Managing APs

Converting Autonomous APs to Lightweight Mode

Information About Converting Autonomous Access Points to Lightweight Mode

You can convert any autonomous mode Cisco Aironet access point, 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 to upgrade an autonomous access point to lightweight mode:

http://www.cisco.com/c/en/us/td/docs/wireless/controller/8-0/configuration-guide/b_cg80/b_cg80_chapter_01101010.html

The following are some guidelines for converting autonomous APs to lightweight mode APs:

- All Cisco lightweight access points support 16 BSSIDs per radio and a total of 16 wireless LANs per access point. When a converted access point associates with a controller, wireless LANs with IDs 1 through 16 are pushed to the access point if the AP is part of the default AP group on the controller. You can use other AP group configurations to push other wireless LANs to the new AP.

  When a 802.11ac module (the RM3000AC) is added to a 3600 AP, you can have only 8 wireless LANs on the 802.11a/n/ac radio.

- Access points converted to lightweight mode must get an IP address and discover the controller using DHCP, DNS, or IP subnet broadcast.

Restrictions for Converting Autonomous Access Points to Lightweight Mode

- 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.
- After you convert an access point to lightweight mode, the console port provides read-only access to the unit.

Converting Autonomous Access Points to Lightweight Mode

1. Download the CAPWAP file matching your access point model from Cisco.com. Two types of CAPWAP files are available:
   - Fully functional CAPWAP files, identified by the *k9w8* string in their name. When booting this image, the AP is fully functional and can join a controller to obtain its configuration.
   - Recovery mode CAPWAP files, identified by the *rcvk9w8* string in their name. These files are smaller than the fully functional *k9w8* CAPWAP files. When booting *rcvk9w8* files, the AP can join a controller to download a fully functional image. The AP will then reboot, use the fully functional image and rejoin a controller to obtain its configuration.
2. position the image on an FTP server
3. Configure the AP to connect to the FTP server as a FTP client. This is done under global configuration mode, with the command **ip ftp** *username*, and **ip ftp** *password*. For example:

```
Ap#configure terminal
ap(config)#ip ftp username cisco
ap(config)#ip ftp password Cisco123
ap(config)#exit
```

4. Once the parameters are configured, you can start the download process on the AP. Use the **archive download-sw** command, with the **/force-reload** argument to have the AP reboot at the end of the cycle, and **/overwrite** to replace the autonomous code with the CAPWAP code. See the following example:

```
ap#archive download-sw /force-reload /overwrite
ftp://10.100.1.31/ap3g2-rcvk9w8-tar.152-4.JB6.tar
examining image...
Loading ap3g2-rcvk9w8-tar.152-4.JB6.tar
extracting info (273 bytes)!
Image info:
    Version Suffix: rcvk9w8-
    Image Name: ap3g2-rcvk9w8-mx
    Version Directory: ap3g2-rcvk9w8-mx
    Ios Image Size: 2335232
    Total Image Size: 2335232
    Image Feature: WIRELESS LAN|CAPWAP|RECOVERY
    Image Family: ap3g2
    Wireless Switch Management Version: 3.0.51.0
Extracting files...
ap3g2-rcvk9w8-mx/ (directory) 0 (bytes)
extracting ap3g2-rcvk9w8-mx/ap3g2-rcvk9w8-mx (2327653 bytes)!!!!!!!!!
extracting ap3g2-rcvk9w8-mx/info (273 bytes)
```

   The AP reboots into lightweight mode and looks for a controller.

Reverting from Lightweight Mode to Autonomous Mode

After you 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. 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.

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 *ap3g2-k9w7-tar.152-4.JB4.tar* for a 2700 or 3700 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 **ap3g2-k9w7-tar.default** for a 2700 or a 3700 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 8-45 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.

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 APs.

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.

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.

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.

Step 3 Under IP Config, select the **Static IP (IPv4/IPv6)** check box if you want to assign a static IP address to this access point. The default value is unselected.

Note The static IP configured on the AP will take precedence over the preferred mode configured on the AP. For example: If AP has static IPV6 address and prefer-mode is set to IPV4, then the AP will join over IPv6.

Step 4 Enter the static IPv4/IPv6 address of the access point, subnet mask/ prefix length assigned to the access point IPv4/IPv6 address, and the IPv4/IPv6 gateway of the access point in the corresponding text boxes.

Step 5 Click **Apply** to commit your changes. The access point reboots and rejoins the controller, and the static IPv4/IPv6 address that you specified in Step 4 is sent to the access point.

Step 6 After the static IPv4/IPv6 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 IPv4/IPv6 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:
For IPv4**—config ap static-ip enable** *Cisco_AP ip_address mask gateway*

For IPv6**—config ap static-ip enable** *Cisco_AP ip_address prefix_length gateway*

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

Note The static IP configured on the AP will take precedence over the preferred mode configured on the AP. For example: If AP has static IPV6 address and prefer-mode is set to IPV4, then the AP will join over IPv6.

Step 2 Enter the **save config** command to save your changes.
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 IPv4/IPv6 address has been sent to the access point, you can configure the DNSv4/DNSv6 server IP address and domain name as follows:

a) To specify a DNSv4/DNSv6 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 DNSv4/DNSv6 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) Enter the **save config** command to save your changes.

Step 4 See the IPv4/IPv6 address configuration for the access point by entering this command:

- For IPv4:
show ap config general *Cisco_AP*

  Information similar to the following appears:

```
show ap config general <Cisco_AP>

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
...
```

- For IPv6:
show ap config general *Cisco_AP*

  Information similar to the following appears:

```
show ap config general <Cisco_AP>
```

```
Cisco AP Identifier.............................. 16
Cisco AP Name.................................... AP2602I-A-K9-1
...
IPv6 Address Configuration....................... DHCPv6
IPv6 Address..................................... 2001:9:2:16:1ae:a1da:c2c7:44b
IPv6 Prefix Length............................... 128
Gateway IPv6 Addr................................ fe80::c60a:cbff:fe79:53c4
NAT External IP Address.......................... None

...
IPv6 Capwap UDP Lite............................. Enabled
Capwap Prefer Mode............................... Ipv6 (ApGroup Config)
Hotspot Venue Group.............................. Unspecified
Hotspot Venue Type............................... Unspecified
DNS server IP ..................... Not Available
```

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.

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 (for example, ap3g2-rcvk9w8-tar.152-4.JB6.tar for 2700 or 3700 APs) 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.

Global Credentials for APs

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 on to the nonprivileged mode and enter **show** and **debug** commands, which poses a security threat. The default enable password must be changed to prevent unauthorized users from accessing to the access point's console port and entering configurable commands.

The following are some guidelines to configure global credentials for access points:

- 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.
- 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 in to the access point's console port. When you log on, you are in nonprivileged mode, and you must enter the enable password in order to use the privileged mode.
- 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.
- You must keep track of the credentials used by the access points. Otherwise, you might not be able to log onto the console port of the access point. 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, choose **Wireless** > **Access Points** > **All APs**, click the AP name and click **Clear All Config** on the controller GUI, or enter the **clear ap config** *Cisco_AP* command on the controller CLI. To clear the access point's configuration except its static IP address, choose **Wireless** > **Access Points** > **All APs**, click the AP name and click **Clear Config Except Static IP**, or enter the **clear ap config** *ap-name* **keep-ip-config** command on the controller CLI. After the access point rejoins a controller, it adopts the default *Cisco*/*Cisco* username and password.

Note Suppose you configure an indoor Cisco AP to go into the mesh mode. If you want to reset the Cisco AP to the local mode, use the **test mesh mode local** command.

- To reset the AP hardware, choose **Wireless** > **Access Points** > **All APs**, click the AP name and click **Reset AP Now**.

Restrictions for Global Credentials for Access Points

- The controller software features are supported on all access points that have been converted to lightweight mode except the 1100 series. VxWorks access points are not supported.
- Telnet is not supported on Cisco Aironet 1810 OEAP, 1810W, 1830, 1850, 2800, and 3800 Series APs.
- A global Access Point login credentials once configured in WLC cannot be removed.

Configuring Global Credentials for Access Points

Configuring Global Credentials for Access Points (GUI)

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

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

Step 3 In the **Password** field, 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.
- The AP passwords or secret passwords should not contain the following characters:

  &, <, >, ", and '

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.
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

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.

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 Telnet and SSH for Access Points

Configuring Telnet and SSH for APs (GUI)

Step 1 Global configuration:

a) Choose **Wireless** > **Access Points** > **Global Configuration**.

b) In the **Global Telnet SSH** area, select or unselect **Telnet** and **SSH** check boxes.

When you enable Telnet or SSH for all APs, the functionality is allowed on APs that are yet to associate with the Cisco WLC regardless of their mode.

c) Click **Apply**.
d) Click **Save Configuration**.

Step 2 Configuration for a specific AP:

a) Choose **Wireless** > **Access Points** > **All APs**.
b) Click an AP name.
c) Click the **Advanced** tab.
d) From the **Telnet** drop-down list, choose **AP Specific** and select the check box to enable the functionality for the AP.
e) From the **SSH** drop-down list, choose **AP Specific** and select the check box to enable the functionality.
f) Click **Apply**.
g) Click **Save Configuration**.

Configuring Telnet and SSH for APs (CLI)

- Configure Telnet or SSH for all APs or a specific AP by entering this command:
  config ap {**telnet** | **ssH**} {**enable** | **disable**} {*ap-name* | **all**}
- Replace the Telnet or SSH configuration for a specific AP with the global configuration by entering this command:
  config ap {**telnet** | **ssH**} **default** *ap-name*

Embedded APs

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.

The following are some guidelines for embedded access points:

- 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.

Note In Release 7.4, all AP modes except bridging (required for mesh) are supported for both AP801 and AP802. In Release 7.5 and later, all AP modes are supported on AP802; however, bridging is not supported on AP801.

- 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, 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.

Note To use the CLI commands mentioned above, the router must be running Cisco IOS Release 12.4(20)T or later releases.

- 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/c/en/us/td/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.

For more information about the AP801, see the documentation for the Cisco 800 Series ISRs at http://www.cisco.com/c/en/us/support/routers/800-series-routers/tsd-products-support-series-home.html.

For more information about the AP802, see the documentation for the Next generation Cisco 880 Series ISRs at http://www.cisco.com/c/dam/en/us/td/docs/routers/access/800/860-880-890/software/configuration/guide/SCG_880_series.pdf.

AP Modules

Spectrum Expert

Information About Spectrum Expert Connection

To obtain detailed spectrum data that can be used to generate RF analysis plots similar to those provided by a spectrum analyzer, you can configure a Cisco CleanAir-enabled access point to connect directly to a Microsoft Windows XP or Vista PC running the Spectrum Expert application (referred to as a *Spectrum Expert console*). You can initiate the Spectrum Expert connection semi-automatically from Prime Infrastructure or by manually launching it from the Cisco WLC. This section provides instructions for the latter.

Note The Cisco Aironet Access Point Module for Wireless Security and Spectrum Intelligence (WSSI) for the Cisco Aironet 3600 Series Access Point tightly couples data connectivity, spectrum analysis, and security threat detection and mitigation into a single, multipurpose access point. With WSSI you have to use Metageek Chanalyzer Pro with CleanAir support and not Spectrum expert for wIPS, CleanAir and spectrum analysis.

Configuring Spectrum Expert (GUI)

Before You Begin

Prior to establishing a connection between the Spectrum Expert console and the access point, make sure that IP address routing is properly configured and the network spectrum interface (NSI) ports are open in any intervening firewalls.

Step 1 Ensure that Cisco CleanAir functionality is enabled for the access point that will be connected to the Spectrum Expert console.

Step 2 Configure the access point for SE-Connect mode using the Cisco WLC GUI or CLI.

Note The SE-Connect mode is set for the entire access point, not just a single radio. However, the Spectrum Expert console connects to a single radio at a time.

If you are using the Cisco WLC GUI, follow these steps:

a) Choose **Wireless** > **Access Points** > **All APs** to open the All APs page.
b) Click the name of the desired access point to open the All APs > Details for page.
c) Choose **SE-Connect** from the AP Mode drop-down list. This mode is available only for access points that are capable of supporting Cisco CleanAir functionality. For the SE-Connect mode to appear as an available option, the access point must have at least one spectrum-capable radio in the Enable state.
d) Click **Apply** to commit your changes.

e) Click **OK** when prompted to reboot the access point.

If you are using the CLI, follow these steps:

a) To configure the access point for SE-Connect mode, enter this command:
config ap mode se-connect *Cisco_AP*

b) When prompted to reboot the access point, enter **Y.**

c) To verify the SE-Connect configuration status for the access point, enter this command:
show ap config {**802.11a** | **802.11b**} *Cisco_AP*

Information similar to the following appears:

```
Cisco AP Identifier.............................. 0
Cisco AP Name.................................... CISCO_AP3500
...
Spectrum Management Information
        Spectrum Management Capable.............. Yes
        Spectrum Management Admin State.......... Enabled
        Spectrum Management Operation State...... Up
        Rapid Update Mode........................ Disabled
        Spectrum Expert connection............... Enabled
   Spectrum Sensor State.................. Configured (Error code = 0)
```

Step 3 On the Windows PC, access the Cisco Software Center from this URL:
http://www.cisco.com/cisco/software/navigator.html

Step 4 Click **Product > Wireless > Cisco Spectrum Intelligence** > **Cisco Spectrum Expert** > **Cisco Spectrum Expert Wi-Fi**, and then download the Spectrum Expert 4.0 executable (*.exe) file.

Step 5 Run the Spectrum Expert application on the PC.

Step 6 When the Connect to Sensor dialog box appears, enter the IP address of the access point, choose the access point radio, and enter the 16-byte network spectrum interface (NSI) key to authenticate. The Spectrum Expert application opens a TCP/IP connection directly to the access point using the NSI protocol.

Note The access point must be a TCP server listening on ports 37540 for 2.4 GHz and 37550 for 5 GHz frequencies. These ports must be opened for the spectrum expert application to connect to the access point using the NSI protocol.

Note On the Cisco WLC GUI, the NSI key appears in the Network Spectrum Interface Key field (below the Port Number field) on the All APs > Details for page. To view the NSI key from the Cisco WLC CLI, enter the **show ap config** {**802.11a** | **802.11b**} *Cisco_AP* command.

When an access point in SE-Connect mode joins a Cisco WLC, it sends a Spectrum Capabilities notification message, and the Cisco WLC responds with a Spectrum Configuration Request. The request contains the 16-byte random NSI key generated by the Cisco WLC for use in NSI authentication. The Cisco WLC generates one key per access point, which the access point stores until it is rebooted.

Note You can establish up to three Spectrum Expert console connections per access point radio. The Number of Spectrum Expert Connections text box on the 802.11a/n/ac (or 802.11b/g/n) Cisco APs > Configure page of the Cisco WLC GUI shows the number of Spectrum Expert applications that are currently connected to the access point radio.

Step 7 Verify that the Spectrum Expert console is connected to the access point by selecting the Slave Remote Sensor text box in the bottom right corner of the Spectrum Expert application. If the two devices are connected, the IP address of the access point appears in this text box.

Step 8 Use the Spectrum Expert application to view and analyze spectrum data from the access point.

Cisco Universal Small Cell 8x18 Dual-Mode Module

Information About Cisco Universal Small Cell 8x18 Dual-Mode Module

Cisco Universal Small Cell 8x18 Dual-Mode Module is an external module (4G/LTE) that can be plugged into the Cisco Aironet 3600I APs or Cisco Aironet 3700I APs. The following features are available:

- You can configure VLAN tagging for the external module's traffic for the following modes:

Mode	Native VLAN	Non-Native VLAN
FlexConnect Local Switching	Supported	Supported
Local Mode Central Switching	Supported	Supported

- The module can be powered up by the PoE+ power supply
- Co-existence detection and warning when Wi-Fi in 2.4 GHz and 3G/4G module are enabled
- The module's inventory details are available on the Cisco WLC GUI at **Wireless** > **Access Points** > ***Access Point name*** > **Inventory**.
- Supported on the following Cisco Wireless Controller models:
  - Cisco 2504 WLC
  - Cisco 5508 WLC
  - Cisco 5520 WLC
  - Cisco Flex 7510 WLC
  - Cisco 8510 WLC
  - Cisco 8540 WLC
  - Cisco Virtual Controller
  - Cisco WiSM2
- Supported on the following Cisco Access Point models:
  - Cisco Aironet 3600I AP
  - Cisco Aironet 3700I AP

Restrictions

Cisco Universal Small Cell 8x18 Dual-Mode Modules are not supported on the following Cisco Access Point models:

- Cisco Aironet 3600E AP
- Cisco Aironet 3700E AP

For more information about Cisco Universal Small Cell 8x18 Dual-Mode modules, see http://www.cisco.com/c/en/us/support/wireless/universal-small-cell-8000-series/tsd-products-support-series-home.html.

Configuring Cisco Universal Small Cell 8x18 Dual-Mode Module

Configuring Cisco Universal Small Cell 8x18 Dual-Mode Module (GUI)

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

Step 2 Click the AP name.
The **All APs > Details** page is displayed.

Step 3 In the **Advanced** tab, check or uncheck the **External Module Status** check box.
You might be prompted with a co-existence warning when Wi-Fi in 2.4-GHz and 3G/4G module are enabled.

Configuring Cisco Universal Small Cell 8x18 Dual-Mode Module (CLI)

- Enable or disable the Cisco USC 8x18 Dual-Mode Module by entering this command:
  config ap module3G {**enable** | **disable**} *ap-name*
  You might be prompted with a co-existence warning when Wi-Fi in 2.4-GHz and 3G/4G module are enabled.

Configuring USC8x18 Dual-Mode Module in Different Scenarios

Configuring VLAN Tagging for USC8x18 Dual-Mode Module in FlexConnect Local Switching (GUI)

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

Step 2 Click the AP name.
The **All APs > Details** page is displayed.

Step 3 In the **FlexConnect** tab, check the **VLAN Support** check box and enter the number of the native VLAN on the remote network (such as 100) in the **Native VLAN ID** box.

Step 4 To enable FlexConnect Local Switching with VLAN ID that is other than 0:

a) Enable **FlexConnect Local Switching** under **External Module**.
b) Enter a value between 2 and 4096 in the **VLAN ID** box.
c) Click **Apply**.

Step 5 To enable FlexConnect local switching with VLAN ID equal to 0:

a) Enable **FlexConnect Local Switching** under **External Module**.

b) Click **Apply**.

Step 6 To remove the FlexConnect local switching per AP configuration, click **Remove AP Specific Config**.

Step 7 Save the configuration.

Configuring VLAN Tagging for USC8x18 Dual-Mode Module in FlexConnect Local Switching (CLI)

- **config ap flexconnect module-vlan enable** *ap-name* —Enables FlexConnect local switching for external module with native VLAN
- **config ap flexconnect module-vlan remove** *ap-name*—Removes the AP specific external module VLAN configuration
- **config ap flexconnect module-vlan enable** *ap-name* **vlan** *vlan-id*—Enables FlexConnect local switching with non-native VLAN for the external module
- **show ap module summary** {*ap-name* | **all**}—Displays detailed information about the external module.
- **show ap inventory** {*ap-name* | **all**}—Displays information about the AP's inventory and the external module, if the module is present
- **show ap flexconnect module-vlan** *ap-name*—Displays status of FlexConnect local switching and VLAN ID value
- **show ap config general** *ap-name*—Displays information about the external module info, if the module is present.

Configuring VLAN Tagging for USC8x18 Dual-Mode Module in FlexConnect Group Local Switching (GUI)

Step 1 Choose **Wireless** > **FlexConnect Groups**.

Step 2 Click **New**, enter the FlexConnect group name, and click **Apply**.

Step 3 On the **FlexConnect Groups > Edit** page, in the **FlexConnect APs** area, click **Add AP**.

Step 4 You can either select an AP from a list of APs associated with the Cisco WLC or directly specify the Ethernet MAC address of the AP that is associated with the Cisco WLC.

Step 5 Click **Add**.

Step 6 To enable FlexConnect Local Switching with VLAN ID:

a) Enable **FlexConnect Local Switching** under **External Module Configuration**.
b) Enter a value between 2 and 4096 in the **VLAN ID** box.
c) Click **Apply**.

Step 7 Save the configuration.

Configuring VLAN Tagging for USC8x18 Dual-Mode Module in FlexConnect Group Local Switching (CLI)

- **config flexconnect group** *group-name* **module-vlan enable vlan** *vlan-id*—Enables FlexConnect local switching for the FlexConnect group
- **config flexconnect group** *group-name* **module-vlan disable**—Disables the FlexConnect local switching for the FlexConnect group
- **show flexconnect group detail** *group-name* **module-vlan**—Displays status of the FlexConnect local switching and VLAN ID in the group

Configuring USC8x18 Dual-Mode Module in Local Mode Central Switching (GUI)

Step 1 Create a Remote LAN.
For instructions to create a remote LAN, see the *Configuring Remote LANs* chapter under *WLANs*.

Step 2 On the **WLANs > Edit** page, click the **Security** tab.

Step 3 In the **Layer 2** sub-tab, uncheck the **MAC Filtering** check box.
Note Remote LAN should be configured only with open security. 802.1X security is not supported.

Step 4 To see the current state of the 3G/4G client, choose **Monitor** > **Clients** to open the **Clients** page.

Step 5 Save the configuration.

Configuring USC8x18 Dual-Mode Module in Local Mode Central Switching (CLI)

- Create a Remote LAN.
  For instructions to create a remote LAN, see the *Configuring Remote LANs* chapter under *WLANs*.
- **config interface 3g-vlan** *interface-name* {**enable** | **disable**}—Enables or disables the 3G/4G-VLAN interface
- **show interface detailed** *interface-name*—Displays status of the 3G/4G-VLAN flag
- **show client summary ip**—Displays status of the 3G/4G clients

LED Settings

Information About Configuring LED States for Access Points

In a wireless LAN network where there are a large number of access points, it is 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.

The LED state configuration at the global level takes precedence over the AP level.

Configuring the LED State for Access Points 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** check box.

Step 3 Choose **Enable** from the drop-down list adjacent to this check box.

Step 4 Click **Apply**.

Configuring the LED State for Access Point in a Network Globally (CLI)

- Set the LED state for all access points associated with a controller by entering this command:
  config ap led-state {**enable** | **disable**} **all**

Configuring LED State on a Specific 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** check box.

Step 4 Choose **Enable** from the drop-down list adjacent to this text box.

Step 5 Click **Apply**.

Configuring LED State on a Specific Access Point (CLI)

Step 1 Determine the ID of the access point for which you want to configure the LED state by entering this command:
show ap summary

Step 2 Configure the LED state by entering the following command:
config ap led-state {**enable** | **disable**} *Cisco_AP*

Configuring Flashing LEDs

Information About Configuring Flashing LEDs

Controller software enables you to flash the LEDs on an access point in order to locate it. All Cisco 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:

1. Configure the LED flash for an AP by entering this command:

   config ap led-state flash {*seconds* | **indefinite** | **disable**} {*Cisco_AP*}

   The valid LED flash duration for the AP is 1 to 3600 seconds. You can also configure the LED to flash indefinitely or to stop flashing the LED.

2. Disable LED flash for an AP after enabling it by entering this command:

   config ap led-state flash disable *Cisco_AP*

   The 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.

3. Save your changes by entering this command:

   save config

4. Check the status of LED flash for the AP by entering this command:

   show ap led-flash *Cisco_AP*

   Information similar to the following appears:

```
(Cisco Controller)> show ap led-flash AP1040_46:b9
Led Flash..................................... Enabled for 450 secs, 425 secs left
```

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.

Configuring LED Flash State on a Specific 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 In the **LED Flash State** section, select one of the following radio buttons:

- Click the LED flash duration for the AP option and enter the duration range from 1 to 3600 seconds.

- Click the **Indefinite** option to configure the LED to flash indefinitely.
- Click the **Disable** option to stop flashing the LED.

Step 4 Click **Apply**.

Access Points with Dual-Band Radios

Configuring Access Points with Dual-Band Radios (GUI)

Step 1 Choose **Wireless** > **Access Points** > **Radios** > **Dual-Band Radios** to open the Dual-Band Radios page.

Step 2 Hover your cursor over the blue drop-down arrow of the AP and click **Configure**.

Step 3 Configure the Admin Status.

Step 4 Configure CleanAir Admin Status as one of the following:

- Enable
- Disable
- 5 GHz Only
- 2.4 GHz Only

Step 5 Click **Apply**.

Step 6 Click **Save Configuration**.

What to Do Next

You can monitor the access points with dual-band radios by navigating to **Monitor** > **Access Points** > **Radios** > **Dual-Band Radios**.

Configuring Access Points with Dual-Band Radios (CLI)

- Configure an access point with dual-band radios by entering this command:
  config 802.11-abgn {**enable** | **disable**} *ap-name*
- Configure the CleanAir features for an access point with dual-band radios by entering this command:
  config 802.11-abgn cleanair {**enable** | **disable**} *ap-name* **band** *2.4-or-5-GHz*

Link Latency

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.

The following are some guidelines for link latency:

- 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.
- You can configure link latency for a specific access point using the controller GUI or CLI or for all access points joined to the controller using the CLI.

Restrictions for Link Latency

- Link latency is supported for use only with FlexConnect access points in connected mode. FlexConnect access points in standalone mode are not supported.

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.

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 reappears, 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*