Controlling Lightweight Access Points

This chapter contains these sections:

- Access Point Communication Protocols, page 9-2
- Searching for Access Points, page 9-9
- Searching for Access Point Radios, page 9-14
- Configuring Global Credentials for Access Points, page 9-16
- Configuring Authentication for Access Points, page 9-20
- Configuring Embedded Access Points, page 9-26
- Converting Autonomous Access Points to Lightweight Mode, page 9-28
- Configuring OfficeExtend Access Points, page 9-51
- Using Cisco Workgroup Bridges, page 9-70
- Configuring Backup Controllers, page 9-77
- Configuring Failover Priority for Access Points, page 9-81
- Configuring Country Codes, page 9-87
- Migrating Access Points from the -J Regulatory Domain to the -U Regulatory Domain, page 9-93
- Using the W56 Band in Japan, page 9-96
- Dynamic Frequency Selection, page 9-96
- Optimizing RFID Tracking on Access Points, page 9-97
- Configuring Probe Request Forwarding, page 9-100
- Retrieving the Unique Device Identifier on Controllers and Access Points, page 9-101
- Performing a Link Test, page 9-102
- Configuring Link Latency, page 9-105
- Configuring the TCP MSS, page 9-108
- Configuring Power over Ethernet, page 9-110
- Configuring Flashing LEDs, page 9-114
- Viewing Clients, page 9-115
- Configuring LED States for Access Points, page 9-120

Access Point Communication Protocols

This section contains the following topics:

- Information About Access Point Communication Protocols, page 9-2
- Guidelines and Limitations, page 9-2
- Configuring Data Encryption, page 9-3
- Viewing CAPWAP Maximum Transmission Unit Information, page 9-6
- Debugging CAPWAP, page 9-7
- Controller Discovery Process, page 9-7
- Verifying that Access Points Join the Controller, page 9-8

Information About Access Point Communication Protocols

Cisco lightweight access points use the IETF standard Control and Provisioning of Wireless Access Points Protocol (CAPWAP) to communicate with the controller and other lightweight access points on the network.

CAPWAP, which is based on LWAPP, is a standard, interoperable protocol that enables a controller to manage a collection of wireless access points. CAPWAP is implemented in controller for these reasons:

- To provide an upgrade path from Cisco products that use LWAPP to next-generation Cisco products that use CAPWAP
- To manage RFID readers and similar devices
- To enable controllers to interoperate with third-party access points in the future

LWAPP-enabled access points can discover and join a CAPWAP controller, and conversion to a CAPWAP controller is seamless. For example, the controller discovery process and the firmware downloading process when using CAPWAP are the same as when using LWAPP. The one exception is for Layer 2 deployments, which are not supported by CAPWAP.

You can deploy CAPWAP controllers and LWAPP controllers on the same network. The CAPWAP-enabled software allows access points to join either a controller running CAPWAP or LWAPP. The only exceptions are that the Cisco Aironet 1040, 1140, 1260, 3500, and 3600 Series Access Points, which support only CAPWAP and join only controllers that run CAPWAP. For example, an 1130 series access point can join a controller running either CAPWAP or LWAPP where an1140 series access point can join only a controller that runs CAPWAP.

Guidelines and Limitations

- If your firewall is currently configured to allow traffic only from access points using LWAPP, you must change the rules of the firewall to allow traffic from access points using CAPWAP.
- Make sure that the CAPWAP UDP ports 5246 and 5247 (similar to the LWAPP UDP ports 12222 and 12223) are enabled and are not blocked by an intermediate device that could prevent an access point from joining the controller.
- If access control lists (ACLs) are in the control path between the controller and its access points, you need to open new protocol ports to prevent access points from being stranded.

- Ensure that the controllers are configured with the correct date and time. If the date and time configured on the controller precedes the creation and installation date of certificates on the access points, the access point fails to join the controller.

Configuring Data Encryption

This section contains the following topics:

- Information About Data Encryption, page 9-3
- Guidelines and Limitations, page 9-3
- Upgrading or Downgrading DTLS Images for Cisco 5500 Series Controllers, page 9-4
- Configuring Data Encryption, page 9-4

Information About Data Encryption

Cisco 5500 Series Controllers enable you to encrypt CAPWAP control packets (and optionally, CAPWAP data packets) that are sent between the access point and the controller using Datagram Transport Layer Security (DTLS). DTLS is a standards-track Internet Engineering Task Force (IETF) protocol based on TLS. CAPWAP control packets are management packets exchanged between a controller and an access point while CAPWAP data packets encapsulate forwarded wireless frames. CAPWAP control and data packets are sent over separate UDP ports: 5246 (control) and 5247 (data). If an access point does not support DTLS data encryption, DTLS is enabled only for the control plane, and a DTLS session for the data plane is not established.

Guidelines and Limitations

- Cisco 1130 and 1240 series access points support DTLS data encryption with software-based encryption, and 1040, 1140, 1250, 1260, 3500, and 3600 series access points support DTLS data encryption with hardware-based encryption.
- DTLS data encryption is enabled automatically for OfficeExtend access points but disabled by default for all other access points. Most access points are deployed in a secure network within a company building, so data encryption is not necessary. In contrast, the traffic between an OfficeExtend access point and the controller travels through an unsecure public network, so data encryption is more important for these access points. When data encryption is enabled, traffic is encrypted at the access point before it is sent to the controller and at the controller before it is sent to the client.
- Encryption limits throughput at both the controller and the access point, and maximum throughput is desired for most enterprise networks.
- In a Cisco unified local wireless network environment, do not enable DTLS on the Cisco 1130 and 1240 access points, as it may result in severe throughput degradation and may render the APs unusable.

  See the "Configuring OfficeExtend Access Points" section on page 9-51 for more information on OfficeExtend access points.
- You can use the controller to enable or disable DTLS data encryption for a specific access point or for all access points.
- The availability of data DTLS for the 7.0.116.0 release is as follows:

  - The Cisco 5500 Series Controller will be available with two licenses options: One that allows data DTLS without any license requirements and another image that requires a license to use data DTLS. See the "Upgrading or Downgrading DTLS Images for Cisco 5500 Series Controllers" section on page 9-4. The images for the DTLS and licensed DTLS images are as follows:
    a. Licensed DTLS—AS_5500_LDPE_x_x_x_x.aes
    b. Non licensed DTLS—AS_5500_x_x_x_x.aes
  - Cisco 2500, WiSM2, WLC2—By default, these platforms do not contain DTLS. To turn on data DTLS, you must install a license. These platforms have a single image with data DTLS turned off. To use data DTLS, you must have a license.
- If your controller does not have a data DTLS license and if the access point associated with the controller has DTLS enabled, the data path will be unencrypted.
- Non-Russian customers using Cisco 5508 Series Controller do not need data DTLS license. However all customers using WISM2 and Cisco 2500 Series Controllers must enable data DTLS.

Upgrading or Downgrading DTLS Images for Cisco 5500 Series Controllers

Step 1 The upgrade operation fails on the first attempt with a warning indicating that the upgrade to a licensed DTLS image is irreversible.

Caution Do not reboot the controller after Step 1.

Step 2 On a subsequent attempt, the license is applied and the image is successfully updated.

Guidelines and Limitations

- You cannot install a regular image (non-Licensed data DTLS) once a licensed data DTLS image is installed.
- You can upgrade from one licensed DTLS image to another licensed DTLS image.
- You can upgrade from a regular image (DTLS) to a licensed DTLS image in a two step process.
- You can use the **show sysinfo** command to verify the LDPE image, before and after the image upgrade.

Configuring Data Encryption

This section contains the following topics:

- Configuring Data Encryption (GUI), page 9-5
- Configuring Data Encryption (CLI), page 9-5

Configuring Data Encryption (GUI)

Prerequisites

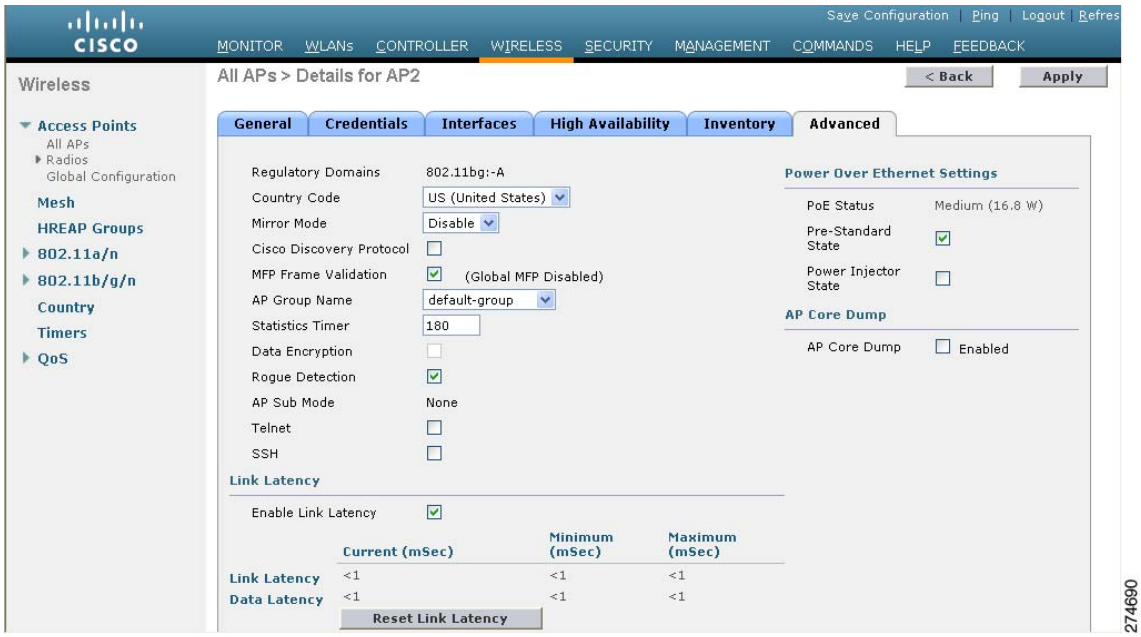
Ensure that the base license is installed on the Cisco 5500 Series Controller. Once the license is installed, you can enable data encryption for the access points. See Chapter 4, "Configuring Controller Settings," for information on obtaining and installing licenses.

Step 1 Choose **Wireless** > **Access Points** > **All APs** to open the All APs page.

Step 2 Click the name of the access point for which you want to enable data encryption.

Step 3 Choose the **Advanced** tab to open the All APs > Details for (Advanced) page.

Figure 9-1 All APs > Details for (Advanced) Page



Step 4 Select the **Data Encryption** check box to enable data encryption for this access point or unselect it to disable this feature. The default value is unselected.

Note Changing the data encryption mode requires the access points to rejoin the controller.

Step 5 Click **Apply** to commit your changes.

Step 6 Click **Save Configuration** to save your changes.

Configuring Data Encryption (CLI)

Note In images without a DTLS license, the **config** or **show** commands are not available.

Step 1 Enable or disable data encryption for all access points or a specific access point by entering this command:

config ap link-encryption {**enable** | **disable**} {**all** | *Cisco_AP*}

The default value is disabled.

Note Changing the data encryption mode requires the access points to rejoin the controller.

Step 2 When prompted to confirm that you want to disconnect the access point(s) and attached client(s), enter **Y**.

Step 3 Enter the **save config** command to save your configuration.

Step 4 See the encryption state of all access points or a specific access point by entering this command:

show ap link-encryption {**all** | *Cisco_AP*}

Information similar to the following appears:

```
                Encryption Dnstream  Upstream Last
AP Name         State      Count     Count    Update
--------------  ---------- --------  --------  --------
AP1130          En         112       1303      23:49
AP1140          En         232      2146       23:49
             auth err: 198 replay err: 0
AP1250          En         0         0         Never
AP1240          En         6191    15011       22:13
```

This command also shows authentication errors, which tracks the number of integrity check failures, and replay errors, which tracks the number of times that the access point receives the same packet.

Step 5 See a summary of all active DTLS connections by entering this command:

show dtls connections

Information similar to the following appears:

```
AP Name         Local Port        Peer IP        Peer Port              Ciphersuite
-------------- -------------- ----------------  -------------- ----------------------------
AP1130          Capwap_Ctrl    172.20.225.163      62369     TLS_RSA_WITH_AES_128_CBC_SHA
AP1250          Capwap_Ctrl    172.20.225.166      19917     TLS_RSA_WITH_AES_128_CBC_SHA
AP1140          Capwap_Ctrl    172.20.225.165       1904     TLS_RSA_WITH_AES_128_CBC_SHA
AP1140          Capwap_Data    172.20.225.165       1904     TLS_RSA_WITH_AES_128_CBC_SHA
AP1130          Capwap_Data    172.20.225.163      62369     TLS_RSA_WITH_AES_128_CBC_SHA
AP1250          Capwap_Data   172.20.225.166     19917    TLS_RSA_WITH_AES_128_CBC_SHA
```

Note If you experience any problems with DTLS data encryption, enter the **debug dtls** {**all** | **event** | **trace** | **packet**} {**enable** | **disable**} command to debug all DTLS messages, events, traces, or packets.

Viewing CAPWAP Maximum Transmission Unit Information

See the maximum transmission unit (MTU) for the CAPWAP path on the controller by entering this command:

show ap config general *Cisco_AP*

The MTU specifies the maximum size of any packet (in bytes) in a transmission.

Information similar to the following appears:

```
Cisco AP Identifier.............................. 9
Cisco AP Name.................................... Maria-1250
Country code..................................... US  - United States
Regulatory Domain allowed by Country............. 802.11bg:-A     802.11a:-A
AP Country code.................................. US  - United States
AP Regulatory Domain............................. 802.11bg:-A    802.11a:-A
Switch Port Number .............................. 1
MAC Address...................................... 00:1f:ca:bd:bc:7c
IP Address Configuration......................... DHCP
IP Address....................................... 1.100.163.193
IP NetMask....................................... 255.255.255.0
CAPWAP Path MTU.............................. 1485
...
```

Debugging CAPWAP

Use these CLI commands to obtain CAPWAP debug information:

- **debug capwap events** {**enable** | **disable**}—Enables or disables debugging of CAPWAP events.
- **debug capwap errors** {**enable** | **disable**}—Enables or disables debugging of CAPWAP errors.
- **debug capwap detail** {**enable** | **disable**}—Enables or disables debugging of CAPWAP details.
- **debug capwap info** {**enable** | **disable**}—Enables or disables debugging of CAPWAP information.
- **debug capwap packet** {**enable** | **disable**}—Enables or disables debugging of CAPWAP packets.
- **debug capwap payload** {**enable** | **disable**}—Enables or disables debugging of CAPWAP payloads.
- **debug capwap hexdump** {**enable** | **disable**}—Enables or disables debugging of the CAPWAP hexadecimal dump.
- **debug capwap dtls-keepalive** {**enable** | **disable**}—Enables or disables debugging of CAPWAP DTLS data keepalive packets.

Controller Discovery Process

In a CAPWAP environment, a lightweight access point discovers a controller by using CAPWAP discovery mechanisms and then sends the controller a CAPWAP join request. The controller sends the access point a CAPWAP join response allowing the access point to join the controller. When the access point joins the controller, the controller manages its configuration, firmware, control transactions, and data transactions.

Guidelines and Limitations

- Upgrade and downgrade paths from LWAPP to CAPWAP or from CAPWAP to LWAPP are supported. An access point with an LWAPP image starts the discovery process in LWAPP. If it finds an LWAPP controller, it starts the LWAPP discovery process to join the controller. If it does not find a LWAPP controller, it starts the discovery in CAPWAP. If the number of times that the discovery process starts with one discovery type (CAPWAP or LWAPP) exceeds the maximum discovery count and the access point does not receive a discovery response, the discovery type changes to the other type. For example, if the access point does not discover the controller in LWAPP, it starts the discovery process in CAPWAP.

- If an access point is in the UP state and its IP address changes, the access point tears down the existing CAPWAP tunnel and rejoins the controller. In previous software releases, the access point notifies the controller, and the session continues with the changed IP address without tearing down the session.
- You must install software release 4.0.155.0 or later releases on the controller before connecting 1100 and 1300 series access points to the controller. The 1120 and 1310 access points were not supported prior to software release 4.0.155.0.
- During the discovery process, the 1040, 1140, 1260, 3500, and 3600 series access points will only query for Cisco CAPWAP Controllers. It will not query for LWAPP controllers. If you want these access points to query for both LWAPP and CAPWAP controllers then you need to update the DNS.
- To configure the IP addresses that the controller sends in its CAPWAP discovery responses, use the **config network ap-discovery nat-ip-only** {**enable** | **disable**} command.
- Ensure that the controller is set to the current time. If the controller is set to a time that has already occurred, the access point might not join the controller because its certificate may not be valid for that time.
- Access points must be discovered by a controller before they can become an active part of the network. The lightweight access points support these controller discovery processes:
  - Layer 3 CAPWAP or LWAPP discovery—This feature can be enabled on different subnets from the access point and uses IP addresses and UDP packets rather the MAC addresses used by Layer 2 discovery.
  - Locally stored controller IP address discovery—If the access point was previously associated to a controller, the IP addresses of the primary, secondary, and tertiary controllers are stored in the access point's nonvolatile memory. This process of storing controller IP addresses on an access point for later deployment is called *priming the access point*.
  - DHCP server discovery—This feature uses DHCP option 43 to provide controller IP addresses to the access points. Cisco switches support a DHCP server option that is typically used for this capability. For more information about DHCP option 43, see the "Using DHCP Option 43 and DHCP Option 60" section on page 9-36.
  - DNS discovery—The access point can discover controllers through your domain name server (DNS). You must configure your DNS to return controller IP addresses in response to CISCO-LWAPP-CONTROLLER.*localdomain* or CISCO-CAPWAP-CONTROLLER.*localdomain*, where *localdomain* is the access point domain name. When an access point receives an IP address and DNS information from a DHCP server, it contacts the DNS to resolve CISCO-LWAPP-CONTROLLER.*localdomain* or CISCO-CAPWAP-CONTROLLER.*localdomain*. When the DNS sends a list of controller IP addresses, the access point sends discovery requests to the controllers.

Verifying that Access Points Join the Controller

When replacing a controller, ensure that access points join the new controller.

This section contains the following topics:

- Verifying that Access Points Join the Controller (GUI), page 9-9
- Verifying that Access Points Join the Controller (CLI), page 9-9

Verifying that Access Points Join the Controller (GUI)

Step 1 Configure the new controller as a primary controller as follows:

a. Choose **Controller > Advanced > Master Controller Mode** to open the Master Controller Configuration page.

b. Select the **Master Controller Mode** check box.

c. Click **Apply** to commit your changes.

d. Click **Save Configuration** to save your changes.

Step 2 (Optional) Flush the ARP and MAC address tables within the network infrastructure.

Step 3 Restart the access points.

Step 4 Once all the access points have joined the new controller, configure the controller not to be a primary controller by unselecting the **Master Controller Mode** check box on the Master Controller Configuration page.

Verifying that Access Points Join the Controller (CLI)

Step 1 Configure the new controller as a primary controller by entering this command:

config network master-base enable

Step 2 (Optional) Flush the ARP and MAC address tables within the network infrastructure.

Step 3 Restart the access points.

Step 4 Configure the controller not to be a primary controller once all the access points have joined the new controller by entering this command:

config network master-base disable

Searching for Access Points

This section contains the following topics:

- Information About Searching for Access Points, page 9-9
- Filtering the AP Search (GUI), page 9-10
- Monitoring the Interface Details (GUI), page 9-12

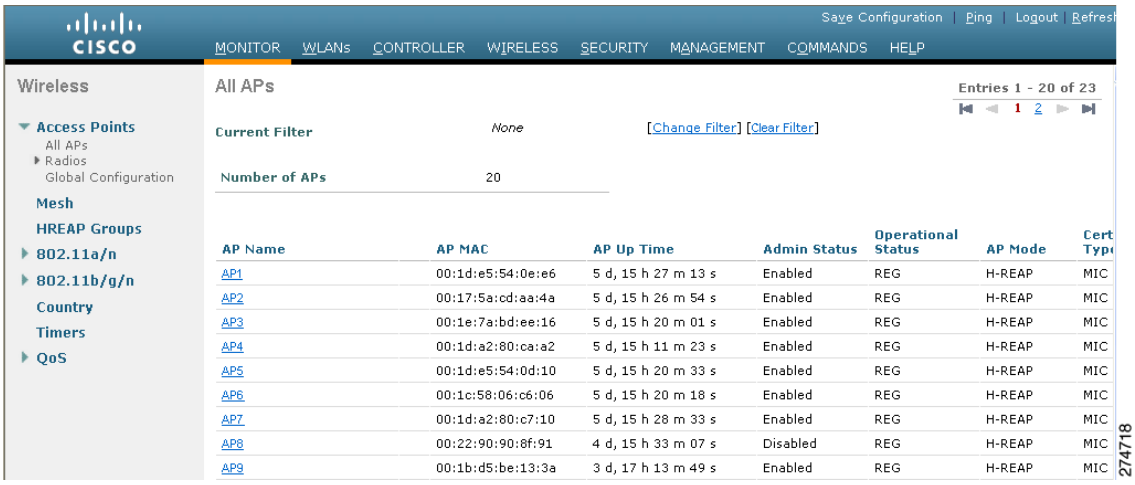
Information About Searching for Access Points

You can search for specific access points in the list of access points on the All APs page. To do so, you create a filter to display only access points that meet certain criteria (such as MAC address, status, access point mode, and certificate type). This feature is especially useful if your list of access points spans multiple pages, preventing you from viewing them all at once.

Filtering the AP Search (GUI)

Step 1 Choose **Monitor > Access Point Summary> All APs > Details** to open the All APs page.

Figure 9-2 All APs Page



This page lists all of the access points joined to the controller. For each access point, you can see its name, MAC address, uptime, status, operating mode, certificates, OfficeExtend access point status, and access point submode.

The total number of access points appears in the upper right-hand corner of the page. If the list of access points spans multiple pages, you can access these pages by clicking the page number links. Each page shows up to 20 access points.

Step 2 Click **Change Filter** to open the Search AP dialog box.

Step 3 Select one or more of the following check boxes to specify the criteria used when displaying access points:

- **MAC Address**—Enter the MAC address of an access point.

  Note When you enable the MAC Address filter, the other filters are disabled automatically. When you enable any of the other filters, the MAC Address filter is disabled automatically.

- **AP Name**—Enter the name of an access point.
- **AP Model**—Enter the model name of an access point.
- **Operating Status**—Select one or more of the following check boxes to specify the operating status of the access points:
  - **UP**—The access point is up and running.
  - **DOWN**—The access point is not operational.
  - **REG**—The access point is registered to the controller.
  - **DEREG**—The access point is not registered to the controller.
  - **DOWNLOAD**—The controller is downloading its software image to the access point.
- **Port Number**—Enter the controller port number to which the access point is connected.

- **Admin Status**—Choose **Enabled** or **Disabled** to specify whether the access points are enabled or disabled on the controller.
- **AP Mode**—Select one or more of the following options to specify the operating mode of the access points:
  - **Local—The default option.**

Note The 600 OEAP series access point uses only local mode.

When an access point in local mode connects to a Cisco Flex 7500 Series Controller, it does not serve clients. The access point details are available in the controller. To enable an access point to serve clients or perform monitoring-related tasks when connected to the Cisco Flex 7500 Series Controller, the access point mode must be in FlexConnect or monitor mode. Use the following command to automatically convert access points to a FlexConnect mode or monitor mode on joining the controller:

config ap autoconvert {**flexconnect** | **monitor** | **disable**}

All access points that connect to the controller will either be converted to FlexConnect mode or monitor mode depending on the configuration provided.

  - **FlexConnect**—This mode is used for 1040, 1130, 1140, 1240, 1250, 1260, 3500, 3600, and 800 access points.
  - **REAP**—This mode is the remote edge lightweight access point.
  - **Monitor**—This mode is the monitor-only mode.
  - **Rogue Detector**—This mode monitors the rogue APs on wire. It does not transmit or receive frames over the air or contain rogue APs.

Note Information about rogues that are detected is not shared between controllers. Therefore, we recommend that every controller has its own connected rogue detector AP when rogue detector APs are used.

  - **Sniffer**—The access point starts sniffing the air on a given channel. It captures and forwards all the packets from the clients on that channel to a remote machine that runs Airopeek or Wireshark (packet analyzers for IEEE 802.11 wireless LANs). It includes information on the time stamp, signal strength, packet size, and so on.

Note The Bridge option is displayed only if the AP is bridge capable.

Note If the AP mode is set to “Bridge” and the AP is not REAP capable, an error appears.

  - **Bridge**—This mode sets the AP mode to “Bridge” if you are connecting a Root AP.
  - **SE-Connect**—This mode allows you to connect to spectrum expert and it allows the access point to perform spectrum intelligence.

Note The AP3500 and the AP3600 support the spectrum intelligence and AP1260 does not support the spectrum intelligence.

Note When an access point is configured in SE-Connect mode, the access point reboots and rejoins the controller. Access points that are configured in this mode do not serve the client.

- **Certificate Type**—Select one or more of the following check boxes to specify the types of certificates installed on the access points:
  - **MIC**—Manufactured-installed certificate
  - **SSC**—Self-signed certificate
  - **LSC**—Local significant certificate

Note See the "Authorizing Access Points" section on page 9-30 for more information about these certificate types.

- **Primary S/W Version**—Select this check box to enter the primary software version number
- **Backup S/W Version**—Select this check box to enter the secondary software version number.

Step 4 Click **Apply** to commit your changes. Only the access points that match your search criteria appear on the All APs page, and the Current Filter parameter at the top of the page specifies the filter used to generate the list (for example, MAC Address:00:1d:e5:54:0e:e6, AP Name:pmsk-ap, Operational Status: UP, Status: Enabled, and so on).

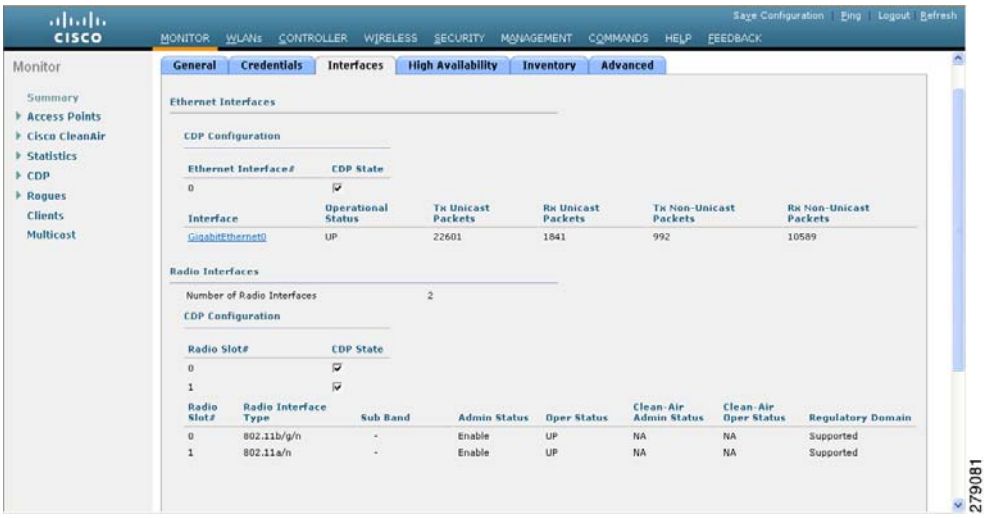
Note If you want to remove the filters and display the entire access point list, click **Clear Filter**.

Monitoring the Interface Details (GUI)

Step 1 Choose **Monitor** > **Summary** > **All APs**. The All APs > Details page appears.

Step 2 Click the **Interfaces** tab.

Figure 9-3 Interfaces Tab



Step 3 Click on the available Interface name. The Interface Details page appears.

Step 4 The Interface Details page displays the following parameter details.

Table 9-1 Interfaces Parameters Details

Button	Description
AP Name	Name of the access point.
Link Speed	Speed of the interference in Mbps.
RX Bytes	Total number of bytes in the error-free packets received on the interface.
RX Unicast Packets	Total number of unicast packets received on the interface.
RX Non-Unicast Packets	Total number of nonunicast or multicast packets received on the interface.
Input CRC	Total number of CRC error in packets while receiving on the interface.
Input Errors	Sum of all errors in the packets while receiving on the interface.
Input Overrun	Number of times the receiver hardware was incapable of handling received data to a hardware buffer because the input rate exceeded the receiver's capability to handle that data.
Input Resource	Total number of resource errors in packets received on the interface.
Runts	Number of packets that are discarded because they are similar to the medium's minimum packet size.
Throttle	Total number of times the interface advised a sending NIC that it was overwhelmed by packets being sent and to slow the pace of delivery.
Output Collision	Total number of packet retransmitted due to an Ethernet collision.
Output Resource	Resource errors in packets transmitted on the interface.
Output Errors	Errors that prevented the final transmission of packets out of the interface.
Operational Status	Operational state of the physical ethernet interface on the AP.
Duplex	Interface's duplex mode.
TX Bytes	Number of bytes in the error-free packets transmitted on the interface.

Table 9-1 Interfaces Parameters Details (continued)

Button	Description
TX Unicast Packets	Total number of unicast packets transmitted on the interface.
TX Non-Unicast Packets	Total number of nonunicast or multicast packets transmitted on the interface.
Input Aborts	Total number of packets terminated while receiving on the interface.
Input Frames	Total number of packets received incorrectly that has a CRC error and a noninteger number of octets on the interface.
Input Drops	Total number of packets dropped while receiving on the interface because the queue was full.
Unknown Protocol	Total number of packets discarded on the interface due to an unknown protocol.
Giants	Number of packets that are discarded because they exceeded the medium's maximum packet size.
Interface Resets	Number of times that an interface has been completely reset.
Output No Buffer	Total number of packets discarded because there was no buffer space.
Output Underrun	Number of times the transmitter has been running faster than the router can handle.
Outout Total Drops	Total number of packets dropped while transmitting from the interface because the queue was full.

Searching for Access Point Radios

This section contains the following topics:

- Information About Searching for Access Point Radios, page 9-14
- Searching for Access Point Radios (GUI), page 9-14

Information About Searching for Access Point Radios

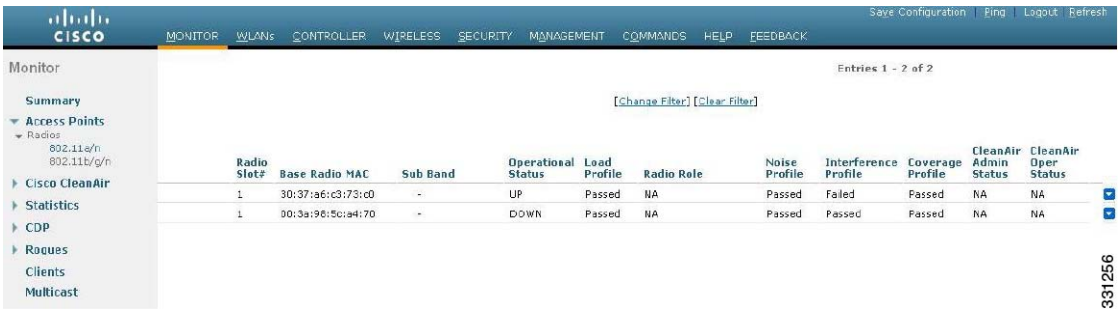
You can search for specific access point radios in the list of radios on the 802.11a/n Radios page or the 802.11b/g/n Radios page. You can access these pages from the Monitor tab on the menu bar when viewing access point radios or from the Wireless tab on the menu bar when configuring access point radios. To search for specific access point radios, you create a filter to display only radios that meet certain criteria (such as radio MAC address, access point name, or CleanAir status). This feature is especially useful if your list of access point radios spans multiple pages, which prevents you from viewing them all at once.

Searching for Access Point Radios (GUI)

Step 1 Perform either of the following:

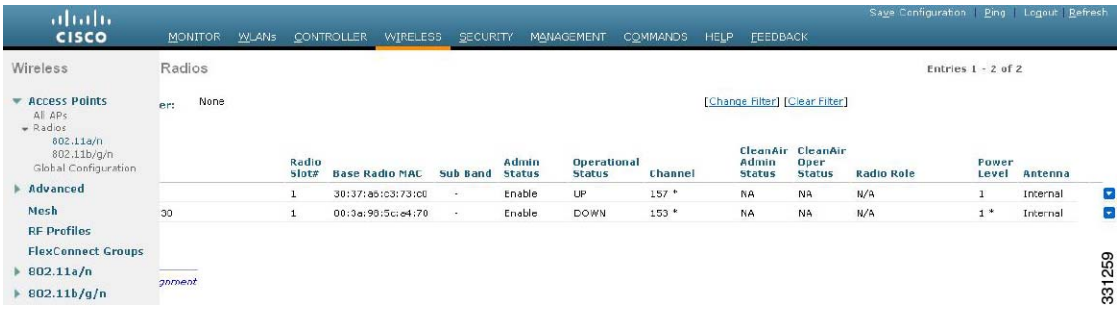
- Choose **Monitor > Access Points Summary> 802.11a/n** (or **802.11b/g/n**) **Radios > Details** to open the 802.11a/n (or 802.11b/g/n) Radios page.

Figure 9-4 802.11a/n Radios Page (from the Monitor Tab)



- Choose **Wireless > Access Points > Radios > 802.11a/n** (or **802.11b/g/n**) to open the 802.11a/n (or 802.11b/g/n) Radios page.

Figure 9-5 802.11a/n Radios Page (from the Wireless Tab)



These pages show all of the 802.11a/n or 802.11b/g/n access point radios that are joined to the controller and their current settings.

The total number of access point radios appears in the upper right-hand corner of the page. If the list of radios spans multiple pages, you can access these pages by clicking the page number links. Each page shows up to 25 access point radios.

Note In a Cisco Unified Wireless Network environment, the 802.11a and 802.11b/g radios should not be differentiated based on their Base Radio MAC addresses, as they may have the same addresses. Instead, the radios should be differentiated based on their physical addresses.

Step 2 Click **Change Filter** to open the Search AP dialog box.

Step 3 Select one of the following check boxes to specify the criteria used when displaying access point radios:

- **MAC Address**—Base radio MAC address of an access point radio.

  Note When you enable the MAC address filter, the other filters are disabled automatically. When you enable any of the other filters, the MAC address filter is disabled automatically.

- **AP Name**—Access point name. If you do not know the exact name of the AP, you can specify the name partially by entering one or more successive characters that are part of the AP name.
- **AP Model**—Access point model check box where you select and enter the model of the access point.
- **Operating Status**—Operating status of the access points:

  - UP—The access point is up and running.
  - DOWN—The access point is not operational.
  - REG—The access point is registered to the controller.
  - DEREG—The access point is not registered to the controller.
  - DOWNLOAD—The controller is downloading its software image to the access point.
- **Admin Status**—Whether the access points are enabled or disabled on the controller.
- **AP Mode**—Options to specify the operating mode of the access points: Local, FlexConnect, REAP, Monitor, Rogue Detector, Sniffer, Bridge, and SE Connect. Depending on the capabilities and support available for the APs, one or more options are displayed.

Note The Cisco OEAP 600 Series access point uses Local mode and the settings cannot be altered. The Cisco OEAP 600 Series access point does not support the following AP Modes: Monitor, FlexConnect, Sniffer, Rogue Detector, Bridge, and SE Connect.

Note To configure an access point for wIPS, you must set the AP mode to one of the following from the AP Mode drop-down list: Local, FlexConnect, and Monitor.

- **Certificate Type**—Check boxes that you can select to specify the types of certificates installed on the access points:
  - MIC—Manufactured-installed certificate
  - SSC—Self-signed certificate
  - LSC—Local significant certificate
- **Primary S/W Version**—Primary controller software version.
- **Secondary S/W Version**—Secondary controller software version.

Step 4 Click **Find** to commit your changes. Only the access point radios that match your search criteria appear on the 802.11a/n Radios page or the 802.11b/g/n Radios page, and the Current Filter parameter at the top of the page specifies the filter used to generate the list (for example, MAC Address:00:1e:f7:75:0a:a0 or AP Name:pmsk-ap).

Note If you want to remove the filter and display the entire access point radio list, click **Clear Filter**.

Configuring Global Credentials for Access Points

This section contains the following topics:

- Information About Configuring Global Credentials for Access Points, page 9-17
- Guidelines and Limitations, page 9-17
- Configuring Global Credentials for Access Points, page 9-17

Information About Configuring Global Credentials for Access Points

Cisco IOS access points are shipped from the factory with *Cisco* as the default enable password. This password allows users to log into the nonprivileged mode and execute **show** and **debug** commands, posing a security threat. The default enable password must be changed to prevent unauthorized access and to enable users to execute configuration commands from the access point's console port.

Guidelines and Limitations

- In controller software releases prior to 5.0, you can set the access point enable password only for access points that are currently connected to the controller. In controller software release 5.0 or later releases, you can set a global username, password, and enable password that all access points that are currently joined to the controller and any that join in the future inherit as they join the controller. If desired, you can override the global credentials and assign a unique username, password, and enable password for a specific access point.
- Also in controller software release 5.0 or later releases, after an access point joins the controller, the access point enables console port security, and you are prompted for your username and password whenever you log into the access point's console port. When you log in, you are in nonprivileged mode, and you must enter the enable password in order to use the privileged mode.
- These controller software release 5.0 or later release features are supported on all access points that have been converted to lightweight mode, except the 1100 series. VxWorks access points are not supported.
- The global credentials that you configure on the controller are retained across controller and access point reboots. They are overwritten only if the access point joins a new controller that is configured with a global username and password. If the new controller is not configured with global credentials, the access point retains the global username and password configured for the first controller.
- The controller name in the AP configuration is case sensitive. Therefore, make sure to configure the exact system name on the AP configuration. Failure to do this results in the AP fallback not working.
- You need to keep careful track of the credentials used by the access points. Otherwise, you might not be able to log into an access point's console port. if you need to return the access points to the default *Cisco*/*Cisco* username and password, you must clear the controller's configuration and the access point's configuration to return them to factory-default settings. To clear the controller's configuration, choose **Commands > Reset to Factory Default > Reset** on the controller GUI, or enter the **clear config** command on the controller CLI. To clear the access point's configuration, enter the **clear ap config** *Cisco_AP* command on the controller CLI. Entering the command does not clear the static IP address of the access point. Once the access point rejoins a controller, it adopts the default *Cisco*/*Cisco* username and password.

Configuring Global Credentials for Access Points

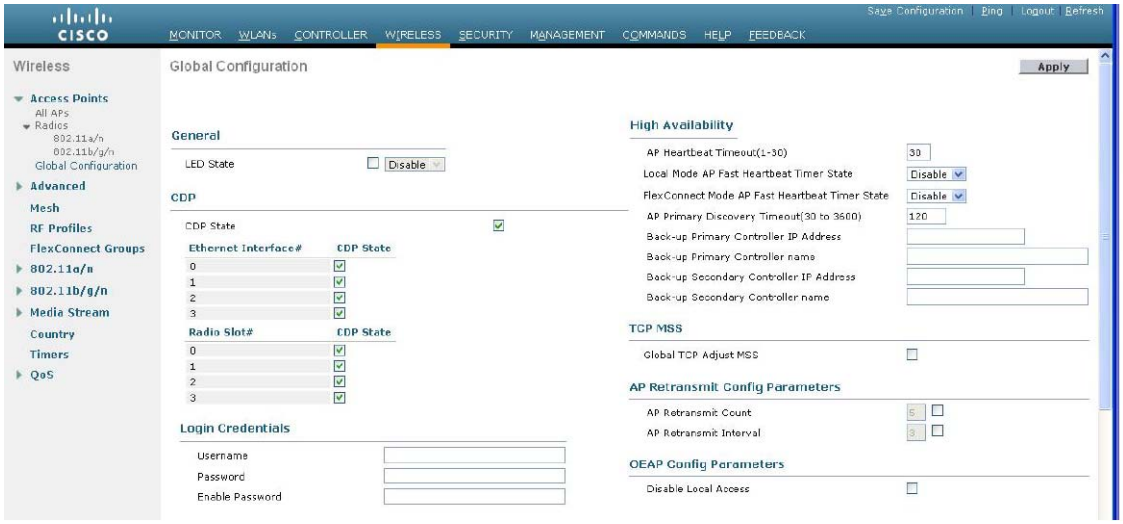
This section contains the following topics:

- Configuring Global Credentials for Access Points (GUI), page 9-18
- Configuring Global Credentials for Access Points (CLI), page 9-19

Configuring Global Credentials for Access Points (GUI)

Step 1 Choose **Wireless > Access Points > Global Configuration** to open the Global Configuration page.

Figure 9-6 Global Configuration Page



Step 2 In the Username text box, enter the username that is to be inherited by all access points that join the controller.

Step 3 In the Password text box, enter the password that is to be inherited by all access points that join the controller.

You can set a global username, password, and enable password that all access points inherit as they join the controller including access points that are currently joined to the controller and any that join in the future. You can override the global credentials and assign a unique username, password, and enable password for a specific access point. The following are requirements enforced on the password:

- The password should contain characters from at least three of the following classes: lowercase letters, uppercase letters, digits, and special characters.
- No character in the password can be repeated more than three times consecutively.
- The password should not contain the management username or the reverse of the username.
- The password should not contain words like Cisco, oscic, admin, nimda or any variant obtained by changing the capitalization of letters by substituting 1, |, or ! or substituting 0 for o or substituting $ for s.

Step 4 In the Enable Password text box, enter the enable password that is to be inherited by all access points that join the controller.

Step 5 Click **Apply** to send the global username, password, and enable password to all access points that are currently joined to the controller or that join the controller in the future.

Step 6 Click **Save Configuration** to save your changes.

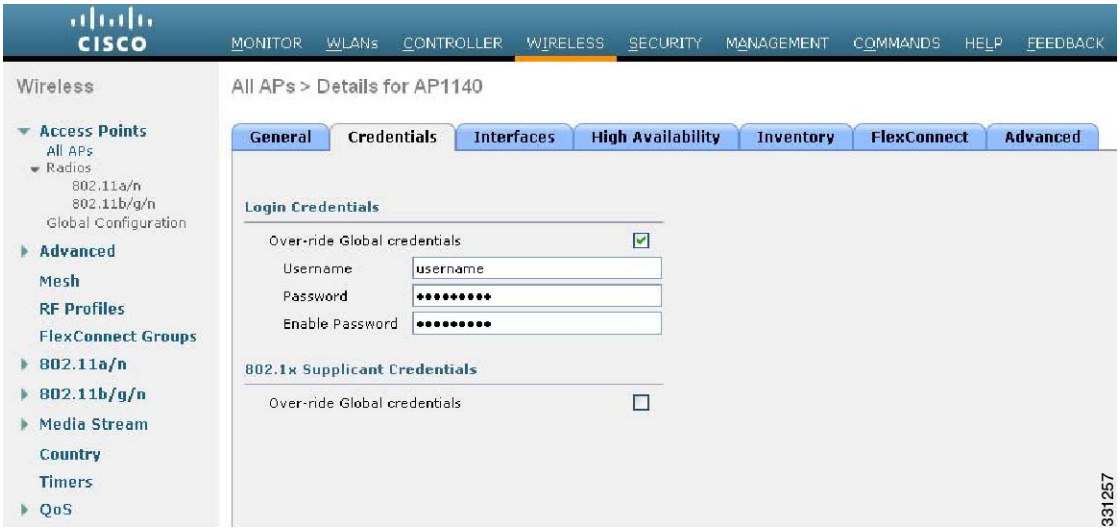
Step 7 (Optional) Override the global credentials for a specific access point and assign a unique username, password, and enable password to this access point as follows:

a. Choose **Access Points > All APs** to open the All APs page.

b. Click the name of the access point for which you want to override the global credentials.

c. Choose the **Credentials** tab. The All APs > Details for (Credentials) page appears.

Figure 9-7 All APs > Details for (Credentials) Page



d. Select the **Over-ride Global Credentials** check box to prevent this access point from inheriting the global username, password, and enable password from the controller. The default value is unselected.

e. In the Username, Password, and Enable Password text boxes, enter the unique username, password, and enable password that you want to assign to this access point.

Note The information that you enter is retained across controller and access point reboots and if the access point joins a new controller.

f. Click **Apply** to commit your changes.

g. Click **Save Configuration** to save your changes.

Note If you want to force this access point to use the controller's global credentials, unselect the **Over-ride Global Credentials** check box.

Configuring Global Credentials for Access Points (CLI)

Step 1 Configure the global username, password, and enable password for all access points currently joined to the controller as well as any access points that join the controller in the future by entering this command:

config ap mgmtuser add username *user* **password** *password* **enablesecret** *enable_password* **all**

Step 2 (Optional) Override the global credentials for a specific access point and assign a unique username, password, and enable password to this access point by entering this command:

config ap mgmtuser add username *user* **password** *password* **enablesecret** *enable_password Cisco_AP*

The credentials that you enter in this command are retained across controller and access point reboots and if the access point joins a new controller.

Note If you want to force this access point to use the controller's global credentials, enter the **config ap mgmtuser delete** *Cisco_AP* command. The following message appears after you execute this command: "AP reverted to global username configuration."

Step 3 Enter the **save config** command to save your changes.

Step 4 Verify that global credentials are configured for all access points that join the controller by entering this command:

show ap summary

Information similar to the following appears:

```
Number of APs.................................. 1
Global AP User Name............................ globalap

AP Name  Slots  AP Model           Ethernet MAC       Location         Port  Country
-------- ------ ------------------ ------------------ ------------------ ----  -------
FlexConnect   2  AIR-AP1131AG-N-K9 00:13:80:60:48:3e  default location  1     US
```

Note If global credentials are not configured, the Global AP User Name text box shows "Not Configured."

To view summary of specific access point you can specify the access point name. You can also use wildcard searches when filtering for access points.

Step 5 See the global credentials configuration for a specific access point by entering this command:

show ap config general *Cisco_AP*

Note The name of the access point is case sensitive.

Information similar to the following appears:

```
Cisco AP Identifier.............................. 0
Cisco AP Name.................................. FlexConnect
...
AP User Mode.................................... AUTOMATIC
AP User Name.................................... globalap
```

Note If this access point is configured for global credentials, the AP User Mode text boxes shows "Automatic." If the global credentials have been overwritten for this access point, the AP User Mode text box shows "Customized."

Configuring Authentication for Access Points

This section contains the following topics:

- Information About Configuring Authentication for Access Points, page 9-21
- Guidelines and Limitations, page 9-21
- Prerequisites for Configuring Authentication for Access Points, page 9-21
- Configuring Authentication for Access Points, page 9-22
- Configuring the Switch for Authentication, page 9-26

Information About Configuring Authentication for Access Points

You can configure 802.1X authentication between a lightweight access point and a Cisco switch. The access point acts as an 802.1X supplicant and is authenticated by the switch using EAP-FAST with anonymous PAC provisioning.

Guidelines and Limitations

- This feature is supported on the following hardware:
  - Cisco Aironet 1040, 1130, 1140, 1240, 1250, 1260, 3500, and 3600 series access points.
  - All controller platforms running in local, flexconnect, monitor, or sniffer mode. Bridge mode is not supported.

Note In flexconnect mode, you can configure local switching with 802.1X authentication if you have configured a local external RADIUS server configured.

  - All Cisco switches that support authentication.

Note See the *Release Notes for Cisco wireless LAN controllers and Lightweight Access Points for Release 7.0.155.0* for a list of supported switch hardware and minimum supported software.

- The OEAP 600 Series access points do not support LEAP.
- You can configure global authentication settings that all access points that are currently joined to the controller and any that join in the future. If desired, you can override the global authentication settings and assign unique authentication settings for a specific access point.

Prerequisites for Configuring Authentication for Access Points

Step 1 If the access point is new, do the following:

a. Boot the access point with the installed recovery image.

b. If you choose not to follow this suggested flow and instead enable 802.1X authentication on the switch port connected to the access point prior to the access point joining the controller, enter this command:

lwapp ap dot1x username *username* **password** *password*

Note If you choose to follow this suggested flow and enable 802.1X authentication on the switch port after the access point has joined the controller and received the configured 802.1X credentials, you do not need to enter this command.

Note This command is available only for access points that are running the 5.1, 5.2, 6.0, or 7.0 recovery image.

c. Connect the access point to the switch port.

Step 2 Install the 5.1, 5.2, 6.0, or 7.0 image on the controller and reboot the controller.

Step 3 Allow all access points to join the controller.

Step 4 Configure authentication on the controller. See the "Configuring Authentication for Access Points (GUI)" section on page 9-22 or the "Configuring Authentication for Access Points (CLI)" section on page 9-24 for information on configuring authentication on the controller.

Step 5 Configure the switch to allow authentication. See the "Configuring the Switch for Authentication" section on page 9-26 for information on configuring the switch for authentication.

Configuring Authentication for Access Points

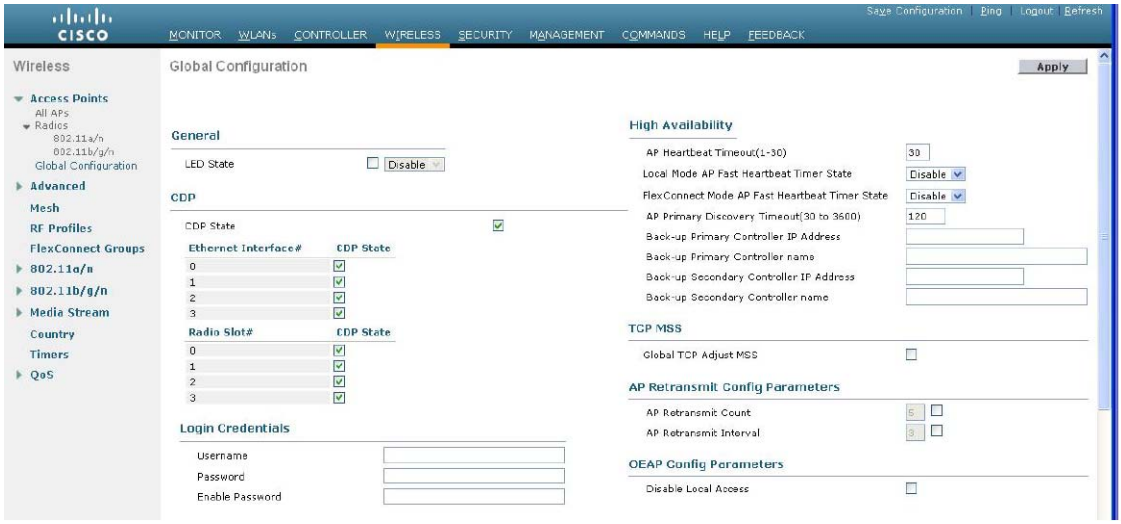
This section contains the following topics:

- Configuring Authentication for Access Points (GUI), page 9-22
- Configuring Authentication for Access Points (CLI), page 9-24

Configuring Authentication for Access Points (GUI)

Step 1 Choose **Wireless** > **Access Points** > **Global Configuration** to open the Global Configuration page.

Figure 9-8 Global Configuration Page



Step 2 Under 802.1x Supplicant Credentials, select the **802.1x Authentication** check box.

Step 3 In the Username text box, enter the username that is to be inherited by all access points that join the controller.

Step 4 In the Password and Confirm Password text boxes, enter the password that is to be inherited by all access points that join the controller.

Note You must enter a strong password in these text boxes. Strong passwords have the following characteristics:
- They are at least eight characters long.
- They contain a combination of uppercase and lowercase letters, numbers, and symbols.
- They are not a word in any language.

Step 5 Click **Apply** to send the global authentication username and password to all access points that are currently joined to the controller and to any that join the controller in the future.

Step 6 Click **Save Configuration** to save your changes.

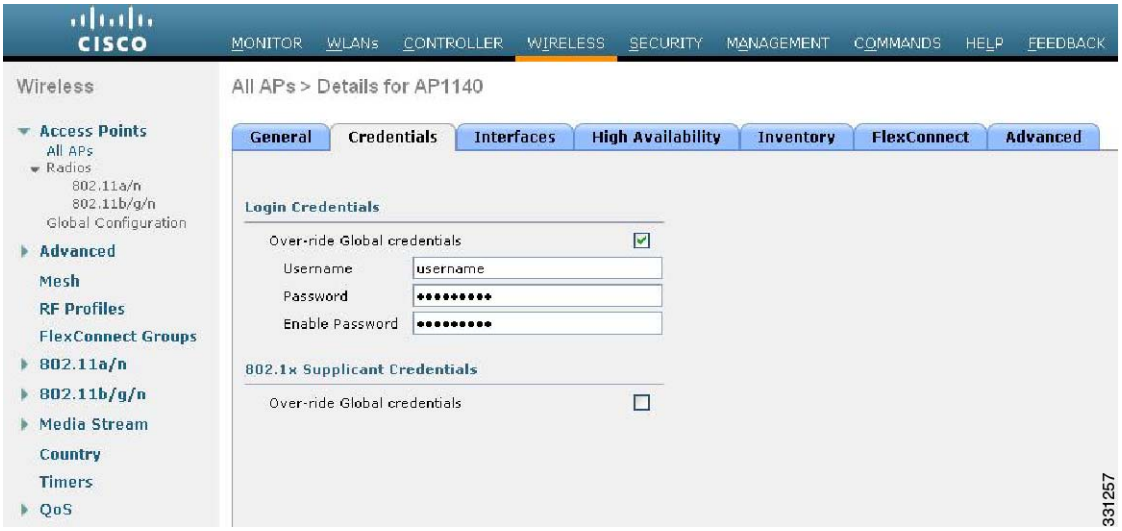
Step 7 If desired, you can choose to override the global authentication settings and assign a unique username and password to a specific access point as follows:

a. Choose **Access Points > All APs** to open the All APs page.

b. Click the name of the access point for which you want to override the authentication settings.

c. Choose the **Credentials** tab to open the All APs > Details for (Credentials) page.

Figure 9-9 All APs > Details for (Credentials) Page



d. Under 802.1x Supplicant Credentials, select the **Over-ride Global Credentials** check box to prevent this access point from inheriting the global authentication username and password from the controller. The default value is unselected.

e. In the Username, Password, and Confirm Password text boxes, enter the unique username and password that you want to assign to this access point.

Note The information that you enter is retained across controller and access point reboots and whenever the access point joins a new controller.

f. Click **Apply** to commit your changes.

g. Click **Save Configuration** to save your changes.

Note If you want to force this access point to use the controller's global authentication settings, unselect the **Over-ride Global Credentials** check box.

Configuring Authentication for Access Points (CLI)

Step 1 Configure the global authentication username and password for all access points currently joined to the controller as well as any access points that join the controller in the future by entering this command:

config ap dot1xuser add username *user* **password** *password* **all**

Note You must enter a strong password for the *password* parameter. Strong passwords have the following characteristics:
- They are at least eight characters long.
- They contain a combination of uppercase and lowercase letters, numbers, and symbols.
- They are not a word in any language.

Step 2 (Optional) Override the global authentication settings and assign a unique username and password to a specific access point. To do so, enter this command:

config ap dot1xuser add username *user* **password** *password Cisco_AP*

Note You must enter a strong password for the *password* parameter. See the note in Step 1 for the characteristics of strong passwords.

The authentication settings that you enter in this command are retained across controller and access point reboots and whenever the access point joins a new controller.

Note If you want to force this access point to use the controller's global authentication settings, enter the **config ap dot1xuser delete** *Cisco_AP* command. The following message appears after you execute this command: "AP reverted to global username configuration."

Step 3 Save your changes by entering this command:

save config

Step 4 (Optional) Disable 802.1X authentication for all access points or for a specific access point by entering this command:

config ap dot1xuser disable {**all** | *Cisco_AP*}

Note You can disable 802.1X authentication for a specific access point only if global 802.1X authentication is not enabled. If global 802.1X authentication is enabled, you can disable 802.1X for all access points only.

Step 5 See the authentication settings for all access points that join the controller by entering this command:

show ap summary

Information similar to the following appears:

```
Number of APs.................................. 1
Global AP User Name............................ globalap
Global AP Dot1x User Name...................... globalDot1x
```

Note If global authentication settings are not configured, the Global AP Dot1x User Name text box shows "Not Configured."

To See summary of specific access point you can specify the access point name. You can also use wildcard searches when filtering for access points.

Step 6 See the authentication settings for a specific access point by entering this command:

show ap config general *Cisco_AP*

Note The name of the access point is case sensitive.

Information similar to the following appears:

```
Cisco AP Identifier.............................. 0
Cisco AP Name.................................... FlexConnect
...
```

```
AP Dot1x User Mode.............................. AUTOMATIC
AP Dot1x User Name.............................. globalDot1x
...
```

Note If this access point is configured for global authentication, the AP Dot1x User Mode text boxes shows "Automatic." If the global authentication settings have been overwritten for this access point, the AP Dot1x User Mode text box shows "Customized."

Configuring the Switch for Authentication

To enable 802.1X authentication on a switch port, on the switch CLI, enter these commands:

- Switch# **configure terminal**
- Switch(config)# **dot1x system-auth-control**
- Switch(config)# **aaa new-model**
- Switch(config)# **aaa authentication dot1x default group radius**
- Switch(config)# **radius-server host** *ip_addr* **auth-port** *port* **acct-port** *port* **key** *key*
- Switch(config)# **interface fastethernet2/1**
- Switch(config-if)# **switchport mode access**
- Switch(config-if)# **dot1x pae authenticator**
- Switch(config-if)# **dot1x port-control auto**
- Switch(config-if)# **end**

Configuring Embedded Access Points

This section contains the following topics:

- Information About Embedded Access Points, page 9-26
- Guidelines and Limitations, page 9-27
- Additional References, page 9-28

Information About Embedded Access Points

Controller software release 7.0.116.0 or later releases support the embedded access points: AP801 and AP802, which are the integrated access points on the Cisco 880 Series Integrated Services Routers (ISRs). This access points use a Cisco IOS software image that is separate from the router Cisco IOS software image. The access points can operate as autonomous access points configured and managed locally, or they can operate as centrally managed access points that utilize the CAPWAP or LWAPP protocol. The AP801 and AP802 access points are preloaded with both an autonomous Cisco IOS release and a recovery image for the unified mode.

Guidelines and Limitations

- Before you use an AP801 or AP802 Series Lightweight Access Point with controller software release 7.0.116.0 or later releases, you must upgrade the software in the Next Generation Cisco 880 Series Integrated Services Routers (ISRs) to Cisco IOS 151-4.M or later.
- When you want to use the AP801 or AP802 with a controller, you must enable the recovery image for the unified mode on the access point by entering the **service-module wlan-ap 0 bootimage unified** command on the router in privileged EXEC mode.
- If the **service-module wlan-ap 0 bootimage unified** command does not work successfully, make sure that the software license is still eligible.
- After enabling the recovery image, enter the **service-module wlan-ap 0 reload** command on the router to shut down and reboot the access point. After the access point reboots, it discovers the controller, downloads the full CAPWAP or LWAPP software release from the controller, and acts as a lightweight access point.
- To use the CLI commands mentioned above, the router must be running Cisco IOS Release 12.4(20)T or later releases. If you experience any issues, See the "Troubleshooting an Upgrade or Reverting the AP to Autonomous Mode" section in the ISR configuration guide at: http://www.cisco.com/c/en/us/td/docs/routers/access/800/software/configuration/guide/SCG800Guide/SCG800_Guide_BookMap_chapter_01001.html
- To support CAPWAP or LWAPP, the router must be activated with at least the Cisco Advanced IP Services IOS license-grade image. A license is required to upgrade to this Cisco IOS image on the router. For licensing information, see http://www.cisco.com/en/US/docs/routers/access/sw_activation/SA_on_ISR.html
- After the AP801 or AP802 boots up with the recovery image for the unified mode, it requires an IP address to communicate with the controller and to download its unified image and configuration from the controller. The router can provide DHCP server functionality, the DHCP pool to reach the controller, and setup option 43 for the controller IP address in the DHCP pool configuration. Use the following configuration to perform this task:

  ip dhcp pool *pool_name*

  network *ip_address subnet_mask*

  dns-server *ip_address*

  default-router *ip_address*

  option 43 hex *controller_ip_address_in_hex*

  Example:

```
ip dhcp pool embedded-ap-pool
    network 60.0.0.0 255.255.255.0
   dns-server 171.70.168.183
   default-router 60.0.0.1
   option 43 hex  f104.0a0a.0a0f   /* single WLC IP address(10.10.10.15) in hex format
*/
```

- The AP801 and AP802 802.11n radio supports lower power levels than the 802.11n radio in the Cisco Aironet 1250 series access points. The AP801 and AP802 access points store the radio power levels and passes them to the controller when the access point joins the controller. The controller uses the supplied values to limit the user's configuration.

  The AP801 and AP802 access points can be used in flexconnect mode.

Additional References

- For more information about FlexConnect, see Chapter 16, "Configuring FlexConnect."
- For more information about the AP801, see the documentation for the Cisco 800 Series ISRs at this URL: http://www.cisco.com/en/US/products/hw/routers/ps380/tsd_products_support_series_home.html.
- For more information about the AP802, see the documentation for the Next generation Cisco 880 Series ISRs at this URL: http://www.cisco.com/en/US/docs/routers/access/800/860-880-890/software/configuration/guide/SCG_880_series.pdf

Converting Autonomous Access Points to Lightweight Mode

This section contains the following topics:

- Information About Autonomous Access Points Converted to Lightweight Mode, page 9-28
- Guidelines and Limitations, page 9-29
- Reverting from Lightweight Mode to Autonomous Mode, page 9-29
- Authorizing Access Points, page 9-30
- Using DHCP Option 43 and DHCP Option 60, page 9-36
- Troubleshooting the Access Point Join Process, page 9-37
- Sending Debug Commands to Access Points Converted to Lightweight Mode, page 9-42
- Understanding How Converted Access Points Send Crash Information to the Controller, page 9-43
- Understanding How Converted Access Points Send Radio Core Dumps to the Controller, page 9-43
- Uploading Memory Core Dumps from Converted Access Points, page 9-45
- Viewing the AP Crash Log Information, page 9-47
- Displaying MAC Addresses for Converted Access Points, page 9-48
- Disabling the Reset Button on Access Points Converted to Lightweight Mode, page 9-48
- Configuring a Static IP Address on a Lightweight Access Point, page 9-48
- Supporting Oversized Access Point Images, page 9-51

Information About Autonomous Access Points Converted to Lightweight Mode

You can use an upgrade conversion tool to convert autonomous Cisco Aironet 1100, 1130AG, 1200, 1240AG, 1260, and 1300 Series Access Points to lightweight mode. When you upgrade one of these access points to lightweight mode, the access point communicates with a controller and receives a configuration and software image from the controller.

See the *Upgrading Autonomous Cisco Aironet Access Points to Lightweight Mode* document for instructions on upgrading an autonomous access point to lightweight mode. You can find this document at this URL:

http://www.cisco.com/en/US/docs/wireless/access_point/conversion/lwapp/upgrade/guide/lwapnote.html

Guidelines and Limitations

- Access points converted to lightweight mode do not support Wireless Domain Services (WDS). Converted access points communicate only with Cisco wireless LAN controllers and cannot communicate with WDS devices. However, the controller provides functionality that is equivalent to WDS when the access point associates to it.
- In controller software release 4.2 or later releases, all Cisco lightweight access points support 16 BSSIDs per radio and a total of 16 wireless LANs per access point. In previous releases, they supported only 8 BSSIDs per radio and a total of 8 wireless LANs per access point. When a converted access point associates to a controller, only wireless LANs with IDs 1 through 16 are pushed to the access point.
- Access points converted to lightweight mode must get an IP address and discover the controller using DHCP, DNS, or IP subnet broadcast.
- After you convert an access point to lightweight mode, the console port provides read-only access to the unit.
- The 1130AG and 1240AG access points support flexconnect mode. For more information about FlexConnect, see Chapter 16, "Configuring FlexConnect."
- The upgrade conversion tool adds the self-signed certificate (SSC) key-hash to only one of the controllers on the Cisco WiSM. After the conversion has been completed, add the SSC key-hash to the second controller on the Cisco WiSM by copying the SSC key-hash from the first controller to the second controller. To copy the SSC key-hash, open the AP Policies page of the controller GUI (**Security > AAA > AP Policies**) and copy the SSC key-hash from the SHA1 Key Hash column under AP Authorization List (see Figure 9-11). Then, using the second controller's GUI, open the same page and paste the key-hash into the SHA1 Key Hash text box under Add AP to Authorization List. If you have more than one Cisco WiSM, use WCS to push the SSC key-hash to all the other controllers.

Reverting from Lightweight Mode to Autonomous Mode

After you use the upgrade tool to convert an autonomous access point to lightweight mode, you can convert the access point from a lightweight unit back to an autonomous unit by loading a Cisco IOS release that supports autonomous mode (Cisco IOS Release 12.3(7)JA or earlier releases). If the access point is associated to a controller, you can use the controller to load the Cisco IOS release. If the access point is not associated to a controller, you can load the Cisco IOS release using TFTP. In either method, the access point must be able to access a TFTP server that contains the Cisco IOS release to be loaded.

This section contains the following topics:

- Reverting to a Previous Release (CLI), page 9-29
- Reverting to a Previous Release (Using the MODE Button and a TFTP Server), page 9-30

Reverting to a Previous Release (CLI)

Step 1 Log on to the CLI on the controller to which the access point is associated.

Step 2 Revert from lightweight mode, by entering this command:

config ap tftp-downgrade *tftp-server-ip-address filename access-point-name*

Step 3 Wait until the access point reboots and reconfigure the access point using the CLI or GUI.

Reverting to a Previous Release (Using the MODE Button and a TFTP Server)

Step 1 Configure the PC on which your TFTP server software runs with a static IP address in the range of 10.0.0.2 to 10.0.0.30.

Step 2 Make sure that the PC contains the access point image file (such as *c1200-k9w7-tar.123-7.JA.tar* for a 1200 series access point) in the TFTP server folder and that the TFTP server is activated.

Step 3 Rename the access point image file in the TFTP server folder to **c1200-k9w7-tar.default** for a 1200 series access point.

Step 4 Connect the PC to the access point using a Category 5 (CAT5) Ethernet cable.

Step 5 Disconnect power from the access point.

Step 6 Press and hold the **MODE** button while you reconnect power to the access point.

Note The MODE button on the access point must be enabled. Follow the steps in the "Disabling the Reset Button on Access Points Converted to Lightweight Mode" section on page 9-48 to select the status of the access point MODE button.

Step 7 Hold the **MODE** button until the status LED turns red (approximately 20 to 30 seconds), and release the MODE button.

Step 8 Wait until the access point reboots as indicated by all LEDs turning green followed by the Status LED blinking green.

Step 9 After the access point reboots, reconfigure the access point using the GUI or the CLI.

Authorizing Access Points

In controller software releases prior to 5.2, the controller may either use self-signed certificates (SSCs) to authenticate access points or send the authorization information to a RADIUS server (if access points have manufactured-installed certificates [MICs]). In controller software release 5.2 or later releases, you can configure the controller to use a local significant certificate (LSC).

This section contains the following topics:

- Authorizing Access Points Using SSCs, page 9-31
- Authorizing Access Points Using MICs, page 9-31
- Authorizing Access Points Using LSCs, page 9-31
- Authorizing Access Points (GUI), page 9-35
- Authorizing Access Points (CLI), page 9-36

Authorizing Access Points Using SSCs

The Control and Provisioning of Wireless Access Points protocol (CAPWAP) secures the control communication between the access point and controller by a secure key distribution requiring X.509 certificates on both the access point and controller. CAPWAP relies on provisioning of the X.509 certificates. Cisco Aironet access points shipped before July 18, 2005 do not have a MIC, so these access points create an SSC when upgraded to operate in lightweight mode. Controllers are programmed to accept local SSCs for authentication of specific access points and do not forward those authentication requests to a RADIUS server. This behavior is acceptable and secure.

Authorizing Access Points Using MICs

You can configure controllers to use RADIUS servers to authorize access points using MICs. The controller uses an access point's MAC address as both the username and password when sending the information to a RADIUS server. For example, if the MAC address of the access point is 000b85229a70, both the username and password used by the controller to authorize the access point are 000b85229a70.

Note The lack of a strong password by the use of the access point's MAC address should not be an issue because the controller uses MIC to authenticate the access point prior to authorizing the access point through the RADIUS server. Using MIC provides strong authentication.

Note If you use the MAC address as the username and password for access point authentication on a RADIUS AAA server, do not use the same AAA server for client authentication.

Authorizing Access Points Using LSCs

You can use an LSC if you want your own public key infrastructure (PKI) to provide better security, to have control of your certificate authority (CA), and to define policies, restrictions, and usages on the generated certificates.

The LSC CA certificate is installed on access points and controllers. You need to provision the device certificate on the access point. The access point gets a signed X.509 certificate by sending a certRequest to the controller. The controller acts as a CA proxy and receives the certRequest signed by the CA for the access point.

Note When the CA server is in manual mode and if there is an AP entry in the LSC SCEP table that is pending enrollment, the controller waits for the CA server to send a pending response. If there is no response from the CA server, the controller retries a total of three times to get a response, after which the fallback mode comes into effect where the AP provisioning times out and the AP reboots and comes up with MIC.

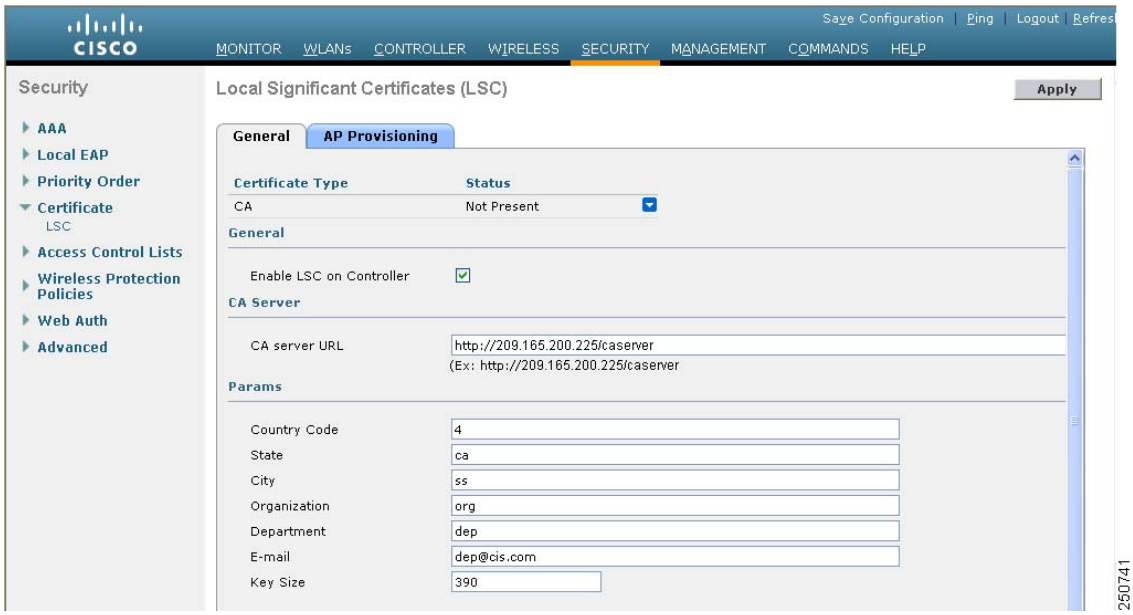
This section contains the following topics:

- Configuring LSC (GUI), page 9-31
- Configuring LSC (CLI), page 9-33

Configuring LSC (GUI)

Step 1 Choose **Security > Certificate > LSC** to open the Local Significant Certificates (LSC) - General page.

Figure 9-10 Local Significant Certificates (LSC) - General Page



Step 2 Select the **Enable LSC on Controller** check box to enable the LSC on the system.

Step 3 In the CA Server URL text box, enter the URL to the CA server. You can enter either a domain name or an IP address.

Step 4 In the Params text boxes, enter the parameters for the device certificate. The key size is a value from 384 to 2048 (in bits), and the default value is 2048.

Step 5 Click **Apply** to commit your changes.

Step 6 To add the CA certificate into the controller's CA certificate database, hover your cursor over the blue drop-down arrow for the certificate type and choose **Add**.

Step 7 Choose the **AP Provisioning** tab to open the Local Significant Certificates (LSC) - AP Provisioning page.

Step 8 Select the **Enable** check box and click **Update** to provision the LSC on the access point.

Step 9 When a message appears indicating that the access points will be rebooted, click **OK**.

Step 10 In the Number of Attempts to LSC text box, enter the number of times that the access point attempts to join the controller using an LSC before the access point reverts to the default certificate (MIC or SSC). The range is 0 to 255 (inclusive), and the default value is 3.

Note If you set the number of retries to a nonzero value and the access point fails to join the controller using an LSC after the configured number of retries, the access point reverts to the default certificate. If you set the number of retries to 0 and the access point fails to join the controller using an LSC, the access point does not attempt to join the controller using the default certificate.

Note If you are configuring LSC for the first time, we recommend that you configure a nonzero value.

Step 11 Enter the access point MAC address in the AP Ethernet MAC Addresses text box and click **Add** to add access points to the provision list.

Note To remove an access point from the provision list, hover your cursor over the blue drop-down arrow for the access point and choose **Remove**.

Note If you configure an access point provision list, only the access points in the provision list are provisioned when you enable AP provisioning. If you do not configure an access point provision list, all access points with a MIC or SSC certificate that join the controller are LSC provisioned.

Step 12 Click **Apply** to commit your changes.

Step 13 Click **Save Configuration** to save your changes.

Configuring LSC (CLI)

Step 1 Enable LSC on the system by entering this command:

config certificate lsc {**enable** | **disable**}

Step 2 Configure the URL to the CA server by entering this command:

config certificate lsc ca-server *http://url:port/path*

where *url* can be either a domain name or IP address.

Note You can configure only one CA server. To configure a different CA server, delete the configured CA server using the **config certificate lsc ca-server delete** command, and then configure a different CA server.

Step 3 Add the LSC CA certificate into the controller's CA certificate database by entering this command:

config certificate lsc ca-cert {**add** | **delete**}

Step 4 Configure the parameters for the device certificate by entering this command:

config certificate lsc subject-params *country state city orgn dept e-mail*

Note The common name (CN) is generated automatically on the access point using the current MIC/SSC format C*xxxx-MacAddr*, where *xxxx* is the product number.

Step 5 Configure a key size by entering this command:

config certificate lsc other-params *keysize*

The *keysize* is a value from 384 to 2048 (in bits), and the default value is 2048.

Step 6 Add access points to the provision list by entering this command:

config certificate lsc ap-provision auth-list add *AP_mac_addr*

Note To remove access points from the provision list, enter the **config certificate lsc ap-provision auth-list delete** *AP_mac_addr command.*

Note If you configure an access point provision list, only the access points in the provision list are provisioned when you enable AP provisioning (in Step 8). If you do not configure an access point provision list, all access points with a MIC or SSC certificate that join the controller are LSC provisioned.

Step 7 Configure the number of times that the access point attempts to join the controller using an LSC before the access point reverts to the default certificate (MIC or SSC) by entering this command:

config certificate lsc ap-provision revert-cert *retries*

where *retries* is a value from 0 to 255, and the default value is 3.

Note If you set the number of retries to a nonzero value and the access point fails to join the controller using an LSC after the configured number of retries, the access point reverts to the default certificate. If you set the number of retries to 0 and the access point fails to join the controller using an LSC, the access point does not attempt to join the controller using the default certificate.

Note If you are configuring LSC for the first time, we recommend that you configure a nonzero value.

Step 8 Provision the LSC on the access point by entering this command:

config certificate lsc ap-provision {**enable** | **disable**}

Step 9 See the LSC summary by entering this command:

show certificate lsc summary

Information similar to the following appears:

```
LSC Enabled..................................... Yes
LSC CA-Server................................... http://10.0.0.1:8080/caserver

LSC AP-Provisioning............................. Yes
    Provision-List.............................. Not Configured
    LSC Revert Count in AP reboots.............. 3

LSC Params:
    Country..................................... 4
    State....................................... ca
    City........................................ ss
    Orgn........................................ org
    Dept........................................ dep
    Email....................................... dep@co.com
    KeySize..................................... 390

LSC Certs:
    CA Cert..................................... Not Configured
    RA Cert..................................... Not Configured
```

Step 10 See details about the access points that are provisioned using LSC by entering this command:

show certificate lsc ap-provision

Information similar to the following appears:

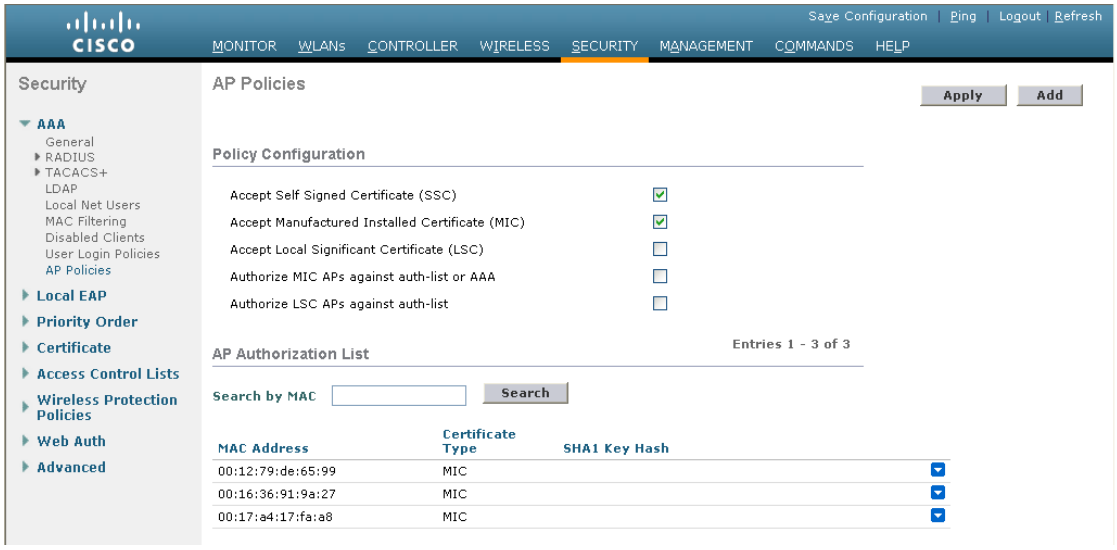
```
LSC AP-Provisioning.......................... Yes
Provision-List............................... Present

Idx     Mac Address
---     ------------
1       00:18:74:c7:c0:90
```

Authorizing Access Points (GUI)

Step 1 Choose **Security** > **AAA** > **AP Policies** to open the AP Policies page.

Figure 9-11 AP Policies Page



Step 2 If you want the access point to accept self-signed certificates (SSCs), manufactured-installed certificates (MICs), or local significant certificates (LSCs), select the appropriate check box.

- If you want the access points to be authorized using a AAA RADIUS server, select the **Authorize MIC APs against auth-list or AAA** check box.
- If you want the access points to be authorized using an LSC, select the **Authorize LSC APs against auth-list** check box.

Step 3 Click **Apply** to commit your changes.

Step 4 Follow these steps to add an access point to the controller's authorization list:

a. Click **Add** to access the Add AP to Authorization List area.

b. In the MAC Address text box, enter the MAC address of the access point.

c. From the Certificate Type drop-down list, choose **MIC**, **SSC**, or **LSC**.

d. Click **Add**. The access point appears in the access point authorization list.

Note To remove an access point from the authorization list, hover your cursor over the blue drop-down arrow for the access point and choose **Remove**.

Note To search for a specific access point in the authorization list, enter the MAC address of the access point in the Search by MAC text box and click **Search**.

Authorizing Access Points (CLI)

- Configure an access point authorization policy by entering this command:

  config auth-list ap-policy {**authorize-ap** {**enable** | **disable**} | **authorize-lsc-ap** {**enable** | **disable**}}

- Configure an access point to accept manufactured-installed certificates (MICs), self-signed certificates (SSCs), or local significant certificates (LSCs) by entering this command:

  config auth-list ap-policy {**mic** | **ssc** | **lsc** {**enable** | **disable**}}

- Configure the user name to be used in access point authorization requests.

  config auth-list ap-policy {**authorize-ap username** *{ap_name | ap_mac | both}*}

- Add an access point to the authorization list by entering this command:

  config auth-list add {**mic** | **ssc** | **lsc**} *ap_mac* [*ap_key*]

  where *ap_key* is an optional key hash value equal to 20 bytes or 40 digits.

Note To delete an access point from the authorization list, enter this command: **config auth-list delete ap_mac**.

- See the access point authorization list by entering this command:

  show auth-list

Using DHCP Option 43 and DHCP Option 60

Cisco Aironet access points use the type-length-value (TLV) format for DHCP option 43. DHCP servers must be programmed to return the option based on the DHCP Vendor Class Identifier (VCI) string (DHCP option 60) of the access point. Table 9-2 lists the VCI strings for Cisco access points capable of operating in lightweight mode.

Table 9-2 VCI Strings For Lightweight Access Points

Access Point	VCI String
Cisco Aironet 1040 Series	Cisco AP c1040
Cisco Aironet 1130 Series	Cisco AP c1130

Table 9-2 VCI Strings For Lightweight Access Points (continued)

Access Point	VCI String
Cisco Aironet 1140 Series	Cisco AP c1140
Cisco Aironet 1240 Series	Cisco AP c1240
Cisco Aironet 1250 Series	Cisco AP c1250
Cisco Aironet 1260 Series	Cisco AP c1260
Cisco Aironet 1520 Series	Cisco AP c1520
Cisco Aironet 1550 Series	Cisco AP c1550
Cisco Aironet 3600 Series	Cisco AP c3600
Cisco Aironet 3500 Series	Cisco AP c3500
Cisco AP801 Embedded Access Point	Cisco AP801
Cisco AP802 Embedded Access Point	Cisco AP802

The format of the TLV block is as follows:

- Type: 0xf1 (decimal 241)
- Length: Number of controller IP addresses * 4
- Value: List of the IP addresses of controller management interfaces

See the product documentation for your DHCP server for instructions on configuring DHCP option 43. The *Upgrading Autonomous Cisco Aironet Access Points to Lightweight Mode* document contains example steps for configuring option 43 on a DHCP server.

If the access point is ordered with the Service Provider Option - AIR-OPT60-DHCP selected, the VCI string for that access point will be different than those listed above. The VCI string will have the “ServiceProvider”. For example, a 1260 with this option will return this VCI string: "Cisco AP c1260-ServiceProvider".

Note The controller IP address that you obtain from the DHCP server should be a unicast IP address. Do not configure the controller IP address as a multicast address when configuring DHCP Option 43.

Troubleshooting the Access Point Join Process

Access points can fail to join a controller for many reasons such as a RADIUS authorization is pending, self-signed certificates are not enabled on the controller, the access point and controller’s regulatory domains do not match, and so on.

Note For join information specific to an OfficeExtend access point, see the “Configuring OfficeExtend Access Points” section on page 9-51.

Controller software release 5.2 or later releases enable you to configure the access points to send all CAPWAP-related errors to a syslog server. You do not need to enable any debug commands on the controller because all of the CAPWAP error messages can be viewed from the syslog server itself.

The state of the access point is not maintained on the controller until it receives a CAPWAP join request from the access point, so it can be difficult to determine why the CAPWAP discovery request from a certain access point was rejected. In order to troubleshoot such joining issues without enabling CAPWAP debug commands on the controller, the controller collects information for all access points that send a discovery message to this controller and maintains information for any access points that have successfully joined this controller.

The controller collects all join-related information for each access point that sends a CAPWAP discovery request to the controller. Collection begins with the first discovery message received from the access point and ends with the last configuration payload sent from the controller to the access point.

You can view join-related information for the following numbers of access points:

- Up to 250 access points for Cisco 5500 Series Controllers
- Up to 300 access points for 4400 series controllers, the Cisco WiSM, and the Catalyst 3750G Integrated Wireless LAN Controller Switch
- Up to three times the maximum number of access points supported by the platform for the Controller Network Module within the Cisco 28/37/38xx Series Integrated Services Routers

When the controller is maintaining join-related information for the maximum number of access points, it does not collect information for any more access points.

An access point sends all syslog messages to IP address 255.255.255.255 by default when any of the following conditions are met:

- An access point that runs software release 4.2 or later releases has been newly deployed.
- An existing access point that runs a software release prior to 4.2 releases has been upgraded to 4.2 or a later release.
- An existing access point that runs software release 4.2 or later releases has been reset after clearing the configuration.

If any of these conditions are met and the access point has not yet joined a controller, you can also configure a DHCP server to return a syslog server IP address to the access point using option 7 on the server. The access point then starts sending all syslog messages to this IP address.

You can also configure the syslog server IP address through the access point CLI, provided the access point is currently not connected to the controller by entering the **lwapp ap log-server** *syslog_server_IP_address command.*

When the access point joins a controller for the first time, the controller pushes the global syslog server IP address (the default is 255.255.255.255) to the access point. After that, the access point sends all syslog messages to this IP address, until it is overridden by one of the following scenarios:

- The access point is still connected to the same controller, and the global syslog server IP address configuration on the controller has been changed using the **config ap syslog host global** *syslog_server_IP_address* command. In this case, the controller pushes the new global syslog server IP address to the access point.
- The access point is still connected to the same controller, and a specific syslog server IP address has been configured for the access point on the controller using the **config ap syslog host specific** *Cisco_AP syslog_server_IP_address* command. In this case, the controller pushes the new specific syslog server IP address to the access point.
- The access point gets disconnected from the controller, and the syslog server IP address has been configured from the access point CLI using the **lwapp ap log-server** *syslog_server_IP_address* command. This command works only if the access point is not connected to any controller.
- The access point gets disconnected from the controller and joins another controller. In this case, the new controller pushes its global syslog server IP address to the access point.

Whenever a new syslog server IP address overrides the existing syslog server IP address, the old address is erased from persistent storage, and the new address is stored in its place. The access point also starts sending all syslog messages to the new IP address, provided the access point can reach the syslog server IP address.

This section contains the following topics:

- Configuring the Syslog Server for Access Points (CLI), page 9-39
- Viewing Access Point Join Information, page 9-39

Configuring the Syslog Server for Access Points (CLI)

Step 1 Perform one of the following:

- To configure a global syslog server for all access points that join this controller, enter this command:

  config ap syslog host global *syslog_server_IP_address*

  Note By default, the global syslog server IP address for all access points is 255.255.255.255. Make sure that the access points can reach the subnet on which the syslog server resides before configuring the syslog server on the controller. If the access points cannot reach this subnet, the access points are unable to send out syslog messages.

- To configure a syslog server for a specific access point, enter this command:

  config ap syslog host specific *Cisco_AP syslog_server_IP_address*

  Note By default, the syslog server IP address for each access point is 0.0.0.0, which indicates that the access point is not yet set. When the default value is used, the global access point syslog server IP address is pushed to the access point.

Step 2 Save your changes by entering this command:

save config

Step 3 See the global syslog server settings for all access points that join the controller by entering this command:

show ap config global

Information similar to the following appears:

```
AP global system logging host..................... 255.255.255.255
```

Step 4 See the syslog server settings for a specific access point by entering this command:

show ap config general *Cisco_AP*

Viewing Access Point Join Information

Join statistics for an access point that sends a CAPWAP discovery request to the controller at least once are maintained on the controller even if the access point is rebooted or disconnected. These statistics are removed only when the controller is rebooted or when you choose to clear the statistics.

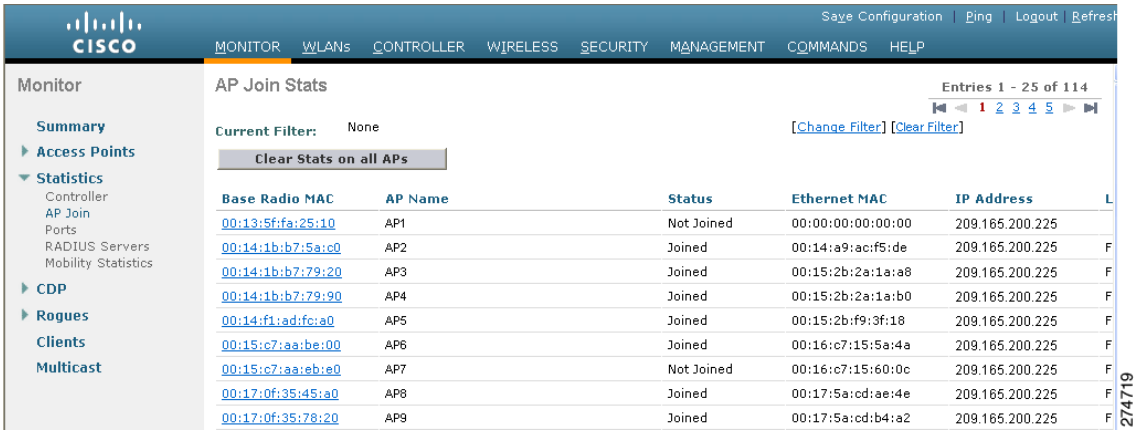
This section contains the following topics:

- Viewing Access Point Join Information (GUI), page 9-40
- Viewing Access Point Join Information (CLI), page 9-41

Viewing Access Point Join Information (GUI)

Step 1 Choose **Monitor** > **Statistics** > **AP Join** to open the AP Join Stats page.

Figure 9-12 AP Join Stats Page



This page lists all of the access points that are joined to the controller or that have tried to join. It shows the radio MAC address, access point name, current join status, Ethernet MAC address, IP address, and last join time for each access point.

The total number of access points appears in the upper right-hand corner of the page. If the list of access points spans multiple pages, you can view these pages by clicking the page number links. Each page shows the join statistics for up to 25 access points.

Note If you want to remove an access point from the list, hover your cursor over the blue drop-down arrow for that access point and click **Remove**.

Note If you want to clear the statistics for all access points and start over, click **Clear Stats on All APs**.

Step 2 If you want to search for specific access points in the list of access points on the AP Join Stats page, follow these steps to create a filter to display only access points that meet certain criteria (such as MAC address or access point name).

Note This feature is especially useful if your list of access points spans multiple pages, preventing you from viewing them all at once.

a. Click **Change Filter** to open the Search AP dialog box.

b. Select one of the following check boxes to specify the criteria used when displaying access points:

- **MAC Address**—Enter the base radio MAC address of an access point.
- **AP Name**—Enter the name of an access point.

Note When you enable one of these filters, the other filter is disabled automatically.

c. Click **Find** to commit your changes. Only the access points that match your search criteria appear on the AP Join Stats page, and the Current Filter parameter at the top of the page specifies the filter used to generate the list (for example, MAC Address:00:1e:f7:75:0a:a0 or AP Name:pmsk-ap).

Note If you want to remove the filter and display the entire access point list, click **Clear Filter**.

Step 3 To see detailed join statistics for a specific access point, click the radio MAC address of the access point. The AP Join Stats Detail page appears.

This page provides information from the controller's perspective on each phase of the join process and shows any errors that have occurred.

Viewing Access Point Join Information (CLI)

Use these CLI commands to see access point join information:

- See the MAC addresses of all the access points that are joined to the controller or that have tried to join by entering this command:

  show ap join stats summary all

  Information similar to the following appears:

```
Number of APs.......................................... 4

Base Mac             AP EthernetMac     AP Name       IP Address       Status
00:0b:85:57:bc:c0    00:0b:85:57:bc:c0   AP1130       10.10.163.217   Joined
00:1c:0f:81:db:80    00:1c:63:23:ac:a0   AP1140       10.10.163.216   Not joined
00:1c:0f:81:fc:20    00:1b:d5:9f:7d:b2   AP1         10.10.163.215   Joined
00:21:1b:ea:36:60   00:0c:d4:8a:6b:c1    AP2         10.10.163.214   Not joined
```

- See the last join error detail for a specific access point by entering this command:

  show ap join stats summary *ap_mac*

  where *ap_mac* is the MAC address of the 802.11 radio interface.

Note To obtain the MAC address of the 802.11 radio interface, enter the **show interfaces Dot11Radio 0** command on the access point.

Information similar to the following appears:

```
Is the AP currently connected to controller..... Yes
Time at which the AP joined this controller last time..... Aug 21 12:50:36.061
Type of error that occurred last..... AP got or has been
disconnected
Reason for error that occurred last..... The AP has been reset by
the controller
Time at which the last join error occurred..... Aug 21 12:50:34.374
```

- See all join-related statistics collected for a specific access point by entering this command:

  show ap join stats detailed *ap_mac*

  Information similar to the following appears:

```
Discovery phase statistics
- Discovery requests received.............................. 2
- Successful discovery responses sent...................... 2
- Unsuccessful discovery request processing................ 0
- Reason for last unsuccessful discovery attempt........... Not applicable
- Time at last successful discovery attempt................ Aug 21 12:50:23.335
- Time at last unsuccessful discovery attempt.............. Not applicable

Join phase statistics
- Join requests received................................... 1
- Successful join responses sent........................... 1
- Unsuccessful join request processing..................... 1
- Reason for last unsuccessful join attempt................ RADIUS authorization
 is pending for the AP
- Time at last successful join attempt..................... Aug 21 12:50:34.481
- Time at last unsuccessful join attempt................... Aug 21 12:50:34.374

Configuration phase statistics
- Configuration requests received.......................... 1
- Successful configuration responses sent.................. 1
- Unsuccessful configuration request processing............ 0
- Reason for last unsuccessful configuration attempt....... Not applicable
- Time at last successful configuration attempt............ Aug 21 12:50:34.374
- Time at last unsuccessful configuration attempt.......... Not applicable

Last AP message decryption failure details
- Reason for last message decryption failure............... Not applicable

Last AP disconnect details
- Reason for last AP connection failure.................... The AP has been reset by
the controller

Last join error summary
- Type of error that occurred last......................... AP got or has been
disconnected
- Reason for error that occurred last...................... The AP has been reset by
the controller
- Time at which the last join error occurred............... Aug 21 12:50:34.374
```

- Clear the join statistics for all access points or for a specific access point by entering this command:

  clear ap join stats {**all** | *ap_mac*}

Sending Debug Commands to Access Points Converted to Lightweight Mode

You can enable the controller to send debug commands to an access point converted to lightweight mode by entering this command:

debug ap {**enable** | **disable** | **command** *cmd*} *Cisco_AP*

When this feature is enabled, the controller sends debug commands to the converted access point as character strings. You can send any debug command supported by Cisco Aironet access points that run Cisco IOS software in lightweight mode.

Understanding How Converted Access Points Send Crash Information to the Controller

When a converted access point unexpectedly reboots, the access point stores a crash file on its local flash memory at the time of the crash. After the unit reboots, it sends the reason for the reboot to the controller. If the unit rebooted because of a crash, the controller pulls up the crash file using existing CAPWAP messages and stores it in the controller flash memory. The crash info copy is removed from the access point flash memory when the controller pulls it from the access point.

Understanding How Converted Access Points Send Radio Core Dumps to the Controller

When a radio module in a converted access point generates a core dump, the access point stores the core dump file of the radio on its local flash memory at the time of the radio crash. It sends a notification message to the controller indicating which radio generated a core dump file. The controller sends a trap that alerts you so that you can retrieve the radio core file from the access point.

The retrieved core file is stored in the controller flash and can be uploaded through TFTP or FTP to an external server for analysis. The core file is removed from the access point flash memory when the controller pulls it from the access point.

This section contains the following topics:

- Retrieving Radio Core Dumps (CLI), page 9-43
- Uploading Radio Core Dumps, page 9-43

Retrieving Radio Core Dumps (CLI)

Step 1 Transfer the radio core dump file from the access point to the controller by entering this command:

config ap crash-file get-radio-core-dump *slot Cisco_AP*

For the *slot* parameter, enter the slot ID of the radio that crashed.

Step 2 Verify that the file was downloaded to the controller by entering this command:

show ap crash-file

Information similar to the following appears:

```
Local Core Files:
lrad_AP1130.rdump0   (156)

The number in parentheses indicates the size of the file. The size should be greater than
zero if a core dump file is available.
```

Uploading Radio Core Dumps

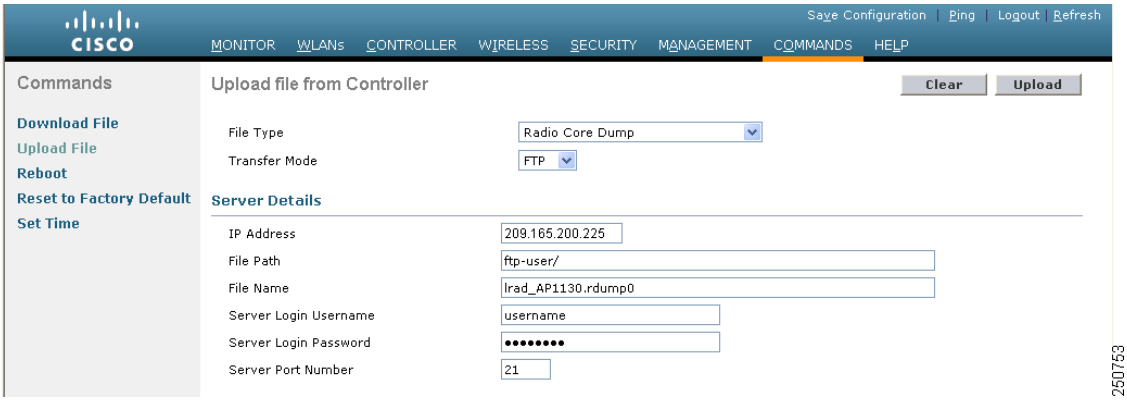
This section contains the following topics:

- Uploading Radio Core Dumps (GUI), page 9-44
- Uploading Radio Core Dumps (CLI), page 9-44

Uploading Radio Core Dumps (GUI)

Step 1 Choose **Commands** > **Upload File** to open the Upload File from Controller page.

Figure 9-13 Upload File from Controller Page



Step 2 From the File Type drop-down list, choose **Radio Core Dump**.

Step 3 From the Transfer Mode drop-down list, choose **TFTP** or **FTP**.

Step 4 In the IP Address text box, enter the IP address of the TFTP or FTP server.

Step 5 In the File Path text box, enter the directory path of the file.

Step 6 In the File Name text box, enter the name of the radio core dump file.

Note The *filename* that you enter should match the filename generated on the controller. You can determine the *filename* on the controller by entering the **show ap crash-file** command.

Step 7 If you chose FTP as the Transfer Mode, follow these steps:

a. In the Server Login Username text box, enter the FTP server login name.

b. In the Server Login Password text box, enter the FTP server login password.

c. In the Server Port Number text box, enter the port number of the FTP server. The default value for the server port is 21.

Step 8 Click **Upload** to upload the radio core dump file from the controller. A message appears indicating the status of the upload.

Uploading Radio Core Dumps (CLI)

Step 1 Transfer the file from the controller to a TFTP or FTP server by entering these commands:

- **transfer upload mode** {**tftp** | **ftp**}
- **transfer upload datatype radio-core-dump**
- **transfer upload serverip** *server_ip_address*
- **transfer upload path** *server_path_to_file*

- **transfer upload filename** *filename*

Note The *filename* that you enter should match the filename generated on the controller. You can determine the *filename* on the controller by entering the **show ap crash-file** command.

Note Ensure that the *filename* and *server_path_to_file* do not contain these special characters: \, :, *, ?, ", <, >, and |. You can use only / (forward slash) as the path separator. If you use the disallowed special characters in the *filename*, then the special characters are replaced with _ (underscores); and if you use the disallowed special characters in the *server_path_to_file*, then the path is set to the root path.

Step 2 If you are using an FTP server, also enter these commands:

- **transfer upload username** *username*
- **transfer upload password** *password*
- **transfer upload port** *port*

Note The default value for the *port* parameter is 21.

Step 3 View the updated settings by entering this command:

transfer upload start

Step 4 When prompted to confirm the current settings and start the software upload, answer **y**.

Uploading Memory Core Dumps from Converted Access Points

By default, access points converted to lightweight mode do not send memory core dumps to the controller.

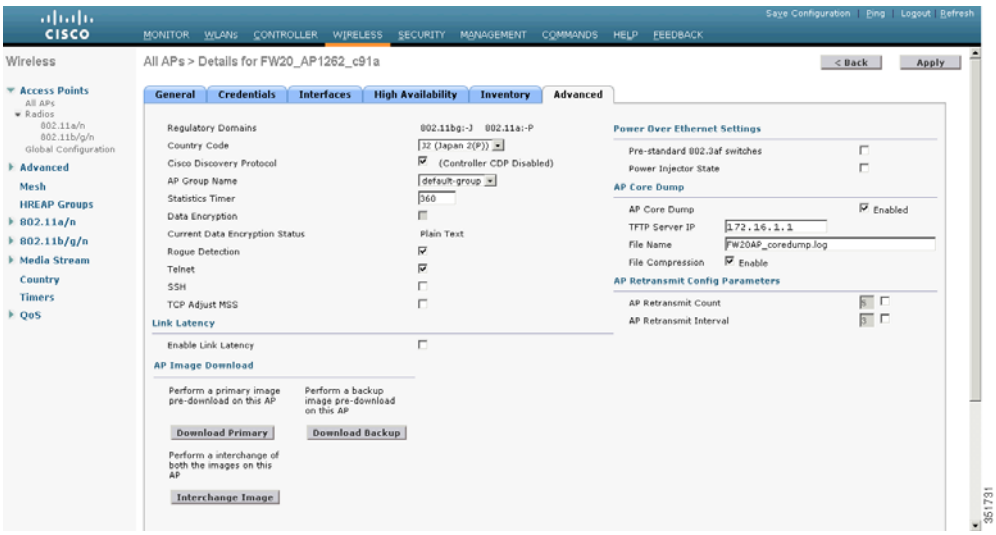
This section contains the following topics:

- Uploading Access Point Core Dumps (GUI), page 9-45
- Uploading Access Point Core Dumps (CLI), page 9-46

Uploading Access Point Core Dumps (GUI)

Step 1 Choose **Wireless** > **Access Points** > **All APs** > *access point name* > and choose the **Advanced** tab to open the All APs > Details for (Advanced) page.

Figure 9-14 All APs > Details for (Advanced) Page



Step 2 Select the **AP Core Dump** check box to upload a core dump of the access point.

Step 3 In the TFTP Server IP text box, enter the IP address of the TFTP server.

Step 4 In the File Name text box, enter a name of the access point core dump file (such as *dump.log*).

Step 5 Select the **File Compression** check box to compress the access point core dump file. When you enable this option, the file is saved with a .gz extension (such as *dump.log.gz*). This file can be opened with WinZip.

Step 6 Click **Apply** to commit your changes.

Step 7 Click **Save Configuration** to save your changes.

Uploading Access Point Core Dumps (CLI)

Step 1 Upload a core dump of the access point by entering this command on the controller:

config ap core-dump enable *tftp_server_ip_address filename* {**compress** | **uncompress**} {*ap_name* | **all**}

where

- *tftp_server_ip_address* is the IP address of the TFTP server to which the access point sends core dump files.

Note The access point must be able to reach the TFTP server.

- *filename* is the name that the access points uses to label the core file.
- **compress** configures the access point to send compressed core files whereas **uncompress** configures the access point to send uncompressed core files.

Note When you choose **compress**, the file is saved with a .gz extension (for example, dump.log.gz). This file can be opened with WinZip.

- *ap_name* is the name of a specific access point for which core dumps are uploaded and **all** is all access points converted to lightweight mode.

Step 2 Save your changes by entering this command:

save config

Viewing the AP Crash Log Information

Whenever the controller reboots or upgrades, the AP crash log information gets deleted from the controller. We recommend that you make a backup of AP crash log information before rebooting or upgrading the controller.

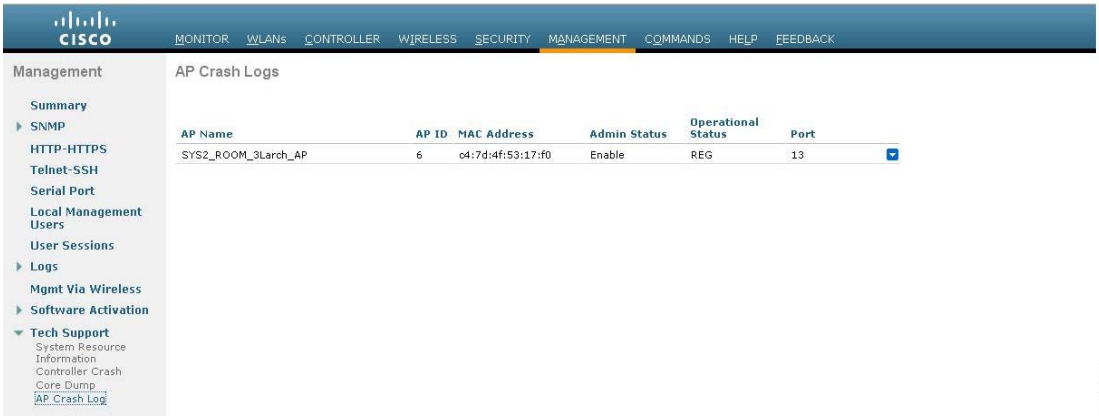
This section contains the following topics:

- Viewing the AP Crash Log information (GUI), page 9-47
- Viewing the AP Crash Log information (CLI), page 9-47

Viewing the AP Crash Log information (GUI)

Step 1 Choose **Management** > **Tech Support** > **AP Crash Log** to open the AP Crash Logs page.

Figure 9-15 AP Crash Logs Page



Viewing the AP Crash Log information (CLI)

Step 1 Verify that the crash file was downloaded to the controller by entering this command:

show ap crash-file

Information similar to the following appears:

```
Local Core Files:
lrad_AP1130.rdump0 (156)
```

```
The number in parentheses indicates the size of the file. The size should be greater than
zero if a core dump file is available.
```

Step 2 See the contents of the AP crash log file by entering this command:

show ap crash-file *Cisoc_AP*

Displaying MAC Addresses for Converted Access Points

There are some differences in the way that controllers display the MAC addresses of converted access points on information pages in the controller GUI:

- On the AP Summary page, the controller lists the Ethernet MAC addresses of converted access points.
- On the AP Detail page, the controller lists the BSS MAC addresses and Ethernet MAC addresses of converted access points.
- On the Radio Summary page, the controller lists converted access points by radio MAC address.

Disabling the Reset Button on Access Points Converted to Lightweight Mode

You can disable the reset button on access points converted to lightweight mode. The reset button is labeled MODE on the outside of the access point.

Use this command to disable or enable the reset button on one or all converted access points associated to a controller:

config ap reset-button {**enable** | **disable**} {*ap-name* | **all**}

The reset button on converted access points is enabled by default.

Configuring a Static IP Address on a Lightweight Access Point

If you want to specify an IP address for an access point rather than having one assigned automatically by a DHCP server, you can use the controller GUI or CLI to configure a static IP address for the access point. Static IP addresses are generally used only for deployments with a limited number of users.

An access point cannot discover the controller using domain name system (DNS) resolution if a static IP address is configured for the access point, unless you specify a DNS server and the domain to which the access point belongs. Previously, these parameters could be configured only using the CLI, but controller software release 6.0 or later releases expand this functionality to the GUI.

Note If you configure an access point to use a static IP address that is not on the same subnet on which the access point's previous DHCP address was, the access point falls back to a DHCP address after the access point reboots. If the access point falls back to a DHCP address, enter the **show ap config general** *Cisco_AP* CLI command to show that the access point is using a fallback IP address. However, the GUI shows both the static IP address and the DHCP address, but it does not identify the DHCP address as a fallback address.

This section contains the following topics:

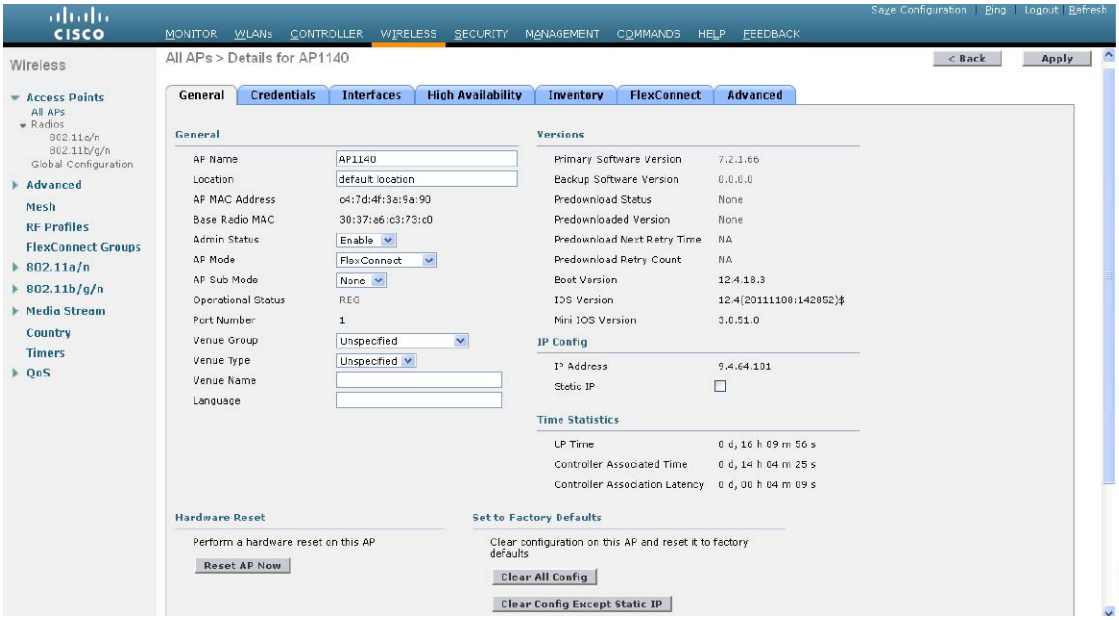
- Configuring a Static IP Address (GUI), page 9-49
- Configuring a Static IP Address (CLI), page 9-50

Configuring a Static IP Address (GUI)

Step 1 Choose **Wireless** > **Access Points** > **All APs** to open the All APs page.

Step 2 Click the name of the access point for which you want to configure a static IP address. The All APs > Details for (General) page appears.

Figure 9-16 All APs > Details for (General) Page



Step 3 Under IP Config, select the **Static IP** check box if you want to assign a static IP address to this access point. The default value is unselected.

Step 4 Enter the static IP address, netmask, and default gateway in the corresponding text boxes.

Step 5 Click **Apply** to commit your changes. The access point reboots and rejoins the controller, and the static IP address that you specified in Step 4 is sent to the access point.

Step 6 After the static IP address has been sent to the access point, you can configure the DNS server IP address and domain name as follows:

a. In the DNS IP Address text box, enter the IP address of the DNS server.

b. In the Domain Name text box, enter the name of the domain to which the access point belongs.

c. Click **Apply** to commit your changes.

d. Click **Save Configuration** to save your changes.

Configuring a Static IP Address (CLI)

Step 1 Configure a static IP address on the access point by entering this command:

config ap static-ip enable *Cisco_AP ip_address mask gateway*

Note To disable static IP for the access point, enter the **config ap static-ip disable** *Cisco_AP* command.

Step 2 Save your changes by entering this command:

save config

The access point reboots and rejoins the controller, and the static IP address that you specified in Step 1 is pushed to the access point.

Step 3 After the static IP address has been sent to the access point, you can configure the DNS server IP address and domain name as follows:

a. To specify a DNS server so that a specific access point or all access points can discover the controller using DNS resolution, enter this command:

config ap static-ip add nameserver {*Cisco_AP* | **all**} *ip_address*

Note To delete a DNS server for a specific access point or all access points, enter the **config ap static-ip delete nameserver** {*Cisco_AP* | **all**} command.

b. To specify the domain to which a specific access point or all access points belong, enter this command:

config ap static-ip add domain {*Cisco_AP* | **all**} *domain_name*

Note To delete a domain for a specific access point or all access points, enter this command: **config ap static-ip delete domain** {*Cisco_AP* | **all**}.

c. To save your changes, enter this command:

save config

Step 4 See the IP address configuration for the access point by entering this command:

show ap config general *Cisco_AP*

Information similar to the following appears:

```
Cisco AP Identifier.............................. 4
Cisco AP Name.................................... AP6
...
IP Address Configuration......................... Static IP assigned
IP Address....................................... 10.10.10.118
IP NetMask....................................... 255.255.255.0
Gateway IP Addr.............................. 10.10.10.1
Domain........................................... Domain1
Name Server.................................. 10.10.10.205
...
```

Supporting Oversized Access Point Images

Controller software release 5.0 or later releases allow you to upgrade to an oversized access point image by automatically deleting the recovery image to create sufficient space. This feature affects only access points with 8 MB of flash (the 1100, 1200, and 1310 series access points). All newer access points have a larger flash size than 8 MB.

Note As of August 2007, there are no oversized access point images, but as new features are added, the access point image size will continue to grow.

The recovery image provides a backup image that can be used if an access point power-cycles during an image upgrade. The best way to avoid the need for access point recovery is to prevent an access point from power-cycling during a system upgrade. If a power-cycle occurs during an upgrade to an oversized access point image, you can recover the access point using the TFTP recovery procedure.

Recovering the Access Point (Using the TFTP Recovery Procedure)

Step 1 Download the required recovery image from Cisco.com (c1100-rcvk9w8-mx, c1200-rcvk9w8-mx, or c1310-rcvk9w8-mx) and install it in the root directory of your TFTP server.

Step 2 Connect the TFTP server to the same subnet as the target access point and power-cycle the access point. The access point boots from the TFTP image and then joins the controller to download the oversized access point image and complete the upgrade procedure.

Step 3 After the access point has been recovered, you may remove the TFTP server.

Configuring OfficeExtend Access Points

This section contains the following topics:

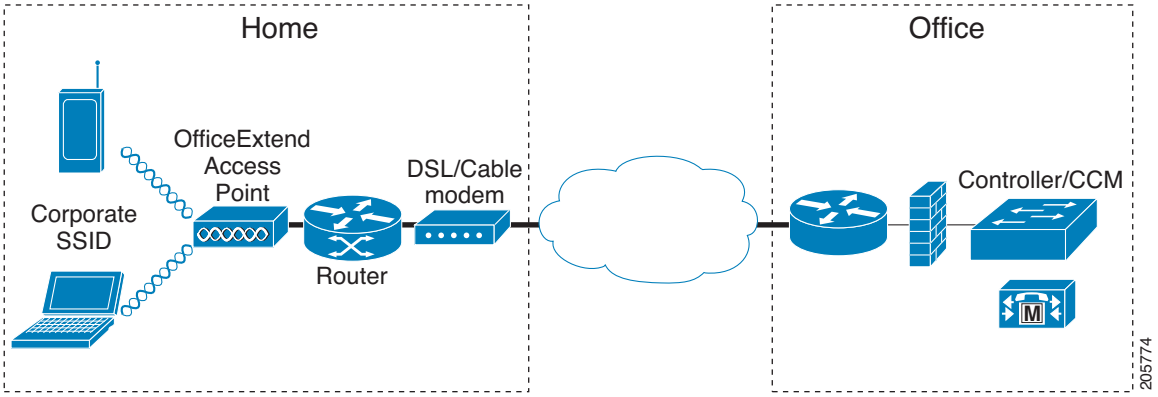
- Information About OfficeExtend Access Points, page 9-52
- OEAP 600 Series Access Points, page 9-52
- Implementing Security, page 9-61
- Licensing for an OfficeExtend Access Point, page 9-62
- Configuring OfficeExtend Access Points, page 9-62
- Configuring a Personal SSID on an OfficeExtend Access Point, page 9-67
- Viewing OfficeExtend Access Point Statistics, page 9-69
- Additional References, page 9-70

Information About OfficeExtend Access Points

An OfficeExtend access point provides secure communications from a controller to an access point at a remote location, seamlessly extending the corporate WLAN over the Internet to an employee's residence. The user's experience at the home office is exactly the same as it would be at the corporate office. Datagram Transport Layer Security (DTLS) encryption between the access point and the controller ensures that all communications have the highest level of security.

Figure 9-17 shows a typical OfficeExtend access point setup.

Figure 9-17 Typical OfficeExtend Access Point Setup



Note OfficeExtend access points are designed to work behind a router or other gateway device that is using network address translation (NAT). NAT allows a device, such as a router, to act as an agent between the Internet (public) and a personal network (private), enabling an entire group of computers to be represented by a single IP address. In controller software release 7.2 or later releases, up to 3 OfficeExtend access points can be deployed behind a NAT device. Prior controller releases could support only one device.

Currently, Cisco 1040, 1130, 1140, 3502I, and 3600 series access points that are associated with a controller can be configured to operate as OfficeExtend access points.

OEAP 600 Series Access Points

This section details the requirements for configuring a Cisco wireless LAN controller for use with the Cisco 600 Series OfficeExtend Access Point. The 600 Series OfficeExtend Access Point supports split mode operation, and it requires configuration through the WLAN controller in local mode. This section describes the configurations necessary for proper connection and supported feature sets.

Note The Cisco 600 Series OfficeExtend access points are designed to work behind a router or other gateway device that is using Network Address Translation (NAT). NAT allows a device, such as a router, to act as an agent between the Internet (public) and a personal network (private), enabling an entire group of computers to be represented by a single IP address. In controller software release 6.0 or later releases, only one OfficeExtend access point can be deployed behind a single NAT device.

Note The CAPWAP UDP 5246 and 5247 ports must be open on the firewall between the WLAN controller and the 600 Series OfficeExtend Access Point.

This section contains the following topics:

- Supported Controller Platforms, page 9-53
- OEAP in Local Mode, page 9-53
- Supported WLAN Settings for 600 Series OfficeExtend Access Point, page 9-54
- WLAN Security Settings for the 600 Series OfficeExtend Access Point, page 9-55
- Authentication Settings, page 9-58
- Supported User Count on 600 Series OfficeExtend Access Point, page 9-58
- Remote LAN Settings, page 9-59
- Channel Management and Settings, page 9-60
- Additional Caveats, page 9-61

Supported Controller Platforms

The 600 Series OfficeExtend Access Point is supported on the Cisco 5508 Series Controller, WISM-2, and Cisco 2500 Series Controllers and requires the controller software 7.0.116.0 release.

The 600 Series OfficeExtend Access Point has DTLS permanently enabled. You cannot disable DTLS on this access point.

OEAP in Local Mode

The 600 Series OfficeExtend Access Point connects to the controller in local mode. You cannot alter these settings.

Note Monitor mode, flexconnect mode, sniffer mode, rogue detector, bridge, and SE-Connect are not supported on the 600 Series OfficeExtend Access Point and are not configurable.

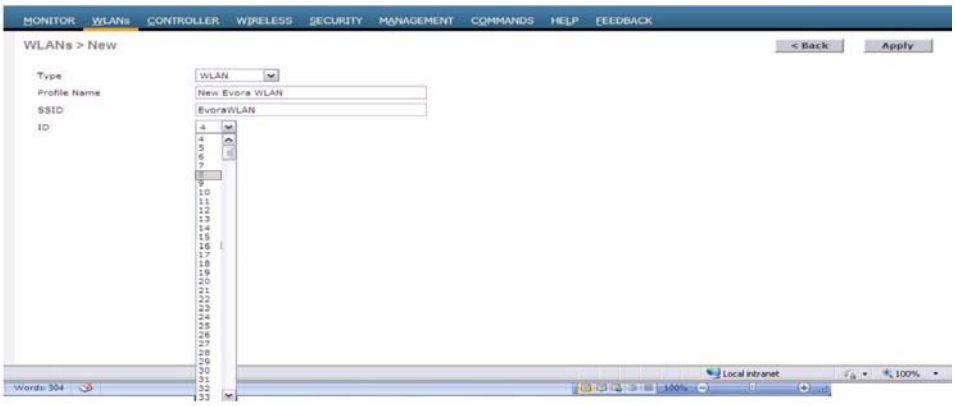
Figure 9-18 OEAP Mode

Supported WLAN Settings for 600 Series OfficeExtend Access Point

The 600 Series OfficeExtend Access Point supports a maximum of three WLANs and one remote LAN. If your network deployment has more than three WLANs, you must place the 600 Series OfficeExtend Access Point in an AP group. If the 600 Series OfficeExtend Access Points are added to an AP group, the same limit of three WLANs and one remote LAN still applies for the configuration of the AP group.

If the 600 Series OfficeExtend Access Point is in the default group, which means that it is not in a defined AP group, the WLAN/remote LAN IDs must be set lower than ID 8.

Figure 9-19 WLAN ID for OEAP



If additional WLANs or remote LANs are created with the intent of changing the WLANs or remote LAN being used by the 600 Series OfficeExtend Access Point, you must disable the current WLANs or remote LAN that you are removing before enabling the new WLANs or remote LAN on the 600 Series OfficeExtend Access Point. If there are more than one remote LANs enabled for an AP group, disable all remote LANs and then enable only one of them.

If more than three WLANs are enabled for an AP group, disable all WLANs and then enable only three of them.

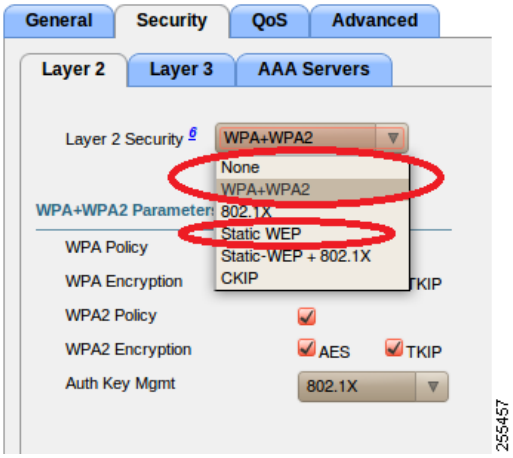
WLAN Security Settings for the 600 Series OfficeExtend Access Point

When configuring the security settings in the WLAN, note that there are specific elements that are not supported on the 600 Series OfficeExtend Access Point. CCX is not supported on the 600 Series OfficeExtend Access Point, and elements related to CCX are not supported.

For Layer 2 Security, the following options are supported for the 600 Series OfficeExtend Access Point:

- None
- WPA+WPA2
- Static WEP
- 802.1X (only for remote LANs)

Figure 9-20 WLAN Security Settings



From the Auth Key Mgmt drop-down list, do not select CCKM in WPA + WPA2 settings; select only 802.1X or PSK.

Figure 9-21 WLAN Security Settings

Security encryption settings must be identical for WPA and WPA2 for TKIP and AES. The following are examples of incompatible settings for TKIP and AES.

Figure 9-22 and Figure 9-23 show the incompatible configuration.

Figure 9-22 Incompatible WPA and WPA2 Security Encryption Settings for OEAP 600 Series

Figure 9-23 Incompatible WPA and WPA2 Security Enctyption Settings for OEAP 600 Series

The following are examples of compatible settings:

Figure 9-24 Compatible Security Settings for OEAP Series

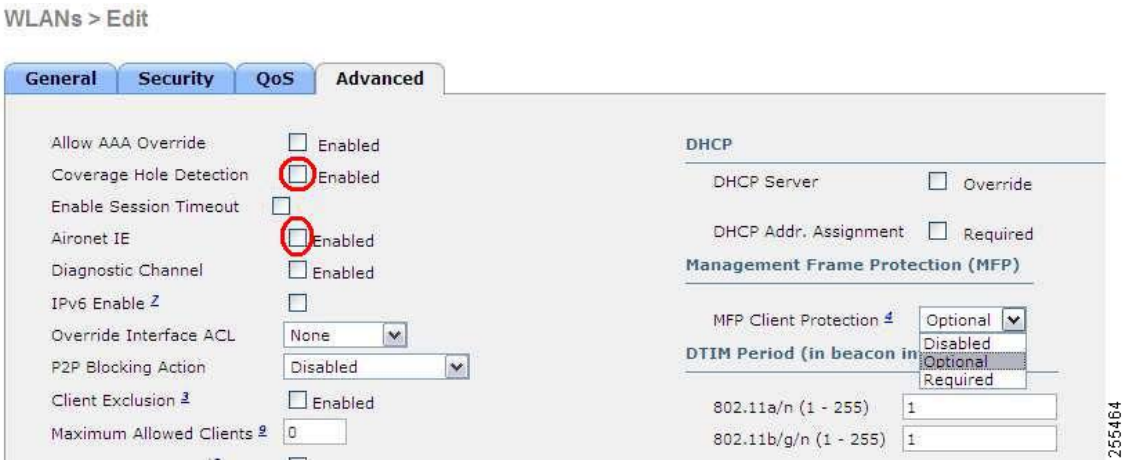
Figure 9-25 Compatible Security Settings for OEAP Series

QoS settings are supported, but CAC is not supported and should not be enabled.

Note Do not enable Coverage Hole Detection.

Note Aironet IE should not be enabled. This option is not supported.

Figure 9-26 QoS Settings for OEAP 600



MFP is also not supported and should be disabled or set to optional.

Figure 9-27 MFP Settings for OEAP Series Access Points

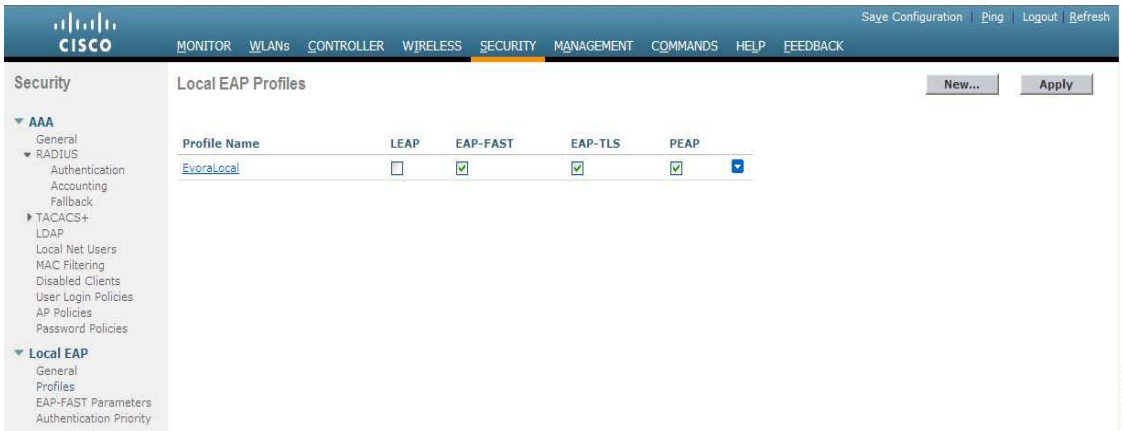
Client Load Balancing and Client Band Select are not supported.

Authentication Settings

For authentication on the 600 Series OfficeExtend Access Point, LEAP is not supported. This configuration needs to be addressed on the clients and RADIUS servers to migrate them to EAP-Fast, EAP-TTLS, EAP-TLS, or PEAP.

If Local EAP is being utilized on the controller, the settings would also have to be modified not to utilize LEAP.

Figure 9-28 Local EAP Profiles



Supported User Count on 600 Series OfficeExtend Access Point

Only 15 users are allowed to connect on the WLAN Controller WLANs provided on the 600 Series OfficeExtend Access Point at any one time, a sixteenth user cannot authenticate until one of the first clients is deauthenticated or timeout on the controller occurs. This number is cumulative across the controller WLANs on the 600 Series OfficeExtend Access Point.

For example, if two controller WLANs are configured and there are fifteen users on one of the WLANs, no users can join the other WLAN on the 600 Series OfficeExtend Access Point at that time.

This limit does not apply to the local private WLANs that the end user configures on the 600 Series OfficeExtend Access Point for personal use. Clients connected on these private WLANs or on the wired ports do not affect these limits.

Remote LAN Settings

Only four clients can connect through a remote LAN port on the 600 Series OfficeExtend Access Point. This number does not affect the fifteen user limit imposed for the Controller WLANs. The remote LAN client limit supports connecting a switch or hub to the remote LAN port for multiple devices or connecting directly to a Cisco IP phone that is connected to that port. Only the first four devices can connect connect until one of the devices is idle for more than one minute.

Remote LAN is configured in the same way that a WLAN or Guest LAN is configured on the controller.

Figure 9-29 Remote LAN Settings for OEAP 600 Series AP

Security settings can be left open, set for MAC filtering, or set for Web Authentication. The default is to use MAC filtering. Additionally, you can specify 802.1X Layer 2 security settings.

The following figure shows Layer 2 security settings for OEAP 600 Series APs in a remote LAN.

Figure 9-30 Layer 2 Security Settings for OEAP 600 Series APs in Remote LANs

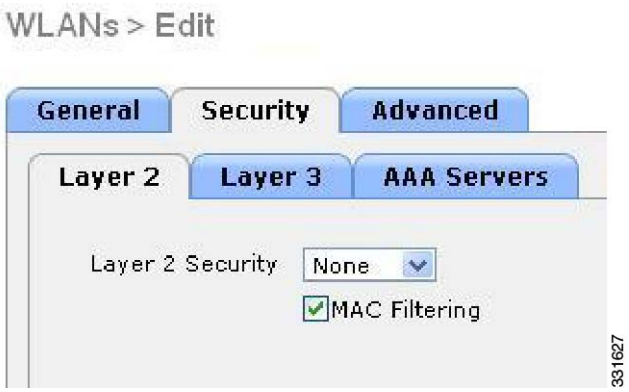
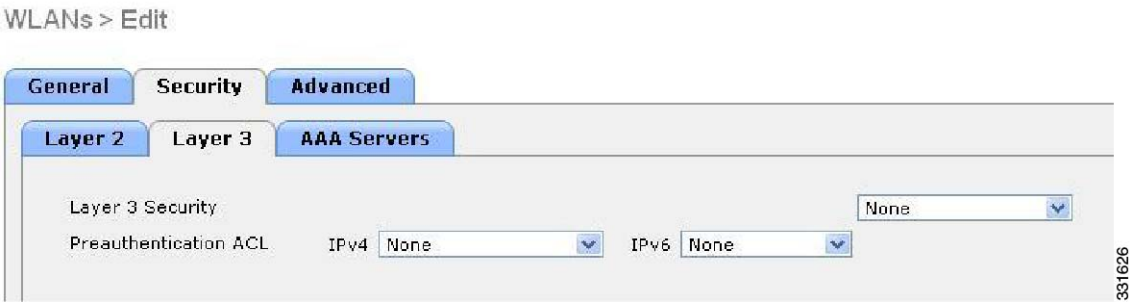


Figure 9-31 shows the Layer 3 security configuration.

Figure 9-31 Layer 3 Security Settings for OEAP 600 Series APs in Remote LANs



Channel Management and Settings

The radios for the 600 Series OfficeExtend Access Point are controlled through the Local GUI on the access point and not through the Wireless LAN Controller. Attempting to control the spectrum channel or power, or to disable the radios through the controller does not have effect on the 600 Series OfficeExtend Access Point. RRM is not supported on the 600 Series OfficeExtend Access Point.

The 600 series scans and chooses channels for 2.4 GHz and 5.0 GHz during startup as long as the default settings on the local GUI are left as default in both spectrums.

Figure 9-32 Channel Selection for OEAP 600 Series APs

The channel bandwidth for 5.0 GHz is also configured on the 600 Series OfficeExtend Access Point Local GUI, for 20 MHz or 40 MHz wide channels. Setting the channel width to 40 MHz for 2.4 GHz is not supported and fixed at 20 MHz.

Figure 9-33 Channel Width for OEAP 600 APs

Additional Caveats

The 600 Series OfficeExtend Access Points are designed for single AP deployments, therefore client roaming between 600 Series OfficeExtend Access Points is not supported.

Disabling the 802.11a/n or 802.11b/g/n on the controller may not disable these spectrums on the 600 Series OfficeExtend Access Point since local SSID may be still working.

Note Your firewall must be configured to allow traffic from access points using CAPWAP. Make sure that UDP ports 5246 and 5247 are enabled and are not blocked by an intermediate device that could prevent an access point from joining the controller.

Implementing Security

Note Configuring LSC is not a requirement but an option. The OfficeExtend access points do not support LSC.

Step 1 Use local significant certificates (LSCs) to authorize your OfficeExtend access points, by following the instructions in the "Authorizing Access Points Using LSCs" section on page 9-31.

Step 2 Implement AAA server validation using the access point's MAC address, name, or both as the username in authorization requests, by entering this command:

config auth-list ap-policy authorize-ap username {*ap_mac* | *Cisco_AP* | **both**}

Using the access point name for validation can ensure that only the OfficeExtend access points of valid employees can join the controller. To implement this security policy, make sure to name each OfficeExtend access point with an employee ID or employee number. When an employee is terminated, run a script to remove this user from the AAA server database, which prevents that employee's OfficeExtend access point from joining the network.

Step 3 Enter the **save config** command to save your configuration.

Note CCX is not supported on the 600 OEAP. Elements related to CCX are not supported. Also, only 802.1x or PSK is supported. TKIP and AES security encryption settings must be identical for WPA and WPA2.

Licensing for an OfficeExtend Access Point

To use OfficeExtend access points, a base license must be installed and in use on the controller. After the license is installed, you can enable the OfficeExtend mode on an 1130 series, a 1140 series, a 1040 series, a 3500 (integrated antenna) series, or a 3600 (integrated antenna) series access point.

Note See Chapter 4, "Configuring Controller Settings," for information on obtaining and installing licenses.

Configuring OfficeExtend Access Points

After the 1130 series, 1140 series, 1040 series, 3500 (integrated antenna) series, or 3600 (integrated antenna) series access point has joined the controller, you can configure it as an OfficeExtend access point.

Note Configuring LSC is not a requirement but an option. The OfficeExtend access points do not support LSC.

This section contains the following topics:

- Configuring OfficeExtend Access Points (GUI), page 9-62
- Configuring OfficeExtend Access Points (CLI), page 9-65

Configuring OfficeExtend Access Points (GUI)

Step 1 Choose **Wireless** to open the All APs page.

Step 2 Click the name of the desired access point to open the All APs > Details page.

Step 3 Enable FlexConnect on the access point as follows:

a. In the **General** tab, choose **FlexConnect** from the AP Mode drop-down list to enable FlexConnect for this access point.

Note For more information on FlexConnect, see Chapter 16, "Configuring FlexConnect."

Step 4 Configure one or more controllers for the access point as follows:

a. Click the **High Availability** tab.

b. Enter the name and IP address of the primary controller for this access point in the Primary Controller Name and Management IP Address text boxes.

Note You must enter both the name and IP address of the controller. Otherwise, the access point cannot join this controller.

c. If desired, enter the name and IP address of a secondary or tertiary controller (or both) in the corresponding Controller Name and Management IP Address text boxes.

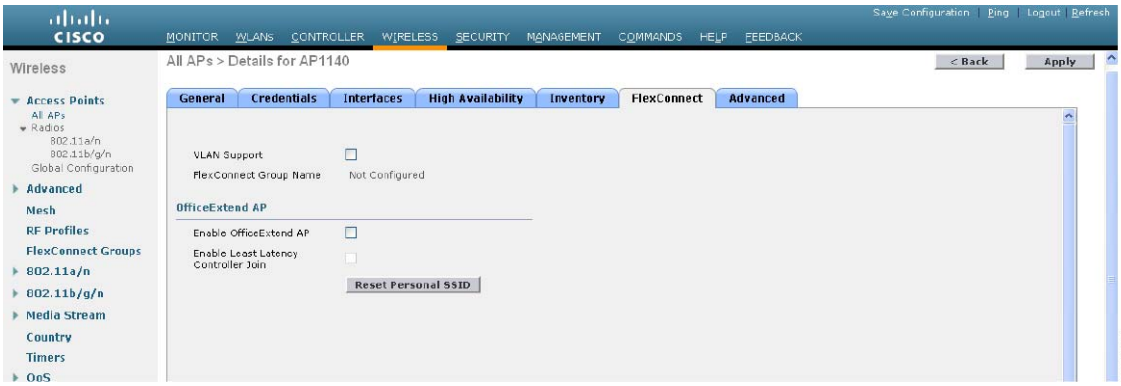
d. Click **Apply** to commit your changes. The access point reboots and then rejoins the controller.

Note The names and IP addresses must be unique for the primary, secondary, and tertiary controllers.

Step 5 Enable OfficeExtend access point settings as follows:

a. Click the **FlexConnect** tab.

Figure 9-34 All APs > Details > Details for FlexConnect



b. Select the **Enable OfficeExtend AP** check box to enable the OfficeExtend mode for this access point. The default value is selected.

Unselecting this check box disables OfficeExtend mode for this access point. It does not undo all of the configuration settings on the access point. If you want to clear the access point's configuration and return it to the factory-default settings, enter **clear ap config** *Cisco_AP* on the controller CLI. If you want to clear only the access point's personal SSID, click **Reset Personal SSID**.

Note Rogue detection is disabled automatically when you enable the OfficeExtend mode for an access point. However, you can enable or disable rogue detection for a specific access point by selecting the **Rogue Detection** check box on the All APs > Details for (Advanced) page. Rogue detection is disabled by default for OfficeExtend access points because these access points, which are deployed in a home environment, are likely to detect a large number of rogue devices. See the "Managing Rogue Devices" section on page 7-81 for more information on rogue detection.

Note DTLS data encryption is enabled automatically when you enable the OfficeExtend mode for an access point. However, you can enable or disable DTLS data encryption for a specific access point by selecting the **Data Encryption** check box on the All APs > Details for (Advanced) page. See the "Configuring Data Encryption" section on page 9-3 for more information on DTLS data encryption.

Note Telnet and SSH access are disabled automatically when you enable the OfficeExtend mode for an access point. However, you can enable or disable Telnet or SSH access for a specific access point by selecting the **Telnet** or **SSH** check box on the All APs > Details for (Advanced) page. See the "Troubleshooting Access Points Using Telnet or SSH" section on page 18-49 for more information on Telnet and SSH.

Note Link latency is enabled automatically when you enable the OfficeExtend mode for an access point. However, you can enable or disable link latency for a specific access point by selecting the **Enable Link Latency** check box on the All APs > Details for (Advanced) page. See the "Configuring Link Latency" section on page 9-105 for more information on this feature.

c. Select the **Enable Least Latency Controller Join** check box if you want the access point to choose the controller with the least latency when joining. Otherwise, leave this check box unselected, which is the default value. When you enable this feature, the access point calculates the time between the discovery request and discovery response and joins the Cisco 5500 Series Controller that responds first.

d. Click **Apply** to commit your changes.

The OfficeExtend AP text box on the All APs page shows which access points are configured as OfficeExtend access points.

Step 6 Configure a specific username and password for the OfficeExtend access point so that the user at home can log into the GUI of the OfficeExtend access point:

a. Click **Credentials** tab.

b. Select the **Over-ride Global Credentials** check box to prevent this access point from inheriting the global username, password, and enable password from the controller. The default value is unselected.

c. In the Username, Password, and Enable Password text boxes, enter the unique username, password, and enable password that you want to assign to this access point.

Note The information that you enter is retained across controller and access point reboots and if the access point joins a new controller.

d. Click **Apply** to commit your changes.

Note If you want to force this access point to use the controller's global credentials, unselect the **Over-ride Global Credentials** check box.

Step 7 Configure access to local GUI, LAN ports, and local SSID of the OfficeExtend access points:

a. Choose **WIRELESS > Access Points > Global Configuration** to open the Global Configuration page.

b. Under OEAP Config Parameters, select or unselect the **Disable Local Access** check box to enable or disable local access of the OfficeExtend access points.

Note By default, the **Disable Local Access** check box is unselected and therefore the Ethernet ports and personal SSIDs are enabled. This configuration does not affect remote LAN. The port is enabled only when you configure a remote LAN.

Step 8 Click **Save Configuration** to save your changes.

Step 9 If your controller supports only OfficeExtend access points, see the "Configuring RRM" section on page 13-5 for instructions on setting the recommended values for the DCA interval, channel scan duration, and neighbor packet frequency.

Configuring OfficeExtend Access Points (CLI)

Step 1 Enable FlexConnect on the access point by entering this command:

config ap mode flexconnect *Cisco_AP*

Note For more information on FlexConnect, see Chapter 16, "Configuring FlexConnect."

Step 2 Configure one or more controllers for the access point by entering one or all of these commands:

config ap primary-base *controller_name Cisco_AP controller_ip_address*

config ap secondary-base *controller_name Cisco_AP controller_ip_address*

config ap tertiary-base *controller_name Cisco_AP controller_ip_address*

Note You must enter both the name and IP address of the controller. Otherwise, the access point cannot join this controller.

Note The names and IP addresses must be unique for the primary, secondary, and tertiary controllers.

Step 3 Enable the OfficeExtend mode for this access point by entering this command:

config flexconnect office-extend {**enable** | **disable**} *Cisco_AP*

The default value is enabled. The **disable** parameter disables OfficeExtend mode for this access point. It does not undo all of the configuration settings on the access point. If you want to clear the access point's configuration and return it to the factory-default settings, enter this command:

clear ap config ***Cisco_AP***

If you want to clear only the access point's personal SSID, enter this command:

config flexconnect office-extend clear-personalssid-config *Cisco_AP.*

Note Rogue detection is disabled automatically when you enable the OfficeExtend mode for an access point. However, you can enable or disable rogue detection for a specific access point or for all access points using the **config rogue detection** {**enable** | **disable**} {*Cisco_AP* | **all**} command. Rogue detection is disabled by default for OfficeExtend access points because these access points, which are deployed in a home environment, are likely to detect a large number of rogue devices. See the "Managing Rogue Devices" section on page 7-81 for more information on rogue detection.

Note DTLS data encryption is enabled automatically when you enable the OfficeExtend mode for an access point. However, you can enable or disable DTLS data encryption for a specific access point or for all access points using the **config ap link-encryption** {**enable** | **disable**} {*Cisco_AP* | **all**} command. See the "Configuring Data Encryption" section on page 9-3 for more information on DTLS data encryption.

Note Telnet and SSH access are disabled automatically when you enable the OfficeExtend mode for an access point. However, you can enable or disable Telnet or SSH access for a specific access point using the **config ap** {**telnet** | **ssh**} {**enable** | **disable**} *Cisco_AP* command. See the "Troubleshooting Access Points Using Telnet or SSH" section on page 18-49 for more information on Telnet and SSH.

Note Link latency is enabled automatically when you enable the OfficeExtend mode for an access point. However, you can enable or disable link latency for a specific access point or for all access points currently associated to the controller using the **config ap link-latency** {**enable** | **disable**} {*Cisco_AP* | **all**} command. See the "Configuring Link Latency" section on page 9-105 for more information on this feature.

Step 4 Enable the access point to choose the controller with the least latency when joining by entering this command:

config flexconnect join min-latency {**enable** | **disable**} *Cisco_AP*

The default value is disabled. When you enable this feature, the access point calculates the time between the discovery request and discovery response and joins the Cisco 5500 Series Controller that responds first.

Step 5 Configure a specific username and password that users at home can enter to log into the GUI of the OfficeExtend access point by entering this command:

config ap mgmtuser add username *user* **password** *password* **enablesecret** *enable_password Cisco_AP*

The credentials that you enter in this command are retained across controller and access point reboots and if the access point joins a new controller.

Note If you want to force this access point to use the controller's global credentials, enter the **config ap mgmtuser delete** *Cisco_AP* command. The following message appears after you execute this command: "AP reverted to global username configuration."

Step 6 To configure access to the local network for the Cisco 600 Series OfficeExtend access points, enter the following command:

config network oeap-600 local-network {**enable** | **disable**}

When disabled, the local SSIDs, local ports are inoperative; and the console is not accessible. When reset, the default restores local access. This configuration does not affect the remote LAN configuration if configured on the access points.

Step 7 Configure the Dual R-LAN Ports feature, which allows the Ethernet port 3 of Cisco 600 Series OfficeExtend access points to operate as a remote LAN by entering this command:

config network oeap-600 dual-rlan-ports {**enable** | **disable**}

This configuration is global to the controller and is stored by the AP and the NVRAM variable. When this variable is set, the behavior of the remote LAN is changed. This feature supports different remote LANs per remote LAN port.

The remote LAN mapping is different depending on whether the default group or AP Groups is used:

- Default Group—If you are using the default group, a single remote LAN with an even numbered remote LAN ID is mapped to port 4. For example, a remote LAN with remote LAN ID 2 is mapped to port 4 (on the Cisco 600 OEAP). The remote LAN with an odd numbered remote LAN ID is mapped to port 3 (on the Cisco 600 OEAP). For example, a remote LAN with remote LAN ID 1 is mapped to port 3 (on the Cisco 600 OEAP).
- AP Groups—If you are using an AP group, the mapping to the OEAP-600 ports is determined by the order of the AP groups. To use an AP group, you must first delete all remote LANs and WLANs from the AP group leaving it empty. Then, add the two remote LANs to the AP group adding the port 3 AP remote LAN first, and the port 4 remote group second, followed by any WLANs.

Step 8 Save your changes by entering this command:

save config

Step 9 If your controller supports only OfficeExtend access points, see the "Configuring RRM" section on page 13-5 for instructions on setting the recommended value for the DCA interval.

Configuring a Personal SSID on an OfficeExtend Access Point

Step 1 Find the IP address of your OfficeExtend access point by doing one of the following:

- Log into your home router and look for the IP address of your OfficeExtend access point.
- Ask your company's IT professional for the IP address of your OfficeExtend access point.
- Use an application such as Network Magic to detect devices on your network and their IP addresses.

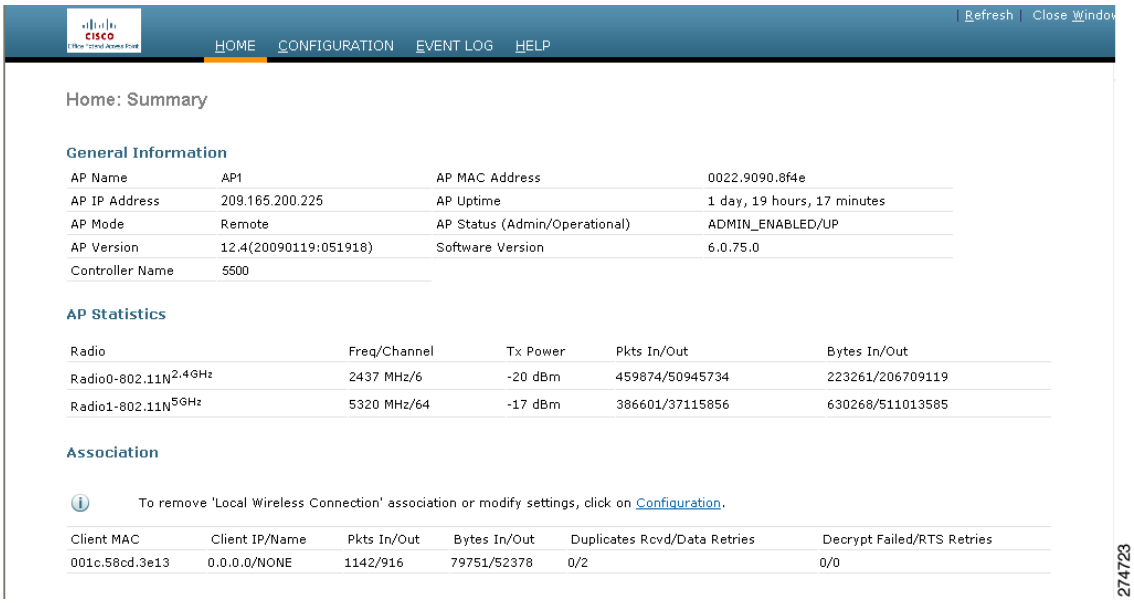
Step 2 With the OfficeExtend access point connected to your home router, enter the IP address of the OfficeExtend access point in the Address text box of your Internet browser and click **Go**.

Note Make sure that you are not connected to your company's network using a virtual private network (VPN) connection.

Step 3 When prompted, enter the username and password to log into the access point.

Step 4 On the OfficeExtend Access Point Welcome page, click **Enter**. The OfficeExtend Access Point Home page appears.

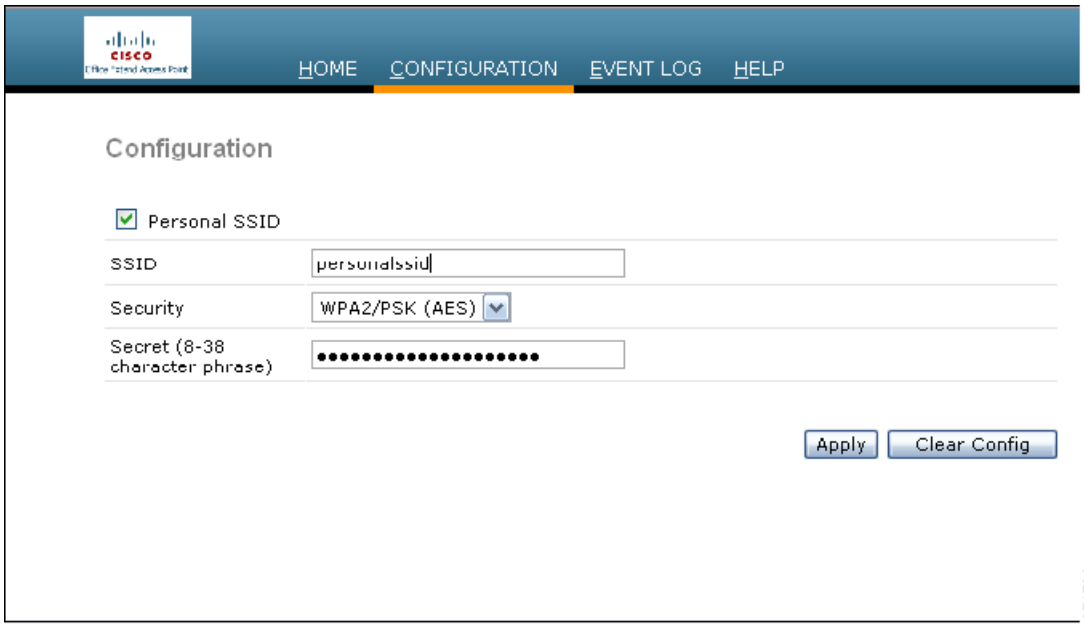
Figure 9-35 OfficeExtend Access Point Home Page



This page shows the access point name, IP address, MAC address, software version, status, channel, transmit power, and client traffic.

Step 5 Choose **Configuration** to open the Configuration page.

Figure 9-36 OfficeExtend Access Point Configuration Page



Step 6 Select the **Personal SSID** check box to enable this wireless connection. The default value is disabled.

Step 7 In the SSID text box, enter the personal SSID that you want to assign to this access point. This SSID is locally switched.

Note A controller with an OfficeExtend access point publishes only up to 15 WLANs to each connected access point because it reserves one WLAN for the personal SSID.

Step 8 From the Security drop-down list, choose **Open**, **WPA2/PSK (AES)**, or **104 bit WEP** to set the security type to be used by this access point.

Note If you choose WPA2/PSK (AES), make sure that the client is configured for WPA2/PSK and AES encryption.

Step 9 If you chose WPA2/PSK (AES) in Step 8, enter an 8- to 38-character WPA2 passphrase in the Secret text box. If you chose 104 bit WEP, enter a 13-character ASCII key in the Key text box.

Step 10 Click **Apply** to commit your changes.

Note If you want to use the OfficeExtend access point for another application, you can clear this configuration and return the access point to the factory-default settings by clicking **Clear Config**. You can also clear the access point's configuration from the controller CLI by entering the **clear ap config** *Cisco_AP* command.

Viewing OfficeExtend Access Point Statistics

Use these commands to view information about the OfficeExtend access points on your network:

- See a list of all OfficeExtend access points by entering this command:

  show flexconnect office-extend summary

  Information similar to the following appears:

```
Summary of OfficeExtend AP
AP Name      Ethernet MAC       Encryption  Join-Mode   Join-Time
-----------  -----------------  ----------  ----------  ---------------------------
AP1130      00:22:90:e3:37:70   Enabled     Latency     Sun Jan  4 21:46:07 2009
AP1140      01:40:91:b5:31:70   Enabled     Latency      Sat Jan  3 19:30:25 2009
```

- See the link delay for OfficeExtend access points by entering this command:

  show flexconnect office-extend latency

  Information similar to the following appears:

```
Summary of OfficeExtend AP link latency
AP Name   Status       Current   Maximum   Minimum
---------  -----------  ----------  ---------  ---------
AP1130      Enabled     15 ms      45 ms      12 ms
AP1140      Enabled     14 ms     179 ms      12 ms
```

- See the encryption state of all access points or a specific access point by entering this command:

  show ap link-encryption {**all** | *Cisco_AP*}

  Information similar to the following appears:

```
                Encryption Dnstream  Upstream Last
```

```
AP Name         State       Count      Count    Update
--------------  ----------- ---------  ---------  ---------
AP1130          En          112       1303       23:49
AP1140          En          232      2146       23:49
             auth err: 198 replay err: 0
AP1250          En          0         0          Never
AP1240          En          6191    15011      22:13
```

This command also shows authentication errors, which track the number of integrity check failures, and replay errors, which track the number of times that the access point receives the same packet. See the data plane status for all access points or a specific access point by entering this command:

show ap data-plane {**all** | *Cisco_AP*}

Information similar to the following appears:

```
                   Min Data           Data           Max Data    Last
AP Name            Round Trip       Round Trip       Round Trip     Update
-----------------  --------------  --------------  -------------- ---------
AP1130               0.012s         0.014s          0.020s       13:46:23
AP1140               0.012s         0.017s          0.111s       13:46:46
```

- To join the statistics for the OfficeExtend access points, see "Viewing Access Point Join Information (CLI)" section on page 9-41.

Additional References

- To troubleshoot OfficeExtend access points, see Appendix 18, "Troubleshooting".

Using Cisco Workgroup Bridges

This section contains the following topics:

- Information About Cisco Workgroup Bridges, page 9-70
- Guidelines and Limitations, page 9-71
- WGB Configuration Example, page 9-73
- Viewing the Status of Workgroup Bridges, page 9-73
- Debugging WGB Issues (CLI), page 9-75

Information About Cisco Workgroup Bridges

A workgroup bridge (WGB) is a mode that can be configured on an autonomous IOS access point to provide wireless connectivity to a lightweight access point on behalf of clients that are connected by Ethernet to the WGB access point. A WGB connects a wired network over a single wireless segment by learning the MAC addresses of its wired clients on the Ethernet interface and reporting them to the lightweight access point using Internet Access Point Protocol (IAPP) messaging. The WGB provides wireless access connectivity to wired clients by establishing a single wireless connection to the lightweight access point. The lightweight access point treats the WGB as a wireless client. See the example in Figure 9-37.

Figure 9-37 WGB Example

Note If the lightweight access point fails, the WGB attempts to associate to another access point.

Guidelines and Limitations

- The WGB can be any autonomous access point that supports the workgroup bridge mode and is running Cisco IOS Release 12.4(3g)JA or later releases (on 32-MB access points) or Cisco IOS Release 12.3(8)JEB or later releases (on 16-MB access points). These access points include the AP1120, AP1121, AP1130, AP1231, AP1240, and AP1310. Cisco IOS releases prior to 12.4(3g)JA and 12.3(8)JEB are not supported.

  Note If your access point has two radios, you can configure only one for workgroup bridge mode. This radio is used to connect to the lightweight access point. We recommend that you disable the second radio.

  Enable the workgroup bridge mode on the WGB as follows:

  – On the WGB access point GUI, choose **Workgroup Bridge** for the role in radio network on the Settings > Network Interfaces page.

  – On the WGB access point CLI, enter the **station-role workgroup-bridge command.**

  Note See the sample WGB access point configuration in the "WGB Configuration Example" section on page 9-73.

- The WGB can associate only to lightweight access points.
- Perform one of the following to enable client mode on the WGB:
  – On the WGB access point GUI, choose **Disabled** for the Reliable Multicast to WGB parameter.
  – On the WGB access point CLI, enter the **no infrastructure client** command.

  Note VLANs are not supported for use with WGBs.

Note See the sample WGB access point configuration in the "WGB Configuration Example" section on page 9-73.

- These features are supported for use with a WGB:
  - Guest N+1 redundancy
  - Local EAP
  - Open, WEP 40, WEP 128, CKIP, WPA+TKIP, WPA2+AES, LEAP, EAP-FAST, and EAP-TLS authentication modes
  - Cisco Centralized Key Management (CCKM)
- These features are not supported for use with a WGB:
  - FlexConnect
  - Idle timeout
  - Web authentication

  Note If a WGB associates to a web-authentication WLAN, the WGB is added to the exclusion list, and all of the WGB wired clients are deleted.

- The WGB supports a maximum of 20 wired clients. If you have more than 20 wired clients, use a bridge or another device.
- Wired clients connected to the WGB are not authenticated for security. Instead, the WGB is authenticated against the access point to which it associates. Therefore, we recommend that you physically secure the wired side of the WGB.
- With Layer 3 roaming, if you plug a wired client into the WGB network after the WGB has roamed to another controller (for example, to a foreign controller), the wired client's IP address displays only on the anchor controller, not on the foreign controller.
- If a wired client does not send traffic for an extended period of time, the WGB removes the client from its bridge table, even if traffic is continuously being sent to the wired client. As a result, the traffic flow to the wired client fails. To avoid the traffic loss, prevent the wired client from being removed from the bridge table by configuring the aging-out timer on the WGB to a large value using the following Cisco IOS commands on the WGB:

  ```
  configure terminal
  bridge bridge-group-number aging-time seconds
  exit
  end
  ```

  where *bridge-group-number* is a value between 1 and 255, and *seconds* is a value between 10 and 1,000,000 seconds. We recommend configuring the *seconds* parameter to a value greater than the wired client's idle period.
- When you delete a WGB record from the controller, all of the WGB wired clients' records are also deleted.
- Wired clients connected to a WGB inherit the WGB's QoS and AAA override attributes.
- These features are not supported for wired clients connected to a WGB:
  - MAC filtering
  - Link tests

  - Idle timeout

- To enable the WGB to communicate with the lightweight access point, create a WLAN and make sure that Aironet IE is enabled.
- Wired clients behind a WGB cannot connect to a DMZ/Anchor controller. To enable wired clients behind a WGB to connect to an anchor controller in a DMZ, you must enable VLANs in the WGB using the **config wgb vlan enable** command.
- If you have to apply ACL to WGB during run time, do not modify the ACL configuration for interface in the controller during run time. If you need to modify any ACLs, then you must diable all WLANs that are in the controller or disable both the 802.11a and 80.11b networks. Also, ensure that there are no clients associated and mapped to that interface and then you can modify the ACL settings.

WGB Configuration Example

The following is an example of the configuration of a WGB access point using static WEP with a 40-bit WEP key:

```
ap# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
ap(config)# dot11 ssid WGB_with_static_WEP
ap(config-ssid)# authentication open
ap(config-ssid)# guest-mode
ap(config-ssid)# exit
ap(config)# interface  dot11Radio 0
ap(config)# station-role workgroup-bridge
ap(config-if)# encry mode wep 40
ap(config-if)# encry key 1 size 40 0 1234567890
ap(config-if)# ssid WGB_with_static_WEP
ap(config-if)# end
```

Verify that the WGB is associated to an access point by entering this command on the WGB:

show dot11 association

Information similar to the following appears:

```
ap# show dot11 associations
802.11 Client Stations on Dot11Radio0:
SSID [FCVTESTING] :
MAC Address    IP address      Device        Name            Parent         State
000b.8581.6aee 10.11.12.1      WGB-client    map1            -              Assoc
ap#
```

Viewing the Status of Workgroup Bridges

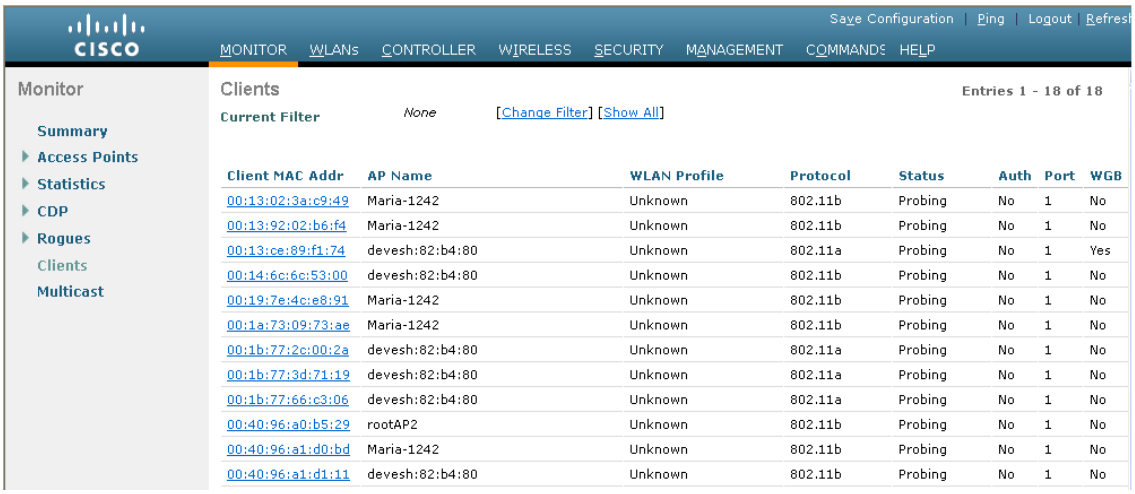
This section contains the following topics:

- Viewing the Status of Workgroup Bridges (GUI), page 9-73
- Viewing the Status of Workgroup Bridges (CLI), page 9-74

Viewing the Status of Workgroup Bridges (GUI)

Step 1 Choose **Monitor** > **Clients** to open the Clients page.

Figure 9-38 Clients Page



The WGB text box on the right side of the page indicates whether any of the clients on your network are workgroup bridges.

Step 2 Click the MAC address of the desired client. The Clients > Detail page appears.

The Client Type text box under Client Properties shows "WGB" if this client is a workgroup bridge, and the Number of Wired Client(s) text box shows the number of wired clients that are connected to this WGB.

Step 3 See the details of any wired clients that are connected to a particular WGB as follows:

a. Click **Back** on the Clients > Detail page to return to the Clients page.

b. Hover your cursor over the blue drop-down arrow for the desired WGB and choose **Show Wired Clients**. The WGB Wired Clients page appears.

Note If you want to disable or remove a particular client, hover your cursor over the blue drop-down arrow for the desired client and choose **Remove** or **Disable**, respectively.

c. Click the MAC address of the desired client to see more details for this particular client. The Clients > Detail page appears.

The Client Type text box under Client Properties shows "WGB Client," and the rest of the text boxes on this page provide additional information for this client.

Viewing the Status of Workgroup Bridges (CLI)

Step 1 See any WGBs on your network by entering this command:

show wgb summary

Information similar to the following appears:

```
Number of WGBs..................................... 1

MAC Address        IP Address AP Name  Status  WLAN  Auth  Protocol  Clients
-----------------  ---------  -------- ------  ----  ----- --------- --------
```

```
00:0d:ed:dd:25:82  10.24.8.73      a1   Assoc   3     Yes   802.11b   1
```

Step 2 See the details of any wired clients that are connected to a particular WGB by entering this command:

show wgb detail *wgb_mac_address*

Information similar to the following appears:

```
Number of wired client(s): 1

MAC Address         IP Address AP Name  Mobility   WLAN   Auth
------------------- ---------- -------- ---------  -----  -----
00:0d:60:fc:d5:0b   10.24.8.75   a1      Local      3     Yes
```

Debugging WGB Issues (CLI)

- Enable debugging for IAPP messages, errors, and packets by entering these commands:
  - **debug iapp all enable**—Enables debugging for IAPP messages.
  - **debug iapp error enable**—Enables debugging for IAPP error events.
  - **debug iapp packet enable**—Enables debugging for IAPP packets.
- Debug an roaming issue by entering this command:

  debug mobility handoff enable
- Debug an IP assignment issue when DHCP is used by entering these commands:
  - **debug dhcp message enable**
  - **debug dhcp packet enable**
- Debug an IP assignment issue when static IP is used by entering these commands:
  - **debug dot11 mobile enable**
  - **debug dot11 state enable**

Configuring Non-Cisco Workgroup Bridges

This section contains the following topics:

- Information About Non-Cisco Workgroup Bridges, page 9-75
- Guidelines and Limitations, page 9-76

Information About Non-Cisco Workgroup Bridges

When a Cisco workgroup bridge (WGB) is used, the WGB informs the access points of all the clients that it is associated with. The controller is aware of the clients associated with the access point. When non-Cisco WGBs are used, the controller has no information about the IP address of the clients on the wired segment behind the WGB. Without this information, the controller drops the following types of messages:

- ARP REQ from the distribution system for the WGB client

- ARP RPLY from the WGB client
- DHCP REQ from the WGB client
- DHCP RPLY for the WGB client

Guidelines and Limitations

- Starting in release 7.0.116.0, the controller can accommodate non-Cisco WGBs so that the controller can forward ARP, DHCP, and data traffic to and from the wired clients behind workgroup bridges by enabling the passive client feature. To configure your controller to work with non-Cisco WGBs, you must enable the passive client feature so that all traffic from the wired clients is routed through the WGB to the access point. All traffic from the wired clients is routed through the work group bridge to the access point.

  To know more about how to configure the controller to use passive clients, see the "Configuring Passive Clients" section on page 74.
- The following restrictions apply to non-Cisco WGB:
  - Only Layer 2 roaming is supported for WGB devices.
  - Layer 3 security (web authentication) is not support for WGB clients.
  - Visibility of wired hosts behind a WGB on a controller is not supported because the non-Cisco WGB device performs MAC hiding. Cisco WGB supports IAPP.
  - ARP poisoning detection does not work on a WLAN when the flag is enabled.
  - VLAN select is not supported for WGB clients.
  - Some third-party WGBs need to operate in non-DHCP relay mode. If problems occur with the DHCP assignment on devices behind the non-Cisco WGB, use the **config dhcp proxy disable** and **config dhcp proxy disable bootp-broadcast disable** commands.

    The default state is DHCP proxy enabled. The best combination depends on the third-party characteristics and configuration.
- When a WGB wired client leaves a multicast group, the downstream multicast traffic to other WGB wired clients is interrupted briefly.
- If you have clients that use PC virtualization software like VMware, you must enable this feature.

Note We have tested multiple third-party devices for compatibility but cannot ensure that all non-Cisco devices work. Support for any interaction or configuration details on the third-party device should be discussed with the device manufacturer.

- You must enable the passive client functionality for all non Cisco workgroup bridges. For more information, see the "Configuring Passive Clients" section on page 74.
- You might need to use the following commands to configure DHCP on clients:
  - Disable DHCP proxy by using the **config dhcp proxy disable** command.
  - Enable DHCP boot broadcast by using the **tconfig dhcp proxy disable bootp-broadcast enable** command.

Configuring Backup Controllers

This section contains the following topics:

- Information About Configuring Backup Controllers, page 9-77
- Guidelines and Limitations, page 9-77
- Configuring Backup Controllers, page 9-78

Information About Configuring Backup Controllers

A single controller at a centralized location can act as a backup for access points when they lose connectivity with the primary controller in the local region. Centralized and regional controllers do not need to be in the same mobility group. In controller software release 4.2 or later releases, you can specify a primary, secondary, and tertiary controller for specific access points in your network. Using the controller GUI or CLI, you can specify the IP addresses of the backup controllers, which allows the access points to fail over to controllers outside of the mobility group.

Guidelines and Limitations

- In controller software release 5.0 or later releases, you can also configure primary and secondary backup controllers (which are used if primary, secondary, or tertiary controllers are not specified or are not responsive) for all access points connected to the controller as well as various timers, including heartbeat timers and discovery request timers. To reduce the controller failure detection time, you can configure the fast heartbeat interval (between the controller and the access point) with a smaller timeout value. When the fast heartbeat timer expires (at every heartbeat interval), the access point determines if any data packets have been received from the controller within the last interval. If no packets have been received, the access point sends a fast echo request to the controller.
- You can configure the fast heartbeat timer only for access points in local and flexconnect modes.
- The access point maintains a list of backup controllers and periodically sends primary discovery requests to each entry on the list. When the access point receives a new discovery response from a controller, the backup controller list is updated. Any controller that fails to respond to two consecutive primary discovery requests is removed from the list. If the access point's local controller fails, it chooses an available controller from the backup controller list in this order: primary, secondary, tertiary, primary backup, and secondary backup. The access point waits for a discovery response from the first available controller in the backup list and joins the controller if it receives a response within the time configured for the primary discovery request timer. If the time limit is reached, the access point assumes that the controller cannot be joined and waits for a discovery response from the next available controller in the list.
- When an access point's primary controller comes back online, the access point disassociates from the backup controller and reconnects to its primary controller. The access point falls back to its primary controller and not to any secondary controller for which it is configured. For example, if an access point is configured with primary, secondary, and tertiary controllers, it fails over to the tertiary controller when the primary and secondary controllers become unresponsive and waits for the primary controller to come back online so that it can fall back to the primary controller. The access point does not fall back from the tertiary controller to the secondary controller if the secondary controller comes back online; it stays connected to the tertiary controller until the primary controller comes back up.

- If you inadvertently configure a controller that is running software release 5.2 or later releases with a failover controller that is running a different software release (such as 4.2, 5.0, or 5.1), the access point might take a long time to join the failover controller because the access point starts the discovery process in CAPWAP and then changes to LWAPP discovery.

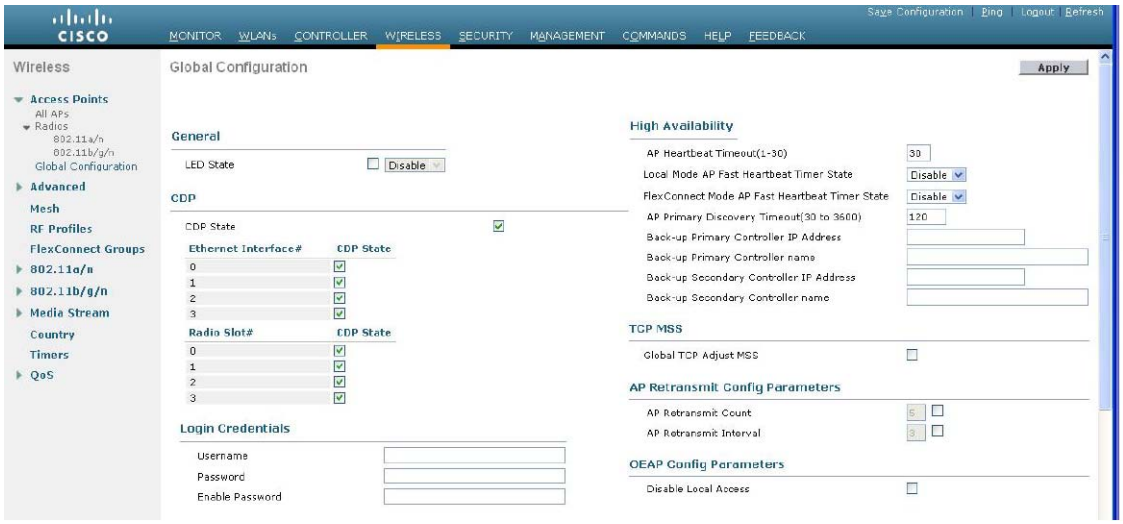
Configuring Backup Controllers

- Configuring Backup Controllers (GUI), page 9-78
- Configuring Backup Controllers (CLI), page 9-79

Configuring Backup Controllers (GUI)

Step 1 Choose **Wireless > Access Points > Global Configuration** to open the Global Configuration page.

Figure 9-39 Global Configuration Page



Step 2 From the Local Mode AP Fast Heartbeat Timer State drop-down list, choose **Enable** to enable the fast heartbeat timer for access points in local mode or choose **Disable** to disable this timer. The default value is Disable.

Step 3 If you chose Enable in Step 2, enter the Local Mode AP Fast Heartbeat Timeout text box to configure the fast heartbeat timer for access points in local mode. Specifying a small heartbeat interval reduces the amount of time it takes to detect a controller failure.

The range for the AP Fast Heartbeat Timeout value for Cisco Flex 7500 Controllers is 10–15 (inclusive) and is 1–10 (inclusive) for other controllers. The default value for the heartbeat timeout for Cisco Flex 7500 Controllers is 10. The default value for other controllers is 1 second.

Step 4 .From the FlexConnect Mode AP Fast Heartbeat Timer State drop-down list, choose **Enable** to enable the fast heartbeat timer for FlexConnect access points or choose **Disable** to disable this timer. The default value is Disable.

Step 5 If you enable FlexConnect fast heartbeat, enter the FlexConnect Mode AP Fast Heartbeat Timeout value in the FlexConnect Mode AP Fast Heartbeat Timeout text box. Specifying a small heartbeat interval reduces the amount of time it takes to detect a controller failure.

The range for the FlexConnect Mode AP Fast Heartbeat Timeout value for Cisco Flex 7500 Controllers is 10–15 (inclusive) and is 1–10 for other controllers. The default value for the heartbeat timeout for Cisco Flex 7500 Controllers is 10. The default value for other controllers is 1 second.

Step 6 In the AP Primary Discovery Timeout text box, a value between 30 and 3600 seconds (inclusive) to configure the access point primary discovery request timer. The default value is 120 seconds.

Step 7 If you want to specify a primary backup controller for all access points, enter the IP address of the primary backup controller in the Back-up Primary Controller IP Address text box and the name of the controller in the Back-up Primary Controller Name text box.

Note The default value for the IP address is 0.0.0.0, which disables the primary backup controller.

Step 8 If you want to specify a secondary backup controller for all access points, enter the IP address of the secondary backup controller in the Back-up Secondary Controller IP Address text box and the name of the controller in the Back-up Secondary Controller Name text box.

Note The default value for the IP address is 0.0.0.0, which disables the secondary backup controller.

Step 9 Click **Apply** to commit your changes.

Step 10 Configure primary, secondary, and tertiary backup controllers for a specific access point as follows:

a. Choose **Access Points > All APs** to open the All APs page.

b. Click the name of the access point for which you want to configure primary, secondary, and tertiary backup controllers.

c. Choose the **High Availability** tab to open the All APs > Details for (High Availability) page.

d. If desired, enter the name and IP address of the primary controller for this access point in the Primary Controller text boxes.

Note Entering an IP address for the backup controller is optional in this step and the next two steps. If the backup controller is outside the mobility group to which the access point is connected (the primary controller), then you need to provide the IP address of the primary, secondary, or tertiary controller, respectively. The controller name and IP address must belong to the same primary, secondary, or tertiary controller. Otherwise, the access point cannot join the backup controller.

e. If desired, enter the name and IP address of the secondary controller for this access point in the Secondary Controller text boxes.

f. If desired, enter the name and IP address of the tertiary controller for this access point in the Tertiary Controller text boxes.

g. Click **Apply** to commit your changes.

Step 11 Click **Save Configuration** to save your changes.

Configuring Backup Controllers (CLI)

Step 1 Configure a primary controller for a specific access point by entering this command:

config ap primary-base *controller_name Cisco_AP* [*controller_ip_address*]

Note The *controller_ip_address* parameter in this command and the next two commands is optional. If the backup controller is outside the mobility group to which the access point is connected (the primary controller), then you need to provide the IP address of the primary, secondary, or tertiary controller, respectively. In each command, the *controller_name* and *controller_ip_address* must belong to the same primary, secondary, or tertiary controller. Otherwise, the access point cannot join the backup controller.

Step 2 Configure a secondary controller for a specific access point by entering this command:

config ap secondary-base *controller_name Cisco_AP* [*controller_ip_address*]

Step 3 Configure a tertiary controller for a specific access point by entering this command:

config ap tertiary-base *controller_name Cisco_AP* [*controller_ip_address*]

Step 4 Configure a primary backup controller for all access points by entering this command:

config advanced backup-controller primary *backup_controller_name backup_controller_ip_address*

Step 5 Configure a secondary backup controller for all access points by entering this command:

config advanced backup-controller secondary *backup_controller_name backup_controller_ip_address*

Note To delete a primary or secondary backup controller entry, enter *0.0.0.0* for the controller IP address.

Step 6 Enable or disable the fast heartbeat timer for local or FlexConnect access points by entering this command:

config advanced timers ap-fast-heartbeat {**local** | **flexconnect** | **all**} {**enable** | **disable**} *interval*

where **all** is both local and FlexConnect access points, and *interval* is a value between 1 and 10 seconds (inclusive). Specifying a small heartbeat interval reduces the amount of time that it takes to detect a controller failure. The default value is disabled.Configure the access point heartbeat timer by entering this command:

config advanced timers ap-heartbeat-timeout *interval*

where *interval* is a value between 1 and 30 seconds (inclusive). This value should be at least three times larger than the fast heartbeat timer. The default value is 30 seconds.

Caution Do not enable the fast heartbeat timer with the high latency link. If you have to enable the fast heartbeat timer, the timer value must be greater than the latency.

Step 7 Configure the access point primary discovery request timer by entering this command:

config advanced timers ap-primary-discovery-timeout *interval*

where *interval* is a value between 30 and 3600 seconds. The default value is 120 seconds.

Step 8 Configure the access point discovery timer by entering this command:

config advanced timers ap-discovery-timeout *interval*

where *interval* is a value between 1 and 10 seconds (inclusive). The default value is 10 seconds.

Step 9 Configure the 802.11 authentication response timer by entering this command:

config advanced timers auth-timeout *interval*

where *interval* is a value between 10 and 600 seconds (inclusive). The default value is 10 seconds.

Step 10 Save your changes by entering this command:

save config

Step 11 See an access point's configuration by entering these commands:

- **show ap config general** *Cisco_AP*
- **show advanced backup-controller**
- **show advanced timers**

Information similar to the following appears for the **show ap config general** *Cisco_AP* command:

```
Cisco AP Identifier.............................. 1
Cisco AP Name.................................... AP5
Country code..................................... US  - United States
Regulatory Domain allowed by Country............. 802.11bg:-AB    802.11a:-AB
AP Country code.................................. US  - United States
AP Regulatory Domain............................. 802.11bg:-A    802.11a:-N
Switch Port Number .............................. 1
MAC Address...................................... 00:13:80:60:48:3e
IP Address Configuration......................... DHCP
IP Address....................................... 1.100.163.133
...
Primary Cisco Switch Name....................... 1-4404
Primary Cisco Switch IP Address.................. 2.2.2.2
Secondary Cisco Switch Name...................... 1-4404
Secondary Cisco Switch IP Address................ 2.2.2.2
Tertiary Cisco Switch Name....................... 2-4404
Tertiary Cisco Switch IP Address................. 1.1.1.4
...
```

Information similar to the following appears for the **show advanced backup-controller** command:

```
AP primary Backup Controller .................... controller1 10.10.10.10
AP secondary Backup Controller ............... 0.0.0.0
```

Information similar to the following appears for the **show advanced timers** command:

```
Authentication Response Timeout (seconds)........ 10
Rogue Entry Timeout (seconds).................... 1300
AP Heart Beat Timeout (seconds).................. 30
AP Discovery Timeout (seconds)................... 10
AP Local mode Fast Heartbeat (seconds)........... 10 (enable)
AP flexconnect mode Fast Heartbeat (seconds)..... disable
AP Primary Discovery Timeout (seconds)........... 120
```

Configuring Failover Priority for Access Points

This section contains the following topics:

- Information About Configuring Failover Priority for Access Points, page 9-82
- Guidelines and Limitations, page 9-82
- Configuring Failover Priority for Access Points, page 9-82

Information About Configuring Failover Priority for Access Points

Each controller has a defined number of communication ports for access points. When multiple controllers with unused access point ports are deployed on the same network and one controller fails, the dropped access points automatically poll for unused controller ports and associate with them.

Guidelines and Limitations

- In controller software releases prior to 5.1, the backup controllers accept association requests in the order that the requests are received until all the ports are in use. As a result, the probability of an access point finding an open port on a backup controller is determined by where in the association request queue it is after the controller failure.
- In controller software release 5.1 or later releases, you can configure your wireless network so that the backup controller recognizes a join request from a higher-priority access point and if necessary disassociates a lower-priority access point as a means to provide an available port.
- Failover priority is not in effect during the regular operation of your wireless network. It takes effect only if there are more association requests after a controller failure than there are available backup controller ports.
- To configure this feature, you must enable failover priority on your network and assign priorities to the individual access points.
- By default, all access points are set to priority level 1, which is the lowest priority level. Therefore, you need to assign a priority level only to those access points that warrant a higher priority.

Configuring Failover Priority for Access Points

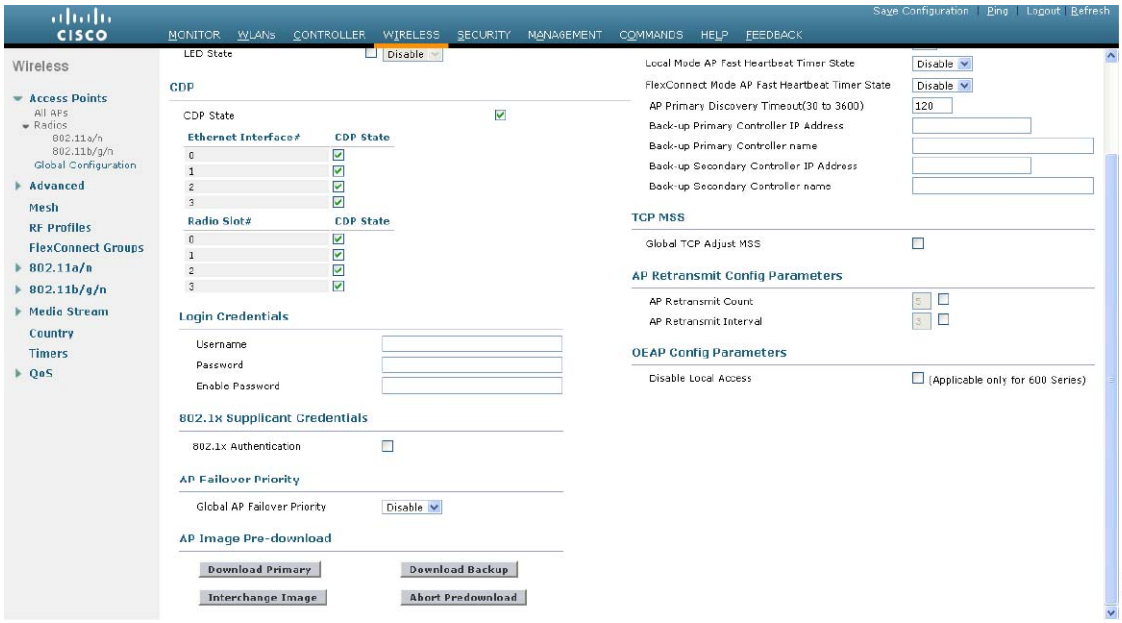
This section contains the following topics:

- Configuring Failover Priority for Access Points (GUI), page 9-82
- Configuring Failover Priority for Access Points (CLI), page 9-83
- Viewing Failover Priority Settings (CLI), page 9-84

Configuring Failover Priority for Access Points (GUI)

Step 1 Choose **Wireless > Access Points > Global Configuration** to open the Global Configuration page.

Figure 9-40 Global Configuration Page



Step 2 From the Global AP Failover Priority drop-down list, choose **Enable** to enable access point failover priority or choose **Disable** to disable this feature and turn off any access point priority assignments. The default value is Disable.

Step 3 Click **Apply** to commit your changes.

Step 4 Click **Save Configuration** to save your changes.

Step 5 Choose **Wireless** > **Access Points** > **All APs** to open the All APs page.

Step 6 Click the name of the access point for which you want to configure failover priority.

Step 7 Choose the **High Availability** tab. The All APs > Details for (High Availability) page appears.

Step 8 From the AP Failover Priority drop-down list, choose one of the following options to specify the priority of the access point:

- **Low**—Assigns the access point to the level 1 priority, which is the lowest priority level. This is the default value.
- **Medium**—Assigns the access point to the level 2 priority.
- **High**—Assigns the access point to the level 3 priority.
- **Critical**—Assigns the access point to the level 4 priority, which is the highest priority level.

Step 9 Click **Apply** to commit your changes.

Step 10 Click **Save Configuration** to save your changes.

Configuring Failover Priority for Access Points (CLI)

Step 1 Enable or disable access point failover priority by entering this command:

config network ap-priority {**enable** | **disable**}

Step 2 Specify the priority of an access point by entering this command:

config ap priority {**1** | **2** | ***3*** | **4**} *Cisco_AP*

where 1 is the lowest priority level and 4 is the highest priority level. The default value is 1.

Step 3 Save your changes by entering this command:

save config

Viewing Failover Priority Settings (CLI)

- Confirm whether access point failover priority is enabled on your network by entering this command:

  show network summary

  Information similar to the following appears:

```
RF-Network Name............................. mrf
Web Mode.................................... Enable
Secure Web Mode............................. Enable
Secure Web Mode Cipher-Option High.......... Disable
Secure Shell (ssh).......................... Enable
Telnet...................................... Enable
Ethernet Multicast Mode..................... Disable
Ethernet Broadcast Mode..................... Disable
IGMP snooping............................... Disabled
IGMP timeout................................ 60 seconds
User Idle Timeout........................... 300 seconds
ARP Idle Timeout............................ 300 seconds
Cisco AP Default Master..................... Disable
AP Join Priority.......................... Enabled
...
```

- See the failover priority for each access point by entering this command:

  show ap summary

  Information similar to the following appears:

```
Number of APs.................................. 2
Global AP User Name............................ user
Global AP Dot1x User Name...................... Not Configured

AP Name  Slots  AP Model           Ethernet MAC       Location   Port Country Priority
-------  -----  ------------------ -----------------  ---------  ---- ------- -------
ap:1252  2      AIR-LAP1252AG-A-K9 00:1b:d5:13:39:74  hallway 6  1    US      1
ap:1121  1      AIR-LAP1121G-A-K9  00:1b:d5:a9:ad:08  reception  1    US      3
```

To see the summary of a specific access point, you can specify the access point name. You can also use wildcard searches when filtering for access points.

Configuring Access Point Retransmission Interval and Retry Count

This section contains the following topics:

- Information About Configuring Access Point Retransmission Interval and Retry Count, page 9-85

- Guidelines and Limitations, page 9-85
- Configuring the Access Point Retransmission Interval and Retry Count, page 9-85

Information About Configuring Access Point Retransmission Interval and Retry Count

The controller and the access points exchange packets using the CAPWAP reliable transport protocol. For each request, a response is defined. This response is used to acknowledge the receipt of the request message. Response messages are not explicitly acknowledged; therefore, if a response message is not received, the original request message is retransmitted after the retransmit interval. If the request is not acknowledged after a maximum number of retransmissions, the session is closed and the access points reassociate with another controller.

Guidelines and Limitations

- You can configure the retransmission intervals and retry count both at a global as well as a specific access point level. A global configuration applies these configuration parameters to all the access points. That is, the retransmission interval and the retry count are uniform for all access points. Alternatively, when you configure the retransmission level and retry count at a specific access point level, the values are applied to that particular access point. The access point specific configuration has a higher precedence than the global configuration.
- Retransmission intervals and the retry count do not apply for mesh access point.

Configuring the Access Point Retransmission Interval and Retry Count

- Configuring the Access Point Retransmission Interval and Retry Count (GUI), page 9-85
- Configuring the Access Point Retransmission Interval and Retry Count (CLI), page 9-86

Configuring the Access Point Retransmission Interval and Retry Count (GUI)

You can configure the retransmission interval and retry count for all access points globally or a specific access point.

Global Configuration

Step 1 Choose **Wireless > Access Points > Global Configuration**.

Step 2 Choose one of the following options under the AP Transmit Config Parameters section:

- AP Retransmit Count—Enter the number of times you want the access point to retransmit the request to the controller. This parameter can take values between 3 and 8.
- AP Retransmit Interval—Enter the time duration between the retransmission of requests. This parameter can take values between 2 and 5.

Step 3 Click **Apply**.

Configuration for a Specific Access Point

Step 1 Choose **Wireless > Access Points > All APs**.

Step 2 Click on the AP Name link for the access point on which you want to set the values.

The **All APs > Details** page appears.

Step 3 Click the **Advanced Tab** to open the advanced parameters page.

Step 4 Choose one of the following parameters under the AP Transmit Config Parameters section:

- **AP Retransmit Count**—Enter the number of times that you want the access point to retransmit the request to the controller. This parameter can take values between 3 and 8.
- **AP Retransmit Interval**—Enter the time duration between the retransmission of requests. This parameter can take values between 2 and 5.

Step 5 Click **Apply**.

Configuring the Access Point Retransmission Interval and Retry Count (CLI)

You can configure the retransmission interval and retry count for all access points globally or a specific access point.

- Configure the retransmission interval and retry count for all access points globally by entering the this command:

  config ap retransmit {interval | count} *seconds* **all**

  The valid range for the **interval** parameter is between 3 and 8. The valid range for the **count** parameter is between 2 and 5.

- Configure the retransmission interval and retry count for a specific access point, by entering this command:

  config ap retransmit {interval | count} *seconds Cisco_AP*

  The valid range for the **interval** parameter is between 3 and 8. The valid range for the **count** parameter is between 2 and 5.

- See the status of the configured retransmit parameters on all or specific APs by entering this command:

  show ap retransmit all

```
(Cisco Controller) >show ap retransmit all
Global control packet retransmit interval: 5
Global control packet retransmit count: 6
AP Name             Retransmit Interval  Retransmit count
------------------  -------------------  -------------------
AP_1131                N/A(Mesh mode)       N/A(Mesh mode)
AP_cisco_              5                 4
abhes_1240             5                 6
```

Note Because retransmit and retry values cannot be set for access points in mesh mode, these values are displayed as N/A (not applicable).

- See the status of the configured retransmit parameters on a specific access point by entering this command:

show ap retransmit *Cisco_AP*

```
(Cisco Controller) >show ap retransmit cisco_AP1
Global control packet retransmit interval: 5
Global control packet retransmit count: 6
AP Name             Retransmit Interval  Retransmit count
-----------------   -------------------  -------------------
cisco_AP1              5                 6
(Cisco Controller) >
```

Configuring Country Codes

This section contains the following topics:

- Information About Configuring Country Codes, page 9-87
- Guidelines and Limitations, page 9-87
- Configuring Country Codes, page 9-88

Information About Configuring Country Codes

Controllers and access points are designed for use in many countries with varying regulatory requirements. The radios within the access points are assigned to a specific regulatory domain at the factory (such as -E for Europe), but the country code enables you to specify a particular country of operation (such as FR for France or ES for Spain). Configuring a country code ensures that each radio's broadcast frequency bands, interfaces, channels, and transmit power levels are compliant with country-specific regulations.

Guidelines and Limitations

- Generally, you configure one country code per controller, the one matching the physical location of the controller and its access points. However, controller software release 4.1 or later releases allows you to configure up to 20 country codes per controller. This multiple-country support enables you to manage access points in various countries from a single controller.
- Although the controller supports different access points in different regulatory domains (countries), it requires all radios in a single access point to be configured for the same regulatory domain. For example, you should not configure a Cisco 1231 access point's 802.11b/g radio for the US (-A) regulatory domain and its 802.11a radio for the Great Britain (-E) regulatory domain. Otherwise, the controller allows only one of the access point's radios to turn on, depending on which regulatory domain you selected for the access point on the controller. Therefore, make sure that the same country code is configured for both of the access point's radios.

  For a complete list of country codes supported per product, see http://tools.cisco.com/cse/prdapp/jsp/externalsearch.do?action=externalsearch&page=EXTERNAL_SEARCH

  or

  http://www.cisco.com/en/US/prod/collateral/wireless/ps5679/ps5861/product_data_sheet0900aecd80537b6a_ps6087_Products_Data_Sheet.html
- When the multiple-country feature is being used, all controllers that are going to join the same RF group must be configured with the same set of countries, configured in the same order.

- When multiple countries are configured and the RRM auto-RF feature is enabled, the RRM assigns the channels that are derived by performing a union of the allowed channels per the AP country code. The APs are assigned channels by the RRM based on their PID country code. APs are only allowed to use legal frequencies that match their PID country code. Ensure that your AP's country code is legal in the country that it is deployed.
- The access point can only operate on the channels for the countries that they are designed for.

Note If an access point was already set to a higher legal power level or is configured manually, the power level is limited only by the particular country to which that access point is assigned.

- The country list configured on the RF group leader determines what channels the members would operate on. This list is independent of what countries have been configured on the RF group members.

Configuring Country Codes

This section contains the following topics:

- Configuring Country Codes (GUI), page 9-88
- Configuring Country Codes (CLI), page 9-90

Configuring Country Codes (GUI)

Step 1 Follow these steps to disable the 802.11a and 802.11b/g networks as follows:

a. Choose **Wireless> 802.11a/n > Network**.

b. Unselect the **802.11a Network Status** check box.

c. Click **Apply** to commit your changes.

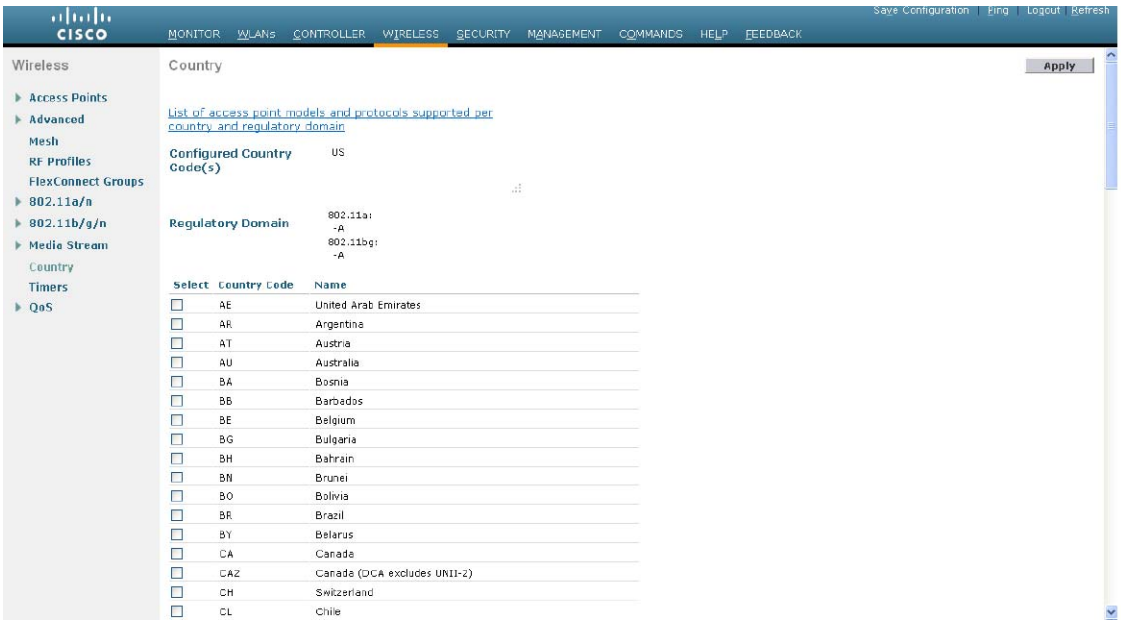
d. Choose **Wireless > 802.11b/g/n > Network**.

e. Unselect the **802.11b/g Network Status** check box.

f. Click **Apply** to commit your changes.

Step 2 Choose **Wireless > Country** to open the Country page.

Figure 9-41 Country Page



Step 3 Select the check box for each country where your access points are installed. If you selected more than one check box, a message appears indicating that RRM channels and power levels are limited to common channels and power levels.

Step 4 Click **OK** to continue or **Cancel** to cancel the operation.

Step 5 Click **Apply** to commit your changes.

If you selected multiple country codes in Step 3, each access point is assigned to a country.

Step 6 See the default country chosen for each access point and choose a different country if necessary as follows:

Note If you remove a country code from the configuration, any access points currently assigned to the deleted country reboot and when they rejoin the controller, they get re-assigned to one of the remaining countries if possible.

a. Perform one of the following:
   - Leave the 802.11a and 802.11b/g networks disabled.
   - Reenable the 802.11a and 802.11b/g networks and then disable only the access points for which you are configuring a country code. To disable an access point, choose **Wireless** > **Access Points** > **All APs**, click the link of the desired access point, choose **Disable** from the Status drop-down list, and click **Apply**.

b. Choose **Wireless** > **Access Points** > **All APs** to open the All APs page.

c. Click the link for the desired access point.

d. Choose the **Advanced** tab to open the All APs > Details for (Advanced) page.

   The default country for this access point appears in the Country Code drop-down list.

e. If the access point is installed in a country other than the one shown, choose the correct country from the drop-down list. The box contains only those country codes that are compatible with the regulatory domain of at least one of the access point's radios.

f. Click **Apply** to commit your changes.

g. Repeat these steps to assign all access points joined to the controller to a specific country.

h. Reenable any access points that you disabled in Step a.

Step 7 Reenable the 802.11a and 802.11b/g networks if you did not enable them in Step 6.

Step 8 Click **Save Configuration** to save your settings.

Configuring Country Codes (CLI)

Step 1 See a list of all available country codes by entering this command:

show country supported

Step 2 Disable the 802.11a and 802.11b/g networks by entering these commands:

config 802.11a disable network

config 802.11b disable network

Step 3 Configure the country codes for the countries where your access points are installed by entering this command:

config country *code1*[,*code2*,*code3*,...]

If you are entering more than one country code, separate each by a comma (for example, **config country US,CA,MX**). Information similar to the following appears:

```
Changing country code could reset channel configuration.
If running in RFM One-Time mode, reassign channels after this command.
Check customized APs for valid channel values after this command.
Are you sure you want to continue? (y/n) y
```

Step 4 Enter **Y** when prompted to confirm your decision. Information similar to the following appears:

```
Configured Country..................................... Multiple Countries:US,CA,MX
Auto-RF for this country combination is limited to common channels and power.
      KEY: * = Channel is legal in this country and may be configured manually.
           A = Channel is the Auto-RF default in this country.
           . = Channel is not legal in this country.
           C = Channel has been configured for use by Auto-RF.
           x = Channel is available to be configured for use by Auto-RF.
         (-) = Regulatory Domains allowed by this country.
------------:+-+-+-+-+-+-+-+-+-+-+-+-+-+-
802.11BG    :
Channels    :                   1 1 1 1 1
            : 1 2 3 4 5 6 7 8 9 0 1 2 3 4
------------:+-+-+-+-+-+-+-+-+-+-+-+-+-+-
 US (-AB)   : A * * * * A * * * * A . . .
 CA (-AB)   : A * * * * A * * * * A . . .
 MX (-NA)   : A * * * * A * * * * A . . .
 Auto-RF    : C x x x x C x x x x C . . .
------------:+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-
 802.11A    :                           1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1
Channels    : 3 3 3 4 4 4 4 4 5 5 6 6 0 0 0 1 1 2 2 2 3 3 4 4 5 5 6 6
--More-- or (q)uit
            : 4 6 8 0 2 4 6 8 2 6 0 4 0 4 8 2 6 0 4 8 2 6 0 9 3 7 1 5
```

```
------------:+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-
 US (-AB)   : . A . A . A . A A A A A * * * * * . . . * * * A A A A *
 CA (-ABN)  : . A . A . A . A A A A A * * * * * . . . * * * A A A A *
 MX (-N)    : . A . A . A . A A A A A . . . . . . . . . . . A A A A *
    Auto-RF : . C . C . C . C C C C C . . . . . . . . . . . C C C C x
```

Step 5 Verify your country code configuration by entering this command:

show country

Step 6 See the list of available channels for the country codes configured on your controller by entering this command:

show country channels

Information similar to the following appears:

```
Configured Country.......................... Multiple Countries:US,CA,MX
Auto-RF for this country combination is limited to common channels and power.
      KEY: * = Channel is legal in this country and may be configured manually.
           A = Channel is the Auto-RF default in this country.
           . = Channel is not legal in this country.
           C = Channel has been configured for use by Auto-RF.
           x = Channel is available to be configured for use by Auto-RF.
         (-) = Regulatory Domains allowed by this country.
------------:+-+-+-+-+-+-+-+-+-+-+-+-+-+-
802.11BG    :
Channels    :                   1 1 1 1 1
            : 1 2 3 4 5 6 7 8 9 0 1 2 3 4
------------:+-+-+-+-+-+-+-+-+-+-+-+-+-+-
 US (-AB)   : A * * * * A * * * * A . . .
 CA (-AB)   : A * * * * A * * * * A . . .
 MX (-NA)   : A * * * * A * * * * A . . .
 Auto-RF    : C x x x x C x x x x C . . .
------------:+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-
 802.11A    :                         1 1 1 1 1 1 1 1 1 1 1 1 1 1 1
Channels    : 3 3 3 4 4 4 4 4 5 5 6 6 0 0 0 1 1 2 2 2 3 3 4 4 5 5 6 6

            : 4 6 8 0 2 4 6 8 2 6 0 4 0 4 8 2 6 0 4 8 2 6 0 9 3 7 1 5
------------:+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-
 US (-AB)   : . A . A . A . A A A A A * * * * * . . . * * * A A A A *
 CA (-ABN)  : . A . A . A . A A A A A * * * * * . . . * * * A A A A *
 MX (-N)    : . A . A . A . A A A A A . . . . . . . . . . . A A A A *
    Auto-RF : . C . C . C . C C C C C . . . . . . . . . . . C C C C x
------------:+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-
```

Step 7 Save your settings by entering this command:

save config

Step 8 See the countries to which your access points have been assigned by entering this command:

To see a summary of specific access point you can specify the access point name. You can also use wildcard searches when filtering for access points.

show ap summary

Information similar to the following appears:

```
Number of APs.................................. 2

AP Name  Slots  AP Model          Ethernet MAC       Location          Port    Country
-------- ------ ----------------- -----------------  ----------------  ------- --------
ap1        2   AP1030            00:0b:85:5b:8e:c0  default location     1      US
ap2        2   AIR-AP1242AG-A-K9  00:14:1c:ed:27:fe  default location     1      US
```

Step 9 If you entered multiple country codes in Step 3, follow these steps to assign each access point to a specific country:

a. Perform one of the following:

- Leave the 802.11a and 802.11b/g networks disabled.
- Reenable the 802.11a and 802.11b/g networks and then disable only the access points for which you are configuring a country code. To Reenable the networks, enter these commands:

  config 802.11a enable network

  config 802.11b enable network

  To disable an access point, enter this command:

  config ap disable *ap_name*

b. To assign an access point to a specific country, enter this command:

config ap country *code* {*ap_name* | **all**}

Make sure that the country code you choose is compatible with the regulatory domain of at least one of the access point's radios.

Note If you enabled the networks and disabled some access points and then run the **config ap country** *code* **all** command, the specified country code is configured on only the disabled access points. All other access points are ignored.

For example, if you enter **config ap country mx all**, information similar to the following appears:

```
To change country code: first disable target AP(s) (or disable all networks).
  Changing the country may reset any customized channel assignments.
  Changing the country will reboot disabled target AP(s).

 Are you sure you want to continue? (y/n) y

AP Name    Country  Status
---------  -------- --------
ap2         US      enabled (Disable AP before configuring country)
ap1         MX      changed (New country configured, AP rebooting)
```

c. To reenable any access points that you disabled in Step a, enter this command:

config ap enable *ap_name*

Step 10 If you did not reenable the 802.11a and 802.11b/g networks in Step 9, enter these commands to reenable them now:

config 802.11a enable network

config 802.11b enable network

Step 11 Save your settings by entering this command:

save config

Migrating Access Points from the -J Regulatory Domain to the -U Regulatory Domain

This section contains the following topics:

- Information About Migrating Access Points from the -J Regulatory Domain to the -U Regulatory Domain, page 9-93
- Guidelines and Limitations, page 9-94
- Migrating Access Points to the -U Regulatory Domain (CLI), page 9-94

Information About Migrating Access Points from the -J Regulatory Domain to the -U Regulatory Domain

The Japanese government has changed its 5-GHz radio spectrum regulations. These regulations allow a text box upgrade of 802.11a 5-GHz radios. Japan allows three frequency sets:

- J52 = 34 (5170 MHz), 38 (5190 MHz), 42 (5210 MHz), 46 (5230 MHz)
- W52 = 36 (5180 MHz), 40 (5200 MHz), 44 (5220 MHz), 48 (5240 MHz)
- W53 = 52 (5260 MHz), 56 (5280 MHz), 60 (5300 MHz), 64 (5320 MHz)

Cisco has organized these frequency sets into the following regulatory domains:

- -J regulatory domain = J52
- -P regulatory domain = W52 + W53
- -U regulatory domain = W52

Regulatory domains are used by Cisco to organize the legal frequencies of the world into logical groups. For example, most of the European countries are included in the -E regulatory domain. Cisco access points are configured for a specific regulatory domain at the factory and, with the exception of this migration process, never change. The regulatory domain is assigned per radio, so an access point's 802.11a and 802.11b/g radios may be assigned to different domains.

Note Controllers and access points may not operate properly if they are not designed for use in your country of operation. For example, an access point with part number AIR-AP1030-A-K9 (which is included in the Americas regulatory domain) cannot be used in Australia. Always be sure to purchase controllers and access points that match your country's regulatory domain.

The Japanese regulations allow the regulatory domain that is programmed into an access point's radio to be migrated from the -J domain to the -U domain. New access points for the Japanese market contain radios that are configured for the -P regulatory domain. -J radios are no longer being sold. In order to make sure that your existing -J radios work together with the new -P radios in one network, you need to migrate your -J radios to the -U domain.

Country codes define the channels that can be used legally in each country. These country codes are available for Japan:

- JP—Allows only -J radios to join the controller
- J2—Allows only -P radios to join the controller

Note J2 -Q works with 7.0.116.0 for all access points except Cisco Aironet 1550 Outdoor Access Points, Cisco 2600 Series Wireless Access Points, and Cisco 3600 Series Access Points. These access points need the -J4 domain to join the controller.

- J3—Uses the -U frequencies but allows both -U and -P radios to join the controller
- J4—Allows 2.4G PQU and 5G JPQU to join the controller.

Note After migration, you need to use the J3 country code. If your controller is running software release 4.1 or later releases, you can use the multiple-country feature to choose both J2 and J3. You can manually configure your -P radios to use the channels not supported by J3.

See the *Channels and Maximum Power Settings for Cisco Aironet Lightweight Access Points* document for the list of channels and power levels supported by access points in the Japanese regulatory domains.

Guidelines and Limitations

- You can migrate only Cisco Aironet 1130, 1200, and 1240 lightweight access points that support the -J regulatory domain and Airespace AS1200 access points. Other access points cannot be migrated.
- Your controller and all access points must be running software release 4.1 or later releases or software release 3.2.193.0.

Note Software release 4.0 is not supported. If you migrate your access points using software release 3.2.193.0, you cannot upgrade to software release 4.0. You can upgrade only to software release 4.1 or later releases or to a later release of the 3.2 software.

- You must have had one or more Japan country codes (JP, J2, or J3) configured on your controller at the time you last booted your controller.
- You must have at least one access point with a -J regulatory domain joined to your controller.
- You cannot migrate your access points from the -U regulatory domain back to the -J domain. The Japanese government has made reverse migration illegal.

Note You cannot undo an access point migration. Once an access point has been migrated, you cannot return to software release 4.0. Migrated access points will have nonfunctioning 802.11a radios under software release 4.0.

- The migration process cannot be performed using the Controller GUI.

Migrating Access Points to the -U Regulatory Domain (CLI)

Step 1 Determine which access points in your network are eligible for migration by entering this command:

show ap migrate

Information similar to the following appears:

```
These 1 APs are eligible for migration:
00:14:1c:ed:27:fe AIR-AP1242AG-J-K9ap1240      "J"Reg. Domain

No APs have already been migrated.
```

Step 2 Disable the 802.11a and 802.11b/g networks by entering these commands:

config 802.11a disable network

config 802.11b disable network

Step 3 Change the country code of the access points to be migrated to J3 by entering this command:

config country J3

Step 4 Wait for any access points that may have rebooted to rejoin the controller.

Step 5 Migrate the access points from the -J regulatory domain to the -U regulatory domain by entering this command:

config ap migrate j52w52 {**all** | *ap_name*}

Information similar to the following appears:

```
Migrate APs with 802.11A Radios in the "J" Regulatory Domain to the "U" Regulatory Domain.
The "J" domain allows J52 frequencies, the "U" domain allows W52 frequencies.
WARNING: This migration is permanent and is not reversible, as required by law.
WARNING: Once migrated the 802.11A radios will not operate with previous OS versions.
WARNING: All attached "J" radios will be migrated.
WARNING: All migrated APs will reboot.
WARNING: All migrated APs must be promptly reported to the manufacturer.
Send the AP list and your company name to: abc@cisco.com

This AP is eligible for migration:
00:14:1c:ed:27:fe AIR-AP1242AG-J-K9ap1240

Begin to migrate Access Points from "J"(J52) to "U"(W52). Are you sure? (y/n)
```

Step 6 Enter **Y** when prompted to confirm your decision to migrate.

Step 7 Wait for all access points to reboot and rejoin the controller. This process may take up to 15 minutes, depending on access point. The AP1130, AP1200, and AP1240 reboot twice; all other access points reboot once.

Step 8 Verify migration for all access points by entering this command:

show ap migrate

Information similar to the following appears:

```
No APs are eligible for migration.

These 1 APs have already been migrated:
00:14:1c:ed:27:fe AIR-AP1242AG-J-K9ap1240      "U"Reg. Domain
```

Step 9 Reenable the 802.11a and 802.11b/g networks by entering these commands:

config 802.11a enable network

config 802.11b enable network

Step 10 Send an e-mail with your company name and the list of access points that have been migrated to this e-mail address: migrateapj52w52@cisco.com. We recommend that you cut and paste the output from the **show ap migrate** command in Step 8 into the e-mail.

Using the W56 Band in Japan

The Japanese government is formally permitting wireless LAN use of the frequencies in the W56 band for 802.11a radios. The W56 band includes the following channels, frequencies, and power levels (in dBm):

Channel	Frequency (MHz)	Maximum Power for AIR-LAP1132AG-Q-K9	Maximum Power for AIR-LAP1242AG-Q-K9
100	5500	17	15
104	5520	17	15
108	5540	17	15
112	5560	17	15
116	5580	17	15
120	5600	17	15
124	5620	17	15
128	5640	17	15
132	5660	17	15
136	5680	17	15
140	5700	17	15

All of the channels in the W56 band require dynamic frequency selection (DFS). In Japan, the W56 band is subject to Japan's DFS regulations. Currently, only the new 1130 and 1240 series access point SKUs (with the -Q product code) support this requirement: AIR-LAP1132AG-Q-K9 and AIR-LAP1242AG-Q-K9.

To set up a network consisting of only -P and -Q access points, configure the country code to J2. To set up a network consisting of -P, -Q, and -U access points, configure the country code to J3.

Dynamic Frequency Selection

The Cisco UWN solution complies with regulations that require radio devices to use dynamic frequency selection (DFS) to detect radar signals and avoid interfering with them.

When a lightweight access point with a 5-GHz radio operates on one of the 15 channels listed in Table 9-3, the controller to which the access point is associated automatically uses DFS to set the operating frequency.

When you manually select a channel for DFS-enabled 5-GHz radios, the controller checks for radar activity on the channel for 60 seconds. If there is no radar activity, the access point operates on the channel that you selected. If there is radar activity on the channel that you selected, the controller automatically selects a different channel, and after 30 minutes, the access point retries the channel.

Note After radar has been detected on a DFS-enabled channel, it cannot be used for 30 minutes.

Note The Rogue Location Detection Protocol (RLDP) and rogue containment are not supported on the channels listed in Table 9-3.

Note The maximum legal transmit power is greater for some 5-GHz channels than for others. When the controller randomly selects a 5-GHz channel on which power is restricted, it automatically reduces transmit power to comply with power limits for that channel.

Table 9-3 DFS-Enabled 5-GHz Channels

52 (5260 MHz)	104 (5520 MHz)	124 (5620 MHz)
56 (5280 MHz)	108 (5540 MHz)	128 (5640 MHz)
60 (5300 MHz)	112 (5560 MHz)	132 (5660 MHz)
64 (5320 MHz)	116 (5580 MHz)	136 (5680 MHz)
100 (5500 MHz)	120 (5600 MHz)	140 (5700 MHz)

Using DFS, the controller monitors operating frequencies for radar signals. If it detects radar signals on a channel, the controller takes these steps:

- It changes the access point channel to a channel that has not shown radar activity within the last 30 minutes. (The radar event is cleared after 30 minutes.) The controller selects the channel at random.
- If the channel selected is one of the channels in Table 9-3, it scans the new channel for radar signals for 60 seconds. If there are no radar signals on the new channel, the controller accepts client associations.
- It records the channel that showed radar activity as a radar channel and prevents activity on that channel for 30 minutes.
- It generates a trap to alert the network manager.

Optimizing RFID Tracking on Access Points

This section contains the following topics:

- Information About Optimizing RFID Tracking on Access Points, page 9-97
- Optimizing RFID Tracking on Access Points, page 9-98

Information About Optimizing RFID Tracking on Access Points

To optimize the monitoring and location calculation of RFID tags, you can enable tracking optimization on up to four channels within the 2.4-GHz band of an 802.11b/g access point radio. This feature allows you to scan only the channels on which tags are usually programmed to operate (such as channels 1, 6, and 11).

Optimizing RFID Tracking on Access Points

This section contains the following topics:

- Optimizing RFID Tracking on Access Points (GUI), page 9-98
- Optimizing RFID Tracking on Access Points (CLI), page 9-99

Optimizing RFID Tracking on Access Points (GUI)

Step 1 Choose **Wireless** > **Access Points** > **All APs** to open the All APs page.

Step 2 Click the name of the access point for which you want to configure monitor mode. The All APs > Details for page appears.

Step 3 From the AP Mode drop-down list, choose **Monitor**.

Step 4 Click **Apply** to commit your changes.

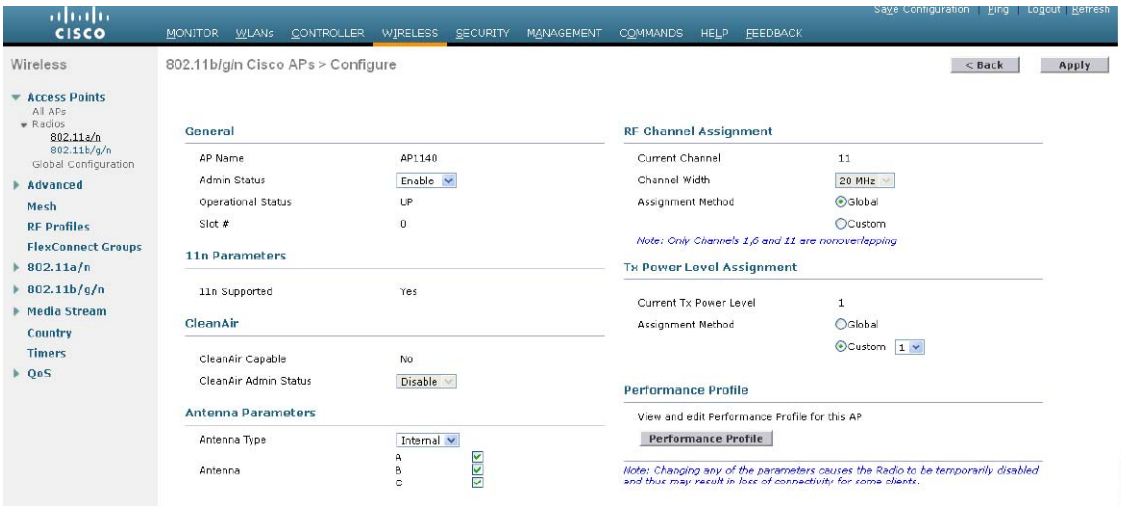
Step 5 Click **OK** when warned that the access point will be rebooted.

Step 6 Click **Save Configuration** to save your changes.

Step 7 Choose **Wireless** > **Access Points** > **Radios** > **802.11b/g/n** to open the 802.11b/g/n Radios page.

Step 8 Hover your cursor over the blue drop-down arrow for the desired access point and choose **Configure**. The 802.11b/g/n Cisco APs > Configure page appears.

Figure 9-42 802.11b/g/n Cisco APs > Configure Page



Step 9 Disable the access point radio by choosing **Disable** from the Admin Status drop-down list and click **Apply**.

Step 10 Enable tracking optimization on the radio by choosing **Enable** from the Enable Tracking Optimization drop-down list.

Step 11 From the four Channel drop-down lists, choose the channels on which you want to monitor RFID tags.

Note You must configure at least one channel on which the tags will be monitored.

Step 12 Click **Apply** to commit your changes.

Step 13 Click **Save Configuration** to save your changes.

Step 14 To reenable the access point radio, choose **Enable** from the Admin Status drop-down list and click **Apply**.

Step 15 Click **Save Configuration** to save your changes.

Optimizing RFID Tracking on Access Points (CLI)

Step 1 Configure an access point for monitor mode by entering this command:

config ap mode monitor *Cisco_AP*

Step 2 When warned that the access point will be rebooted and asked if you want to continue, enter **Y**.

Step 3 Save your changes by entering this command:

save config

Step 4 Disable the access point radio by entering this command:

config 802.11b disable *Cisco_AP*

Step 5 Configure the access point to scan only the DCA channels supported by its country of operation by entering this command:

config ap monitor-mode tracking-opt *Cisco_AP*

Note To specify the exact channels to be scanned, enter the **config ap monitor-mode tracking-opt** *Cisco_AP* command in Step 6.

Note To disable tracking optimization for this access point, enter the **config ap monitor-mode no-optimization** *Cisco_AP* command.

Step 6 After you have entered the command in Step 5, you can enter this command to choose up to four specific 802.11b channels to be scanned by the access point:

config ap monitor-mode 802.11b fast-channel *Cisco_AP channel1 channel2 channel3 channel4*

Note In the United States, you can assign any value between 1 and 11 (inclusive) to the *channel* variable. Other countries support additional channels. You must assign at least one channel.

Step 7 Reenable the access point radio by entering this command:

config 802.11b enable *Cisco_AP*

Step 8 Save your changes by entering this command:

save config

Step 9 See a summary of all access points in monitor mode by entering this command:

show ap monitor-mode summary

Information similar to the following appears:

```
AP Name             Ethernet MAC         Status      Scanning Channel List
------------------ -------------------- ----------  ------------------------
AP1131:46f2.98ac    00:16:46:f2:98:ac    Tracking        1, 6, NA, NA
```

Configuring Probe Request Forwarding

This section contains the following topics:

- Information About Configuring Probe Request Forwarding, page 9-100
- Configuring Probe Request Forwarding (CLI), page 9-100

Information About Configuring Probe Request Forwarding

Probe requests are 802.11 management frames sent by clients to request information about the capabilities of SSIDs. By default, access points forward acknowledged probe requests to the controller for processing. Acknowledged probe requests are probe requests for SSIDs that are supported by the access point. If desired, you can configure access points to forward both acknowledged and unacknowledged probe requests to the controller. The controller can use the information from unacknowledged probe requests to improve the location accuracy.

Configuring Probe Request Forwarding (CLI)

Step 1 Enable or disable the filtering of probe requests forwarded from an access point to the controller by entering this command:

config advanced probe filter {**enable** | **disable**}

If you enable probe filtering, the default filter setting, the access point forwards only acknowledged probe requests to the controller. If you disable probe filtering, the access point forwards both acknowledged and unacknowledged probe requests to the controller.

Step 2 Limit the number of probe requests sent to the controller per client per access point radio in a given interval by entering this command:

config advanced probe limit *num_probes interval*

where

- *num_probes* is the number of probe requests (from 1 to 100) forwarded to the controller per client per access point radio in a given interval.
- *interval* is the probe limit interval (from 100 to 10000 milliseconds).

The default value for *num_probes* is 2 probe requests, and the default value for *interval* is 500 milliseconds.

Step 3 Save your changes by entering this command:

save config

Step 4 See the probe request forwarding configuration by entering this command:

show advanced probe

Information similar to the following appears:

```
Probe request filtering.........................  Enabled
Probes fwd to controller per client per radio....  2
Probe request rate-limiting interval..........  500 msec
```

Retrieving the Unique Device Identifier on Controllers and Access Points

This section contains the following topics:

- Information About Retrieving the Unique Device Identifier on Controllers and Access Points, page 9-101
- Retrieving the Unique Device Identifier on Controllers and Access Points, page 9-101

Information About Retrieving the Unique Device Identifier on Controllers and Access Points

The Unique Device Identifier (UDI) standard uniquely identifies products across all Cisco hardware product families, enabling customers to identify and track Cisco products throughout their business and network operations and to automate their asset management systems. The standard is consistent across all electronic, physical, and standard business communications. The UDI consists of five data elements:

- The orderable product identifier (PID)
- The version of the product identifier (VID)
- The serial number (SN)
- The entity name
- The product description

The UDI is burned into the EEPROM of controllers and lightweight access points at the factory.

Retrieving the Unique Device Identifier on Controllers and Access Points

This section contains the following topics:

- Retrieving the Unique Device Identifier on Controllers and Access Points (GUI), page 9-101
- Retrieving the Unique Device Identifier on Controllers and Access Points (CLI), page 9-102

Retrieving the Unique Device Identifier on Controllers and Access Points (GUI)

Step 1 Choose **Controller** > **Inventory** to open the Inventory page.

Figure 9-43 Inventory Page

This page shows the five data elements of the controller UDI.

Step 2 Choose **Wireless** > **Access Points** > **All APs** to open the All APs page.

Step 3 Click the name of the desired access point.

Step 4 Choose the **Inventory** tab to open the All APs > Details for (Inventory) page.

This page shows the inventory information for the access point.

Retrieving the Unique Device Identifier on Controllers and Access Points (CLI)

Use these commands to retrieve the UDI on controllers and access points using the controller CLI:

- **show inventory**—Shows the UDI string of the controller. Information similar to the following appears:

```
NAME: "Chassis"    , DESCR: "Cisco Wireless Controller"
PID: WS-C3750G-24PS-W24,  VID: V01,  SN: FLS0952H00F
```

- **show inventory ap** *ap_id*—Shows the UDI string of the access point specified.

Performing a Link Test

This section contains the following topics:

- Information About Performing a Link Test, page 9-103
- Performing a Link Test, page 9-103

Information About Performing a Link Test

A link test is used to determine the quality of the radio link between two devices. Two types of link-test packets are transmitted during a link test: request and response. Any radio receiving a link-test request packet fills in the appropriate text boxes and echoes the packet back to the sender with the response type set.

The radio link quality in the client-to-access point direction can differ from that in the access point-to-client direction due to the asymmetrical distribution of the transmit power and receive sensitivity on both sides. Two types of link tests can be performed: a ping test and a CCX link test.

With the *ping link test*, the controller can test link quality only in the client-to-access point direction. The RF parameters of the ping reply packets received by the access point are polled by the controller to determine the client-to-access point link quality.

With the *CCX link test*, the controller can also test the link quality in the access point-to-client direction. The controller issues link-test requests to the client, and the client records the RF parameters (received signal strength indicator [RSSI], signal-to-noise ratio [SNR], and so on). of the received request packet in the response packet. Both the link-test requestor and responder roles are implemented on the access point and controller. Not only can the access point or controller initiate a link test to a CCX v4 or v5 client, but a CCX v4 or v5 client can initiate a link test to the access point or controller.

The controller shows these link-quality metrics for CCX link tests in both directions (out— access point to client; in— client to access point):

- Signal strength in the form of RSSI (minimum, maximum, and average)
- Signal quality in the form of SNR (minimum, maximum, and average)
- Total number of packets that are retried
- Maximum retry count for a single packet
- Number of lost packets
- Data rate of a successfully transmitted packet

The controller shows this metric regardless of direction:

- Link test request/reply round-trip time (minimum, maximum, and average)

The controller software supports CCX versions 1 through 5. CCX support is enabled automatically for every WLAN on the controller and cannot be disabled. The controller stores the CCX version of the client in its client database and uses it to limit the features for this client. If a client does not support CCXv4 or v5, the controller performs a ping link test on the client. If a client supports CCXv4 or v5, the controller performs a CCX link test on the client. If a client times out during a CCX link test, the controller switches to the ping link test automatically. See the "Configuring Cisco Client Extensions" section on page 8-57 for more information on CCX.

Note CCX is not supported on the AP1030.

Performing a Link Test

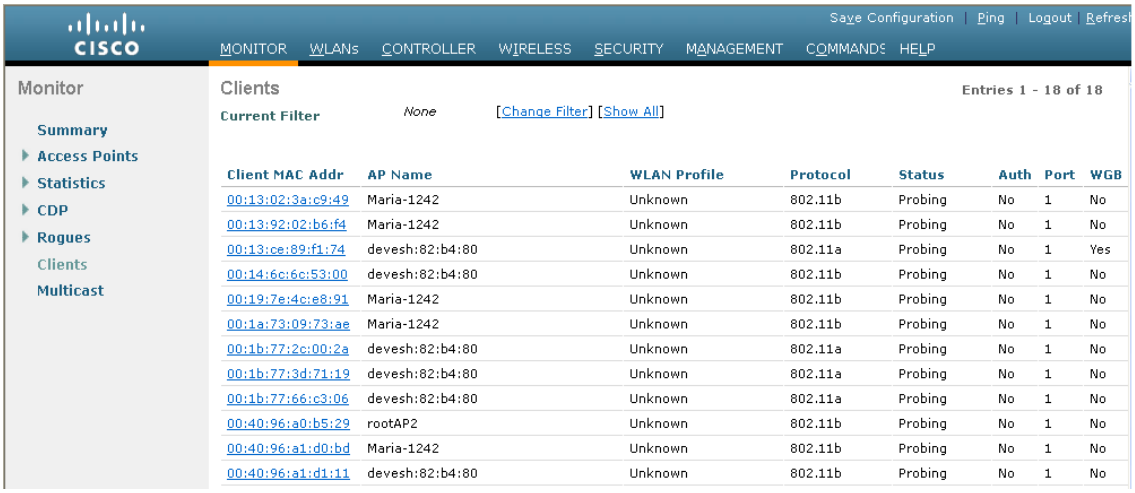
This section contains the following topics:

- Performing a Link Test (GUI), page 9-104
- Performing a Link Test (CLI), page 9-105

Performing a Link Test (GUI)

Step 1 Choose **Monitor** > **Clients** to open the Clients page.

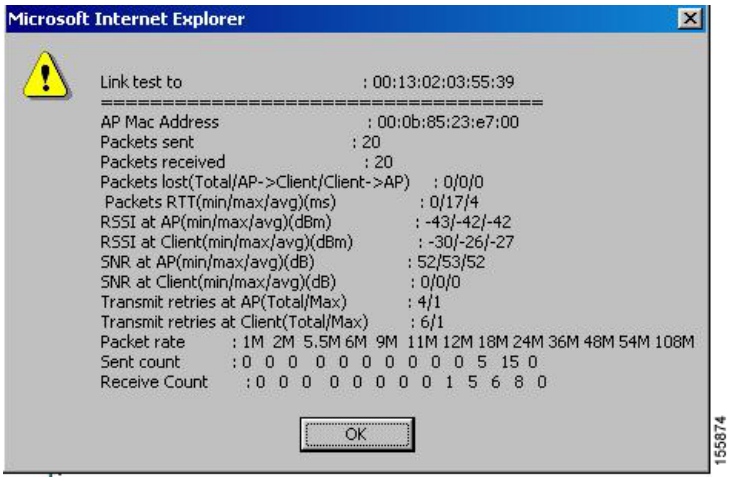
Figure 9-44 Clients Page



Step 2 Hover your cursor over the blue drop-down arrow for the desired client and choose **LinkTest**. A link test page appears.

Note You can also access this page by clicking the MAC address of the desired client and then clicking the **Link Test** button on the top of the Clients > Detail page.

Figure 9-45 Link Test Page



This page shows the results of the CCX link test.

Note If the client and/or controller does not support CCX v4 or later releases, the controller performs a ping link test on the client instead, and a much more limited link test page appears.

Note The Link Test results of CCX clients when it fails will default to ping test results if the client is reachable.

Step 3 Click **OK** to exit the link test page.

Performing a Link Test (CLI)

Use these commands to run a link test using the controller CLI:

- Run a link test by entering this command:

  linktest *ap_mac*

  When CCX v4 or later releases is enabled on both the controller and the client being tested, information similar to the following appears:

```
CCX Link Test to 00:0d:88:c5:8a:d1.
     Link Test Packets Sent..................................... 20
     Link Test Packets Received................................. 10
     Link Test Packets Lost (Total/AP to Client/Client to AP).... 10/5/5
     Link Test Packets round trip time (min/max/average)........ 5ms/20ms/15ms
     RSSI at AP (min/max/average)............................... -60dBm/-50dBm/-55dBm
     RSSI at Client (min/max/average)........................... -50dBm/-40dBm/-45dBm
     SNR at AP (min/max/average)................................ 40dB/30dB/35dB
     SNR at Client (min/max/average)............................ 40dB/30dB/35dB
     Transmit Retries at AP (Total/Maximum)..................... 5/3
     Transmit Retries at Client (Total/Maximum).................. 4/2
     Transmit rate:  1M   2M   5.5M   6M   9M  11M 12M 18M   24M   36M  48M  54M  108M
     Packet Count:   0     0     0    0    0    0   0   0     0     2    0   18     0
     Transmit rate:  1M   2M   5.5M   6M   9M  11M 12M 18M   24M   36M  48M  54M  108M
     Packet Count:   0     0     0    0    0    0   0   0     0     2    0    8     0
```

  When CCX v4 or later releases is not enabled on either the controller or the client being tested, fewer details appear:

```
Ping Link Test to 00:0d:88:c5:8a:d1.
        Link Test Packets Sent..................... 20
        Link Test Packets Received................. 20
        Local Signal Strength...................... -49dBm
        Local Signal to Noise Ratio................ 39dB
```

- Adjust the link-test parameters that are applicable to both the CCX link test and the ping test by entering these commands from configuration mode:

  linktest frame-size *size_of_link-test_frames*

  linktest num-of-frame *number_of_link-test_request_frames_per_test*

Configuring Link Latency

This section contains the following topics:

- Information About Configuring Link Latency, page 9-106
- Guidelines and Limitations, page 9-106
- Configuring Link Latency, page 9-106

Information About Configuring Link Latency

You can configure link latency on the controller to measure the link between an access point and the controller. This feature can be used with all access points joined to the controller but is especially useful for FlexConnect and OfficeExtend access points, for which the link could be a slow or unreliable WAN connection.

Guidelines and Limitations

- Link latency is supported for use only with FlexConnect access points in connected mode. FlexConnect access points in standalone mode are not supported.

  Link latency monitors the round-trip time of the CAPWAP heartbeat packets (echo request and response) from the access point to the controller and back. This time can vary due to the network link speed and controller processing loads. The access point timestamps the outgoing echo requests to the controller and the echo responses received from the controller. The access point sends this delta time to the controller as the system round-trip time. The access point sends heartbeat packets to the controller at a default interval of 30 seconds.

Note Link latency calculates the CAPWAP response time between the access point and the controller. It does not measure network latency or ping responses.

- The controller displays the current round-trip time as well as a running minimum and maximum round-trip time. The minimum and maximum times continue to run as long as the controller is up or can be cleared and allowed to restart.

Configuring Link Latency

This section contains the following topics:

- Configuring Link Latency (GUI), page 9-106
- Configuring Link Latency (CLI), page 9-107

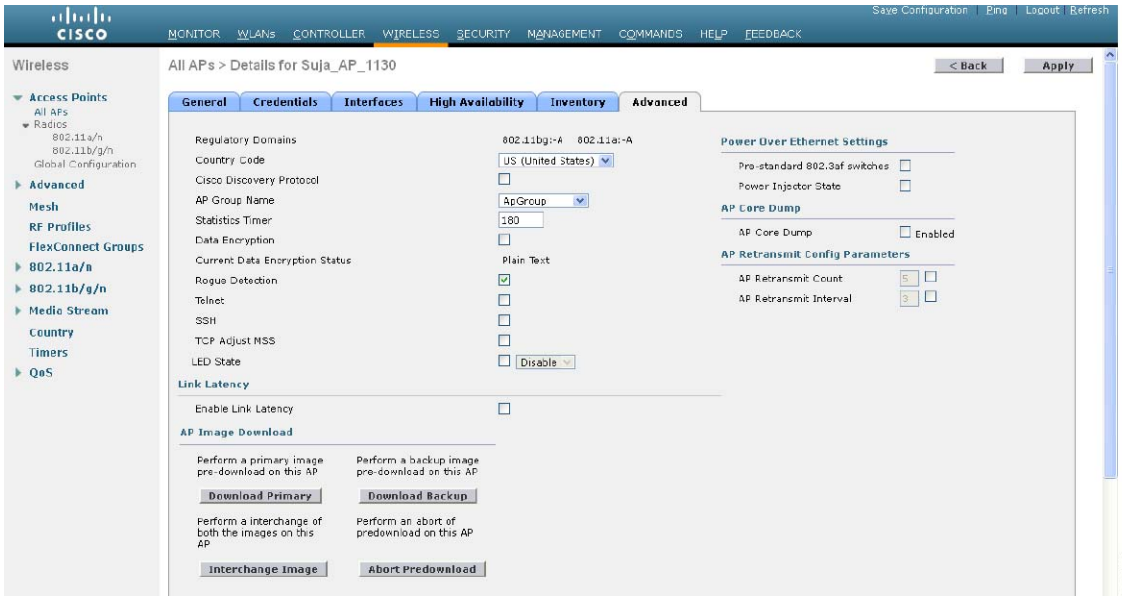
Configuring Link Latency (GUI)

Step 1 Choose **Wireless > Access Points > All APs** to open the All APs page.

Step 2 Click the name of the access point for which you want to configure link latency.

Step 3 Choose the **Advanced** tab to open the All APs > Details for (Advanced) page.

Figure 9-46 All APs > Details for (Advanced) Page



Step 4 Select the **Enable Link Latency** check box to enable link latency for this access point or unselect it to prevent the access point from sending the round-trip time to the controller after every echo response is received. The default value is unselected.

Step 5 Click **Apply** to commit your changes.

Step 6 Click **Save Configuration** to save your changes.

Step 7 When the All APs page reappears, click the name of the access point again.

Step 8 When the All APs > Details for page reappears, choose the **Advanced** tab again. The link latency and data latency results appear below the Enable Link Latency check box:

- **Current**—The current round-trip time (in milliseconds) of CAPWAP heartbeat packets or data packets from the access point to the controller and back.
- **Minimum**—Since link latency has been enabled or reset, the minimum round-trip time (in milliseconds) of CAPWAP heartbeat packets or data packets from the access point to the controller and back.
- **Maximum**—Since link latency has been enabled or reset, the maximum round-trip time (in milliseconds) of CAPWAP heartbeat packets or data packets from the access point to the controller and back.

Step 9 To clear the current, minimum, and maximum link latency and data latency statistics on the controller for this access point, click **Reset Link Latency**.

Step 10 After the page refreshes and the All APs > Details for page reap]pears, choose the **Advanced** tab. The updated statistics appear in the Minimum and Maximum text boxes.

Configuring Link Latency (CLI)

Step 1 Enable or disable link latency for a specific access point or for all access points currently associated to the controller by entering this command:

config ap link-latency {**enable** | **disable**} {*Cisco_AP* | **all**}

The default value is disabled.

Note The **config ap link-latency** {**enable** | **disable**} **all** command enables or disables link latency only for access points that are currently joined to the controller. It does not apply to access points that join in the future.

Step 2 See the link latency results for a specific access point by entering this command:

show ap config general *Cisco_AP*

Information similar to the following appears:

```
Cisco AP Identifier.............................. 1
Cisco AP Name.................................... AP1
...
AP Link Latency.................................. Enabled
 Current Delay................................... 1 ms
 Maximum Delay................................... 1 ms
 Minimum Delay................................... 1 ms
 Last updated (based on AP Up Time)............. 0 days, 05 h 03 m 25 s
```

The output of this command contains the following link latency results:

- **Current Delay**—The current round-trip time (in milliseconds) of CAPWAP heartbeat packets from the access point to the controller and back.
- **Maximum Delay**—Since link latency has been enabled or reset, the maximum round-trip time (in milliseconds) of CAPWAP heartbeat packets from the access point to the controller and back.
- **Minimum Delay**—Since link latency has been enabled or reset, the minimum round-trip time (in milliseconds) of CAPWAP heartbeat packets from the access point to the controller and back.

Step 3 Clear the current, minimum, and maximum link latency statistics on the controller for a specific access point by entering this command:

config ap link-latency reset *Cisco_AP*

Step 4 See the results of the reset by entering this command:

show ap config general *Cisco_AP*

Configuring the TCP MSS

This section contains the following topics:

- Information About Configuring the TCP MSS, page 9-109
- Configuring TCP MSS, page 9-109

Information About Configuring the TCP MSS

If the client's maximum segment size (MSS) in a Transmission Control Protocol (TCP) three-way handshake is greater than the maximum transmission unit can handle, the client might experience reduced throughput and the fragmentation of packets. To avoid this problem in controller software release 6.0 or later releases, you can specify the MSS for all access points that are joined to the controller or for a specific access point.

When you enable this feature, the access point selects for TCP packets to and from wireless clients in its data path. If the MSS of these packets is greater than the value that you configured or greater than the default value for the CAPWAP tunnel, the access point changes the MSS to the new configured value.

Configuring TCP MSS

This section contains the following topics:

- Configuring TCP MSS (GUI), page 9-109
- Configuring TCP MSS (CLI), page 9-109

Configuring TCP MSS (GUI)

Step 1 Choose **WIRELESS > Access Points > Global Configuration** to open the Global Configuration page.

Step 2 Under TCP MSS, select the **Global TCP Adjust MSS** check box and set the MSS for all access points that are associated with the controller. The valid range is between 536 and 1363 bytes.

Configuring TCP MSS (CLI)

Step 1 Enable or disable the TCP MSS on a particular access point or on all access points by entering this command:

config ap tcp-adjust-mss {**enable** | **disable**} {*Cisco_AP* | **all**} *size*

where the *size* parameter is a value between 536 and 1363 bytes. The default value varies for different clients.

Step 2 Save your changes by entering this command:

save config

Step 3 See the current TCP MSS setting for a particular access point or all access points by entering this command:

show ap tcp-mss-adjust {*Cisco_AP* | **all**}

Information similar to the following appears:

```
AP Name              TCP State  MSS Size
------------------   --------   -------
AP-1140             enabled    536
AP-1240              disabled   -
AP-1130             disabled    -
```

Configuring Power over Ethernet

This section contains the following topics:

- Information About Configuring Power over Ethernet, page 9-110
- Guidelines and Limitations, page 9-110
- Configuring Power over Ethernet, page 9-111

Information About Configuring Power over Ethernet

When an access point that has been converted to lightweight mode (such as an AP1131 or AP1242) or a 1250 series access point is powered by a power injector that is connected to a Cisco pre-Intelligent Power Management (pre-IPM) switch, you need to configure Power over Ethernet (PoE), also known as *inline power*.

The dual-radio 1250 series access points can operate in four different modes when powered using PoE:

- 20.0 W (Full Power)—This mode is equivalent to using a power injector or an AC/DC adapter.
- 16.8 W—Both transmitters are used but at reduced power. Legacy data rates are not affected, but the M0 to M15 data rates are reduced in the 2.4-GHz band. Throughput should be minimally impacted because all data rates are still enabled. The range is affected because of the lower transmit power. All receivers remain enabled.
- 15.4 W—Only a single transmitter is enabled. Legacy data rates and M0 to M7 rates are minimally affected. M8 to M15 rates are disabled because they require both transmitters. Throughput is better than that received with legacy access points but less than the 20 and 16.8 W power modes.
- 11.0 W (Low Power)—The access point runs, but both radios are disabled.

Guidelines and Limitations

- When a dual-radio 1250 series access point is powered using 15.4-W PoE, it cannot operate at full functionality, which requires 20 W. The access point can operate with dual radios on 15.4-W PoE, but performance is reduced in terms of throughput and range. If full functionality is required on 15.4 W, you can remove one of the radios from the 1250 series access point chassis or disable it in controller software release 6.0 or later releases so that the other radio can operate in full 802.11n mode. After the access point radio is administratively disabled, the access point must be rebooted for the change to take effect. The access point must also be rebooted after you reenable the radio to put it into reduced throughput mode.

  These modes provide the flexibility of running the 1250 series access points with the available wired infrastructure to obtain the desired level of performance. With enhanced PoE switches (such as the Cisco Catalyst 3750-E Series Switches), the 1250 series access points can provide maximum features and functionality with a minimum total cost of ownership. Alternatively, if you decide to power the access point with the existing PoE (802.3af) switches, the access point chooses the appropriate mode of operation based on whether it has one radio or two.

Note For more information on the Cisco PoE switches, see this URL: http://www.cisco.com/en/US/prod/switches/epoe.html

- Table 9-4 shows the maximum transmit power settings for 1250 series access points using PoE.

Table 9-4 Maximum Transmit Power Settings for 1250 Series Access Points Using PoE

Radio Band	Data Rates	Number of Transmitters	Cyclic Shift Diversity (CSD)	Maximum Transmit Power (dBm)[1]		
				802.3af Mode (15.4 W)	ePoE Power Optimized Mode (16.8 W)	ePoE Mode (20 W)
2.4 GHz	802.11b	1	—	20	20	20
	802.11g	1	—	17	17	17
	802.11n MCS 0-7	1 2	Disabled Enabled (default)	17 Disabled	17 14 (11 per Tx)	17 20 (17 per Tx)
	802.11n MCS 8-15	2	—	Disabled	14 (11 per Tx)	20 (17 per Tx)
5 GHz	802.11a	1	—	17	17	17
	802.11n MCS 0-7	1 2	Disabled Enabled (default)	17 Disabled	17 20 (17 per Tx)	17 20 (17 per Tx)
	802.11n MCS 8-15	2	—	Disabled	20 (17 per Tx)	20 (17 per Tx)

1. Maximum transmit power varies by channel and according to individual country regulations. See the product documentation for specific details.

- When powered with a non-Cisco standard PoE switch, the 1250 series access point operates under 15.4 Watts. Even if the non-Cisco switch or midspan device is capable of providing higher power, the access point does not operate in enhanced PoE mode.

Configuring Power over Ethernet

This section contains the following topics:

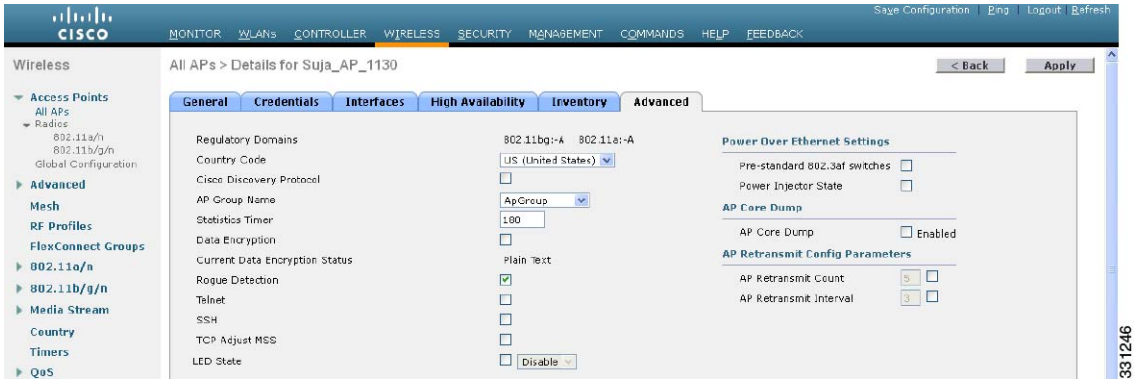
- Configuring Power over Ethernet (GUI), page 9-111
- Configuring Power over Ethernet (CLI), page 9-113

Configuring Power over Ethernet (GUI)

Step 1 Choose **Wireless** > **Access Points** > **All APs** and then the name of the desired access point.

Step 2 Choose the **Advanced** tab to open the All APs > Details for (Advanced) page.

Figure 9-47 All APs > Details for (Advanced) Page



The PoE Status text box shows the power level at which the access point is operating: High (20 W), Medium (16.8 W), or Medium (15.4 W). This text box is not configurable. The controller auto-detects the access point's power source and displays the power level here.

Note This text box applies only to 1250 series access points that are powered using PoE. There are two other ways to determine if the access point is operating at a lower power level. First, the "Due to low PoE, radio is transmitting at degraded power" message appears under the Tx Power Level Assignment section on the 802.11a/n (or 802.11b/g/n) Cisco APs > Configure page. Second, the "PoE Status: degraded operation" message appears in the controller's trap log on the Trap Logs page.

Step 3 Perform one of the following:

- Select the **Pre-standard 802.3af switches** check box if the access point is being powered by a high-power 802.3af Cisco switch. This switch provides more than the traditional 6 Watts of power but do not support the intelligent power management (IPM) feature.
- Unselect the **Pre-standard 802.3af switches** check box if power is being provided by a power injector. This is the default value.

Step 4 Select the **Power Injector State** check box if the attached switch does not support IPM and a power injector is being used. If the attached switch supports IPM, you do not need to select this check box.

Step 5 If you selected the Power Injector State check box in the previous step, the Power Injector Selection and Injector Switch MAC Address parameters appear. The Power Injector Selection parameter enables you to protect your switch port from an accidental overload if the power injector is inadvertently bypassed. Choose one of these options from the drop-down list to specify the desired level of protection:

- **Installed**—This option examines and remembers the MAC address of the currently connected switch port and assumes that a power injector is connected. Choose this option if your network contains older Cisco 6-Watt switches and you want to avoid possible overloads by forcing a double-check of any relocated access points.

  If you want to configure the switch MAC address, enter the MAC address in the Injector Switch MAC Address text box. If you want the access point to find the switch MAC address, leave the Injector Switch MAC Address text box blank.

Note Each time an access point is relocated, the MAC address of the new switch port fails to match the remembered MAC address, and the access point remains in low-power mode. You must then physically verify the existence of a power injector and reselect this option to cause the new MAC address to be remembered.

- **Override**—This option allows the access point to operate in high-power mode without first verifying a matching MAC address. You can use this option if your network does not contain any older Cisco 6-W switches that could be overloaded if connected directly to a 12-W access point. The advantage of this option is that if you relocate the access point, it continues to operate in high-power mode without any further configuration. The disadvantage of this option is that if the access point is connected directly to a 6-W switch, an overload occurs.

Step 6 Click **Apply** to commit your changes.

Step 7 If you have a dual-radio 1250 series access point and want to disable one of its radios in order to enable the other radio to receive full power, follow these steps:

a. Choose **Wireless** > **Access Points** > **Radios** > **802.11a/n** or **802.11b/g/n** to open the 802.11a/n (or 802.11b/g/n) Radios page.

b. Hover your cursor over the blue drop-down arrow for the radio that you want to disable and choose **Configure**.

c. On the 802.11a/n (or 802.11b/g/n) Cisco APs > Configure page, choose **Disable** from the Admin Status drop-down list.

d. Click **Apply** to commit your changes.

e. Manually reset the access point in order for the change to take effect.

Step 8 Click **Save Configuration** to save your settings.

Configuring Power over Ethernet (CLI)

Use these commands to configure and See PoE settings using the controller CLI:

- If your network contains any older Cisco 6-W switches that could be accidentally overloaded if connected directly to a 12-W access point, enter this command:

  config ap power injector enable {*Cisco_AP* | **all**} **installed**

  The access point remembers that a power injector is connected to this particular switch port. If you relocate the access point, you must reissue this command after the presence of a new power injector is verified.

  Note Make sure CDP is enabled before entering this command. Otherwise, this command will fail. See the "Configuring the Cisco Discovery Protocol" section on page 4-95 for information on enabling CDP.

- Remove the safety checks and allow the access point to be connected to any switch port by entering this command:

  config ap power injector enable {*Cisco_AP* | **all**} **override**

You can use this command if your network does not contain any older Cisco 6-W switches that could be overloaded if connected directly to a 12-W access point. The access point assumes that a power injector is always connected. If you relocate the access point, it continues to assume that a power injector is present.

- If you know the MAC address of the connected switch port and do not want to automatically detect it using the installed option, enter this command:

  config ap power injector enable {*Cisco_AP* | **all**} *switch_port_mac_address*

- If you have a dual-radio 1250 series access point and want to disable one of its radios in order to enable the other radio to receive full power, enter this command:

  config {**802.11a** | **802.11b**} **disable** *Cisco_AP*

  Note You must manually reset the access point in order for the change to take effect.

- See the PoE settings for a specific access point by entering this command:

  show ap config general *Cisco_AP*

  Information similar to the following appears:

```
Cisco AP Identifier.............................. 1
Cisco AP Name.................................... AP1
...
PoE Pre-Standard Switch.......................... Enabled
PoE Power Injector MAC Addr...................... Disabled
Power Type/Mode.................................. PoE/Low Power (degraded mode)
...
```

  The Power Type/Mode text box shows “degraded mode” if the access point is not operating at full power.

- See the controller’s trap log by entering this command:

  show traplog

  If the access point is not operating at full power, the trap contains “PoE Status: degraded operation.”

Configuring Flashing LEDs

This section contains the following topics:

- Information About Configuring Flashing LEDs, page 9-114
- Configuring Flashing LEDs (CLI), page 9-114

Information About Configuring Flashing LEDs

Controller software release 4.0 or later releases enables you to flash the LEDs on an access point in order to locate it. All IOS lightweight access points support this feature.

Configuring Flashing LEDs (CLI)

Use these commands to configure LED flashing from the privileged EXEC mode of the controller:

Note The output of these commands is sent only to the controller console, regardless of whether the commands were entered on the console or in a TELNET/SSH CLI session.

- Enable the controller to send commands to the access point from its CLI by entering this command:

  debug ap enable *Cisco_AP*

- Cause a specific access point to flash its LEDs for a specified number of seconds by entering this command:

  debug ap command "**led flash** *seconds*" *Cisco_AP*

  You can enter a value between 1 and 3600 seconds for the *seconds* parameter.

- Disable LED flashing for a specific access point by entering this command:

  debug ap command "**led flash disable**" *Cisco_AP*

  This command disables LED flashing immediately. For example, if you run the previous command (with the *seconds* parameter set to 60 seconds) and then disable LED flashing after only 20 seconds, the access point's LEDs stop flashing immediately.

Viewing Clients

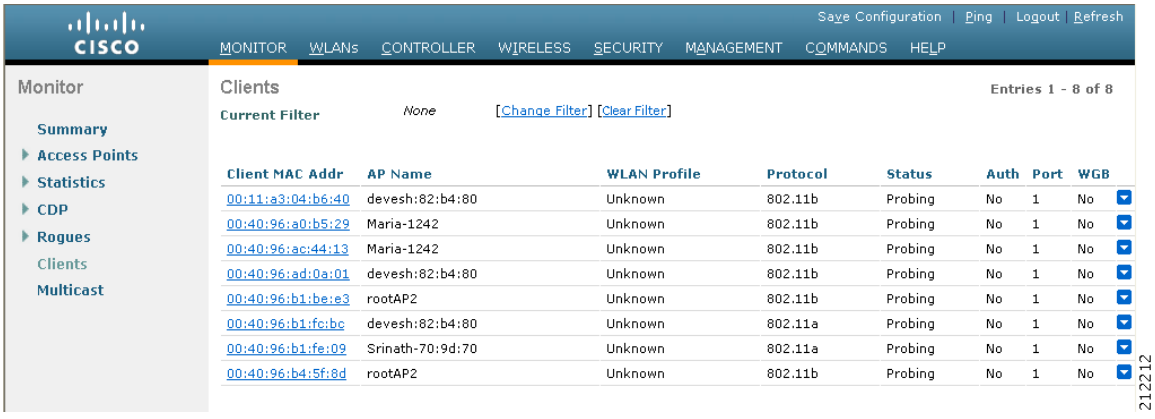
This section contains the following topics:

- Viewing Clients (GUI), page 9-115
- Viewing Clients (CLI), page 9-119

Viewing Clients (GUI)

Step 1 Choose **Monitor** > **Clients** to open the Clients page.

Figure 9-48 Clients Page



This page lists all of the clients that are associated to the controller's access points. It provides the following information for each client:

- The MAC address of the client
- The name of the access point to which the client is associated
- The name of the WLAN used by the client
- The type of client (802.11a, 802.11b, 802.11g, or 802.11n)

Note If the 802.11n client associates to an 802.11a radio that has 802.11n enabled, then the client type shows as 802.11a/n. If the 802.11n client associates to an 802.11b/g radio with 802.11n enabled, then the client type shows as 802.11b/n.

- The status of the client connection
- The authorization status of the client
- The port number of the access point to which the client is associated
- An indication of whether the client is a WGB

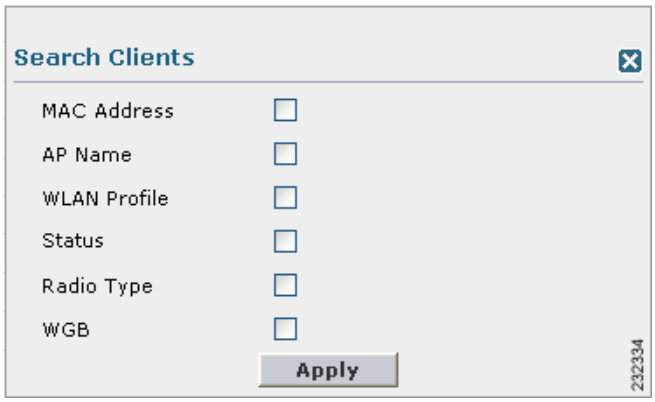
Note See the "Using Cisco Workgroup Bridges" section on page 9-70 for more information on the WGB status.

Note If you want to remove or disable a client, hover your cursor over the blue drop-down arrow for that client and choose **Remove** or **Disable**, respectively. If you want to test the connection between the client and the access point, hover your cursor over the blue drop-down arrow for that client and choose **Link Test**.

Step 2 Create a filter to display only clients that meet certain criteria (such as the MAC address, status, or radio type) as follows:

a. Click **Change Filter** to open the Search Clients dialog box.

Figure 9-49 Search Clients Dialog Box



b. Select one or more of the following check boxes to specify the criteria used when displaying clients:

- **MAC Address**—Enter a client MAC address.

Note When you enable the MAC address filter, the other filters are disabled automatically. When you enable any of the other filters, the MAC address filter is disabled automatically.

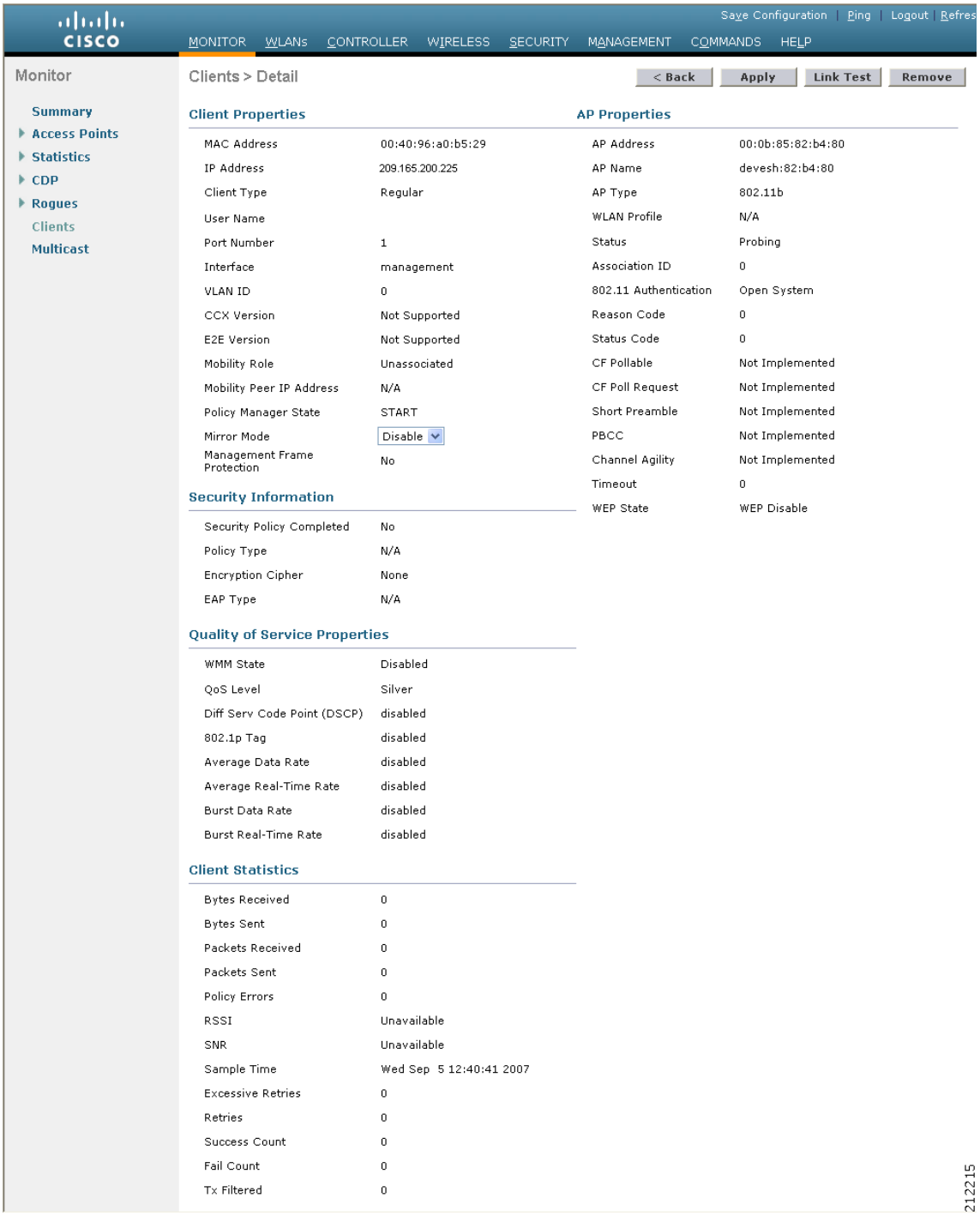
- **AP Name**—Enter the name of an access point.
- **WLAN Profile**—Choose one of the available WLAN profiles from the drop-down list.
- **Status**—Select the **Associated**, **Authenticated**, **Excluded**, and/or **Idle** check boxes.
- **Radio Type**—Choose **802.11a**, **802.11b**, **802.11g**, **802.11an**, **802.11bn** or **Mobile**.
- **WGB**—Enter the WGB clients associated to the controller's access points.

c. Click **Apply** to commit your changes. The Current Filter parameter at the top of the Clients page shows the filters that are currently applied.

Note If you want to remove the filters and display the entire client list, click **Clear Filter**.

Step 3 Click the MAC address of the client to view detailed information for a specific client. The Clients > Detail page appears.

Figure 9-50 Clients > Detail Page



This page shows the following information:

- The general properties of the client
- The security settings of the client
- The QoS properties of the client

- Client statistics
- The properties of the access point to which the client is associated

Viewing Clients (CLI)

Use these commands to view client information:

- See the clients associated to a specific access point by entering this command:

  show client ap {**802.11a** | **802.11b**} *Cisco_AP*

  Information similar to the following appears:

```
MAC Address        AP Id   Status         WLAN Id Authenticated
-----------------  ------  -------------  ---------  -------------
00:13:ce:cc:8e:b8   1     Associated      1          No
```

- See a summary of the clients associated to the controller's access points by entering this command:

  show client summary

  Information similar to the following appears:

```
Number of Clients.............................. 1

MAC Address       AP Name      Status    WLAN/Guest-Lan Auth Protocol Port Wired
----------------- ------------ ---------- --------------- ---- -------- ---- -----
00:13:02:2d:96:24 AP_1130      Associated      1         Yes  802.11a  1    No
```

- See detailed information for a specific client by entering this command:

  show client detail *client_mac*

  Information similar to the following appears:

```
Client MAC Address............................. 00:40:96:b2:a3:44
Client Username ............................... N/A
AP MAC Address................................. 00:18:74:c7:c0:90
Client State................................... Associated
Wireless LAN Id................................ 1
BSSID.......................................... 00:18:74:c7:c0:9f
Channel........................................ 56
IP Address..................................... 192.168.10.28
Association Id................................. 1
Authentication Algorithm....................... Open System
Reason Code.................................... 0
Status Code.................................... 0
Session Timeout................................ 0
Client CCX version............................. 5
Client E2E version............................. No E2E support
Diagnostics Capability......................... Supported
S69 Capability................................. Supported
Mirroring...................................... Disabled
QoS Level...................................... Silver
...
```

Configuring LED States for Access Points

In a wireless LAN nework, there may be numerous access points that could be associated with a controller. It can be difficult to locate a specific access point associated with the controller. You can configure the controller to set the LED state of an access point so that it blinks and the access point can be located. This configuration can be done in the wireless network on a global as well as per-AP level.

Guidelines and Limitations

The LED state configuration at the global level takes precedence over the AP level.

Configuring LED State of Access Point in a Network Globally (GUI)

Step 1 Choose **Wireless > Access Points > Global Configuration** to open the **Global Configuration** page.

Step 2 Select the **LED state** checkbox.

Step 3 Select **Enable** from the drop-down list adjacent to this text box.

Step 4 Click **Apply**.

Configuring LED State of Access Point in a Network Globally (CLI)

Use the following command to set the LED state of all access points associated to a contoller:

config ap led-state {**enable** | **disable**} **all**

Configuring LED State on an Access Point (GUI)

Step 1 Choose **Wireless > Access Points > All APs** and then the name of the desired access point.

Step 2 Choose the **Advanced** tab to open the All APs > Details for (Advanced) page.

Step 3 Select the **LED state** checkbox.

Step 4 Select **Enable** from the drop-down list adjacent to this text box.

Step 5 Click **Apply**.

Configuring LED State on an Access Point (CLI)

Use the following command to set the LED state of a specific access point:

Step 1 Determine the access point for which you want to configure the LED state by entering this command:

show ap summary

Obtain the access point ID from the list.

Step 2 Configure the LED state by entering the following command:

config ap led-state {**enable** | **disable**} *Cisco_AP*