Chapter 5 Contents

Chapter 5

Installing and Configuring Access Points

The largest hurdle toward getting your wireless LAN (WLAN) up and running is the configuration of your access points (APs) and wireless clients. The next two chapters examine how you can install and configure both devices. First, let's consider the AP.

Site Survey

Before you install or configure an AP, you should first conduct a site survey. This exercise shows you where the best—and worst—places are in your organization for Wi-Fi reception.

You use an AP and a client to conduct a site survey. Both the AP and client move around to various, temporary locations in an effort to find ideal placement.

Once completed, a thorough site survey tells you:

- Coverage of APs and the ideal location of APs in your WLAN.
- Bit rates and error rates in different locations.
- Whether the number of APs you plan to deploy is enough.
- The performance of applications on the WLAN.

AP Location for Site Survey

When you perform a site survey, try to situate the AP as close to its ultimate location as possible. This helps resolve any problems that might creep up after you mount the AP.

In most cases, you should mount APs at ceiling height. In warehouses and other sites with high ceilings, it's best to mount them between 15 and 25 feet. If you mount them at this height, power delivered to the devices must be addressed. Power over Ethernet (PoE) is discussed in greater detail later, but this is an excellent scenario where you should deliver power in via a power injector, line-power enabled devices (such as Catalyst switches), or line-power patch panels (sometimes referred to as a *mid-span* device). PoE can save a lot of headache and expense.

In some environments it might be desirable to keep the AP out of sight. If you opt to place the AP above ceiling panels, you should place antennas below the ceiling for optimal reception. If this is the case, you should purchase an AP that fits for remote antenna capability.

NOTE: Check your local fire codes. You might need plenum-rated APs and cabling if they are placed above the ceiling tiles.

Performing the Survey

There are two ways you can perform a site survey: manually or assisted. You typically use the manual method when you first install a WLAN.

If you already have a WLAN in place and just want to tweak it, an assisted site survey saves you a lot of shoe leather.

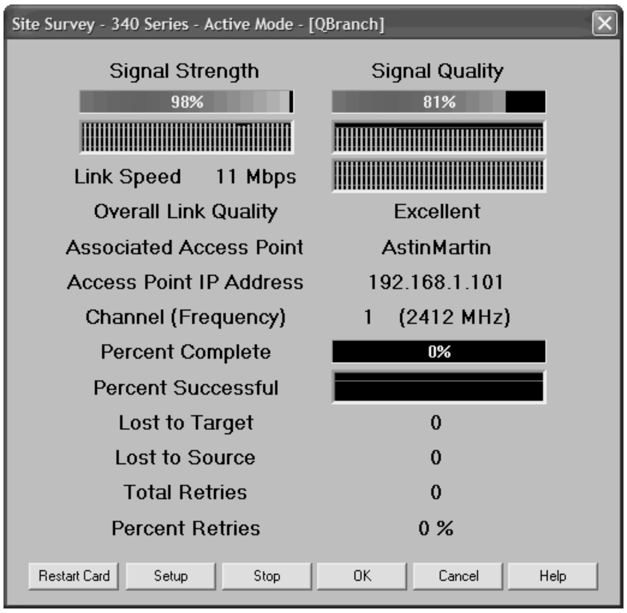
Manual Site Survey

The first way to conduct a site survey is called a *manual* site survey. This means you pick up a Wi-Fi-enabled laptop, palmtop, or specialized wireless survey device and walk around your site and record data from the temporarily located AP as you go.

You should place the AP and antennas where you decide to mount them. However, before you actually mount them, perform the survey, and take your Wi-Fi-enabled device to various client locations within its coverage area.

Cisco wireless client adapters (which are examined in greater detail in Chapter 6, “Configuring Clients”) include the Cisco Aironet Desktop Utility, which includes a site survey tool component. This tool allows you to view the strength of your AP’s signal, the quality of the signal, packet retries, and a host of other data. This tool is shown in Figure 5-1.

Figure 5-1 *Aironet Desktop Utility Site Survey Tool*



Site Survey - 340 Series - Active Mode - [QBranch]

Signal Strength	Signal Quality
98%	81%

Link Speed 11 Mbps	
Overall Link Quality	Excellent
Associated Access Point	AstinMartin
Access Point IP Address	192.168.1.101
Channel (Frequency)	1 (2412 MHz)
Percent Complete	0%
Percent Successful	
Lost to Target	0
Lost to Source	0
Total Retries	0
Percent Retries	0 %

When you conduct a site survey, be aware of these issues:

- Wood floors can cause floor-to-floor interaction between APs. Think three dimensionally. Make sure channel selections are appropriate for APs located on adjacent floors.
- Office and room doors should be closed before beginning the survey. This shows how the WLAN performs in real, day-to-day functioning.
- Metal blinds should be closed because, in this position, they are major disruptors of signal quality.

Follow these steps when you perform a manual site survey:

Step 1. Start with a building map or layout that shows all the coverage areas.

Step 2. Identify and record possible sources of interference, including elevators, microwave ovens, HVAC units, power distribution closets, and so forth. Metal bookshelves and cabinets can also disrupt your AP's signal.

Step 3. Move around your facility, and make note of signal strength, signal-to-noise ratio (SNR), and packet retry counts.

Step 4. Move the AP to a different location and with a fresh copy of the facility schematic, repeat step 3.

It's easy to look at the signal strength meter on your site survey tool and make assumptions based on the strength of the signal you receive. However, you should also be cognizant of the signal-to-noise ratio (SNR). If noise in the band is too high, it can cause reception problems—even if you have a strong signal from the AP. Use the SNR and *packet retry count* (the number of times packets were retransmitted for successful reception) to get an accurate view of your signal quality.

Packet retry count should be below 10 percent in all areas. You should use packet retry in tandem with the SNR reading for a good picture of signal quality. The signal might be strong enough, but because of noise or multipath interference, packets are resent. Without an SNR reading, you cannot tell if packet retries spike because you are out of range, there's too much noise, or the signal is too low.

Assisted Site Survey

If you use the CiscoWorks Wireless LAN Solution Engine (WLSE) or a Wireless LAN Controller, you can perform an *assisted* site survey. This survey allows you to simulate the optimal radio transmit power and channel selection in an existing WLAN. You can select specific APs in your WLAN, and then generate your results. The assisted site survey allows you to:

- Select specific APs to test
- Perform a radio scan
- Perform a client walkabout (not performed on the WLAN Controller)
- Generate radio parameters

The benefit of this test is that it allows you to conduct the site survey without the need to walk all over your office (unless you chose the client walkabout test, of course). It also allows you a certain level of granularity, to pick and choose which devices to test. Although this tool is great for WLANs with existing APs, it's not ideal for pre-installation work.

We discuss CiscoWorks WLSE in greater detail in Chapter 10, "CiscoWorks Wireless LAN Solution Engine (WLSE)."

Analyzing Your Site

After you conduct your site survey, it's time to analyze the data. If you conduct a manual site survey, bring a map along with you and record site data for each location. After you complete the survey, sit down and examine the map. Do you notice poor signal reception in certain areas? What characteristics are at play in that area that might affect signal quality?

You should also experiment with different AP and antenna locations to find the best site. Use different maps for different AP placement options, as this helps you keep your data clear and easy to understand.

If you encounter interference you simply cannot locate, you might need to use a spectrum analyzer. These devices scan a wide frequency band to locate transmissions. Unfortunately, they are also expensive. You can expect to pay thousands of dollars for one (or you can rent one). On top of the expense, there's a steep learning curve in their configuration, setup, and use. If the purchase of a spectrum analyzer is not in your budget, you might hire a consultant with specialized tools to conduct the site survey.

Cabling

There are four options to power your AP. The options depend on whether or not your AP receives power from a power supply or if it receives inline power. The four connection options are:

- A switch with inline power (such as a Catalyst switch).
- An inline power patch panel between the switch and the AP.
- A power injector between the switch and the AP. A power injector is a device that plugs into a wall socket, and then connects into the Ethernet line to provide power to one port (in this case, the AP).
- A local power supply.

Of these power methods, the first three use PoE to supply power to the AP.

NOTE: If you use the AP's 5-GHz radio, make sure your switch and patch panel provide enough power to the device. The 2.4-GHz radios are widely covered, but there might not be enough support for the 5-GHz radio.

PoE is a technology that eliminates the need for a separate power supply to plug into the AP. That is, power is delivered—as the name suggests—over the same Ethernet cable used to deliver data. This is ideal for places where it might be difficult, if not impossible, to provide a separate power source.

NOTE: You should not use PoE in conjunction with a separate power supply. This can cause the powered Ethernet switch port to shut down.

You must also consider the distance between the AP and the switch. The maximum range for 100BaseT Ethernet is 100 meters.

Encryption and Authentication

Wired Equivalent Privacy (WEP) keys protect your data and keep your WLAN secure at the most basic level. WEP is easy to beat, so a better option is 802.1X authentication. This section explains how you can set up either of these mechanisms on your AP.

40/64-Bit Versus 104/128-Bit Encryption

Although WEP keys are not the best option for WLAN security, they are better than nothing. If you find yourself in a situation in which 802.1X authentication is not possible, you should at least use WEP keys. WEP keys come in two “strengths”: 64- and 128-bit.

NOTE: WEP keys are often referred to as 40- and 104-bit, or 64- and 128-bit. The terms are interchangeable. 40-bit and 64-bit keys offer the same level of protection.

So what’s happening to the other 24 bits?

Those “missing” 24 bits are the key’s initialization vector. So, in a 64-bit WEP environment, only 40 bits are considered part of the actual key.

Ideally, you use 128-bit encryption whenever possible, because it is more difficult to break than 64-bit encryption. So why include 64-bit encryption at all? It’s largely a matter of backwards compatibility with early wireless clients that supported only 64-bit encryption. In almost every case, if you have to use WEP, opt for 128-bit over 64-bit encryption.

To establish a WEP setting is straightforward and you can perform it quickly with the **Express Security** selection on the AP configuration screen (the first screen that appears when you log onto your AP). Simply open the screen and enter your WEP key.

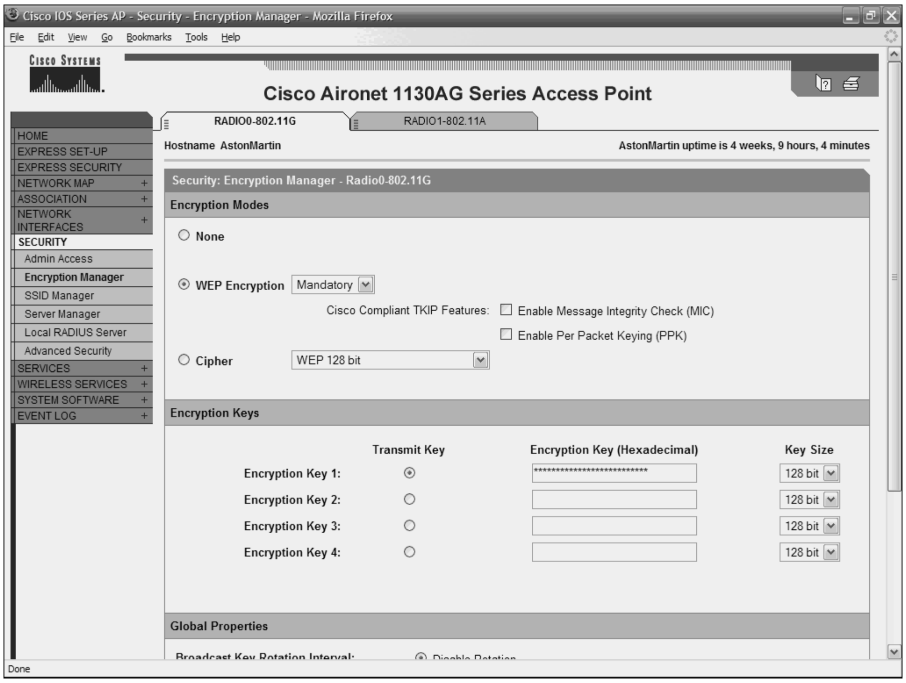
You can perform more detailed WEP key tasks if you follow these steps:

Step 1. On the Cisco 1130AG AP, use a web browser and navigate to the device’s home page.

Step 2. On the menu located to the left side of the window, click **Security**.

Step 3. When the Security section expands, click **Encryption Manager**. This spawns the screen shown in Figure 5-2.

Figure 5-2 *Managing WEP Keys on the Cisco AP*



Cisco Aironet 1130AG Series Access Point

Hostname AstonMartin

AstonMartin uptime is 4 weeks, 9 hours, 4 minutes

Security: Encryption Manager - Radio0-802.11G

Encryption Modes

○ None

● WEP Encryption Mandatory

Cisco Compliant TKIP Features: □ Enable Message Integrity Check (MIC)

□ Enable Per Packet Keying (PPK)

○ Cipher WEP 128 bit

Encryption Keys

	Transmit Key	Encryption Key (Hexadecimal)	Key Size
Encryption Key 1:	●	**************************	128 bit
Encryption Key 2:	○		128 bit
Encryption Key 3:	○		128 bit
Encryption Key 4:	○		128 bit

Global Properties

Broadcast Key Rotation Interval: ● Disable Rotation

Step 4. This screen allows you to manage your WEP key settings:

- The Encryption Modes area contains settings to disable WEP, enable WEP, or establish cipher settings.
- The Encryption Keys area is the section in which up to four WEP keys and their lengths are entered. For security, the WEP keys are not shown as you enter them. Because of this, it is somewhat difficult to determine if you mistype the key. Enter a key on each line if you plan on rotating through WEP keys.
- The Global Properties area is used to manage the behavior of your WEP keys. Here, you can select whether to rotate between keys, how long the interval is between each rotation, and how to manage keys within your group.

Step 5. Because the Cisco 1130 AP has both 2.4-GHz and 5-GHz radios, you can apply these settings to one radio or both radios. In this case, click **Apply-Radio0** to establish these settings for the 2.4-GHz radio. **Apply-All** sends the settings to both radios.

Setting WEP Keys Using the CLI

If you prefer to use the command-line interface to configure WEP keys on your Aironet AP, follow these settings:

```
ap1130# configure terminal
ap1130(config)# configure interface dot11radio 0
ap1130(config-if)# encryption vlan 07 key 1 size 128 abc123abc123abc123abc123cc
    transmit-key
ap1130(config-ssid)# end
ap1130# copy running-config startup-config
```

Table 5-1 explains the meaning of each command.

Table 5-1 *Configuration Commands for WEP Key Configuration.*

Command	Description
configure terminal	Enters global configuration mode.
configure interface dot11radio {**0** | **1**}	Enters interface configuration mode for the radio. The 2.4-GHz radio is **0**; the 5-GHz radio is **1**.
encryption [**vlan** *vlan-id*] **key** *key-number size* {**40** | **128**} [**transmit-key**]	Establishes the settings for your WEP key. **vlan** is optional. It allows you to select the VLAN for which you wish to use the WEP key. Sets which key number you want to use. You can set up to four WEP keys. Enters the size of the WEP key. Settings are either 40- or 128-bit and contain 26 hexadecimal digits. **transmit-key** is optional. By default, the key in slot 1 is the default transmit key, but you can use this setting to specify which key (1 through 4) to use.
End	Returns to privileged EXEC mode.
copy running-config startup-config	An optional step that allows you to save your entries to the configuration file.

In this example, a 128-bit WEP key was configured on the AP's 2.4-GHz radio. The key—specified as the first key—was established as a transmit key in the 07 VLAN.

802.1X Configuration

A stronger means of security is 802.1X authentication. Like most other aspects of Aironet configuration, Cisco gives you the option to set it up quickly, or really dig down into the configuration details.

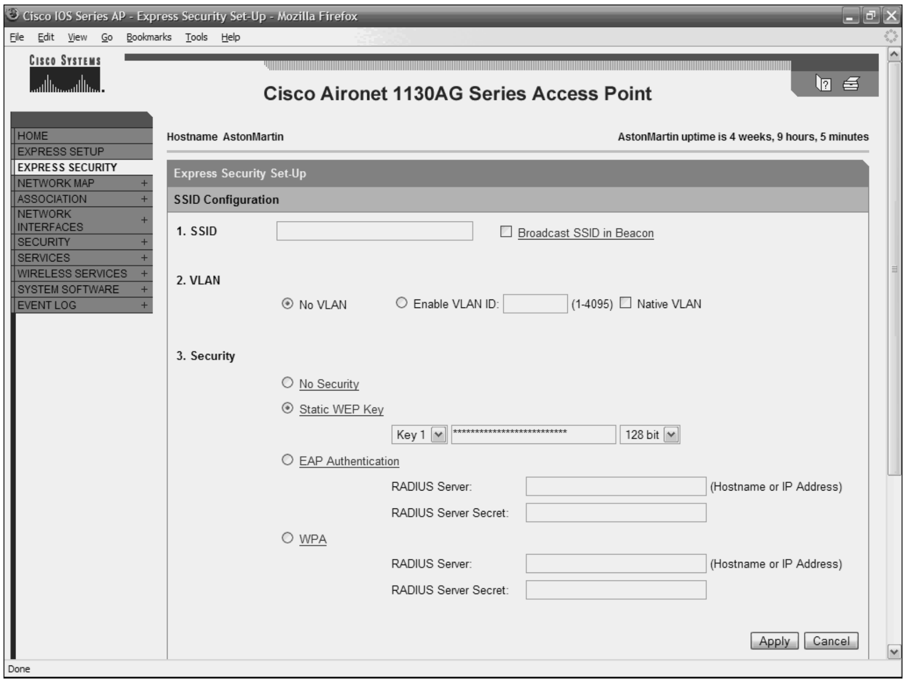
NOTE: To set up 802.1X authentication, you must have a RADIUS server on your network. Without it, you cannot set up 802.1X authentication. The AP itself, or routers, can also act as RADIUS servers.

To configure 802.1X authentication, follow these steps:

Step 1. Navigate to the AP's home page.

Step 2. Click **Express Security** from the menu on the left. This calls up the screen shown in Figure 5-3.

Figure 5-3 *802.1X Input Information on the Express Security Screen.*



Cisco Aironet 1130AG Series Access Point

Hostname AstonMartin

AstonMartin uptime is 4 weeks, 9 hours, 5 minutes

Express Security Set-Up

SSID Configuration

1. SSID ☐ Broadcast SSID in Beacon

2. VLAN

● No VLAN ○ Enable VLAN ID: (1-4095) ☐ Native VLAN

3. Security

○ No Security

● Static WEP Key

Key 1 ************************** 128 bit

○ EAP Authentication

RADIUS Server: (Hostname or IP Address)

RADIUS Server Secret:

○ WPA

RADIUS Server: (Hostname or IP Address)

RADIUS Server Secret:

Step 3. In the Security area, you establish whether you want no security, a static WEP key (along with a place to enter the key), Extensible Authentication Protocol (EAP) authentication, or Wi-Fi Protected Access (WPA) authentication.

Step 4. To set up LEAP, Protected EAP (PEAP), EAP-Transport Layer Security (EAP-TLS), EAP-Tunneled TLS (EAP-TTLS), EAP- Generic Token Card (EAP-GTC), EAP-Subscriber Identity Module (EAP-SIM), and other 802.1X/EAP-based protocols, click the **EAP Authentication** radio button. To use WPA, click the **WPA** radio button.

Step 5. In the boxes next to the **EAP Authentication** radio button or **WPA** radio button, enter the name of the RADIUS server and the secret that will be shared between the AP and the RADIUS server.

Step 6. Click **Apply**.

These settings allow for a quick configuration of 802.1X authentication. For more control over your AP's handling of 802.1X, click **Security** from the menu on the left. This allows you to do such things as specify backup RADIUS servers, enable accounting, manage the authentication port, and manage several other details.

802.1X CLI Configuration

If you prefer to use the command-line interface to configure authentication on your Aironet AP, follow these settings:

```
ap1130# configure terminal
ap1130(config)# interface dot11radio 0
ap1130(config-if)# ssid qbranch
ap1130(config-ssid)# authentication open mac moneypenny alternate eap moneypenny
ap1130(config-ssid)# authentication key-management wpa optional
ap1130(config-ssid)# end
ap1130# copy running-config startup-config
```

Table 5-2 explains these commands.

Table 5-2 *CLI Commands for 802.1X Authentication*

Command	Description
configure terminal	Enters global configuration mode.
interface dot11radio {**1** | **0**}	Enters the configuration mode for the radio interface. The 2.4-GHz radio is **0**; the 5-GHz radio is **1**.
ssid *ssid-string*	Create a Service Set ID (SSID) and enter configuration mode for the new SSID.

Table 5-2 *CLI Commands for 802.1X Authentication (Continued)*

Command	Description
authentication open [**mac-address** *list-name* [**alternate**]] [**eap** *list-name*]	This step is optional. It sets the authentication type to open for this SSID. **mac-address** sets the SSID's authentication type to open with MAC address authentication. This requires all clients to perform MAC address authentication before joining the network. The keyword **alternate** is used to allow clients to join using either EAP or MAC authentication. **eap** sets the SSID's authentication type to open with EAP authentication. The AP requires all clients to perform EAP authentication before joining the network. For *list-name,* specify the authentication method list.
authentication shared [**mac-address** *list-name*] [**eap** *list-name*]	This is an optional step and is used to set the authentication type for the SSID to shared key. **mac-address** sets the SSID's authentication type to shared key with MAC address authentication. For *list-name*, enter the authentication method list. **eap** sets the SSID's authentication type to shared key with EAP address authentication. For *list-name*, enter the authentication method list.
authentication network-eap ***list-name*** [**mac-address** *list-name*]	This step is optional. It is used to set the authentication type for the SSID to Network-EAP. It is used to authenticate an EAP client with an EAP-compatible RADIUS server. The SSID's authentication type can be altered so that it also requires MAC address authentication. For *list-name*, enter the authentication method list.

continues

Table 5-2 *CLI Commands for 802.1X Authentication (Continued)*

Command	**Description**
authentication key-management {[**wpa**] [**cckm**]} [**optional**]	This is an optional step and is used to set the authentication type for the SSID to WPA, Cisco Centeralized Key Management (CCKM), or both. If you use the keyword **optional**, clients that do not use WPA or CCKM are allowed to use the SSID. However, if **optional** is not used, clients must use WPA or CCKM to connect. If you choose to enable CCKM for an SSID, you must also enable Network-EAP authentication. To enable WPA for an SSID, you must also enable Open authentication, Network-EAP, or both.
end	Return to privileged EXEC mode.
copy running-config startup-config	This step is optional and saves your entries in the configuration file.

In this example, the authentication type for the SSID qbranch on the 2.4-GHz radio has been set to Network-EAP with WPA key management. Clients that use qbranch are authenticated with the moneypenny server list.

Antenna Placement

APs that require external antennas need special care. You need to configure the antennas properly, consider what role the AP serves (AP or bridge), and consider where the antennas are placed.

For more information on Wi-Fi antennas, flip back to Chapter 2, "Cisco Antennas."

Ideally, you locate the AP as close as possible to the antennas. The farther the signal has to travel across the cabling between the AP and the antenna, the more signal reduction (also known as *RF attenuation*) you experience. For instance, if you are locating an antenna in a courtyard to service clients roaming outside, don't place the AP in a closet, dozens of feet away from the antenna. Instead, place the AP outside in a weatherproof enclosure, so it's closer to the antenna. An even better idea is to use a 1300 series, which is weatherproof.

Signal loss depends on what type of cable you use. Cisco offers two types of cable. One is similar to LMR400 and has a loss of 6.7dB per 100 feet, whereas the other is similar to LMR600 with 4.4dB per 100 feet. For every 3dB, you lose about half the signal's power. This loss occurs on both transmission and reception. You can use higher-quality cable to reduce signal loss over longer cables, but keep in mind that higher-quality cable is more expensive.

In addition, if you use an 802.11a product, cable loss is an even more significant issue. Loss increases with frequency, and coaxial cable has even more attenuation with 5-GHz signals than 2.4-GHz signals.

Initial Settings

Cisco APs contain pages and pages of configuration settings. These settings are good when you need to fine tune your AP's performance and role in the network; however, if you want to get started right away, the AP contains two *express* pages:

- Express Set-Up
- Express Security Set-Up

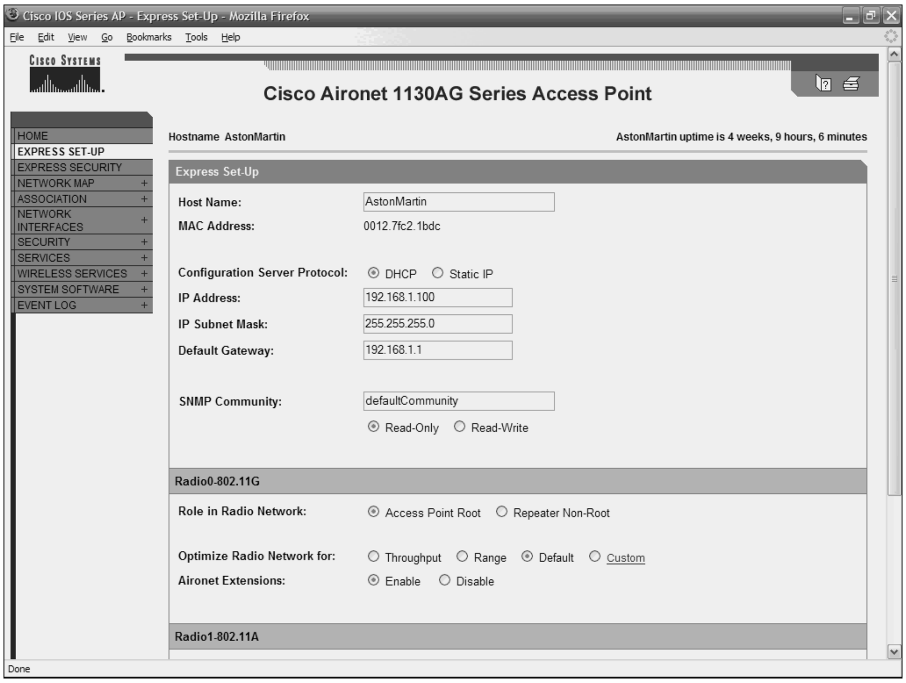
Express Security Set-Up was covered earlier in this chapter. Express Set-Up is the page you want to use when you first configure your Cisco AP.

Express Set-Up

Express Set-Up is shown in Figure 5-4. This page allows you to manage such details as:

- Host name
- How an IP address is acquired (dynamic host configuration protocol [DHCP], or statically)
- IP address
- IP subnet mask
- Default gateway
- SNMP community
- The radio's role in the network (AP or repeater)
- Options for general AP performance optimization
- Whether Aironet extensions are enabled or disabled

Figure 5-4 *Express Set-Up Allows You to Quickly Enter AP Information in One Place*



Hostname AstonMartin

AstonMartin uptime is 4 weeks, 9 hours, 6 minutes

Express Set-Up

Host Name:	AstonMartin
MAC Address:	0012.7fc2.1bdc
Configuration Server Protocol:	● DHCP ○ Static IP
IP Address:	192.168.1.100
IP Subnet Mask:	255.255.255.0
Default Gateway:	192.168.1.1
SNMP Community:	defaultCommunity ● Read-Only ○ Read-Write

Radio0-802.11G

Role in Radio Network:	● Access Point Root ○ Repeater Non-Root
Optimize Radio Network for:	○ Throughput ○ Range ● Default ○ Custom
Aironet Extensions:	● Enable ○ Disable

Radio1-802.11A

Express Security Set-Up

Express Security Set-Up is used to quickly manage your AP's security features. Similar to Express Set-Up, this screen is used to manage the broad strokes of your device's security functions. The details are managed from elsewhere on the device. Figure 5-3 shows the Express Security Set-Up screen.

This page allows you to:

- Establish your AP's SSIDs
- Enable and specify VLANs
- Set up security protocols
  - — WEP (including specifying WEP keys)
  - — WPA
  - — 802.1X
- View a table that shows your AP's SSIDs

APs as Repeaters

Most of this chapter deals with the issue of how to connect an AP to your WLAN. However, to extend the range of your WLAN, you can add a repeater AP to the network. This AP is not physically connected to the WLAN, but is instead added to augment range and the clients that access the WLAN.

NOTE: Because APs have two radios, only one can be used as a repeater. You must configure the other as a root radio.

Repeater Overview

The repeater forwards traffic between wireless clients and the AP connected to the wired LAN (or other repeaters). APs configured as repeaters do not forward traffic from the Ethernet port (although this might change in future versions of the software).

NOTE: After your AP is configured as a repeater, it shuts down its Ethernet connection. Any devices connected to the Ethernet port are disconnected from the AP.

You can configure multiple APs as a chain of repeaters. However, throughput suffers as additional APs are added to the chain, because each repeater must receive and then retransmit the packet on the same channel. Because of this, throughput is cut in half for each repeater added.

Following are some guidelines to bear in mind when you place an AP in repeater mode:

- It's best to use repeaters to serve clients that do not demand high throughput.
- Cisco AP repeaters work best when clients are Cisco devices. Problems occur when third-party devices try to associate with repeater APs.
- Ensure the data rates configured on the repeater AP match the data rates of the parent AP.

Configuring Repeater APs

Follow these steps to configure your Cisco AP as a repeater AP:

Step 1. The first step to configure a repeater AP is to enable Aironet extensions on both the parent and repeater APs. By default, these extensions are enabled. Aironet extensions are useful for the AP to communicate with other Cisco wireless devices. However, if you have problems getting non-Cisco equipment to talk to the AP, a first step is to disable Aironet extensions.

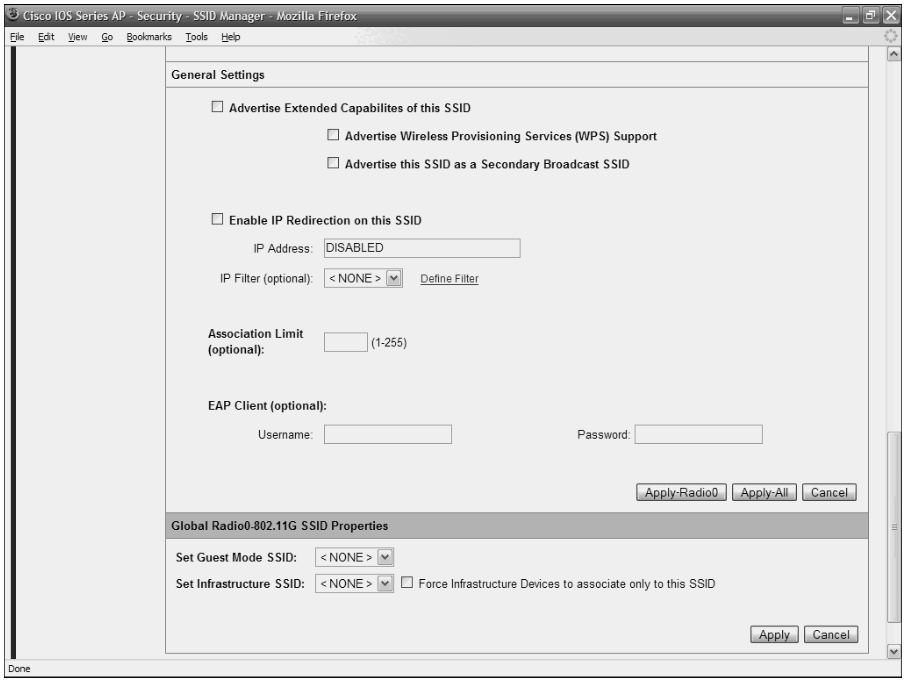
Step 2. Next, open the Security page from the menu at the left of the AP's main page.

Step 3. Select **SSID Manager** from the submenu.

Step 4. Click the tab at the top of the screen to indicate which radio you want to set up as a repeater.

Step 5. Scroll to the bottom of the screen to the section named Global Radio0-802.11G SSID Properties. Of course, if you had selected to manage the 802.11a radio, you would have to scroll to the section indicating that radio. This is shown in Figure 5-5.

Figure 5-5 *Selecting the Radio's SSID Properties*


Cisco IOS Series AP - Security - SSID Manager - Mozilla Firefox
File Edit View Go Bookmarks Tools Help
Done

General Settings

☐ Advertise Extended Capabilites of this SSID

☐ Advertise Wireless Provisioning Services (WPS) Support

☐ Advertise this SSID as a Secondary Broadcast SSID

☐ Enable IP Redirection on this SSID

IP Address: DISABLED

IP Filter (optional): < NONE > Define Filter

Association Limit (optional): (1-255)

EAP Client (optional):

Username: Password:

Apply-Radio0 Apply-All Cancel

Global Radio0-802.11G SSID Properties

Set Guest Mode SSID: < NONE >

Set Infrastructure SSID: < NONE > ☐ Force Infrastructure Devices to associate only to this SSID

Apply Cancel

Step 6. In the **Set Infrastructure SSID** drop-down menu, select the name of the SSID the repeater uses to associate to a root AP.

Step 7. Clicking the checkbox next to the drop-down menu forces infrastructure devices to associate to the repeater AP that uses this SSID.

Step 8. Click **Apply**.

Step 9. Click the **Express Setup** selection from the menu at the left.

Step 10. For the radio you want to establish as a repeater, click the radio button next to **Repeater Non-Root**.

Step 11. In the Aironet Extensions section, click the radio button next to **Enable**.

Step 12. Click **Apply** at the bottom of the screen.

Most WLAN problems stem from improperly configured APs or clients. If you properly install and configure your APs, you are on the right track to an effective WLAN.

Configuring a Repeater Using the CLI

If you want to configure your AP as a repeater and use the command-line interface, the following is an example configuration setting. This example configures the AP with two parents:

```
ap1130# configure terminal
ap1130(config)# interface dot11radio 0
ap1130(config-if)# ssid qbranch
ap1130(config-ssid)# infrastructure-ssid
ap1130(config-ssid)# exit
ap1130(config-if)# station-role repeater
ap1130(config-if)# dot11 extensions aironet
ap1130(config-if)# parent 1 0012.7fc2.1bdc 1000
ap1130(config-if)# parent 2 0012.44b4.b250 1000
ap1130(config-if)# end
ao1130# copy running-config startup-config
```

Table 5-3 explains each command in this list.

Table 5-3 *CLI Commands for Configuring an AP as a Repeater*

Command	**Description**
configure terminal	Enters global configuration mode.
interface dot11radio {**1** | **0**}	Enters the configuration mode for the radio interface. The 2.4-GHz radio is 0; the 5-GHz radio is 1.
ssid *ssid-string*	Creates the SSID the repeater uses to associate to a root AP. The next step is used to designate this SSID as an infrastructure SSID. If an infrastructure SSID was created on the root AP, create the same SSID on the repeater.
infrastructure-ssid [**optional**]	Assigns the SSID as an infrastructure SSID. This is the SSID the repeater uses to associate to the root AP. Infrastructure devices must associate to the repeater AP and use this SSID unless the **optional** keyword is entered.

continues

Table 5-3 *CLI Commands for Configuring an AP as a Repeater (Continued)*

Command	Description
exit	Exits SSID configuration mode and returns to radio interface configuration.
station-role repeater	Establishes this AP's role as a repeater.
dot11 extensions aironet	Enables Aironet extensions.
parent {*parent-number*} *mac-address* [*timeout*]	This step is optional and is used to enter the MAC address for each AP to which the repeater should associate. MAC addresses for up to four parents can be entered. If the repeater fails to associate to the first parent, it moves to the next on the list. You can enter a timeout value (numerous seconds between 0 and 65535), which establishes how long the repeater tries to associate to a parent before it moves to the next.
end	Returns to privileged EXEC mode.
copy running-config startup-config	This step is optional and saves your entries in the configuration file.

In this example, the SSID qbranch is configured as a repeater and attempts to associate to one of two parent APs. qbranch attempts to associate to each parent for 1000 seconds before it moves on to the next.

Other Resources

The complete reference guides for Cisco APs are found online; just follow these steps:

Step 1. Go to www.cisco.com.

Step 2. In the Quick Links section, click **Products & Solutions**.

Step 3. Click **Wireless**. A window appears that contains a partial list of Cisco products.

Step 4. Click **All Wireless Products**.

Step 5. Scroll down to the Product Portfolio section to locate the Wireless LAN subsection.

Step 6. Select the desired Cisco AP.

- **Cisco 1000 deployment guide that includes site survey guide**:

  http://www.cisco.com/univercd/cc/td/doc/product/wireless/airo1000/a1kinit/1dep.pdf