

D-Link *AirPremier*™ DWL-2210AP

**802.11g Wireless
Adaptive Access Point**

Manual

D-Link®
Building Networks for People

Contents

Package Contents	3
LEDs and Connections.....	4
Overview.....	5
Features and Benefits	6
Prelaunch Checklist.....	9
Quick Steps for Setup.....	19
Configuring Basic Settings	28
Managing Access Points and Clusters	35
Managing User Accounts	43
Session Monitoring.....	47
Setting the Ethernet (Wired) Interface.....	50
Setting the Wireless Interface.....	56
Enabling the Network Time Protocol Server.....	61
Configuring Security.....	64
Configuring Radio Settings.....	85
Controlling Access by MAC Address Filtering	90
Load Balancing.....	93
Configuring Queues for Quality of Service	96
Configuring the Wireless Distribution System	105
Setting Up Guest Access.....	113
Maintenance and Monitoring	117
Appendix A: Configuring Security Settings for Wireless Clients	130
Appendix B: Troubleshooting	162
Glossary	166
Technical Specifications	184
Contacting Technical Support.....	188
Warranty	189
Registration	192

Package Contents



Contents of Package:

- **D-Link AirPremier DWL-2210AP**
802.11g Wireless Adaptive Access Point
- Power over Ethernet base unit
- Power Adapter-DC 48V, 0.4A
- Power cord
- Manual and Warranty on CD
- Quick Installation Guide
- Ethernet Cable

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

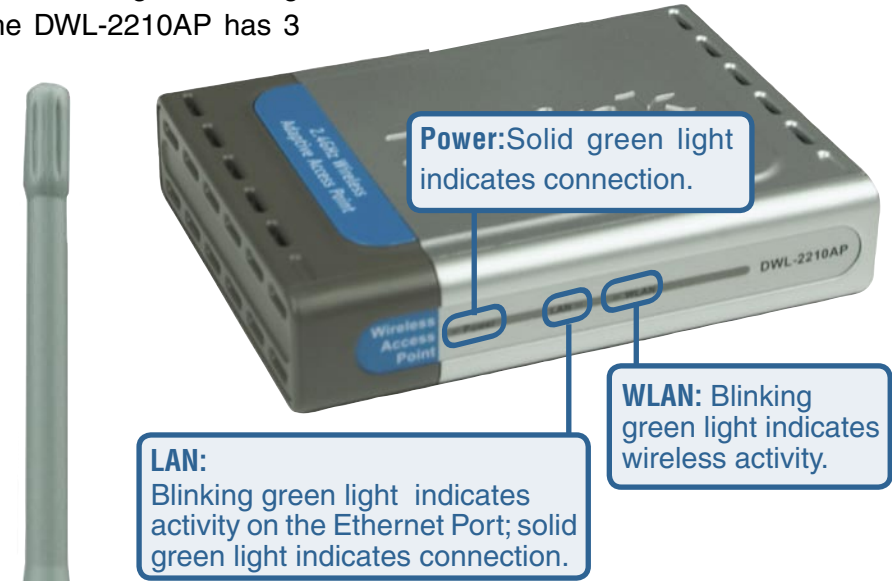
Note: Using a power supply with a different voltage rating than the one included with the DWL-2210AP will cause damage and void the warranty for this product.

System Requirements for Configuration:

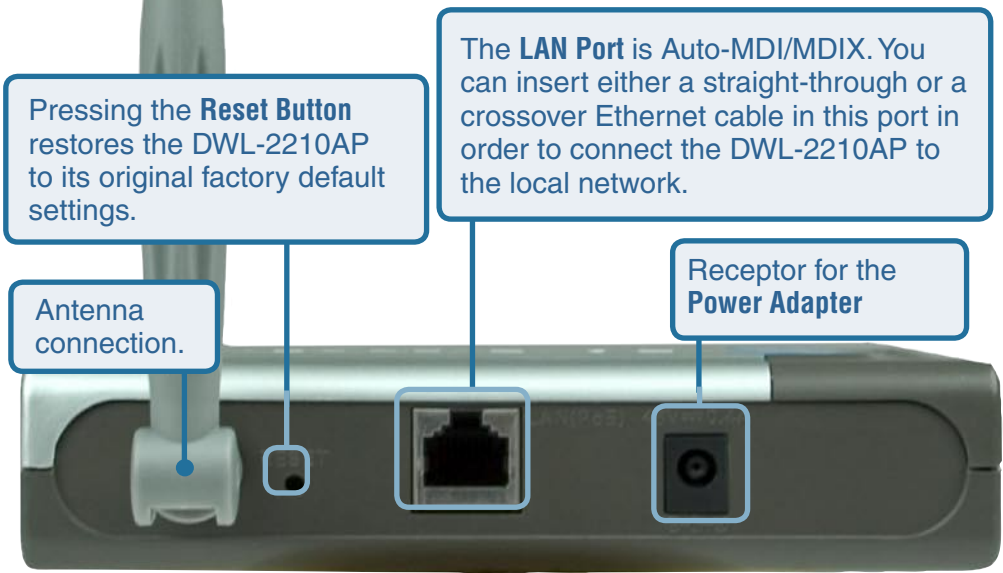
- Computers with Windows, Macintosh, or Linux-based operating systems with an installed Ethernet adapter
- Internet Explorer Version 6.0 or Netscape Navigator Version 6.0 and Above

LEDs

LED stands for light-emitting diode. The DWL-2210AP has 3 LEDs.



Connections



Overview of the D-Link DWL-2210AP

The D-Link DWL-2210AP provides continuous, high-speed access between your wireless and Ethernet devices. It is an advanced, standards-based solution for wireless networking in small and medium-sized businesses. The D-Link DWL-2210AP enables zero-administration wireless local area network (WLAN) deployment while providing state-of-the-art wireless networking features.

The D-Link DWL-2210AP provides best-of-breed security, ease-of-administration and industry standards, providing a standalone and fully-secured wireless network without the need for additional management and security server software.

The D-Link DWL-2210AP is a single band access point with one radio capable of broadcasting in either IEEE 802.11b or IEEE 802.11g mode.

The following section lists features and benefits of the D-Link DWL-2210AP.

Features and Benefits

IEEE Standards Support and Wi-Fi Compliance

- Support for IEEE 802.11b and IEEE 802.11g wireless networking standards.
- Provides bandwidth of up to 54Mbps* IEEE 802.11g (11Mbps* for IEEE 802.11b)
- Wi-Fi certification

Wireless Features

- Auto channel selection at startup
- Transmit power adjustment
- Wireless Distribution System (WDS) for connecting multiple access points wirelessly. Extends your network with less cabling and provides a seamless experience for roaming clients.
- Quality of Service (QoS) for enhanced throughput and better performance of time-sensitive wireless traffic like Voice over IP (VoIP) and streaming media
- Load Balancing
- Built-in support for multiple SSIDs (network names) and multiple BSSIDs (basic service set IDs) on the same access point
- Neighboring access point detection (also known as “rogue” AP detection)

“Maximum wireless signal rate based on IEEE Standard 802.11a and 802.11g 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”.

Features and Benefits (continued)

Security Features

- Inhibit SSID Broadcast
- Ignore SSID Broadcast
- Weak IV avoidance
- Wireless Equivalent Privacy (WEP)
- Wi-Fi Protected Access (WPA)
- Advanced Encryption Standard (AES)
- User based access control with local authentication server
- Local user database and user life-cycle management
- MAC address filtering

Out-of-the-Box Guest Interface

- Unique network name (SSID) for the Guest interface
- Captive portal to guide guests to customized, guest-only Web page
- VLANs for Guest and Internal networks when Guest Access is enabled

Clustering and Auto-Management

- Automatic setup with Kickstart
- Provisioning and auto-configuration of APs through clustering and cluster rendezvous

The administrator can specify how new access points should be configured before they are added to the network. When new access points are added, they can automatically rendezvous with the cluster, and securely download the correct configuration. The process does not require manual intervention, but is under the control of the administrator.

- Single universal view of clustered access points and cluster configuration settings

Configuration for all access points in a cluster can be managed from a single interface. Changes to common parameters are automatically reflected in all members of the cluster.

Features and Benefits (continued)

Clustering and Auto-Management (continued)

- Self-managed access points with automatic configuration synchronization
The access points in a cluster periodically check that the cluster configuration is consistent, and check for the presence and availability of the other members of the cluster. The administrator can monitor this information through the user interface.
- Enhanced local authentication using 802.1x without additional IT setup
A cluster can maintain a user authentication server and database stored on the access points. This eliminates the need to install, configure, and maintain a RADIUS infrastructure, and simplifies the administrative task of deploying a secure wireless network.
- Hardware watchdog

Networking

- Dynamic Host Configuration Protocol (DHCP) support for dynamically assigning network configuration information to systems on the LAN
- Virtual Local Area Network (VLAN) support (for Guest Access)

Maintainability

- Status, monitoring, and tracking views of the network including session monitoring, client associations, transmit/receive statistics, and event log
- Link integrity monitoring to continually verify connection to the client, regardless of network traffic activity levels
- Reset configuration option
- Firmware upgrade

What's Next?

Ready to get started with wireless networking? Read through the **PreLaunch Checklist: Default Settings and Supported Administrator/Client Platforms** and then follow the steps in **Quick Steps for Setup and Launch of Your Wireless Network**.

Prelaunch Checklist:

Default Settings and Supported Administrator/Client Platforms

Before you plug in and boot a new access point, review the following sections for a quick check of required hardware components, software, client configurations, and compatibility issues. Make sure you have everything you need ready to go for a successful launch and test of your new (or extended) wireless network.

- D-Link DWL-2210AP
- Default Settings for the D-Link DWL-2210AP
- What the Access Point Does Not Provide
- Administrator's Computer
- Wireless Client Computers
- Understanding Dynamic and Static IP Addressing on the D-Link DWL-2210AP
- How Does the Access Point Obtain an IP Address at Startup?
- Dynamic IP Addressing
- Static IP Addressing

D-Link DWL-2210AP

The D-Link DWL-2210AP is a wireless communications hub for devices on your network. It provides continuous, high-speed access between your wireless and Ethernet devices in 802.11b and 802.11g.

The D-Link DWL-2210AP offers an out-of-the-box *Guest Interface* feature that allows you to configure access points for controlled guest access of the wireless network. This can be accomplished by using Virtual LANs. (For more information on the Guest interface, see **Setting up Guest Access** and **A Note About Setting Up Connections for a Guest Network.**)

Default Settings:

Option	Default Settings	Related Information
System Name	DWL-2210AP	“Setting the DNS Name” in “Setting the Ethernet (Wired) Interface”
User Name	admin The user name is read-only. It cannot be modified.	
Password	admin	“Provide Administrator Password and Wireless Network Name” in “Configuring Basic Settings” and “Setting the Administrator Password”
Network Name (SSID)	Internal interface: “default” Guest interface: “default (guest)”	“Review / Describe the Access Point” in “Configuring Basic Settings.” “Configuring Internal LAN Wireless Settings” in “Setting the Wireless Interface.” “Configuring Guest Network Wireless Settings” in “Setting the Wireless Interface.”
Network Time Protocol (NTP)	None	“Enabling the Network Time Protocol Server.”
IP Address	192.168.0.50 The default IP address is used if you do not use a <i>Dynamic Host Configuration Protocol</i> (DHCP) server. You can assign a new static IP address through the Administration Web pages. If you have a DHCP server on the network, then an IP address will be dynamically assigned by the server at AP startup.	

Default Settings (continued):

Option	Default Settings	Related Information
Connection Type	<p><i>Dynamic Host Configuration Protocol (DHCP)</i></p> <p>If you do not have a DHCP server on the Internal network and do not plan to use one, the first thing you must do after bringing up the access point is to change the Connection Type from “DHCP” to “Static IP.” The Guest network must have a DHCP server.</p>	
Subnet Mask	<p>None</p> <p>This is determined by your network setup and DHCP server configuration.</p>	
Radio	On	“Configuring Radio Settings”
IEEE 802.11 Mode	802.11g	“Configuring Radio Settings”
802.11g Channel	Auto	“Configuring Radio Settings”
Beacon Interval	100	“Configuring Radio Settings”
DTIM Period	2	“Configuring Radio Settings”
Fragmentation Threshold	2346	“Configuring Radio Settings”
RTS Threshold	2347	“Configuring Radio Settings”
MAX Stations	2007	“Configuring Radio Settings”
Transmit Power	100 percent	“Configuring Radio Settings”
Rate Sets Supported (Mbps)	<ul style="list-style-type: none"> • IEEE 802.1g: 54, 48, 36, 24, 18, 12, 11, 9, 6, 5.5, 2, 1 • IEEE 802.1b: 11, 5.5, 2, 1 	“Configuring Radio Settings”

Default Settings (continued):

Option	Default Settings	Related Information
Rate Sets (Mbps) (Basic/Advertised)	<ul style="list-style-type: none"> • IEEE 802.1g: 11, 5.5, 2, 1 • IEEE 802.1b: 2, 1 	“Configuring Radio Settings”
Broadcast SSID	Allow	“Broadcast SSID and Security Mode” in “Configuring Security”
Security Mode	None (plain text)	“Broadcast SSID and Security Mode” in “Configuring Security”
Authentication Type	None	
MAC Filtering	Allow any station unless in list	“Controlling Access by MAC Address Filtering”
Guest Login and Management	Disabled	“Setting up Guest Access”
Load Balancing	Disabled	“Load Balancing”
WDS Settings	None	“Configuring the Wireless Distribution System (WDS)”

What the Access Point Does Not Provide

The D-Link DWL-2210AP is not designed to function as a gateway to the Internet. To connect your wireless LAN (WLAN) to other LANs or to the Internet, you need a gateway device.

Administrator's Computer

Configuration and administration of the D-Link DWL-2210AP is accomplished with the KickStart utility (which you run from the CD) and through a Web-based user interface.

The DWL-2210AP must be installed into a DHCP-enabled network in order to use the KickStart utility for configuration. The following table describes the minimum requirements for the administrator's computer.

Required Software or Component	Description
Ethernet Connection to the First Access Point	<p>The computer used to configure the first access point with KickStart must be connected to the access point (either directly or through a hub) by an Ethernet cable.</p> <p>For more information on this step, see "Step 2. Connect the access point to network and power" in Quick Steps for Setup and Launch of Your Wireless Network.</p>
Wireless Connection to the Network	<p>After initial configuration and launch of the first access points on your new wireless network, you can make subsequent configuration changes through the Administration Web pages using a wireless connection to the "Internal" network. For wireless connection to the access point, your administration device will need Wi-Fi capability similar to that of any wireless client:</p> <ul style="list-style-type: none">• Portable or built-in Wi-Fi client adapter that supports one or more of the IEEE 802.11 modes in which you plan to run the access point. (IEEE 802.11b, 802.11g, and 802.11g Turbo modes are supported.)• Wireless client software such as Microsoft Windows XP or Funk Odyssey wireless client configured to associate with the D-Link DWL-2210AP. <p>For more details on Wi-Fi client setup, see "Wireless Client Computers" in this manual.</p>

Administrator's Computer (continued)

Required Software or Component	Description
<p>Web Browser / Operating System</p>	<p>Configuration and administration of the D-Link DWL-2210AP is provided through a Web-based user interface hosted on the access point. We recommend using one of the following supported Web browsers to access the access point Administration Web pages:</p> <ul style="list-style-type: none"> • Microsoft Internet Explorer version 5.5 or 6.x (with up-to-date patch level for either major version) on Microsoft Windows XP or Microsoft Windows 2000 • Netscape Mozilla on Redhat Linux version 2.4 <p>The administration Web browser must have JavaScript enabled to support the interactive features of the administration interface. It must also support HTTP uploads to use the firmware upgrade feature.</p>
<p>KickStart Wizard on CD-ROM</p>	<p>You can run the KickStart Wizard on the D-Link CD-ROM on any Windows laptop or computer that is connected to the access point either directly or through a switch. It detects D-Link DWL-2210APs on the network. When used in a DHCP-enabled network, the wizard steps you through initial configuration of new access points, and provides a link to the Administration Web pages where you finish up the basic setup process in a step-by-step mode and launch the network.</p> <p>For more about using the KickStart Wizard, see “Step 3. Run KickStart Wizard to find access points on the network” in “Quick Steps for Setup and Launch of Your Wireless Network” in this manual.</p>
<p>CD-ROM Drive</p>	<p>The administrator's computer must have a CD-ROM drive to run the KickStart Wizard on the CD-ROM.</p>
<p>Security Settings</p>	<p>Ensure that security is disabled on the wireless client used to initially configure the access point.</p>

Wireless Client Computers

The D-Link DWL-2210AP provides wireless access to any client with a properly configured Wi-Fi client adapter for the 802.11b and 802.11g modes in which the access point is running.

Multiple client operating systems are supported. Clients can be laptops or desktops, personal digital assistants (PDAs), or any other hand-held, portable or stationary device equipped with a Wi-Fi adapter and supporting drivers.

In order to connect to the access point, wireless clients need the following software and hardware.

Required Software or Component	Description
Wi-Fi Client Adapter	<p>Portable or built-in Wi-Fi client adapter that supports one or more of the IEEE 802.11 modes in which you plan to run the access point. (IEEE 802.11b and 802.11g modes are supported.)</p> <p>Wi-Fi client adapters vary considerably. The adapter can be a PC card built in to the client device, a portable PCMCIA or PCI card (types of NICs), or an external device such as a USB or Ethernet adapter that you connect to the client by means of a cable.</p> <p>The access point supports 802.11b/g modes, but you will probably make a decision during network design phase as to which mode to use. The fundamental requirement for clients is that they all have configured adapters that match the 802.11 mode for which your access point(s) is configured.</p>
Wireless Client Software	Client software such as Microsoft Windows Supplicant or Funk Odyssey wireless client configured to associate with the D-Link DWL-2210AP.

Wireless Client Computers (continued)

Required Software or Component	Description
Client Security Settings	<p>Security should be disabled on the client used to do initial configuration of the access point.</p> <p>If the Security mode on the access point is set to anything other than plain text, wireless clients will need to set a profile to the authentication mode used by the access point and provide a valid username and password, certificate, or similar user identity proof. Security modes are Static WEP, IEEE 802.1x, WPA with RADIUS server, and WPA-PSK.</p> <p>For information on configuring security on the access point, see the “Configuring Security” section in this manual.</p>

Understanding Dynamic and Static IP Addressing on the D-Link DWL-2210AP

When installed in a DHCP network (dynamic IP addressing), the D-Link DWL-2210APs are designed to auto-configure, with very little setup required for the first access point and no configuration required for additional access points subsequently joining a pre-configured cluster.

How Does the Access Point Obtain an IP Address at Startup?

When you deploy the access point, it looks for a network DHCP server and, if it finds one, obtains an IP address from the DHCP server. If no DHCP server is found on the network, the AP will continue to use its default static IP address (192.168.0.50) until you reassign it a new static IP address (and specify a static IP addressing policy) or until a DHCP server is brought online.

If you configure both an Internal and Guest network and plan to use a dynamic addressing policy for both, separate DHCP servers must be running on each network.

A DHCP server is a requirement for the Guest network.



You must have the DWL-2210AP installed in a DHCP network in order to use the Kickstart Wizard.

When you run the KickStart Wizard on the CD-ROM, it discovers the D-Link DWL-2210APs on the network and lists their IP addresses and MAC addresses. In DHCP networks, KickStart Wizard also provides a link to the administration Web pages of each access point using the IP address in the URL. (For more information about the KickStart Wizard, see “Run KickStart Wizard to find access points on the network” in this manual.)

Dynamic IP Addressing

The D-Link DWL-2210AP generally expects that a DHCP server is running on the network where the AP is deployed. Most home and small business networks already have DHCP service provided either via a gateway device or a centralized server. However, if no DHCP server is present on the Internal network, the AP will use the default static IP address for first time startup.

Similarly, wireless clients and other network devices (such as printers) will receive their IP addresses from the DHCP server, if there is one. If no DHCP server is present on the network, you must manually assign static IP addresses to your wireless clients and other network devices. The Guest network must have a DHCP server.

Understanding Dynamic and Static IP Addressing

Static IP Addressing

The D-Link DWL-2210AP ships with a default Static IP Address of 192.168.0.50. (See “Default Settings for the D-Link DWL-2210AP” in this manual.) If no DHCP server is found on the network, the AP retains this static IP address at first-time startup.

After AP startup, you have the option of specifying a static IP addressing policy on D-Link DWL-2210APs and assigning static IP addresses to APs on the Internal network via the access point Administration Web pages. (See information about the **Connection Type** field and related fields in “Configuring Internal Interface Ethernet Settings.”)



If you do not have a DHCP server on the Internal network and do not plan to use one, the first thing you must do after bringing up the access point is change the connection type from DHCP to static IP. You can either assign a new static IP address to the AP or continue using the default address. We recommend assigning a new static IP address so that if later you bring up another D-Link DWL-2210AP on the same network, the IP address for each AP will be unique.

Configuring the IP address of the DWL-2210AP in a network with no DHCP server

If you do not have a DHCP server in your network, you will not use the Kickstart utility to configure the DWL-2210AP. To configure the DWL-2210AP, you will need to first change the IP address of the computer to be within the IP address range of the DWL-2210AP. That range is 192.168.0.1 to 192.168.0.254, excluding 192.168.0.50 (the IP address of the DWL-2210AP). You will then open the Web browser and type “192.168.0.50” into the address field. The login screen will appear. Enter “admin” for Admin and Password. The Web configuration screen will appear. You can change the static IP address of the DWL-2210AP so that it is within the range of your network. If you do this, you must also revert your computer’s IP address to its previous setting within your network’s range.

Recovering an IP Address

If you experience trouble communicating with the access point, you can recover a static IP address by resetting the AP configuration to the factory defaults (see “Resetting the Configuration” in this manual), or you can get a dynamically assigned address by connecting the AP to a network that has DHCP.

Quick Steps for the Setup and Launch of Your Wireless Network

Setting up and deploying one or more D-Link DWL-2210APs is in effect creating and launching a *wireless network*. The KickStart Wizard (for DHCP-enabled networks) and corresponding Basic Settings Administration Web page simplify this process. Here is a step-by-step guide to setting up your D-Link DWL-2210APs and the resulting wireless network. Have the CD-ROM handy, and familiarize yourself with the “PreLaunch Checklist: Default Settings and Supported Administrator/Client Platforms” discussed earlier in this manual. The topics covered here are:

- Step 1. Unpack the access point
- Step 2. Connect the access point to network and power
- Step 3. Power on the access point
- Step 4. Run KickStart Wizard on the CD-ROM to find access points on the network
- Step 5. Log on to the Administration Web pages
- Step 6. Configure “Basic Settings” and start the wireless network

Step 1. Unpack the access point

Unpack the access point (AP) and familiarize yourself with its hardware ports, associated cables, and accessories.

Access Point Hardware and Ports

The access point includes:

- Ethernet ports for connection to the Local Area Network (LAN) via Ethernet network cable
- Power port and power adapter
- Single radio
- Power over Ethernet base unit

For more information on the specifics of your access point, see the booklet provided by the manufacturer.

Step 1. Unpack the access point (continued)

What's inside the box?

D-Link AirPremier DWL-2210AP
802.11g Wireless Adaptive Access Point
Power over Ethernet base unit
Power Adapter-DC 48V, 0.4A
Power cord
Manual and Warranty on CD
Quick Installation Guide
Ethernet Cable

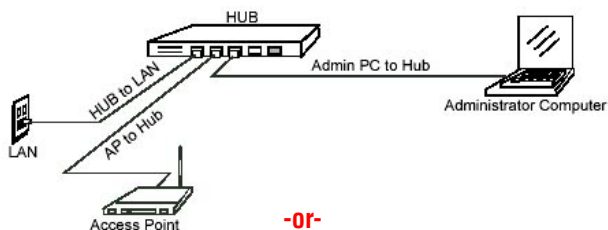
Step 2. Connect the access point to network and power

The next step is to set up the network and power connections.

1. Do one of the following to create an Ethernet connection between the access point and the computer:

- Connect one end of an Ethernet cable to the network port on the access point and the other end to the same hub where your PC is connected.

ETHERNET CONNECTIONS WHEN USING DHCP FOR INITIAL CONFIGURATION



- Connect one end of an Ethernet cable to the network port on the access point and the other end of the cable to the Ethernet port on the PC.

ETHERNET CONNECTIONS WHEN USING STATIC IP FOR INITIAL CONFIGURATION



Step 2. Connect the access point (continued)

- If you use a hub, the device you use must permit broadcast signals from the access point to reach all other devices on the network. A standard hub should work fine. Some *switches*, however, do not allow directed or subnet broadcasts through. You may have to configure the switch to allow directed broadcasts.
- If for initial configuration you use a direct Ethernet (wired) connection (via Ethernet cable) between the access point and the computer, you will need to reconfigure the cabling for subsequent startup and deployment of the access point so that the access point is no longer connected directly to the PC but instead is connected to the LAN (either via a Hub or directly).
- It is possible to detect access points on the network (using KickStart Wizard on the CD-ROM with a wireless connection). However, we strongly advise against using this method. In most environments you may have no way of knowing whether you are actually connecting to the intended AP and also because many of the initial configuration changes required will cause you to lose connectivity with the AP over a wireless connection.

2. Connect the power adapter to the power port on the back of the access point, and then plug the other end of the power cord into a power outlet (preferably, via a surge protector).

-or-

You can also power ON the DWL-2210AP by utilizing the PoE (Power over Ethernet) function. Connect one end of a Cat5 cable into the LAN(PoE) port on the back of the DWL-2210AP, and connect the other end into the P+DATA OUT port on the PoE base unit. Connect another Cat5 cable into the DATA IN port of the PoE base unit and connect the other end into a LAN port on your computer or switch. Connect the power adapter to the power port on the back of the PoE base unit, and plug the other end of the power cord into a power outlet (preferably, via a surge protector)

A Note About Setting Up Connections for a Guest Network

The D-Link DWL-2210AP offers an out-of-the-box Guest Interface that allows you to configure an access point for controlled guest access to the network. The same access point can function as a bridge for two different wireless networks: a secure “Internal” LAN and a public “Guest” network. The same AP broadcasts as two different networks (Internal and Guest). This is accomplished by defining two different Virtual LANs (VLANs) via the Administration UI.

Hardware Connections for a Guest VLAN

If you plan to configure a guest network using VLANs, do the following:

- Connect a network port on the access point to a VLAN-capable switch
- Define VLANs on that switch

Once you have the required physical connections set up, the rest of the configuration process is accomplished through the Administration UI. For information on configuring Guest interface settings on the Administration UI, see “Setting up Guest Access.”

Step 3. Run KickStart Wizard on the CD-ROM to find access points on a DHCP network



The DWL-2210AP is DHCP enabled by default. The DWL-2210AP CD-ROM contains the KickStart Wizard to simplify access point configuration on a network with a DHCP server. Use Kickstart **only** when there is a DHCP server in your network.

KickStart Wizard is an easy-to-use utility for discovering and identifying new D-Link DWL-2210APs in a network with a DHCP server. KickStart scans the network looking for access points, and displays ID details on those it finds.

- Keep in mind that KickStart Wizard recognizes and configures only D-Link DWL-2210APs. Kickstart will not find any other devices.
- Run Kickstart only in the subnet of the “Internal” network (SSID). Do not run Kickstart on the guest subnetwork.
- Kickstart Wizard will find only those access points that have IP addresses. IP addresses are dynamically assigned to APs if you have a DHCP server running on the network. Keep in mind that if you deploy the AP on a network with no DHCP server, the default static IP address (192.168.0.50) will be used.

Use caution with non-DHCP enabled networks: Do not deploy more than one new AP on a non-DHCP network because they will use the same default static IP addresses and conflict with each other. (For more information, see “Understanding Dynamic and Static IP Addressing on the D-Link DWL-2210AP” and “How Does the Access Point Obtain an IP Address at Startup?”)

Run the CD-ROM on a laptop or computer that is connected to the same network as your access points and use it to step through the discovery process as follows:

1. Insert the CD-ROM into the CD-ROM drive on your computer, and click Kickstart.



The Kickstart Welcome screen will appear (as shown on the next page).

Step 3. Run KickStart Wizard (continued)

Click **Next** to search for access points.

2. Wait for the search to complete, or until the KickStart Wizard has found your new access points.

If no access points are found, Kickstart indicates this and presents some troubleshooting information about your LAN and power connections. Once you have checked hardware power and Ethernet connections, you can click the Kickstart **Back** button to search again for access points.

3. Review the list of access points found. KickStart will detect the IP addresses of D-Link DWL-2210APs. Access points are listed with their locations, Media Access Control (MAC) addresses, and IP addresses. If you are installing the first access point on a single-access-point network, only one entry will be displayed on this screen. Verify the MAC addresses shown here against the hardware labels for each access point. This will be especially helpful later in providing or modifying the descriptive "Location" name for each access point.

Click **Next**.



Step 3. Run KickStart Wizard (continued)

4. Go to the Access Point Administration Web pages by taking the link provided on the KickStart page.



KickStart provides a link to the Administration Web pages via the IP address of the first access point of each model. (For more information about model types and clustering see “What Kinds of APs Can Cluster Together?”) The Administration Web pages are a centralized management tool that you can access via the IP address for any access point in a cluster. Once your other access points are configured, you can also link to the Administration Web pages by using the IP address for any of the other D-Link DWL-2210APs in a URL (<http://IPAddressOfAccessPoint>).

Step 4a. Log on to the Administration Web pages when using Kickstart in a DHCP network

When you follow the link from KickStart to the D-Link DWL-2210AP Administration Web pages, you are prompted for a user name and password.

Field	Default Setting
Username	admin
Password	admin The user name is read-only. It cannot be modified.

Enter the username and password and click **OK**.



Step 4b. Log on to the Administration Web pages without Kickstart, in a non-DHCP network

When the DWL-2210AP is installed in a network with no DHCP server, after configuring your computer's static IP address to be within the IP address range of the DWL-2210AP, you will enter the IP address of the DWL-2210AP into the address field of your web browser; the browser window shown below will appear.

Field	Default Setting
Username	admin
Password	admin
	The user name is read-only. It cannot be modified.



Enter the username and password and click **OK**.

Viewing Basic Settings for Access Points

When you first log in, the **Basic Settings** page for D-Link DWL-2210AP administration is displayed. These are global settings for all access points that are members of the cluster and, if automatic configuration is specified, for any new access points that are added later.

Step 5. Configure “Basic Settings”

Provide a minimal set of configuration information by defining the basic settings for your wireless network. These settings are all available on the **Basic Settings** page of the Administration Web interface, and are categorized into steps 1-4 on the Web page.

For a detailed description of these “Basic Settings” and how to properly configure them, please see “Configuring Basic Settings.” Summarized briefly here, the steps are:

1. Review Description of this Access Point

Provide IP addressing information. For more information, see “Review / Describe the Access Point” in this manual.

2. Provide Network Settings

Provide a new administrator password for clustered access points. For more information, see “Provide Administrator Password and Wireless Network Name” in this manual.

3. Set Configuration Policy for New Access Points.

Choose to configure new access points automatically (as new members of the cluster) or ignore new access points.

If you set a configuration policy to *configure new access points automatically*, new access points added to this network will join the cluster and be configured automatically based on the settings you defined here. Updates to the Network settings on any cluster member will be shared with all other access points in the group.

If you chose to *ignore new access points*, then as you add new access points they will run in standalone mode. In standalone mode, an access point does not share the cluster configuration with other access points; it must be configured manually.

You can always update the settings on a standalone access point to have it join the cluster. You can also remove an access point from a cluster thereby switching it to run in standalone mode.

For more information, see “Set Configuration Policy for New Access Points in this manual.

4. Start Wireless Networking

Click the **Update** button to activate the wireless network with these new settings. For more information, see “Update Basic Settings” in this manual.

Default Configuration

If you follow the steps above and accept all the defaults, the access point will have the default configuration described in “Default Settings for the D-Link DWL-2210AP” in this manual.

What’s Next?

Next, make sure the access point is connected to the LAN, bring up some wireless clients, and connect the clients to the network. Once you have tested the basics of your wireless network, you can enable more security and fine-tune by modifying advanced configuration features on the access point.

Make Sure the Access Point is Connected to the LAN

If you configured the access point and administrator PC by connecting both into a network hub, then your access point is already connected to the LAN. That’s it—you’re up and running! The next step is to test some wireless clients.

If you configured the access point using a direct wired connection via Ethernet cable from your computer to the access point, do the following:

1. Disconnect the Ethernet cable from the computer and the access point.
2. Connect the Ethernet cable from the access point to the LAN.
3. Connect your computer to the LAN either via Ethernet cable or wireless client card.

Test LAN Connectivity with Wireless Clients

Test the D-Link DWL-2210AP by trying to detect it and associate with it from some wireless client devices. (See “Wireless Client Computers” in the PreLaunch Checklist: Default Settings and Supported Administrator/Client Platforms for information on requirements for these clients.)

Secure and Fine-Tune the Access Point Using Advanced Features

Once you have the wireless network up and running and have tested against the access point with some wireless clients, you can add in more layers of security, add users, configure a Guest interface, and fine-tune performance settings.

Configuring Basic Settings

The basic configuration tasks are described in the following sections:

- Navigating to Basic Settings
- Review / Describe the Access Point
- Provide Administrator Password and Wireless Network Name
- Set Configuration Policy for New Access Points
- Update Basic Settings
- Summary of Settings
- Basic Settings for a Standalone Access Point
- Your Network at a Glance: Understanding Indicator Icons

Navigating to Basic Settings

To configure initial settings, click **Basic Settings**.

If you use KickStart Wizard to link to the Administration Web pages, the Basic Settings page is displayed by default.

BASIC SETTINGS Provide basic settings

Cluster

Access Points

Users

Sessions

Status

Interfaces

Events

Statistics

Associations

Neighbors

Advanced

1 Review Description of this Access Point ...

These fields show information specific to this access point.

IP Address: 192.168.0.100
 MAC Address: 00:0d:8b:e6:f6:c5
 Firmware Version: 1.0.2.3
 Location:

2 Provide Network Settings ...

These settings apply to this access point. The same settings will apply to new access points joining the cluster if the policy for adding new access points is set to "configure automatically".

Current Password:
 New Password:
 Confirm New Password:
 Network Name (SSID):

3 Set Configuration Policy for New Access Points ...

If you choose "configure automatically" as the policy for adding new access points, new access points will join the cluster when they are powered up and inherit the settings specified on this page. (If you choose to ignore new access points, you must configure them manually.)

New Access Points:

4 Settings ...

Click "update" to save the new settings.

?

Clustered

For a typical access point which is a member of a cluster, provide the minimal set of configuration information needed to set up the access point and start wireless networking as described in the numbered steps on this page.

1 Access Point

0 User Accounts

For a **standalone access point** the Basic Settings page indicates only that the current mode is standalone and provides a button for adding the access point to a cluster (group). If you click on any of the Cluster tabs for an AP in standalone mode you will be redirected to this Basic Settings page because Cluster settings do not apply to standalone APs.

Caution:
If you do not have a DHCP server on the internal network and do not plan to use one, the first thing you must do after bringing up the access point is change the Connection Type from DHCP to Static IP.

To change the Connection Type, go to the [Ethernet](#) tab.
[More ...](#)

Fill in the fields on the Basic Settings screen as described on the following page.

Review / Describe the Access Point

▶ Review Description of this Access Point ...

These fields show information specific to this access point.

IP Address: 10.10.103.250
MAC Address: 00:90:27:1d:40:90
Firmware Version: dkeehn
Location


Field	Description
IP Address	Shows IP address assigned to this access point. This field is not editable because the IP address is already assigned (either via DHCP, or statically through the Ethernet (wired) settings as described in “Configuring Guest Interface Ethernet Settings” in this manual.
MAC Address	Shows the MAC address of the access point. A MAC address is a permanent, unique hardware address for any device that represents an interface to the network. The MAC address is assigned by the manufacturer. You cannot change the MAC address. It is provided here for informational purposes as a unique identifier for an interface. The address shown here is the MAC address for the bridge (br0). This is the address by which the AP is known externally to other networks. To see MAC addresses for Guest and Internal interfaces on the AP, see the Status > Interfaces tab.
Firmware Version	Version information about the firmware currently installed on the access point. As new versions of the D-Link DWL-2210AP firmware become available, you can upgrade the firmware on your access points to take advantages of new features and enhancements. (You can download the most recent firmware from http://support.dlink.com/). For instructions on how to upgrade the firmware, see “Upgrading the Firmware” in this manual.
Location	Specify a location description for this access point.

Provide Administrator Password and Wireless Network

2 Provide Network Settings ...

These settings apply to this access point. The same settings will apply to new access points joining the cluster if the policy for adding new access points is set to "configure automatically".

Current Password	<input type="password"/>
New Password	<input type="password"/>
Confirm New Password	<input type="password"/>
Network Name (SSID)	<input type="text" value="default"/>

Field	Description
Administrator Password	<p>Enter a new administrator password. The characters you enter will be displayed as "*" characters to prevent others from seeing your password as you type.</p> <p>The Administrator password must be an alphanumeric strings of up to 32 characters. Do not use special characters or spaces.</p> <div style="border: 1px solid #ccc; padding: 5px; margin-top: 10px;">  <p>As an immediate first step in securing your wireless network, we recommend that you change the administrator password from the default.</p> </div>
Administrator Password (again)	<p>Re-enter the new administrator password to confirm that you typed it as intended.</p>
Wireless Network Name (SSID)	<p>Enter a name for the wireless network as a character string. This name will apply to all access points on this network. As you add more access points, they will share this SSID.</p> <p>The <i>Service Set Identifier</i> (SSID) is an alphanumeric string of up to 32 characters.</p> <p>Note: If you are connected as a wireless client to the same AP that you are administering, resetting the SSID will cause you to lose connectivity to the AP. You will need to reconnect to the new SSID after you save this new setting.</p>

The D-Link DWL-2210AP is not designed for multiple, simultaneous configuration changes. If you have a network that includes multiple access points, and more than one administrator is logged on to the Administration Web pages and making changes to the configuration, all access points in the cluster will stay in synch but there is no guarantee that all configuration changes specified by multiple users will be applied.

Set Configuration Policy for New Access Points

3 Set Configuration Policy for New Access Points ...

If you choose “configure automatically” as the policy for adding new access points, new access points will join the cluster when they are powered up and inherit the settings specified on this page. (If you choose to ignore new access points, you must configure them manually.)

New Access Points

Field	Description
New Access Points	<p>Choose the policy you want to put in effect for adding New Access Points to the network.</p> <p>If you choose “are configured automatically”, then when a new access point is added to the network it automatically joins the existing <i>cluster</i>. The cluster configuration is copied to the new access point, and no manual configuration is required to deploy it.</p> <ul style="list-style-type: none"> If you choose “are ignored”, new access points will not join the cluster; they will be considered <i>standalone</i>. You need to configure standalone access points manually by using KickStart Wizard on the CD-ROM and the Administration Web pages residing on the standalone access points. (To get to the Web page for a standalone access point, use its IP address in a URL as follows: <code>http://IPAddressOfAccessPoint.</code>) <p>Note: If you change the policy so that new access points “are ignored,” then any new access points you add to the network will not join the cluster. Existing clustered access points will not be aware of these standalone APs. Therefore, if you are viewing the Administration Web pages via the IP address of a clustered access point, the new standalone APs will not show up in the list of access points on the Cluster > Access Points tab. The only way to see a standalone AP is to browse to it directly by using its IP address in the URL.</p> <p>If you later change the policy back to the default so that new access points “are configured automatically,” all subsequent new APs will automatically join the cluster. Standalone APs, however, will stay in standalone mode until you explicitly add them to the cluster.</p> <p>For information on how to add standalone APs to the cluster, see “Adding an Access Point to a Cluster” in this manual.</p>

Update Basic Settings

4 Settings ...

Click "update" to save the new settings.



When you have reviewed the new configuration, click **Update** to apply the settings and deploy the access points as a wireless network.

Summary of Settings

When you update the Basic Settings, a summary of the new settings is shown along with information about next steps.

The screenshot shows the 'Summary of settings' page. On the left is a navigation menu with categories: BASIC SETTINGS (highlighted), Cluster, Access Points, Users, Sessions, Status, Interfaces, Events, Statistics, Associations, Neighbors, Advanced, Ethernet, Wireless, Security, Guest Login, and Radio. The main content area is titled 'Summary of settings' and contains the following information:

- Summary ...**
- The IP address of this access point is: **10.10.103.250**
- The location of the access point is: **not set**
- The SSID of the network is: **default**
- If you need to change these settings, click the "Basic Settings" tab.

Below this is a 'Next ...' section with three items:

- Security** - Until you choose a security option, unauthorized users can connect to your wireless network without restriction. [Set Security Options](#)
- User Accounts** - If you have chosen to use the local authentication server in your security settings, manage your user accounts here. [Add Users or Manage User Accounts](#)
- Access Points** - Manage your access point(s) here. [Manage Access Points](#)

On the right side, there is a 'Clustering' section with options: Clustering (with a group icon), 1 Access Point (with a single person icon), and 2 User Accounts (with a two people icon). Below this is a 'Caution' box:

Caution: If you do not have a DHCP server on the Internal network and do not plan to use one, the first thing you must do after bringing up the access point is change the Connection Type from DHCP to Static IP.

To change the Connection Type, go to the [Ethernet \(Wired\) Settings](#) tab.

[More ...](#)

At initial startup, no security is in place on the access point. An important next step is to configure security, as described in "Configuring Security" in this manual.

At this point if you click Basic Settings again, the summary of settings page is replaced by the standard Basic Settings configuration options.




Basic Settings for a Standalone Access Point

The Basic Settings tab for a standalone access point indicates only that the current mode is standalone and provides a button for adding the access point to a cluster (group). If you click on any of the Cluster tabs on the Administration pages for an access point in standalone mode, you will be redirected to the Basic Settings page because Cluster settings do not apply to standalone APs.

For more information see “Standalone Mode” and “Adding an Access Point to a Cluster” in this manual.

Your Network at a Glance: Understanding Indicator Icons

All the Cluster settings tabs on the Administration Web pages include visual indicator icons showing current network activity.

Icon	Description
<p>Clustered </p>	<p>When one or more APs on your network are available for service, the “Wireless Network Available” icon is shown. The clustering icon indicates whether the current access point is “Clustered” or “Not Clustered” (that is, standalone).</p> <p>For information about clustering, see “Understanding Clustering” in this manual.</p>
<p>1 Access Point </p>	<p>The number of access points available for service on this network is indicated by the “Access Points” icon.</p> <p>For information about managing access points, see “Managing Access Points and Clusters” in this manual.</p>
<p>2 User Accounts </p>	<p>The number of client user accounts created and enabled on this network is indicated by the “User Accounts” icon.</p> <p>For information about setting up user accounts on the access point for use with the built-in authentication server, see “Managing User Accounts” in this manual. See also “IEEE 802.1x” and “WPA with RADIUS” in this manual, which are the two security modes that offer the option of using the built-in authentication server.</p>

Managing Access Points and Clusters

The D-Link DWL-2210AP shows current basic configuration settings for clustered access points (location, IP address, MAC address, status, and availability) and provides a way of navigating to the full configuration for specific APs if they are cluster members.

Standalone access points or those which are not members of this cluster do not show up in this listing. To configure standalone access points, you must discover (via Kickstart) or know the IP address of the access point and by using its IP address in a URL (<http://IPAddressOfAccessPoint>).

The D-Link DWL-2210AP is not designed for multiple, simultaneous configuration changes. If you have a network that includes multiple access points, and more than one administrator is logged on to the Administration Web pages and making changes to the configuration, all access points in the cluster will stay in synch but there is no guarantee that all configuration changes specified by multiple users will be applied.

The following topics are covered:

- Navigating to Access Points Management
- Understanding Clustering
 - What is a Cluster?
 - How Many APs Can a Cluster Support?
 - What Kinds of APs Can Cluster Together?
 - Which Settings are Shared as Part of the Cluster Configuration and Which Are Not?
 - Cluster Mode
 - Standalone Mode
 - Cluster Formation
 - Cluster Size and Membership
 - Intra-Cluster Security
 - Auto-Synch of Cluster Configuration
- Understanding Access Point Settings
- Modifying the Location Description
- Removing an Access Point from the Cluster
- Adding an Access Point to a Cluster
- Navigating to Configuration Information for a Specific AP and Managing Standalone APs

Navigating to Access Points Management

To view or edit information on access points in a cluster, click the **Cluster > Access Points** tab.

The screenshot shows the 'Manage access points in the cluster' page. On the left is a navigation menu with tabs: Basic Settings, Cluster, Access Points (highlighted), Users, Sessions, Status, Interfaces, Events, Statistics, Associations, Neighbors, and Advanced. The main content area is titled 'Access Points...' and shows the status 'connected to cluster.' Below this is a 'Refresh' button and a table with columns for 'Location', 'MAC Address', and 'IP Address'. The table contains one entry: 'not set', '00:0c:41:0a:33:7e', and '10.10.103.250'. There is a 'Remove' button and text indicating it will remove the selected APs. On the right, there is a sidebar with icons for 'Clustered', '1 Access Point', and '2 User Accounts'. A help box on the far right explains that the page shows basic configuration settings for clustered APs and provides links to sections on 'What Kinds of APs Can Cluster Together?' and 'Standalone Mode'.

Understanding Clustering

A key feature of the D-Link DWL-2210AP is the ability to form a dynamic, configuration-aware group (called a *cluster*) with other D-Link DWL-2210APs in a network in the same subnet. Access points can participate in a self-organizing cluster which makes it easier for you to deploy, administer, and secure your wireless network. The cluster provides a single point of administration and lets you view the deployment of access points as a single wireless network rather than a series of separate wireless devices.

What is a Cluster?

A cluster is a group of access points which are coordinated as a single group via D-Link DWL-2210AP administration. You cannot create multiple clusters on a single wireless network (SSID). Only one cluster per wireless network is supported.

How Many APs Can a Cluster Support?

Up to eight access points are supported in a cluster at any one time. If a new AP is added to a network with a cluster that is already at full capacity, the new AP is added in *standalone mode*. Note that when the cluster is full, extra APs are added in standalone mode regardless of the configuration policy in effect for new access points.

For related information, see “Cluster Mode”, “Standalone Mode”, and “Set Configuration Policy for New Access Points” in this manual.

What Kinds of APs Can Cluster Together?

A single D-Link DWL-2210AP can form a cluster with itself (a “cluster of one”) and with other D-Link DWL-2210APs. In order to be members of the same cluster, access points must be:

- Of the same radio and band configuration (all one-radio, single-band APs; the D-Link DWL-2210AP is a one-radio, single-band AP)
- On the same LAN

Having a mix of APs on the network does not adversely affect D-Link DWL-2210AP clustering in any way. However, it is helpful to understand the clustering behavior for administration purposes:

- Access points of the same model will form a cluster.
- Access points of other brands will not join the cluster. These APs should be administered with their own associated Administration tools.

Which Settings are Shared as Part of the Cluster Configuration and Which Are Not?

Most configuration settings defined via the D-Link DWL-2210AP Administration Web

Settings Shared in the Cluster Configuration

The cluster configuration includes:

- Network name (SSID)
- Administrator password
- Configuration policy
- User accounts and authentication
- Wireless interface settings
- Guest Welcome screen settings
- Network Time Protocol (NTP) settings
- Radio settings
- Security settings
- QoS queue parameters
- MAC address filtering

Settings Not Shared by the Cluster

The few exceptions (settings *not* shared among clustered access points) are the following most of which, by nature, must be unique:

- IP addresses
- MAC addresses
- Location descriptions
- WDS bridges
- Ethernet (Wired) Settings, including enabling or disabling Guest access
- Guest interface configuration

Settings that are not shared must be configured individually on the Administration pages for each access point. To get to the Administration pages for an access point that is a member of the current cluster, click on its IP Address link on the Cluster > Access Points page of the current AP.

Cluster Mode

When an access point is a cluster member, it is considered to be in cluster mode. You define whether you want new access points to join the cluster or not via the configuration policy you set in the Basic Settings. (See “Set Configuration Policy for New Access Points” in this manual.) You can reset an access point in cluster mode to standalone mode. (See “Removing an Access Point from the Cluster” in this manual.)

When the cluster is full (eight APs is the limit), extra APs are added in *standalone mode* regardless of the configuration policy in effect for new access points. See “How Many APs Can a Cluster Support?” in this manual.

Standalone Mode

The D-Link DWL-2210AP can be configured in *standalone* mode. In standalone mode, an access point is not a member of the cluster and does not share the cluster configuration, but rather requires manual configuration that is not shared with other access points. (See “Set Configuration Policy for New Access Points” and “Removing an Access Point from the Cluster” in this manual.)

Standalone access points are not listed on the Cluster > Access Points tab in the Administration UIs of APs that are cluster members. You need to know the IP address for standalone access points in order to configure and manage it directly. (See “Navigating to an AP by Using its IP Address in a URL” in this manual.)

The Basic Settings tab for a standalone access point indicates only that the current mode is standalone and provides a button for adding the access point to a cluster (group).

If you click on any of the Cluster tabs on the Administration pages for an access point in standalone mode, you will be redirected to the Basic Settings page because Cluster settings do not apply to standalone APs.

When the cluster is full (eight APs is the limit), extra APs are added in *standalone mode* regardless of the configuration policy in effect for new access points. See “How Many APs Can a Cluster Support?” in this manual.

You can re-enable cluster mode on a standalone access point. (See “Adding an Access Point to a Cluster” in this manual.)

Cluster Formation

A cluster is formed when the first D-Link DWL-2210AP is configured. (See “Quick Steps for Setup and Launch of Your Wireless Network” and “Configuring Basic Settings” in this manual.)

If a cluster configuration policy is in place, when a new access point is deployed, it attempts to rendezvous with an existing cluster.

If it is unable to locate a cluster, then it establishes a new cluster on its own.

If it locates a cluster but is rejected because the cluster is full, or the clustering policy is to ignore new access points, then the access point will deploy in standalone mode.

Cluster Size and Membership

The upper limit of a cluster is eight access points. The “Cluster” Web administration pages provides a real-time, visual indicator of the number of access points in the current cluster and warn when the cluster has reached capacity. (See “Step 6. Configure “Basic Settings” and start the wireless network” in this manual.)

If a cluster is present but is already full, new access points will deploy in standalone mode.

Intra-Cluster Security

To ensure that the security of the cluster as a whole is equivalent to the security of a single access point, communication of certain data between access points in a cluster is done using Secure Sockets Layer (typically referred to as SSL) with private key encryption.

Both the cluster configuration file and the user database are transmitted among access points using SSL.

Auto-Synch of Cluster Configuration

If you are making changes to the AP configuration that require a relatively large amount of processing (such as adding several new users), you may encounter a synchronization progress bar after clicking “Update” on any of the Administration pages.

The progress bar indicates that the system is busy performing an auto-synch of the updated configuration to all APs in the cluster. The Administration Web pages are not editable during the auto-synch.



Note that auto-synchronization always occurs during configuration updates that affect the cluster, but the processing time is usually negligible. The auto-synch progress bar is displayed only for longer-than-usual wait times.

Understanding Access Point Settings

The access points tab provides information about all access points in the cluster.

From this tab, you can view location descriptions, IP addresses, enable (activate) or disable (deactivate) *clustered* access points, and remove access points from the cluster. You can also modify the location description for an access point.

The IP address links provide a way to navigate to configuration settings and data on an access point.

Standalone access points (those which are not members of the cluster) are not shown on this page.

Field	Description
Location	Description of where the access point is physically located.
MAC Address	<p>Media Access Control (MAC) address of the access point.</p> <p>A MAC address is a permanent, unique hardware address for any device that represents an interface to the network. The MAC address is assigned by the manufacturer.</p> <p>You cannot change the MAC address. It is provided here for informational purposes as a unique identifier for the access point.</p> <p>The address shown here is the MAC address for the bridge (br0). This is the address by which the AP is known externally to other networks.</p> <p>To see MAC addresses for Guest and Internal interfaces on the AP, see the Status > Interfaces tab.</p>
IP Address	<p>Specifies the IP address for the access point. Each IP address is a link to the Administration Web pages for that access point. You can use the links to navigate to the Administration Web pages for a specific access point. This is useful for viewing data on a specific access point to make sure a cluster member is picking up cluster configuration changes, to configure advanced settings on a particular access point, or to switch a standalone access point to cluster mode.</p>

The following table describes the access point settings and information display in detail.

Modifying the Location Description

To make modifications to the location description:

1. Navigate to the **Basic Settings** tab.
2. Update the Location description in section 1 under “Review Description of this Access Point.”
3. Click **Update** button to apply the changes.

Removing an Access Point from the Cluster

To remove an access point from the cluster, do the following.

1. Click the checkbox next to the access point so that the box is checked.
2. Click **Remove from Cluster**.

The change will be reflected under Status for that access point; the access point will now show as *standalone* (instead of *cluster*).

In some situations it is possible for the cluster to become out of sync. If after removing an access point from the cluster, the AP list still reflects the deleted AP or shows an incomplete display; refer to the information on Cluster Recovery in “Appendix B. Troubleshooting” in this manual.

Adding an Access Point to a Cluster

To add an access point that is currently in standalone mode back into a cluster, do the following.

1. Go to the Administration Web pages for the standalone access point. (See “Navigating to an AP by Using its IP Address in a URL” in this manual.)

The Administration Web pages for the standalone access point are displayed.

2. Click the Basic Settings tab in the Administration pages for the standalone access point.

The Basic Settings tab for a standalone access point indicates that the current mode is standalone and provides a button for adding the access point to a cluster (group).

If you click on any of the Cluster tabs on the Administration pages for an access point in standalone mode, you will be redirected to the Basic Settings page because Cluster settings do not apply to standalone APs.

3. Click the **Join Cluster** button.

The access point is now a cluster member. Its Status (Mode) on the Cluster > Access Points tab now indicates “cluster” instead of “standalone.”

In some situations it is possible for the cluster to become out of sync. If after removing an access point from the cluster, the AP list still reflects the deleted AP or shows an incomplete display; refer to the information on Cluster Recovery in “Appendix B. Troubleshooting” in this manual.

Navigating to Configuration Information for a Specific AP and Managing Standalone APs

In general, the D-Link DWL-2210AP is designed for central management of *clustered* access points. For access points in a cluster, all access points in the cluster reflect the same configuration. In this case, it does not matter which access point you actually connect to for administration.

There may be situations, however, when you want to view or manage information on a particular access point. For example, you might want to check status information such as client associations or events for an access point. Or you might want to configure and manage features on an access point that is running in *standalone* mode. In these cases, you can navigate to the Administration Web interface for individual access points by clicking the IP address links on the Access Points tab.

All clustered access points are shown on the Cluster > Access Points page. To navigate to clustered access points, you can simply click on the IP address for a specific cluster member shown in the list.

Navigating to an AP by Using its IP Address in a URL

You can also link to the Administration Web pages of a specific access point, by entering the IP address for that access point as a URL directly into a Web browser address bar in the following form:

`http://IPAddressOfAccessPoint`

where *IPAddressOfAccessPoint* is the address of the particular access point you want to monitor or configure.

For standalone access points, this is the only way to navigate to their configuration information.

If you do not know the IP address for a standalone access point, use KickStart Wizard on the CD-ROM to find all APs on the network and you should be able to derive which ones are standalone by comparing KickStart findings with access points listed on the Cluster > Access Points tab. The APs that KickStart Wizard finds that are not shown on the this tab are probably standalone APs. (For more information on using KickStart, see “Step 3. Run KickStart on the CD-ROM to find access points on the network” in this manual.)

Managing User Accounts

The D-Link DWL-2210AP includes user management capabilities for controlling client access to access points.

User management and authentication must always be used in conjunction with the following two security modes, which require use of a RADIUS server for user authentication and management.

- IEEE 802.1x mode (see “IEEE 802.1x” in the Configuring Security section)
- WPA with RADIUS mode (see “WPA with RADIUS” in the Configuring Security section)

You have the option of using either the internal RADIUS server embedded in the D-Link DWL-2210AP or an external RADIUS server that you provide. If you use the embedded RADIUS server, use this Administration Web page on the access point to set up and manage user accounts. If you are using an external RADIUS server, you will need to set up and manage user accounts on the Administrative interface for that server.

On the User Management page, you can create, edit, remove, and view client *user accounts*. Each user account consists of a user name and password. The set of users specified here represent approved *clients* that can log in and use one or more access points to access local and possibly external networks via your wireless network.

Users specified here are clients of the access point(s) who use the APs as a connectivity hub, not administrators of the wireless network. Only those with the administrator username and password and knowledge of the administration URL can log in as an administrator and view or modify configuration settings.

The following topics are covered:

- Navigating to User Management for Clustered Access Points
- Viewing User Accounts
- Adding a User
- Editing a User Account
- Enabling and Disabling User Accounts
- Removing a User Account

Navigating to User Management for Clustered Access Points

To set up or modify user accounts, click the **Cluster > Users** tab.

Basic Settings

Cluster

Access Points

Users

Sessions

Status

Interfaces

Events

Statistics

Associations

Neighbors

Advanced

Ethernet

Wireless

Security

Guest Login

Radio

MAC Filtering

Load Balancing

Manage user accounts

User Accounts...

To edit a user account, click a user name.

To enable or disable a user, click the "enable" or "disable" button. Likewise, to remove a user, click the "remove" button. Ensure that you have selected at least one user prior to any of these actions.

Note: These user accounts apply only when the security mode is set to "IEEE 802.1x" or "WPA with RADIUS" and the built-in authentication server is chosen. See the Help panel for more information.

<input type="checkbox"/> Edit	User Name	Real Name	Status
<input type="checkbox"/> [Edit]	samantha	Elizabeth Montgomery	enabled
<input type="checkbox"/> [Edit]	andora	Agnes Moorhead	enabled

Selected users:

Add a user...

To add a user, fill in the fields below and click "add account".

User Name

Real Name

Password

Password (nqain for safety)

Clustered

1 Access Point

2 User Accounts

? User accounts specified here are wireless clients of the access point, not Administrators.

These user accounts are applicable only when the security mode on the access point is set to either "IEEE 802.1x" or "WPA with RADIUS" and the Built-in authentication server is chosen. If you use an external RADIUS server for user authentication, you must set up and manage user accounts on the Administrative interface for that server.

To configure the security mode, go to the [security](#) tab.

User accounts (if any) are shown at the top of the screen under "User Accounts"

User name, real name, and status (enabled or disabled) are shown.

To modify an existing user account click "Edit" next to the user name.

To enable, disable, or remove an existing account, select the checkbox next to a user name and then choose an action.

To add a user, fill in user name, real name, and password under "Add a user..." and click "add account"

[More...](#)

Viewing User Accounts

User accounts are shown at the top of the screen under "User Accounts" User name, real name and status (enabled or disabled) are shown. You make modifications to an existing user account by first selecting the checkbox next to a user name and then choosing an action. (See "Editing a User Account" in this manual.)

Adding a User

To create a new user, do the following:

1. Under "Add a User," provide information in the following fields.

Fields	Description
Username	Provide a user name. User names are alphanumeric strings of up to 256 characters. Do not use special characters or spaces.

Fields	Description
Real Name	For information purposes, provide the user's full name. There is a 256 character limit on real names.
Password	Specify a password for this user. Passwords are alphanumeric strings of up to 256 characters. Do not use special characters or spaces.

2. When you have filled in the fields, click **Add Account** to add the account.

The new user is then displayed in the "User Accounts." The user account is *enabled* by default when you first create it.

A limit of 100 user accounts per access point is imposed by the Administration user interface. Network usage may impose a more practical limit, depending upon the demand from each user

Editing a User Account

Once you have created a user account, it is displayed under "User Accounts" at the top of the **User Management** Administration Web page. To make modifications to an existing user account, first click the checkbox next to the user name so that the box is checked.

Then, choose an action such Edit, Enable, Disable, or Remove.

Enabling and Disabling User Accounts

A user account must be enabled for the user to log on as a client and use the access point.

You can *enable* or *disable* any user account. With this feature, you can maintain a set of user accounts and authorize or prevent users from accessing the network without having to remove or recreate

User Accounts...

To edit a user account, click a user name.

To enable or disable a user, click the "enable" or "disable" button. Likewise, to remove a user, click the "remove" button. Ensure that you have selected at least one user prior to any of these actions.

Note: These user accounts apply only when the security mode is set to "IEEE 802.1x" or "WPA with RADIUS" and the Built-In authentication server is chosen. See the Help panel for more information.

<input type="checkbox"/>	Edit	User Name	Real Name	Status
<input checked="" type="checkbox"/>	[Edit]	samantha	Elizabeth Montgomery	enabled
<input type="checkbox"/>	[Edit]	endora	Agnes Moorhead	enabled

Selected users:

Add a user...

To add a user, fill in the fields below and click "add account".

User Name

Real Name

Password

Password (again for safety)

This can come in handy in situations where users have an occasional need to access the network. For example, contractors who do work for your company on an intermittent but regular basis might need network access for 3 months at a time, then be off for 3 months, and back on for another assignment. You can enable and disable these user accounts as needed, and control access as appropriate.

Enabling a User Account

To enable a user account, click the checkbox next to the user name and click **Enable**.

A user with an account that is *enabled* can log on to the wireless access points in your network as a client.

Disabling a User Account

To disable a user account, click the checkbox next to the user name and click **Disable**.

A user with an account that is *disabled* cannot log on to the wireless access points in your network as a client. However, the user remains in the database and can be enabled later as needed.

Removing a User Account

To remove a user account, click the checkbox next to the user name and click **Remove**.

If you think you might want to add this user back in at a later date, you might consider *disabling* the user rather than removing the account altogether.

Session Monitoring

The D-Link DWL-2210AP provides real-time session monitoring information including which clients are associated with a particular access point, data rates, transmit/receive statistics, signal strength, and idle time.

The following Session Monitoring topics are covered here:

- Navigating to Session Monitoring
- Understanding Session Monitoring Information
- Viewing Session Information for Access Points
- Sorting Session Information
- Refreshing Session Information

Navigating to Session Monitoring

To view session monitoring information, click the **Cluster > Sessions** tab.

The screenshot shows a web interface for monitoring active client station sessions. On the left is a navigation menu with options: Basic Settings, Cluster, Access Points, Users, Sessions (highlighted), Status, Interfaces, Events, and Statistics. The main content area is titled "Monitor active client station sessions" and contains a "Sessions..." section. Below this, there is a message: "You may sort the following table by clicking on any of the column names." A "Display" dropdown menu is set to "Idle Time" with a "Go" button next to it. Below the dropdown is a table with the following data:

User	AP Location	User MAC	Idle
samantha	not set	00:0c:41:dc:09:e1	120

Below the table, a note states: "The last column displayed in the sessions table may be changed by selecting an alternate field in the choice box above. Click the 'Go' button to apply the new selection." On the right side of the interface, there are two tabs: "Clustered" (selected) and "2 User Accounts". A help icon (?) is present, with a tooltip explaining that the page provides real-time session monitoring information including which clients are associated with a particular access point, along with idle time, data rates, signal strength, utilization, transmit/receive statistics, and error rates for each AP. A definition of a "session" is also provided: "A 'session' is the period of time in which a user on a client device (station) with a unique MAC address maintains a connection with the wireless network (but not necessarily to the same AP)." A "More..." link is visible at the bottom of the help tooltip.

Understanding Session Monitoring Information

The Sessions page shows information on client stations associated with access points in the cluster. Each client is identified by user name and user MAC address, along with the AP (location) to which it is currently connected.

To view a particular statistic for client sessions, select an item from the Display drop-down list and click **Go**. You can view information on Idle Time, Data Rate, Signal, Utilization, and so on; all of which are described in detail in the table below.

A “session” in this context is the period of time in which a user on a client device (station) with a unique MAC address maintains a connection with the wireless network. The session begins when the client logs on to the network, and the session ends when the client either logs off intentionally or loses the connection for some other reason.

A *session* is not the same as an *association*, which describes a client connection to a particular access point. A client network connection can shift from one clustered AP to another within the context of the same session. A client station can roam between APs and maintain the session. For information about monitoring *associations* and *link integrity monitoring*, see “Associated Wireless Clients” in this manual.

Details about the session information shown is described below.

Field	Description
User Name	Indicates the client user name of IEEE 802.1x clients. Note: This field is relevant only for clients that are connected to APs using IEEE 802.1x security mode <i>and</i> local authentication server. (For more information about this mode, see “IEEE 802.1x” in “Configuring Security” .) For clients of APs using IEEE 802.1x with RADIUS server or other security modes, no user name will be shown here.
AP Location	Indicates the location of the access point. This is derived from the location description specified on the Basic Settings tab.
User MAC Address	Indicates the MAC address of the user’s client device (station). A MAC address is a hardware address that uniquely identifies each node of a network.
Idle Time	Indicates the amount of time this station has remained inactive. A station is considered to be “idle” when it is not receiving or transmitting data.
Data Rate	The speed at which this access point is transferring data to the specified client. The data transmission rate is measured in <i>megabits per second</i> (Mbps)

Field	Description
Data Rate (continued)	This value should fall within the range of the advertised rate set for the IEEE 802.1x mode in use on the access point.
Signal	<p>Indicates the strength of the radio frequency (RF) signal the client receives from the access point.</p> <p>The measure used for this is an IEEE 802.1x value known as <i>Received Signal Strength Indication</i> (RSSI), and will be a value between 0 and 100.</p> <p>RSSI is determined by a an IEEE 802.1x mechanism implemented on the network interface card (NIC) of the client station.</p>
Utilization	<p>Utilization rate for this station.</p> <p>For example, if the station is “active” (transmitting and receiving data) 90% of the time and inactive 10% of the time, its “utilization rate” is 90%.</p>
Receive Total	Indicates number of total packets received by the client during the current session.
Transmit Total	Indicates number of total packets transmitted to the client during this session.
Error Rate	Indicates the percentage of time frames are dropped during transmission on this access point.

Viewing Session Information for Access Points

You can view session information for all access points on the network at the same time, or set the display to show session information for a specified access point chosen from the drop-down menu at the top of the screen.

To view information on all access points, select the **Show all access points** radio button at the top of the page.

To view session information on a particular access point, select the **Show only this access point** radio button and choose the access point name from the drop-down menu.

Sorting Session Information

To order (sort) the information shown in the tables by a particular indicator, click on the column label by which you want to order things. For example, if you want to see the table rows ordered by Utilization rate, click on the Utilization column label. The entries will be sorted by Utilization rate.

Refreshing Session Information

You can force an update of the information displayed on the Session Monitoring page by clicking the **Refresh** button.

Setting the Ethernet (Wired) Interface

Ethernet (Wired) Settings describe the configuration of your Ethernet local area network (LAN).

The Ethernet Settings, including guest access, are not shared across the cluster. These settings must be configured individually on the Administration pages for each access point. To get to the Administration pages for an access point that is a member of the current cluster, click on its IP Address link on the Cluster > Access Points page of the current AP. For more information about which settings are shared by the cluster and which are not, see “Which Settings are Shared as Part of the Cluster Configuration and Which Are Not?” in this manual.

The following sections describe how to configure “Wired” address and related settings on the D-Link DWL-2210AP:

- Navigating to Ethernet
- Setting the DNS Name
- Configuring an Internal LAN and a Guest Network
- Using VLANs for the Guest Network
- Configuring Internal Interface Ethernet Settings
- Configuring Guest Interface Ethernet Settings
- Updating Settings

Navigating to Ethernet

To set the wired address for an access point, navigate to the **Advanced > Ethernet** tab, and update the fields as described in the following pages.

Basic Settings
Modify Ethernet (Wired) settings
?

Cluster

Access Points

Users

Sessions

Status

Interfaces

Events

Statistics

Associations

Neighbors

Advanced

Ethernet

Wireless

Security

Guest Login

Radio

MAC Filtering

Load Balancing

QoS

WDS

DNS Name

Guest Access Enabled Disabled

Note: Enabling Guest access requires VLAN IDs to be specified.

Internal Interface Settings

MAC Address **00:00:88:E6:F6:C5**

VLAN ID

Connection Type DHCP

Static IP Address DHCP

Subnet Mask

Default Gateway

DNS Nameservers Dynamic Manual

Guest Interface Settings

MAC Address n/a

VLAN ID

Subnet n/a

Ethernet (Wired) settings describe the configuration of your Ethernet local area network (LAN), which is the Wired interface between the access point and the network.

Use this page to configure Guest and Internal networks to adhere as virtual LANs (with internal and guest VLAN IDs).

Specify the connection type (DHCP or Static IP addressing) for the Internal network.

The settings on this page (including guest access) are **not shared** across the cluster. You must configure these settings individually on each access point.

Caution: If you reconfigure the Guest and Internal interfaces to use VLANs, you may lose connectivity to the access point. Verify that the switch and DHCP server can support VLANs, and then re-connect to the new IP address.

[More...](#)

Setting the DNS Name

Field	Description
DNS Name	<p>Enter the DNS name for the access point in the text box.</p> <p>This is the host name. It may be provided by your ISP or network administrator, or you can provide your own.</p> <p>The rules for system names are:</p> <ul style="list-style-type: none">• This name can be up to 20 characters long.• Only letters, numbers and dashes are allowed.• The name must start with a letter and end with either a letter or a number.

Enabling or Disabling Guest Access

You can provide controlled guest access over an isolated network and a secure internal LAN on the same D-Link DWL-2210AP.

Configuring an Internal LAN and a Guest Network

A *Local Area Network* (LAN) is a communications network covering a limited area, for example, one floor of a building. A LAN connects multiple computers and other network devices like storage and printers.

Ethernet is the most common technology implementing a LAN. Wi-Fi (IEEE) is another very popular LAN technology.

The D-Link DWL-2210AP allows you to configure two different LANs on the same access point: one for a secure *internal* LAN and another for a public *guest* network with no security and little or no access to internal resources. To configure these networks, you need to provide both Wireless and Ethernet (Wired) settings.

Information on how to configure the Ethernet (Wired) settings is provided in the sections below.

(For information on how to configure the Wireless settings, see “Setting the Wireless Interface” in this manual. For an overview of how to set up the Guest interface, see “Setting up Guest Access” in this manual.)

Enabling or Disabling Guest Access

The D-Link DWL-2210AP ships with the Guest Access feature disabled by default. If you want to provide guest access on your AP, enable Guest access on the Ethernet tab.

Field	Description
Guest Access	By default, the D-Link DWL-2210AP ships with Guest Access disabled. <ul style="list-style-type: none">• To enable Guest Access, click Enabled.• To disable Guest Access, click Disabled.

Using VLANs for the Guest Network

If you enable Guest Access, two virtual LANs (VLANs) will be used: one for the Internal network and one for the Guest network. To use VLANs, the LAN port on the access point must be connected to a tagged port on a VLAN capable switch and then you must define two different Virtual LANs on this Administration page. (For more information, see “Setting up Guest Access” in this manual.)

Enabling Guest Access will enable the “VLAN” settings where you must provide a VLAN ID. See also “Configuring Guest Interface Ethernet Settings” in this manual.



If you enable Guest access and configure the Guest and Internal interfaces to use VLANs, you may lose connectivity to the access point. First, be sure to verify that the switch and DHCP server you are using can support VLANs per the IEEE 802.1Q standard. After configuring the VLAN on the Advanced > Ethernet page, physically reconnect the Ethernet cable on the switch to the tagged packet (VLAN) port. Then, reconnect via the Administration Web pages to the new IP address. (If necessary, check with the infrastructure support administrator regarding the VLAN and DHCP configurations.)

Configuring Internal Interface Ethernet Settings

To configure Ethernet (Wired) settings for the Internal LAN, fill in the fields as described below.

Field	Description
MAC Address	Shows the MAC address for the Internal interface for the Ethernet port on this access point. This is a read-only field that you cannot change.
VLAN ID	<p>If you configure enable Guest access and configure Internal and Guest networks on “VLANs”, this field will be enabled.</p> <p>Provide a number between 1 and 4094 for the Internal VLAN.</p> <p>This will cause the access point to send DHCP requests with the VLAN tag. The switch and the DHCP server must support VLAN IEEE 802.1Q frames. The access point must be able to reach the DHCP server.</p> <p>Check with the Administrator regarding the VLAN and DHCP configurations.</p>
Connection Type	<p>You can select “DHCP Client” or “Static IP”.</p> <p>The <i>Dynamic Host Configuration Protocol</i> (DHCP) is a protocol specifying how a centralized server can provide network configuration information to devices on the network. A DHCP server “offers” a “lease” to the client system. The information supplied includes the IP addresses and netmask plus the address of its DNS servers and gateway.</p> <p>Static IP indicates that all network settings are provided manually. You must provide the IP address for the D-Link DWL-2210AP, its subnet mask, the IP address of the default gateway, and the IP address of at least one DNS nameserver. If you select “DHCP Client”, the D-Link DWL-2210AP will acquire its IP Address, subnet mask, and DNS and gateway information from the DHCP Servers. Otherwise, if you select “Static IP”, fill in the items described in “Static IP Settings.”</p> <p>Caution: If you do not have a DHCP server on the Internal network and do not plan to use one, the first thing you must do after bringing up the AP is change the Connection Type from DHCP to Static IP. When you change the Connection Type to Static IP, you can either assign a new Static IP Address to the AP or continue using the default address. We recommend assigning a new address so that if later you bring up another D-Link DWL-2210AP on the same network, the IP addresses for the two APs will be unique.</p> <p>If you need to recover the default Static IP address, you can do so by resetting the AP to the factory defaults as described in “Resetting the Configuration” in this manual.</p>

Field	Description
Static IP Address enabled.	If you chose “Static IP” as the Connection Type, these fields will be enabled. Enter the Static IP Address in the text boxes.
Subnet Mask	Enter the Subnet Mask in the text boxes. You must obtain this information from your ISP or network administrator.
Default Gateway	Enter the Default Gateway in the text boxes.
DNS Nameservers	The <i>Domain Name Service</i> (DNS) is a system that resolves the descriptive name (<i>domain name</i>) of a network resource (for example, www.dlink.com) to its numeric IP address (for example, 66.93.138.219). A DNS server is called a <i>Nameserver</i> . There are usually two Nameservers; a Primary Nameserver and a Secondary Nameserver. You can choose Dynamic or Manual mode. <ul style="list-style-type: none"> • If you choose Manual, you should assign static IP addresses manually. • If you choose Dynamic, the IP addresses for the DNS servers will be assigned automatically via DHCP. (This option is only available if you specified DHCP for the Connection Type.)

Configuring Guest Interface Ethernet Settings

To configure Ethernet settings for the “Guest” interface, fill in the fields as described below.

Field	Description
MAC Address	Shows the MAC address for the Guest interface for the Ethernet port on this access point. This is a read-only field that you cannot change.
VLAN ID	If you enable Guest access and configure Internal and Guest networks by “VLANs”, this field will be enabled. Provide a number between 1 and 4094 for the Guest VLAN.

Updating Settings

To apply your changes, click **Update**.

Setting the Wireless Interface

Wireless settings describe aspects of the local area network (LAN) related specifically to the radio device in the access point (802.11 Mode and Channel) and to the network interface to the access point (MAC address for access point and wireless network name, also known as SSID).

The following sections describe how to configure the “Wireless” address and related settings on the D-Link DWL-2210AP:

- Navigating to Wireless Settings
- Configuring the Radio Interface
- Configuring “Internal” LAN Wireless Settings
- Configuring “Guest” Network Wireless Settings
- Updating Settings

Navigating to Wireless Settings

To set the wireless address for an access point, navigate to the **Advanced > Wireless** tab, and update the fields as described below.

The following figure shows the Wireless settings page for a two-radio AP. The Administration Web page for the single-radio AP will look slightly different.

Basic Settings | *Modify wireless settings*

Cluster

Access Points

Users

Sessions

Status

Interfaces

Events

Statistics

Associations

Neighbors

Advanced

Ethernet

Wireless

Radio Interface

Mode: IEEE 802.11b

Channel: 8

Internal Settings

MAC Address: 00:0C:41:0A:93:7E

SSID: default

Guest Settings

MAC Address: n/a

SSID: Guest Instant802 Network

? Wireless settings describe aspects of the local area network (LAN) related specifically to the radio device in the access point (802.11 Mode and Channel) and to the network interface to the access point (MAC address for access point and Wireless Network name, also known as SSID). For a complete set of Radio configuration options, go to the [Radio](#) tab. If you are setting up a Guest network, you need to specify network interfaces for both Internal and Guest networks. [More ...](#)

Configuring the Radio Interface

The radio interface allows you to set the radio Channel and 802.11 mode as described below.

Field	Description
<p>MAC Addresses (Shown on two-radio AP only)</p>	<p>Indicates the Media Access Control (MAC) addresses for the interface.</p> <p>A MAC address is a permanent, unique hardware address for any device that represents an interface to the network. The MAC address is assigned by the manufacturer. You cannot change the MAC address. It is provided here for informational purposes as a unique identifier for an interface.</p>
<p>Mode</p>	<p>The <i>Mode</i> defines the <i>Physical Layer</i> (PHY) standard being used by the radio.</p> <p>Select one of these modes:</p> <ul style="list-style-type: none"> • IEEE 802.11b • IEEE 802.11g
<p>Channel</p>	<p>Select the Channel. The range of channels and the default is determined by the Mode of the radio interface.</p> <p>The Channel defines the portion of the radio spectrum the radio uses for transmitting and receiving. Each mode offers a number of channels, dependent on how the spectrum is licensed by national and transnational authorities such as the Federal Communications Commission (FCC) or the International Telecommunication Union (ITU-R).</p> <p>The default is “Auto”, which picks the least busy channel at startup time.</p>

Configuring “Internal” LAN Wireless Settings

The Internal Settings describe the MAC Address (read-only) and Network Name (also known as the SSID) for the internal *Wireless LAN* (WLAN) as described below.

Field	Description
MAC Address	<p>Shows the MAC address(es) for Internal interface for this access point. This a read-only field that you cannot change.</p> <p>Although this access is point is physically a single device, it can be represented on the network as two or more nodes each with a unique MAC Address. This is accomplished by using multiple <i>Basic Service Set Identifiers</i> (BSSIDs) for a single access point.</p> <p>The MAC address(es) shown for the “Internal” access point is the BSSID(s) for the “Internal” interface.</p> <p>For the two-radio AP, two MAC addresses are shown: one for each Radio on the Internal interface.</p>
SSID	<p>Enter the SSID for the internal WLAN.</p> <p>The <i>Service Set Identifier</i> (SSID) is an alphanumeric string of up to 32 characters that uniquely identifies a wireless local area network. It is also referred to as the <i>Network Name</i>. There are no restrictions on the characters that may be used in an SSID.</p>

Configuring “Guest” Network Wireless Settings

The Guest Settings describe the MAC Address (read-only) and wireless network name (SSID) for the *Guest Network* as described below. Configuring an access point with two different network names (SSIDs) allows you to leverage the Guest interface feature on the D-Link DWL-2210AP. For more information, see “Setting up Guest Access” in this manual.

Field	Description
<p>MAC Address</p>	<p>Shows the MAC address for the Guest interface for this access point. This is a read-only field that you cannot change.</p> <p>Although this access point is physically a single device, it can be represented on the network as two or more nodes each with a unique MAC Address. This is accomplished by using multiple <i>Basic Service Set Identifiers</i> (BSSID) for a single access point.</p> <p>The MAC address(es) shown for the “Guest” access point is the BSSID(s) for the “Guest” interface.</p>
<p>SSID</p>	<p>Enter the SSID for the <i>guest network</i>.</p> <p>The <i>Service Set Identifier</i> (SSID) is an alphanumeric string of up to 32 characters that uniquely identifies a wireless local area network. It is also referred to as the <i>Network Name</i>. There are no restrictions on the characters that may be used in an SSID.</p> <p>For the guest network, provide an SSID that is different from the internal SSID and easily identifiable as the “guest” network.</p>

Updating Settings

To apply your changes, click **Update**.

Enabling the Network Time Protocol Server

The *Network Time Protocol* (NTP) is an Internet standard protocol that synchronizes computer clock times on your network. NTP servers transmit *Coordinated Universal Time* (UTC, also known as *Greenwich Mean Time*) to their client systems. NTP sends periodic time requests to servers, using the returned time stamp to adjust its clock.

The timestamp will be used to indicate the date and time of each event in log messages.

See <http://www.ntp.org> for more general information on NTP.

The following sections describe how to configure the D-Link DWL-2210AP to use a specified NTP server:

- Navigating to Time Protocol Settings
- Enabling or Disabling a Network Time Protocol (NTP) Server
- Updating Settings

Navigating to Time Protocol Settings

To enable an NTP server, navigate to the **Advanced > Time Protocol** tab, and update the fields as described below.

Basic Settings

Cluster

Access Points

Users

Sessions

Status

Interfaces

Events

Statistics

Associations

Neighbors

Advanced

Ethernet

Wireless

Security

Guest Login

Radio

MAC Filtering

Load Balancing

QoS

WDS

Time Protocol

Reboot

Reset

Upgrade

Modify how the access point discovers the time

Network Time Protocol (NTP) Enabled Disabled

NTP Server

?

Use this page to configure the access point to use a specified Network Time Protocol (NTP) server.

"NTP" is an Internet standard protocol that synchronizes computer clock times on a network.

NTP servers transmit Coordinated Universal Time (UTC, also known as Greenwich Mean Time) to their client systems. NTP sends periodic time requests to servers, using the returned time stamp to adjust its clock.

See <http://www.ntp.org> for more information on NTP.

[More ...](#)

Copyright © 2004 D-Link Systems, Inc. All rights reserved. Powered By **Instant802 Networks**

Enabling or Disabling a Network Time Protocol (NTP) Server

To configure your access point to use a network time protocol (NTP) server, first *enable* the use of NTP, and then select the NTP server you want to use. (To shut down NTP service on the network, disable NTP on the access point.)

Field	Description
Network Time Protocol	<p>NTP provides a way for the access point to obtain and maintain its time from a server on the network. Using an NTP server gives your AP the ability to provide the correct time of day in log messages and session information.</p> <p>(See http://www.ntp.org for more general information on NTP.)</p> <p>Choose to either enable or disable use of a network time protocol (NTP) server:</p> <ul style="list-style-type: none">• Enabled• Disabled
NTP Server	<p>If NTP is enabled, select the NTP server you want to use.</p> <p>You can specify the NTP server by host name or IP address, although using the IP address is not recommended as these can change more readily.</p>

Updating Settings

To apply your changes, click **Update**.

Configuring Security

The following sections describe how to configure Security settings on the D-Link DWL-2210AP:

- Understanding Security Issues on Wireless Networks
- How Do I Know Which Security Mode to Use?
- Comparison of Security Modes for Key Management, Authentication and Encryption Algorithms
- Does Prohibiting the Broadcast SSID Enhance Security?
- Navigating to Security Settings
- Configuring Security Settings
- Broadcast SSID and Security Mode
- Plaintext
- Static WEP
- IEEE 802.1x
- WPA with RADIUS
- WPA-PSK
- Updating Settings

Understanding Security Issues on Wireless Networks

Wireless mediums are inherently less secure than wired mediums. For example, an Ethernet NIC transmits its packets over a physical medium such as coaxial cable or twisted pair. A wireless NIC broadcasts radio signals over the air allowing a wireless LAN to be easily tapped without physical access or sophisticated equipment. A hacker equipped with a laptop, a wireless NIC, and a bit of knowledge can easily attempt to compromise your wireless network. One does not even need to be within normal range of the access point. By using a sophisticated antenna on the client, a hacker may be able to connect to the network from many miles away.

The D-Link DWL-2210AP provides a number of authentication and encryption schemes to ensure that your wireless infrastructure is accessed only by the intended users. The details of each security mode are described in the sections below.

See also the related topic, “Appendix A: Configuring Security Settings on Wireless Clients” in this manual.

How Do I Know Which Security Mode to Use?

In general, we recommend that on your Internal network you use the most robust security mode that is feasible in your environment. When configuring security on the access point, you first must choose the security mode, then in some modes an authentication algorithm, and whether to allow clients not using the specified security mode to associate.

Wi-Fi Protected Access (WPA) with Remote Authentication Dial-In User Service (RADIUS) using the CCMP (AES) encryption algorithm provides the best data protection available and is clearly the best choice if all client stations are equipped with WPA supplicants. However, backward compatibility or interoperability issues with clients or even with other access points may require that you configure WPA with RADIUS with a different encryption algorithm or choose one of the other security modes.

That said, however, security may not be as much of a priority on some types of networks. If you are simply providing internet and printer access, as on a guest network, plain text mode (no security) may be the appropriate choice. To prevent clients from accidentally discovering and connecting to your network, you can disable the broadcast SSID so that your network name is not advertised. If the network is sufficiently isolated from access to sensitive information, this may offer enough protection in some situations. This level of protection is the only one offered for guest networks, and also may be the right convenience trade-off for other scenarios where the priority is making it as easy as possible for clients to connect. (See “Does Prohibiting the Broadcast SSID Enhance Security?” in this manual.)

Following is a brief discussion of what factors make one mode more secure than another, a description of each mode offered, and when to use each mode.

Comparison of Security Modes for Key Management, Authentication and Encryption Algorithms

Three major factors that determine the effectiveness of a security protocol are:

- How the protocol manages keys
- Presence or absence of integrated user authentication in the protocol
- Encryption algorithm or formula the protocol uses to encode/decode the data

Following is a list of the security modes available on the D-Link DWL-2210AP along with a description of the key management, authentication, and encryption algorithms used in each mode. We include some suggestions as to when one mode might be more appropriate than another.

- When to Use Plain Text
- When to Use Static WEP
- When to Use IEEE 802.1x
- When to Use WPA with RADIUS
- When to Use WPA-PSK

When to Use Plain Text

Plain text mode by definition provides no security. In this mode, the data is not encrypted but rather sent as “plain text” across the network. No key management, data encryption or user authentication is used.

Recommendations

Plain text mode is **not recommended** for regular use on the Internal network because it is not secure.

Plain text mode is the only mode in which you can run the Guest network, which is by definition an unsecure LAN always virtually or physically separated from any sensitive information on the Internal LAN.

Therefore, use plain text mode on the Guest network, and on the Internal network for initial setup, testing, or problem solving only.

See Also

For information on how to configure plain text mode, see “Plaintext” under “Configuring Security Settings” in this manual.

When to Use Static WEP

Static *Wired Equivalent Privacy* (WEP) is a data encryption protocol for 802.11 wireless networks. All wireless stations and access points on the network are configured with a static 64-bit (40-bit secret key + 24-bit initialization vector (IV) or 128-bit (104-bit secret key + 24-bit IV) Shared Key for data encryption.

Key Management	Encryption Algorithm	User Authentication
<p>Static WEP uses a fixed key that is provided by the administrator. WEP keys are indexed in different slots (up to four on the D-Link DWL -2210AP).</p> <p>The client stations must have the same key indexed in the same slot to access data on the access point.</p>	<p>An RC4 stream cipher is used to encrypt the frame body and <i>cyclic redundancy checking</i> (CRC) of each 802.11 frame.</p>	<p>If you set the Authentication Algorithm to Shared Key, this protocol provides a rudimentary form of user authentication.</p> <p>However, if the Authentication Algorithm is set to “Open System”, no authentication is performed.</p> <p>If the algorithm is set to “Both”, only WEP clients are authenticated.</p>

Recommendations

Static WEP was designed to provide the security equivalent of sending unencrypted data through an Ethernet connection, however it has major flaws and it does not provide even this intended level of security.

Therefore, **Static WEP is not recommended** as a secure mode. The only time to use Static WEP is when interoperability issues make it the only option available to you and you are not concerned with the potential of exposing the data on your network.

See Also

For information on how to configure Static WEP security mode, see “Static WEP” under “Configuring Security Settings” in this manual.

When to Use IEEE 802.1x

IEEE 802.1x is the standard for passing the Extensible Authentication Protocol (EAP) over an 802.11 wireless network using a protocol called EAP Encapsulation Over LANs (EAPOL). This is a newer, more secure standard than static WEP.

Key Management Encryption Algorithm

User Authentication

<p>IEEE 802.1x provides dynamically-generated keys that are periodically refreshed.</p> <p>There are different Unicast keys for each station.</p>	<p>An RC4 stream cipher is used to encrypt the frame body and <i>cyclic redundancy checking</i> (CRC) of each 802.11 frame.</p>	<p>IEEE 802.1x mode supports a variety of authentication methods, like certificates, Kerberos, and public key authentication with a RADIUS server.</p> <p>You have a choice of using the D-Link DWL-2210AP embedded RADIUS server or an external RADIUS server. The embedded RADIUS server supports Protected EAP (PEAP) and MSCHAP V2.</p>
---	---	---

Recommendations

IEEE 802.1x mode is a better choice than Static WEP because keys are dynamically generated and changed periodically. However, the encryption algorithm used is the same as that of Static WEP and is therefore not as reliable as the more advanced encryption methods such as TKIP and CCMP (AES) used in *Wi-Fi Protected Access* (WPA).

Additionally, compatibility issues may be cumbersome because of the variety of authentication methods supported and the lack of a standard implementation method.

Therefore, IEEE 802.1x mode is not as secure a solution as *Wi-Fi Protected Access* (WPA). If, you cannot use WPA because some of your client stations do not have WPA, then a better solution than using IEEE 802.1x mode is to **use WPA with RADIUS mode instead and check the “Allow non-WPA IEEE 802.1x clients” checkbox** to allow non-WPA clients. This way, you get the benefit of IEEE 802.1x key management for non-WPA clients along with even better data protection of TKIP and CCMP (AES) key management and encryption algorithms for your WPA clients.

See Also

For information on how to configure IEEE 802.1x security mode, see “IEEE 802.1x” under “Configuring Security Settings” in this manual.

When to Use WPA with RADIUS

Wi-Fi Protected Access (WPA) with *Remote Authentication Dial-In User Service* (RADIUS) is a Wi-Fi Alliance subset of IEEE 802.11i, which includes *Temporal Key Integrity Protocol* (TKIP), *Counter mode/CBC-MAC Protocol* (CCMP), and *Advanced Encryption Standard* (AES) mechanisms. This mode requires the use of a RADIUS server to authenticate users. WPA with RADIUS provides the best security available for wireless networks.

Key Management Encryption Algorithm

User Authentication

WPA with RADIUS provides dynamically generated keys that are periodically refreshed.

There are different Unicast keys for each station.

- *Temporal Key Integrity Protocol (TKIP)*
- *Counter mode/CBC-MAC Protocol (CCMP) Advanced Encryption Standard (AES)*

Remote Authentication Dial-In User Service (RADIUS).

You have a choice of using the D-Link DWL-2210AP embedded RADIUS server or an external RADIUS server. The embedded RADIUS server supports Protected EAP (PEAP) and MSCHAP V2.

Recommendations

WPA with RADIUS mode is the **recommended mode**. The CCMP (AES) and TKIP encryption algorithms used with WPA modes are far superior to the RC4 algorithm used for Static WEP or IEEE 802.1x modes. Therefore, CCMP (AES) or TKIP should be used whenever possible. All WPA modes allow you to use these encryption schemes, so WPA security modes are recommended above the others when using WPA is an option.

Additionally, this mode (WPA with RADIUS) incorporates a RADIUS server for user authentication which gives it an edge over WPA-PSK.

Use the following guidelines for choosing options within the WPA with RADIUS security mode:

1. The best security you can have to date on a wireless network is WPA with RADIUS using CCMP (AES) encryption algorithm. AES is a symmetric 128-bit block data encryption technique that works on multiple layers of the network. It is the most effective encryption system currently available for wireless networks. If all clients or other APs on the network are WPA/CCMP compatible, use this encryption algorithm.
2. The second best choice is WPA with RADIUS with the encryption algorithm set to “Both” (that is, both TKIP and CCMP). This lets WPA client stations without CCMP associate, uses TKIP for encrypting Multicast and Broadcast frames, and allows clients to select whether to use CCMP or TKIP for Unicast (AP-to-single-station) frames. This WPA configuration allows more interoperability, at the expense of some security. Client stations that support CCMP can use it for their Unicast frames. If you encounter AP-to-station interoperability problems with the “Both” encryption algorithm setting, then you will need to select TKIP instead.
3. The third best choice is WPA with RADIUS with the encryption algorithm set to TKIP. Some clients have interoperability issues with CCMP and TKIP enabled at the same time. If you encounter this problem, then choose TKIP as the encryption algorithm. This is the standard WPA mode, and most interoperable mode with client Wireless software security features. TKIP is the only encryption algorithm that is being tested in Wi-Fi WPA certification.

If there are older client stations on your network that do not support WPA, you can configure WPA with RADIUS (with Both, CCMP, or TKIP) and check the “Allow non-WPA IEEE 802.1x clients” checkbox to allow non-WPA clients. This way, you get the benefit of IEEE 802.1x key management for non-WPA clients along with even better data protection of TKIP and CCMP (AES) key management and encryption algorithms for your WPA clients.

A typical scenario is that one is upgrading a current 802.1x network to use WPA. You might have a mix of clients; some new clients that support WPA and some older ones that do not support WPA. You might even have other access points on the network that support only 802.1x and some that support WPA with RADIUS. For as long as this mix persists, use the “Allow non-WPA IEEE 802.1x clients” option.

When all the stations have been upgraded to use WPA, you should disable the “Allow non-WPA IEEE 802.1x clients” option.

See Also

For information on how to configure WPA with RADIUS security mode, see “WPA with RADIUS” under “Configuring Security Settings” in this manual.

When to Use WPA-PSK

Wi-Fi Protected Access (WPA) with Pre-Shared Key (PSK) is a Wi-Fi Alliance subset of IEEE 802.11i, which includes *Temporal Key Integrity Protocol (TKIP) Advanced Encryption Algorithm (AES)*, and *Counter mode/CBC-MAC Protocol (CCMP)* mechanisms. This mode offers the same encryption algorithms as WPA with RADIUS but without the ability to integrate a RADIUS server for user authentication.

Key Management	Encryption Algorithm	User Authentication
<p>WPA-PSK provides dynamically-generated keys that are periodically refreshed.</p> <p>There are different Unicast keys for each station.</p>	<ul style="list-style-type: none"> • <i>Temporal Key Integrity Protocol (TKIP)</i> • <i>Counter mode/CBC-MAC Protocol (CCMP) Advanced Encryption Standard (AES)</i> 	<p>The use of a Pre-Shared (PSK) key provides user authentication similar to that of shared keys in WEP.</p>

Recommendations

WPA w/PSK not recommended for use with the D-Link DWL-2210AP when WPA with RADIUS is an option.

We recommend that you use WPA with RADIUS mode instead, unless you have interoperability issues that prevent you from using this mode.

For example, some devices on your network may not support WPA with EAP talking to a RADIUS server. Embedded printer servers or other small client devices with very limited space for implementation may not support RADIUS. For such cases, we recommend that you use WPA-PSK.

See Also

For information on how to configure WPA-PSK security mode, see “WPA-PSK” under “Configuring Security Settings” in this manual.

Does Prohibiting the Broadcast SSID Enhance Security?

You can suppress (prohibit) this broadcast to discourage stations from automatically discovering your access point. When the AP’s broadcast SSID is suppressed, the network name will not be displayed in the List of Available Networks on a client station. Instead, the client must have the exact network name configured in the supplicant before it will be able to connect.

Disabling the broadcast SSID is sufficient to prevent clients from accidentally connecting to your network, but it will not prevent even the simplest of attempts by a hacker to connect, or monitor plain text traffic.

This offers a very minimal level of protection on an otherwise exposed network (such as a guest network) where the priority is making it easy for clients to get a connection and where no sensitive information is available.

(See also “Guest Network” in this manual.)

Navigating to Security Settings

To set the security mode, navigate to the **Advanced > Security** tab, and update the fields as described below.

Modify security settings that apply to the Internal Network

Broadcast SSID Allow Prohibit

Security Mode WPA with RADIUS

Cipher Suites TKIP

Authentication Server Built-in

Radius IP 127 . 0 . 0 . 1

Radius Key XXXXXXXXXX

Enable radius accounting

Allow non-WPA IEEE 802.1x clients

Update [More ...](#)

? Use this page to configure a security mode for the access point:

Plain-text mode (no security)

Static Wired Equivalent Privacy (WEP)

IEEE 802.1x

Wi-Fi Protected Access (WPA) with Remote Authentication Dial-In User Service (RADIUS)

WPA with Pre-Shared Key (PSK).

WPA with RADIUS is the recommended mode because it leverages TKIP and CCMP(AES) encryption algorithms and dynamic pre-shared keys. The D-Link® DWL2210AP uses an embedded RADIUS server so you do not need to provide one.

The plain-text, non-secure mode is only recommended for initial setup or problem-solving use.

These settings apply to the Internal network; the Guest network always uses plain-text mode.

Configuring Security Settings

The following configuration information explains how to configure security modes on the access point. Keep in mind that each wireless client that wants to exchange data with the access point must be configured with the same security mode and encryption key settings consistent with access point security.

On a two-radio AP, these security settings apply to both radios.

Security modes other than Plaintext apply only to configuration of the “Internal” network. On the “Guest” network, you can use only Plaintext mode. (For more information about guest networks, see “Setting up Guest Access” in this manual.)

Broadcast SSID and Security Mode

To configure security on the access point, select a security mode and fill in the related fields as described in the following table. (Note you can also allow or prohibit the Broadcast SSID as an extra precaution as mentioned below.)

Field	Description
Broadcast SSID	<p>Select the Broadcast SSID setting by clicking the “Allow” or “Prohibit” radio button.</p> <p>By default, the access point broadcasts (allows) the <i>Service Set Identifier</i> (SSID) in its beacon frames.</p> <p>You can suppress (prohibit) this broadcast to discourage stations from automatically discovering your access point. When the AP’s broadcast SSID is suppressed, the network name will not be displayed in the List of Available Networks on a client station. Instead, the client must have the exact network name configured in the supplicant before it will be able to connect.</p>
Security Mode	<p>Select the Security Mode. Select one of the following:</p> <ul style="list-style-type: none"> • Plaintext • Static WEP • IEEE 802.1x • WPA with RADIUS • WPA-PSK <p>For a Guest network, only the “Plaintext” setting can be used. (For more information, see “Setting up Guest Access” in this manual.) Security modes other than Plaintext apply only to configuration of the “Internal” network; on the Guest network, you can use only Plaintext mode.</p>

Plaintext

Plain Text means any data transferred to and from the D-Link DWL-2210AP is not encrypted.

There are no further options for “Plaintext” mode.

Plain text mode can be useful during initial network configuration or for problem solving, but it is not recommended for regular use on the Internal network because it is not secure.

Guest Network

Plain text mode is the only mode in which you can run the Guest network, which is by definition an easily accessible, unsecure LAN always virtually or physically separated from any sensitive information on the Internal LAN. For example, the guest network might simply provide internet and printer access for day visitors.

The absence of security on the Guest AP is designed to make it as easy as possible for guests to get a connection without having to program any security settings in their clients.

For a minimum level of protection on a guest network, you can choose to suppress (prohibit) the broadcast of the SSID (network name) to discourage client stations from automatically discovering your access point. (See also “Does Prohibiting the Broadcast SSID Enhance Security?” in this manual). For more about the Guest network, see “Setting up Guest Access” in this manual.

Static WEP

Wired Equivalent Privacy (WEP) is a data encryption protocol for 802.11 wireless networks. All wireless stations and access points on the network are configured with a static 64-bit (40-bit secret key + 24-bit initialization vector (IV)) or 128-bit (104-bit secret key + 24-bit IV) Shared Key for data encryption.

You cannot mix 64-bit and 128-bit WEP keys between the access point and its client stations. Static WEP is not the most secure mode available, but it offers more protection than plaintext mode as it does prevent an outsider from easily sniffing out unencrypted wireless traffic. (For more secure modes, see the sections on “IEEE 802.1x,” “WPA with RADIUS,” or “WPA-PSK” in this manual. WEP encrypts data moving across the wireless network based on a static key. (The encryption algorithm is a “stream” cipher called RC4.)

The access point uses a key to transmit data to the client stations. Each client station must use that same key to decrypt data it receives from the access point.

Client stations can use different keys to transmit data to the access point. (Or they can all use the same key, but this is less secure because it means one station can decrypt the data being sent by another.)

If you selected “Static WEP” Security Mode, provide the following on the access point settings:

Security Mode

Transfer Key Index

Key Length 64 bits 128 bits

Key Type ASCII Hex

Characters Required

WEP Keys

1:

2:

3:

4:

Authentication Algorithms

Field	Description
Transfer Key Index	<p>Select a key index from the drop-down menu. Key indexes 1 through 4 are available. The default is 1.</p> <p>The Transfer Key Index indicates which WEP key the access point will use to encrypt the data it transmits.</p>
Key Length	<p>Specify the length of the key by clicking one of the radio buttons:</p> <ul style="list-style-type: none"> • 64-bits • 128-bits
Key Type	<p>Select the key type by clicking one of the radio buttons:</p> <ul style="list-style-type: none"> • ASCII • Hex
Characters Required	<p>Indicates the number of characters required in the WEP key.</p> <p>The number of characters required updates automatically based on how you set Key Length and Key Type.</p>
WEP Keys	<p>You can specify up to four WEP keys. In each text box, enter a string of characters for each key.</p> <p>If you selected “ASCII”, enter any combination of integers and letters 0-9, a-z, and A-Z. If you selected “HEX”, enter hexadecimal digits (any combination of 0-9 and a-f or A-F).</p> <p>Use the same number of characters for each key as specified in the “Characters Required” field. These are the RC4 WEP keys shared with the stations using the access point.</p> <p>Each client station must be configured to use one of these same WEP keys in the same slot as specified here on the AP. (See “Rules to Remember for Static WEP” in this manual.)</p>

Field	Description
Authentication Algorithm	<p>The authentication algorithm defines the method used to determine whether a client station is allowed to associate with an access point when static WEP is the security mode.</p> <p>Specify the authentication algorithm you want to use by choosing one of the following from the drop-down menu:</p> <ul style="list-style-type: none">• Open System• Shared Key• Both <p>Open System authentication allows any client station to associate with the access point whether that client station has the correct WEP key or not. This algorithm is also used in plaintext, IEEE 802.1x, and WPA modes. When the authentication algorithm is set to “Open System”, any client can associate with the access point.</p> <p>Note that just because a client station is allowed to <i>associate</i> does not ensure it can exchange traffic with an access point. A station must have the correct WEP key to be able to successfully access and decrypt data from an access point, and to transmit readable data to the access point.</p> <p>Shared Key authentication requires the client station to have the correct WEP key in order to associate with the access point. When the authentication algorithm is set to “Shared Key”, a station with an incorrect WEP key will not be able to associate with the access point.</p> <p>Both is the default. When the authentication algorithm is set to “Both”:</p> <ul style="list-style-type: none">• Client stations configured to use WEP in shared key mode must have a valid WEP key in order to associate with the access point.• Client stations configured to use WEP as an open system (shared key mode not enabled) will be able to associate with the access point even if they do not have the correct WEP key.

Rules to Remember for Static WEP

- All client stations must have the Wireless LAN (WLAN) security set to WEP and all clients must have one of the WEP keys specified on the AP in order to decode AP-to-station data transmissions.
- The AP must have all keys used by clients for station-to-AP transmit so that it can decode the station transmissions.
- The same key must occupy the same slot on all nodes (AP and clients). For example if the AP defines abc123 key as WEP key 3, then the client stations must define that same string as WEP key 3.
- On some wireless client software (like Funk Odyssey), you can configure multiple WEP keys and define a client station “transfer key index”, and then set the stations to encrypt the data they transmit using different keys. This ensures that neighboring APs cannot decode each other’s transmissions.

Example of Using Static WEP

For a simple example, suppose you configure three WEP keys on the access point. In our example, the Transfer Key Index for the AP is set to “3”. This means that the WEP key in slot “3” is the key the access point will use to encrypt the data it sends.

Setting the AP Transfer Key on the Access Point

Security Mode

Transfer Key Index

Key Length 64 bits 128 bits

Key Type ASCII Hex

Characters Required

WEP Keys

1:

2:

3:

4:

Authentication Algorithms

You must then set all client stations to use WEP and provide each client with one of the slot/key combinations you defined on the AP.

For this example, we’ll set WEP key 1 on a Windows client.
(Please see the next page.)

Providing a Wireless Client with a WEP Key

If you have a second client station, that station also needs to have one of the WEP keys defined on the AP.

You could give it the same WEP key you gave to the first station. Or for a more secure solution, you could give the second station a different WEP key (key 2, for example) so that the two stations cannot decrypt each other's transmissions.

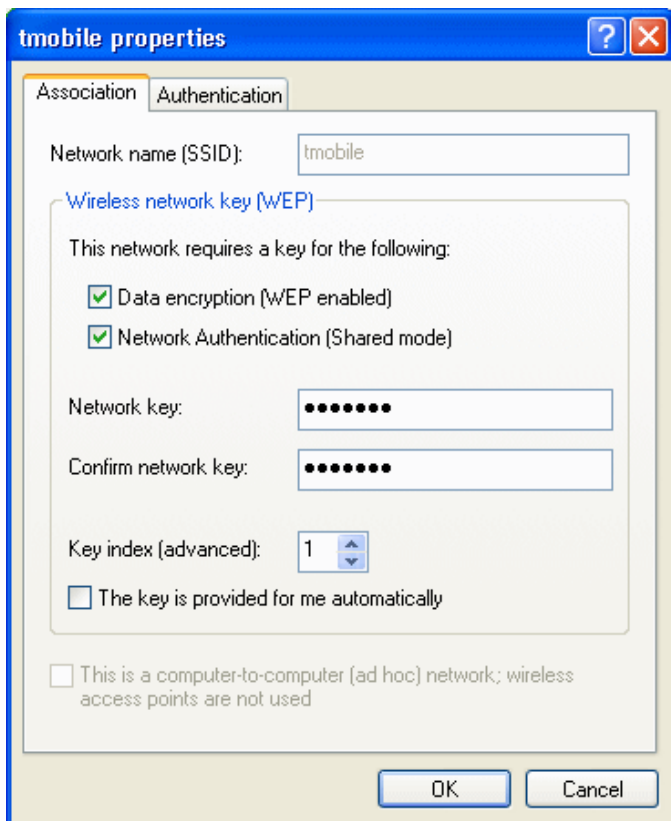
Static WEP with Transfer Key Indexes on Client Stations

Some wireless client software (like Funk Odyssey) lets you configure multiple WEP keys and set a transfer key index on the client station, then you can specify different keys to be used for station-to-AP transmissions.

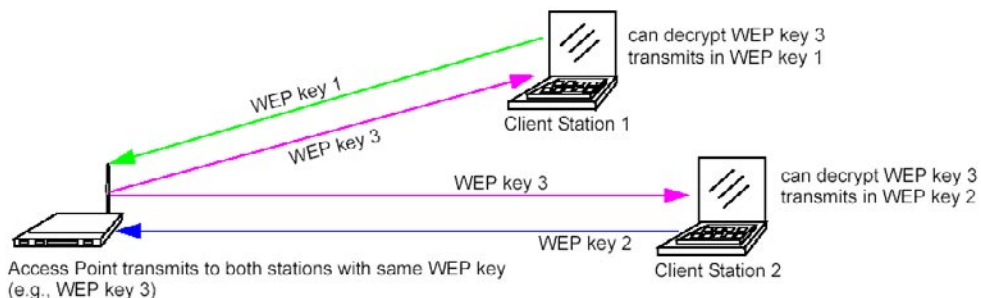
(The standard Windows wireless client software does not allow you to do this.)

To build on our example, using Funk Odyssey client software you could give each of the clients WEP key 3 so that they can decode the AP transmissions with that key and also give client 1 WEP key 1 and set this as its transfer key. You could then give client 2 WEP key 2 and set this as its transfer key index.

The figure on the next page illustrates the dynamics of the AP and two client stations using multiple WEP keys and a transfer key index.



Example of Using Multiple WEP Keys and Transfer Key Index on Client Stations



IEEE 802.1x

IEEE 802.1x is the standard defining port-based authentication and infrastructure for doing key management. Extensible Authentication Protocol (EAP) messages sent over an IEEE 802.11 wireless network using a protocol called EAP Encapsulation Over LANs (EAPOL). IEEE 802.1x provides dynamically-generated keys that are periodically refreshed. An RC4 stream cipher is used to encrypt the frame body and cyclic redundancy checking (CRC) of each 802.11 frame.

This mode requires the use of a RADIUS server to authenticate users, and configuration of user accounts via the Cluster > Users tab.

The access point requires a RADIUS server capable of EAP, such as the Microsoft Internet Authentication Server or the D-Link DWL-2210AP internal authentication server. To work with Windows clients, the authentication server must support Protected EAP (PEAP) and MSCHAP V2.

When configuring IEEE 802.1x mode, you have a choice of whether to use the embedded RADIUS server or an external RADIUS server that you provide. The D-Link DWL-2210AP embedded RADIUS server supports Protected EAP (PEAP) and MSCHAP V2.

If you use your own RADIUS server, you have the option of using any of a variety of authentication methods that the IEEE 802.1x mode supports, including certificates, Kerberos, and public key authentication. Keep in mind, however, that the client stations must be configured to use the same authentication method being used by the access point.

If you selected “IEEE 802.1x” Security Mode, provide the following:

Security Mode

Authentication Server

Radius IP . . .

Radius Key

Enable radius accounting

Field	Description
<p>Authentication Server</p>	<p>Select one of the following from the drop-down menu:</p> <ul style="list-style-type: none"> • Built-in - To use the authentication server provided with the D-Link DWL-2210AP. If you choose this option, you do not have to provide the Radius IP and Radius Key; they are automatically provided. • External - To use an external authentication server. If you choose this option you must supply a Radius IP and Radius Key of the server you want to use. <p>Note: The RADIUS server is identified by its IP address and UDP port numbers for the different services it provides. On the current release of the D-Link DWL-2210AP, the RADIUS server User Datagram Protocol (UDP) ports used by the access point are not configurable. (The D-Link DWL-2210AP is hard-coded to use RADIUS server UDP port 1812 for authentication and port 1813 for accounting.)</p>
<p>Radius IP</p>	<p>Enter the Radius IP in the text box.</p> <p>The <i>Radius IP</i> is the IP address of the RADIUS server.</p> <p>(The D-Link DWL-2210AP internal authentication server is 127.0.0.1.)</p> <p>For information on setting up user accounts, see “Managing User Accounts” in this manual.</p>
<p>Radius Key</p>	<p>Enter the Radius Key in the text box.</p> <p>The <i>Radius Key</i> is the shared secret key for the RADIUS server. The text you enter will be displayed as “*” characters to prevent others from seeing the RADIUS key as you type.</p> <p>(The D-Link DWL-2210AP internal authentication server key is secret.)</p> <p>This value is never sent over the network.</p>
<p>Enable RADIUS Accounting</p>	<p>Click “Enable RADIUS Accounting” if you want to track and measure the resources a particular user has consumed such system time, amount of data transmitted and received, and so on.</p>

WPA with RADIUS

Wi-Fi Protected Access (WPA) with Remote Authentication Dial-In User Service (RADIUS) is a Wi-Fi Alliance subset of IEEE 802.11i, which includes Temporal Key Integrity Protocol (TKIP), Counter mode/ CBC-MAC Protocol (CCMP), and Advanced Encryption Standard (AES) mechanisms. This mode requires the use of a RADIUS server to authenticate users, and configuration of user accounts via the Cluster > Users tab.

When configuring WPA with RADIUS mode, you have a choice of whether to use the embedded RADIUS server or an external RADIUS server that you provide. The D-Link DWL-2210AP embedded RADIUS server supports Protected EAP (PEAP) and MSCHAP V2.

If you selected “WPA with RADIUS” **Security Mode**, provide the following:

Security Mode ▼

Cipher Suites ▼

Authentication Server ▼

Radius IP . . .

Radius Key

Enable radius accounting

Allow non-WPA IEEE 802.1x clients

Field	Description
Cipher Suites	<p>Select the cipher you want to use from the drop-down menu:</p> <ul style="list-style-type: none"> • TKIP • CCMP (AES) • Both <p>Temporal Key Integrity Protocol (TKIP) is the default.</p> <p>TKIP provides a more secure encryption solution than WEP keys. The TKIP process more frequently changes the encryption key used and better ensures that the same key will not be reused to encrypt data (a weakness of WEP). TKIP uses a 128-bit “temporal key” shared by clients and access points. The temporal key is combined with the client’s MAC address and a 16-octet initialization vector to produce the key that will encrypt the data. This ensures that each client station uses a different key to encrypt data. TKIP uses RC4 to perform the encryption, which is the same as WEP. But TKIP changes temporal keys every 10,000 packets and distributes them, thereby greatly improving the security of the network.</p> <p>Counter mode/CBC-MAC Protocol (CCMP) is an encryption method for IEEE 802.11i that uses the Advanced Encryption Algorithm (AES). It uses a CCM combined with Cipher Block Chaining Counter mode (CBC-CTR) and Cipher Block Chaining Message Authentication Code (CBC-MAC) for encryption and message integrity.</p> <p>When the authentication algorithm is set to “Both”, both TKIP and AES clients can associate with the access point. Client stations configured to use WPA with RADIUS must have one of the following to be able to associate with the AP:</p> <ul style="list-style-type: none"> • A valid TKIP RADIUS IP address and valid shared Key • A valid CCMP (AES) IP address and valid shared Key <p>Clients not configured to use WPA with RADIUS will not be able to associate with AP.</p> <p>Both is the default. When the authentication algorithm is set to “Both”, client stations configured to use WPA with RADIUS must have one of the following:</p> <ul style="list-style-type: none"> • A valid TKIP RADIUS IP address and RADIUS Key • A valid CCMP (AES) IP address and RADIUS Key

Field	Description
Authentication Server	<p>Select one of the following from the drop-down menu:</p> <ul style="list-style-type: none"> • Built-in - To use the authentication server provided with the D-Link DWL-2210AP. If you choose this option, you do not have to provide the Radius IP and Radius Key; they are automatically provided. • External - To use an external authentication server. If you choose this option you must supply a Radius IP and Radius Key of the server you want to use. <p>Note: The RADIUS server is identified by its IP address and UDP port numbers for the different services it provides. On the current release of the D-Link DWL-2210AP, the RADIUS server User Datagram Protocol (UDP) ports used by the access point are not configurable. (The D-Link DWL-2210AP is hard-coded to use RADIUS server UDP port 1812 for authentication and port 1813 for accounting.)</p>
Radius IP	<p>Enter the Radius IP in the text box.</p> <p>The <i>Radius IP</i> is the IP address of the RADIUS server. (The D-Link DWL-2210AP internal authentication server is 127.0.0.1.)</p> <p>For information on setting up user accounts, see “Managing User Accounts” in this manual.</p>
Radius Key	<p>Enter the Radius Key in the text box.</p> <p>The <i>Radius Key</i> is the shared secret key for the RADIUS server. The text you enter will be displayed as “*” characters to prevent others from seeing the RADIUS key as you type.</p> <p>(The D-Link DWL-2210AP internal authentication server key is secret.)</p> <p>This value is never sent over the network.</p>
Key Type	<p>Select the key type by clicking one of the radio buttons:</p> <ul style="list-style-type: none"> • ASCII • HEX
Enable RADIUS Accounting	<p>Click “Enable RADIUS Accounting” if you want to enforce authentication for WPA client stations with user names and passwords for each station.</p> <p>See also “Managing User Accounts” in this manual.</p>
Allow non-WPA Clients	<p>Click the “Allow non-WPA clients” checkbox if you want to let non-WPA (802.11), unauthenticated client stations use this access point.</p>

WPA-PSK

Wi-Fi Protected Access (WPA) with *Pre-Shared Key (PSK)* is a Wi-Fi Alliance subset of IEEE 802.11i, which includes *Temporal Key Integrity Protocol (TKIP)*, *Advanced Encryption Algorithm (AES)*, and *Counter mode/CBC-MAC Protocol (CCMP)* mechanisms. PSK employs a pre-shared key. This is used for an initial check of credentials only. If you selected “WPA-PSK” **Security Mode**, provide the following:

Security Mode

Cipher Suites

Key

Field	Description
Cipher Suites	<p>Select the cipher you want to use from the drop-down menu:</p> <ul style="list-style-type: none"> • TKIP • CCMP (AES) • Both <p>Temporal Key Integrity Protocol (TKIP) is the default. TKIP provides a more secure encryption solution than WEP keys. The TKIP process more frequently changes the encryption key used and better ensures that the same key will not be reused to encrypt data (a weakness of WEP). TKIP uses a 128-bit “temporal key” shared by clients and access points. The temporal key is combined with the client’s MAC address and a 16-octet initialization vector to produce the key that will encrypt the data. This ensures that each client station uses a different key to encrypt data. TKIP uses RC4 to perform the encryption, which is the same as WEP. But TKIP changes temporal keys every 10,000 packets and distributes them, thereby greatly improving the security of the network.</p> <p>Counter mode/CBC-MAC Protocol (CCMP) is an encryption method for IEEE 802.11i that uses the Advanced Encryption Algorithm (AES). It uses a CCM combined with Cipher Block Chaining Counter mode (CBC-CTR) and Cipher Block Chaining Message Authentication Code (CBC-MAC) for encryption and message integrity.</p> <p>When the authentication algorithm is set to “Both”, both TKIP and AES clients can associate with the access point. WPA clients must have one of the following to be able to associate with the AP:</p> <ul style="list-style-type: none"> • A valid TKIP key • A valid CCMP (AES) key
Key	<p>Clients not configured to use WPA-PSK will not be able to associate with AP. The <i>Pre-shared Key</i> is the shared secret key for WPA-PSK. Enter a string of at least 8 characters to a maximum of 63 characters.</p>

Updating Settings

To apply your changes, click **Update**.

Configuring Radio Settings

The following sections describe how to configure Radio Settings on the D-Link DWL-2210AP:

- Understanding Radio Settings
- Configuring Radio Settings
- Updating Settings

Understanding Radio Settings

Radio settings directly control the behavior of the radio device in the access point and its interaction with the physical medium; that is, how/what type of electromagnetic waves the AP emits. You can specify whether the radio is on or off, radio frequency (RF) broadcast channel, beacon interval (amount of time between AP beacon transmissions), transmit power, IEEE 802.11 mode in which the radio operates, and so on.

The D-Link DWL-2210AP is a single band access point with one radio capable of broadcasting in either IEEE 802.11b or IEEE 802.11g mode.

The IEEE mode along with other radio settings are configured as described in “Navigating to Radio Settings” and “Configuring Radio Settings” in this manual.

Navigating to Radio Settings

To specify radio settings, navigate to **Advanced > Radio** tab, and update the fields as described below.

- Basic Settings
- Cluster
- Access Points
- Users
- Sessions
- Status
- Interfaces
- Events
- Statistics
- Associations
- Neighbors
- Advanced
- Ethernet
- Wireless
- Security
- Guest Login
- Radio
- MAC Filtering
- Load Balancing
- QoS
- WDS
- Time Protocol
- Reboot
- Reset
- Upgrade

Modify radio settings

Status On Off

Mode IEEE 802.11g
IEEE 802.11b
IEEE 802.11n

Channel 6

Beacon Interval 100 (Msec, Range: 20 - 2000)

DTIM Period 2 (Range: 1-255)

Fragmentation Threshold 2346 (Range: 256-2346, even numbers only)

RTS Threshold 2347 (Range: 0-2347)

Maximum Stations 2007 (Range: 0-2007)

Transmit Power 100 (Percent)

Rate Sets

Rate	Supported	Basic
54 Mbps	<input checked="" type="checkbox"/>	<input type="checkbox"/>
48 Mbps	<input checked="" type="checkbox"/>	<input type="checkbox"/>
36 Mbps	<input checked="" type="checkbox"/>	<input type="checkbox"/>
24 Mbps	<input checked="" type="checkbox"/>	<input type="checkbox"/>
18 Mbps	<input checked="" type="checkbox"/>	<input type="checkbox"/>
12 Mbps	<input checked="" type="checkbox"/>	<input type="checkbox"/>
11 Mbps	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
9 Mbps	<input checked="" type="checkbox"/>	<input type="checkbox"/>
6 Mbps	<input checked="" type="checkbox"/>	<input type="checkbox"/>
5.5 Mbps	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
2 Mbps	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
1 Mbps	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

?

Radio settings directly control the behavior of the radio device in the access point and its interaction with the physical medium; that is, how/what type of electromagnetic waves the AP emits.

You can specify whether the radio is on or off, radio frequency (RF) broadcast channel, beacon interval (amount of time between AP beacon transmissions), transmit power, IEEE 802.11 mode in which the radio operates, and so on.

[More...](#)

Configuring Radio Settings

Field	Description
Status (On/Off)	Specify whether you want the radio on or off by clicking On or Off.
Mode	<p>The <i>Mode</i> defines the <i>Physical Layer</i> (PHY) standard being used by the radio.</p> <p>Select one of these modes:</p> <ul style="list-style-type: none"> • IEEE 802.11b • IEEE 802.11g
Channel	<p>The Channel defines the portion of the radio spectrum that the radio uses for transmitting and receiving. The range of channels and the default channel are determined by the Mode of the radio interface.</p> <p>For most Modes, the default is “Auto”. Auto is the recommended mode because it automatically detects the best channel choices based on signal strength, traffic loads, and so on.</p>
Beacon Interval	<p>Beacon frames are transmitted by an access point at regular intervals to announce the existence of the wireless network. The default behavior is to send a beacon frame once every 100 milliseconds (or 10 per second).</p> <p>The <i>Beacon Interval</i> value is set in milliseconds. Enter a value from 20 to 2000.</p>
DTIM Period	<p>The <i>Delivery Traffic Information Map</i> (DTIM) message is an element included in some Beacon frames. It indicates which client stations, currently sleeping in low-power mode, have data buffered on the access point awaiting pickup.</p> <p>The DTIM period you specify here indicates how often the clients served by this access point should check for buffered data still on the AP awaiting pickup.</p> <p>Specify a DTIM period within the given range (1 - 255).</p> <p>The measurement is in beacons. For example, if you set this to “1” clients will check for buffered data on the AP at every beacon. If you set this to “2”, clients will check on every other beacon. If you set this to 10, clients will check on every 10th beacon.</p>

Field	Description
Fragmentation Threshold	<p>Specify a number between 256 and 2,346 to set the frame size threshold in bytes.</p> <p>The <i>fragmentation threshold</i> is a way of limiting the size of packets (frames) transmitted over the network. If a packet exceeds the fragmentation threshold set here, the fragmentation function will be activated and the packet will be sent as multiple 802.11 frames.</p> <p>If the packet being transmitted is equal to or less than the threshold, fragmentation will not be used.</p> <p>Setting the threshold to the largest value (2,346 bytes) effectively disables fragmentation.</p> <p>Fragmentation involves more overhead both because of the extra work of dividing up and reassembling of frames it requires, and because it increases message traffic on the network. However, fragmentation can help <i>improve</i> network performance and reliability if properly configured.</p> <p>Sending smaller frames (by using lower fragmentation threshold) may help with some interference problems; for example, with microwave ovens.</p> <p>By default, fragmentation is off. We recommend not using fragmentation unless you suspect radio interference. The additional headers applied to each fragment increase the overhead on the network and can greatly reduce throughput.</p>
RTS Threshold	<p>Specify an RTS Threshold value between 0 and 2347.</p> <p>The RTS threshold specifies the packet size of a request to send (RTS) transmission. This helps control traffic flow through the access point, especially one with a lot of clients.</p> <p>If you specify a low threshold value, RTS packets will be sent more frequently. This will consume more bandwidth and reduce the throughput of the packet.</p> <p>On the other hand, sending more RTS packets can help the network recover from interference or collisions which might occur on a busy network, or on a network experiencing electromagnetic interference.</p>
Maximum Stations	<p>Specify the maximum number of stations allowed to access this access point at any one time.</p> <p>You can enter a value between 0 and 2007.</p>

Field	Description
<p>Transmit Power</p>	<p>Provide a percentage value to set the transmit power for this access point.</p> <p>The default is to have the access point transmit using 100 percent of its power.</p> <p>Recommendations:</p> <ul style="list-style-type: none"> • For most cases, we recommend keeping the default and having the transmit power set to 100 percent. This is more cost-efficient as it gives the access point a maximum broadcast range, and reduces the number of APs needed. • To increase capacity of the network, place APs closer together and reduce the value of the transmit power. This will help reduce overlap and interference among APs. A lower transmit power setting can also keep your network more secure because weaker wireless signals are less likely to propagate outside of the physical location of your network.
<p>Rate Sets</p>	<p>Check the transmission rate sets you want the access point to support and the basic rate sets you want the access point to advertise.</p> <p>Rates are expressed in megabits per second.</p> <ul style="list-style-type: none"> • Supported Rate Sets indicate rates that the access point supports. You can check multiple rates (click a checkbox to select or deselect a rate). The AP will automatically choose the most efficient rate based on factors like error rates and distance of client stations from the AP. • Basic Rate Sets indicate rates that the access point will advertise to the network for the purposes of setting up communication with other APs and client stations on the network. It is generally more efficient to have an AP broadcast a subset of its supported rate sets.

Updating Settings

To apply your changes, click **Update**.

If you are using the two-radio version of the D-Link DWL-2210AP, keep in mind that both Radio One and Radio Two are configured on this tab. The displayed settings apply to either Radio One or Radio Two, depending on which radio you choose in the Radio field (first field on tab). When you have configured settings for one of the radios, click “Update” and then select and configure the other radio. Be sure to click “Update” to apply the second set of configuration settings for the other radio.

Controlling Access by MAC Address Filtering

A *Media Access Control* (MAC) address is a hardware address that uniquely identifies each node of a network. All IEEE 802 network devices share a common 48-bit MAC address format, usually displayed as a string of 12 hexadecimal digits separated by colons, for example FE:DC:BA:09:87:65.

Each wireless network interface card (NIC) used by a wireless client has a unique MAC address.

You can control client access to your wireless network by switching on “MAC Filtering” and specifying a list of approved MAC addresses. When MAC Filtering is on, only clients with a listed MAC address can access the network.

The following sections describe how to use MAC address filtering on the D-Link DWL-2210AP:

- Navigating to MAC Filtering Settings
- Using MAC Filtering
- Updating Settings

Navigating to MAC Filtering Settings

To enable filtering by MAC address, navigate to the **Advanced > MAC Filtering** tab, and update the fields as described below.

Basic Settings

Cluster

Access Points

Users

Sessions

Status

Interfaces

Events

Statistics

Associations

Neighbors

Advanced

Ethernet

Wireless

Security

Guest Login

Radio

MAC Filtering

Load Balancing

QoS

Configure MAC Filtering of client stations

Filter

Allow only stations in list

Allow any station unless in list

Stations List

Remove

: : : : : Add

Update

? Media Access Control (MAC) Filtering is used to exclude or allow only listed client stations to authenticate with the access point.

These settings apply to both the Internal and Guest networks.

Stations are filtered by "MAC" address, a hardware ID that uniquely identifies each node of a network.

A MAC address consists of a string of twelve (12) hexadecimal digits separated by colons, for example FE:DC:BA:09:87:65.

[More...](#)

Using MAC Filtering

This page allows you to control access to D-Link DWL-2210AP based on *Media Access Control* (MAC) addresses. Based on how you set the filter, you can *allow* only client stations with a listed MAC address or *prevent* access to the stations listed.

For the Guest interface, MAC Filtering settings apply to both BSSes.

On a two-radio AP, MAC Filtering settings apply to both radios.

Field	Description
Filter	To set the MAC Address Filter , click one of the following radio buttons: <ul style="list-style-type: none">• Allow only stations in the list• Allow any station unless in list
Stations List	To add a MAC Address to Stations List, enter its 48-bit MAC address into the lower text boxes, then click Add . The MAC Address is added to the Stations List. To remove a MAC Address from the Stations List, select its 48-bit MAC address, then click Remove . The stations in the list will either be allowed or prevented from accessing the AP based on how you set the Filter.

Updating Settings

To apply your changes, click **Update**.

Load Balancing

The D-Link DWL-2210AP allows you to balance the distribution of wireless client connections across multiple access points. Using load balancing, you can prevent scenarios where a single access point in your network shows performance degradation because it is handling a disproportionate share of the wireless traffic.

The following sections describe how to configure Load Balancing on your wireless network:

- Understanding Load Balancing
- Identifying the Imbalance: Overworked or Under-utilized Access Points
- Specifying Limits for Utilization and Client Associations
- Load Balancing and QoS
- Navigating to Load Balancing Settings
- Configuring Load Balancing
- Updating Settings

Understanding Load Balancing

Like most configuration settings on the D-Link DWL-2210AP, load balancing settings are shared among clustered access points.

In some cases you might want to set limits for only one access point that is consistently overutilized. You can apply unique settings to a particular access point if it is operating in standalone mode. (See “Understanding Clustering” and “Navigating to Access Points Management” in this manual.)

Identifying the Imbalance: Overworked or Under-utilized Access Points

A typical scenario is that a comparison of Session Monitoring data for multiple access points allows you to identify an access point that is consistently handling a disproportionately large percentage of wireless traffic. This can happen when location placement or other factors causes one access point to transmit the strongest signal to a majority of clients on a network. By default, that access point will receive most of client requests while the other access points stay idle much of the time.

Imbalances in distribution of wireless traffic across access points will be evident in Session Monitoring statistics, which will show higher “Utilization” rates on overworked APs and conversely, higher “Idle” times on under-utilized APs. An AP that is handling more than its fair share of traffic might also show slower data rates or lower transmit/receive rates due to the overload.

Specifying Limits for Utilization and Client Associations

You can correct for imbalances in network AP utilization by enabling load balancing and setting limits on utilization rates and number of client associations allowed per access point.

Load Balancing and QoS

Load balancing also plays a part in contributing to *Quality of Service* (QoS) for *Voice Over IP* (VoIP) and other such time-sensitive applications competing for bandwidth and timely access to the air waves on a wireless network. For more information about configuring your network for QoS, see “Configuring Queues for Quality of Service (QoS)” in this manual.

Navigating to Load Balancing Settings

On the Administration UI, navigate to the **Advanced > Load Balancing** tab, and update the fields as described in the next section.

The screenshot displays the 'Modify load balancing settings' page. On the left is a sidebar with navigation tabs: Basic Settings, Cluster, Access Points, Users, Sessions, Status, Interfaces, Events, Statistics, Associations, Neighbors, Advanced, Ethernet, Wireless, Security, Guest Login, Radio, MAC Filtering, Load Balancing (highlighted), and QoS. The main content area is titled 'Modify load balancing settings' and contains the following settings:

- Load Balancing**: Radio buttons for Enabled and Disabled.
- Utilization for No New Associations**: A text input field with '(Percent, 0 disables)' as a hint.
- Utilization for Disassociation**: A text input field with '(Percent, 0 disables)' as a hint.
- Station Threshold for Disassociation**: A text input field with '(Range: 0-2007)' as a hint.

An 'Update' button is located at the bottom right of the settings area. On the right side of the page is a help panel with a question mark icon, containing the following text:

Use this page to load balance the distribution of wireless client connections across multiple access points.

This applies to the AP load as a whole (both Internal and Guest networks together).

With load balancing, you can ensure that all access points on the network handle a proportionate share of wireless traffic, and that no single access point gets overloaded.


[More...](#)

Configuring Load Balancing

To configure load balancing, *enable* “Load Balancing” and set limits and behavior to be triggered by a specified utilization rate of the access point.

- To view the current Utilization Rates for access points, click Cluster > Sessions on the Administration Web pages. (See “Session Monitoring” in this manual.)
 - Even when clients are disassociated from an AP, the network will still provide continuous service to client stations if another access point is within range so that clients can reconnect to the network. Clients should automatically retry the AP they were originally connected to and other APs on the subnet. Clients who are disassociated from one AP should experience a seamless transition to another AP on the same subnet.
- Load Balancing settings apply to the AP load as a whole. When Guest access is enabled, the settings apply to both Internal and Guest networks together.
- On a two-radio access point, Load Balancing settings apply to both radios but the load of each radio is calculated independently and includes both the Internal and Guest network (when Guest access is enabled).

Field	Description
Load Balancing	To enable load balancing on this access point, click Enable . To disable load balancing on this access point, click Disable .
Utilization for No New Associations	<p>Utilization rate limits relate to wireless bandwidth utilization.</p> <p>Provide a bandwidth utilization rate percentage limit for this access point to indicate when to stop accepting new client associations.</p> <p>When the utilization rate for this access point exceeds the specified limit, no new client associations will be allowed on this access point.</p> <p>If you specify 0 in this field, all new associations will be allowed regardless of the utilization rate.</p>

Field	Description
Utilization for Disassociation	<p>Utilization rate limits relate to wireless bandwidth utilization.</p> <p>Provide a bandwidth utilization rate percentage limit for this access point to indicate when to disassociate current clients.</p> <p>When the utilization rate exceeds the specified limit, a client currently associated with this access point will be disconnected.</p> <p>If you specify 0 in this field, current clients will never be disconnected regardless of the utilization rate.</p>
Stations Threshold for Disassociation	<p>Specify the number of client stations you want as a “stations threshold” for disassociation. If the number of client stations associated with the AP at any one time is equal to or less than the number you specify here, no stations will be disassociated regardless of the “Utilization for Disassociation” value.</p> <p>Theoretically, the maximum number of client stations allowed is 2007.</p> <p> We recommend setting the maximum to between 30 and 50 client stations. This allows for a workable load on the access point, given that bandwidth is shared among the AP clients.</p>

Updating Settings

To apply your changes, click **Update Settings**.

Configuring Queues for Quality of Service (QoS)

Quality of Service (QoS) provides you with the ability to specify parameters on multiple queues for increased throughput and better performance of differentiated wireless traffic like *Voice-over-IP* (VoIP), video, and streaming media as well as traditional IP data over the D-Link DWL-2210AP.

The following sections describe how to configure Quality of Service queues on the D-Link DWL-2210AP:

- Understanding QoS
- QoS and Load Balancing
- 802.11e and WME Standards Support
- QoS Queues and Parameters to Coordinate Traffic Flow
- Navigating to QoS Settings
- Configuring QoS Queues
- Updating Settings

Understanding QoS

A primary factor that affects QoS is network congestion due to an increased number of clients attempting to access the air waves and higher traffic volume competing for bandwidth during a busy time of day. The most noticeable degradation in service on a busy, overloaded network will be evident in time-sensitive applications like *Voice-over-IP* (VoIP) and streaming media.

Unlike typical data files which are less affected by variability in QoS, VoIP and streaming media must be sent in a specific order, at a consistent rate, and with minimum delay between Packet transmission. If the quality of service is compromised, the audio or video will be distorted.

QoS and Load Balancing

By using a combination of load balancing (see “Load Balancing” on page 95) and QoS techniques, you can provide a high quality of service for time-sensitive applications even on a busy network. Load balancing is a way of better distributing the traffic volume across access points. QoS is a means of allocating bandwidth and network access based on transmission priorities for different types of wireless traffic within a single access point.

802.11e and WME Standards Support

QoS describes a range of technologies for controlling data streams on shared network connections. The IEEE 802.11e task group is in the process of defining a QoS standard for transmission quality and availability of service on wireless networks. QoS is designed to provide better network service by minimizing network congestion; limiting Jitter, Latency, and Packet Loss; supporting dedicated bandwidth for time-sensitive or mission critical applications, and prioritizing wireless traffic for channel access.

As with all IEEE 802.11 working group standards, the goal is to provide a standard way of implementing QoS features so that components from different companies are interoperable. The D-Link DWL-2210AP provides QoS based on the *Wireless Multimedia Enhancement* (WME) specification, which is an implementation of a subset of 802.11e features.

QoS Queues and Parameters to Coordinate Traffic Flow

Configuring QoS options on the D-Link DWL-2210AP consists of setting parameters on existing queues for different types of wireless traffic. You can configure different minimum and maximum wait times for the transmission of packets in each queue based on the requirements of the media being sent. Queues automatically provide minimum transmission delay for VoIP, multimedia, and mission critical applications, and rely on best-effort parameters for traditional IP data.

For example, time-sensitive multimedia and VoIP are given effectively higher priority for transmission (lower wait times for channel access), while other applications and traditional IP data which are less time-sensitive but often more data-intensive are expected to tolerate longer wait times.

The D-Link DWL-2210AP implements QoS with a custom extension to the traffic control mechanism in the Linux kernel. Our Linux-based queuing class is used to tag packets and establish multiple queues. The queues provided offer built-in prioritization and routing based on the type of data being transmitted.

The Administration UI provides a way for you to configure parameters on the queues.

QoS Queues and Type of Service (ToS) on Packets

QoS on the D-Link DWL-2210AP leverages existing information in the IP packet header related to Type of Service (ToS). Every IP packet sent over the network includes a ToS field in the header that indicates how the data should be prioritized and transmitted over the network. The ToS field consists of a 3 to 7 bit value with each bit representing a different aspect or degree of priority for this data as well as other meta-information (low delay, high throughput, high reliability, low cost, and so on).

For example, the ToS for FTP data packets is likely to be set for maximum throughput since the critical consideration for FTP is the ability to transmit relatively large amounts of data in one go. Interactive feedback is a nice-to-have in this situation but certainly less critical. VoIP data packets are set for minimum delay because that is a critical factor in quality and performance for that type of data.

The access point examines the ToS field in the headers of all packets that pass through the AP. Based on the value in a packet's ToS field, the AP prioritizes the packet for transmission by assigning it to one of the queues. This process occurs automatically, regardless of whether you deliberately configure QoS or not.

A different type of data is associated with each queue. The queue and associated priorities and parameters for transmission are as follows:

- Data 0 (bulk). Lowest priority queue, high throughput. Bulk data that requires maximum throughput and is not time-sensitive is sent to this queue (FTP data, for example).
- Data 1 (best effort). Medium priority queue, medium throughput and delay. Most traditional IP data is sent to this queue.
- Data 2 (interactive). Highest priority queue, minimum delay. Time-sensitive data such as VoIP and streaming media are automatically sent to this queue.
- Data 3 (not used)

Packets in a higher priority queue will be transmitted before packets in a lower priority queue. Interactive data in the queue labeled “Data 2” is always sent first, best effort data in “Data 1” is sent next, and bulk data in “Data 0” is sent last. Each lower priority queue (class of traffic) gets bandwidth that is left over after the higher classes of traffic have been sent. At an extreme end if you have enough interactive data to keep the access point busy all the time, low priority traffic would never get sent.

Using the QoS settings on the Administration UI, you can configure parameters that determine how each queue is treated when it is sent by the access point.

Wireless traffic travels:

- Downstream from the access point to the client station
- Upstream from client station to access point
- Upstream from access point to network
- Downstream from network to access point

QoS settings on the D-Link DWL-2210AP affect only the first of these; *downstream* traffic flowing from the access point to client station. The other phases of the traffic flow are not under control of the QoS settings on the AP.

DCF Control of Data Frames and Interframe Spaces

Data is transmitted over 802.11 wireless networks in *frames*. A *Frame* consists of a discrete portion of data along with some descriptive meta-information packaged for transmission on a wireless network.

A Frame is similar in concept to a *Packet*, the difference being that a packet operates on the Network layer (layer 3 in the OSI model) whereas a frame operates on the Data-Link layer (layer 2 in the OSI model).

Each frame includes a source and destination MAC address, a control field with protocol version, frame type, frame sequence number, frame body (with the actual information to be transmitted) and frame check sequence for error detection.

The 802.11 standard defines various *frame* types for management and control of the wireless infrastructure, and for data transmission. 802.11 frame types are (1) *management frames*, (2) *control frames*, and (3) *data frames*. Management and control frames (which manage and control the availability of the wireless infrastructure) automatically have higher priority for transmission.

802.11e uses *interframe spaces* to regulate which frames get access to available channels and to coordinate wait times for transmission of different types of data.

Management and control frames wait a minimum amount of time for transmission; they wait a *short interframe space* (SIF). These wait times are built-in to 802.11 as infrastructure support and are not configurable.

The D-Link DWL-2210AP supports the *Distribution Coordination Function* (DCF) as defined by the 802.11e standard. DCF, which is based on CSMA/CA protocol, defines the interframe space (IFS) between *data frames*. Data frames wait for an amount of time defined as the *DCF interframe space* (DIF) before transmitting.

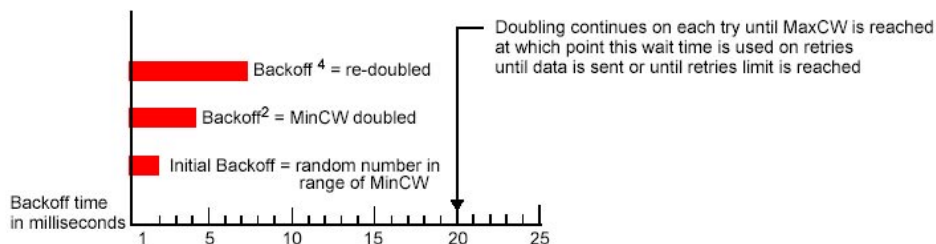
This parameter is configurable.

(Note that sending data frames in DIFs allows higher priority management and control frames to be sent in SIFs first.)

The DCF ensures that multiple access points do not try sending data at the same time but instead wait until a channel is free.

Random Backoff and Minimum / Maximum Contention Windows

If an access point detects that the medium is in use (busy), it uses the DCF *random backoff* timer to determine the amount of time to wait before attempting to access a given channel again. Each access point waits some random period of time between retries. The wait time (initially a random value within a range specified as the *Minimum Contention Window*) increases exponentially up to a specified limit (*Maximum Contention Window*). The random delay avoids most of the collisions that would occur if multiple APs got access to the medium at the same time and tried to transmit data simultaneously. The more active users you have on a network, the more significant the performance gains of the backoff timer will be in reducing the number of collisions and retransmissions.



The random backoff used by the access point is a configurable parameter. To describe the random delay, a “Minimum Contention Window” (MinCW) and a “Maximum Contention Window” (MaxCW) is defined.

- The value specified for the Minimum Contention Window is the upper limit of a range for the initial random backoff wait time. The number used in the random backoff is initially a random number between 0 and the number defined for the Minimum Contention Window.
- If the first random backoff time ends before successful transmission of the data frame, the access point increments a retry counter, and doubles the value of the random backoff window. The value specified in the Maximum Contention Window is the upper limit for this doubling of the random backoff. This doubling continues until either the data frame is sent or the Maximum Contention Window size is reached.

Packet Bursting for Better Performance

The D-Link DWL-2210AP includes 802.11e based *packet bursting* technology that increases data throughput and speed of transmission over the wireless network. Packet bursting enables the transmission of multiple packets without the extra overhead of header information. The effect of this is to increase network speed and data throughput. The size of packet bursts allowed (maximum burst length) is a configurable parameter.

Navigating to QoS Settings

To set up queues for QoS, navigate to the **Advanced > QoS** tab, and configure settings as described below.

Queue	Inter-Frame Space (1-255)	Min. Contention Window	Max. Contention Window	Max. Burst Length (ms)
Data 0 (bulk)	1	3	7	3.3
Data 1 (best-effort)	1	7	15	6.0
Data 2 (interactive)	3	15	63	0
Data 3	7	15	1023	0

Update

? Quality of Service (QoS) allows you to specify different queue parameters for different types of wireless traffic.

These settings apply to the AP load as a whole, and Internal and Guest network traffic is queued together.

QoS specifically relates to providing minimum delay service for Voice over IP (VoIP) and other time-sensitive types of data.

You do not need to modify these parameters to activate QoS. Queuing for Quality of Service (with the default parameters) automatically occurs whenever an AP is in service.

[More...](#)

Configuring QoS Queues

Configuring Quality of Service (QoS) on the D-Link DWL-2210AP consists of setting parameters on existing queues for different types of wireless traffic, and effectively specifying minimum and maximum wait times (via *Contention Windows*) for transmission. The settings described here apply to data transmission behavior on the access point only, not to that of the client stations.

- For the Guest interface, QoS queue settings apply to the access point load as a whole (both BSSes together).
- On a two-radio access point these settings apply to both radios but the traffic for each radio is queued independently. (The exception to this is guest traffic as noted below.)
- Internal and Guest network traffic is always queued together within each radio. This is the case on both one-radio and two-radio APs.

Field	Description
<p>Queue</p>	<p>Queues are defined for different types of data transmitted from AP-to-station:</p> <p>Data 0 (bulk)</p> <p>Lowest priority queue, high throughput. Bulk data that requires maximum throughput and is not time-sensitive is sent to this queue (FTP data, for example).</p> <p>For information purposes, the hexadecimal values to describe this queue are in the following ranges:</p> <p>0X02 - 0X03 0X08 - 0X0F</p> <p>Data 1 (best effort)</p> <p>Medium priority queue, medium throughput and delay. Most traditional IP data is sent to this queue.</p> <p>For information purposes, the hexadecimal values to describe this queue are in the following ranges:</p> <p>0x00 - 0X01 0X04 - 0X07 0X18 - 0X1F</p> <p>Data 2 (interactive)</p> <p>Highest priority queue, minimum delay. Time-sensitive data such as VoIP and streaming media are automatically sent to this queue.</p> <p>For information purposes, the hexadecimal values to describe this queue are in the following ranges:</p> <p>0x10 - 0X17</p> <p>Data 3 (not used)</p> <p>For more information, see “QoS Queues and Parameters to Coordinate Traffic Flow” in this manual.</p>
<p>Inter-Frame Space</p>	<p>The Interframe Space specifies a wait time (in milliseconds) for <i>data frames</i>.</p> <p>For more information, see “DCF Control of Data Frames and Interframe Spaces” in this manual.</p>

Field	Description
Min. Contention Window	<p>This parameter is input to the algorithm that determines the initial random backoff wait time (“window”) for retry of a transmission.</p> <p>The value specified here in the <i>Minimum Contention Window</i> is the upper limit (in milliseconds) of a range from which the initial random backoff wait time is determined.</p> <p>The first random number generated will be a number between 0 and the number specified here. If the first random backoff wait time expires before the data frame is sent, a retry counter is incremented and the random backoff value (window) is doubled.</p> <p>Doubling will continue until the size of the random backoff value reaches the number defined in the Maximum Contention Window.</p> <p>For more information, see “Random Backoff and Minimum / Maximum Contention Windows” in this manual.</p>
Max. Contention Window	<p>The value specified here in the <i>Maximum Contention Window</i> is the upper limit (in milliseconds) for the doubling of the random backoff value. This doubling continues until either the data frame is sent or the Maximum Contention Window size is reached. Once the Maximum Contention Window size is reached, retries will continue until a maximum number of retries allowed is reached.</p> <p>For more information, see “Random Backoff and Minimum / Maximum Contention Windows” in this manual.</p>
Max. Burst Length	<p>This value specifies (in milliseconds) the Maximum Burst Length allowed for packet bursts on the wireless network. A <i>packet burst</i> is a collection of multiple frames transmitted without header information. The decreased overhead results in higher throughput and better performance.</p> <p>For more information, see “Packet Bursting for Better Performance” in this manual.</p>

Updating Settings

To apply your changes, click **Update Settings**.

Configuring the Wireless Distribution System (WDS)

The D-Link DWL-2210AP lets you connect multiple access points using a Wireless Distribution System (WDS). WDS allows access points to communicate with one another wirelessly in a standardized way. This capability is critical in providing a seamless experience for roaming clients and for managing multiple wireless networks. It can also simplify the network infrastructure by reducing the amount of cabling required.

The following sections describe how to configure the WDS on the D-Link DWL-2210AP:

- Understanding the Wireless Distribution System
- Using WDS to Bridge Distant Wired LANs
- Using WDS to Extend the Network Beyond the Wired Coverage Area
- Backup Links and Unwanted Loops in WDS Bridges
- Security Considerations Related to WDS Bridges
- Navigating to WDS Settings
- Configuring WDS Settings
- Example of Configuring a WDS Link
- Updating Settings

Understanding the Wireless Distribution System

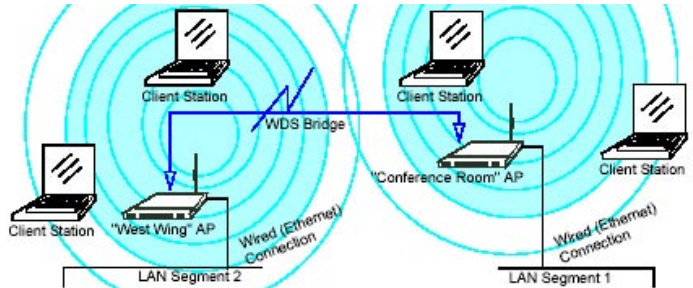
A *Wireless Distribution System* (WDS) is an 802.11f technology that wirelessly connects access points, known as Basic Service Sets (BSS), to form what is known as an *Extended Service Set* (ESS).

A BSS generally equates to an access point (deployed as a single-AP wireless “network”), except in cases where multi-BSSID features make a single access point look like two or more access points to the network. In such cases, the access point has multiple unique BSSIDs

Using WDS to Bridge Distant Wired LANs

In an ESS, a network of multiple access points, each access point serves part of an area which is too large for a single access point to cover. You can use WDS to bridge distant Ethernets to create a single LAN. For example, suppose you have one access point which is connected to the network by Ethernet and serving multiple client stations in the Conference Room (LAN Segment 1), and another Ethernet-wired access point serving stations in the West Wing offices (LAN Segment 2).

You can bridge the Conference Room and West Wing access points with a WDS link to create a single network for clients in both areas.

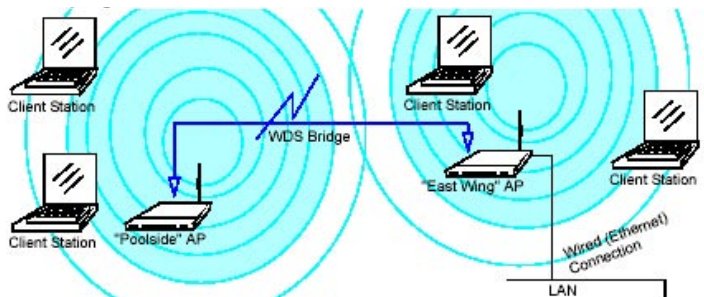


Using WDS to Extend the Network Beyond the Wired Coverage Area

An ESS can extend the reach of the network into areas where cabling would be difficult, costly, or inefficient.

For example, suppose you have an access point which is connected to the network by Ethernet and serving multiple client stations in one area ("East Wing" in our example) but cannot reach others which are out of range. Suppose also that it is too difficult or too costly to wire the distant area with Ethernet cabling.

You can solve this problem by placing a second access point closer to second group of stations ("Poolside" in our example) and bridge the two APs with a WDS link. This *extends* your network wirelessly by providing an extra hop to get to distant stations.



Backup Links and Unwanted Loops in WDS Bridges

Another use for WDS bridging, the creation of backup links, is not supported in this release of the D-Link DWL-2210AP. The topic is included here to emphasize that you should not try to use WDS in this way; backup links will result in unwanted, endless loops of data traffic.

If an access point provides *Spanning Tree Protocol* (STP), WDS can be used to configure backup paths between access points across the network. For example, between two access points you could have both a primary path via Ethernet and a secondary (backup) wireless path via a WDS link. If the Ethernet connection goes down, STP would reconfigure its map of the network and effectively fix the down network segment by activating the backup wireless path.

The D-Link DWL-2210AP does not provide STP for this release. Without STP, it is possible that both connections (paths) may be active at the same time, and result in an endless loop of traffic on the LAN.

Therefore, be sure not create loops with either WDS bridges or combinations of Wired (Ethernet) connections and WDS bridges.

For more information, see the “Do not create loops” note under “Configuring WDS Settings” in this manual.

Security Considerations Related to WDS Bridges

Static *Wired Equivalent Privacy* (WEP) is a data encryption protocol for 802.11 wireless networks. Both access points in a given WDS link must be configured with the same security settings. For static WEP, either a static 64-bit (40-bit secret key + 24-bit initialization vector (IV)) or 128-bit (104-bit secret key + 24-bit IV) Shared Key is specified for data encryption.

You can enable Static WEP on the WDS link (bridge). When WEP is enabled, all data exchanged between the two access points in a WDS link is encrypted using a fixed WEP key that you provide.

Static WEP is the only security mode available for the WDS link, and it does not provide effective data protection to the level of other security modes available for service to client stations. If you use WDS on a LAN intended for secure wireless traffic you are putting your network at risk. Therefore, we recommend using WDS to bridge the Guest network only for this release. Do not use WDS to bridge access points on the Internal network unless you are not concerned about the security risk for data traffic on that network.

For more information about the effectiveness of different security modes, see “Configuring Security” in this manual. This topic also covers use of plain text security mode for AP-to-station traffic on the Guest network, which is intended for less sensitive data traffic.

Navigating to WDS Settings

To specify the details of traffic exchange from this access point to others, navigate to the **Advanced > WDS** tab, and update the fields as described below.

The following figure shows the WDS settings page for the two-radio AP. The Administration Web page for the one-radio AP will look slightly different.

Basic Settings

Cluster

Access Points

Users

Sessions

Status

Interfaces

Events

Statistics

Associations

Neighbors

Advanced

Ethernet

Wireless

Security

Guest Login

Radio

MAC Filtering

Load Balancing

QoS

WDS

Time Protocol

Reboot

Reset

Upgrade

Configure WDS bridges to other access points

Local Address	00:0C:41:0A:33:7E
<hr/>	
Remote Address	<input type="text"/>
Bridge with	Internal Network <input type="button" value="v"/>
WEP	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled
Key Length	<input type="radio"/> 64 bits <input checked="" type="radio"/> 128 bits
Key Type	<input type="radio"/> ASCII <input checked="" type="radio"/> Hex
Characters Required	<input type="text" value="26"/>
WEP Key	<input type="text"/>
<hr/>	
Remote Address	<input type="text"/>
Bridge with	Internal Network <input type="button" value="v"/>
WEP	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled
Key Length	<input type="radio"/> 64 bits <input checked="" type="radio"/> 128 bits
Key Type	<input type="radio"/> ASCII <input checked="" type="radio"/> Hex
Characters Required	<input type="text" value="26"/>
WEP Key	<input type="text"/>
<hr/>	
Remote Address	<input type="text"/>
Bridge with	Internal Network <input type="button" value="v"/>
WEP	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled
Key Length	<input type="radio"/> 64 bits <input checked="" type="radio"/> 128 bits
Key Type	<input type="radio"/> ASCII <input checked="" type="radio"/> Hex
Characters Required	<input type="text" value="26"/>
WEP Key	<input type="text"/>
<hr/>	
Remote Address	<input type="text"/>
Bridge with	Internal Network <input type="button" value="v"/>
WEP	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled
Key Length	<input type="radio"/> 64 bits <input checked="" type="radio"/> 128 bits
Key Type	<input type="radio"/> ASCII <input checked="" type="radio"/> Hex
Characters Required	<input type="text" value="26"/>
WEP Key	<input type="text"/>

?

The Wireless Distribution System (WDS) allows you to bridge wireless traffic between access points.

By wirelessly connecting APs to one another in an Extended Service Set, you can bridge distant subnets into a single LAN with each AP serving part of an area too large for a single AP to cover. WDS can extend the reach of your network into areas where cabling might be too difficult.

Caution: Do not create loops with either WDS bridges or combinations of Wired (Ethernet) connections and WDS bridges.

Loops created by WDS bridges with the intention of establishing backup links or extended service sets (ESS) with two WDS bridges on one AP will not work; they will result in endless loop data traffic on the network because Spanning Tree Protocol (STP) is not on the AP to prevent it.

[More...](#)

Configuring WDS Settings

The following notes summarize some critical guidelines regarding WDS configuration. Please read all the notes before proceeding with WDS configuration.

- The only security mode available on the WDS link is Static WEP, which is not particularly secure. Therefore, we recommend using WDS to bridge the Guest network only for this release. Do not use WDS to bridge access points on the Internal network unless you are not concerned about the security risk for data traffic on that network.
- When using WDS, be sure to configure WDS settings on *both* access points participating in the WDS link.
- You can have only one WDS link between any pair of access points. That is, a remote MAC address may appear only once on the WDS page for a particular access point.

Both access points participating in a WDS link must be on the same Radio channel and using the same IEEE 802.11 mode. (See “Configuring Radio Settings” in this manual for information on configuring the Radio mode and channel.)

Do not create loops with either WDS bridges or combinations of Wired (Ethernet) connections and WDS bridges. *Spanning Tree Protocol* (STP), which manages path redundancy and prevent unwanted loops, is not enabled for this release. Keep these rules in mind when working with WDS on this release of the D-Link DWL-2210AP:

- Any two access points can be connected by only a single path; either a WDS bridge (wireless) or an Ethernet connection (wired), but not both.
- Do not create “backup” links.
- If you can trace more than one path between any pair of APs going through any combination of Ethernet or WDS links, you have a loop.
- You can only extend or bridge either the Internal or Guest network but not both.

To configure WDS on this access point, describe each AP intended to receive handoffs and send information to this AP. Each destination AP needs the descriptions shown on the following page.

Field	Description
Local Address	<p>Indicates the Media Access Control (MAC) addresses for this access point.</p> <p>A MAC address is a permanent, unique hardware address for any device that represents an interface to the network. The MAC address is assigned by the manufacturer. You cannot change the MAC address. It is provided here for informational purposes as a unique identifier for the access point or interface.</p> <p>The MAC address for the Bridge (br0) is shown at the top of the WDS settings page. This is the address by which the AP is known externally to other networks.</p>
Remote Address	<p>Specify the MAC address of the destination access point; that is, the access point to which data will be sent or “handed-off” and from which data will be received.</p>
Bridge with guest	<p>The D-Link DWL-2210AP provides the capability of setting up and internal networks on the same access point. (See “Setting up Guest Access” in this manual.)</p> <p>The guest network typically provides internet access but isolates guest clients from more sensitive areas of your internal network. It is common to have security disabled on the guest network to provide open access.</p> <p>Alternatively, the <i>internal</i> network provides full access to protected information behind a firewall and requires secure logins or certificates for access.</p> <p>When using WDS to link up one access point to another, you need to identify within which of these networks you want the data exchange to occur.</p> <p>Specify the network to which you want to bridge this access point:</p> <ul style="list-style-type: none"> • Internal Network • Guest Network
WEP	<p>Specify whether you want <i>Wired Equivalent Privacy</i> (WEP) encryption enabled for the WDS link.</p> <ul style="list-style-type: none"> • Enabled • Disabled <p><i>Wired Equivalent Privacy</i> (WEP) is a data encryption protocol for 802.11 wireless networks. Both access points on the WDS link must be configured with the same security settings. For static WEP, a static 64-bit (40-bit secret key + 24-bit initialization vector (IV)) or 128-bit (104-bit secret key + 24-bit IV) Shared Key for data encryption.</p>
Key Length	<p>If WEP is enabled, specify the length of the WEP key:</p> <ul style="list-style-type: none"> • 64-bits • 128-bits

Field	Description
Key Type	If WEP is enabled, specify the WEP key type: <ul style="list-style-type: none">• ASCII• Hex
Characters Required	Indicates the number of characters required in the WEP key. The number of characters required updates automatically based on how you set Key Length and Key Type.
WEP Key	Enter a string of characters. If you selected "ASCII", enter any combination of 0-9. If you selected "HEX", enter hexadecimal digits (any combination of 0-9 and a-f or A-F). These are the RC4 encryption keys shared with the stations using the access point.

Example of Configuring a WDS Link

When using WDS, be sure to configure WDS settings on both access points on the WDS link.

For example, to create a WDS link between a pair of access points "MyAP1" and "MyAP2" do the following:

1. Open the Administration Web pages for MyAP1, by entering the IP address for MyAP1 as a URL in the Web browser address bar in the following form:

`http://IPAddressOfAccessPoint`

where *IPAddressOfAccessPoint* is the address of MyAP1.

2. Navigate to the WDS tab on MyAP1 Administration Web pages.

The MAC address for MyAP1 (the access point you are currently viewing) will show as the “Local Address” at the top of the page.

3. Configure a WDS interface for data exchange with MyAP2.

Start by entering the MAC address for MyAP2 as the “Remote Address” and fill in the rest of the fields to specify the network (guest or internal), security, and so on. Save the settings (click Update).

4. Navigate to the radio settings on the Administration Web pages (**Advanced**—>**Radio**) to verify or set the mode and the radio channel on which you want MyAP1 to broadcast.

Remember that the two access points participating in the link, MyAP1 and MyAP2, must be set to the same Mode and be transmitting on the same channel.

For our example, let's say we're using IEEE 802.11b Mode and broadcasting on Channel (We'd choose Mode and Channel from the drop-down menus on the Radio tab.)

5. Now repeat the same steps for MyAP2:

- Open Administration Web pages for MyAP2 by using MyAP2's IP address in a URL.
- Navigate to the WDS tab on MyAP2 Administration Web pages. (MyAP2's MAC address will show as the “Local Address”.)
- Configure a WDS interface for data exchange with MyAP1, starting with the MAC address for MyAP1.
- Navigate to the radio settings for MyAP2 to verify that it is using the same mode and broadcasting on the same channel as MyAP1. (For our example Mode is 802.11b and the channel is 6.)
- Be sure to save the settings by clicking Update.

Updating Settings

To apply your changes, click **Update**.

Setting up Guest Access

Out-of-the-box *Guest Interface* features allow you to configure the D-Link DWL-2210AP for controlled guest access to an isolated network. You can configure the same access point to broadcast and function as two different wireless networks: a secure “Internal” LAN and a public “Guest” network.

Guest clients can access the guest network without a username or password. When guests log in, they see a guest Welcome screen (also known as a *captive portal*).

The following sections are included here:

- Understanding the Guest Interface
- Configuring the Guest Interface
- Configuring Internal and Guest VLANs
- Configuring the Welcome Screen (Captive Portal)
- Using the Guest Network as a Client
- Deployment Example

Understanding the Guest Interface

You can define unique parameters for *guest* connectivity and isolate guest clients from other more sensitive areas of the network. No security is provided on the guest network; only plaintext security mode is allowed.

Simultaneously, you can configure a secure *internal* network (using the same access point as your guest interface) that provides full access to protected information behind a firewall and requires secure logins or certificates for access.

The Guest and Internal interfaces are set up on VLANs in the Advanced > Ethernet (Wired) Settings on the Administration Web pages for the D-Link DWL-2210AP as described below.

The Guest Access feature leverage *multiple BSSID* and *Virtual LAN (VLAN)* technologies that are built-in to the D-Link DWL-2210AP. The Internal and Guest networks are implemented as multiple BSSIDs on the same access point, each with different network names (SSIDs) on the Wireless interface and different VLAN IDs on the wired interface.

Configuring the Guest Interface

To configure the Guest interface on the D-Link DWL-2210AP, perform these configuration steps:

1. Configure the access point to represent two *virtually* separate networks as described in the section below, “Configuring Internal and Guest VLANs” in this manual.
2. Set up the guest Welcome screen for the guest captive portal as described in the section below, “Configuring the Welcome Screen (Captive Portal)” in this manual.

Guest Interface settings are not shared among access points across the cluster. These settings must be configured individually on the Administration pages for each access point. To get to the Administration pages for an access point that is a member of the current cluster, click on its IP Address link on the Cluster > Access Points page of the current AP. For more information about which settings are shared by the cluster and which are not, see “Which Settings are Shared as Part of the Cluster Configuration and Which Are Not?” in this manual.

Configuring Internal and Guest VLANs

If you want to configure the Guest and Internal networks on Virtual LAN (VLANs), the switch and DHCP server you are using must support VLANs. As a prerequisite step, configure a port on the switch for handling VLAN tagged packets as described in the IEEE 802.1Q standard.

Guest Welcome Screen settings are shared among access points across the cluster. When you update these settings for one access point, the configuration will be shared with the other access points in the cluster. For more information about which settings are shared by the cluster and which are not, see “Which Settings are Shared as Part of the Cluster Configuration and Which Are Not?” in this manual.

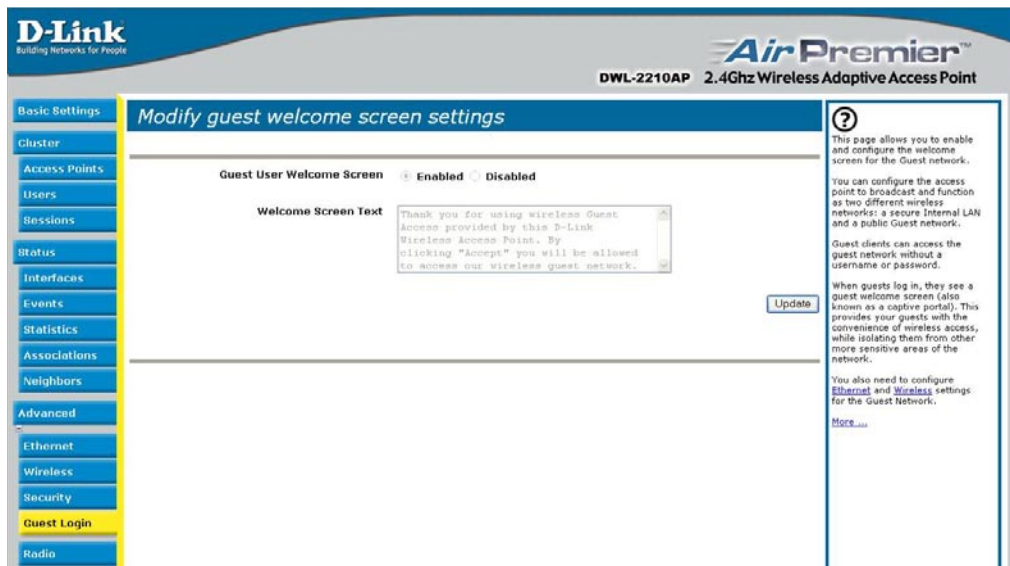
To configure Internal and Guest networks on Virtual LANs, do the following:

1. Configure Ethernet (wired) Settings for Internal and Guest networks on VLANs as described in the sections in “Setting the Ethernet (Wired) Interface” in this manual. (Start by choosing “For Internal and Guest access, use two: **VLANs**” as described in “Using VLANs for the Guest Network” in this manual.)
2. Provide the radio interface settings and network names (SSIDs) for both Internal and Guest networks as described in “Setting the Wireless Interface” in this manual.
3. Configure other settings on the access point needed (not necessarily specific to the guest network) as described in this manual.

Configuring the Welcome Screen (Captive Portal)

You can set up or modify the Welcome screen guest clients see when they open a Web browser or try to browse the Web. To set up the captive portal, do the following.

1. Navigate to the **Advanced > Guest Login** tab.



2. Choose **Enabled** to activate the Welcome screen.
3. In the **Welcome Screen Text** field, type the text message you would like guest clients to see on the captive portal.
4. Click **Update** to apply the changes.

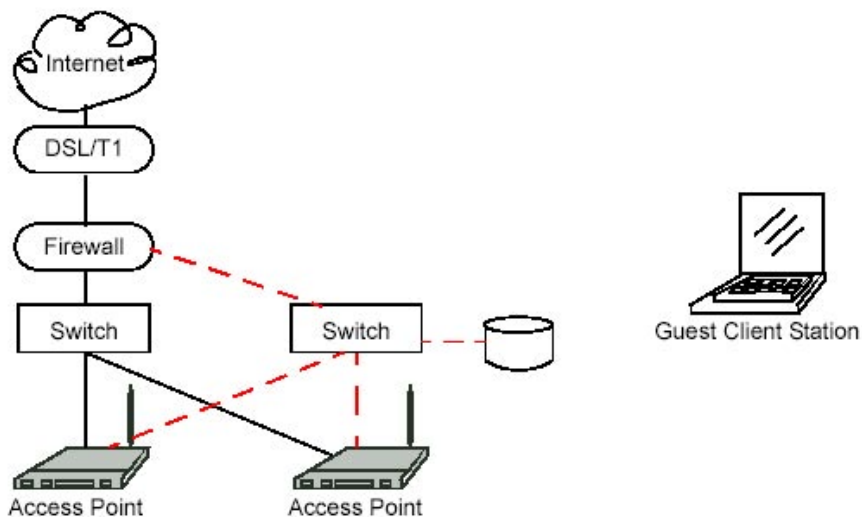
Using the Guest Network as a Client

Once the guest network is configured, a client can access the guest network as follows:

1. A guest client enters an area of coverage and scans for wireless networks.
2. The guest network advertises itself via a Guest SSID or some similar name, depending on how the guest SSID is specified in the Administration Web pages for the Guest interface.
3. The guest client chooses Guest SSID.
4. The guest client starts a Web browser and receives a Guest Welcome screen.
5. The Guest Welcome Screen provides a button for the client to click to continue.
6. The guest client is now enabled to use the “guest” network.

Deployment Example

In the figure below, the dotted red lines indicate dedicated guest connections. All access points and all connections (including guests) are administered from the same D-Link DWL-2210AP Administration Web pages.



Maintenance and Monitoring

The maintenance and monitoring tasks described here all pertain to viewing and modifying settings on specific access points; *not* on a cluster configuration that is automatically shared by multiple access points.

Therefore, it is important to ensure that you are accessing the Administration Web pages for the particular access point you want to configure. For information on this, see “Navigating to Configuration Information for a Specific AP and Managing Standalone APs” in this manual.

The following maintenance and monitoring topics are covered.

- Interfaces
- Event Log
- Statistics
- Associated Wireless Clients
- Rebooting the Access Point
- Resetting the Configuration
- Upgrading the Firmware
- Neighbors

Interfaces

To monitor wired LAN and wireless LAN (WLAN) settings, navigate to **Status > Interfaces** on the access point you want to monitor.

On a two-radio access point, current wireless settings for both Radio One and Radio Two are shown. On a one-radio access point, settings are shown for one radio. The Interfaces page for a two-radio AP is shown in the following figure.

This page displays the current settings of the D-Link DWL-2210AP. It displays the **Ethernet (Wired) Settings** and the **Wireless Settings**.

Ethernet (Wired) Settings

The Internal interface includes the Ethernet MAC Address, IP Address, Subnet Mask, and Associated Network Wireless Name (SSID).

The Guest interface includes the MAC Address, VLAN ID, and Associated Network Wireless Name (SSID).

If you want to change any of these settings, click the “Configure” link.

Wireless Settings

The *Radio* Interface settings radio Mode, and Channel. Also shown here are MAC addresses (read-only) for internal and guest interfaces. (See “Setting the Wireless Interface” in this manual and “Configuring Radio Settings” in this manual for more information.)

If you want to change any of these settings, click the “Configure” link.

Event Log

To view transmit/receive statistics for a particular access point, navigate to **Status > Events** on the Administration Web pages for the access point you want to monitor.

The screenshot shows a web interface with a sidebar on the left containing menu items: Basic Settings, Cluster, Access Points, Users, Sessions, Status, Interfaces, Events (highlighted), Statistics, Associations, Neighbors, Advanced, Ethernet, Wireless, Security, Guest Login, Radio, MAC Filtering, Load Balancing, QoS, and WDS. The main content area is titled "View events generated by this access point" and contains a "System Events Log" table and a "Kernel Log" section.

Time	Severity	Service	Description
Jul 2 14:22:53	info	udhcp	Lease of 10.10.100.250 obtained, lease time 200
Jul 2 14:22:28	info	hostapd	vlan0: STA 00:0c:41:dc:09:e1 WPA: group key exchange completed
Jul 2 14:21:20	info	hostapd	vlan0: STA 00:0c:41:dc:09:e1 WPA: group key exchange completed
Jul 2 14:20:28	info	hostapd	vlan0: STA 00:0c:41:dc:09:e1 IEEE 802.1X: authenticated - identity 'samantha' EAP type: 25 (PEAP)
Jul 2 14:20:28	info	hostapd	vlan0: STA 00:0c:41:dc:09:e1 WPA: group key exchange completed
Jul 2 14:20:27	info	hostapd	vlan0: STA 00:0c:41:dc:09:e1 WPA: pairwise key exchange completed
Jul 2 14:20:26	info	hostapd	vlan0: STA 00:0c:41:dc:09:e1 IEEE 802.11: associated (aid 1, interface wlan0)
Jul 2 14:20:26	info	hostapd	vlan0: STA 00:0c:41:dc:09:e1 IEEE 802.11: authenticated
Jul 2 14:20:23	info	udhcp	Lease of 10.10.100.250 obtained, lease time 300
Jul 2 14:20:22	debug	udhcp	Sending discover...
Jul 2 14:20:22	info	udhcp	udhcp client (v0.9.8-pre) started

Severity	Description
debug	vlan0.11: RX decryptError (1) hIndex=36 decrypted=1
info	br0: topology change detected, propagating
info	br0: port 1(vlan0) entering forwarding state
info	br0: topology change detected, propagating
info	br0: port 2(vlan0) entering forwarding state
info	br0: port 1(vlan0) entering learning state
info	br0: port 2(vlan0) entering learning state
warn:	RF failed to complete in calibration window
warn	RF failed to complete in calibration window
info	device wlan0 entered promiscuous mode
info	device wlan0 entered promiscuous mode
warn	EXT2-fs warning: mounting unchecked fs, running e2fsck is recommended
info	rs52.11 wlan0.11: Device an 0cc4850000, IRQ 10
info	rs52.11 hwsdr: 0000c41: dA:30:7F
debug	vlan0.11: supported modes: 11A 11G 11B TURBO
warn	vlan0 receiver: mac 5:0 phy 4:1 analog 1:7 eeprom 2:4

On the right side of the screenshot, there is a help icon (question mark) and text: "This page lists the most recent events generated by this access point." Below that, it says: "The System Events Log shows stations associating, being authenticated, and other occurrences." and "The Kernel Log lists error conditions." There is also a "More..." link.

This page lists the most recent events generated by this access point.

It displays the System Events Log, which shows stations associating, being authenticated, and other occurrences.

It provides a Kernel Log, which lists error conditions, such as dropping frames.

The D-Link DWL-2210AP acquires its date and time information using the network time protocol (NTP). This data is reported in UTC format (also known as *Greenwich Mean Time*). You need to convert the reported time to your local time.

For information on setting the network time protocol, see “Enabling the Network Time Protocol Server” in this manual.

Statistics

To view transmit/receive statistics for a particular access point, navigate to **Status > Statistics** on the Administration Web pages for the access point you want to monitor.

The following figure shows the Transmit / Receive page for a two-radio AP. The Administration Web page for the one-radio AP will look slightly different.

Basic Settings

Cluster

Access Points

Users

Sessions

Status

Interfaces

Events

Statistics

Associations

Neighbors

Advanced

Ethernet

View transmit and receive statistics for this access point

Type	Ethernet		Radio	
Name	Internal	Guest	Internal	Guest
IP Address	10.10.100.250			
MAC Address	00:0C:41:0A:33:7E n/s		00:0C:41:0A:33:7E n/s	
VLAN ID				
SSID		default		Guest Instant002 Network

Transmit

Type	Ethernet		Radio	
Name	Internal	Guest	Internal	Guest
Total packets	183		902	
Total bytes	114741		344063	
Errors	0		0	

Receive

Type	Ethernet		Radio	
Name	Internal	Guest	Internal	Guest
Total packets	553		339	
Total bytes	41004		42209	
Errors	0		0	

? This page provides information about data transmitted and received by this access point.

The tables show total packets transmitted and received since the access point was booted, along with error rate information.

[More ...](#)

This page provides some basic information about the current access point and a real-time display of the transmit and receive statistics for this access point as described in the following table. All transmit and receive statistics shown are totals since the access point was last started. If the AP is rebooted, these figures indicate transmit/receive totals since the reboot.

Field	Description
IP Address	IP Address for the access point.
MAC Address	<p>Media Access Control (MAC) address for the specified interface.</p> <p>A MAC address is a permanent, unique hardware address for any device that represents an interface to the network. The MAC address is assigned by the manufacturer.</p> <p>The D-Link DWL-2210AP has a unique MAC address for each interface. A two-radio access point has a different MAC address for each interface on each of its two radios.</p>
VLAN ID	<p>Virtual LAN (VLAN) ID.</p> <p>A VLAN is a software-based, logical grouping of devices on a network that allow them to act as if they are connected to a single physical network, even though they may not be.</p> <p>VLANs can be used to establish internal and guest networks on the same access point.</p>
SSID	<p>Wireless network name. Also known as the SSID, this alphanumeric key uniquely identifies a wireless local area network.</p> <p>The SSID is set on the Basic Settings tab. (See “Provide Administrator Password and Wireless Network Name” in this manual.)</p>
Transmit and Receive Information	
Total Packets	Indicates total packets sent (in Transmit table) or received (in Received table) by this access point.
Total Bytes	Indicates total bytes sent (in Transmit table) or received (in Received table) by this access point.
Errors	Indicates total errors related to sending and receiving data on this access point.

Associated Wireless Clients

To view the client stations associated with a particular access point, navigate to **Status > Associations** on the Administration Web pages for the access point you want to monitor.

Network	Station	Status	Authenticated	Associated	From Station Packets	From Station Bytes	To Station Packets	To Station Bytes
Internal	00:0c:41:dc:09:e1	Yes	Yes	Yes	569	65184	417	327073

The associated stations are displayed along with information about packet traffic transmitted and received for each station.

Link Integrity Monitoring

The D-Link DWL-2210AP provides *link integrity monitoring* to continually verify its connection to each associated client (even when there is no data exchange occurring). To do this, the AP sends data packets to clients every few seconds when no other traffic is passing. This allows the access point to detect when a client goes out of range, even during periods when no normal traffic is exchanged. The client connection drops off the list of associated clients within 300 seconds of a client disappearing, even if they do not disassociate (but went out of range).

What is the Difference Between an Association and a Session?

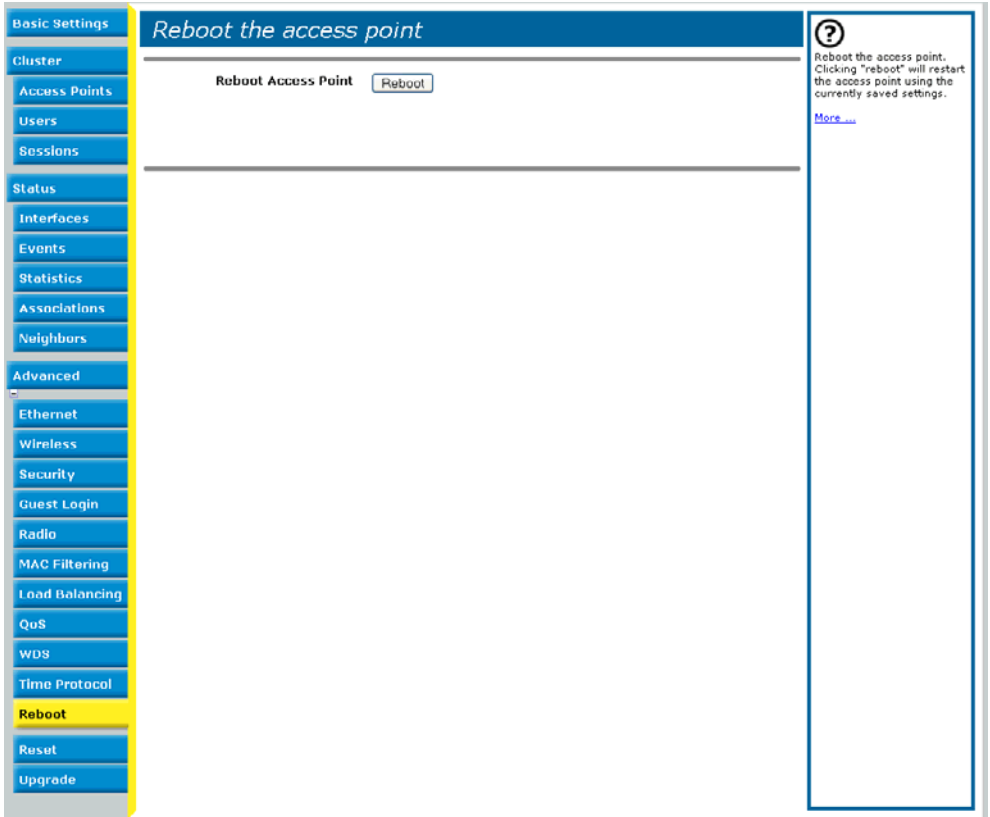
An *association* describes a client connection to a particular access point. A *session* describes a client connection to the network. A client network connection can shift from one clustered AP to another within the context of the same session. A client station can roam between APs and maintain the session.

For information on monitoring *sessions*, see “Understanding Session Monitoring Information” in this manual.

Rebooting the Access Point

For maintenance purposes or as a troubleshooting measure, you can reboot the D-Link DWL-2210AP as follows.

1. Click the **Advanced > Reboot** tab.



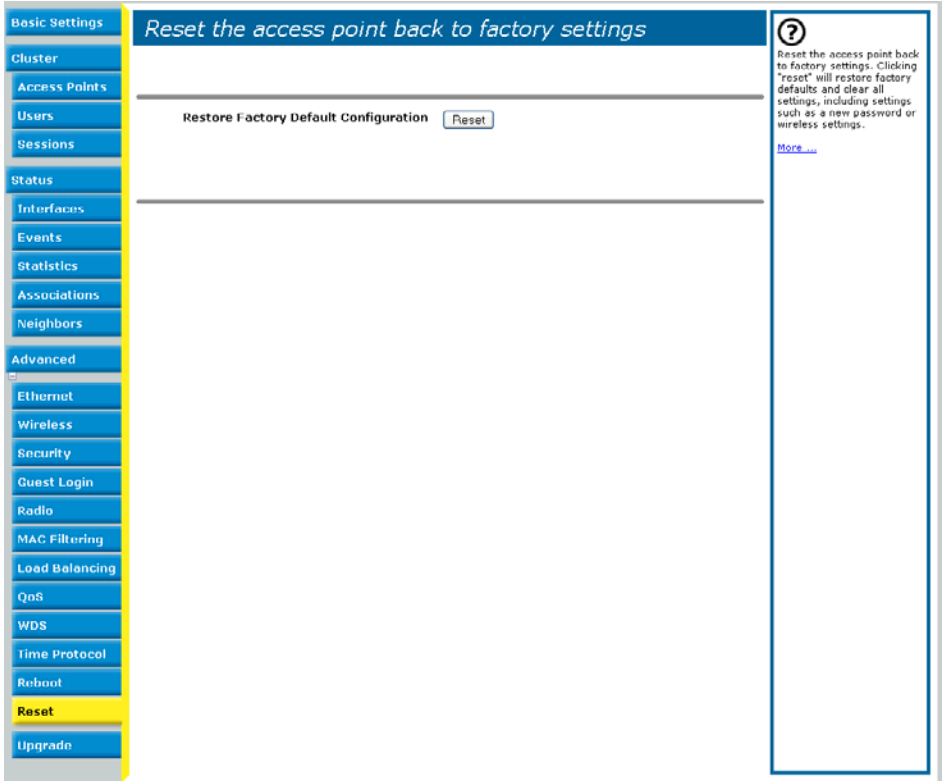
2. Click the **Reboot** button.

The AP reboots.

Resetting the Configuration

If you are experiencing extreme problems with the D-Link DWL-2210AP and have tried all other troubleshooting measures, use the **Reset Configuration** function. This will restore factory defaults and clear all settings, including settings such as a new password or wireless settings.

1. Click the **Advanced > Reset** tab.



2. Click the **Reset** button.

Factory defaults are restored.

Keep in mind that if you do reset the configuration from this page, you are doing so for this access point only; not for other access points in the cluster. For information on the factory default settings, see "Default Settings for the D-Link DWL-2210AP" in this manual.

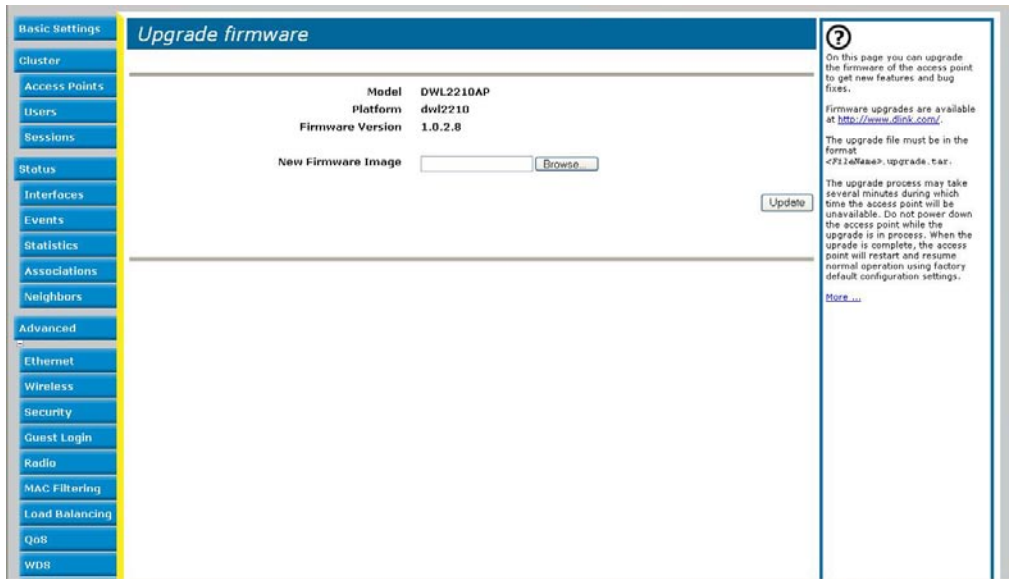
Upgrading the Firmware

As new versions of the D-Link DWL-2210AP firmware become available, you can upgrade the firmware on your devices to take advantages of new features and enhancements.

You must do this per access point; you cannot upgrade firmware automatically across the cluster. Keep in mind that a successful firmware upgrade restores the access point configuration to the factory defaults. (See “Default Settings for the D-Link DWL-2210AP” in this manual.)

To upgrade the firmware on a particular access point:

1. Navigate to **Advanced > Upgrade** on the Administration Web pages for that access point.



Information about the current firmware version is displayed and an option to upgrade a new firmware image is provided.

2. If you know the path to the **New Firmware Image** file, enter it in the textbox. Otherwise, click the **Browse** button and locate the firmware image file.

The firmware upgrade file supplied must be in the format <FileName>.upgrade.tar. Do not attempt to use <FileName>.bin files or files of other formats for the upgrade; these will not work.

Update

Click **Update** to apply the new firmware image.

Upon clicking **Update** for the firmware upgrade, a popup confirmation window is displayed that describes the upgrade process.

Click **OK** to confirm the upgrade, and start the process.



The firmware upgrade process begins once you click Update and then OK in the popup confirmation window.

The upgrade process may take several minutes during which time the access point will be unavailable. Do not power down the access point while the upgrade is in process. When the upgrade is complete, the access point will restart and resume normal operation using the factory default configuration settings.

Verifying the Firmware Upgrade

To verify that the firmware upgrade completed successfully, check the firmware version shown on the Advanced > Upgrade tab (and also on the Basic Settings tab). If the upgrade was successful, the updated version name or number will be indicated.

Neighbors

The status page for “neighboring access points” provides real-time statistics for all access points within range of the access point on which you are viewing the Administration Web pages.

To view information about other access points on the wireless network, navigate to **Status > Neighbors**.

The screenshot displays the 'View neighboring access points' configuration page. On the left is a vertical sidebar with menu items: Basic Settings, Cluster, Access Points, Users, Sessions, Status, Interfaces, Events, Statistics, Associations, Neighbors (highlighted in yellow), and Advanced. The main content area has a blue header with the title 'View neighboring access points'. Below the header, there is a section for 'AP Detection' with two radio buttons: 'Enabled' (unselected) and 'Disabled' (selected). To the right of this section is an 'Update' button. The main content area contains the text 'AP detection is disabled.' On the right side of the page is a help panel with a question mark icon, a paragraph of text explaining the page's function, and a 'More ...' link.

Information provided on neighboring access points is described in the following table:

Field	Description
MAC Address	<p>Shows the MAC address of the neighboring access point.</p> <p>A MAC address is a hardware address that uniquely identifies each node of a network.</p>
Beacon Interval	<p>Shows the Beacon interval being used by this access point.</p> <p>Beacon frames are transmitted by an access point at regular intervals to announce the existence of the wireless network. The default behavior is to send a beacon frame once every 100 milliseconds (or 10 per second).</p> <p>The Beacon Interval is set on Advanced > Radio Settings. (See “Configuring Radio Settings” in this manual.)</p>
Type	<p>Indicates the type of device:</p> <ul style="list-style-type: none"> • AP indicates the neighboring device is an access point that supports the IEEE 802.11 Wireless Networking Framework in Infrastructure Mode. • Ad hoc indicates a neighboring station running in Ad hoc Mode. Stations set to ad hoc mode communicate with each other directly, without the use of a traditional access point. Ad-hoc mode is an IEEE 802.11 Wireless Networking Framework also referred to as <i>peer-to-peer</i> mode or an <i>Independent Basic Service Set</i> (IBSS).
SSID	<p>The <i>Service Set Identifier</i> (SSID) for the access point.</p> <p>The SSID is an alphanumeric string of up to 32 characters that uniquely identifies a wireless local area network. It is also referred to as the <i>Network Name</i>.</p> <p>The SSID is set in Basic Settings. (See “Configuring Basic Settings” in this manual) or in Advanced > Wireless (see “Setting the Wireless Interface” in this manual.)</p> <p>A Guest network and an Internal network running on the same access point must always have two different network names.</p>
Privacy	<p>Indicates whether there is any security on the neighboring device.</p> <ul style="list-style-type: none"> • Off indicates that the Security mode on the neighboring device is set to “plain text” mode (no security). • On indicates that the neighboring device has some security in place. <p>Security is configured on the AP at Advanced > Security. For more information on security settings, see “Configuring Security” in this manual.</p>
WPA	<p>Indicates whether WPA security is “on” or “off” for this access point.</p>

Field	Description
Band	<p>This indicates the IEEE 802.11 mode being used on this access point. (For example, IEEE 802.11b and IEEE 802.11g.)</p> <p>The number shown indicates the mode according to the following map:</p> <ul style="list-style-type: none"> • 2.4 indicates IEEE 802.11b mode or IEEE 802.11g mode
Channel	<p>Shows the channel on which the access point is currently broadcasting.</p> <p>The Channel defines the portion of the radio spectrum that the radio uses for transmitting and receiving.</p> <p>The channel is set in Advanced > Radio Settings. (See “Configuring Radio Settings” in this manual.)</p>
Rate	<p>Shows the rate (in megabits per second) at which this access point is currently transmitting.</p> <p>The current rate will always be one of the rates shown in Supported Rates.</p>
Signal	<p>Indicates the strength of the radio signal emitting from this access point as measured in decibels (Db).</p>
# of Beacons	<p>Shows the total number of beacons transmitted by this access point since it was last booted.</p>
Last Beacon	<p>Shows the date and time of the most recent beacon was transmitted from the access point.</p>
Rates	<p>Shows supported and basic (advertised) rate sets for the neighboring access point. Rates are shown in megabits per second (Mbps).</p> <p>All Supported Rates are listed, with Basic Rates shown in bold.</p> <p>Rate sets are configured on Advanced > Radio Settings. (See “Configuring Radio Settings” in this manual.) The rates shown for an access point will always be the rates currently specified for that AP in its Radio Settings.</p>

Appendix A. Configuring Security Settings on Wireless Clients

Typically, users will configure security on their wireless clients for access to many different networks (access points). The list of “Available Networks” will change depending on the location of the client and which APs are online and detectable in that location.* Once an AP has been detected by the client and security is configured for it, it remains in the client’s list of networks but shows as either reachable or unreachable depending on the situation. For each network (AP) you want to connect to, configure security settings on the client to match the security mode being used by that network.

We describe security setup on a client that uses Microsoft Windows client software for wireless connectivity. The Windows client software is used as the example because of its widespread availability on Windows computers and laptops. These procedures will vary slightly if you use different software on the client (such as Funk Odyssey), but the configuration information you need to provide is the same.

The recommended sequence for security configuration is (1) set up security on the access point, and (2) configure security on each of the wireless clients.

We expect that initially, you will connect to an access point that has no security set (plain text mode) from an unsecure wireless client. With this initial connection, you can go to the access point Administration Web pages and configure a security mode (Advanced > Security).

When you reconfigure the access point with a security setting and click “Update”, your wireless client will be disassociated and you will lose connectivity to the AP Administration Web pages. In some cases, you may need to make additional changes to the AP security settings before configuring the client. Therefore, you must have a backup Ethernet (wired) connection.

The following sections describe how to set up each of the supported security modes on wireless clients of a network served by the D-Link DWL-2210AP.

- Network Infrastructure and Choosing Between Built-in or External Authentication Server
- Make Sure the Wireless Client Software is Up-to-Date
- Accessing the Microsoft Windows Wireless Client Security Settings
- Configuring a Client to Access an Unsecure Network (Plain Text mode)
- Configuring Static WEP Security on a Client
- Configuring IEEE 802.1x Security on a Client
- Configuring WPA with RADIUS Security on a Client
- Configuring WPA-PSK Security on a Client

* The exception to this is if the access point is set to prohibit the broadcast of its network name. In this case the SSID will not show up in the list of Available Networks on the client. Instead, the client must have the exact network name configured in the network connection properties before it will be able to connect.

- Configuring an External RADIUS Server to Recognize the D-Link DWL-2210AP
- Obtaining a TLS-EAP Certificate for a Client

Network Infrastructure and Choosing Between Built-in or External Authentication Server

Network security configurations including *Public Key Infrastructures* (PKI), *Remote Authentication Dial-in User Server* (RADIUS) servers, and *Certificate Authority* (CA) can vary a great deal from one organization to the next in terms of how they provide *Authentication*, *Authorization*, and *Accounting* (AAA). Ultimately, the particulars of your infrastructure will determine how clients should configure security to access the wireless network. Rather than try to predict and address the details of every possible scenario, this document provides general guidelines about each type of client configuration supported by the D-Link DWL-2210AP.

I Want to Use the Built-in Authentication Server (EAP-PEAP)

If you do not have a RADIUS server or PKI infrastructure in place and/or are unfamiliar with many of these concepts, we strongly recommend setting up the D-Link DWL-2210APs with security that uses the *Built-in Authentication Server* on the AP. This will mean setting up the AP to use either IEEE 802.1x or WPA with RADIUS security mode. (The built-in authentication server uses EAP-PEAP authentication protocol.)

- If the D-Link DWL-2210AP is set up to use IEEE 802.1x mode and the Built-in Authentication Server, then configure wireless clients as described in “IEEE 802.1x Client Using EAP/PEAP” in this manual.
- If the D-Link DWL-2210AP is configured to use WPA with RADIUS mode and the Built-in Authentication Server, configure wireless clients as described in “WPA with RADIUS Client Using EAP/PEAP” in this manual.

I Want to Use an External RADIUS Server with EAP-TLS Certificates or EAP-PEAP

We make the assumption that if you have an external RADIUS server and PKI/CA setup, you will know how to configure client security options appropriate to your security infrastructure beyond the fundamental suggestions given here. Topics covered here that particularly relate to client security configuration in a RADIUS - PKI environment are:

- “IEEE 802.1x Client Using EAP/TLS Certificate” in this manual.
- “WPA with RADIUS Client Using EAP-TLS Certificate” in this manual.
- “Configuring an External RADIUS Server to Recognize the D-Link DWL-2210AP” in this manual.
- “Obtaining a TLS-EAP Certificate for a Client” in this manual.

Details on how to configure an EAP-PEAP client with an external RADIUS server are not covered in this document.

Make Sure the Wireless Client Software is Up-to-Date

Before starting out, please keep in mind that service packs, patches, and new releases of drivers and other supporting technologies for wireless clients are being generated at a fast pace. A common problem encountered in client security setup is not having the right driver or updates to it on the client. For example; if you are setting up WPA on the client, make sure you have a driver installed that supports WPA, which is a relatively new technology. Even many client cards currently available do not ship from the factory with the latest drivers.

Accessing the Microsoft Windows Wireless Client Security Settings

Generally, on Windows XP there are two ways to get to the security properties for a wireless client:

1. From the wireless connection icon on the Windows task bar:

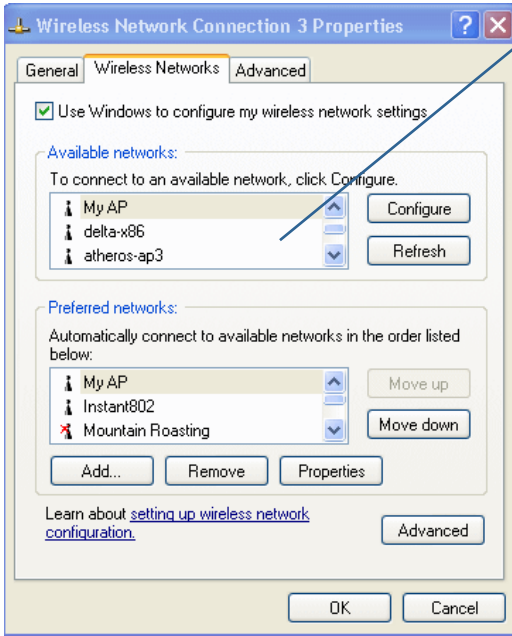
- Right-click on the Wireless connection icon in your Windows task bar and select **View available wireless networks**.
- Select the SSID of the network to which you want to connect and click **Advanced** to bring up the Wireless Network Connection Properties dialog.

-Or-

1. From the Windows Start menu at the left end of the task bar:

- From the Windows Start menu on the task bar, choose **Start > My Network Places** to bring up the Network Connections window.
- From the Network Tasks menu on the left, click **View Network Connections** to bring up the Network Connections window.
- Select the Wireless Network Connection you want to configure, right-mouse click and choose **View available wireless networks**.
- Select the SSID of the network to which you want to connect and click **Advanced** to bring up the Wireless Network Connection Properties dialog.

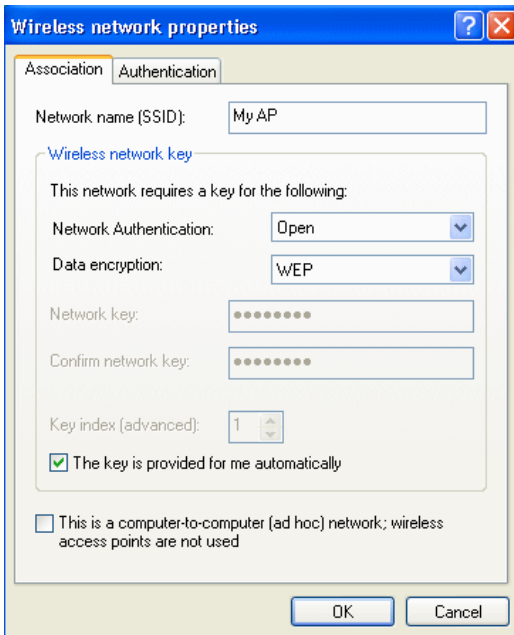
The Wireless Networks tab (which should be automatically displayed) lists Available networks and Preferred networks.



List of available networks will change depending on client location. Each network (or access point) that is detected by the client shows up in this list. (“Refresh” updates the list with current information.)

For each network you want to connect to, configure security settings on the client to match the security mode being used by that network.

Note: The exception to this is if the AP is configured to prohibit broadcast of its network name, the name will not show on this list. In that case you would need to type in the exact network name to be able to connect to it.



- From the list of “Available networks”, select the SSID of the network to which you want to connect and click **Configure**.

This brings up the Wireless Network Connection Properties dialog with the Association and Authentication tabs for the selected network.

Use this dialog for configuring all the different types of client security described in the following sections. Make sure that the Wireless Network Properties dialog you are working in pertains to the Network Name (SSID) for the network you want to reach on the wireless client you are configuring.

Configuring a Client to Access an Unsecure Network (Plain Text mode)

If the access point or wireless network to which you want to connect is configured as “Plain Text” security mode (no security), you need to configure the client accordingly. A client using no security to connect is configured with Network Authentication “Open” to that network and Data Encryption “Disabled” as described below.

If you do have security configured on a client for properties of an unsecure network, the security settings actually can prevent successful access to the network because of the mismatch between client and access point security configurations.

To configure the client to not use any security, bring up the client Network Properties dialog and configure the following settings.

The screenshot shows the 'Wireless network properties' dialog box with the 'Authentication' tab selected. The 'Network name (SSID)' is 'My AP'. Under 'Wireless network key', it says 'This network requires a key for the following:'. The 'Network Authentication' dropdown is set to 'Open' and 'Data encryption' is set to 'Disabled'. There are also fields for 'Network key', 'Confirm network key', and 'Key index (advanced)' set to 1. At the bottom, there are 'OK' and 'Cancel' buttons. Two callout boxes are present: one pointing to the 'Network Authentication' dropdown with the text 'Set Network Authentication to Open', and another pointing to the 'Data encryption' dropdown with the text 'Set Data Encryption to Disabled'.

Association Tab

Network Authentication Open

Data Encryption Disabled

Configuring Static WEP Security on a Client

Static *Wired Equivalent Privacy* (WEP) encrypts data moving across a wireless network based on a static (non-changing) key. The encryption algorithm is a “stream” cipher called RC4. The access point uses a key to transmit data to the client stations. Each client must use that same key to decrypt data it receives from the access point. Different clients can use different keys to transmit data to the access point. (Or they can all use the same key, but this is less secure because it means one station can decrypt the data being sent by another.)

If you configured the D-Link DWL-2210AP to use Static WEP security mode . . .

D-Link
Building Networks for People

Air Premier™
DWL-2210AP 2.4Ghz Wireless Adaptive Access Point

Basic Settings | **Modify security settings that apply to the Internal Network**

Cluster

Access Points

Users

Sessions

Status

Interfaces

Events

Statistics

Associations

Neighbors

Advanced

Ethernet

Wireless

Security

Guest Login

Radio

Broadcast SSID Allow Prohibit

Security Mode **Static WEP**

Transfer Key Index **1**

Key Length 64 bits 128 bits

Key Type ASCII Hex

Characters Required **26**

WEP Keys

1:

2:

3:

4:

Authentication Algorithms **Both**

? Use this page to configure a security mode for the access point.

Plain-text mode (no security)

Static Wired Equivalent Privacy (WEP)

IEEE 802.1x

Wi-Fi Protected Access (WPA) with Remote Authentication Dial-In User Service (RADIUS)

WPA with Pre-Shared Key (PSK).

WPA with RADIUS is the recommended mode because it leverages TKIP and CCMP(AES) encryption algorithms and dynamic pre-shared keys. The D-Link® DWL2210AP uses an embedded RADIUS server so you do not need to provide one.

The plain-text, non-secure mode is only recommended for initial setup or problem-solving use.

These settings apply to the Internal network; the Guest network always uses plain-text mode.

[More ...](#)

... then configure WEP security on each client as follows.

The screenshot shows the 'Wireless network properties' dialog box with the 'Authentication' tab selected. The 'Network name (SSID)' is 'My AP'. The 'Network Authentication' is set to 'Open' and 'Data encryption' is set to 'WEP'. The 'Network key' and 'Confirm network key' fields are filled with dots. The 'Key index (advanced)' is set to '1'. The checkbox 'The key is provided for me automatically' is unchecked. The 'OK' and 'Cancel' buttons are at the bottom right.

Association Tab

Network Authentication	<p>“Open” or “Shared”, depending on how you configured this option on the access point.</p> <p>Note: When the Authentication Algorithm on the access point is set to “Both”, clients set to either Shared or Open can associate with the AP. Clients configured to use WEP in Shared mode must have a valid WEP key in order to associate with the AP. Clients configured to use WEP as an Open system can associate with the AP even without a valid WEP key (but a valid key will be required to actually view and exchange data). For more information, see Administrators Guide and Online Help on the access point.</p>
Data Encryption	WEP
Network Key	<p>Provide the WEP key you entered on the access point Security settings in the Transfer Key Index position.</p> <p>For example, if the Transfer Key Index on the access point is set to “1”, then for the client Network Key specify the WEP Key you entered as WEP Key 1 on the access point.</p>
Key Index	<p>Set key index to indicate which of the WEP keys specified on the access point Security page will be used to transfer data from the client back to the access point.</p> <p>For example, you can set this to 1, 2, 3, or 4 if you have all four WEP keys configured on the access point.</p>
The key is provided for me automatically	Disable this option (click to uncheck the box).

Authentication Tab

Enable IEEE 802.1x authentication for this network

Make sure that IEEE 802.1x authentication is disabled (box should be unchecked).
(Setting the encryption mode to WEP should automatically disable authentication.)

Click **OK** on the Wireless Network Properties dialog to close it and save your changes.

Connecting to the Wireless Network with a Static WEP Client

Static WEP clients should now be able to associate and authenticate with the access point. As a client, you will not be prompted for a WEP key. The WEP key configured on the client security settings is automatically used when you connect.

Configuring IEEE 802.1x Security on a Client

IEEE 802.1x is the standard defining port-based authentication and infrastructure for doing key management. *Extensible Authentication Protocol* (EAP) messages sent over an IEEE 802.11 wireless network using a protocol called EAP Encapsulation Over LANs (EAPOL). IEEE 802.1x provides dynamically-generated keys that are periodically refreshed. An RC4 stream cipher is used to encrypt the frame body and cyclic redundancy checking (CRC) of each 802.11 frame.

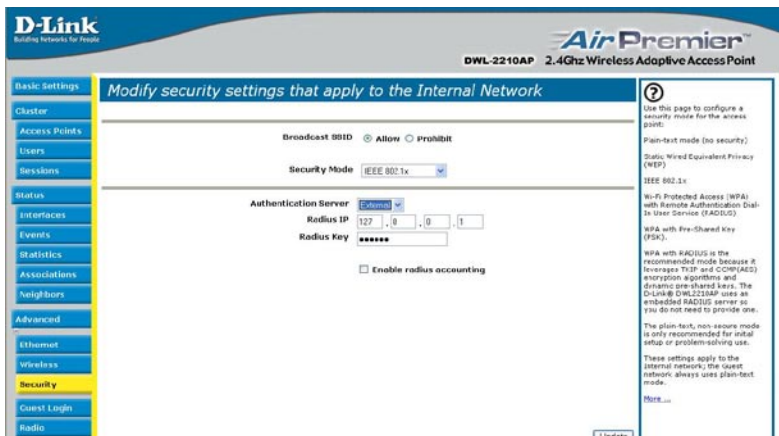
IEEE 802.1x Client Using EAP/PEAP

The Built-In Authentication Server on the D-Link DWL-2210AP uses Protected *Extensible Authentication Protocol* (EAP) referred to here as “EAP/PEAP”

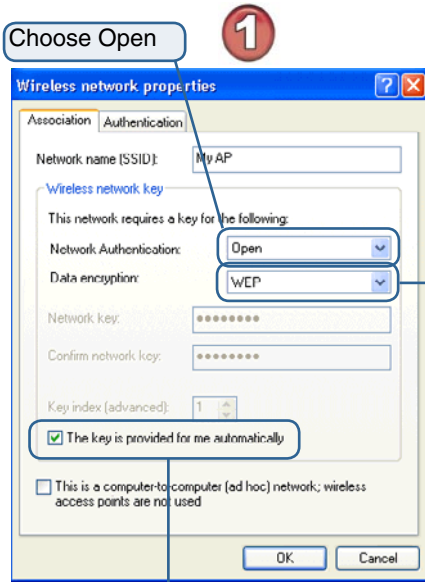
- If you are using the Built-in Authentication server with “IEEE 802.1x” security mode on the D-Link DWL-2210AP, then you will need to set up wireless clients to use PEAP.
- Additionally, you may have an external RADIUS server that uses EAP/PEAP. If so, you will need to (1) add the D-Link DWL-2210AP to the list of RADIUS server clients, and (2) configure your IEEE 802.1x wireless clients to use PEAP.

The following example assumes you are using the Built-in Authentication server that comes with the D-Link DWL-2210AP. If you are setting up EAP/PEAP on a client of an AP that is using an external RADIUS server, the client configuration process will differ somewhat from this example especially with regard to certificate validation.

If you configured the D-Link DWL-2210AP to use IEEE 802.1x security mode . . .

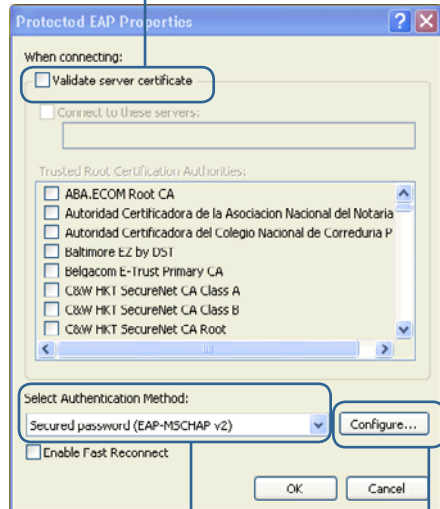


. . . then configure IEEE 802.1x security with PEAP authentication on each client as follows.



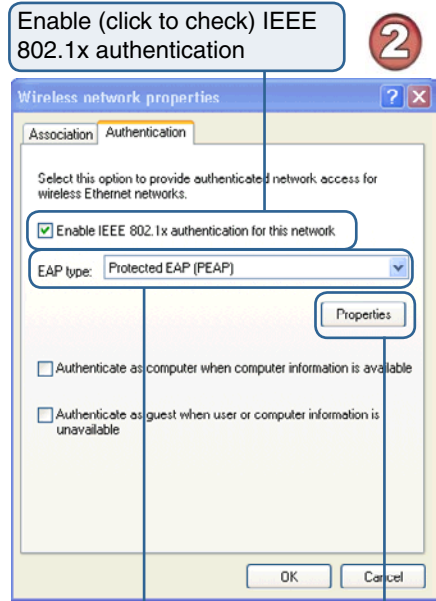
Enable auto key option

Disable (click to uncheck) "Validate server certificate"



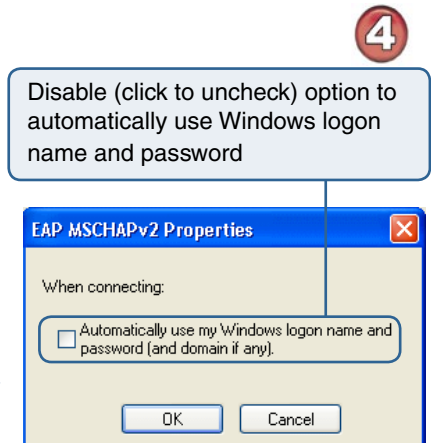
Choose "secured password (EAP-MSCHAP v2)"

... then click "Configure"



Choose Protected EAP (PEAP)

... then, click "Properties"



Disable (click to uncheck) option to automatically use Windows logon name and password

1. Configure the following settings on the Association tab on the Network Properties dialog.

Association Tab

Network Authentication	Open
Data Encryption	WEP Note: An RC4 stream cipher is used to encrypt the frame body and cyclic redundancy checking (CRC) of each IEEE 802.11 frame. this is the same encryption algorithm as is used for Static WEP; therefore, the data encryption method configured on the client for this mode is WEP.
This key is provided for me automatically	Enable (click to check) this option

2. Configure this setting on the Authentication tab.

Authentication Tab

EAP Type	Choose "Protected EAP (PEAP)".
----------	--------------------------------

3. Click **Properties** to bring up the Protected EAP Properties dialog and configure the following settings.

Protected EAP Properties Dialog

Validate Server Certificate	Disable this option (click to uncheck the box). Note: This example assumes you are using the Built-in Authentication server on the AP. If you are setting up EAP/PEAP on a client of an AP that is using an external RADIUS server, you might certificate validation and choose a certificate, depending on your infrastructure.
Select Authentication Method	Choose "Secured password (EAP-MSCHAP v2)".

4. Click **Configure** to bring up the EAP MSCHAP v2 Properties dialog.

On this dialog, disable (click to uncheck) the option to "Automatically use my Windows login name . . ." etc.

Click **OK** on all dialogs (starting with the EAP MSCHAP v2 Properties dialog) to close and save your changes.

Logging on to the Wireless Network with an IEEE 802.1x PEAP Client

IEEE 802.1x PEAP clients should now be able to associate with the access point. Client users will be prompted for a user name and password to authenticate with the network.

IEEE 802.1x Client Using EAP/TLS Certificate

Extensible Authentication Protocol (EAP) Transport Layer Security (TLS), or EAP-TLS, is an authentication protocol that supports the use of smart cards and certificates. You have the option of using EAP-TLS with both WPA with RADIUS and IEEE 802.1x modes if you have an external RADIUS server on the network to support it.

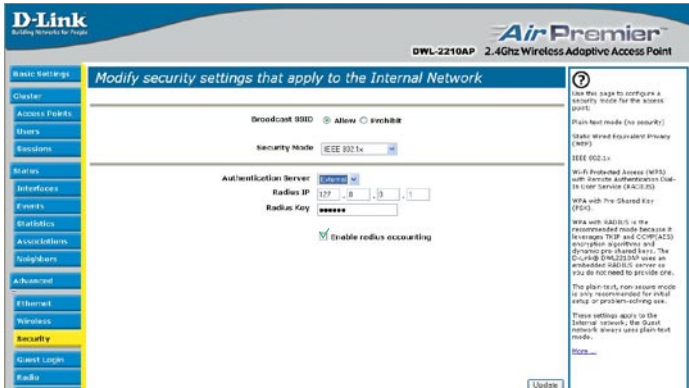
If you want to use IEEE 802.1x mode with EAP-TLS certificates for authentication and authorization of clients, you must have an external RADIUS server and a *Public Key Authority Infrastructure (PKI)*, including a *Certificate Authority (CA)*, server configured on your network. It is beyond the scope of this document to describe these configuration of the RADIUS server, PKI, and CA server. Consult the documentation for those products.

Some good starting points available on the Web for the Microsoft Windows PKI software are: “How to Install/Uninstall a Public Key Certificate Authority for Windows 2000” at <http://support.microsoft.com/default.aspx?scid=kb;EN-US;231881> and How to Configure a Certificate Server at <http://support.microsoft.com/default.aspx?scid=kb;en-us;318710#3>.

To use this type of security, you must do the following:

1. Add the D-Link DWL-2210AP to the list of RADIUS server clients. (See “Configuring an External RADIUS Server to Recognize the D-Link DWL-2210AP” in this manual.)
2. Configure the D-Link DWL-2210AP to use your RADIUS server (by providing the RADIUS server IP address as part of the “IEEE 802.1x” security mode settings).
3. Configure wireless clients to use IEEE 802.1x security and “Smart Card or other Certificate” as described in this section.
4. Obtain a certificate for this client as described in “Obtaining a TLS-EAP Certificate for a Client” in this manual.

If you configured the D-Link DWL-2210AP to use IEEE 802.1x security mode with an external RADIUS server . . .



. . . then configure IEEE 802.1x security with certificate authentication on each client as follows.

Choose WEP
Data Encryption
mode

Choose Open

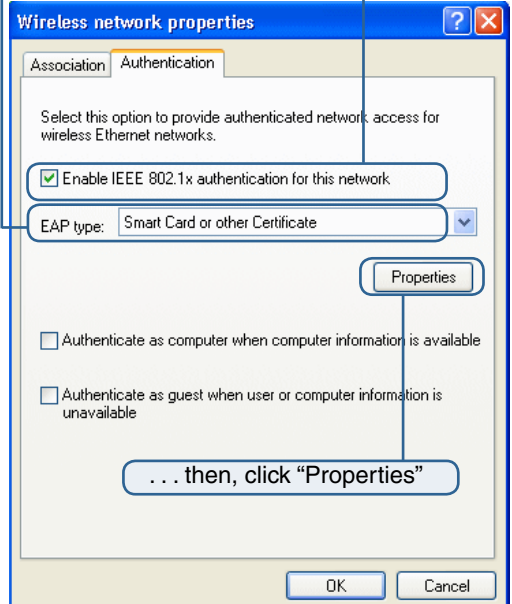
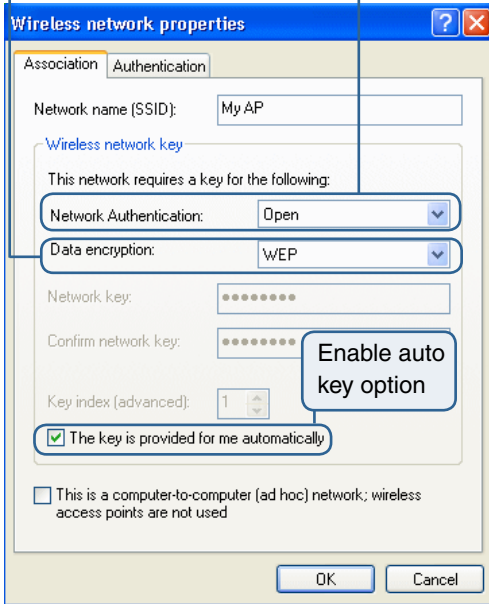
Choose Smart Card/Certificate

Enable (click to check) IEEE
802.1x authentication

Enable auto
key option

Properties

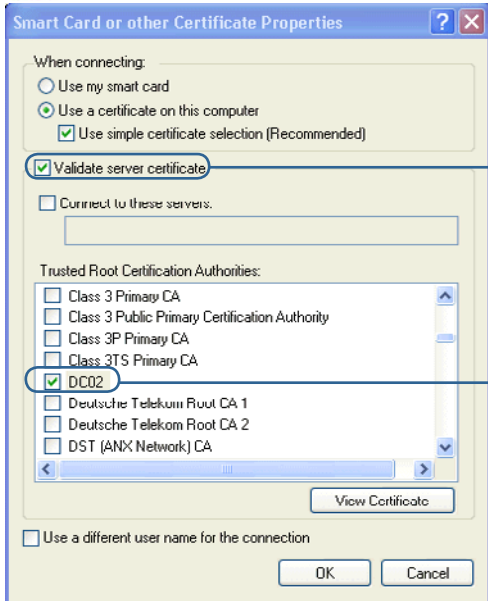
. . . then, click "Properties"



1

2

3



Enable (click to check) “validate server certificate.”

Select (check) the name of certificate on this client (downloaded from RADIUS server in a prerequisite procedure)

1. Configure the following settings on the Association tab on the Network Properties dialog.

Association Tab

Network Authentication
Data Encryption

Open
WEP

Note: An RC4 stream cipher is used to encrypt the frame body and cyclic redundancy checking (CRC) of each IEEE 802.11 frame. This is the same encryption algorithm as is used for Static WEP; therefore, the data encryption method configured on the client for this mode is WEP.

This key is provided for me automatically

Enable (click to check)

2. Configure these settings on the Authentication tab.

Authentication Tab

Enable IEEE 802.1x authentication for this network

Enable (click to check) this option.

EAP Type

Choose Smart Card or other Certificate.

3. Click **Properties** to bring up the Smart Card or other Certificate Properties dialog and enable the “Validate server certificate” option.

Smart Card or other Certificate Properties Dialog

Validate Server Certificate Enable this option (click to check the box).

Certificates In the certificate list shown, select the certificate for this client.

Click **OK** on all dialogs to close and save your changes.

4. To complete the client configuration you must now obtain a certificate from the RADIUS server and install it on this client. For information on how to do this see “Obtaining a TLS-EAP Certificate for a Client” in this manual.

Connecting to the Wireless Network with an IEEE 802.1x Client Using a Certificate

IEEE 802.1x clients should now be able to connect to the access point using their TLS certificates. The certificate you installed is used when you connect, so you will not be prompted for login information. The certificate is automatically sent to the RADIUS server for authentication and authorization.

Configuring WPA with RADIUS Security on a Client

Wi-Fi Protected Access (WPA) with Remote Authentication Dial-In User Service (RADIUS) is a Wi-Fi Alliance subset of IEEE 802.11i, which includes Temporal Key Integrity Protocol (TKIP), and Counter mode/CBC-MAC Protocol IEEE. This mode requires the use of a RADIUS server to authenticate users, and configuration of user accounts on the access point.

When you configure WPA with RADIUS security mode on the access point, you have a choice of whether to use the Built-in Authentication Server or an external RADIUS server that you provide.

The D-Link DWL-2210AP Built-in Authentication Server supports Protected *Extensible Authentication Protocol* (EAP) known as “EAP/PEAP” and *Microsoft Challenge Handshake Authentication Protocol Version 2* (MSCHAP V2), which provides authentication for point-to-point (PPP) connections between a Windows-based computer and network devices such as access points.

So, if you configure the network (access point) to use security mode and choose the Built-in Authentication server, you must configure client stations to use WPA with RADIUS and EAP/PEAP.

If you configure the network (access point) to use this security mode with an external RADIUS server, you must configure the client stations to use WPA with RADIUS and whichever security protocol your RADIUS server is configured to use.

WPA with RADIUS Client Using EAP/PEAP

The Built-In Authentication Server on the D-Link DWL-2210AP uses Protected *Extensible Authentication Protocol* (EAP) known as “EAP/PEAP”.

- If you are using the Built-in Authentication server with “WPA with RADIUS” security mode on the D-Link DWL-2210AP, then you will need to set up wireless clients to use PEAP.
- Additionally, you may have an external RADIUS server that uses EAP/PEAP. If so, you will need to (1) add the D-Link DWL-2210AP to the list of RADIUS server clients, and (2) configure your “WPA with RADIUS” wireless clients to use PEAP.

The following example assumes you are using the Built-in Authentication server that comes with the D-Link DWL-2210AP. If you are setting up EAP/PEAP on a client of an AP that is using an external RADIUS server, the client configuration process will differ somewhat from this example especially with regard to certificate validation.

If you configured the D-Link DWL-2210AP to use WPA with RADIUS security mode and to use either the Built-in Authentication Server or an external RADIUS server that uses EAP/PEAP . . .

First set up user accounts on the access point (Cluster > User Management). . . .

. . . then configure WPA security with PEAP authentication on each client as follows.

1 Choose WPA

Choose either TKIP or AES for the Data Encryption mode

2 Choose Protected EAP (PEAP)

... then, click "Properties"

3 Disable (click to uncheck) "Validate server certificate"

Choose "secured password (EAP-MSCHAP v2)"

... then click "Configure"

4 Disable (click to uncheck) option to automatically use Windows logon name and password

1. Configure the following settings on the Association and Authentication tabs on the Network Properties dialog.

Association Tab

Network Authentication	WPA
Data Encryption	TKIP or AES depending on how this option is configured on the access point. Note: When the Cipher Suite on the access point is set to “Both”, then TKIP clients with a valid TKIP key and AES clients with a valid CCMP (AES) key can associate with the access point. For more information, see Administrators Guide and Online Help on the access point.

2. Configure this setting on the Authentication tab.

Authentication Tab

EAP Type	Choose “Protected EAP (PEAP)”
-----------------	-------------------------------

3. Click **Properties** to bring up the Protected EAP Properties dialog and configure the following settings.

Protected EAP Properties Dialog

Validate Server Certificate	Disable this option (click to uncheck the box). Note: This example assumes you are using the Built-in Authentication server on the AP. If you are setting up EAP/PEAP on a client of an AP that is using an external RADIUS server, you might certificate validation and choose a certificate, depending on your infrastructure.
Select Authentication Method	Choose “Secured password (EAP-MSCHAP v2)”

4. Click **Configure** to bring up the EAP MSCHAP v2 Properties dialog.

On this dialog, disable (click to uncheck) the option to “Automatically use my Windows login name . . .etc. so that upon login you will be prompted for user name and password.

Click **OK** on all dialogs (starting with the EAP MSCHAP v2 Properties dialog) to close and save your changes.

Logging on to the Wireless Network with a WPA PEAP Client

“WPA with RADIUS” PEAP clients should now be able to associate with the access point. Client users will be prompted for a user name and password to authenticate with the network.

WPA with RADIUS Client Using EAP-TLS Certificate

Extensible Authentication Protocol (EAP) Transport Layer Security (TLS), or EAP-TLS, is an authentication protocol that supports the use of smart cards and certificates. You have the option of using EAP-TLS with both WPA with RADIUS and IEEE 802.1x modes if you have an external RADIUS server on the network to support it.

If you want to use IEEE 802.1x mode with EAP-TLS certificates for authentication and authorization of clients, you must have an external RADIUS server and a *Public Key Authority Infrastructure (PKI)*, including a *Certificate Authority (CA)*, server configured on your network. It is beyond the scope of this document to describe these configuration of the RADIUS server, PKI, and CA server. Consult the documentation for those products.

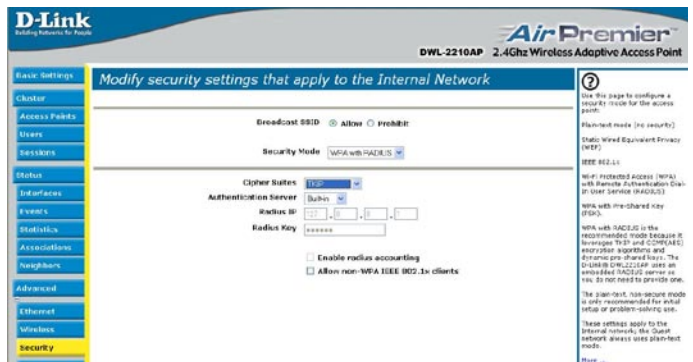
Some good starting points available on the Web for the Microsoft Windows PKI software are: “How to Install/Uninstall a Public Key Certificate Authority for Windows 2000” at <http://support.microsoft.com/default.aspx?scid=kb;EN-US;231881> and How to Configure a Certificate Server at <http://support.microsoft.com/default.aspx?scid=kb;en-us;318710#3>.

To use this type of security, you must do the following:

1. Add the D-Link DWL-2210AP to the list of RADIUS server clients. (See “Configuring an External RADIUS Server to Recognize the D-Link DWL-2210AP” in this manual.)
2. Configure the D-Link DWL-2210AP to use your RADIUS server (by providing the RADIUS server IP address as part of the “WPA with RADIUS” security mode settings).
3. Configure wireless clients to use WPA security and “Smart Card or other Certificate” as described in this section.
4. Obtain a certificate for this client as described in “Obtaining a TLS-EAP Certificate for a Client” in this manual.

If you configured the D-Link DWL-2210AP to use WPA with RADIUS security mode with an external RADIUS server . . .

. . . then configure WPA security with certificate authentication on each client as shown on the following page.



1

Wireless network properties

Association Authentication

Network name (SSID): My AP

Wireless network key

This network requires a key for the following:

Network Authentication: WPA

Data encryption: TKIP

Network key:

Confirm network key:

Key index (advanced): 1

The key is provided for me automatically

This is a computer-to-computer (ad hoc) network; wireless access points are not used

OK Cancel

Choose WPA

Choose either TKIP or AES for the Data Encryption mode

2

Choose Smart Card or other certificate and enable "Authenticate as computer when info is available"

Then click "Properties"

Wireless network properties

Association Authentication

Select this option to provide authenticated network access for wireless Ethernet networks.

Enable IEEE 802.1x authentication for this network

EAP type: Smart Card or other Certificate

Properties

Authenticate as computer when computer information is available

Authenticate as guest when user or computer information is unavailable

OK Cancel

3

Smart Card or other Certificate Properties

When connecting:

Use my smart card

Use a certificate on this computer

Use simple certificate selection (Recommended)

Validate server certificate

Connect to these servers:

Trusted Root Certification Authorities:

- Class 3 Primary CA
- Class 3 Public Primary Certification Authority
- Class 3P Primary CA
- Class 3TS Primary CA
- DC02
- Deutsche Telekom Root CA 1
- Deutsche Telekom Root CA 2
- DST (ANX Network) CA

View Certificate

Use a different user name for the connection

OK Cancel

Enable (click to check) "Validate server certificate"

Select (check) the name of the certificate on this client (downloaded from RADIUS server in a prerequisite procedure)

1. Configure the following settings on the Association tab on the Network Properties dialog.

Association Tab

Network Authentication	WPA
Data Encryption	TKIP or AES depending on how this option is configured on the access point. Note: When the Cipher Suite on the access point is set to “Both”, then TKIP clients with a valid TKIP key and AES clients with a valid CCMP (AES) key can associate with the access point. For more information, see Administrators Guide and Online Help on the access point.

2. Configure these settings on the Authentication tab.

Authentication Tab

Enable IEEE 802.1x authentication for this network	Enable (click to check) this option.
EAP Type	Choose Smart Card or other Certificate.

3. Click **Properties** to bring up the Smart Card or other Certificate Properties dialog and enable the “Validate server certificate” option.

Smart Card or other Certificate Properties Dialog

Validate Server Certificate	Enable this option (click to check the box).
Certificates	In the certificate list shown, select the certificate for this client.

Click **OK** on all dialogs to close and save your changes.

4. To complete the client configuration you must now obtain a certificate from the RADIUS server and install it on this client. For information on how to do this see “Obtaining a TLS-EAP Certificate for a Client” in this manual.

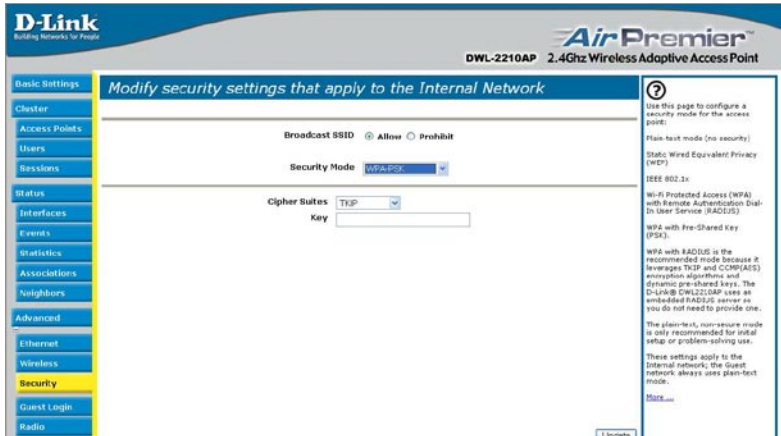
Logging on to the Wireless Network with a WPA Client Using a Certificate

WPA clients should now be able to connect to the access point using their TLS certificates. The certificate you installed is used when you connect, so you will not be prompted for login information. The certificate is automatically sent to the RADIUS server for authentication and authorization.

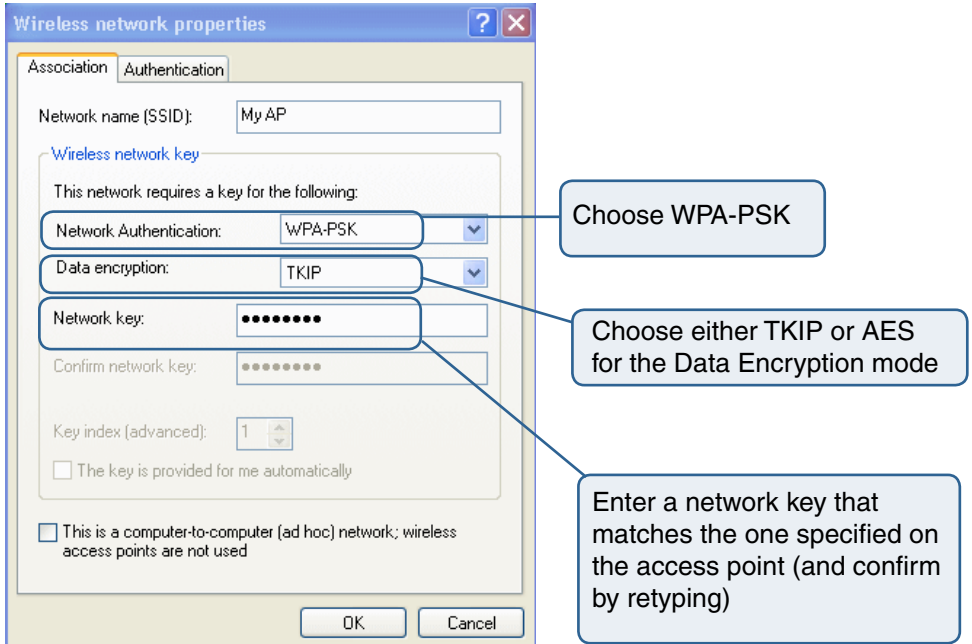
Configuring WPA-PSK Security on a Client

Wi-Fi Protected Access (WPA) with Pre-Shared Key (PSK) is a Wi-Fi Alliance subset of IEEE 802.11i, which includes *Temporal Key Integrity Protocol (TKIP)*, *Advanced Encryption Algorithm (AES)*, and *Counter mode/CBC-MAC Protocol (CCMP)* mechanisms. PSK employs a pre-shared key for an initial check of client credentials.

If you configured the D-Link DWL-2210AP to use WPA-PSK security mode . . .



. . . then configure WPA-PSK security on each client as follows.



Association Tab

Network Authentication	WPA-PSK
Data Encryption	TKIP or AES depending on how this option is configured on the access point. Note: When the Cipher Suite on the access point is set to “Both”, then TKIP clients with a valid TKIP key and AES clients with a valid CCMP (AES) key can associate with the access point. For more information, see Administrators Guide and Online Help on the access point.
Network Key	Provide the key you entered on the access point Security settings for the cipher suite you are using. For example, if the key on the access point is set to use a TKIP key of “012345678”, then a TKIP client specify this same string as the network key.
The key is provided for me automatically	This box should be disabled automatically based on other settings.

Authentication Tab

Enable IEEE 802.1x authentication for this network	Make sure that IEEE 802.1x authentication is disabled (unchecked). (Setting the encryption mode to WEP should automatically disable authentication.)
---	---

Click **OK** on the Wireless Network Properties dialog to close it and save your changes.

Connecting to the Wireless Network with a WPA-PSK Client

WPA-PSK clients should now be able to associate and authenticate with the access point. As a client, you will not be prompted for a key. The TKIP or AES key you configured on the client security settings is automatically used when you connect.

Configuring an External RADIUS Server to Recognize the D-Link DWL-2210AP

An external *Remote Authentication Dial-in User Server* (RADIUS) server running on the network can support of EAP-TLS smart card/certificate distribution to clients in a *Public Key Infrastructure* (PKI) as well as EAP-PEAP user account setup and authentication. By *external* RADIUS server, we mean an authentication server external to the access point itself. This is to distinguish between the scenario in which you use a network RADIUS server versus one in which you use the *Built-in Authentication Server* on the D-Link DWL-2210AP.

This section provides an example of configuring an external RADIUS server for the purposes of authenticating and authorizing TLS-EAP certificates from wireless clients of a particular D-Link DWL-2210AP configured for either “WPA with RADIUS” or “IEEE 802.1x” security modes. The intention of this section is to provide some idea of what this process will look like; procedures will vary depending on the RADIUS server you use and how you configure it. For this example, we use the Internet Authentication Service that comes with Microsoft Windows 2003 server.

This document does not describe how to set up Administrative users on the RADIUS server. In this example, we assume you already have RADIUS server user accounts configured. You will need a RADIUS server user name and password for both this procedure and the following one that describes how to obtain and install a certificate on the wireless client. Please consult the documentation for your RADIUS server for information on setting up user accounts.

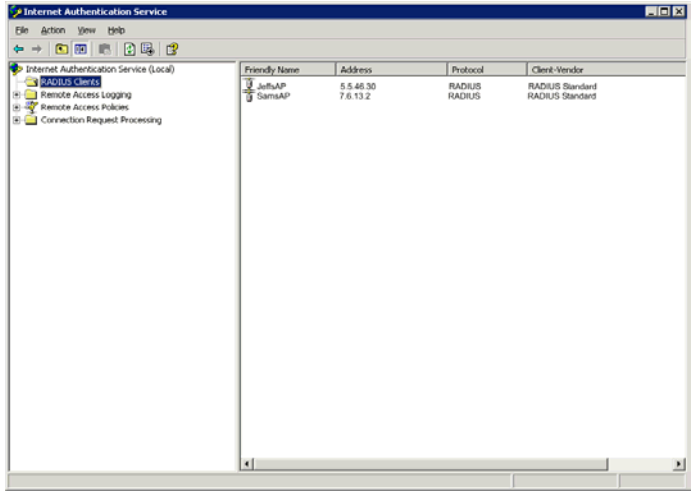
The purpose of this procedure is to identify your D-Link DWL-2210AP as a “client” to the RADIUS server. The RADIUS server can then handle authentication and authorization of wireless clients for the AP. This procedure is required *per access point*. If you have more than one access point with which you plan to use an external RADIUS server, you need to follow these steps for each of those APs.

Keep in mind that the information you need to provide to the RADIUS server about the access point corresponds to settings on the access point (Advanced > Security) and vice versa. You should have already provided the RADIUS server IP Address to the AP; in the steps that follow you will provide the access point address to the RADIUS server. The RADIUS Key provided on the AP is the “shared secret” you will provide to the RADIUS server.



The RADIUS server is identified by its IP address and UDP port numbers for the different services it provides. On the current release of the D-Link DWL-2210AP, the RADIUS server *User Datagram Protocol* (UDP) ports used by the access point are not configurable. (The D-Link DWL-2210AP is hard-coded to use RADIUS server UDP port 1812 for authentication and port 1813 for accounting.)

1. Log on to the system hosting your RADIUS server and bring up the Internet Authentication Service.



2. In the left panel, right click on “RADIUS Clients” node and choose New > Radius Client from the popup menu.

3. On the first screen of the New RADIUS Client wizard provide information about the D-Link DWL-2210AP to which you want your clients to connect:

- A logical (friendly) name for the access point. (You might want to use DNS name or location.)

- IP address for the access point.

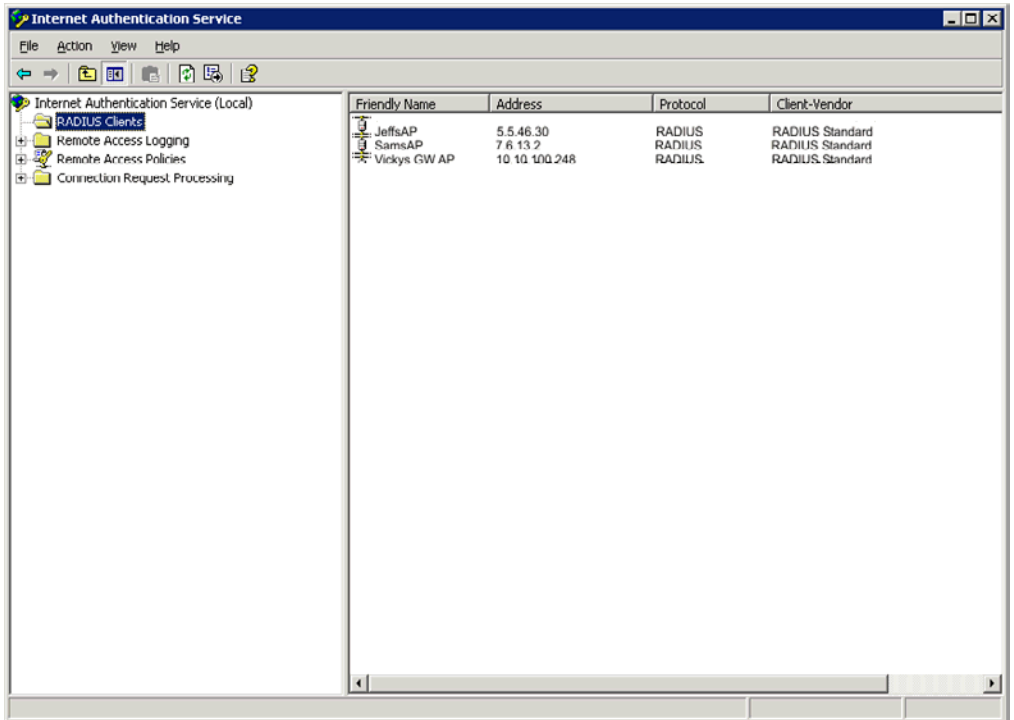
The screenshot shows a dialog box titled "New RADIUS Client" with a close button (X) in the top right corner. The dialog is divided into a header section and a main content area. The header section is titled "Name and Address". Below the header, there is a text label: "Type a friendly name and either an IP Address or DNS name for the client." There are two input fields: "Friendly name:" with the text "Vickys GW AP" and "Client address (IP or DNS):" with the text "10.10.100.248". To the right of the "Client address" field is a "Verify..." button. At the bottom of the dialog, there are three buttons: "< Back", "Next >", and "Cancel".

Click **Next**.

4. For the "Shared secret" enter the RADIUS Key you provided to the access point (on the Advanced >Security page). Retype the key to confirm.

The screenshot shows the same "New RADIUS Client" dialog box, but now on the "Additional Information" tab. The header section is titled "Additional Information". Below the header, there is a text label: "If you are using remote access policies based on the client vendor attribute, specify the vendor of the RADIUS client." There is a "Client-Vendor:" dropdown menu with "RADIUS Standard" selected. Below that are two "Shared secret:" input fields, both containing masked text (*****). At the bottom, there is a checkbox labeled "Request must contain the Message Authenticator attribute" which is currently unchecked. At the bottom of the dialog, there are three buttons: "< Back", "Finish", and "Cancel".

5. Click **Finish**.



The access point is now displayed as a client of the Authentication Server.

Obtaining a TLS-EAP Certificate for a Client

If you want to use IEEE 802.1x mode with EAP-TLS certificates for authentication and authorization of clients, you must have an external RADIUS server and a *Public Key Authority Infrastructure* (PKI), including a *Certificate Authority* (CA), server configured on your network. It is beyond the scope of this document to describe these configuration of the RADIUS server, PKI, and CA server. Consult the documentation for those products. Some good starting points available on the Web for the Microsoft Windows PKI software are: “How to Install/Uninstall a Public Key Certificate Authority for Windows 2000” at <http://support.microsoft.com/default.aspx?scid=kb;EN-US;231881> and How to Configure a Certificate Server at <http://support.microsoft.com/default.aspx?scid=kb;en-us;318710#3>.

Wireless clients configured to use either “WPA with RADIUS” or” IEEE 802.1x” security modes with an external RADIUS server that supports TLS-EAP certificates must obtain a TLS certificate from the RADIUS server.

This is an initial onetime step that must be completed on each client that uses either of these modes with certificates. In this procedure, we use the Microsoft Certificate Server as an example.

To obtain a certificate for a client, follow these steps.

1. Go to the following URL in a Web browser:

`https://IPAddressOfServer/certsrv/`

Where *IPAddressOfServer* is the IP address of your external RADIUS server, or of the *Certificate Authority* (CA), depending on the configuration of your infrastructure.

2. Click “Yes” to proceed to the secure Web page for the server.



The Welcome screen for the Certificate Server is displayed in the browser.

Microsoft Certificate Services -- dc01

Home

Welcome

Use this Web site to request a certificate for your Web browser, e-mail client, or other program. By using a certificate, you can verify your identity to people you communicate with over the Web, sign and encrypt messages, and, depending upon the type of certificate you request, perform other security tasks.

You can also use this Web site to download a certificate authority (CA) certificate, certificate chain, or certificate revocation list (CRL), or to view the status of a pending request.

For more information about Certificate Services, see [Certificate Services Documentation](#).

Select a task:

[Request a certificate](#)

[View the status of a pending certificate request](#)

[Download a CA certificate, certificate chain, or CRL](#)

3. Click “Request a certificate” to get the login prompt for the RADIUS server.

4. Provide a valid user name and password to access the RADIUS server.

Connect to 10.10.1.9

Connecting to 10.10.1.9]

User name:

Password:

Remember my password

OK Cancel

The user name and password you need to provide here is for access to the RADIUS server, for which you will already have user accounts configured at this point. This document does not describe how to set up Administrative user accounts on the RADIUS server. Please consult the documentation for your RADIUS server for these procedures.

5. Click “User Certificate” on the next page displayed.

Microsoft Certificate Services -- dc01

Home

Request a Certificate

Select the certificate type:

[User Certificate](#)

Or, submit an [advanced certificate request](#).

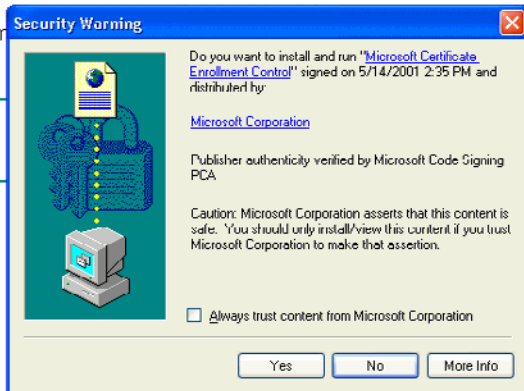
6. Click “Yes” on the dialog displayed to install the certificate.

Microsoft Certificate Services -- dc01

Home

User Certificate - Identifying Information

No further identifying information

[More Options >>](#)

7. Click “Submit” to complete and click “Yes” to confirm the submittal on the popup dialog.

Microsoft Certificate Services -- dc01

Home

User Certificate - Identifying Information

No further identifying information is required. To complete your certificate, press submit.

[More Options >>](#)

Potential Scripting Violation



This Web site is requesting a new certificate on your behalf. You should allow only trusted Web sites to request a certificate for you. Do you want to request a certificate now?

8. Click “Install this certificate” to install the newly issued certificate on your client station. (Also, click “Yes” on the popup windows to confirm the install and to add the certificate to the Root Store.)

Microsoft Certificate Services -- dc01

[Home](#)

Certificate Issued

The certificate you requested was issued to you.



[Install this certificate](#)

Potential Scripting Violation



This Web site is adding one or more certificates to this computer. Allowing an untrusted Web site to update your certificates is a security risk. The Web site could install certificates you do not trust, which could allow programs that you do not trust to run on this computer and gain access to your data.

Do you want this program to add the certificates now? Click Yes if you trust this Web site. Otherwise, click No.

Root Certificate Store



Do you want to ADD the following certificate to the Root Store?

Subject : DC02, lab, instant802, com

Issuer : Self Issued

Time Validity : Monday, November 10, 2003 through Monday, November 10, 2008

Serial Number : 7C275AA0 6E022B97 48881486 AD85E655

Thumbprint (sha1) : A608357F F932040B C4D05C72 7C78051A 840AF935

Thumbprint (md5) : 87CF128E 6169B880 AD45215D 8E287391

Microsoft Certificate Services -- dc01

[Home](#)

Certificate Installed

Your new certificate has been successfully installed.

Appendix B. Troubleshooting

This section provides information about how to solve common problems you might encounter in the course of updating network configurations on networks served by multiple, clustered access points.

Cluster Recovery

In cases where the access points in a cluster become out of sync or an access point cannot join or be removed from a cluster, the following methods for cluster recovery are recommended.

Reboot or Reset Access Point

These recovery methods are given in the order you should try them. In all but the last case (stop clustering), you only need to reset or reboot the particular access point whose configuration is out of sync with other cluster members or cannot remove/join cluster.

- Reboot the access point from its Administration UI. To do this, go to `http://IPAddressOfAccessPoint`, navigate to **Advanced > Reboot** and click the **Reboot** button. (IP addresses for APs are on the Cluster > Access Points page for cluster members.)
- Physically reboot the access point by pressing the Power button on the device.
- Reset the access point from its Administration UI. To do this, go to `http://IPAddressOfAccessPoint`, navigate to **Advanced > Reset**, and click the **Reset** button. (IP addresses for APs are on the Cluster > Access Points page for any cluster member.)
- Physically reset the access point by pressing the Reset button on the device.
- In some extreme cases, reboot or reset may not solve the problem. In these cases, follow the procedure described next in “Stop Clustering and Reset Each Access Point in the Cluster” to recover every access point on the subnet.

Stop Clustering and Reset Each Access Point in the Cluster

If the previous reboot or reset methods do not solve the problem, do the following to stop clustering and reset all APs.

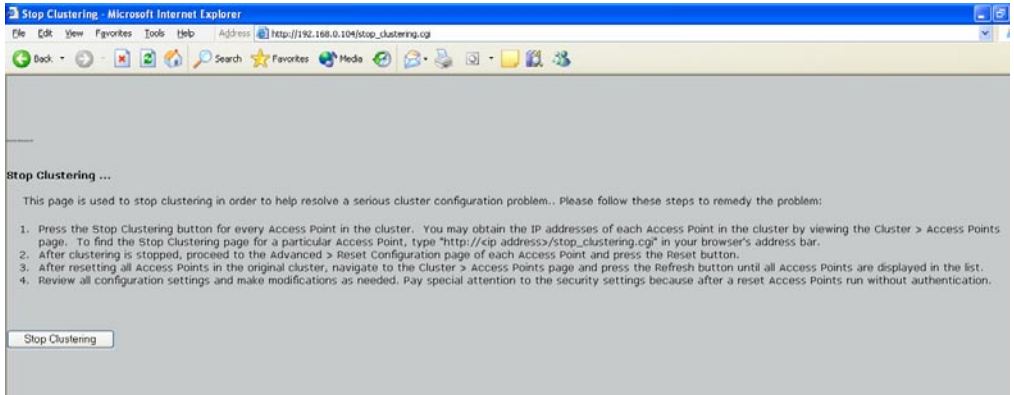
1. Stop clustering on each access point in the cluster.

To do this, enter the Stop Clustering URL in the address bar of your Web browser as follows:

```
http://IPAddressOfAccessPoint/stop_clustering.cgi
```

Where *IPAddressOfAccessPoint* is the IP address of the access point you want to stop clustering. You can find the IP addresses for the cluster members on the Cluster > Access Points page for any of the clustered access points. We recommend making a note of all IP addresses at this point.

The Stop Clustering page for this access point is displayed.



Click the **Stop Clustering** button.

Repeat this “stop clustering” step for every access point in the cluster.

Table 1:

Do not proceed to the next step of resetting any access points until you have stopped clustering on all of them. Make sure that you first “Stop Clustering” on every access point on the subnet, and only then perform the next part of the process of resetting each one to the factory defaults.

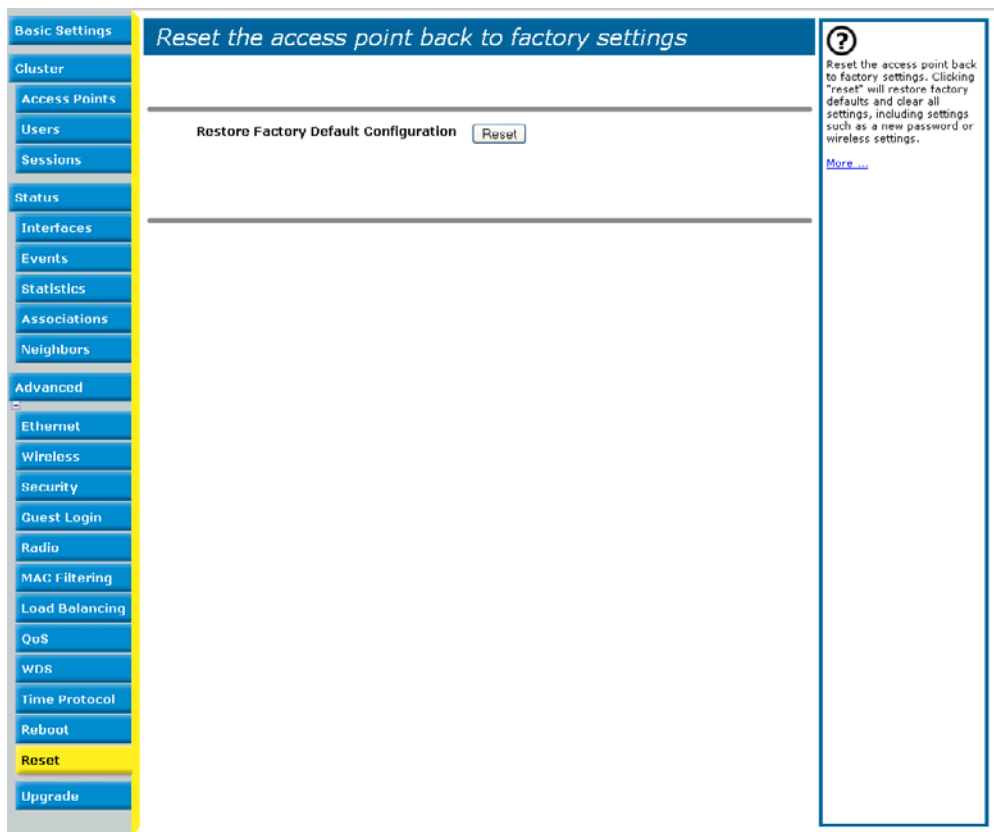
2. Reset each access point.

To do this, go to the Administration Web pages of the access point you want to reset by entering its URL into the address bar of your Web browser:

`http://IPAddressOfAccessPoint/`

Where *IPAddressOfAccessPoint* is the IP address of the access point you want to reset.

On the Administration UI left-hand tabs, click **Advanced** > **Reset** to bring up the Reset page.



Click **Reset** to restore the factory defaults on the access point. (This will clear all of your previous settings, including updated passwords.)

Repeat this “reset” step for every access point in the cluster.

Table 2:

Do not proceed to the next step until you have stopped clustering on all of access points in the preexisting cluster.

3. Refresh the cluster view as follows.

On the Administration Web pages for any one of the access points, click **Cluster** > **Access Points** to bring up the Access Points cluster management page and click the **Refresh** button.

Basic Settings Manage access points in the cluster

Cluster

Access Points Access Points...

Status: connected to cluster.

the list of Access Points.

<input type="checkbox"/>	Location	MAC Address	IP Address
<input type="checkbox"/>	not set	00:0c:41:0a:33:7e	10.10.100.250

the selected Access Points from the cluster.

Clustered

1 Access Point

2 User Accounts

? This page shows current basic configuration settings for clustered access points (location, MAC address, and IP address). To see the full configuration for a specific AP, click on an IP address in the list. Standalone access points or those which are not members of this cluster do not show up in this listing. If you are looking for APs on the network that are not listed here, they may be in standalone mode or members of a different cluster. See the sections [What Kinds of APs Can Cluster Together?](#) and [Standalone Mode](#) in the Online Help. [More...](#)

At this point you should see all previous cluster members displayed in the list.

Before proceeding to the last step, verify that the cluster has reformed by making sure all access points are listed.

4. Review all configuration settings and make modifications as needed.

Pay special attention to the security settings because after a reset, Access Points run without any security in place.

Glossary

802

IEEE 802 (IEEE Std. 802-2001) is a family of standards for peer-to-peer communication over a LAN. These technologies use a shared-medium, with information broadcast for all stations to receive. The basic communications capabilities provided are packet-based. The basic unit of transmission is a sequence of data octets (8-bits), which can be of any length within a range that is dependent on the type of LAN.

Included in the 802 family of IEEE standards are definitions of bridging, management, and security protocols.

802.1x

IEEE 802.1x (IEEE Std. 802.1x-2001) is a standard for passing EAP packets over an 802.11 wireless network using a protocol called *EAP Encapsulation Over LANs* (EAPOL). It establishes a framework that supports multiple authentication methods.

IEEE 802.1x authenticates users not machines.

802.2

IEEE 802.2 (IEEE Std. 802.2.1998) defines the LLC layer for the 802 family of standards.

802.3

IEEE 802.3 (IEEE Std. 802.3-2002) defines the MAC layer for networks that use CSMA/CA. Ethernet is an example of such a network.

802.11

IEEE 802.11 (IEEE Std. 802.11-1999) is a medium access control (MAC) and physical layer (PHY) specification for wireless connectivity for fixed, portable, and moving stations within a local area. It uses direct sequence spread spectrum (DSSS) in the 2.4 GHz ISM band and supports raw data rates of 1 and 2Mbps. It was formally adopted in 1997 but has been mostly superseded by 802.11b.

IEEE 802.11 is also used generically to refer to the family of IEEE standards for wireless local area networks.

802.11b

IEEE 802.11b (IEEE Std. 802.11b-1999) is an enhancement of the initial 802.11 PHY to include 5.5 Mbps and 11 Mbps data rates. It uses direct sequence spread spectrum (DSSS) or frequency hopping spread spectrum (FHSS) in the 2.4 GHz ISM band as well as complementary code keying (CCK) to provide the higher data rates. It supports data rates ranging from 1 to 11 Mbps.

802.11e

IEEE 802.11e is a developing IEEE standard for MAC enhancements to support QoS. It provides a mechanism to prioritize traffic within 802.11. It defines allowed changes in the Arbitration Interframe Space, a minimum and maximum Contention Window size, and the maximum length (in μ sec) of a burst of data.

IEEE 802.11e is still a draft IEEE standard (most recent version is D5.0, July 2003). A currently available subset of 802.11e is the *Wireless Multimedia Enhancements* (WME) standard.

802.11f

IEEE 802.11f (IEEE Std. 802.11f-2003) is a standard that defines the inter access point protocol (IAPP) for access points (wireless hubs) in an extended service set (ESS). The standard defines how access points communicate the associations and reassociations of their mobile stations.

802.11g

IEEE 802.11g (IEEE Std. 802.11g-2003) is a higher speed extension (up to 54 Mbps) to the 802.11b PHY, while operating in the 2.4 GHz band. It uses orthogonal frequency division multiplexing (OFDM). It supports data rates ranging from 1 to 54 Mbps.

802.11i

IEEE 802.11i is a developing IEEE standard for security in a wireless local area network (WLAN). It defines enhancements to the MAC Layer to counter some of the weaknesses of WEP. 802.11i will incorporate 802.1x and stronger encryption techniques, such as Advanced Encryption Standard (AES).

IEEE 802.11i is still a draft IEEE standard (most recent version is D5.0, August 2003). A currently available subset of 802.11i is the Wi-Fi *Protected Access* (WPA) standard.

802.1Q

IEEE 802.1Q is the IEEE standard for *Virtual Local Area Networks* (VLANs) specific to wireless technologies. (See <http://www.ieee802.org/1/pages/802.1Q.html>.)

The standard addresses the problem of how to break large networks into smaller parts to prevent broadcast and multicast data traffic from consuming more bandwidth than is necessary. 802.1Q also provides for better security between segments of internal networks. The 802.1Q specification provides a standard method for inserting VLAN membership information into Ethernet frames.

Access Point

An *access point* is the communication hub for the devices on a WLAN, providing a connection or bridge between wireless and wired network devices. It supports a Wireless Networking Framework called Infrastructure Mode.

When one access point is connected to a wired network and supports a set of wireless stations, it is referred to as a basic service set (BSS). An extended service set (ESS) is created by combining two or more BSSs.

Ad hoc Mode

Ad hoc mode is a Wireless Networking Framework in which stations communicate directly with each other. It is useful for quickly establishing a network in situations where formal infrastructure is not required.

Ad hoc mode is also referred to as *peer-to-peer mode* or an independent basic service set (IBSS).

AES

The *Advanced Encryption Standard (AES)* is a symmetric 128-bit block data encryption technique developed to replace DES encryption. AES works at multiple network layers simultaneously.

Further information is available on the NIST Web site.

Basic Rate Set

The *basic rate set* defines the transmission rates that are mandatory for any station wanting to join this wireless network. All stations must be able to receive data at the rates listed in this set.

Beacon

Beacon frames provide the “heartbeat” of a WLAN, announcing the existence of the network, and enabling stations to establish and maintain communications in an orderly fashion. It carries the following information (some of which is optional):

- The *Timestamp* is used by stations to update their local clock, enabling synchronization among all associated stations.
- The *Beacon interval* defines the amount of time between transmitting beacon frames. Before entering power save mode, a station needs the beacon interval to know when to wake up to receive the beacon.
- The *Capability Information* lists requirements of stations that want to join the WLAN. For example, it indicates that all stations must use WEP.
- The *Service Set Identifier (SSID)*.
- The Basic Rate Set is a bitmap that lists the rates that the WLAN supports.
- The optional *Parameter Sets* indicates features of the specific signaling methods in use (such as frequency hopping spread spectrum, direct sequence spread spectrum, etc.).
- The optional *Traffic Indication Map (TIM)* identifies stations, using power saving mode, that have data frames queued for them.

Bridge

A connection between two local area networks (LANs) using the same protocol, such as Ethernet or IEEE 802.1x.

Broadcast

A *Broadcast* sends the same message at the same time to everyone. In wireless networks, broadcast usually refers to an interaction in which the access point sends data traffic in the form of IEEE 802.1x Frames to all client stations on the network.

Some wireless security modes distinguish between how unicast, multicast, and broadcast frames are encrypted or whether they are encrypted.

See also Unicast and Multicast.

Broadcast Address

See IP Address.

BSS

A *basic service set* (BSS) is an Infrastructure Mode Wireless Networking Framework with a single access

point. Also see extended service set (ESS) and independent basic service set (IBSS).

BSSID

In Infrastructure Mode, the *Basic Service Set Identifier* (BSSID) is the 48-bit MAC address of the wireless interface of the Access Point.

CCMP

Counter mode/CBC-MAC Protocol (CCMP) is an encryption method for 802.11i that uses AES. It employs a *CCM* mode of operation, combining the Cipher Block Chaining Counter mode (CBC-CTR) and the Cipher Block Chaining Message Authentication Code (CBC-MAC) for encryption and message integrity.

AES-CCMP requires a hardware coprocessor to operate.

CGI

The *Common Gateway Interface* (CGI) is a standard for running external programs from an HTTP server. It specifies how to pass arguments to the executing program as part of the HTTP request. It may also define a set of environment variables.

A CGI program is a common way for an HTTP server to interact dynamically with users. For example, an HTML page containing a form can use a CGI program to process the form data after it is submitted.

Channel

The *Channel* defines the portion of the radio spectrum the radio uses for transmitting and receiving. Each 802.11 standard offers a number of channels, dependent on how the spectrum is licensed by national and transnational authorities such as the Federal Communications Commission (FCC), the European Telecommunications Standards Institute (ETSI), the Korean Communications Commission, or the Telecom Engineering Center (TELEC).

CSMA/CA

Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA) is a low-level network arbitration/contention protocol. A station listens to the media and attempts to transmit a packet when the channel is quiet. When it detects that the channel is idle, the station transmits the packet. If it detects that the channel is busy, the station waits a random amount of time and then attempts to access the media again.

CSMA/CA is the basis of the IEEE 802.11e Distributed Control Function (DCF). See also RTS and CTS.

The CSMA/CA protocol used by 802.11 networks is a variation on CSMA/CD (used by Ethernet networks). In CSMA/CD the emphasis is on collision *detection* whereas with CSMA/CA the emphasis is on collision *avoidance*.

CTS

A *clear to send* (CTS) message is a signal sent by an IEEE 802.11 client station in response to a *request to send* (RTS) message. The CTS message indicates that the channel is clear for the sender of the RTS message to begin data transfer. The other stations will wait to keep the air waves clear. This message is a part of the IEEE 802.11 CSMA/CA protocol. (See also RTS.)

DCF

The *Distribution Control Function* is a component of the IEEE 802.11e Quality of Service (QoS) technology standard. The DCF coordinates channel access among multiple stations on a wireless network by controlling wait times for channel access. Wait times are determined by a random backoff timer which is configurable by defining minimum and maximum contention windows.

DHCP

The *Dynamic Host Configuration Protocol* (DHCP) is a protocol specifying how a central server can dynamically provide network configuration information to clients. A DHCP server “offers” a “lease” (for a pre-configured period of time—see Lease Time) to the client system. The information supplied includes the client’s IP addresses and netmask plus the address of its DNS servers and Gateway.

DNS

The *Domain Name Service* (DNS) is a general-purpose query service used for translating *fully-qualified names* into Internet addresses. A fully-qualified name consists of the hostname of a system plus its domain name. For example, `www` is the host name of a Web server and `www.dlink.com` is the fully-qualified name of that server. DNS translates the domain name `www.dlink.com` to some IP address, for example `66.93.138.219`.

A *domain name* identifies one or more IP addresses. Conversely, an IP address may map to more than one domain name.

A domain name has a suffix that indicates which *top level domain* (TLD) it belongs to. Every country has its own top-level domain, for example `.de` for Germany, `.fr` for France, `.jp` for Japan, `.tw` for Taiwan, `.uk` for the United Kingdom, `.us` for the U.S.A., and so on. There are also `.com` for commercial bodies, `.edu` for educational institutions, `.net` for network operators, and `.org` for other organizations as well as `.gov` for the U. S. government and `.mil` for its armed services.

DOM

The *Document Object Model* (DOM) is an interface that allows programs and scripts to dynamically access and update the content, structure, and style of documents. The DOM allows you to model the objects in an HTML or XML document (text, links, images, tables), defining the attributes of each object and how they can be manipulated.

Further details about the DOM can be found at the W3C.

DTIM

The *Delivery Traffic Information Map* (DTIM) message is an element included in some Beacon frames. It indicates which stations, currently sleeping in low-power mode, have data buffered on the Access Point awaiting pickup. Part of the DTIM message indicates how frequently stations must check for buffered data.

Dynamic IP Address

See IP Address.

EAP

The *Extensible Authentication Protocol* (EAP) is an authentication protocol that supports multiple methods, such as token cards, Kerberos, onetime passwords, certificates, public key authentication, and smart cards.

Variations on EAP include EAP Cisco Wireless (LEAP), Protected EAP (PEAP), EAP-TLS, and EAP Tunnelled TLS (EAP-TTLS).

ESS

An *extended service set* (ESS) is an Infrastructure Mode Wireless Networking Framework with multiple access points, forming a single subnetwork that can support more clients than a basic service set (BSS). Each access point supports a number of wireless stations, providing broader wireless coverage for a large space, for example, an office.

Ethernet

Ethernet is a local-area network (LAN) architecture supporting data transfer rates of 10Mbps to 1Gbps. The Ethernet specification is the basis for the IEEE 802.3 standard, which specifies the physical and lower software layers. It uses the CSMA/CA access method to handle simultaneous demands.

Ethernet supports data rates of 10 Mbps, *Fast Ethernet* supports 100 Mbps, and *Gigabit Ethernet* supports 1Gbps. Its cables are classified as “XbaseY”, where X is the data rate in Mbps and Y is the category of cabling. The original cable was *10base5* (Thicknet or “Yellow Cable”). Some others are *10base2* (Cheapernet), *10baseT* (Twisted Pair), and *100baseT* (Fast Ethernet). The latter two are commonly supplied using *CAT5* cabling with *RJ-45* connectors. There is also *1000baseT* (Gigabit Ethernet).

ERP

The *Extended Rate Protocol* refers to the protocol used by IEEE 802.11g stations (over 20 Mbps transmission rates at 2.4GHz) when paired with Orthogonal Frequency Division Multiplexing (OFDM). Built into ERP and the IEEE 802.11g standard is a scheme for effective interoperability of IEEE 802.11g stations with IEEE 802.11b nodes on the same channel.

Legacy IEEE 802.11b devices cannot detect the ERP-OFDM signals used by IEEE 802.11g stations, and this can result in collisions between data frames from IEEE 802.11b and IEEE 802.11g stations.

If there is a mix of 802.11b and 802.11g nodes on the same channel, the IEEE 802.11g stations detect this via an ERP flag on the access point and enable *request to send* (RTS) and *clear to send* (CTS) protection before sending data.

See also CSMA/CA protocol.

Frame

A *Frame* consists of a discrete portion of data along with some descriptive meta-information packaged for transmission on a wireless network. Each frame includes a source and destination MAC address, a control field with protocol version, frame type, frame sequence number, frame body (with the actual information to be transmitted) and frame check sequence for error detection. A Frame is similar in concept to a Packet, the difference being that a packet operates on the Network layer (layer 3 in the OSI model) whereas a frame operates on the Data-Link layer (layer 2 in the OSI model).

Gateway

A *gateway* is a network node that serves as an entrance to another network. A gateway also often provides a proxy server and a firewall. It is associated with both a router, which use headers and forwarding tables to determine where packets are sent, and a switch or bridge, which provides the actual path for the packet in and out of the gateway.

Before a host on a LAN can access the Internet, it needs to know the address of its *default gateway*.

HTML

The *Hypertext Markup Language* (HTML) defines the structure of a document on the World Wide Web. It uses tags and attributes to hint about a layout for the document.

An HTML document starts with an `<html>` tag and ends with a `</html>` tag. A properly formatted document also contains a `<head> ... </head>` section, which contains the metadata to define the document, and a `<body> ... </body>` section, which contains its content. Its markup is derived from the *Standard Generalized Markup Language* (SGML), which is defined in ISO 8879:1986.

HTML documents are sent from server to browser via HTTP. Also see XML.

HTTP

The *Hypertext Transfer Protocol* (HTTP) defines how messages are formatted and transmitted on the World Wide Web. An HTTP message consists of a URL and a command (GET, HEAD, POST, etc.), a request followed by a response.

IAPP

The *Inter Access Point Protocol* (IAPP) is an IEEE standard (802.11f) that defines communication between the access points in a “distribution system”. This includes the exchange of information about mobile stations and the maintenance of bridge forwarding tables, plus securing the communications between access points.

IBSS

An *independent basic service set* (IBSS) is an Ad hoc Mode Wireless Networking Framework in which stations communicate directly with each other.

IEEE

The Institute of Electrical and Electronic Engineers (IEEE) is an international standards body that develops and establishes industry standards for a broad range of technologies, including the 802 family of networking and wireless standards. (See 802, 802.1x, 802.11, 802.11a, 802.11b, 802.11e, 802.11f, 802.11g, and 802.11i.)

For more information about IEEE task groups and standards, see <http://standards.ieee.org/>.

Infrastructure Mode

Infrastructure Mode is a Wireless Networking Framework in which wireless stations communicate with each other by first going through an Access Point. In this mode, the wireless stations can communicate with each other or can communicate with hosts on a wired network. The access point is connected to a wired network and supports a set of wireless stations.

An infrastructure mode framework can be provided by a single access point (BSS) or a number of access points (ESS).

Intrusion Detection

The *Intrusion Detection System* (IDS) inspects all inbound network activity and reports suspicious patterns that may indicate a network or system attack from someone attempting to break into the system. It reports access attempts using unsupported or known insecure protocols.

IP

The *Internet Protocol* (IP) specifies the format of packets, also called datagrams, and the addressing scheme. IP is a connectionless, best-effort packet switching protocol. It provides packet routing, fragmentation and reassembly. It is combined with higher-level protocols, such as TCP or UDP, to establish the virtual connection between destination and source.

The current version of IP is *IPv4*. A new version, called *IPv6* or *IPng*, is under development. *IPv6* is an attempt to solve the shortage of IP addresses.

IP Address

Systems are defined by their *IP address*, a four-byte (octet) number uniquely defining each host on the Internet. It is usually shown in form 192.168.2.254. This is called dotted-decimal notation.

An IP address is partitioned into two portions: the network prefix and a host number on that network. A Subnet Mask is used to define the portions. There are two special host numbers:

- The Network Address consists of a host number that is all zeroes (for example, 192.168.2.0).

- The Broadcast Address consists of a host number that is all ones (for example, 192.168.2.255).

There are a finite number of IP addresses that can exist. Therefore, a local area network typically uses one of the IANA-designated address ranges for use in private networks. These address ranges are:

10.0.0.0 to 10.255.255.255
172.16.0.0 to 172.31.255.255
192.168.0.0 to 192.168.255.255

A Dynamic IP Address is an IP address that is automatically assigned to a host by a DHCP server or similar mechanism. It is called dynamic because you may be assigned a different IP address each time you establish a connection.

A Static IP Address is an IP address that is hard-wired for a specific host. A static address is usually required for any host that is running a server, for example, a Web server.

IPSec

IP Security (IPSec) is a set of protocols to support the secure exchange of packets at the IP layer. It uses shared public keys. There are two encryption modes: Transport and Tunnel.

- *Transport* mode encrypts only the data portion (payload) of each packet, but leaves the headers untouched.
- The more secure *Tunnel* mode encrypts both the header and the payload.

ISP

An *Internet Service Provider* (ISP) is a company that provides access to the Internet to individuals and companies. It may provide related services such as virtual hosting, network consulting, Web design, etc.

Jitter

Jitter is the difference between the latency (or delay) in packet transmission from one node to another across a network. If packets are not transmitted at a consistent rate (including Latency), QoS for some types of data can be affected. For example, inconsistent transmission rates can cause distortion in VoIP and streaming media. QoS is designed to reduce jitter along with other factors that can impact network performance.

Latency

Latency, also known as *delay*, is the amount of time it takes to transmit a Packet from sender to receiver. Latency can occur when data is transmitted from the access point to a client and vice versa. It can also occur when data is transmitted from access point to the Internet and vice versa. Latency is caused by *fixed network* factors such as the time it takes to encode and decode a packet, and also by *variable network* factors such as a busy or overloaded network. QoS features are designed to minimize latency for high priority network traffic.

LAN

A *Local Area Network* (LAN) is a communications network covering a limited area, for example, the computers in your home that you want to network together or a couple of floors in a building. A LAN

connects multiple computers and other network devices such as storage and printers. Ethernet is the most common technology implementing a LAN.

Wireless Ethernet (802.11) is another very popular LAN technology (also see WLAN).

LDAP

The *Lightweight Directory Access Protocol* (LDAP) is a protocol for accessing online directory services. It is used to provide an authentication mechanism. It is based on the X.500 standard, but less complex.

Lease Time

The *Lease Time* specifies the period of time the DHCP Server gives its clients an IP Address and other required information. When the lease expires, the client must request a new lease. If the lease is set to a short span, you can update your network information and propagate the information provided to the clients in a timely manner.

LLC

The *Logical Link Control* (LLC) layer controls frame synchronization, flow control, and error checking. It is a higher level protocol over the PHY layer, working in conjunction with the MAC layer.

MAC

The *Media Access Control* (MAC) layer handles moving data packets between NICs across a shared channel. It is a higher level protocol over the PHY layer. It provides an arbitration mechanism in an attempt to prevent signals from colliding.

It uses a hardware address, known as the *MAC address*, that uniquely identifies each node of a network. IEEE 802 network devices share a common 48-bit MAC address format, displayed as a string of twelve (12) hexadecimal digits separated by colons, for example FE:DC:BA:09:87:65.

MDI and MDI-X

Medium Dependent Interface (MDI) and *MDI crossover* (MDIX) are twisted pair cabling technologies for Ethernet ports in hardware devices. Built-in twisted pair cabling and auto-sensing enable connection between like devices with the use of a standard Ethernet cable. (For example, if a wireless access point supports MDI/MDIX, one can successfully connect a PC and that access point with an Ethernet cable rather than having to use a crossover cable).

MSCHAP V2

Microsoft Challenge Handshake Authentication Protocol Version 2 (MSCHAP V2) provides authentication for PPP connections between a Windows-based computer and an Access Point or other network access device.

MTU

The *Maximum Transmission Unit* is the largest physical packet size, measured in bytes, that a network can transmit. Any messages larger than the MTU are fragmented into smaller packets before being sent.

Multicast

A *Multicast* sends the same message to a select group of recipients. Sending an e-mail message to a mailing list is an example of multicasting. In wireless networks, multicast usually refers to an interaction in which the access point sends data traffic in the form of IEEE 802.1x Frames to a specified set of client stations (MAC addresses) on the network.

Some wireless security modes distinguish between how unicast, multicast, and broadcast frames are encrypted or whether they are encrypted. See also Unicast and Broadcast.

NAT

Network Address Translation is an Internet standard that masks the internal IP addresses being used in a LAN. A NAT server running on a gateway maintains a translation table that maps all internal IP addresses in outbound requests to its own address and converts all inbound requests to the correct internal host.

NAT serves three main purposes: it provides security by obscuring internal IP addresses, enables the use of a wide range of internal IP addresses without fear of conflict with the addresses used by other organizations, and it allows the use of a single Internet connection.

Network Address

See IP Address.

NIC

A *Network Interface Card* is an adapter or expansion board inserted into a computer to provide a physical connection to a network. Most NICs are designed for a particular type of network, protocol, and media, for example, Ethernet or wireless.

NTP

The *Network Time Protocol* assures accurate synchronization of the system clocks in a network of computers. NTP servers transmit *Coordinated Universal Time* (UTC, also known as *Greenwich Mean Time*) to their client systems. An NTP client sends periodic time requests to servers, using the returned time stamp to adjust its clock.

OSI

The *Open Systems Interconnection* (OSI) reference model is a framework for network design. The OSI model consists of seven layers:

- Layer 1, the Physical layer, identifies the physical medium used for communication between nodes. In the case of wireless networks, the physical medium is air, and radio frequency (RF) waves are a components of the physical layer.
- Layer 2, the Data-Link layer, defines how data for transmission will be structured and formatted, along with low-level protocols for communication and addressing. For example, protocols such as CSMA/CA and components like MAC addresses, and Frames are all defined and dealt with as a part of the Data-Link layer.

- Layer 3, the Network layer, defines the how to determine the best path for information traversing the network. Packets and logical IP Addresses operate on the network layer.
- Layer 4, the Transport layer, defines connection oriented protocols such as TCP and UDP.
- Layer 5, the Session layer, defines protocols for initiating, maintaining, and ending communication and transactions across the network. Some common examples of protocols that operate on this layer are network file system (NFS) and structured query language (SQL). Also part of this layer are communication flows like single mode (device sends information bulk), half-duplex mode (devices take turns transmitting information in bulk), and full-duplex mode (interactive, where devices transmit and receive simultaneously).
- Layer 6, the Presentation layer, defines how information is presented to the application. It includes meta-information about how to encrypt/decrypt and compress/decompress the data. JPEG and TIFF file formats are examples of protocols at this layer.
- Layer 7, the Application layer, includes protocols like hypertext transfer protocol (HTTP), simple mail transfer protocol (SMTP), and file transfer protocol (FTP).

Packet

Data and media are transmitted among nodes on a network in the form of *packets*. Data and multimedia content is divided up and packaged into *packets*. A packet includes a small chunk of the content to be sent along with its destination address and sender address. Packets are pushed out onto the network and inspected by each node. The node to which it is addressed is the ultimate recipient.

Packet Loss

Packet Loss describes the percentage of packets transmitted over the network that did not reach their intended destination. A 0 percent package loss indicates no packets were lost in transmission. QoS features are designed to minimize packet loss.

PHY

The Physical Layer (PHY) is the lowest layer in the network layer model (see OSI). The Physical Layer conveys the bit stream - electrical impulse, light or radio signal — through the network at the electrical and mechanical level. It provides the hardware means of sending and receiving data on a medium, including defining cables, NICs, and physical aspects.

Ethernet and the 802.11 family are protocols with physical layer components.

PID

The *Process Identifier* (PID) is an integer used by Linux to uniquely identify a process. A PID is returned by the `fork()` system call. It can be used by `wait()` or `kill()` to perform actions on the given process.

Port Forwarding

Port Forwarding creates a ‘tunnel’ through a firewall, allowing users on the Internet access to a service running on one of the computers on your LAN, for example, a Web server, an FTP or SSH server, or other services. From the outside user’s point of view, it looks like the service is running on the firewall.

PPP

The Point-to-Point Protocol is a standard for transmitting network layer datagrams (IP packets) over serial point-to-point links. PPP is designed to operate both over asynchronous connections and bit-oriented synchronous systems.

PPPoE

Point-to-Point Protocol over Ethernet (PPPoE) is a specification for connecting the users on a LAN to the Internet through a common broadband medium, such as a single DSL or cable modem line.

PPtP

Point-to-Point Tunneling Protocol (PPtP) is a technology for creating a *Virtual Private Network* (VPN) within the *Point-to-Point Protocol* (PPP). It is used to ensure that data transmitted from one VPN node to another are secure.

Proxy

A *proxy* is server located between a client application and a real server. It intercepts requests, attempting to fulfill them itself. If it cannot, it forwards them to the real server. Proxy servers have two main purposes: improve performance by spreading requests over several machines and filter requests to prevent access to specific servers or services.

PSK

Pre-Shared Key (PSK), see Shared Key.

Public Key

A *public key* is used in public key cryptography to encrypt a message which can only be decrypted with the recipient's private or secret key. Public key encryption is also called asymmetric encryption, because it uses two keys, or Diffie-Hellman encryption. Also see Shared Key.

QoS

Quality of Service (QoS) defines the performance properties of a network service, including guaranteed throughput, transit delay, and priority queues. QoS is designed to minimize Latency, Jitter, Packet Loss, and network congestion, and provide a way of allocating dedicated bandwidth for high priority network traffic.

The IEEE standard for implementing QoS on wireless networks is currently in-work by the 802.11e task group. A subset of 802.11e features is described in the WME specification.

RADIUS

The *Remote Authentication Dial-In User Service* (RADIUS) provides an authentication and accounting system. It is a popular authentication mechanism for many ISPs.

RC4

A symmetric stream cipher provided by RSA Security. It is a variable key-size stream cipher with byte-oriented operations. It allows keys up to 2048 bits in length.

Router

A *router* is a network device which forwards packets between networks. It is connected to at least two networks, commonly between two local area networks (LANs) or between a LAN and a wide-area network (WAN), for example, the Internet. Routers are located at gateways—places where two or more networks connect.

A router uses the content of headers and its tables to determine the best path for forwarding a packet. It uses protocols such as the Internet Control Message Protocol (ICMP), Routing Information Protocol (RIP), and Internet Router Discovery Protocol (IRDP) to communicate with other routers to configure the best route between any two hosts. The router performs little filtering of data it passes.

RSSI

The *Received Signal Strength Indication* (RSSI) is an 802.11x value that calculates voltage relative to the received signal strength. RSSI is one of several ways of measuring and indicating *radio frequency* (RF) signal strength. Signal strength can also be measured in mW (milliwatts), dBm (decibel milliwatts), and a percentage value.

RTP

Real-Time Transport Protocol (RTP) is an Internet protocol for transmitting real-time data like audio and video. It does not guarantee delivery but provides support mechanisms for the sending and receiving applications to enable streaming data. RTP typically runs on top of the UDP protocol, but can support other transport protocols as well.

RTS

A *request to send* (RTS) message is a signal sent by a client station to the access point, asking permission to send a data packet and to prevent other wireless client stations from grabbing the radio waves. This message is a part of the IEEE 802.11 CSMA/CA protocol. (See also RTS Threshold and CTS.)

RTS Threshold

The *RTS threshold* specifies the packet size of a request to send (RTS) transmission. This helps control traffic flow through the access point, and is especially useful for performance tuning on an access point with a many clients.

Shared Key

A *shared key* is used in conventional encryption where one key is used both for encryption and decryption. It is also called *secret-key* or *symmetric-key* encryption.

Also see Public Key.

SNMP

The *Simple Network Management Protocol* (SNMP) was developed to manage and monitor nodes on a network. It is part of the TCP/IP protocol suite.

SNMP consists of managed devices and their agents, and a management system. The agents store data about their devices in *Management Information Bases* (MIBs) and return this data to the SNMP management system when requested.

SSID

The *Service Set Identifier* (SSID) is a thirty-two character alphanumeric key that uniquely identifies a wireless local area network. It is also referred to as the *Network Name*. There are no restrictions on the characters that may be used in an SSID.

Static IP Address

See IP Address.

STP

The *Spanning Tree Protocol* (STP) an IEEE 802.1 standard protocol (related to network management) for MAC bridges that manages path redundancy and prevents undesirable loops in the network created by multiple active paths between client stations. Loops occur when there multiple routes between access points. STP creates a tree that spans all of the switches in an extended network, forcing redundant paths into a standby, or blocked, state. STP allows only one active path at a time between any two network devices (this prevents the loops) but establishes the redundant links as a backup if the initial link should fail. If STP costs change, or if one network segment in the STP becomes unreachable, the spanning tree algorithm reconfigures the spanning tree topology and reestablishes the link by activating the standby path. Without spanning tree in place, it is possible that both connections may be simultaneously live, which could result in an endless loop of traffic on the LAN

Subnet Mask

A *Subnet Mask* is a number that defines which part of an IP address is the network address and which part is a host address on the network. It is shown in dotted-decimal notation (for example, a 24-bit mask is shown as 255.255.255.0) or as a number appended to the IP address (for example, 192.168.2.0/24).

The subnet mask allows a router to quickly determine if an IP address is local or needs to be forwarded by performing a bitwise AND operation on the mask and the IP address. For example, if an IP address is

192.168.2.128 and the netmask is 255.255.255.0, the resulting Network address is 192.168.2.0.

The bitwise AND operator compares two bits and assigns 1 to the result only if both bits are 1. The following table shows the details of the netmask:

```
IP address 192.168.2.128 11000000 10101000 00000010 10000000
Netmask 255.255.255.0 11111111 11111111 11111111 00000000
Resulting network address 192.168.2.0 11000000 10101000 00000010 00000000
```

Supported Rate Set

The *supported rate set* defines the transmission rates that are available on this wireless network. A station may be able to receive data at any of the rates listed in this set. All stations must be able to receive data at the rates listed in the Basic Rate Set.

TCP

The *Transmission Control Protocol* (TCP) is built on top of Internet Protocol (IP). It adds reliable communication (guarantees delivery of data), flow-control, multiplexing (more than one simultaneous connection), and connection-oriented transmission (requires the receiver of a packet to acknowledge receipt to the sender). It also guarantees that packets will be delivered in the same order in which they were sent.

TCP/IP

The Internet and most local area networks are defined by a group of protocols. The most important of these is the *Transmission Control Protocol over Internet Protocol* (TCP/IP), the de facto standard protocols. TCP/IP was originally developed by Defense Advanced Research Projects Agency (DARPA, also known as ARPA, an agency of the US Department of Defense).

Although TCP and IP are two specific protocols, TCP/IP is often used to refer to the entire protocol suite based upon these, including ICMP, ARP, UDP, and others, as well as applications that run upon these protocols, such as telnet, FTP, etc.

TKIP

The *Temporal Key Integrity Protocol* (TKIP) provides an extended 48-bit initialization vector, per-packet key construction and distribution, a Message Integrity Code (MIC, sometimes called “Michael”), and a re-keying mechanism. It uses a RC4 stream cipher to encrypt the frame body and CRC of each 802.11 frame before transmission. It is an important component of the WPA and 802.11i security mechanisms.

ToS

TCP/IP packet headers include a 3-to-5 bit *Type of Service* (ToS) field set by the application developer that indicates the appropriate type of service for the data in the packet. The way the bits are set determines whether the packet is queued for sending with minimum delay, maximum throughput, low cost, or midway “best-effort” settings depending upon the requirements of the data. The ToS field is used by the D-Link DWL-2210AP to provide configuration control over *Quality of Service* (QoS) queues for data transmitted from the AP to client stations.

UDP

The *User Datagram Protocol* (UDP) is a transport layer protocol providing simple but unreliable datagram services. It adds port address information and a checksum to an IP packet. UDP neither guarantees delivery nor does it require a connection. It is lightweight and efficient. All error processing and retransmission must be performed by the application program.

Unicast

A *Unicast* sends a message to a single, specified receiver. In wireless networks, unicast usually refers to an interaction in which the access point sends data traffic in the form of IEEE 802.1x Frames directly to a single client station MAC address on the network.

Some wireless security modes distinguish between how unicast, multicast, and broadcast frames are encrypted or whether they are encrypted.

See also Multicast and Broadcast.

URL

A *Uniform Resource Locator* (URL) is a standard for specifying the location of objects on the Internet, such as a file or a newsgroup. URLs are used extensively in HTML documents to specify the target of a hyperlink which is often another HTML document (possibly stored on another computer). The first part of the URL indicates what protocol to use and the second part specifies the IP address or the domain name where that resource is located.

For example, `ftp://ftp.d-link.com/downloads/myfile.tar.gz` specifies a file that should be fetched using the FTP protocol; `http://www.dlink.com/index.html` specifies a Web page that should be fetched using the HTTP protocol.

VLAN

A *virtual LAN* (VLAN) is a software-based, logical grouping of devices on a network that allow them to act as if they are connected to a single physical network, even though they may not be. The nodes in a VLAN share resources and bandwidth, and are isolated on that network. The D-Link DWL-2210AP supports the configuration of a wireless VLAN. This technology is leveraged on the access point for the “virtual” guest network feature.

VPN

A *Virtual Private Network* (VPN) is a network that uses the Internet to connect its nodes. It uses encryption and other mechanisms to ensure that only authorized users can access its nodes and that data cannot be intercepted.

WAN

A *Wide Area Network* (WAN) is a communications network that spans a relatively large geographical area, extending over distances greater than one kilometer. A WAN is often connected through public networks, such as the telephone system. It can also be connected through leased lines or satellites. The Internet is essentially a very large WAN.

WDS

A *Wireless Distribution System* (WDS) allows the creation of a completely wireless infrastructure. Typically, an Access Point is connected to a wired LAN. WDS allows access points to be connected wirelessly. The access points can function as wireless repeaters or bridges.

WEP

Wired Equivalent Privacy (WEP) is a data encryption protocol for 802.11 wireless networks. All wireless stations and access points on the network are configured with a static 64-bit (40-bit secret key + 24-bit initialization vector (IV)) or 128-bit (104-bit secret key + 24-bit IV) Shared Key for data encryption. It uses a RC4 stream cipher to encrypt the frame body and CRC of each 802.11 frame before transmission.

Wi-Fi

A test and certification of interoperability for WLAN products based on the IEEE 802.11 standard promoted by the Wi-Fi Alliance, a nonprofit trade organization.

WINS

The *Windows Internet Naming Service* (WINS) is a server process for resolving Windows-based computer names to IP addresses. It provides information that allows these systems to browse remote networks using the *Network Neighborhood*.

Wireless Networking Framework

There are two ways of organizing a wireless network:

- Stations communicate directly with one another in an Ad hoc Mode network, also known as an independent basic service set (IBSS).
- Stations communicate through an Access Point in an Infrastructure Mode network. A single access point creates an infrastructure basic service set (BSS) whereas multiple access points are organized in an extended service set (ESS).

WLAN

Wireless Local Area Network (WLAN) is a LAN that uses high-frequency radio waves rather than wires to communicate between its nodes.

WME

Wireless Multimedia Enhancements (WME) is a subset of the 802.11e draft specification. It uses four priority queues between an Access Point and its clients. WME provides an interim, standards-based QoS solution.

WPA

Wi-Fi Protected Access (WPA) is a Wi-Fi Alliance version of the draft IEEE 802.11i standard. It provides more sophisticated data encryption than WEP and also provides user authentication. WPA includes TKIP and 802.1x mechanisms.

WRAP

Wireless Robust Authentication Protocol (WRAP) is an encryption method for 802.11i that uses AES but another encryption mode (OCB) for encryption and integrity.

XML

The *Extensible Markup Language* (XML) is a specification developed by the W3C. XML is a simple, flexible text format derived from *Standard Generalized Markup Language* (SGML), which is defined in ISO 8879:1986, designed especially for electronic publishing.

Technical Specifications

Standards

- IEEE 802.11b
- IEEE 802.11g
- IEEE 802.3
- IEEE 802.3af
- IEEE 802.3u
- IEEE 802.3x

Device Management

- Web-Based – Internet Explorer v6 or later; Netscape Navigator v6 or later; or other Java-enabled browsers.
- Telnet
- Kickstart

Data Rate*

For 802.11g:

- 108, 54, 48, 36, 24, 18, 12, 9 and 6Mbps

For 802.11b:

- 11, 5.5, 2, and 1Mbps

Security

- 64-, 128-, 152-bit WEP
- WPA – TKIP/AES PSK Mode
- WPA – RADIUS Server Mode (EAP-MD5/TLS/TTLS/PEAP)
- Embedded RADIUS Server
- Weak IV Avoidance
- Ignore/Inhibit SSID Broadcast
- MAC Address Access Control List

Wireless Frequency Range

- 2.4GHz to 2.4835GHz

**Maximum wireless signal rate derived from IEEE Standard 802.11a and 802.11g 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”.

Technical Specifications (continued)

Wireless Operating Range*

802.11g (Full Power with 5dBi gain diversity dipole antenna)

Indoors:

- 98ft (30m) @ 54Mbps
- 108ft (33m) @ 48Mbps
- 121ft (37m) @ 36Mbps
- 151ft (46m) @ 24Mbps
- 203ft (62m) @ 18Mbps
- 223ft (68m) @ 12Mbps
- 256ft (78m) @ 9Mbps
- 302ft (92m) @ 6Mbps

Outdoors:

- 328ft (100m) @ 54Mbps
- 968ft (295m) @ 11Mbps
- 1378ft (420m) @ 6Mbps

Antenna Type

- Dipole antenna with 5dBi gain

Operating Voltage

- 48VDC +/- 10% for PoE

Radio and Modulation Type

For 802.11b:

DSSS:

- DBPSK @ 1Mbps
- DQPSK @ 2Mbps
- CCK @ 5.5 and 11Mbps

For 802.11g:

OFDM:

- BPSK @ 6 and 9Mbps
- QPSK @ 12 and 18Mbps
- 16QAM @ 24 and 36Mbps
- 64QAM @ 48 and 54Mbps

DSSS:

- DBPSK @ 1Mbps
- DQPSK @ 2Mbps
- CCK @ 5.5 and 11Mbps

Technical Specifications (continued)

Transmit Output Power

For 802.11b:

- 63mW (18dBm)
- 40mW (16dBm)
- 32mW (15dBm)
- 23mW (13dBm)
- 10mW (10dBm)
- 6mW (7dBm)
- 1mW (0dBm)

For 802.11g:

- 63mW (18dBm)
- 40mW (16dBm)
- 32mW (15dBm)
- 6mW (7dBm)
- 1mW (0dBm)

Receiver Sensitivity

For 802.11b:

- 1Mbps: -94dBm
- 2Mbps: -90dBm
- 5.5Mbps: -88dBm
- 11Mbps: -85dBm

For 802.11g:

- 1Mbps: -94dBm
- 2Mbps: -91dBm
- 5.5Mbps: -89dBm
- 6Mbps: -91dBm
- 9Mbps: -90dBm
- 11Mbps: -86dBm
- 12Mbps: -89dBm
- 18Mbps: -87dBm
- 24Mbps: -84dBm
- 36Mbps: -80dBm
- 48Mbps: -76dBm
- 54Mbps: -73dBm

Technical Specifications (continued)

LEDs

- Power
- 10M/100M
- WLAN

Temperature

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

Humidity

- Operating: 10%~90% (non-condensing)
- Storing: 5%~95% (non-condensing)

Certifications

- FCC Part 15
- UL

Dimensions

- L = 5.59 inches (142mm)
- W = 4.29 inches (109mm)
- H = 1.22 inches (31mm)

Weight

- 0.44 lbs (200g)

Warranty

- 1 Year

* Environmental factors may adversely affect wireless range

Technical Support

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

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

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

Tech Support for customers within the United States:

D-Link Technical Support over the Telephone:

(877) 453-5465

Monday to Friday 6:00am to 6:00pm PST

D-Link Technical Support over the Internet:

<http://support.dlink.com>

email:support@dlink.com

Tech Support for customers within Canada:

D-Link Technical Support over the Telephone:

(800) 361-5265

Monday to Friday 6:00am to 6:00pm PST

D-Link Technical Support over the Internet:

<http://support.dlink.ca>

email:support@dlink.ca

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

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

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

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

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

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

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

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

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

- The customer must submit with the product as part of the claim a written description of the Hardware defect or Software nonconformance in sufficient detail to allow D-Link to confirm the same.

- The original product owner must obtain a Return Material Authorization (“RMA”) number from the Authorized D-Link Service Office and, if requested, provide written proof of purchase of the product (such as a copy of the dated purchase invoice for the product) before the warranty service is provided.
- After an RMA number is issued, the defective product must be packaged securely in the original or other suitable shipping package to ensure that it will not be damaged in transit, and the RMA number must be prominently marked on the outside of the package. Do not include any manuals or accessories in the shipping package. D-Link will only replace the defective portion of the Product and will not ship back any accessories.
- The customer is responsible for all inbound shipping charges to D-Link. No Cash on Delivery (“COD”) is allowed. Products sent COD will either be rejected by D-Link or become the property of D-Link. Products shall be fully insured by the customer. D-Link will not be held responsible for any packages that are lost in transit to D-Link. The repaired or replaced packages will be shipped to the customer via UPS Ground or any common carrier selected by D-Link, with shipping charges prepaid. Expedited shipping is available if shipping charges are prepaid by the customer and upon request.
- Return Merchandise Ship-To Address
USA: 17595 Mt. Herrmann, Fountain Valley, CA 92708
Canada: 2180 Winston Park Drive, Oakville, ON, L6H 5W1 (Visit <http://www.dlink.ca> for detailed warranty information within Canada)

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

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

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

Limitation of Liability: TO THE MAXIMUM EXTENT PERMITTED BY LAW, D-LINK IS NOT LIABLE UNDER ANY CONTRACT, NEGLIGENCE, STRICT LIABILITY OR OTHER LEGAL OR EQUITABLE THEORY FOR ANY LOSS OF USE OF THE PRODUCT, INCONVENIENCE OR DAMAGES OF ANY CHARACTER, WHETHER DIRECT, SPECIAL, INCIDENTAL OR CONSEQUENTIAL (INCLUDING, BUT NOT LIMITED TO, DAMAGES FOR LOSS OF GOODWILL, LOSS OF REVENUE OR PROFIT, WORK STOPPAGE, COMPUTER FAILURE OR MALFUNCTION, FAILURE OF OTHER EQUIPMENT OR COMPUTER PROGRAMS TO WHICH D-LINK’S PRODUCT IS CONNECTED WITH, LOSS OF INFORMATION OR DATA CONTAINED IN, STORED ON, OR INTEGRATED WITH ANY PRODUCT RETURNED TO D-LINK FOR WARRANTY SERVICE) RESULTING FROM THE USE OF THE PRODUCT, RELATING TO WARRANTY SERVICE, OR ARISING OUT OF ANY BREACH OF THIS LIMITED WARRANTY, EVEN IF D-LINK HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. THE SOLE REMEDY FOR A BREACH OF THE FOREGOING LIMITED WARRANTY IS REPAIR, REPLACEMENT OR REFUND OF THE DEFECTIVE OR 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 the product owner may also have other rights which vary from state to state.

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

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

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

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

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

FCC Caution:

The manufacturer is not responsible for any radio or TV interference caused by unauthorized modifications to this equipment; such modifications could void the user's authority to operate the 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.

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

Registration

Register your D-Link product online at <http://support.dlink.com/register/>

(5/12/05)

