will indicate that the ports are enabled.

**Note:** Some ISPs block access to port 80 and other commonly used Internet ports to conserve bandwidth. Check with your ISP so that you can open the appropriate ports accordingly. If your ISP does not pass traffic on port 80, you will need to change the port the camera uses from 80 to something else, such as 800. Not all routers are the same, so refer to your user manual for specific instructions on how to open ports.

Enter valid ports in the Virtual Server section of your router. Please make sure to check the box next to the camera name on the Virtual Server List to enable your settings.

**D-Link**

DIR-655 // SETUP ADVANCED TOOLS STATUS SUPPORT

**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.

Save Settings Don't Save Settings

**24--VIRTUAL SERVERS LIST**

|                                     | Name     | IP Address    | Port | Traffic Type | Schedule |
|-------------------------------------|----------|---------------|------|--------------|----------|
| <input checked="" type="checkbox"/> | DCS-942L | 192.168.0.120 | 80   | TCP          | Always   |
| <input checked="" type="checkbox"/> | DCS-942L | 192.168.0.120 | 554  | TCP          | Always   |
| <input type="checkbox"/>            |          | 0.0.0.0       | 0    | TCP          | Always   |

**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

# Troubleshooting

This chapter provides solutions to problems that can occur during the installation and operation of the DCS-942L.

Read the following descriptions if you are having problems. (The examples below are illustrated in Windows Vista® and XP. If you have a different operating system, the screenshots on your computer will look similar to the following examples.)

## 1. What is Remote Access? How do I enable it?

Remote Access allows you to access your camera from any PC connected to the Internet through a web browser. This lets you view your camera feed and manage your camera's settings when you're away from home.

To enable Remote Access, simply go through the Camera Installation Wizard included on the Installation CD that came in your package. You can also download the wizard from the following websites:

The image contains two screenshots of the mydlink website. The left screenshot shows the login page with a red box around the 'language English' dropdown menu and an arrow pointing to it from the text '1. Select the language'. The right screenshot shows the support page with a red box around the 'Wizard' section and an arrow pointing to it from the text '3. Support page for selecting Camera to download the online wizard'. A second arrow points from the text '2. Click into the support page' to a red box around a button in the footer of the left screenshot.

After going through the wizard, you should see Remote Status: Enabled on the summary page.

If you see Remote Status: Disabled, make sure that:

...the back LED on your camera is lit solid green

...your Internet connection is working

...your router's LAN & WAN connections are working properly

...your router has UPnP enabled (if your router does not support UPnP, please refer to Appendix A)

...your router can get a public IP

...your router is upgraded to the latest firmware

...you have tried rebooting your router by unplugging it, then plugging it back in

After checking the above items, you can click the Retry button to refresh the summary screen to see if Remote Access has been enabled.

### **2. What can I do if I forget my password?**

If you forget your password, you will need to perform a hard reset of your camera. This process will change all your settings back to the factory defaults.

To reset your camera, please use an unfolded paperclip to press and hold the RESET button for at least 3 seconds while your camera is plugged in.

### **3. In addition to using mydlink.com, is there another way to access my camera remotely over the Internet?**

Yes, you can access your camera over the Internet through the following URL after successfully installing your camera through the Camera Installation Wizard:

`http://[mydlink No.].mydlink.com`

For example, if your camera's mydlink No. was 12345678, you would be able to access your camera remotely by opening your web browser and going to `http://12345678.mydlink.com`

This URL will open a webpage where you will be asked to log in by entering your camera's password. After entering your password, your camera's Live View window will open, and you will be able to configure your camera as well.

### **4. Why does the LED not light up?**



The power supply might be faulty. Confirm that you are using the provided DC 5V power supply for this network camera. Verify that the power supply is correctly connected. If the camera is functioning normally, the LED may have been disabled. See page 39 for information about how to enable the LED.

### **5. Why is the camera's network connection unreliable?**

There might be a problem with the network cable. To confirm that the cables are working, PING the address of a known device on the network. If the cabling is OK and your network is reachable, you should receive a reply similar to the following (...bytes = 32 time = 2 ms).

Another possible problem may be that the network device such as a hub or switch utilized by the Network Camera is not functioning properly. Please confirm the power for the devices are well connected and functioning properly.

### **6. Why does the Network Camera work locally but not remotely?**

This might be caused by the firewall protection. Check the Internet firewall with your system administrator. The firewall may need to have some settings changed in order for the Network Camera to be accessible outside your local LAN. For more information, please refer to the section about installing your camera behind a router.

Make sure that the Network Camera isn't conflicting with any Web server you may have running on your network.

The default router setting might be a possible reason. Check that the configuration of the router settings allow the Network Camera to be accessed outside your local LAN.

### **7. Why does a series of broad vertical white lines appear through out the image?**

It could be that the CMOS sensor (a square panel situated behind the lens that measures the light signals and changes it into a digital format so your computer can present it into an image that you are familiar with) has become overloaded when it has been exposed to bright lights such as direct exposure to sunlight or halogen lights. Reposition the Network Camera into a more shaded area immediately as prolonged exposure to bright lights will damage the CMOS sensor.

### **8. The camera is producing noisy images. How can I solve the problem?**

The video images might be noisy if the Network Camera is used in a very low light environment.

### **9. The images are poor quality, how can I improve the image quality?**

Make sure that your computer's display properties are set to at least 6-bit color. Using 16 or 256 colors on your computer will produce dithering artifacts in the image, making the image look as if it is of poor quality.

The configuration on the Network Camera image display is incorrect. The Web Configuration Video section of the Web management allows you to adjust the related-parameters for improved images such as: brightness, contrast, hue and light frequency. Please refer to the Web Configuration section for detailed information.

### **10. Why are no images available through the Web browser?**

ActiveX might be disabled. If you are viewing the images from Internet Explorer make sure ActiveX has been enabled in the Internet Options menu. You may also need to change the security settings on your browser to allow the ActiveX plug-in to be installed.

If you are using Internet Explorer with a version number lower than 7, then you will need to upgrade your Web browser software in order to view the streaming video transmitted by the Network Camera.

# 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.

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

## What is Wireless?

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

## Why D-Link Wireless?

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

## How does wireless work?

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

## Wireless Local Area Network (WLAN)

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

## Who uses wireless?

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

### Home

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

### Small Office and Home Office

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

## Where is wireless used?

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

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

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

### Tips

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

#### Centralize your router or Access Point

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

#### Eliminate Interference

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

#### Security

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

# Wireless Modes

There are basically two modes of networking:

- **Infrastructure** – All wireless clients will connect to an access point or wireless router.
- **Ad-Hoc** – Directly connecting to another computer, for peer-to-peer communication, using wireless network adapters on each computer, such as two or more DCS-942L wireless network Cardbus adapters.

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

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

# Networking Basics

## Check your IP address

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

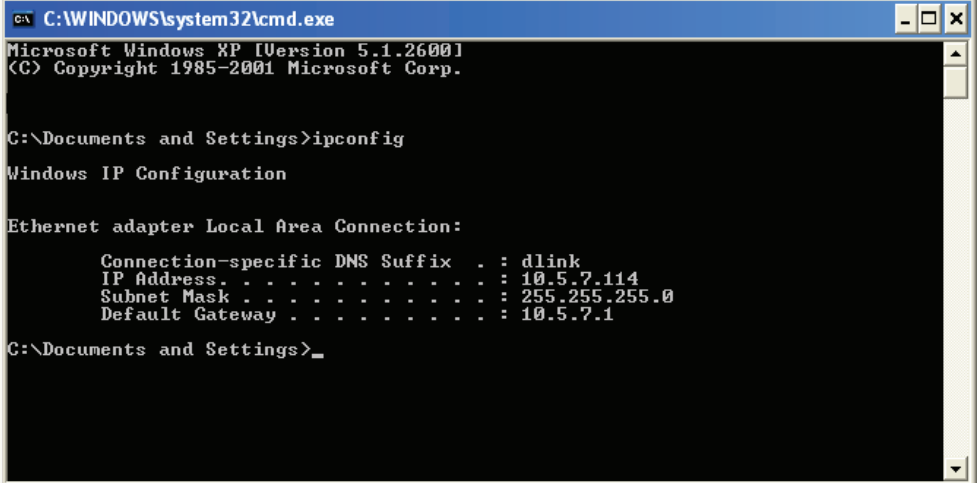
Click on **Start > Run**. In the run box type **cmd** and click **OK**. (Windows® 7/Vista® users type cmd in the Start Search box)

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.

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



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

C:\Documents and Settings>ipconfig

Windows IP Configuration

Ethernet adapter Local Area Connection:

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

C:\Documents and Settings>_
```



## Statically Assign an IP Address

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

### Step 1

Windows® 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**.

### Step 2

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

### Step 3

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

### Step 4

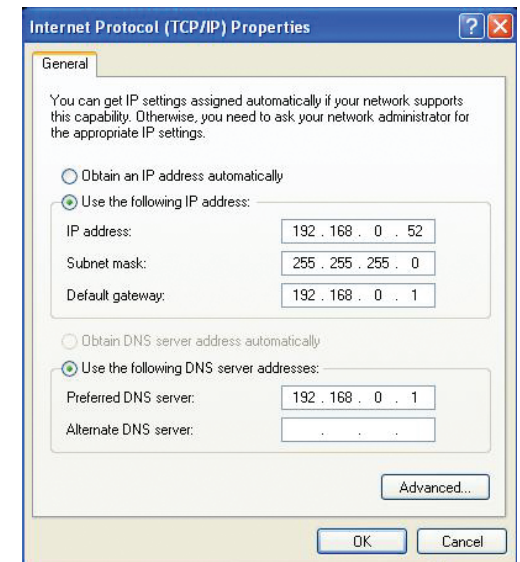
Click **Use the following IP address** and enter an IP address that is on the same subnet as your network or the LAN IP address on your router.

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

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

### Step 5

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



# Technical Specifications

## SYSTEM REQUIREMENTS

- Operating System: Microsoft Windows® XP, Vista®, Windows® 7, Mac OS.
- Internet Explorer 7 or above , Firefox 3.5 or above, Safari 4 or Google Chrome

## • NETWORKING PROTOCOL

- IPV4, ARP, TCP, UDP, ICMP
- DHCP Client
- NTP Client (D-Link)
- DNS Client
- DDNS Client (DynDNS and D-Link)
- SMTP Client
- FTP Client
- HTTP Server
- PPPoE
- UPnP Port Forwarding
- 3GPP (Video only)
- Bonjour

## BUILT-IN NETWORK INTERFACE

- 10/100BASE-TX Fast Ethernet
- 802.11g/n WLAN

## WIRELESS CONNECTIVITY

- 802.11g/n Wireless with WEP/WPA/WPA2 security

## WIRELESS TRANSMIT OUTPUT POWER

- 16 dbm for 11b, 12 dbm for 11g,  
12 dbm for 11n (typical)

## SDRAM

- 128 MB

## FLASH MEMORY

- 16 MB

## RESET BUTTON

- Reset to factory default

## VIDEO CODECS

- H.264
- MPEG-4
- MJPEG

## VIDEO FEATURES

- Adjustable image size and quality
- Time stamp and text overlay
- Flip and Mirror

## RESOLUTION

- 640 x 480 at up to 30 fps
- 320 x 240 at up to 30 fps
- 160 x 112 at up to 30 fps

## LENS

- Focal length: 3.15 mm, F2.8
- Shutter Speed: 1/15, 1/10, 1/7.5, 1/3.75

## SENSOR

- VGA 1/5 inch CMOS Sensor

### MINIMUM ILLUMINATION

- 1 lux @ F2.8

### VIEW ANGLE

- Horizontal: 45.3°
- Vertical: 34.5°
- Diagonal: 54.9°

### IR LED

- 4 IR LEDs (5 Meter distance)

### DIGITAL ZOOM

- Up to 4x

### 3A CONTROL

- AGC (Auto Gain Control)
- AWB (Auto White Balance)
- AES (Auto Electronic Shutter)

### MICROPHONE

- Omni-directional
- Frequency 20 to 20,000 Hz
- S/N ratio: over 58 dB

### AUDIO

- ADPCM

### SD CARD SLOT

- Micro SD card

### PIR SENSOR

- Built-in Piezoelectricity Passive Infrared sensor for motion detection

### POWER

- Input: 100-240 V AC, 50/60 Hz
- Output: 5 V DC, 1.2 A
- External AC-to-DC switching power adapter

### DIMENSIONS (W X D X H)

- Including the bracket and stand:  
65.8 x 65 x 126 mm
- Camera only:  
27.2 x 60 x 96 mm

### WEIGHT

- 76.9 g (without bracket and stand)

### MAX POWER CONSUMPTION

- 2 W

### OPERATION TEMPERATURE

- 0 °C to 40 °C (32 °F to 104 °F)

### STORAGE TEMPERATURE

- -20 °C to 70 °C (-4 °F to 158 °F)

### HUMIDITY

- 20-80% RH non-condensing

### EMISSION (EMI), SAFETY & OTHER CERTIFICATIONS

- FCC Class B
- IC
- C-Tick
- CE

# Contacting Technical Support

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

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

- Model number of the product (e.g. DCS-942L)
- Hardware Revision (located on the label on the bottom of the Network Camera (e.g. rev A1))
- Serial Number (s/n number located on the label on the bottom of the Network Camera).

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

## For customers within the United States:

**Phone Support:**

(877) 453-5465

**Internet Support:**

<http://support.dlink.com>

## For customers within Canada:

**Phone Support:**

(800) 361-5265

**Internet Support:**

<http://support.dlink.ca>

# Warranty

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

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

## Limited Warranty:

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

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

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

### **Limited Software Warranty:**

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

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

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

### **Submitting A Claim:**

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

- The customer must submit with the product as part of the claim a written description of the Hardware defect or Software nonconformance in sufficient detail to allow D-Link to confirm the same, along with proof of purchase of the product (such as a copy of the dated purchase invoice for the product) if the product is not registered.
- The customer must obtain a Case ID Number from D-Link Technical Support (USA 1-877-453-5465 or Canada 1-800-361-5265), who will attempt to assist the customer in resolving any suspected defects with the product. If the product is considered defective, the customer must obtain a Return Material Authorization (“RMA”) number by completing the RMA form. Enter the assigned Case ID Number at <https://rma.dlink.com/> (USA only) or <https://rma.dlink.ca> (Canada only).

- After an RMA number is issued, the defective product must be packaged securely in the original or other suitable shipping package to ensure that it will not be damaged in transit, and the RMA number must be prominently marked on the outside of the package. Do not include any manuals or accessories in the shipping package. D-Link will only replace the defective portion of the product and will not ship back any accessories.
- The customer is responsible for all in-bound shipping charges to D-Link. No Cash on Delivery (“COD”) is allowed. Products sent COD will either be rejected by D-Link or become the property of D-Link. Products shall be fully insured by the customer and shipped to D-Link Systems, Inc.
- **USA residents** send to 17595 Mt. Herrmann, Fountain Valley, CA 92708. D-Link will not be held responsible for any packages that are lost in transit to D-Link. The repaired or replaced packages will be shipped to the customer via UPS Ground or any common carrier selected by D-Link. Return shipping charges shall be prepaid by D-Link if you use an address in the United States, otherwise we will ship the product to you freight collect. Expedited shipping is available upon request and provided shipping charges are prepaid by the customer. D-Link may reject or return any product that is not packaged and shipped in strict compliance with the foregoing requirements, or for which an RMA number is not visible from the outside of the package. The product owner agrees to pay D-Link’s reasonable handling and return shipping charges for any product that is not packaged and shipped in accordance with the foregoing requirements, or that is determined by D-Link not to be defective or non-conforming.
- **Canadian residents** send to D-Link Networks, Inc., 2525 Meadowvale Boulevard Mississauga, Ontario, L5N 5S2 Canada. D-Link will not be held responsible for any packages that are lost in transit to D-Link. The repaired or replaced packages will be shipped to the customer via Purolator Canada or any common carrier selected by D-Link. Return shipping charges shall be prepaid by D-Link if you use an address in Canada, otherwise we will ship the product to you freight collect. Expedited shipping is available upon request and provided shipping charges are prepaid by the customer. D-Link may reject or return any product that is not packaged and shipped in strict compliance with the foregoing requirements, or for which an RMA number is not visible from the outside of the package. The product owner agrees to pay D-Link’s reasonable handling and return shipping charges for any product that is not packaged and shipped in accordance with the foregoing requirements, or that is determined by D-Link not to be defective or non-conforming. RMA phone number: 1-800-361-5265 Hours of Operation: Monday-Friday, 9:00AM – 9:00PM EST

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

The Limited Warranty provided herein by D-Link does not cover:

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

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

**Disclaimer of Other Warranties:**

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

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

**Limitation of Liability:**

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

**Governing Law:**

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

**Trademarks:**

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



### **Copyright Statement:**

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

Copyright ©2011 by D-Link Corporation/D-Link Systems, Inc. All rights reserved.

### **CE Mark Warning:**

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

### **FCC Statement:**

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

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

### **FCC Caution:**

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

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.

If this device is going to be operated in 5.15 ~ 5.25GHz frequency range, then it is restricted in indoor environment only.

### **IMPORTANT NOTICE:**

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

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

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

#### **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.

### **IMPORTANT NOTE:**

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

This equipment complies with Canada radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 20cm between the radiator and your body.

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

# Registration

Register your product online at [registration.dlink.com](http://registration.dlink.com)



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

Version 1.0  
July 21, 2011

## 警語

經型式認證合格之低功率射頻電機，非經許可，公司，商號或使用者均不得擅自變更頻率，加大功率或變更原設計之特性及功能

低功率射頻電機之使用不得影響飛航影響安全及干擾合法通信，經發現有干擾現象時，應立即停用，並改善至無干擾時方得繼續使用

前項合法通信，指一電信法規定作業之無線電通信低功率射頻電機需忍受合法通信或工業，科學及醫療用電波輻射性電機設備之干擾

# FCC Notices

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.

CAUTION: Change or modification not expressly approved by the party responsible for compliance could void the user's authority to operate this equipment.

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 or more of the following measures:

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

## CAUTION:

Any changes or modifications not expressly approved by the grantee of this device could void the user's authority to operate the equipment.

## RF exposure warning

This equipment must be installed and operated in accordance with provided instructions and the antenna(s) used for this transmitter must be installed to provide a separation distance of at least 20 cm from all persons and must not be co-located or operating in conjunction with any other antenna or transmitter. End-users and installers must be provide with antenna installation instructions and transmitter operating conditions for satisfying RF exposure compliance."

# **Canada Notices**

## **Industry Canada regulatory information**

**Operation is subject to the following two conditions: (1) this device may not cause interference, and (2) this device must accept any interference, including interference that may cause undesired operation of the device.**

**The user is cautioned that this device should be used only as specified within this manual to meet RF exposure requirements. Use of this device in a manner inconsistent with this manual could lead to excessive RF exposure conditions.**