DAVID SHONKA
Acting General Counsel

LAURA D. BERGER (FL Bar No. 11762)
Federal Trade Commission
901 Market Street, Suite 570
San Francisco, CA 94103
P: (202) 326-2471/F: (415) 848-5184
lberger@ftc.gov;

KEVIN H. MORIARTY (DC Bar No. 975904)
CATHLIN TULLY (NY Bar)
Federal Trade Commission
600 Pennsylvania Ave N.W.
Washington, DC 20580
P: (202) 326-3644/F: (202) 326-3062
kmoriarty@ftc.gov; ctully@ftc.gov

Attorneys for Plaintiff Federal Trade Commission

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA
SAN FRANCISCO DIVISION

FEDERAL TRADE COMMISSION, Plaintiff, v. D-LINK CORPORATION and D-LINK SYSTEMS, INC., corporations, Defendants.	**Case No. _____** **COMPLAINT FOR PERMANENT INJUNCTION AND OTHER EQUITABLE RELIEF**

1. Plaintiff, the Federal Trade Commission ("FTC"), for its Complaint, brings this action under Section 13(b) of the Federal Trade Commission Act ("FTC Act"), 15 U.S.C.

REDACTED VERSION OF DOCUMENT SOUGHT TO BE SEALED

§ 53(b), to obtain permanent injunctive relief and other equitable relief against Defendants for engaging in unfair or deceptive acts or practices in violation of Section 5(a) of the FTC Act, 15 U.S.C. § 45(a), in connection with Defendants' failure to take reasonable steps to secure the routers and Internet-protocol cameras they designed for, marketed, and sold to United States consumers.

JURISDICTION AND VENUE

2. This Court has subject matter jurisdiction pursuant to 28 U.S.C. §§ 1331, 1337(a), and 1345, and 15 U.S.C. §§ 45(a) and 53(b).

3. Venue in the Northern District of California is proper under 28 U.S.C. § 1391(b) and (c) and 15 U.S.C. § 53(b).

PLAINTIFF

4. The FTC is an independent agency of the United States Government created by statute. 15 U.S.C. §§ 41-58. The FTC enforces Section 5(a) of the FTC Act, 15 U.S.C. § 45(a), which prohibits unfair or deceptive acts or practices in or affecting commerce.

5. The FTC is authorized to initiate federal district court proceedings, by its own attorneys, to enjoin violations of the FTC Act and to secure such other equitable relief as may be appropriate in each case. 15 U.S.C. §§ 53(b), 56(a)(2)(A).

DEFENDANTS

6. Defendant D-Link Corporation ("D-Link") is a Taiwanese corporation with its principal office or place of business at No. 289, Xinhu 3rd Rd., Neihu District, Taipei City, Taiwan 114. D-Link transacts or has transacted business in this district and throughout the United States. At all times material to this Complaint, acting alone or in concert with others, D-Link purposefully directed its activities to the United States by designing, developing, marketing, and manufacturing routers, Internet-protocol ("IP") cameras, and related software and services, intended for use by consumers throughout the United States.

7. Defendant D-Link Systems, Inc., ("DLS") is a California corporation with its principal office or place of business at 17595 Mt. Herrmann St., Fountain Valley, California

REDACTED VERSION OF DOCUMENT SOUGHT TO BE SEALED

92708. DLS transacts or has transacted business in this district and throughout the United States. At all times material to this Complaint, acting alone or in concert with others, DLS has advertised, marketed, distributed, or sold routers, IP cameras, and related software and services, intended for use by consumers throughout the United States. The Chairman of DLS's Board of Directors has served as D-Link's Chief Executive Officer and the two entities have coordinated closely regarding the security of Defendants' routers and IP cameras.

8. The FTC's claims against D-Link and DLS arise from or relate to Defendants' acts or practices aimed at or taking place in the United States.

COMMERCE

9. At all times material to this Complaint, Defendants have maintained a substantial course of trade in or affecting commerce, as "commerce" is defined in Section 4 of the FTC Act, 15 U.S.C. § 44.

DEFENDANTS' BUSINESS PRACTICES

10. D-Link is a hardware device manufacturer that designs, develops, markets, and manufactures networking devices, including devices with core functions that relate to security, such as consumer routers and IP cameras. D-Link designs, develops, and manufactures these products, their marketing materials, and related software and services for distribution or sale to United States consumers through its subsidiary, DLS. [redacted] When releasing new software for such routers and IP cameras, D-Link uses a digital signature issued in its name, known as a "private key," to sign the software, in order to assure entities, such as browsers and operating systems, that the software comes from an authentic or "trusted" source and is not malware.

11. DLS is a subsidiary of D-Link and is nearly 98% owned by D-Link and its holding company, D-Link Holding Company, Ltd. DLS provides marketing and after-sale services integral to D-Link's operations, including by marketing and acting as the sole

distributor of Defendants' routers and IP cameras throughout the United States. [redacted] Among other services, DLS acts as the primary point-of-contact for problems that United States consumers have with Defendants' routers, IP cameras, or related software and services; [redacted] DLS also assists in notifying United States consumers about the availability of security updates through means such as DLS's websites.

12. Defendants have provided software applications that enable users to access their routers and IP cameras from a mobile device ("mobile apps"), including a free "mydlink Lite" mobile app. Defendants designed the mydlink Lite app to require the user to enter a user name and password ("login credentials") the first occasion that a user employs the app on a particular mobile device. After that first occasion, the app stores the user's login credentials on that mobile device, keeping the user logged into the mobile app on that device.

DEFENDANTS' ROUTERS

13. Defendants' routers, like other routers, operate to forward data packets along a network. In addition to routing network traffic, they typically play a key role in securing consumers' home networks, functioning as a hardware firewall for the local network, and acting as the first line of defense in protecting consumer devices on the local network, such as computers, smartphones, IP cameras, and other connected appliances, against malicious incoming traffic from the Internet.

DEFENDANTS' IP CAMERAS

14. Defendants' IP cameras, akin to many such IP cameras, play a key security role for consumers, by enabling consumers to monitor private areas of their homes or businesses, to detect any events that may place the property or its occupants at risk. In many instances, Defendants offer them as a means to monitor the security of a home while consumers are away,

REDACTED VERSION OF DOCUMENT SOUGHT TO BE SEALED

or to monitor activities within the household, including the activities of young children, while a consumer is at home. Consumers seeking to monitor the security of their homes or the safety of young children may access live video and audio feeds ("live feeds") from their cameras over the Internet, using a mobile device or other computer.

DEFENDANTS' SECURITY FAILURES

15. Defendants have failed to take reasonable steps to protect their routers and IP cameras from widely known and reasonably foreseeable risks of unauthorized access, including by failing to protect against flaws which the Open Web Application Security Project has ranked among the most critical and widespread web application vulnerabilities since at least 2007. Among other things:

a. Defendants repeatedly have failed to take reasonable software testing and remediation measures to protect their routers and IP cameras against well-known and easily preventable software security flaws, such as "hard-coded" user credentials and other backdoors, and command injection flaws, which would allow remote attackers to gain control of consumers' devices;

b. Defendant D-Link has failed to take reasonable steps to maintain the confidentiality of the private key that Defendant D-Link used to sign Defendants' software, including by failing to adequately restrict, monitor, and oversee handling of the key, resulting in the exposure of the private key on a public website for approximately six months; and

c. Defendants have failed to use free software, available since at least 2008, to secure users' mobile app login credentials, and instead have stored those credentials in clear, readable text on a user's mobile device.

THOUSANDS OF CONSUMERS AT RISK

16. As a result of Defendants' failures, thousands of Defendants' routers and cameras have been vulnerable to attacks that subject consumers' sensitive personal information and local networks to a significant risk of unauthorized access. In fact, the press

has reported that Defendants' routers and cameras have been vulnerable to a range of such attacks and have been compromised by attackers, including by being made part of large scale networks of computers infected by malicious software, known as "botnets."

17. The risk that attackers would exploit these vulnerabilities to harm consumers was significant. In many instances, remote attackers could take simple steps, using widely available tools, to locate and exploit Defendants' devices, which were widely known to be vulnerable. For example, remote attackers could search for vulnerable devices over the Internet and obtain their IP addresses using readily available tools, such as a popular search engine that can locate devices running particular software versions or operating in particular locations. Alternatively, attackers could use readily accessible scanning tools to identify vulnerable devices operating in particular areas or on particular networks. In many instances, an attacker could then take simple steps to exploit vulnerabilities in Defendants' routers and IP cameras, impacting not only consumers who purchased these devices, but also other consumers, who access the Internet in public or private locations served by the routers or who visit locations under the IP cameras' surveillance.

18. By creating these vulnerabilities, Defendants put consumers at significant risk of harm in a variety of ways. An attacker could compromise a consumer's router, thereby obtaining unauthorized access to consumers' sensitive personal information. For example, using a compromised router, an attacker could re-direct consumers seeking a legitimate financial site to a spoofed website, where they would unwittingly provide the attacker with sensitive financial account information. Alternatively, using a compromised router, an attacker could obtain consumers' tax returns or other files stored on the router's attached storage device or could use the router to attack other devices on the local network, such as computers, smartphones, IP cameras, or connected appliances. Similarly, by exploiting the vulnerabilities described in Paragraph 15, an attacker could compromise a consumer's IP camera, thereby monitoring consumers' whereabouts to target them for theft or other criminal activity or to observe and record over the Internet their personal activities and conversations or those of their young children. In many instances, attackers could carry out such exploits covertly, such that

REDACTED VERSION OF DOCUMENT SOUGHT TO BE SEALED

consumers would have no reason to know that an attack was ongoing. Finally, during the time Defendant D-Link's private key was available on a public website, consumers seeking to download legitimate software from Defendants were at significant risk of downloading malware, signed by malicious actors using D-Link's private key.

DEFENDANTS' SECURITY STATEMENTS

19. Defendants have disseminated or caused to be disseminated to consumers statements regarding the security of their products, including their routers and IP cameras.

SECURITY EVENT RESPONSE POLICY

20. From approximately December 2013 until early September 2015, after highly-publicized security flaws were found to affect many of its products, Defendant DLS posted a Security Event Response Policy on its product support webpage, **http://support.dlink.com/securityadvisories.aspx**, in the general form of Exhibit 1. Within its Security Event Response Policy, under a bolded heading "D-Link's commitment to Product Security," Defendant DLS stated:

> D-Link prohibits at all times, including during product development by D-Link or its affiliates, any intentional product features or behaviors which allow unauthorized access to the device or network, including but not limited to undocumented account credentials, covert communication channels, 'backdoors' or undocumented traffic diversion. All such features and behaviors are considered serious and will be given the highest priority.

PROMOTIONAL CLAIMS

21. Defendants highlight their routers' security features in a wide range of materials available on Defendant DLS's website, including user manuals and promotional brochures, which describe these features alongside language that specifically references the device's "security". Such materials include, but are not limited to, brochures in the general form of Exhibits 2-5, which state:

a. Under a bolded, italicized, all-capitalized heading, "***EASY TO SECURE***," that the router:

> supports the latest wireless security features to help prevent unauthorized access, be it from over a wireless network or from the Internet. Support for WPA™ and WPA2™ standards ensure that you will be able to use the best possible encryption, regardless of your client devices. In addition [the router] utilizes dual active firewalls (SPI and NAT) to prevent potential attacks from across the Internet.
>
> Delivering great wireless performance, network security and coverage [the router] is ideal for upgrading your existing wireless network. (*See* PX 2).

b. Under a bolded, italicized, all-capitalized heading, "***ADVANCED NETWORK SECURITY***," that the router:

> ensures a secure Wi-Fi network through the use of WPA/WPA2 wireless encryption. Simply press the WPS button to quickly establish a secure connection to new devices. The [router] also utilizes dual-active firewalls (SPI and NAT) to prevent potential attacks and intrusions from across the Internet. (*See* PX 3).

c. Under a bolded heading, "**Advanced Network Security**," that the router:

> supports the latest wireless security features to help prevent unauthorized access, be it from over a wireless network or from the Internet. Support for WPA™ and WPA2™ standards ensure that you will be able to use the best possible encryption method. In addition, this [router] utilizes Stateful Packet Inspection Firewalls (SPI) to help prevent potential attacks from across the Internet. (*See* PX 4).

d. Under a heading "128-bit Security Encryption," that the router:

> protects your network with 128-bit AES data security encryption – the same technology used in E-commerce or online banking. Create your own network

> name and password or put it at the tip of your fingers with 'Push Button Security' standard on every Amplifi device. With hassle-free plug and play installation, and advanced Wi-Fi protected setup, the [router] is not only one of the fastest routers available, its [sic] also one of the safest. (*See* PX 5).

22. Defendants highlight the security of their IP cameras in a wide range of materials available on Defendant DLS's website, including user manuals and promotional brochures, which describe these features alongside language that specifically references the device's "security". Such materials include, but are not limited to, brochures in the general form of Exhibit 6, which display the word "SECURITY" in large, capital letters, in a vividly-colored footer across the bottom of each page. (*See* PX 6). In addition, Defendants have designed their IP camera packaging, including in the general form of Exhibit 7, to display security-related terms. Such terms include the words "secure connection," next to a lock icon, among the product features listed on the side of the box (*see* PX 7).

INTERACTIVE SECURITY FEATURES

23. Defendants' routers offer numerous security features that Defendants present alongside instructions that specifically reference the device's "security". In particular, in many instances, to begin using the router, users must access a graphical user interface (hereinafter, "Defendants' router GUI"), in the general form of Exhibits 8 and 9, which includes instructions, such as:

a. "To secure your new networking device, please set and verify a password below" (*see* PX 8); and

b. "It is highly recommended that you create a password to keep your router secure." (*See* PX 9).

24. Defendants' IP cameras offer numerous security features that Defendants present alongside language that specifically references the device's "security". In particular, to begin using the camera, in many instances, users must access a GUI (hereinafter "Defendants' IP camera GUI"), in the general form of Exhibits 10 and 11, which include language, such as:

REDACTED VERSION OF DOCUMENT SOUGHT TO BE SEALED

a. instructions to "Set up an Admin ID and Password" or "enter a password" in order "to secure your camera" (*see* PX 10); and

b. security-related banners, including, but not limited to, the words "SECURICAM Network," alongside a lock icon, across the top of the GUI (*see* PX 11).

D-LINK DIRECTS ITS PRACTICES TO U.S. CONSUMERS

25. [redacted]

VIOLATIONS OF THE FTC ACT

26. Section 5(a) of the FTC Act, 15 U.S.C. § 45(a), prohibits "unfair or deceptive acts or practices in or affecting commerce."

27. Acts or practices are unfair under Section 5 of the FTC Act if they cause or are likely to cause substantial injury to consumers that consumers cannot reasonably avoid themselves and that is not outweighed by countervailing benefits to consumers or competition. 15 U.S.C. § 45(n).

COUNT I

Unfairness

28. In numerous instances, Defendants have failed to take reasonable steps to secure the software for their routers and IP cameras, which Defendants offered to consumers, respectively, for the purpose of protecting their local networks and accessing sensitive personal information.

29. Defendants' practices caused, or are likely to cause, substantial injury to consumers in the United States that is not outweighed by countervailing benefits to consumers or competition and is not reasonably avoidable by consumers.

30. Therefore, Defendants' acts and practices as described in Paragraphs 15-18 of this Complaint constitute unfair acts or practices in or affecting commerce, in violation of Section 5 of the FTC Act, 15 U.S.C. §§ 45(a) and 45(n).

COUNT II

Security Event Response Policy Misrepresentation

31. Through the means described in Paragraph 20, Defendant DLS has represented, directly or indirectly, expressly or by implication, that Defendants took reasonable steps to secure their products from unauthorized access.

32. In truth and in fact, as described in Paragraphs 15-18, Defendants did not take reasonable steps to secure their products from unauthorized access.

33. Therefore, the making of the representation set forth in Paragraph 31 of this Complaint constitutes a deceptive act or practice, in or affecting commerce in violation of Section 5(a) of the FTC Act, 15 U.S.C. § 45(a).

COUNT III

Router Promotional Misrepresentations

34. Through the means described in Paragraph 21, Defendants have represented, directly or indirectly, expressly or by implication, that the routers described by these claims were secure from unauthorized access.

35. In truth and in fact, as described in Paragraphs 15-18, Defendants' routers were not secure from unauthorized access and control.

36. Therefore, the making of the representation set forth in Paragraph 34 of this Complaint constitutes a deceptive act or practice, in or affecting commerce in violation of Section 5(a) of the FTC Act, 15 U.S.C. § 45(a).

COUNT IV

IP Camera Promotional Misrepresentations

37. Through the means described in Paragraph 22, Defendants have represented, directly or indirectly, expressly or by implication, that the IP cameras described by these claims were secure from unauthorized access and control.

38. In truth and in fact, as described in Paragraphs 15-18, Defendants' IP cameras were not secure from unauthorized access and control.

39. Therefore, the making of the representation set forth in Paragraph 37 of this Complaint constitutes a deceptive act or practice, in or affecting commerce in violation of Section 5(a) of the FTC Act, 15 U.S.C. § 45(a).

COUNT V

Router GUI Misrepresentations

40. Through the means described in Paragraph 23, Defendants have represented, directly or indirectly, expressly or by implication, that the routers described by these claims were secure from unauthorized access.

41. In truth and in fact, as described in Paragraphs 15-18, Defendants' routers were not secure from unauthorized access and control.

42. Therefore, the making of the representation set forth in Paragraph 40 of this Complaint constitutes a deceptive act or practice, in or affecting commerce in violation of Section 5(a) of the FTC Act, 15 U.S.C. § 45(a).

COUNT VI

IP Camera GUI Misrepresentations

43. Through the means described in Paragraph 24, Defendants have represented, directly or indirectly, expressly or by implication, that the IP cameras described by these claims were secure from unauthorized access and control.

44. In truth and in fact, as described in Paragraphs 15-18, Defendants' IP cameras were not secure from unauthorized access and control.

45. Therefore, the making of the representation set forth in Paragraph 43 of this Complaint constitutes a deceptive act or practice, in or affecting commerce in violation of Section 5(a) of the FTC Act, 15 U.S.C. § 45(a).

CONSUMER INJURY

46. Consumers are likely to suffer substantial injury as a result of Defendants' violations of the FTC Act. Absent injunctive relief by this Court, Defendants are likely to injure consumers and harm the public interest.

THIS COURT'S POWER TO GRANT RELIEF

47. Section 13(b) of the FTC Act, 15 U.S.C. § 53(b), empowers this Court to grant injunctive and such other relief as the Court may deem appropriate to halt and redress violations of any provision of law enforced by the FTC.

PRAYER FOR RELIEF

Wherefore, Plaintiff FTC, pursuant to Section 13(b) of the FTC Act, 15 U.S.C. § 53(b), and the Court's own equitable powers, requests that the Court:

A. Enter a permanent injunction to prevent future violations of the FTC Act by Defendants; and

B. Award Plaintiff the costs of bringing this action, as well as such other and additional relief as the Court may determine to be just and proper.

Respectfully submitted,

DAVID SHONKA
Acting General Counsel

Dated: January 5, 2017

/s/ Cathlin Tully
LAURA D. BERGER
KEVIN H. MORIARTY
CATHLIN TULLY

Attorneys for Plaintiff
FEDERAL TRADE COMMISSION

REDACTED VERSION OF DOCUMENT SOUGHT TO BE SEALED

PX 1

INTERNET ARCHIVE WayBackMachine
http://support.dlink.com/SecurityAdvisories.aspx
Go
19 captures
11 Nov 13 - 8 Sep 15
MAY SEP OCT
2014 8 2015 2016
Close
Help

D-Link
Building Networks for People

PX 1

Security
Advisories

Consumer Business

Security Event Response Policy

Security Advisory List | Report a Potential Vulnerability | Security Event Response Policy

In case of a security vulnerability event emergency, proceed directly to "Suspected Security Vulnerability Support and Reporting."

Summary of Policy

Summary of Policy

Product Security Event Response

Suspected Security Vulnerability Support and Reporting
Security Event Response Team Support Information
General Security-Related Questions
Customer Care Contact Points

Tracking Security Vulnerability Information from D-Link
Direct Internet Contact

Public Relations Contacts for Security Vulnerability Information
Public Relations Contacts

D-Link's Commitment to Product Security

Product Security Event Response

D-Link's response to security issues for D-Link products is a distributed responsibility among all of its regional business units. Coordinated security response is managed by our security event response teams located D-Link US, D-Link Europe, and D-Link Corporate Headquarters. The D-Link security event response team is the global team that is responsible for the gathering, investigation, and public reporting of potential security vulnerability issues related to D-Link products. With our global team, our intent is to work with and respond as quickly as possible to D-Link customers, vendors, partners, consultants, security researchers, industry organizations, and others to identify potential security issues in our products and network deployments.

Suspected Security Vulnerability Support and Reporting

It is highly recommended that anyone suspecting a product security issue contact our security event response team. D-Link encourages reports from any source, including but not limited to customers, vendors, partners, independent researchers, industry organizations, and other sources. If contact is made through other channels, methods, regional offices, customer care there is a strong risk issues may not get the urgency necessary for these reports. The team uses English as a common language but we accept local languages and will translate as needed.

Security Event Response Team Support Information

E-mail: security@dlink.com
Hours: Support requests received via e-mail are monitored 24/7/365 and are not subject to business and Customer Care hours.

Recognized Event Reports are listed on http://securityadvisories.dlink.com/security/

Reports are typically acknowledged within 24 hours on the above site. Plan of actions are typically offered with in 48 hours of a recognition and posting of a report. All communication to the public will be done thru the report posted above.

General Security-Related Questions

The D-Link Customer Care center can provide assistance for all technical and configuration issues related to security matters, as well as with non-sensitive security events including security bug fixes and software upgrades.

Customer Care Contact Points

Phone:

- For US Consumer Retail Products +1 (877) 453-5465 / For US Business Products +1 (877) 354-6555 – Business Hours
- For EU Products 0871 873 3000* 9.00 am - 7.00 pm, M- F
- For Canadian Products 1-800-361-5265 English (9am-8pm EST) & French (12pm-9pm EST) M-F
- For All Other Regions please contact D-Link International @ this website link

E-mail: support@dlink.com
Web: Chat, E-Mail, Call Numbers
Hours: 24 hours a day, 7 days a week for email and web support

Tracking Security Vulnerability Information from D-Link

To stay updated with the latest security vulnerability information from D-Link, please refer to the following:

Direct Internet Contact

Web: securityadvisories.dlink.com/security
E-mail: Announcement-Service Q2'2014
RSS: RSS Feed Q2'2014
Twitter: Twitter Feed Q2'2014

Public Relations Contacts for Security Vulnerability Information

D-Link public relations contacts for security vulnerability information are as follows:

Public Relations Contacts

United States Contact: Daniel Kelley
E-mail: Daniel Kelley <dan.kelley@dlink.com>

European Union Contact: Mary Harrison
E-Mail: mary.harrison@dlink.com

Canada Contact: Please Submit by Web
Web Contact: Link

All Others Regions: Contact: Dmitri Detwyler
E-mail: Dmitri_Detwyler@dlink.com.tw
Additional Public Relations: press@dlink.com

D-Link's Commitment to Product Security

D-Link prohibits at all times, including during product development by D-Link or its affiliates, any intentional product features or behaviors which allow unauthorized access to the device or network, including but not limited to undocumented account credentials, covert communication channels, "backdoors" or undocumented traffic diversion. All such features and behaviors are considered serious and will be given the highest priority.

D-Link reserves the right to change or update this document without notice at any time. All of the information, instructions and recommendations in this document are offered on a strictly "as is" basis. This material is offered without any warranty: expressed or implied. D-Link shall not be liable for any direct, indirect, incidental or consequential damages that may result from anything that is contained in this document or action that is a result thereof. It is up to the reader to determine the suitability of any directions or information in this document.

PX 2

D-Link®

N 300

WIRELESS N 300 ROUTER

Powerful Wireless N 300 technology outperforms Wireless G[1]

Parental controls to supervise Internet activity

Built-in QoS engine enhances Internet experience

UPGRADE YOUR NETWORK

The D-Link Wireless N 300 Router (DIR-615) provides a better wireless signal for your network than previous-generation Wireless G technology. Upgrading your home network to Wireless N 300 provides an excellent solution for sharing an Internet connection and files such as video, music, photos, and documents. D-Link Wireless N 300 products use Intelligent Antenna technology to transmit multiple streams of data which enables you to receive wireless signals in the farthest corners of your home. Not only does the D-Link Wireless N 300 technology extend your wireless range, it also works with previous-generation wireless devices. The DIR-615 also includes QoS (Quality of Service) Prioritization Technology that analyzes and separates multiple data streams based on sensitivity to delay, enabling multiple applications to stream smoothly across your network[2].

EASY TO SET UP

The D-Link Quick Router Setup Wizard quickly configures your new Wireless N 300 Router to get you up and running in minutes. Our Setup Wizard walks you step by step through the installation process to configure your Internet connection, wireless network settings and security, and everything else you need to get your network up and running so that you don't have to be a networking expert to get it set up.

EASY TO SECURE

The DIR-615 supports the latest wireless security features to help prevent unauthorized access, be it from over a wireless network or from the Internet. Support for WPA™ and WPA2™ standards ensure that you will be able to use the best possible encryption, regardless of your client devices. In addition, the Wireless N 300 Router utilizes dual active firewalls (SPI and NAT) to prevent potential attacks from across the Internet.

Delivering great wireless performance, network security and coverage, the D-Link Wireless N 300 Router (DIR-615) is ideal for upgrading your existing wireless home network.

D-Link®

DIR-615

WHAT THIS PRODUCT DOES

Create a wireless network to share high-speed Internet access with computers, game consoles, and media players from greater distances around your home.

BENEFITS OF A WIRELESS N 300 ROUTER

This Wireless N 300 Router uses powerful 802.11n technology with multiple intelligent antennas to maximize the speed and range of your wireless signal to significantly outperform previous-generation Wireless G MIMO devices[1]. The antennas on the Wireless N 300 Router make use of your home's environment by bouncing multiple wireless signals off walls and ceilings to work around obstructions and help eliminate dead spots.

YOUR NETWORK SETUP

TECHNICAL SPECIFICATIONS

STANDARDS
+ IEEE 802.11n
+ IEEE 802.11g
+ IEEE 802.3
+ IEEE 802.3u

DEVICE INTERFACE
+ 4 10/100 LAN Ports
+ 1 10/100 WAN Port

SECURITY
+ Wi-Fi Protected Access (WPA, WPA2)[2]

ADVANCED FIREWALL FEATURES
+ Network Address Translation (NAT)
+ Stateful Packet Inspection (SPI)
+ VPN Pass-through / Multi-sessions PPTP / L2TP / IPSec

DEVICE MANAGEMENT
+ Internet Explorer® v7 or Later; Mozilla Firefox® v3.0 or Later; or other Java-enabled Browsers

LEDS
+ Power
+ WLAN (Wireless Connection)
+ LAN (10/100)
+ Internet Status

CERTIFICATIONS
+ FCC Class B
+ IC
+ Wi-Fi®

DIMENSIONS
+ Item (WxDxH): 7.8" x 5" x 1.2" (198.1mm x 127mm x 30.5mm)
+ Packaging (WxDxH): 10.5" x 2.6" x 8.1" (276.9mm x 66mm x 205.8mm)

WEIGHT
+ Item: 0.6 lbs (272.2 grams)
+ Packaging: 1.4 lbs (635 grams)

WARRANTY
+ 1-Year Limited[3]

RECOMMENDED SYSTEM REQUIREMENTS
For Optimal Wireless Performance, use with:
+ Wireless N 300 Adapter (DWA-130)

MINIMUM SYSTEM REQUIREMENTS
Computer with:
+ Windows® 7[4], Windows Vista®[4], Windows® XP SP3, or Mac OS® X (v10.4)[5]
+ Internet Explorer v7 or Mozilla Firefox v3.0
+ CD-ROM Drive
+ Network Interface Card

For Internet Access:
+ Cable or DSL Modem
+ Subscription with an Internet Service Provider (ISP)

PACKAGE CONTENTS
+ Wireless N 300 Router
+ CAT5Ethernet Cable
+ Power Adapter
+ CD-ROM[6] with
  - Installation Wizard
  - Product Documentation

[1] Maximum wireless signal rate derived from IEEE Standard 802.11 specifications. Actual data throughput will vary. Network conditions and environmental factors, including volume of network traffic, building materials and construction, and network overhead, lower actual data throughput rate. Environmental factors will adversely affect wireless signal range. Wireless range and speed rates are D-Link RELATIVE performance measurements based on the wireless range and speed rates of a standard Wireless G product from D-Link. Maximum throughput based on D-Link Wireless N devices.
[2] QoS feature available in hardware version B1 and above.
[3] 1-Year Limited Warranty available only in the USA and Canada.
[4] Computer must adhere to Microsoft's recommended System Requirements.
[5] The software included with this product is not Mac-compatible.
[6] Latest software and documentation are available at http://support.dlink.com.
[7] Hardware version C1 and above are equipped with non-detachable antennas.

All references to speed and range are for comparison purposes only. Product specifications, size, and shape are subject to change without notice, and actual product appearance may differ from that depicted herein.

Hardware Version I1

Compatible with Windows 7

bgn Wi Fi CERTIFIED®

Wi-Fi PROTECTED SETUP

WIRELESS N

D-Link Systems, Inc. | 17595 Mt. Herrmann Street Fountain Valley, CA 92708 | www.dlink.com
©2006-2011 D-Link Corporation/D-Link Systems, Inc. All rights reserved. D-Link and the D-Link logo registered trademarks of D-Link Corporation or its subsidiaries in the United States and/or other countries. Other trademarks or registered trademarks are the property of their respective owners.

PX 3

MOBILE WIRELESS ROUTER

Create a reliable mobile high-speed wireless network wherever you go[1]

Attach your mobile adapter to the router's USB port to enjoy Internet service with your family or colleagues

Use your mobile connection as a backup for your ADSL/cable Internet service

MAXIMUM PORTABILITY

The D-Link® Mobile Wireless Router (DIR-412) allows users to access worldwide mobile broadband[1]. Simply insert a compatible mobile broadband USB adapter into the DIR-412 to share your mobile broadband Internet connection through a secure, high-speed 802.11n wireless network. A 10/100 Ethernet WAN port allows you to access a DSL/Cable modem as the primary backup connection. Auto-failover ensures an uninterrupted connection by automatically connecting to your mobile broadband network whenever your Ethernet network goes down.

ADVANCED NETWORK SECURITY

The DIR-412 ensures a secure Wi-Fi network through the use of WPA/WPA2 wireless encryption. Simply press the WPS button to quickly establish a secure connection to new devices. The DIR-412 also utilizes dual-active firewalls (SPI and NAT) to prevent potential attacks and intrusions from across the Internet.

SIMPLE TO INSTALL AND USE

The Mobile Wireless Router can be installed quickly and easily almost anywhere. This router is great for situations where an impromptu wireless network must be set up, or wherever conventional network access is available. The DIR-412 can be installed on RVs, trains, or boats, allowing passengers to check e-mail or chat online while commuting.

D-Link®

DIR-412

WHAT THIS PRODUCT DOES

The DIR-412 allows you to connect a mobile broadband adapter for mobile broadband connectivity. The incoming connection is then shared via a 802.11n wireless network. The standard Ethernet port on the back can be used as a primary or backup connection.

WIRELESS N 150 TECHNOLOGY

Using Wireless N technology, the DIR-412 provides optimal wireless performance and faster file transfers, enabling you to receive better reception across your home. Not only does the D-Link Wireless N 150 technology extend your wireless range, it is also compatible with previous-generation Wireless G devices[1].

MOBILE WIRELESS ROUTER BENEFITS

+ Provides high-speed connectivity in areas without conventional 802.11 wireless access
+ Compatible with EV-DO/CDMA/HSUPA/HSDPA/UMTS networks
+ Supports WAN failover for persistent connections

YOUR NETWORK SETUP

TECHNICAL SPECIFICATIONS

COMPATIBLE MOBILE NETWORKS
+ 1 x EV-DO/CDMA
+ HSUPA/HSDPA/UMTS

STANDARDS
+ 802.11n
+ 802.11g
+ 802.11b
+ 802.3
+ 802.3u

WIRELESS SECURITY
+ 64/128-bit WEP (Wired Equivalent Privacy)
+ Wi-Fi Protected Access™ (WPA & WPA2)
+ WPS (PBC/PIN)

FIREWALL
+ Network Address Translation (NAT)
+ Stateful Packet Inspection (SPI)
+ MAC Address Filtering
+ Website Filtering

VPN
+ L2TP/PPTP/IPSEC VPN Pass-through
+ PPTP/L2TP Connection

ANTENNA
+ Internal antenna

PORTS
+ 1 x Ethernet (RJ-45)
+ 1 x USB 2.0

LED STATUS INDICATORS
+ Power
+ Internet
+ Wireless
+ Ethernet
+ WPS

DIMENSIONS (W x D x H)
+ Item: 4.75" x 3.75" x 1"
(121mm x 95mm x 25mm)

OPERATING TEMPERATURE
+ 32° to 104°F (0° to 40°C)

OPERATING HUMIDITY
+ 10% to 95% (Non-condensing)

POWER
+ DC 5V/2.5A +/-5%

ADVANCED FEATURES
+ Mobile Modem/Ethernet WAN Backup
+ Auto WAN Failover
+ QoS Management

CERTIFICATIONS
+ FCC CLass B
+ CE
+ RoHS Compliant

WARRANTY
+ 1-Year Limited[2]

[1] Requires third party mobile Internet access subscription. Check with your service provider for service coverage and applicable fees. D-Link does not guarantee compatibility with all EV-DO/CDMA/HSUPA/HSDPA/UTMS wireless networks or third party Internet PC adapters.
[2] 1-Year Limited Warranty available only in the USA and Canada.
[3] Computer must adhere to Microsoft's recommended System Requirements.
[4] The software included with this product is not Mac-compatible.
[5] Latest software and documentation are available at http://support.dlink.com.

All references to speed and range are for comparison purposes only. Product specifications, size and shape are subject to change without notice, and actual product appearance may differ from that depicted herein.

©2010 D-Link Corporation/D-Link Systems, Inc. All rights reserved. D-Link and the D-Link logo are registered trademarks of D-Link Corporation or its subsidiaries in the United States and/or other countries. Windows and Windows Vista are registered trademarks of Microsoft Corporation in the United States and/or other countries. Other trademarks or registered trademarks are the property of their respective owners.

WIRELESS

MINIMUM SYSTEM REQUIREMENTS
Computer with:
+ Windows® 7®, Windows Vista®®, Windows XP SP3®, or Mac OS X (v10.4)®
+ Internet Explorer v7
+ Network Interface Card
+ CD-ROM Drive
For Internet Access:
+ Cable or DSL Modem or USB Dongle Modem
+ Subscription with an Internet Service Provider (ISP)

PACKAGE CONTENTS
+ Mobile Broadband Wireless Router
+ CD-ROM® with
  - Product Documentation

PX 4

D-Link®

DUAL BAND N 600

Dual-band performance - Up to 600Mbps speed

Simultaneous 2.4GHz and 5GHz wireless bands for HD video and everyday use

Create a faster Wi-Fi network with superior home coverage

Wireless N Dual Band Router

Product Highlights

Delivers faster speeds and farther range than previous-generation Wireless G

Award-winning QoS Engine prioritizes Internet traffic to enable enhanced gaming and phone calling (VoIP) experience

Easy to install and use with the included Quick Router Setup Wizard

What this product does

The D-Link ® Wireless N Dual Band Router (DIR-815) features simultaneous wireless bands for faster wireless network speeds up to 600Mbps, enabling you to create a faster Wi-Fi network with superior home coverage.

Dual Band Advantage

Dual Band is two Wi-Fi networks in one router. The dual band technology in the DIR-815 supports both 2.4GHz and 5GHz wireless signals simultaneously. You can check e-mail and browse the Internet using the 2.4GHz band while playing lag-free games and streaming HD movies on the clearer 5GHz band.

DIR-815

PX 4

D-Link®

DIR-815 Wireless N Dual Band Router

Exceptional Performance

The D-Link® Wireless N Dual Band Router (DIR-815) is a Wireless N compliant device that delivers faster speeds[1] and farther range[1] than previous-generation Wireless G devices. Connect the Wireless N Dual Band Router to a cable or DSL modem and provide high-speed Internet access to multiple computers, game consoles, and media players. Create a secure wireless network to share photos, files, music, printers, and more, from greater distances throughout your entire home or office. With D-Link's award-winning QoS engine that prioritizes time-sensitive online traffic, this router enables smooth Internet phone calls (VoIP) and responsive gaming.

Advanced Network Security

The Wireless N Dual Band Router supports the latest wireless security features to help prevent unauthorized access, be it from over a wireless network or from the Internet. Support for WPA™ and WPA2™ standards ensure that you will be able to use the best possible encryption method. In addition, this Wireless N Dual Band Router utilizes Stateful Packet Inspection firewalls (SPI) to help prevent potential attacks from across the Internet.

Package Contents

- Wireless N Dual Band Router (DIR-815)
- Ethernet Cable
- Power Adapter
- CD-ROM[2]
- Quick Install Guide[2]

Minimum System Requirements

Computer with:

- Windows® 7[3], Windows Vista®[3] or Windows® XP SP2[3] or Mac OS® X (v10.4)[4]
- Internet Explorer® v6 or Mozilla® Firefox® v3.0
- CD-ROM Drive
- Network Interface Card

For Internet Access:

- Cable or DSL Modem
- Subscription to an Internet Service Provider (ISP)

Suggested Products:

- D-Link Xtreme N® Dual Band USB Adapter (DWA-160)

Features

- IEEE 802.11n, 802.11g, and 802.11a Compliant
- Dual Band Technology for Superior Wireless Performance[1]
- Wi-Fi® Protected Setup™ (WPS) for Simple Push-Button Wireless Network Configuration
- Built-in QoS Engine Enhances Internet Experience
- 4 Fast Ethernet Ports
- Supports Secure Wireless Encryption Using WPA™ or WPA2™
- 24/7 Basic Installation Support[5]
- 1-Year Limited Warranty[6]

Choose the Right Product for You	N 150	N 300	DUAL BAND N 600
SPEED & RANGE			
Share the Internet throughout your home network	■	■	■
Easy file sharing within your home network	■	■	■
Better range and speed over Wireless G	■	■	■
Backwards compatible with Wireless G	■	■	■
Network connection safe with wireless encryption and Dual Active firewall	■	■	■
Push button Wi-Fi protected setup (WPS)	■	■	■
Intelligent antenna technology for better Wi-Fi coverage		■	■
Enhanced router performance for a more reliable network		■	■
QoS engine prioritizes video and gaming traffic			■
Designed for more coverage and performance throughout your home			■
Use 5GHz band for streaming HD content with less interference			■

DIR-815 Wireless N Dual Band Router

Back

Technical Specifications

Standards
- IEEE 802.11n
- IEEE 802.11g
- IEEE 802.11a
- IEEE 802.3
- IEEE 802.3u

Device Interface
- 4 10/100 LAN Ports
- 1 10/100 WAN Ports

Security
- Wi-Fi Protected Access (WPA, WPA2)[6]

LEDs
- Power
- Internet
- WLAN 2.4 GHz (Wireless Connection)
- WLAN 5Ghz (Wireless Connection)
- LAN (10/100)

Operating Temperature
- 32°F to 104°F (0°C to 40°C)

Certifications
- FCC Class B
- IC
- Wi-Fi®

Dimensions
- Item: 6.25" x 4.72" x 1.27" (158.87mm x 120.04mm x 32.18mm)
- Packaging: 8.1" x 10.9" x 2.6" (205.7mm x 276.9mm x 66mm)

Weight
- Item: 0.47 lbs (213.2grams)
- Packaging: 1.0 lbs (453.6grams)

Warranty
- 1-Year Warranty[2]

[1] Maximum wireless signal rate derived from IEEE Standard 802.11g, 802.11a, 802.11b, and 802.11n specifications. Actual data throughput will vary. Network conditions and environmental factors, including volume of network traffic, building materials and construction, and network overhead, lower actual data throughput rate. Environmental factors will adversely a effect wireless signal range. Wireless range and speed rates are D-Link RELATIVE performance measurements based on the wireless range and speed rates of a standard Wireless G product from D-Link. Maximum throughput based on D-Link's 802.11n devices.

[2] Latest software and documentation are available at http://support.dlink.com

[3] Computer must adhere to Microsoft's recommended System Requirements.

[4] The software included with this product is not Mac-compatible.

[5] 24/7 Basic Installation Support is available only in the USA for the first 30 days from date of original purchase. An additional 60 days of Basic Installation Support (for a total of 90 days from date of original purchase) is available in the USA by registering this product at support.dlink.com/register within the aforementioned 30-day period. Extended premium support available. 61-Year Limited Warranty available only in the USA and Canada.

All references to speed and range are for comparison purposes only. Product specifications, size, and shape are subject to change without notice, and actual product appearance may differ from that depicted on the package. See inside package for warranty details.

For more information

U.S.A. | 17595 Mt. Herrmann Street | Fountain Valley, CA 92708 | 800.326.1688 | dlink.com **Canada** | 2525 Meadowvale Blvd | Mississauga, ON L5N 5S2 | 800.361.5265 | dlink.ca

©2012 D-Link Corporation/D-Link Systems, Inc. All rights reserved. D-Link, the D-Link logo, D-Link Green, the D-Link Green Logo, RangeBooster N and the D-Link RoHS logo are trademarks or registered trademarks of D-Link Corporation or its subsidiaries in the United States and/or other countries. Other trademarks or registered trademarks are the property of their respective owners. Visit www.dlink.com for more details.

Updated 03/02/12

D-Link®
Building Networks for People

PX 5

 PX 5

D-Link®

with SMART BEAM™

AMPLIFI N+ 300

SmartBeam technology for whole home coverage

SharePort for sharing any USB device

4 Gigabit Ethernet ports for great wired connectivity

AMPLIFI™ \ hole Home Router 1000

Wi-Fi coverage to the farthest corners of your home

DIR-645

Whole Home Router 1000

The D-Link Whole Home Router 1000 is designed to enhance your wireless signal and extend coverage. SmartBeam™ technology provides wireless signals to every corner of your house[1] by directly beaming bandwidth to your wireless devices. Since SmartBeam works in real time, you're free to move around with your laptop or iPad® without losing this superior signal.

Give your wireless devices the bandwidth they crave. Give them SmartBeam.

Build a wireless home network capable of delivering the bandwidth to handle HD video streams, large media file downloads, and online gaming to multiple devices, simultaneously. SmartBeam uses 6 multi-directional antennas to find and track individual devices, then focus beams of bandwidth to those devices, ensuring a seamless connection anywhere in the home. Ideal for large homes or small offices where concrete walls, successive floors in multi-storied buildings, or other architectural impediments can weaken a wireless signal, SmartBeam is designed to handle large home networks and can even power devices across large backyards. What's more, this tracks mobile devices in real-time so the Whole Home Router 1000 supllies this boosted bandwidth to your iPad or or smartphones as you move around. Eliminate wireless dead spots and unleash comprehensive whole-home coverage on all your devices, all at once – the Whole Home Router 1000 provides uninterrupted connectivity to any device, anywhere in your home or small office.

Now Playing: Everything

The Whole Home Router 1000 has not only been engineered to deliver seamless connectivity to your favorite wireless devices, but comes equipped with 4 high-performance Gigabit Ethernet ports to power your digital entertainment system as well. HDTVs, the Boxee Box by D-Link, Blu-Ray Players, xBox 360®, Playstation 3 –Connect your favorite performance devices and give them the 300 Mbps speed and advanced QoS bandwidth prioritization they need for seamless iPad® HD video streams, high-performance gaming, and VOIP calls without annoying glitches or lags. Connect printers, NAS servers - even security cameras - Shareport Plus USB 2.0 lets you stream from any USB device. There's even a SharePort App for Android® and iPhone® OS for online gaming support like Onlive.

Advanced Home Networking. Simple Setup

High-performance entertainment devices. Wireless signals anywhere in your home. Multiple laptops. Network storage systems. iPads, iPhones – It used to be that designing a home network capable of handling so many devices required some serious hardware and some seriously messy installation. Not with Amplifi™- the Whole Home Router 1000 has not only been engineered with the power to handle all of your digital demands, but with the smarts to put it at the tip of your fingers. Whole Home Routers offer Wireless G backwards-compatibility and Wi-PnP technology for simple wireless connections through a USB drive. IPv6 allows for intelligent self-detect and router setup.

128-bit Security Encryption

The Whole Home Router 1000 protects your network with 128-bit AES data security encryption – the same technology used in E-commerce or online banking. Create your own network name and password or put it at the tip of your fingers with 'Push Button Security' standard on every Amplifi device. With hassle-free plug and play installation, and advanced Wi-Fi protected setup, the Whole Home Router 1000 is not only one of the fastest routers available, its also one of the safest.

Get Ready for the Future - IPv6 Equipped

With the growing number of Internet-enabled applications requiring IP addresses, the supply of IP addresses under the current Internet Protocol version 4 (IPv4) system has already been exhausted. The IPv6 protocol solves this network addressing exhaustion by creating more IP addresses, but migration from IPv4 to IPv6 is not necessarily automatic. No worries - This D-Link product is IPv6 Certified and ready for the future.

The Whole Home Router is great for:

Large Homes

Homes or offices with cold or dead spots

Mobile devices like iPads and tablets

Outdoor wireless connectivity[1]

Features
+ 4 Gigabit Ethernet Ports[1]
+ IEEE 802.11n and 802.11g Compliant
+ WPS (Wi-Fi® Protected Setup™) for simple Push-Button Wireless Network Configuration
+ Supports Secure Wireless Encryption Using WPA™ or WPA2™
+ Parental Controls powered by OpenDNS
+ UPnP® Support
+ 24/7 Basic Installation Support[2]
+ 1-Year Limited Warranty[3]

Think Green
While this may look like your average router, it's not. This is a D-Link Green router, which is as good for your wallet as it is for the environment. The Whole Home Router 1000 is designed to conserve energy, protect our environment from harmful substances and reduce waste by using recyclable packaging. D-Link Green devices provide eco-friendly alternatives without compromising performance. To learn more, visit www.dlinkgreen.com.

D-Link Green™ Technology[2]
+ Power saving by link status
+ Power saving by cable length
+ Power saving by wireless LAN scheduling
+ Complies with the EU RoHS directive that restricts the use of certain hazardous materials
+ Uses soy ink and recyclable packaging to reduce harmful environmental waste

Technical Specifications

STANDARDS
+ IEEE 802.11n
+ IEEE 802.11g
+ IEEE 802.3
+ IEEE 802.3u
+ IEEE 802.3ab

DEVICE INTERFACE
+ 4 Gigabit LAN Ports
+ 1 Gigabit WAN Port
+ Push Button (for Wi-Fi Protected Setup™)
+ USB Port (SharePort™ Plus)
+ Power Button

ANTENNA TYPE
+ Smartbeam

SECURITY
+ Wi-Fi Protected Access™ (WPA, WPA2)®
+ Wi-Fi Protected Setup (WPS) - Push Button

ADVANCED FIREWALL FEATURES
+ Network Address Translation (NAT)
+ Stateful Packet Inspection (SPI)
+ VPN Pass-through / Multi-sessions PPTP / L2TP / IPSec

DEVICE MANAGEMENT
+ Internet Explorer® v7 or Later; Mozilla Firefox® v3.0 or Later; or other Java-enabled Browsers

LEDs
+ Internet
+ WLAN
+ WPS
+ Power

CERTIFICATIONS
+ FCC Class B
+ IC
+ Wi-Fi®
+ WPS - PBC/PIN

DIMENSIONS
+ Item (WxDxH): 4.6" x 7.6" x 1.2" (117mm x 190mm x 97mm)

WEIGHT
+ Item: 0.7 lbs
+ Packaging: 2.0 lbs

WARRANTY
+ 1-Year Limited[3]

[1] Maximum wireless signal rate derived from IEEE Standard 802.11 specifications. Actual data throughput will vary. Network conditions and environmental factors, including volume of network traffic, buildings materials and construction, and network overhead, lower actual data throughput rate. Environmental factors will adversely affect wireless signal range. Wireless range and speed rates are D-Link RELATIVE performance measurements based on the wireless range and speed rates of a standard Wireless G product from D-Link. Maximum throughput based on D-Link draft Wireless N devices.

[2] D-Link Green references contained herein apply to Hardware version A3 or later. SharePort references contained herein apply to Firmware version 1.21 or later.

[3] 1-Year Limited Warranty available only in the USA and Canada.

[4] Computer must adhere to Microsoft's recommended System Requirements.

[5] The software included with this product is not Mac-compatible.

[6] Latest software and documentation are available at http://support.dlink.com.

All references to speed and range are for comparison purposes only. Product specifications, size, and shape are subject to change without notice, and actual product appearance may differ from that depicted herein.

© 2011 D-Link Corporation/D-Link Systems, Inc. All rights reserved. D-Link, the D-Link logo, D-Link Green, and the D-Link Green logo are trademarks or registered trademarks of D-Link Corporation or its subsidiaries in the United States and/or other countries. Other trademarks or registered trademarks are the property of their respective owners.

For more help deciding which product to choose, scan this QR code with your Smartphone

DIR-645

Package Contents
+ Whole Home Router 1000 (DIR-645)
+ CAT5 Ethernet Cable
+ CD-ROM[6]
+ Power Adapter
+ Quick Install Guide

Minimum Requirements
Computer with:
+ Windows® 7[4], Windows Vista®[4], Windows® XP SP2[4], Windows® 2000[4], or Mac OS® X (v10.4)[5]
+ Internet Explorer® v6 or Mozilla® Firefox® v3.0
+ CD-ROM Drive
+ Network Interface Card

For Internet Access:
+ Cable or DSL Modem
+ Subscription with an Internet Service Provider (ISP)

For optimal wireless performance, use with D-Link Xtreme N® Desktop PCI Adapter (DWA-552), D-Link Xtreme N® Desktop PCI Express Adapter (DWA-556), or D-Link Wireless N Nano USB Adapter (DWA-131).

PX 6

D-Link®

PX 6

Remote Viewing Surveillance

+ Instant Notifications

+ Easy do-it-yourself Installation

+ 11n Wireless Connectivity

mydlink™ enabled

Available in the android market

Available on the App Store

Wireless N Network Camera

Compact Size, Easy Installation

The mydlink-enabled Wireless N Network Camera (DCS-930L) comes with everything you need to quickly add a surveillance camera to your home or small office network. It works right out of the box. Simply connect the cables, plug in the camera, run the short installation wizard and setup is complete. To view what the camera is seeing, simply log on to mydlink.com, choose your device, and start viewing – there is no need to configure your router to open up ports or remember hard-to-memorize Internet addresses.

Benefits Of mydlink™

mydlink products are created for people who long to embrace a world connected through the Internet, but are afraid they lack the technical expertise to do so. mydlink products remove the learning curve that is typically associated with today's high-tech devices because they are truly plug-and-play with zero or extremely easy configuration. mydlink provides you easy and straightforward access to your digital life all from our intuitive, convenient website (www.mydlink.com). mydlink makes it easy to get the most from your digital lifestyle without the learning curve.

Convenient Access, Anywhere, Anytime

As a mydlink-enabled device, you can access the DCS-930L anytime, anywhere you have Internet access. Get peace of mind by keeping an eye on your kids, pets, home or office from almost anywhere by simply logging on to the mydlink website and selecting your camera or download the free mydlink™ app from the App store[7] or Android™ market for on-the-go Live video viewing. Since the DCS-930L comes with a built-in microphone, you can see and hear for yourself that everything is well at home.

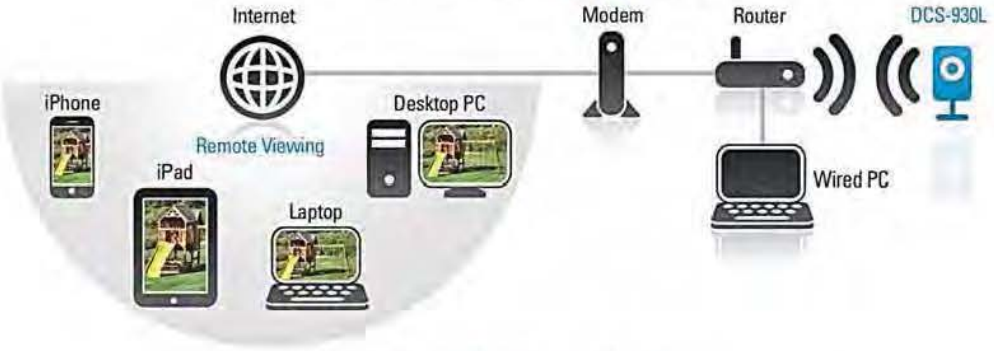
Camera Management

For advanced users that want more out of their camera, the DCS-930L also comes with D-Link D-ViewCam™ management software. D-ViewCam comes with a host of features including the ability to record directly from the camera to a local hard drive, trigger motion detection, set recording schedules, set e-mail alert notifications, and even support for up to 32 cameras. D-ViewCam also allows you to upload a floor plan of your home or small business and create a realistic layout of where your cameras are located, providing you with better access to your camera. For even greater recording flexibility, you can record video directly to a Network Attached Storage (NAS) device, eliminating the need for a dedicated computer to store video.

D-Link®

DCS-930L

Various Viewing Applications



Technical Specifications

Network Protocol
+ IPV4, ARP, TCP, UDP, ICMP
+ DHCP Client
+ NTP Client (D-link)
+ DNS Client
+ DDNS Client (Dynds and D-link)
+ SMTP Client
+ FTP Client
+ HTTP server
+ PPPoE
+ UPnP Port Forwarding
+ LLTD

Built-in Network Interface
+ 10/100Base-TX Fast Ethernet
+ 802.11b/g/n WLAN

Wireless Connectivity
+ 802.11b/g/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
+ 32 MB

Flash Memory
+ 4 MB

Reset Button
+ Reset to factory default

Video Codecs
+ MJPEG
+ JPEG for still images

Video Features
+ Adjustable image size and quality
+ Time stamp and text overlay
+ Flip and Mirror

Resolution
+ 640 x 480 at up to 20 fps
+ 320 x 240 at up to 30 fps
+ 160 x 120 at up to 30 fps

Lens
+ Focal length: 5.01 mm, F2.8

Sensor
+ VGA 1/5 inch CMOS Sensor

Minimum Illumination
+ 1 Lux @ F2.8

View Angle
+ Horizontal: 45.3°
+ Vertical: 34.5°
+ Diagonal: 54.9°

Digital Zoom
+ Up to 4x

3A Control
+ AGC (Auto Gain Control)
+ AWB (Auto White Balance)
+ AES (Auto Electronic Shutter)

Power
+ Input: 100-249 V AC, 50/60Hz
+ Output: 5 V DC, 1.2A
+ External AC-to-DC switching power adapter

Max Power Consumption
+ 4.5W

Operation Temperature
+ 32°F to 140°F (0°C to 40°C)

Storage Temperature
+ -4°F to 158°F (-20°C to 70°C)

Humidity
+ 20-80% RH Non-Condensing

Dimensions (W x D x H)
+ Including the bracket and stand:
  2.6" x 2.6" x 5" (65.8mm x 65mm x 126mm)

Camera only
+ 1.1" x 2.4" x 3.8" (27.2mm x 60mm x 96mm)

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

Support
+ 24/7 Basic Installation Support[2]

Warranty
+ 1-Year Limited[3]

[1]Maximum wireless signal rate derived from IEEE Standard 802.11 specifications. Actual data throughput will vary. Network conditions and environmental factors, including volume of network traffic, building materials and construction, and network overhead, lower actual data throughput rate. Environmental factors will adversely affect wireless signal range. Wireless range and speed rates are D-Link RELATIVE performance measurements based on the wireless range and speed rates of a standard Wireless G product from D-Link. Maximum throughput based on D-Link's 802.11n devices. [2]24/7 Basic Installation Support is available only in the USA for the first 30 days from date of original purchase. [3]1-Year Limited Warranty available only in the USA and Canada. [4]Computer must adhere to Microsoft's recommended system requirements. [5]D-View Cam software included is not Mac-compatible. [6]Latest Software and Documentation available at http://support.dlink.com. [7]The inclusion of a specific product or manufacturer does not imply its endorsement of D-Link or the D-Link product.

©2010 D-Link Corporation/D-Link Systems, Inc. All rights reserved. D-Link, the D-Link logo, the D-Link RoHS logo, D-ViewCam, and mydlink are trademarks or registered trademarks of D-Link Corporation or its subsidiaries in the United States and/or other countries. Other trademarks or registered trademarks are the property of their respective owners. iPhone and iPad are registered trademarks of Apple Inc. Android is a trademark of Google Inc.

SECURITY

Minimum System Requirements for Installation
+ Wired (10/100 Fast Ethernet) or Wireless (802.11g or 802.11n) Network
(Wireless N network recommended for optimum wireless performance)
Computer with:
+ 1.3GHz Processor
+ 128MB Memory
+ Windows® 7®, Windows Vista®[4] and Windows® XP SP2[4], or Mac OS X (10.5 and above, Intel Processor)
+ Internet Explorer® v6, Mozilla® Firefox® v3.0, Google® Chrome v2, or Safari® v4
+ CD-ROM Drive
For Internet Access:
+ Cable or DSL Modem
+ Subscription with an Internet Service Provider (ISP)

Package Contents
+ Wireless N Network Camera
+ CAT5 Ethernet Cable
+ Power Adapter
+ Camera Base and Mounting Kit
+ Quick Install Guide
+ CD-ROM[5] with:
  - D-View Cam Software[5]
  - Product Documentation[6]

PX 7

Digital Baby Monitor
Day / Night Cloud Camera
Digital Baby Monitor
Perfect for viewing on multiple devices
Experience peace of mind from anywhere, anytime
mydlink™ Lite App
D-Link
Use your Smartphone as a baby monitor
View at home or on the go
Day
Night
Digital Baby Monitor
Day / Night Cloud Camera
Day / Night Monitoring
4x Digital Zoom
Sound/Motion Detection
Secure Connection
Expand Wireless Network
Unlimited Range Using Smartphones and Tablets
Package Contents
Minimum Requirements
1-Year
24/7
SOY INK
Easy out-of-the-box setup
Secure connection for a private monitoring experience
Sound and motion monitoring
See your baby in low light and even complete darkness
D-Link

PX 7

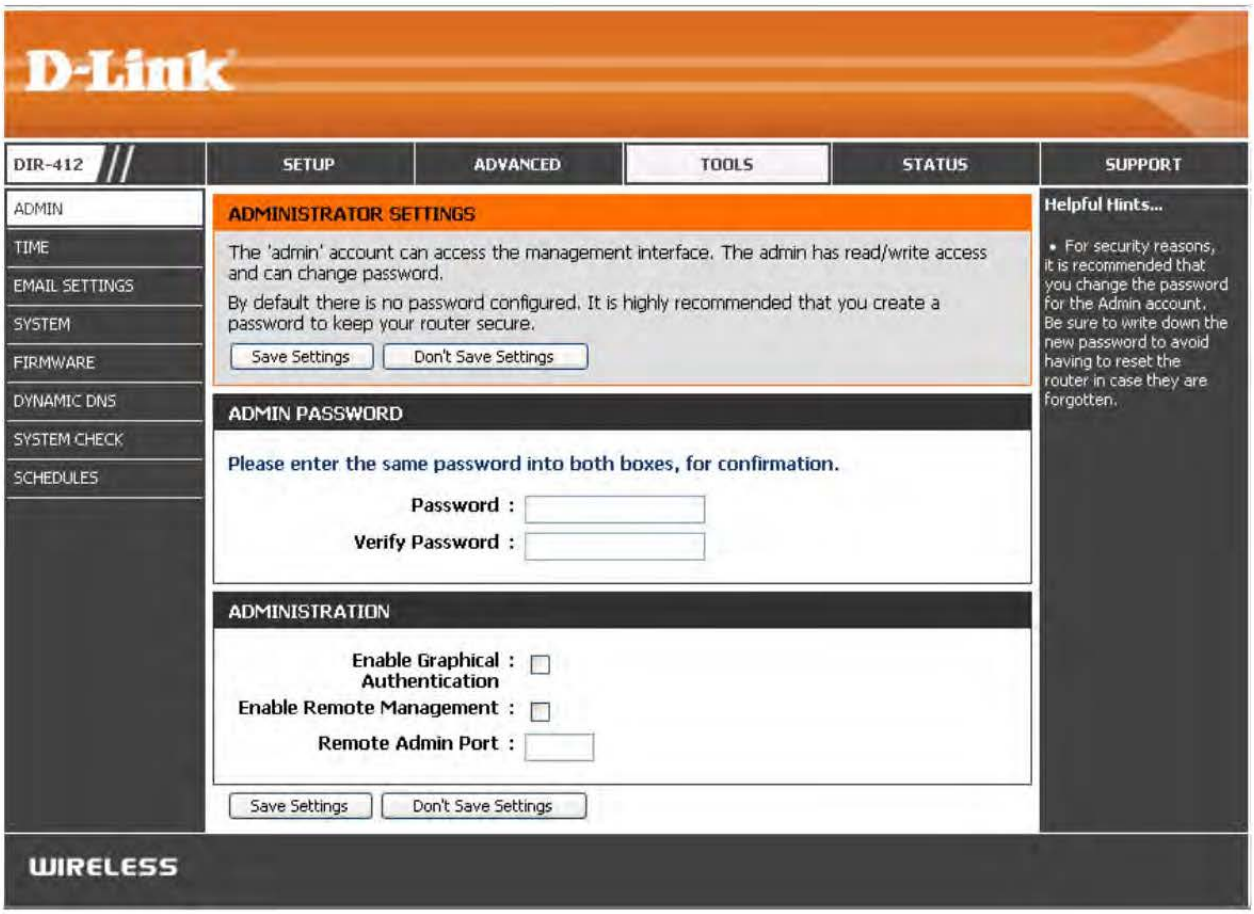
Day / Night Monitoring
4x Digital Zoom
Sound/Motion Detection
Secure Connection
Expand Wireless Network
Unlimited Range Using Smartphones and Tablets*
Package Contents
1 Digital Baby Monitor (DCS-933L/B)
+ Ethernet Cable
+ Power Adapter
+ Camera Base and Mounting Kit
+ Quick Install Guide
Minimum Requirements
Wired (10/100 Fast Ethernet) or Wireless (802.11g or 802.11n) Network (Wireless N network recommended for optimum wireless performance)
Computer with:
- 1.3GHz Processor
- 128MB Memory
- Windows® 8*, Windows® 7*, Windows Vista®* and Windows® XP SP2**, or Mac OS X (10.5 and above, Intel Processor)
Internet Explorer® v6, Mozilla® Firefox®, Google® Chrome, or Safari® v4
For Internet Access:
- Cable or DSL Modem
- Subscription with an Internet Service Provider (ISP)
tor

PX 8

STEP 1: SET YOUR PASSWORD
By default, your new D-Link Router does not have a password configured for administrator access to the Web-based configuration pages. To secure your new networking device, please set and verify a password below:
Password :
Verify Password :
Prev
Next
Cancel
Connect

PX. 8

PX 9


D-Link
DIR-412
SETUP
ADVANCED
TOOLS
STATUS
SUPPORT
ADMIN
TIME
EMAIL SETTINGS
SYSTEM
FIRMWARE
DYNAMIC DNS
SYSTEM CHECK
SCHEDULES
ADMINISTRATOR SETTINGS
The 'admin' account can access the management interface. The admin has read/write access and can change password.
By default there is no password configured. It is highly recommended that you create a password to keep your router secure.
Save Settings
Don't Save Settings
ADMIN PASSWORD
Please enter the same password into both boxes, for confirmation.
Password :
Verify Password :
ADMINISTRATION
Enable Graphical Authentication :
Enable Remote Management :
Remote Admin Port :
Save Settings
Don't Save Settings
Helpful Hints...
• For security reasons, it is recommended that you change the password for the Admin account. Be sure to write down the new password to avoid having to reset the router in case they are forgotten.
WIRELESS

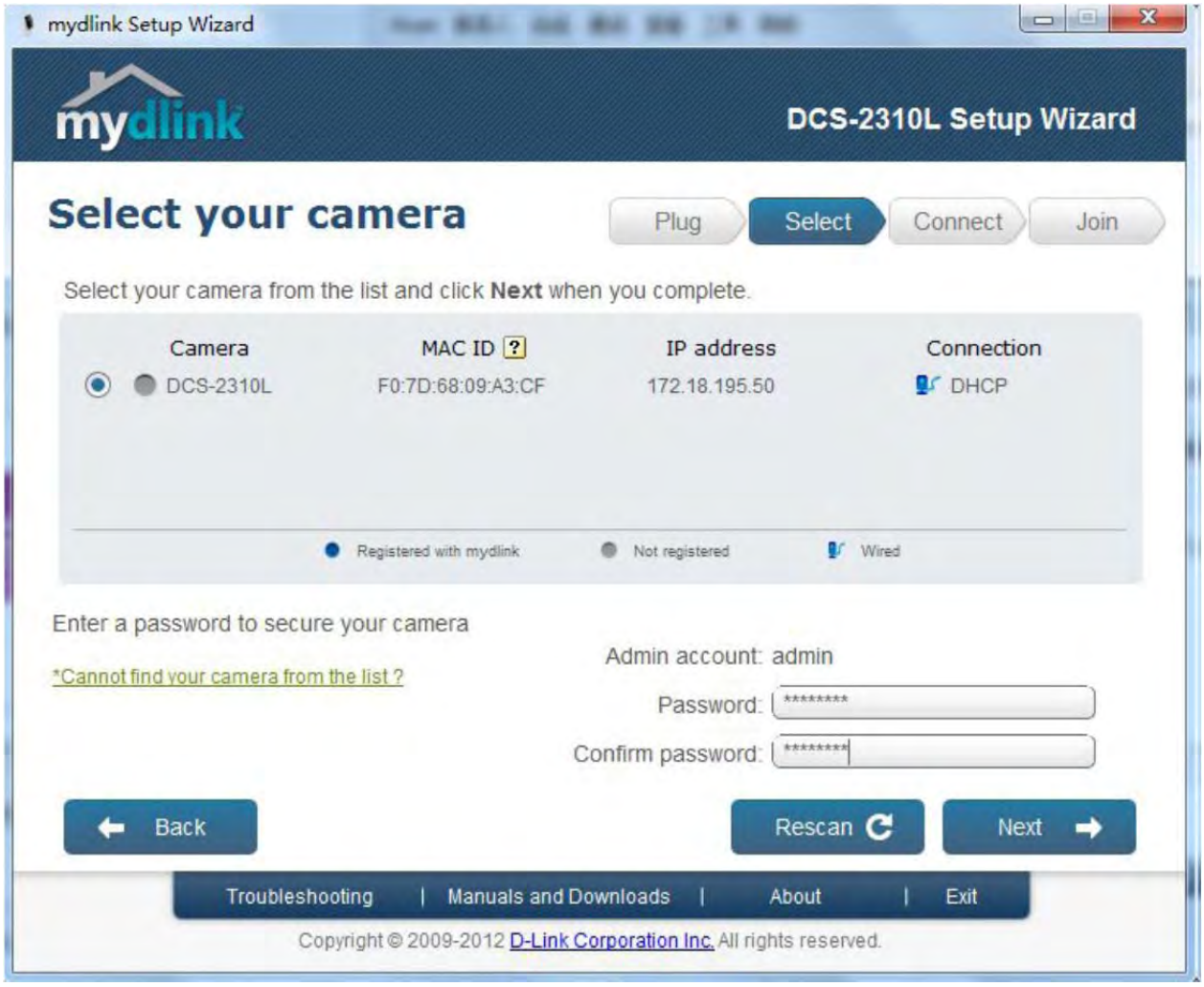
PX. 9

PX 10

D-Link
Building Networks for People
SECURICAM Network
Set up an Admin ID and Password to secure your camera.
Click Next to continue.
Admin ID
Password
Change
New ID
Reconfirm
Change
New Password
Reconfirm
Back
Next
Exit

PX 10

PX 11


mydlink Setup Wizard
mydlink
DCS-2310L Setup Wizard
Select your camera
Plug
Select
Connect
Join
Select your camera from the list and click Next when you complete.
Camera
MAC ID
IP address
Connection
DCS-2310L
F0:7D:68:09:A3:CF
172.18.195.50
DHCP
Registered with mydlink
Not registered
Wired
Enter a password to secure your camera
*Cannot find your camera from the list ?
Admin account: admin
Password:
Confirm password:
Back
Rescan
Next
Troubleshooting
Manuals and Downloads
About
Exit
Copyright © 2009-2012 D-Link Corporation Inc. All rights reserved.

PX11