Controlling Mesh Access Points

This chapter describes Cisco indoor and outdoor mesh access points and explains how to connect them to the controller and manage access point settings. It contains these sections:

Cisco Aironet Mesh Access Points

Controller software release 6.0 supports these Cisco Aironet mesh access points:

- Cisco Aironet 1520 series outdoor mesh access points consist of the 1522 dual-radio mesh access point and the 1524PS/1524SB multi-radio mesh access point.

  Note Refer to the *Cisco Aironet 1520 Series Outdoor Mesh Access Point Hardware Installation Guide* for details on the physical installation and initial configuration of the mesh access points at the following link:

  http://www.cisco.com/c/en/us/support/wireless/aironet-1520-series/tsd-products-support-series-home.html

- Cisco Aironet 1130AG and 1240AG series indoor mesh access points.

  Note AP1130 and AP1240 must be converted to operate as indoor mesh access points. Refer to the "Converting Indoor Access Points to Mesh Access Points (1130AG, 1240AG)" section on page 8-54.

Note All features discussed in this chapter apply to indoor (1130, 1240) and outdoor mesh access points (1522, 1524PS/1524SB) unless noted otherwise. *Mesh access point* or *MAP* is hereafter used to address both indoor and outdoor mesh access points.

Note Cisco Aironet 1505 and 1510 access points are not supported in this release.

Note Refer to the *Release Notes for Cisco Wireless LAN Controllers and Mesh Access Points for Release 6.0* for mesh feature summary, operating notes and software upgrade steps for migrating from 4.1.19x.xx mesh releases to controller release 6.0 at:

http://www.cisco.com/c/en/us/support/wireless/4400-series-wireless-lan-controllers/products-release-notes-list.html

Licensing for Indoor Mesh Access Points on a 5500 Series Controller

In order to use indoor mesh access points with a 5500 series controller, a wplus license must be used on the controller. If an indoor mesh access point attempts to join a controller that is using only a base license (and not the wplus license), the following message appears in the controller trap log: "License Not Available for feature: IndoorMeshAP." To view the controller trap log, choose **Monitor** and click **View All** under "Most Recent Traps" on the controller GUI.

Refer to the *Configuring Controller Settings* chapter for information on obtaining and installing licenses.

Note Outdoor mesh access points do not require a wplus license.

Note Other controller platforms (such as the 2100 and 4400 series controllers) also require a license for use with indoor mesh access points.

Note The wplus license is not applicable for controller release 6.0.196.0 and above.

Access Point Roles

Access points within a mesh network operate as either a root access point (RAP) or a mesh access point (MAP).

RAPs have wired connections to their controller, and MAPs have wireless connections to their controller.

MAPs communicate among themselves and back to the RAP using wireless connections over the 802.11a radio backhaul. MAPs use the Cisco Adaptive Wireless Path Protocol (AWPP) to determine the best path through the other mesh access points to the controller.

All the possible paths between the MAPs and RAPs form the wireless mesh network.

Network Access

Wireless mesh networks can simultaneously carry two different traffic types: wireless LAN client traffic and MAP Ethernet port traffic.

Wireless LAN client traffic terminates on the controller, and the Ethernet traffic terminates on the Ethernet ports of the mesh access points.

Access to the wireless LAN mesh for mesh access points is managed by:

- MAC authentication–Mesh access points are added to a reference-able database to ensure they are allowed access to a given controller and the mesh network. Refer to "Adding Mesh Access Points to the Mesh Network" section on page 8-11.
- External RADIUS authentication–Mesh access points can be externally authorized and using a RADIUS server such as Cisco ACS (4.1 and later) that supports the client authentication type of EAP-FAST with certificates. Refer to the "Configuring RADIUS Servers" section on page 8-14.

Network Segmentation

Membership to the wireless LAN mesh network for mesh access points is controlled by:

- Bridge group name–Mesh access points can be placed in like bridge groups to manage membership or provide network segmentation. Refer to "Using the GUI to Configure Antenna Gain" section on page 8-28.

Deployment Modes

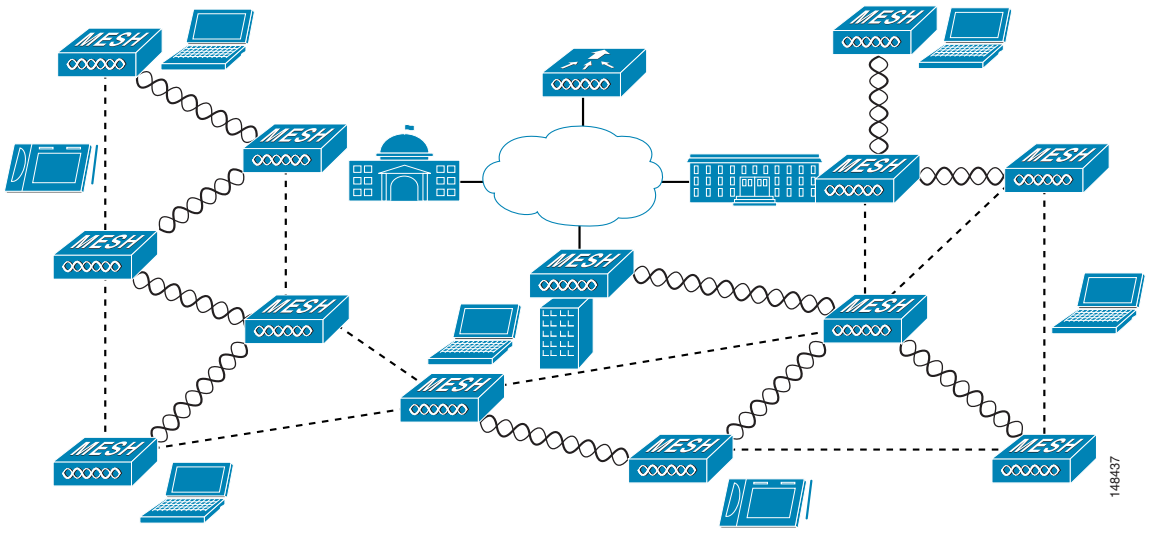
Mesh access points support multiple deployment modes, including the following:

- Wireless mesh
- WLAN backhaul
- Point-to-multipoint wireless bridging
- Point-to-point wireless bridging

Cisco Wireless Mesh Network

In a Cisco wireless outdoor mesh network, multiple mesh access points comprise a network that provides secure, scalable outdoor wireless LANs. Figure 8-1 shows an example mesh deployment.

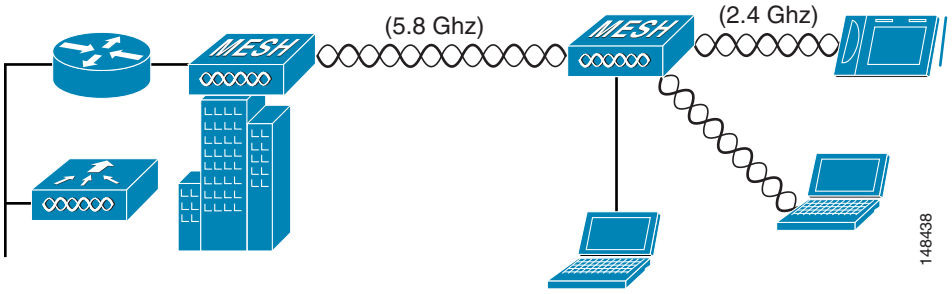
Figure 8-1 Wireless Mesh Deployment



Wireless Backhaul

Mesh access points can provide a simple wireless backhaul solution, which provides 802.11b/g services to wireless LAN and wired clients. This configuration is basically a wireless mesh with one MAP. Figure 8-2 shows an example of this deployment type.

Figure 8-2 Wireless Backhaul Deployment



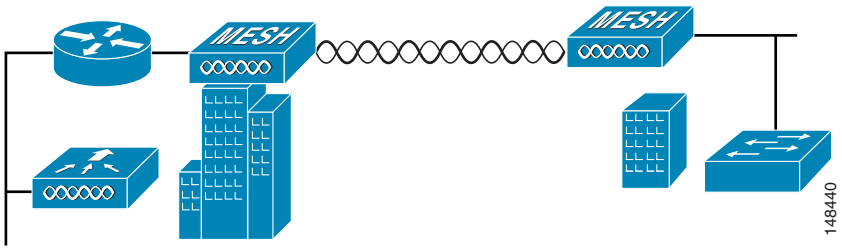
Point-to-Point Wireless Bridging

Mesh access points can support a point-to-point bridging application. In this deployment, mesh access points extend a Layer 2 network by using the backhaul radio to bridge two segments of a switched network (see Figure 8-3). This is fundamentally a wireless mesh network with one MAP and no wireless LAN clients.

Client access can be provided with Ethernet bridging enabled, although if bridging between buildings, MAP coverage from a high rooftop might not be suitable for client access.

If you intend to use an Ethernet bridged application, you must enable the bridging feature on the RAP and on all MAPs in that segment. Also verify that any attached switches to the Ethernet ports of your MAPs are not using VLAN Trunking Protocol (VTP). VTP can reconfigure the trunked VLANs across your mesh and possibly cause a loss in connection for your RAP to its primary WLC. If improperly configured, it can take down your mesh deployment.

Figure 8-3 Wireless Point-to-Point Bridge Deployment

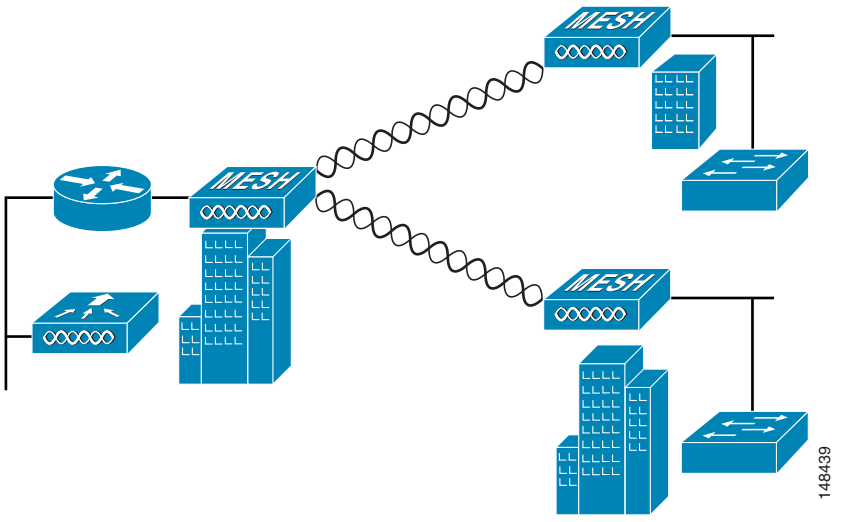


Point-to-Multipoint Wireless Bridging

Mesh access points support point-to-multipoint bridging applications. Specifically, a RAP acting as a root bridge connects to multiple MAPs as non-root bridges with their associated wired LANs. By default, bridging is disabled for all MAPs. If Ethernet bridging is used, you must enable it on the controller for the respective MAP and for the RAP. Refer to the "Configuring Ethernet Bridging and Ethernet VLAN Tagging" section on page 8-31 for configuration details.

Figure 8-4 shows a simple point-to-multipoint deployment with one RAP and two MAPs. This configuration is fundamentally a wireless mesh network with no wireless LAN clients. Client access can be provided with Ethernet bridging enabled; however, if bridging between buildings, MAP coverage from a high rooftop might not be suitable for client access.

Figure 8-4 Wireless Point-to-Multipoint Bridge Deployment



Architecture Overview

CAPWAP

CAPWAP is the provisioning and control protocol used by the controller to manage access points (mesh and non-mesh) in the network. This protocol replaces LWAPP in controller software release 5.2 or later.

Cisco Adaptive Wireless Path Protocol Wireless Mesh Routing

The Cisco Adaptive Wireless Path Protocol (AWPP) is designed specifically for wireless mesh networking. The path decisions of AWPP are based on link quality and the number of hops.

Ease of deployment, fast convergence, and minimal resource consumption are also key components of AWPP.

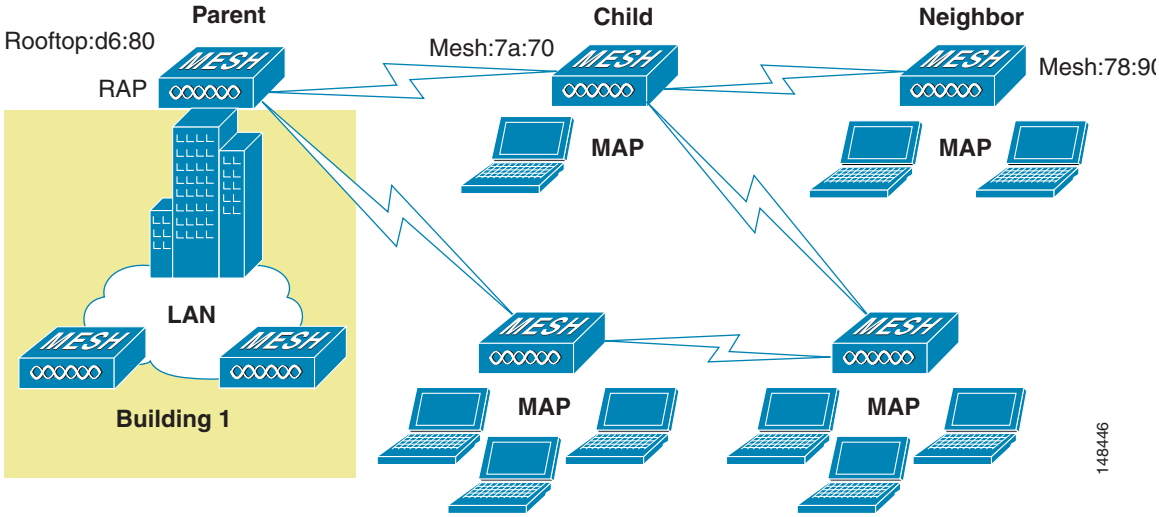
The goal of AWPP is to find the best path back to a RAP for each MAP that is part of the RAP's bridge group. To do this, the MAP actively solicits for neighbor MAPs. During the solicitation, the MAP learns all of the available neighbors back to a RAP, determines which neighbor offers the best path, and then synchronizes with that neighbor.

Mesh Neighbors, Parents, and Children

Relationships among access points with the mesh network are labelled as parent, child, or neighbor (see Figure 8-5).

- A parent access point offers the best route back to the RAP based on its ease values. A parent can be either the RAP itself or another MAP.
  - Ease is calculated using the SNR and link hop value of each neighbor. Given multiple choices, generally an access point with a higher ease value is selected.
- A child access point selects the parent access point as its best route back to the RAP.
- A neighbor access point is within the radio frequency (RF) range of another access point but is not selected as its parent or a child because its *ease* values are lower than that of the parent.

Figure 8-5 Parent, Child and Neighbor Access Points



Wireless Mesh Constraints

Here are a few system characteristics to consider when designing and building a wireless mesh network. Some of these apply to the backhaul network design and others to the CAPWAP controller design:

- Cisco recommends setting the backhaul rate to **auto**.

  When the bridge data rate is set to **auto**, the mesh backhaul chooses the highest rate where the next higher rate cannot be used due to unsuitable conditions for that specific rate (and not because of conditions that affect all rates).

  - Typically, 24 Mbps is chosen as the optimal backhaul rate because it corresponds with the maximum coverage of the WLAN portion of the client WLAN of the MAP; that is, the distance between MAPs using 24 Mbps backhaul should allow for seamless WLAN client coverage between the MAPs.
  - A lower bit rate might allow a greater distance between mesh access points, but there are likely to be gaps in the WLAN client coverage, and the capacity of the backhaul network is reduced.
  - An increased bit rate for the backhaul network either requires more mesh access points or results in a reduced SNR between mesh access points, limiting mesh reliability and interconnection.
  - The wireless mesh backhaul bit rate is set on the access point.

  Note To set backhaul bit rate for each access point, choose **WIRELESS > Access Points > All APs**, then click an AP name and click the **Mesh** tab.

  - The required minimum LinkSNR for backhaul links per data rate is shown in Table 8-1.

Table 8-1 Backhaul Data Rates and Minimum LinkSNR Requirements

Data Rate	Minimum Required LinkSNR (dB)
54 Mbps	31
48 Mbps	29
36 Mbps	26
24 Mbps	22
18 Mbps	18
12 Mbps	16
9 Mbps	15
6 Mbps	14

- The required minimum LinkSNR is driven by the data rate and the following formula: Minimum SNR + fade margin. Table 8-2 summarizes the calculation by data rate.
  - Minimum SNR refers to an ideal state of non-interference, non-noise and a system packet error rate (PER) of no more than 10%
  - Typical fade margin is approximately 9 to 10 dB
  - We do not recommend using data rates greater than 24 Mbps in municipal mesh deployments as the SNR requirements do not make the distances practical

Table 8-2 Minimum Required LinkSNR Calculations by Data Rate

Date Rate	Minimum SNR (dB) +	Fade Margin =	Minimum Required LinkSNR (dB)
6	5	9	14
9	6	9	15
12	7	9	16
18	9	9	18
24	13	9	22
36	17	9	26

- Number of backhaul hops is limited to eight, but three to four is recommended

  The number of hops is recommended to be limited to three–four primarily to maintain sufficient backhaul throughput, because each mesh AP uses the same radio for transmission and reception of backhaul traffic. This means that throughput is approximately halved over every hop. For example, the maximum throughput for 24 Mbps is approximately 14 Mbps for the first hop, 9 Mbps for the second hop, and 4 Mbps for the third hop.
- Number of MAPs per RAP

  There is no current software limitation of how many MAPs per RAP you can configure. However, it is suggested that you limit this to 20 MAPs per RAP.
- Number of controllers

  The number of controllers per mobility group is limited to 72.
- Number of mesh access points supported per controller (see Table 8-3).

Table 8-3 Mesh Access Point Support by Controller Model

Controller Model	Local AP Support (non-mesh)[1]	Maximum Possible Mesh AP Support	RAPs	MAPs	Total Mesh AP Support (RAP + MAP)
5508[2]	250	250	1	249	250
			100	150	250
			150	100	250
			250	0	250
4404[3]	100	150	1	149	150
			50	100	150
			75	50	125
			100	0	100
2106[3]	6	11	1	10	11
			2	8	10
			3	6	9
			4	4	8
			5	2	7
			6	0	6
2112[2]	12	12	1	11	12
			3	9	12
			6	6	12
			9	3	12
			12	0	12
2125[2]	25	25	1	24	25
			5	20	25
			10	15	25
			15	10	25
			20	5	25
			25	0	25
WiSM[3]	300	375	1	374	375
			100	275	375
			250	100	350
			300	0	300

1. Local AP support is the total number of non-mesh APs supported on the controller model.
2. For 5508, 2112, and 2125 controllers, the number of MAPs is equal to (local AP support - number of RAPs).
3. For 4404, 2106, and WiSM controllers, the number of MAPs is equal to ((local AP support - number of RAPs) x 2), not to exceed the maximum possible mesh AP support.

Adding Mesh Access Points to the Mesh Network

This section assumes that the controller is already active in the network and is operating in Layer 3 mode. Layer 3 mode is recommended for large deployments.

Before adding a mesh access point to a network, do the following:

1. Add the MAC address of the MAP to the controller's MAC filter. See the "Adding MAC Addresses of Mesh Access Points to the Controller Filter List" section on page 8-12.
   - To configure external authentication of MAC addresses using an external RADIUS server, see the "Configuring External Authentication and Authorization Using a RADIUS Server" section on page 8-14.
2. Configure the DCA channels for the mesh access points. See the "Using the GUI to Configure Dynamic Channel Assignment" section on page 11-13 for details.
3. Configure the AP mode for the mesh access point. See the "Configuring the AP Mode" section on page 8-17.

Note This procedure is not required for 1520 series access points. The default mode for 1520 series access points is Bridge.

4. Define the role (RAP or MAP) for the mesh access point. See the "Defining the Mesh Access Point Role" section on page 8-18.
5. Configure the channel assignment on the RAP for serial backhaul (if desired). See the "Antennas and Channel Assignment on the AP1524SB" section on page 8-19.
6. Configure a primary, secondary, and tertiary controller for each MAP. See the "Verifying that Access Points Join the Controller" and "Configuring Backup Controllers" sections in Chapter 7.
7. Configure global mesh parameters. See the "Configuring Global Mesh Parameters" section on page 8-22.
8. Configure bridging parameters. See the "Configuring Ethernet Bridging and Ethernet VLAN Tagging" section on page 8-31.
   a. Configure Bridge Group Names.
   b. Assign IP addresses to MAPs unless using DHCP.

      If using DHCP, configure Option 43 and Option 60. Refer to the *Cisco Aironet 1520 Series Outdoor Mesh Access Point Hardware Installation Guide.*
9. Configure mobility groups (if desired) and assign controllers. See the Chapter 12, "Configuring Mobility Groups."
10. Configure advanced features such as using voice and video in the network. See the "Configuring Advanced Features" section on page 8-38.

Adding MAC Addresses of Mesh Access Points to the Controller Filter List

You must enter the MAC address for all mesh access points that you want to use in the mesh network into the appropriate controller. A controller only responds to discovery requests from outdoor radios that appear in its authorization list. MAC filtering is enabled by default on the controller, so only the MAC addressed need be configured.

You can add the access point using either the GUI or the CLI.

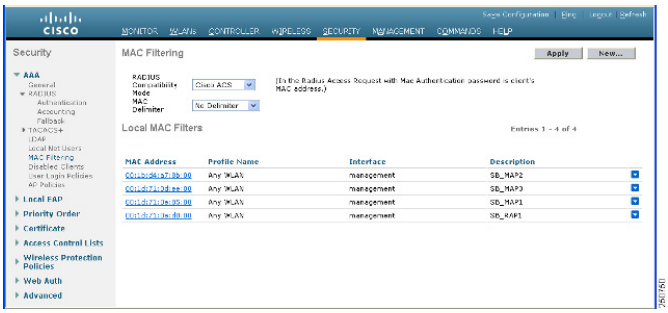
Note You can also download the list of access point MAC addresses and push them to the controller using the Cisco Wireless Control System (WCS). Refer to the *Cisco Wireless Control System Configuration Guide, Release 6.0* for instructions.

Using the GUI to Add MAC Addresses of Mesh Access Points to the Controller Filter List

Using the controller GUI, follow these steps to add a MAC filter entry for the access point on the controller.

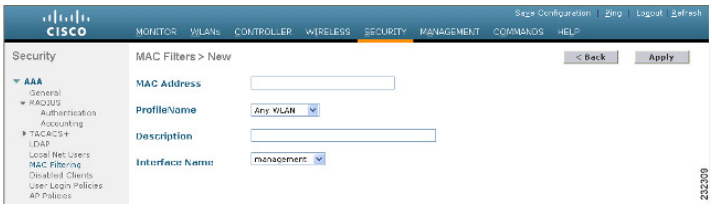
Step 1 Click **Security** > **AAA** > **MAC Filtering** to open the MAC Filtering page (see Figure 8-6).

Figure 8-6 MAC Filtering Page



Step 2 Click **New** to open the MAC Filters > New page (see Figure 8-7).

Figure 8-7 MAC Filters > New Page



Step 3 In the MAC Address field, enter the MAC address of the mesh access point.

Note For 1522 and 1524PS/1524SB outdoor mesh access points, enter the BVI MAC address of the mesh access point into the controller as a MAC filter. For 1130 and 1240 indoor mesh access points, enter the Ethernet MAC address. If the required MAC address does not appear on the exterior of the mesh access point, enter the following command from the access point console to determine the BVI and Ethernet MAC addresses: **sh int | i Hardware**.

Step 4 From the Profile Name drop-down box, choose **Any WLAN**.

Step 5 In the Description field, enter a description of the access point. The text that you enter identifies the mesh access point on the controller.

Note You might want to include an abbreviation of its name and the last few digits of the MAC address, such as *ap1522:62:39:10*. You can also note details on its location, such as *roof top* or *pole top* or its cross streets.

Step 6 From the Interface Name drop-down box, choose the controller interface to which the access point is to connect.

Step 7 Click **Apply** to commit your changes. The access point now appears in the list of MAC filters on the MAC Filtering page.

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

Step 9 Repeat this procedure to add the MAC addresses of additional access points to the list.

Using the CLI to Add MAC Addresses of Mesh Access Points to the Controller Filter List

Using the controller CLI, follow these steps to add a MAC filter entry for the access point on the controller.

Step 1 To add the MAC address of an access point to the controller filter list, enter this command:

config macfilter add *ap_mac wlan_id interface* [*description*]

A value of zero (0) for the *wlan_id* parameter specifies any WLAN, and a value of zero (0) for the *interface* parameter specifies none. You can enter up to 32 characters for the optional *description* parameter.

Step 2 To save your changes, enter this command:

save config

Configuring External Authentication and Authorization Using a RADIUS Server

Controller software release 5.2 or later supports external authorization and authentication of mesh access points using a RADIUS server such as Cisco ACS (4.1 and later). The RADIUS server must support the client authentication type of EAP-FAST with certificates.

Before you employ external authentication within the mesh network, you must make these changes:

- Configure the RADIUS server to be used as an AAA server on the controller.
- Configure the controller on the RADIUS server.
- Add the mesh access point configured for external authorization and authentication to the user list of the RADIUS server. For additional details, refer to the "Adding a Username to a RADIUS Server" section on page 8-15.
- Configure EAP-FAST on the RADIUS server and install the certificates. EAP-FAST authentication is required if mesh access points are connected to the controller using an 802.11a interface; the external RADIUS servers need to trust Cisco Root CA 2048. For information on installing and trusting the CA certificates, see the "Configuring RADIUS Servers" section on page 8-14.

Note If mesh access points connect to a the controller using a Fast Ethernet or Gigabit Ethernet interface, only MAC authorization is required.

Note This feature also supports local EAP and PSK authentication on the controller.

Configuring RADIUS Servers

Follow these steps to install and trust the CA certificates on the RADIUS server:

Step 1 Using Internet Explorer, download the CA certificates for Cisco Root CA 2048:

- http://www.cisco.com/security/pki/certs/crca2048.cer
- http://www.cisco.com/security/pki/certs/cmca.cer

Step 2 Install the certificates:

a. From the CiscoSecure ACS main menu, click, click **System Configuration > ACS Certificate Setup > ACS Certification Authority Setup**.

b. In the **CA certificate file** box, type the CA certificate location (path and name). For example: c:\Certs\crca2048.cer.

c. Click **Submit**.

Step 3 Configure the external RADIUS servers to trust the CA certificate.

a. From the CiscoSecure ACS main menu, choose **System Configuration > ACS Certificate Setup > Edit Certificate Trust List**. The Edit Certificate Trust List appears.

b. Check the check box next to the **Cisco Root CA 2048 (Cisco Systems)** certificate name.

c. Click **Submit**.

d. To restart ACS, choose **System Configuration > Service Control**, and then click **Restart**.

Note For additional configuration details on Cisco ACS servers, refer to the following links:
http://www.cisco.com/c/en/us/support/security/secure-access-control-server-windows/products-installation-and-configuration-guides-list.html (Windows)

http://www.cisco.com/c/en/us/support/security/secure-access-control-server-unix/tsd-products-support-configure.html (UNIX)

Adding a Username to a RADIUS Server

Add MAC addresses of mesh access point that are authorized and authenticated by external RADIUS servers to the user list of that server *prior* to enabling RADIUS authentication for a mesh access point.

For remote authorization and authentication, EAP-FAST uses the manufacturer's certificate (CERT) to authenticate the child mesh access point. Additionally, this manufacturer certificate-based identity serves as the username for the mesh access point in user validation.

For IOS-based mesh access points (1130, 1240, 1522, 1524), in addition to adding the MAC address to the user list, you need to enter the *platform_name_string–Ethernet_MAC_address* string to the user list (for example, c1240-001122334455). The controller first sends the MAC address as the username; if this first attempt fails, then the controller sends the *platform_name_string–Ethernet_MAC_address* string as the username.

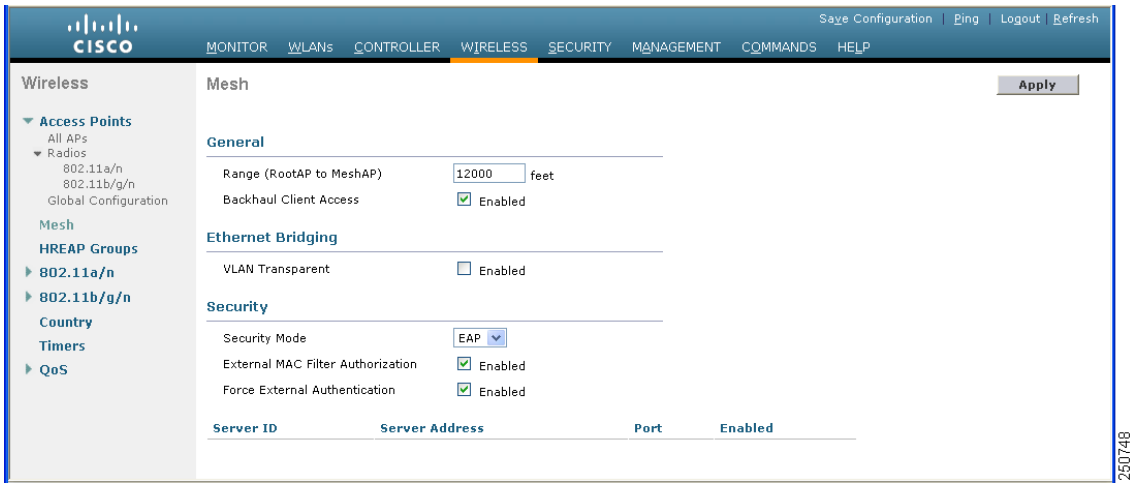
Note If you enter only the *platform_name_string–Ethernet_MAC_address* string to the user list, you will see a first-try failure log on the AAA server; however, the IOS-based mesh access point will still be authenticated on the second attempt using the *platform_name_string–Ethernet_MAC_address* string as the username.

Using the GUI to Enable External Authentication of Mesh Access Points

Using the controller GUI, follow these steps to enable external authentication for a mesh access point.

Step 1 Click **Wireless > Mesh** to open the Mesh page (see Figure 8-8).

Figure 8-8 Mesh Page



Step 2 Choose **EAP** from the Security Mode drop-down box.

Step 3 Check the **Enabled** check boxes for the External MAC Filter Authorization and Force External Authentication options.

Step 4 Click **Apply** to commit your changes.

Step 5 Click **Save Configuration** to save your changes.

Using the CLI to Enable External Authentication of Mesh Access Points

To enable external authentication for mesh access points using the CLI, enter the following commands:

config mesh security eap

config macfilter mac-delimiter colon

config mesh security rad-mac-filter enable

config mesh radius-server *index* enable

config mesh security force-ext-auth enable (Optional)

Using the CLI to View Security Statistics

To view security statistics for mesh access points using the CLI, enter the following command:

show mesh security-stats *Cisco_AP*

Command shows packet error statistics and a count of failures, timeouts, and association and authentication successes as well as reassociations and reauthentications for the specified access point and its child.

Configuring the AP Mode

Note This procedure is not required for 1520 series access points. The default mode for 1520 series access points is Bridge.

By default, access points are configured as Local. To configure the mesh access points, you first must change the access point mode to Bridge using the GUI or CLI.

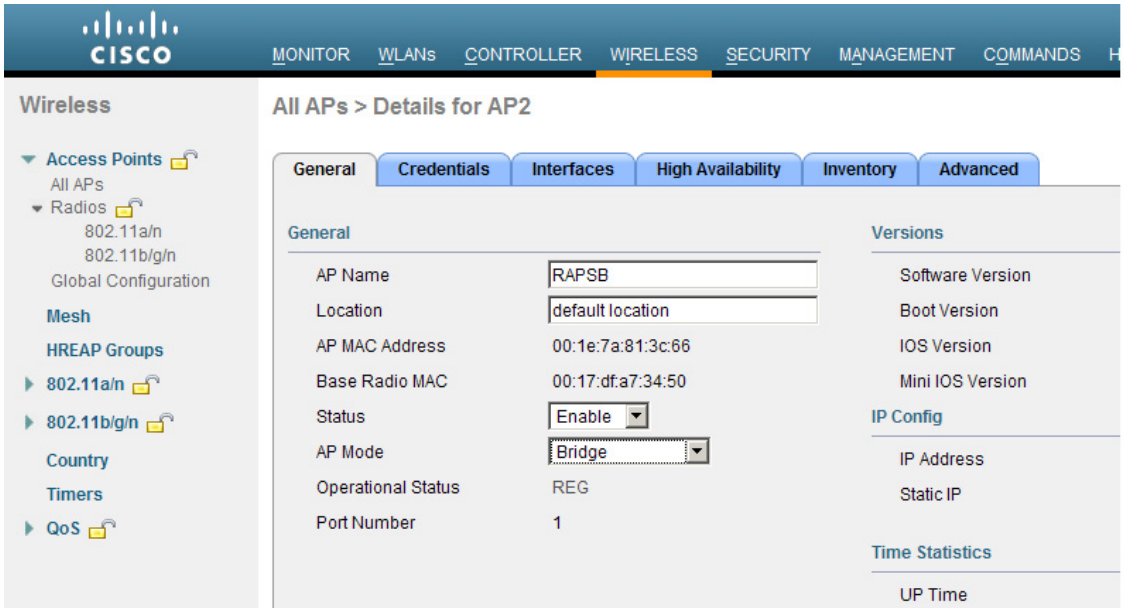
Using the GUI to Configure the AP Mode

To configure the AP mode using the GUI, follow these steps:

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

Step 2 Click the name of an access point. The All APs > Details (General) page appears (Figure 8-9).

Figure 8-9 All APs > Details for (General) Page



Step 3 Choose **Bridge** from the AP Mode drop-down box.

Step 4 Click **Apply** to commit your changes and to cause the access point to reboot.

Using the CLI to Configure the AP Mode

To configure the AP mode using the CLI, enter the following command:

config ap mode bridge *Cisco_AP*

Defining the Mesh Access Point Role

By default, the 152x mesh access points are shipped with a radio role set to MAP. You must reconfigure a mesh access point to act as a RAP.

Note In order to use the AP1130 and AP1240 indoor mesh access points with a 5500 series controller, a wplus license must be used on the controller.

Using the GUI to Configure the AP Role

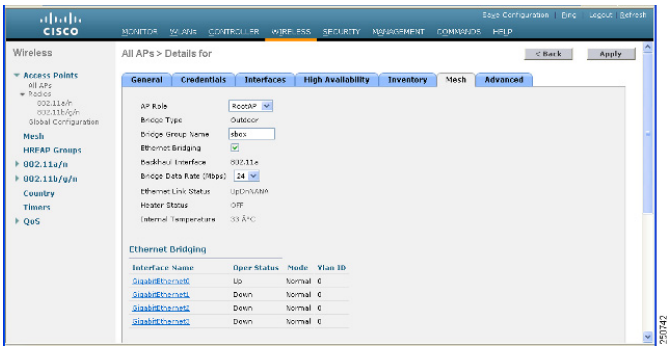
To configure the role of a mesh access point using the GUI, follow these steps:

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

Step 2 Click the name of an access point. The All APs > Details (General) page appears.

Step 3 Click the **Mesh** tab (Figure 8-10).

Figure 8-10 All APs > Details for (Mesh) Page



Step 4 Choose **RootAP or MeshAP** from the AP Role drop-down box.

Step 5 Click **Apply** to commit your changes and to cause the access point to reboot.

Using the CLI to Configure the AP Role

To configure the role of a mesh access point using the CLI, enter the following command:

config ap role {**rootAP** | **meshAP**} *Cisco_AP*

Antennas and Channel Assignment on the AP1524SB

The AP1524SB (serial backhaul) access point is introduced in controller software release 6.0. The AP1524SB has two backhaul radios: one uplink and one downlink. The AP1524SB is suitable for linear deployments.

The AP1524SB mesh access point operates as a RAP or a MAP. The antenna ports are labeled on the AP1524SB and are connected internally to the radios in each slot. The AP1524SB has six ports with three radio slots (0, 1, 2) as described in Table 8-4:

Table 8-4 AP1524SB Antenna Ports

Antenna Port	Radio Slot	Description
1	1	5 GHz Used for backhaul and universal client access
2	0	2.4 GHz Used for client access
3	0	2.4 GHz Used for client access
4	0	2.4 GHz Used for client access
5	–	Not connected
6	2	5 GHz Used for backhaul **Note** We recommend that you use the directional antenna on the MAPs for uplink on the slot 2 radio.

Note Depending on product model, the AP1524SB could have either 5.0-GHz radios or 5.8-GHz sub-band radios installed in slot 1 and slot 2. Regardless of the radios installed, the AP1524SB running controller software release 6.0 is restricted to the UNII-3 channels (149, 153, 157, 161, and 165) in slot 1 and slot 2.

The two 5.8-GHz radios are used for the serial backhaul, which provides uplink and downlink access. Each 5.8-GHz radio backhaul is configured with a different backhaul channel, so there is no need to use the same shared wireless medium between the north-bound and south-bound traffic in a mesh tree-based network.

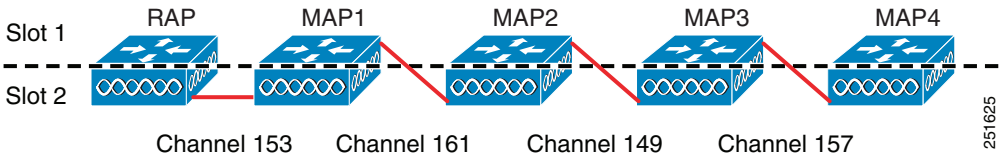
On the RAP, the radio in slot 2 is used to extend the backhaul in the downlink direction; the radio in slot 1 is used for client access.

On the MAP, the radio in slot 2 is used for the backhaul in the uplink direction; the radio in slot 1 is used for the backhaul in the downlink direction as well as client access.

You only need to configure the RAP downlink (slot 2) channel. The MAPs automatically select their channels from the channel subset. The available channels for the 5.8 GHz band are 149, 153, 157, 161, and 165.

Figure 8-11 shows a channel selection example when the RAP downlink channel is 153.

Figure 8-11 Channel Selections Examples

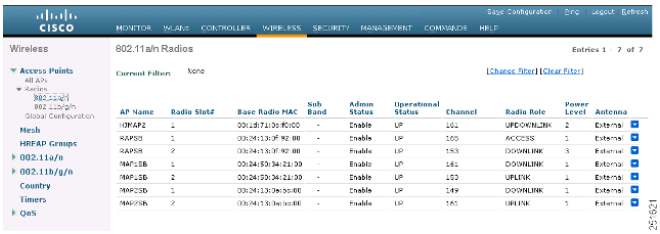


Using the GUI to Configure the Channels on the Serial Backhaul

Follow these steps to configure channels on the serial backhaul on the RAP using the controller GUI:

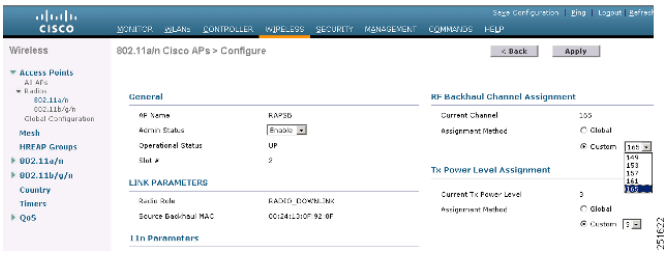
Step 1 Click **Wireless** > **Access Points** > **Radios** > **802.11a/n** to open the 802.11a/n Radios page (see Figure 8-12).

Figure 8-12 802.11a/n Radios Page



Step 2 Hover your cursor over the blue drop-down arrow for the RAP antenna in slot 2 (the backhaul downlink) and choose **Configure**. The 802.11a/n Cisco APs > Configure page appears (see Figure 8-13).

Figure 8-13 802.11a/n Cisco APs > Configure Page



Step 3 For the RF Backhaul Channel Assignment, choose the **Custom** assignment method, and select a channel from the drop-down list. The available channels for the 5.8-GHz band are 149, 153, 157, 161, and 165.

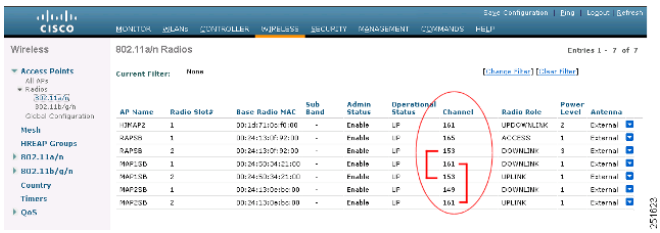
Step 4 For the Tx Power Level Assignment, choose the **Custom** assignment method, and select a power level. Valid values are 1 through 5; the default value is 1.

Note Radio Resource Management (RRM) is disabled by default; RRM cannot be enabled for the backhaul.

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

Step 6 From the 802.11a/n Radios page, verify that uplink and downlink channels have been assigned (see Figure 8-14).

Figure 8-14 Channel Assignment



Using the CLI to Configure the Channels on the Serial Backhaul

Follow these steps to configure channels on the serial backhaul on the RAP using the controller CLI:

Step 1 To configure the backhaul channel on the radio in slot 2 of the RAP, enter this command:

config slot 2 channel ap *Cisco_RAPSB channel*

The available channels for the 5.8-GHz band are 149, 153, 157, 161, and 165.

Step 2 To configure the transmit power level on the radio in slot 2 of the RAP, enter this command:

config slot 2 txPower ap *Cisco_RAPSB power*

Valid values are 1 through 5; the default value is 1.

Step 3 To display the configurations on the mesh access points, enter these commands:

- **show mesh path** *MAP*

  Information similar to the following appears:

```
AP Name/Radio      Channel Rate Link-Snr Flags    State
-----------------  ------- ---- -------- -------  -----

MAP1SB             161     auto 60       0x10ea9d54 UPDATED NEIGH PARENT BEACON
RAPSB              153     auto 51       0x10ea9d54 UPDATED NEIGH PARENT BEACON
RAPSB             is a Root AP.
```

- **show mesh backhaul** *RAPSB*

  Information similar to the following appears:

```
Current Backhaul Slot(s)..................... 1, 2,

Basic Attributes for Slot  1
    Radio Type.............................. RADIO_TYPE_80211a
    Radio Role.............................. ACCESS
    Administrative State ................... ADMIN_ENABLED
    Operation State ........................ UP
    Current Tx Power Level ................. 1
    Current Channel ........................ 165
    Antenna Type............................ EXTERNAL_ANTENNA
    External Antenna Gain (in .5 dBm units)...... 0

Basic Attributes for Slot  2
    Radio Type.............................. RADIO_TYPE_80211a
    Radio Role.............................. RADIO_DOWNLINK
    Administrative State ................... ADMIN_ENABLED
    Operation State ........................ UP
    Current Tx Power Level ................. 3
    Current Channel ........................ 153
    Antenna Type............................ EXTERNAL_ANTENNA
    External Antenna Gain (in .5 dBm units)...... 0
```

- **show ap channel** *MAP1SB*

  Information similar to the following appears:

```
802.11b/g Current Channel ................. 11
Slot Id ................................... 0
Allowed Channel List..................... 1,2,3,4,5,6,7,8,9,10,11
802.11a(5.8Ghz) Current Channel ........... 161
Slot Id ................................... 1
Allowed Channel List..................... 149,153,157,161,165
802.11a(5.8Ghz) Current Channel ........... 153
Slot Id ................................... 2
Allowed Channel List..................... 149,153,157,161,165
```

Configuring Global Mesh Parameters

This section provides instructions for configuring the access point to establish a connection with the controller including:

- Setting the maximum range between RAP and MAP (not applicable to 1130 and 1240 indoor mesh access points)
- Enabling a backhaul to carry client traffic
- Defining whether VLAN tags are forwarded or not
- Defining the authentication mode (EAP or PSK) and method (local or external) for mesh access points including security settings (local and external authentication).

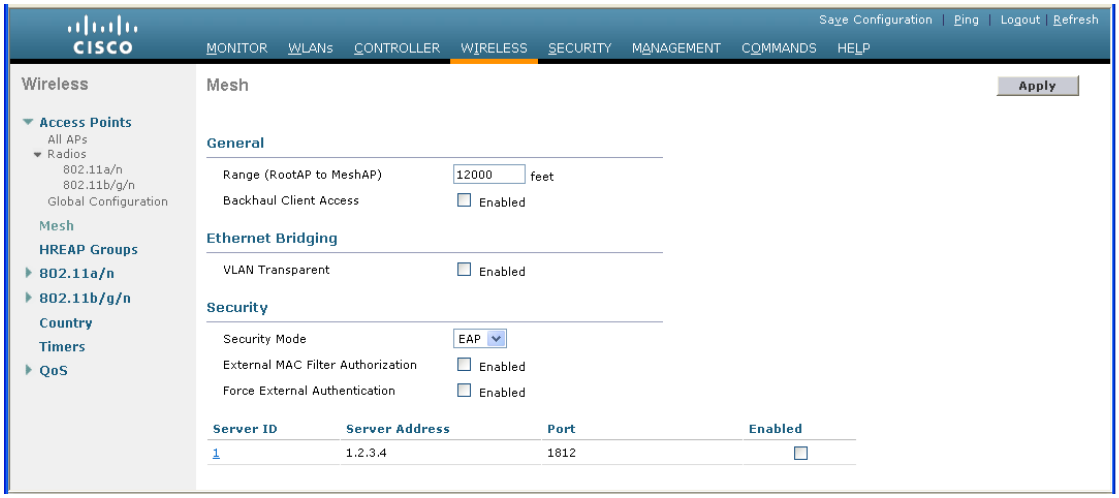
You can configure the necessary mesh parameters using the controller GUI or CLI. All parameters are applied globally.

Using the GUI to Configure Global Mesh Parameters

Using the controller GUI, follow these steps to configure global mesh parameters.

Step 1 Click **Wireless** > **Mesh** to open the Mesh page (see Figure 8-15).

Figure 8-15 Mesh Page



Step 2 Modify the mesh parameters as appropriate. Table 8-5 describes each parameter.

Table 8-5 Global Mesh Parameters

Parameter	Description
Range (RootAP to MeshAP)	**Note** This parameter applies to outdoor mesh access point. The optimum distance (in feet) that should exist between the root access point (RAP) and the mesh access point (MAP). This global parameter applies to all access points when they join the controller and all existing access points in the network. **Range:** 150 to 132,000 feet **Default:** 12,000 feet **Note** After this feature is enabled, all outdoor mesh access points reboot.
IDS (Rogue and Signature Detection	**Note** This parameter applies to outdoor mesh access points. When you enable this feature, IDS reports are generated for all traffic on the backhaul. These reports can be useful for university or enterprise outdoor campus areas, or for public safety users who want to find out who is operating in 4.9 GHz. When you disable this feature, no IDS reports are generated, which preserves bandwidth on the backhaul. **Note** IDS reporting is enabled for all indoor mesh access points and cannot be disabled. **Default:** Disabled

Table 8-5 Global Mesh Parameters (continued)

Parameter	Description
Backhaul Client Access	**Note** This parameter applies to mesh access points with two or more radios (1524SB, 1522, 1240 and 1130) *excluding* the 1524PS. When this feature is enabled, mesh access points allow wireless client association over the 802.11a radio. Therefore, a mesh access point can carry both backhaul traffic and 802.11a client traffic over the same 802.11a radio. When this feature is disabled, the mesh access point carries backhaul traffic over the 802.11a radio and allows client association only over the 802.11b/g radio. **Default:** Disabled **Note** After this feature is enabled, all mesh access points reboot.
VLAN Transparent	This feature determines how a mesh access point handles VLAN tags for Ethernet bridged traffic. **Note** See the "Configuring Ethernet Bridging and Ethernet VLAN Tagging" section on page 8-31 for overview and additional configuration details. When this feature is enabled, VLAN tags are not handled and packets are bridged as if they are untagged. When this feature is disabled, all packets are tagged as non-VLAN transparent or VLAN-opaque and all tagged packets are dropped. Unselect the check box to enable the VLAN Tagging feature. **Note** VLAN Transparent is enabled as a default to ensure a smooth software upgrade from 4.1.192.xxM releases to release 5.2 or later releases. Release 4.1.192.xxM does not support VLAN tagging. **Note** See the "Configuring Ethernet Bridging and Ethernet VLAN Tagging" section on page 8-31 for more details. The default is Enabled.
Security Mode	Defines the security mode for mesh access points: Pre-Shared Key (PSK) or Extensible Authentication Protocol (EAP). **Note** EAP must be selected if external MAC filter authorization using a RADIUS server is configured. **Note** Local EAP or PSK authentication is performed within the controller if the External MAC Filter Authorization parameter is disabled (check box unchecked). **Options:** PSK or EAP **Default:** EAP

Table 8-5 Global Mesh Parameters (continued)

Parameter	Description
External MAC Filter Authorization	MAC filtering uses the local MAC filter on the controller by default. When external MAC filter authorization is enabled, if the MAC address is not found in the local MAC filter, then the MAC address in the external RADIUS server is used. This protects your network against rogue mesh access points by preventing access points that are not defined on the external server from joining. Before you employ external authentication within the mesh network, the following configuration is required: • The RADIUS server to be used as an AAA server must be configured on the controller. • The controller must also be configured on the RADIUS server. • The mesh access point configured for external authorization and authentication must be added to the user list of the RADIUS server. – For remote authorization and authentication, EAP-FAST uses the manufacturer's certificate (CERT) to authenticate the child mesh access point. Additionally, this manufacturer certificate-based identity serves as the username for the mesh access point in user validation. – For IOS-based mesh access points (1130, 1240, 1522, 1524), in addition to adding the MAC address to the user list, you need to enter the *platform_name_string-Ethernet_MAC_address* string (for example, c1240-001122334455). The controller first sends the MAC address as the username; if this first attempt fails, the controller sends the *platform_name_string-Ethernet_MAC_address* string as the username. **Note** If you only enter the *platform_name_string-Ethernet_MAC_address* string to the user list, you will see a first-try failure log on the AAA server; however, the IOS-based mesh access point will still be authenticated on the second attempt using the *platform_name_string–Ethernet_MAC_address* string as the username. • The certificates must be installed and EAP-FAST must be configured on the RADIUS server. See the "Configuring RADIUS Servers" section on page 8-14 section for information on installing certificates. **Note** When this capability is not enabled, the controller authorizes and authenticates mesh access points using the MAC address filter. **Default:** Disabled.
Force External Authorization	When enabled along with *EAP* and *External MAC Filter Authorization* parameters, an external RADIUS server (such as Cisco 4.1 and later) handles external authorization and authentication for mesh access points by default. The RADIUS server overrides local authentication of the MAC address by the controller which is the default. **Default:** Disabled.

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

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

Using the CLI to Configure Global Mesh Parameters

Using the controller CLI, follow these steps to configure global mesh parameters.

Note Refer to the "Using the GUI to Configure Global Mesh Parameters" section on page 8-23 for descriptions, valid ranges, and default values of the parameters used in the CLI commands.

Step 1 To specify the maximum range (in feet) of all access points in the network, enter this command:

config mesh range *feet*

To see the current range, enter **show mesh range**.

Step 2 To enable or disable IDS reports for all traffic on the backhaul, enter this command:

config mesh ids-state {**enable** | **disable**}

Step 3 To specify the rate (in Mb/s) at which data is shared between access points on the backhaul interface, enter this command:

config ap bhrate {*rate* | **auto**} *Cisco_AP*

Step 4 To enable or disable client association on the primary backhaul (802.11a) of an access point, enter these commands:

config mesh client-access {**enable** | **disable**}

config ap wlan {**enable** | **disable**} **802.11a** *Cisco_AP*

config ap wlan {add | delete} 802.11a *wlan_id Cisco_AP*

Step 5 To enable or disable VLAN transparent, enter this command:

config mesh ethernet-bridging vlan-transparent {enable | disable}

Step 6 To define a security mode for the mesh access point, enter one of the following commands:

a. To provide local authentication of the mesh access point by the controller, enter this command:
config mesh security {eap | psk}

b. To store MAC address filter in an external RADIUS server for authentication instead of the controller (local), enter these commands:

config macfilter mac-delimiter colon

config mesh security rad-mac-filter enable

config mesh radius-server *index* enable

c. To provide external authentication on a RADIUS server and define a local MAC filter on the controller, enter these commands:

config mesh security eap

config macfilter mac-delimiter colon

config mesh security rad-mac-filter enable

config mesh radius-server *index* **enable**

config mesh security force-ext-auth enable

d. To provide external authentication on a RADIUS server using a MAC username (such as *c1520-123456*) on the RADIUS server, enter these commands:

config macfilter mac-delimiter colon

config mesh security rad-mac-filter enable

config mesh radius-server *index* enable

config mesh security force-ext-auth enable

Step 7 To save your changes, enter this command:

save config

Using the CLI to View Global Mesh Parameter Settings

Use these commands to obtain information on global mesh settings:

- **show mesh client-access**—Shows the status of the client-access backhaul as either enabled or disabled. When this option is enabled, mesh access points are able to associate with 802.11a wireless clients over the 802.11a backhaul. This client association is in addition to the existing communication on the 802.11a backhaul between the root and mesh access points.

```
controller >show mesh client-access
Backhaul with client access status: enabled
```

- **show mesh ids-state—S**hows the status of the IDS reports on the backhaul as either enabled or disabled.

```
controller >show mesh ids-state
Outdoor Mesh IDS(Rogue/Signature Detect): .... Disabled
```

- **show mesh env** {**summary** | *Cisco_AP*}—Shows the temperature, heater status, and Ethernet status for either all access points (summary) or a specific access point (*Cisco_AP*). The access point name, role (RootAP or MeshAP), and model are also shown.
  - The temperature is shown in both Fahrenheit and Celsius.
  - The heater status is ON or OFF.
  - The Ethernet status is UP or DOWN.

Note Battery status appears as N/A (not applicable) in the **show mesh env** *Cisco_AP* status display because it is not provided for access points.

```
controller >show mesh env summary

AP Name             Temperature(C/F)  Heater  Ethernet  Battery
------------------  ----------------  ------  --------  -------
SB_RAP1              39/102           OFF     UpDnNANA  N/A
SB_MAP1              37/98            OFF     DnDnNANA  N/A
SB_MAP2              42/107           OFF     DnDnNANA  N/A
SB_MAP3              36/96            OFF     DnDnNANA  N/A

controller >show mesh env SB_RAP1

AP Name..................................... SB_RAP1
AP Model.................................... AIR-LAP1522AG-A-K9
AP Role..................................... RootAP
```

```
Temperature..................................... 39 C, 102 F
Heater.......................................... OFF
Backhaul........................................ GigabitEthernet0

GigabitEthernet0 Status......................... UP
    Duplex...................................... FULL
    Speed....................................... 100
    Rx Unicast Packets.......................... 988175
    Rx Non-Unicast Packets...................... 8563
    Tx Unicast Packets.......................... 106420
    Tx Non-Unicast Packets...................... 17122
GigabitEthernet1 Status......................... DOWN
  POE Out....................................... OFF

Battery......................................... N/A
```

Configuring Local Mesh Parameters

After configuring global mesh parameters, you must configure the following local mesh parameters:

- Antenna Gain—Refer to the "Configuring Antenna Gain" section on page 8-28.
- Workgroup Bridge Groups—Refer to the "Workgroup Bridge Groups on Mesh Access Points" section on page 8-30.

Configuring Antenna Gain

Using the controller GUI or controller CLI, configure the antenna gain for the access point to match that of the installed antenna.

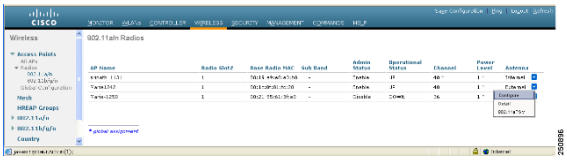
Note Refer to the "External Antennas" section of the *Cisco Aironet 1520 Series Outdoor Mesh Access Points Getting Started Guide* for a summary of supported antennas and their antenna gains at http://www.cisco.com/en/US/docs/wireless/access_point/1520/quick/guide/ap1520qsg.html

Using the GUI to Configure Antenna Gain

Using the controller GUI, follow these steps to configure the antenna gain.

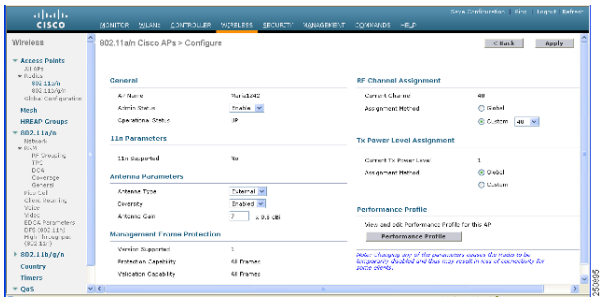
Step 1 Click **Wireless** > **Access Points** > **Radios** > **802.11a/n** to open the 802.11a/n Radios page (see Figure 8-16).

Figure 8-16 802.11a/n Radios Page



Step 2 Hover your cursor over the blue drop-down arrow for the mesh access point antenna that you want to configure and choose **Configure**. The 802.11a/n Cisco APs > Configure page appears (see Figure 8-17).

Figure 8-17 802.11a/n Cisco APs > Configure Page



Step 3 Under the Antenna Parameters section, enter the antenna gain in 0.5-dBm units in the Antenna Gain field. For example, 2.5 dBm = 5.

Note You can configure gain settings only on external antennas. The value that you enter must match the value specified by the vendor for that antenna.

Step 4 Click **Apply** to commit your changes.

Step 5 Click **Save Configuration** to save your changes.

Using the CLI to Configure Antenna Gain

Using the controller CLI, follow these steps to configure the antenna gain.

Step 1 To configure the antenna gain for the 802.11a backhaul radio, enter this command:

config 802.11a antenna extAntGain *antenna_gain Cisco_AP*

where *antenna_gain* is in 0.5-dBm units (for example, 2.5 dBm = 5).

Step 2 To save your changes, enter this command:

save config

Workgroup Bridge Groups on Mesh Access Points

A workgroup bridge (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 mesh access point using Internet Access Point Protocol (IAPP) messaging. The mesh access point treats the WGB as a wireless client.

When configured as a WGB, the 1130, 1240, and 1310 autonomous access points as well as the series 3200 mobile access router (MAR) can associate with mesh access points. The mesh access points can be configured as RAPs or MAPs. WGB association is supported on both the 2.4-GHz (802.11b) and 5-GHz (802.11a) radio on the 1522, and the 2.4-GHz (802.11b) and 4.9-GHz (public safety radio) on the 1524PS.

Note Refer to the "Cisco Workgroup Bridges" section on page 7-61 for configuration details.

Supported Workgroup Modes and Capacities

- The 1130, 1240, 1310 autonomous access point must be running Cisco IOS release 12.4(3g)JA or later (on 32-MB access points) or Cisco IOS release 12.3(8)JEB or later (on 16-MB access points). Cisco IOS releases prior to 12.4(3g)JA and 12.3(8)JEB are not supported.

  Note If your mesh access point has two radios, you can only configure workgroup bridge mode on one of the radios. Cisco recommends that you disable the second radio. Workgroup bridge mode is not supported on access points with three radios such as 1524.

- Client mode WGB (BSS) is supported; however, infrastructure WGB is not supported.
- Mesh access points can support up to 200 clients including wireless clients, WGBs, and wired clients behind the associated WGBs.
- WGBs operating with Cisco IOS release 12.4(3g)JA cannot associate with mesh access points if the WLAN is configured with WPA1 (TKIP) +WPA2 (AES), and the corresponding WGB interface is configured with only one of these encryptions (either WPA1 or WPA2).

Client Roaming

High-speed roaming of Cisco Compatible Extension (CX), version 4 (v4) clients is supported at speeds up to 70 mph in outdoor mesh deployments of 1522 and 1524 mesh access points. An application example might be maintaining communication with a terminal in an emergency vehicle as it moves within a mesh public network.

Three Cisco CX v4 Layer 2 client roaming enhancements are supported:

- **Access point assisted roaming**—This feature helps clients save scanning time. When a Cisco CX v4 client associates to an access point, it sends an information packet to the new access point listing the characteristics of its previous access point. Roaming time decreases when the client recognizes and uses an access point list built by compiling all previous access points to which each client was associated and sent (unicast) to the client immediately after association. The access point list contains the channels, BSSIDs of neighbor access points that support the client's current SSID(s), and time elapsed since disassociation.
- **Enhanced neighbor list**—This feature focuses on improving a Cisco CX v4 client's roam experience and network edge performance, especially when servicing voice applications. The access point provides its associated client information about its neighbors using a neighbor-list update unicast message.

- **Roam reason report**—This feature enables Cisco CX v4 clients to report the reason why they roamed to a new access point. It also allows network administrators to build and monitor a roam history.

Note Client roaming is enabled by default.

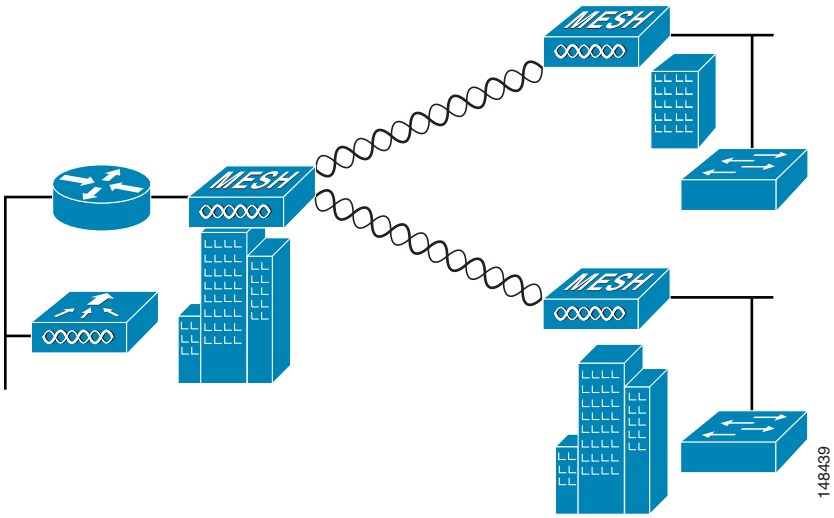
Configuring Ethernet Bridging and Ethernet VLAN Tagging

Ethernet bridging is used in two mesh network scenarios:

- Point-to-point and point-to-multipoint bridging between MAPs (untagged packets). A typical trunking application might be bridging traffic between buildings within a campus (Figure 8-18).

Note You do not need to configure VLAN tagging to use Ethernet bridging for point-to-point and point-to-multipoint bridging deployments.

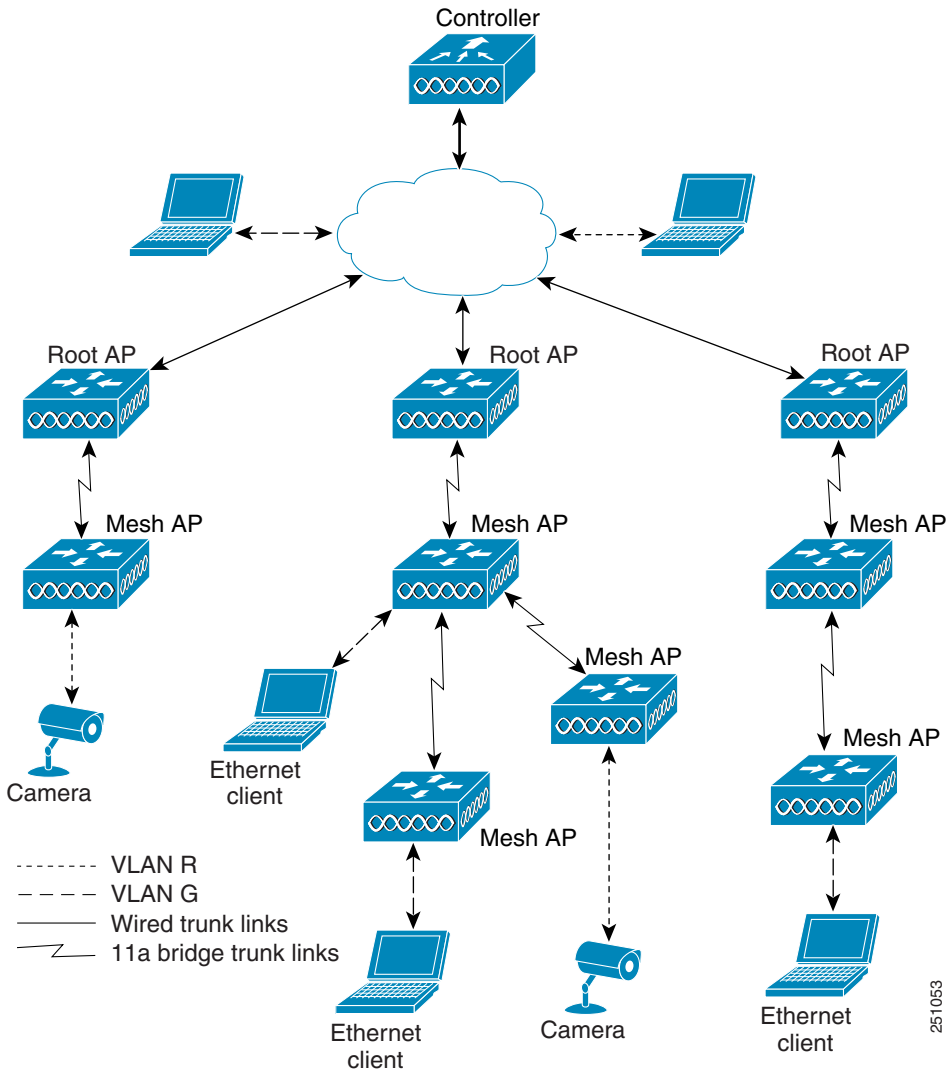
Figure 8-18 Point-to-Multipoint Bridging



- Ethernet VLAN tagging allows specific application traffic to be segmented within a wireless mesh network and then forwarded (bridged) to a wired LAN (access mode) or bridged to another wireless mesh network (trunk mode).

  A typical public safety access application using Ethernet VLAN tagging is placement of video surveillance cameras at various outdoor locations within a city. Each of these video cameras has a wired connection to a MAP. The video of all these cameras is then streamed across the wireless backhaul to a central command station on a wired network (see Figure 8-19).

Figure 8-19 Ethernet VLAN Tagging



Ethernet VLAN Tagging Guidelines

- For security reasons the Ethernet port on a mesh access point (RAP and MAP) is disabled by default. It is enabled by configuring Ethernet Bridging on the mesh access point port.
- Ethernet bridging must be enabled on all the access points in the mesh network to allow Ethernet VLAN tagging to operate.
- VLAN mode must be set as non-VLAN transparent (global mesh parameter). Refer to "Configuring Global Mesh Parameters" section on page 8-22.
  - VLAN transparent is enabled by default. To set as non-VLAN transparent you must uncheck the VLAN transparent option in the global mesh parameters window.
- VLAN configuration on a mesh access point is only applied if all the uplink mesh access points are able to support that VLAN.
  - If uplink access points are not able to support the VLAN, then the configuration is stored rather than applied.

- VLAN tagging can only be configured on Ethernet interfaces.
  - On 152x mesh access points, three of the four ports can be used as *secondary Ethernet interfaces*: *port 0-PoE in, port 1-PoE out, and port 3- fiber. Port 2 - cable* cannot be configured as a secondary Ethernet interface.
  - In Ethernet VLAN tagging, *port 0-PoE in* on the RAP is used to connect to the trunk port of the switch of the wired network. *Port 1-PoE out* on the MAP is used to connect to external devices such as video cameras.
- Backhaul interfaces (802.11a radios) act as *primary Ethernet interfaces*. Backhauls function as trunks in the network and carry all VLAN traffic between the wireless and wired network. No configuration of primary Ethernet interfaces is required.
- The switch port in the wired network that is attached to the RAP (*port 0–PoE in*) must be configured to accept tagged packets on its trunk port. The RAP forwards all tagged packets received from the mesh network to the wired network.
- No configuration is required to support VLAN tagging on any 802.11a backhaul Ethernet interface within the mesh network.
  - This includes the RAP uplink Ethernet port. The required configuration happens automatically using a registration mechanism.
  - Any configuration changes to an 802.11a Ethernet link acting as a backhaul are ignored and a warning results. When the Ethernet link no longer functions as a backhaul the modified configuration is applied.
- VLAN configuration is not allowed on port-02-cable modem port of an 152x access point. VLANs can be configured on ports 0 (PoE-in), 1 (PoE-out) and 3 (fiber).
- If bridging between two MAPs, enter the distance (mesh range) between the two access points that are bridging. (Not applicable to applications in which you are forwarding traffic connected to the MAP to the RAP, access mode)
- Up to 16 VLANs are supported on each sector. Therefore, the cumulative number of VLANs supported by a RAP's children (MAPs) cannot exceed 16.
- Ethernet ports on access points function as either *access* or *trunk* ports within an Ethernet tagging deployment.
- Access Mode– In this mode only untagged packets are accepted. All packets are tagged with a user-configured VLAN called access-VLAN. For this mode to take effect, the global VLAN mode should be non-VLAN transparent.
  - This option is used for applications in which information is collected from devices connected to the MAP such as cameras or PCs and then forwarded to the RAP. The RAP then applies tags and forwards traffic to a switch on the wired network.
- Trunk mode—This mode requires the user to configure a native VLAN and an allowed VLAN list (no defaults). In this mode, both tagged and untagged packets are accepted. Untagged packets are always accepted and are tagged with the user specified native VLAN. Tagged packets are accepted if they are tagged with a VLAN in the allowed VLAN list. For this mode to take effect, the global VLAN mode should be non-VLAN transparent.
  - This option is used for bridging applications such as forwarding traffic between two MAPs resident on separate buildings within a campus.
- The switch port connected to the RAP must be a trunk.
  - The trunk port on the switch and the RAP trunk port must match.
- A configured VLAN on a MAP Ethernet port cannot function as a Management VLAN.

- The RAP must always connect to the native VLAN (ID 1) on a switch.
  - The RAP's primary Ethernet interface is by default the native VLAN of 1.

Note You cannot bridge VLAN ID 1 when using VLAN-Opaque Ethernet bridging because VLAN 1 is the internal native VLAN within a mesh network. This setting cannot be changed.

Using the GUI to Enable Ethernet Bridging and VLAN Tagging

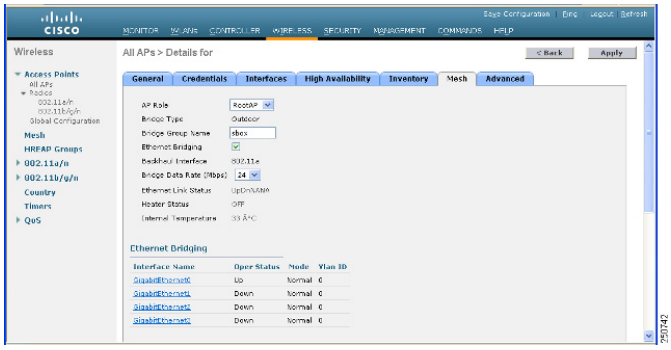
Using the controller GUI, follow these steps to enable Ethernet bridging on a RAP or MAP.

Step 1 Click **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 Ethernet bridging.

Step 3 Click the **Mesh** tab to open the All APs > Details for (Mesh) page (see Figure 8-20).

Figure 8-20 All APs > Details for (Mesh) Page



Step 4 Choose one of the following options from the AP Role drop-down box.

- **MeshAP**—Choose this option if the 1520 series access point has a wireless connection to the controller. This is the default setting.
- **RootAP**—Choose this option if the 1520 series access point has a wired connection to the controller.

Note You must set at least one mesh access point to RootAP in the mesh network.

Step 5 To assign this access point to a bridge group, enter a name for the group in the Bridge Group Name field.

Step 6 Check the **Ethernet Bridging** check box to enable Ethernet bridging or uncheck it to disable this feature.

Step 7 Select the appropriate backhaul rate for the 802.11a backhaul interface from the **Bridge Data Rate** drop-down menu. Cisco recommends setting the backhaul rate to **auto**.

When the bridge data rate is set to **auto**, the mesh backhaul picks the highest rate where the next higher rate cannot be used due to unsuitable conditions for that specific rate (and not because of conditions that affect all rates).

Step 8 Click **Apply** to commit your changes. An Ethernet Bridging section appears at the bottom of the page listing each of the Ethernet ports of the mesh access point.

Step 9 You can perform one of the following procedures to configure the Ethernet Ports. The options are as follows:

- Configure the Ethernet Port as the Access Port
- Configure the Ethernet Port as the Trunk Port

Configure the Ethernet Port as the Access Port

To configure the ethernet port as the access port, follow these steps:

a. Click **gigabitEthernet1** (port 1-PoE out).

b. Select **access** from the mode drop-down menu.

c. Enter a VLAN ID. The VLAN ID can be any value between 2 and 4095.

Note You cannot bridge VLAN ID 1 when using VLAN-Opaque Ethernet bridging because VLAN 1 is the internal native VLAN within a mesh network. This setting cannot be changed.

Note A maximum of 16 VLANs are supported across all of a RAP's subordinate MAPs.

Configure the Ethernet Port as the Trunk Port

To configure the ethernet port as the trunk port, follow these steps:

a. Click **gigabitEthernet1** (port 0-PoE in), **gigabitEthernet1**(port 1-PoE out), or **gigabitEthernet1** (port 3- fiber).

b. Select **trunk** from the mode drop-down menu.

c. Enter a native VLAN ID for *incoming* traffic. The native VLAN ID can be any value between 2 and 4095. Do not assign any value assigned to a user-VLAN (access).

d. Enter a trunk VLAN ID for *outgoing* packets:

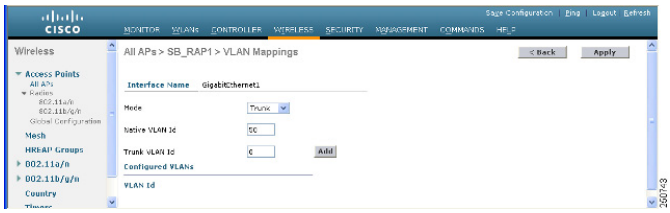
e. If forwarding *untagged* packets, do not change the default trunk VLAN ID value of zero. (MAP-to-MAP bridging, campus environment)

f. If forwarding *tagged* packets, enter a VLAN ID (2 to 4095) that is not already assigned. (RAP to switch on wired network).

g. Click **Add** to add the trunk VLAN ID to the allowed VLAN list. The newly added VLAN displays under the Configured VLANs section on the window.

Note To remove a VLAN from the list, select the Remove option from the arrow drop-down to the right of the desired VLAN.

Figure 8-21 All APs > AP > VLAN Mappings Page



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

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

Table 8-6 describes display-only parameters on the mesh page.

Table 8-6 Display Parameters for Access Points

Parameter	Description
Bridge type	Displays either outdoor (152x access points) or indoor (1130 or 1240 access points)
Backhaul Interface	Displays the radio band that this MAP uses to transfer data to other MAPs. The only possible value is 802.11a.
Ethernet Link Status	Displays the up or down status of the Ethernet link of the AP152x. The Up or Down (Dn) status of the four Ethernet ports is reported in the following format: port0:port1:port2:port3. For example, *UpDnDnDn* indicates that port0 is Up and ports 1, 2, and 3 are Down (Dn). **Note** If *NA* displays in the status string, then the port has no wired connection to that port.
Heater Status	Displays status of either ON or OFF.
Internal Temperature	Displays the internal temperature of the 1522 and 1524PS/1524SB.

Using the CLI to Configure Ethernet Bridging Parameters

Using the controller CLI, follow these steps to configure Ethernet bridging on a RAP or MAP.

Step 1 To specify that your AP152x has bridge functionality, enter this command:

config ap mode bridge *Cisco_AP*

Step 2 To specify the role of this access point in the mesh network, enter this command:

config ap role {**rootAP** | **meshAP**} *Cisco_AP*

Use the **meshAP** parameter if the access point has a wireless connection to the controller or use the **rootAP** parameter if the access point has a wired connection to the controller.

Note The default access point role is **meshAP**.

Step 3 To assign the access point to a bridge group, enter this command:

config ap bridgegroupname set *groupname Cisco_AP*

Step 4 To enable Ethernet bridging on the access point, enter this command:

config mesh ethernet-bridging vlan transparent *disable*

Step 5 To specify the rate (in Mb/s) at which data is shared between access points on the backhaul interface, enter this command:

config ap bhrate {*rate* | **auto**} *Cisco_AP*

When the bridge data rate is set to **auto**, the mesh backhaul picks the highest rate where the next higher rate cannot be used due to unsuitable conditions for that rate (and not because of conditions that affect all rates).

Step 6 To save your settings, enter this command:

save config

Using the CLI to Configure Ethernet VLAN Tagging

VLAN ID 1 is not reserved as the default VLAN.

A maximum of 16 VLANs are supported across all of a RAP's subordinate MAPs.

A VLAN ID can be any value between 1 and 4095. Do not assign any value assigned to another VLAN.

- To configure a MAP access port, enter this command:

  config ap ethernet 1 mode access enable *AP1520-MAP 50*

  where *AP1520-MAP* is the variable *Cisco_AP* and *50* is the variable *access_vlan ID*
- To configure a RAP or MAP trunk port, enter this command:

  config ap ethernet 0 mode trunk enable *AP1520-MAP 60*

  where *AP1520-MAP* is the variable *Cisco_AP* and *60* is the variable *native_vlan ID*
  - To add a VLAN to the VLAN allowed list of the native VLAN, enter this command:

    config ap ethernet 0 mode trunk add *AP1522-MAP3 65*

    where *AP1522-MAP 3* is the variable *Cisco_AP* and *65* is the variable *vlan ID*

Configuring Advanced Features

Configuring Voice Parameters in Mesh Networks

You can configure call admission control (CAC) and QoS on the controller to manage voice quality on the mesh network.

Note Voice is supported only on indoor mesh networks (1130 and 1240 access points).

CAC

CAC enables an access point to maintain controlled quality of service (QoS) when the wireless LAN is experiencing congestion. The Wi-Fi Multimedia (WMM) protocol deployed in CCXv3 ensures sufficient QoS as long as the wireless LAN is not congested. However, in order to maintain QoS under different network loads, CAC in CCXv4 or later is required.

Note CAC is supported in Cisco Compatible Extensions (CCX) v4 or later. See the "Configuring Cisco Client Extensions" section on page 6-19 for more information on CCX.

All calls on a mesh access point use bandwidth-based CAC. Load-based CAC is not supported.

Bandwidth-based, or static CAC enables the client to specify how much bandwidth or shared medium time is required to accept a new call. Each access point determines whether it can accommodate a particular call by looking at the bandwidth available and compares it against the bandwidth required for the call. If not enough bandwidth is available to maintain the maximum allowed number of calls with acceptable quality, the access point rejects the call.

QoS and DSCP Marking

QoS 802.11e is supported on the access and backhaul radios of mesh access points. MAPs can prioritize client traffic based on the QoS setting defined on the controller. CAC is implemented on the backhaul.

Mesh access points recognize DSCP markings from devices. DSCP is performed on the originating Cisco 7920 voice handset (client) and the terminating voice handset or terminal. No DSCP marking is performed on the controller, MAP or CAC.

Note QoS only is relevant when there is congestion on the network.

You can configure bandwidth-based CAC and QoS for mesh networks using the controller GUI or CLI. The instructions for configuring these features is the same for both mesh and non-mesh networks with the exception of QoS settings.

- Follow the instructions in the "Configuring Voice and Video Parameters" section on page 4-73 to configure voice and video parameters.
  - Refer to the "Guidelines for Using Voice on the Mesh Network" section on page 8-39 for mesh-specific configuration guidelines for voice including QoS.

The instructions for viewing voice and video details using the CLI are different for mesh and non-mesh access points.

- Follow the instructions in the "Using the CLI to View Voice Details for Mesh Networks" section on page 8-41 to view details for mesh access points.

Guidelines for Using Voice on the Mesh Network

- Voice is only supported on indoor mesh access points, 1130 and 1240.
- When voice is operating on a mesh network, calls must not traverse more than two hops.
  - Each sector must be configured to require no more than two hops for voice.

- On the **802.11a** or **802.11b/g/n >** *Global* parameters window:
  - Enable dynamic target power control (DTPC)
  - Disable all data rates less than 11 Mbps
- On the **802.11a** or **802.11b/g/n >** *Voice* parameters window:
  - Load-based CAC must be disabled
  - Enable admission control (ACM) for CCXv4 or v5 clients that have WMM enabled. Otherwise, bandwidth-based CAC does not operate properly.
  - Set the maximum RF bandwidth to 50%
  - Set the reserved roaming bandwidth to 6%
  - Enable traffic stream metrics
- On the **802.11a** or **802.11b/g/n >** *EDCA* parameters window:
  - Set the EDCA profile for the interface as voice optimized
  - Disable low latency MAC
- On the **QoS >** *Profile* window:
  - Create a voice profile and select 802.1q as the wired QoS protocol type
- On the **WLANs >** *Edit* > *QoS* window:
  - Select a QoS of platinum for voice and gold for video on the backhaul
  - Select allowed as the WMM policy
- On the **WLANs >** *Edit* > *QoS* window:
  - Select CCKM for authorization (*auth*) key management (*mgmt*) if you want to support fast roaming. Refer to the "Client Roaming" section on page 8-30
- On the **x > *y*** window:
  - Disable voice active detection (VAD)

Voice Call Support in a Mesh Network

Table 8-7 lists a projected minimum and maximum of voice calls supported by radio type and mesh access point role (RAP or MAP) for planning purposes.

Table 8-7 Projected Voice Call Support on a Mesh Network

Mesh Access Point Role	Radio	Minimum Calls Supported[1]	Maximum Calls Supported[2]
RAP	802.11a	14	18
	802.11b/g/n	14	18
MAP1	802.11a	6	9
	802.11b/g/n	11	18
MAP2	802.11a	4	7
	802.11b/g/n	5	9

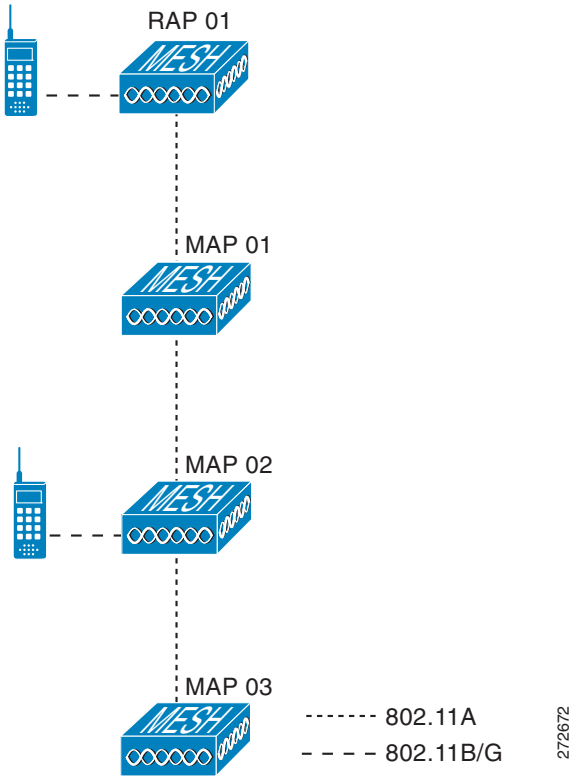
1. Bandwidth of 855 transmit units (TUs) with 50% of the bandwidth reserved for voice calls.
2. Bandwidth of 1076 TUs with 50% of the bandwidth reserved for voice calls.

Using the CLI to View Voice Details for Mesh Networks

Use the commands in this section to view details on voice calls on the mesh network.

Refer to Figure 8-22 when using the CLI commands and viewing their output.

Figure 8-22 Mesh Network Example



- To view the total number of voice calls and the bandwidth used for voice calls on each root access point, enter this command:

  show mesh cac summary

  Information similar to the following appears:

```
AP Name          Slot#   Radio  BW Used/Max  Calls
------------    -------  -----  -----------  -----
SB_RAP1              0   11b/g     0/23437    0
                     1   11a       0/23437    2
SB_MAP1              0   11b/g     0/23437    0
                     1   11a       0/23437    0
SB_MAP2              0   11b/g     0/23437    0
                     1   11a       0/23437    0
SB_MAP3              0   11b/g     0/23437    0
                     1   11a       0/23437    0
```

- To view the mesh tree topology for the network and the bandwidth utilization (used/maximum available) of voice calls and video links for each access point and radio, enter this command:

  show mesh cac bwused {**voice** | **video**} *Cisco_AP*

Information similar to the following appears:

```
AP Name        Slot#    Radio      BW Used/Max
-------------- -------  -----      -----------
SB_RAP1          0      11b/g       1016/23437
                 1      11a         3048/23437
|SB_MAP1         0      11b/g       0/23437
                 1      11a         3048/23437
||  SB_MAP2      0      11b/g       2032/23437
                 1      11a         3048/23437
||| SB_MAP3      0      11b/g       0/23437
                 1      11a         0/23437
```

Note The bars (|) to the left of the AP Name field indicate the number of hops that the mesh access point is away from its root access point (RAP).

Note When the radio type is the same, the backhaul bandwidth used (bw used/max) at each hop is identical. For example, mesh access points *map1*, *map2*, *map3*, and *rap1* are all on the same radio backhaul (802.11a) and are using the same bandwidth (3048). All of the calls are in the same interference domain. A call placed anywhere in that domain affects the others.

- To view the mesh tree topology for the network and display the number of voice calls that are in progress by access point radio, enter this command:

  show mesh cac access *Cisco_AP*

  Information similar to the following appears:

```
AP Name             Slot#   Radio     Calls
-------------      -------  -----    -----
SB_RAP1              0      11b/g      0
                     1      11a        0
|   SB_MAP1          0      11b/g      0
                     1      11a        0
||  SB_MAP2          0      11b/g      1
                     1      11a        0
||| SB_MAP3          0      11b/g      0
                     1      11a        0
```

Note Each call received by an access point radio causes the appropriate calls summary column to increment by one. For example, if a call is received on the 802.11b/g radio on *map2*, then a value of one is added to the existing value in that radio's calls column. In this case, the new call is the only active call on the 802.11b/g radio of *map2*. If one call is active when a new call is received, the resulting value is two.

- To view the mesh tree topology for the network and display the voice calls that are in progress, enter this command:

  show mesh cac callpath *Cisco_AP*

Information similar to the following appears:

```
AP Name             Slot#   Radio     Calls
-------------      -------  -----    -----
SB_RAP1              0      11b/g      0
                     1      11a        1
|   SB_MAP1          0      11b/g      0
                     1      11a        1
||  SB_MAP2          0      11b/g      1
                     1      11a        1
||| SB_MAP3          0      11b/g      0
                     1      11a        0
```

Note The *calls* column for each mesh access point radio in a call path increments by one. For example, for a call that initiates at *map2* (**show mesh cac call path** *SB_MAP2*) and terminates at *rap1* by way of *map1,* one call is added to the *map2* 802.11b/g and 802.11a radio *calls* column*,* one call to the *map1* 802.11a backhaul radio *calls* column, and one call to the *rap1* 802.11a backhaul radio *calls* column.

- To view the mesh tree topology of the network, the voice calls that are rejected at the access point radio because of insufficient bandwidth, and the corresponding access point radio where the rejection occurred, enter this command:

  show mesh cac rejected *Cisco_AP*

  Information similar to the following appears:

```
AP Name             Slot#   Radio     Calls
-------------      -------  -----    -----
SB_RAP1              0      11b/g      0
                     1      11a        0
|   SB_MAP1          0      11b/g      0
                     1      11a        0
||  SB_MAP2          0      11b/g      1
                     1      11a        0
||| SB_MAP3          0      11b/g      0
                     1      11a        0
```

Note If a call is rejected at the *map2* 802.11b/g radio, its *calls* column increments by one.

- To view the number of bronze, silver, gold, platinum, and management queues active on the specified access point. The peak and average length of each queue are shown as well as the overflow count.

  show mesh queue-stats {*Cisco_AP* | **all**}

  Information similar to the following appears:

```
Queue Type  Overflows  Peak length  Average length
 ----------  ---------  -----------  --------------
 Silver      0          1            0.000
 Gold        0          4            0.004
 Platinum    0          4            0.001
 Bronze      0          0            0.000
 Management  0          0            0.000
```

Overflows—The total number of packets dropped because of queue overflow.

Peak Length—The peak number of packets waiting in the queue during the defined statistics time interval.

Average Length—The average number of packets waiting in the queue during the defined statistics time interval.

Enabling Mesh Multicast Containment for Video

You can use the controller CLI to configure three mesh multicast modes to manage video camera broadcasts on all mesh access points. When enabled, these modes reduce unnecessary multicast transmissions within the mesh network and conserve backhaul bandwidth.

Mesh multicast modes determine how bridging-enabled access points [mesh access points (MAPs) and root access points (RAPs)] send multicasts among Ethernet LANs within a mesh network. Mesh multicast modes manage non-CAPWAP multicast traffic only. CAPWAP multicast traffic is governed by a different mechanism.

The three mesh multicast modes are:

- **Regular mode**—Data is multicast across the entire mesh network and all its segments by bridging-enabled RAPs and MAPs.
- **In mode**—Multicast packets received from the Ethernet by a MAP are forwarded to the RAP's Ethernet network. No additional forwarding occurs, which ensures that non-CAPWAP multicasts received by the RAP are not sent back to the MAP Ethernet networks within the mesh network (their point of origin), and MAP-to-MAP multicasts do not occur because they are filtered out. In mode is the default mode.
- **In-out mode**—The RAP and MAP both multicast but in a different manner:
  - If multicast packets are received at a MAP over Ethernet, they are sent to the RAP; however, they are not sent to other MAP Ethernets, and the MAP-to-MAP packets are filtered out of the multicast.
  - If multicast packets are received at a RAP over Ethernet, they are sent to all the MAPs and their respective Ethernet networks. When the in-out mode is in operation, it is important to properly partition your network to ensure that a multicast sent by one RAP is not received by another RAP on the same Ethernet segment and then sent back into the network.

Note If 802.11b clients need to receive CAPWAP multicasts, then multicast must be enabled globally on the controller as well as on the mesh network (using the **config network multicast global enable** CLI command). If multicast does not need to extend to 802.11b clients beyond the mesh network, the global multicast parameter should be disabled (using the **config network multicast global disable** CLI command).

Using the CLI to Enable Multicast on the Mesh Network

- To enable multicast mode on the mesh network to receive multicasts from beyond the mesh networks, enter these commands:

  config network multicast global enable

  config mesh multicast {**regular** | **in** | **in-out**}

- To enable multicast mode only the mesh network (multicasts do not need to extend to 802.11b clients beyond the mesh network), enter these commands:

  config network multicast global disable

  config mesh multicast {**regular** | **in** | **in-out**}

Note Multicast for mesh networks cannot be enabled using the controller GUI.

Backhaul Client Access (Universal Access) for Indoor and Outdoor Mesh Access Points

You can configure the backhaul for mesh access points (1524SB, 1522, 1240 and 1130) to accept client traffic. When this feature is enabled, mesh access points allow wireless client association over the 802.11a radio. This universal access allows an access point to carry both backhaul traffic and 802.11a client traffic over the same 802.11a radio. When this feature is disabled, backhaul traffic is only transmitted over the 802.11a radio and client association is only allowed over the 802.11b/g radio.

After this feature is enabled, all mesh access points reboot.

Default: Disabled.

Note This parameter applies to mesh access points with two or more radios (1524SB, 1522, 1240 and 1130) *excluding* the 1524PS.

To enable this feature on the controller, check the **Backhaul Client Access** check box on the Wireless > Mesh window. Refer to the "Configuring Global Mesh Parameters" section on page 8-22.

Viewing Mesh Statistics and Reports

Viewing Mesh Statistics for an Access Point

This section explains how to use the controller GUI or CLI to view mesh statistics for specific access points.

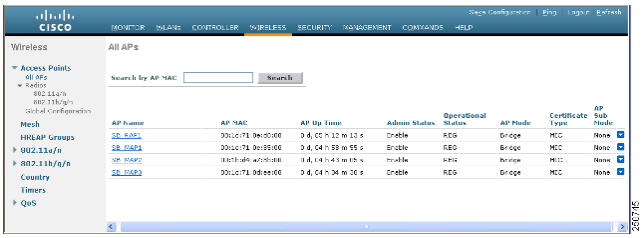
Note You can modify the Statistics Timer interval setting on the All APs > Details page of the controller GUI.

Using the GUI to View Mesh Statistics for an Access Point

Follow these steps to view mesh statistics for a specific access point using the controller GUI.

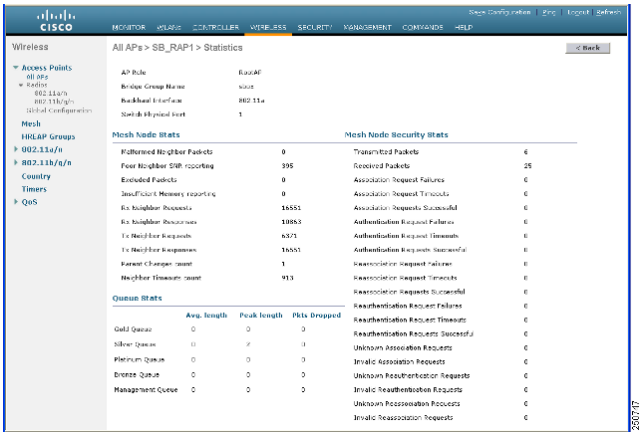
Step 1 Click **Wireless** > **Access Points** > **All APs** to open the All APs page (see Figure 8-23).

Figure 8-23 All APs Page



Step 2 To view statistics for a specific access point, hover your cursor over the blue drop-down arrow for the desired access point and choose **Statistics**. The All APs > *Access Point Name* > Statistics page for the access point appears (see Figure 8-24).

Figure 8-24 All APs > Access Point Name > Statistics Page



This page shows the role of the access point in the mesh network, the name of the bridge group to which the access point belongs, the backhaul interface on which the access point operates, and the number of the physical switch port. It also displays a variety of mesh statistics for this access point. Table 8-8 describes each of the statistics.

Table 8-8 Mesh Access Point Statistics

Statistics	Parameter	Description
Mesh Node Stats	Malformed Neighbor Packets	The number of malformed packets received from the neighbor. Examples of malformed packets include malicious floods of traffic such as malformed or short DNS packets and malformed DNS replies.
	Poor Neighbor SNR Reporting	The number of times the signal-to-noise ratio falls below 12 dB on the backhaul link.
	Excluded Packets	The number of packets received from excluded neighbor mesh access points.
	Insufficient Memory Reporting	The number of insufficient memory conditions.
	Rx Neighbor Requests	The number of broadcast and unicast requests received from the neighbor mesh access points.
	Rx Neighbor Responses	The number of responses received from the neighbor mesh access points.
	Tx Neighbor Requests	The number of unicast and broadcast requests sent to the neighbor mesh access points.
	Tx Neighbor Responses	The number of responses sent to the neighbor mesh access points.
	Parent Changes Count	The number of times a mesh access point (child) moves to another parent.
	Neighbor Timeouts Count	The number of neighbor timeouts.
Queue Stats	Gold Queue	The average and peak number of packets waiting in the gold (video) queue during the defined statistics time interval.
	Silver Queue	The average and peak number of packets waiting in the silver (best effort) queue during the defined statistics time interval.
	Platinum Queue	The average and peak number of packets waiting in the platinum (voice) queue during the defined statistics time interval.
	Bronze Queue	The average and peak number of packets waiting in the bronze (background) queue during the defined statistics time interval.
	Management Queue	The average and peak number of packets waiting in the management queue during the defined statistics time interval.

Table 8-8 Mesh Access Point Statistics (continued)

Statistics	Parameter	Description
Mesh Node Security Stats	Transmitted Packets	The number of packets transmitted during security negotiations by the selected mesh access point.
	Received Packets	The number of packets received during security negotiations by the selected mesh access point.
	Association Request Failures	The number of association request failures that occur between the selected mesh access point and its parent.
	Association Request Timeouts	The number of association request timeouts that occur between the selected mesh access point and its parent.
	Association Requests Successful	The number of successful association requests that occur between the selected mesh access point and its parent.
	Authentication Request Failures	The number of failed authentication requests that occur between the selected mesh access point and its parent.
	Authentication Request Timeouts	The number of authentication request timeouts that occur between the selected mesh access point and its parent.
	Authentication Requests Successful	The number of successful authentication requests between the selected mesh access point and its parent.
	Reassociation Request Failures	The number of failed reassociation requests between the selected mesh access point and its parent.
	Reassociation Request Timeouts	The number of reassociation request timeouts between the selected mesh access point and its parent.
	Reassociation Requests Successful	The number of successful reassociation requests between the selected mesh access point and its parent.
	Reauthentication Request Failures	The number of failed reauthentication requests between the selected mesh access point and its parent.
	Reauthentication Request Timeouts	The number of reauthentication request timeouts that occur between the selected mesh access point and its parent.
	Reauthentication Requests Successful	The number of successful reauthentication requests that occur between the selected mesh access point and its parent.
	Unknown Association Requests	The number of unknown association requests received by the parent mesh access point from its child. The unknown association requests often occur when a child is an unknown neighbor mesh access point.
	Invalid Association Requests	The number of invalid association requests received by the parent mesh access point from the selected child mesh access point. This state may occur when the selected child is a valid neighbor but is not in a state that allows association.

Table 8-8 Mesh Access Point Statistics (continued)

Statistics	Parameter	Description
Mesh Node Security Stats (continued)	Unknown Reauthentication Requests	The number of unknown reauthentication requests received by the parent mesh access point node from its child. This state may occur when a child mesh access point is an unknown neighbor.
	Invalid Reauthentication Requests	The number of invalid reauthentication requests received by the parent mesh access point from a child. This state may occur when a child is a valid neighbor but is not in a proper state for reauthentication.
	Unknown Reassociation Requests	The number of unknown reassociation requests received by the parent mesh access point from a child. This state may occur when a child mesh access point is an unknown neighbor.
	Invalid Reassociation Requests	The number of invalid reassociation requests received by the parent mesh access point from a child. This state may occur when a child is a valid neighbor but is not in a proper state for reassociation.

Using the CLI to View Mesh Statistics for an Access Point

Use these commands to view mesh statistics for a specific access point using the controller CLI.

- To view packet error statistics; a count of failures, timeouts, association and authentication successes; and reassociations and reauthentications for a specific access point, enter this command:

  show mesh security-stats {*Cisco_AP* | **all**}

  Information similar to the following appears:

```
AP MAC : 00:0B:85:5F:FA:F0
Packet/Error Statistics:
----------------------------
x Packets 14, Rx Packets 19, Rx Error Packets 0

Parent-Side Statistics:
-------------------------
Unknown Association Requests 0
Invalid Association Requests 0
Unknown Re-Authentication Requests 0
Invalid Re-Authentication Requests 0
Unknown Re-Association Requests 0
Invalid Re-Association Requests 0
Unknown Re-Association Requests 0
Invalid Re-Association Requests 0

Child-Side Statistics:
-------------------------
Association Failures 0
Association Timeouts 0
Association Successes 0
Authentication Failures 0
Authentication Timeouts 0
Authentication Successes 0
Re-Association Failures 0
Re-Association Timeouts 0
```

```
Re-Association Successes 0
Re-Authentication Failures 0
Re-Authentication Timeouts 0
Re-Authentication Successes 0
```

- To view the number of packets in the queue by type, enter this command:

  show mesh queue-stats *Cisco_AP*

  Information similar to the following appears:

```
Queue Type  Overflows  Peak length  Average length
 ----------  ---------  -----------  --------------
 Silver      0          1            0.000
 Gold        0          4            0.004
 Platinum    0          4            0.001
 Bronze      0          0            0.000
 Management  0          0            0.000
```

  Overflows—The total number of packets dropped because of queue overflow.

  Peak Length—The peak number of packets waiting in the queue during the defined statistics time interval.

  Average Length—The average number of packets waiting in the queue during the defined statistics time interval.

Viewing Neighbor Statistics for an Access Point

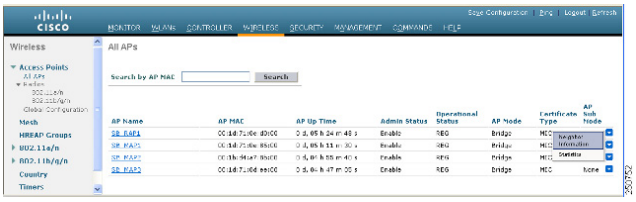
This section explains how to use the controller GUI or CLI to view neighbor statistics for a selected access point. It also describes how to run a link test between the selected access point and its parent.

Using the GUI to View Neighbor Statistics for an Access Point

Using the controller GUI, follow these steps to view neighbor statistics for an access point.

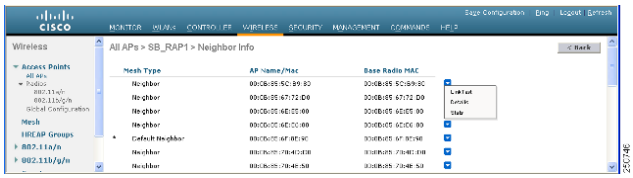
Step 1 Click **Wireless** > **Access Points** > **All APs** to open the All APs page (see Figure 8-25).

Figure 8-25 All APs Page



Step 2 To view neighbor statistics for a specific access point, hover your cursor over the blue drop-down arrow for the desired access point and choose **Neighbor Information**. The All APs > *Access Point Name* > Neighbor Info page for the access point appears (see Figure 8-26).

Figure 8-26 All APs > Access Point Name > Neighbor Info Page

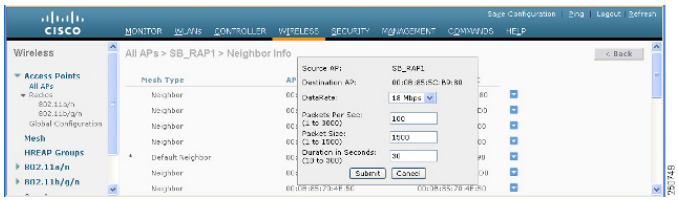


This page lists the parent, children, and neighbors of the access point. It provides each access point's name and radio MAC address.

Step 3 To perform a link test between the access point and its parent or children, follow these steps:

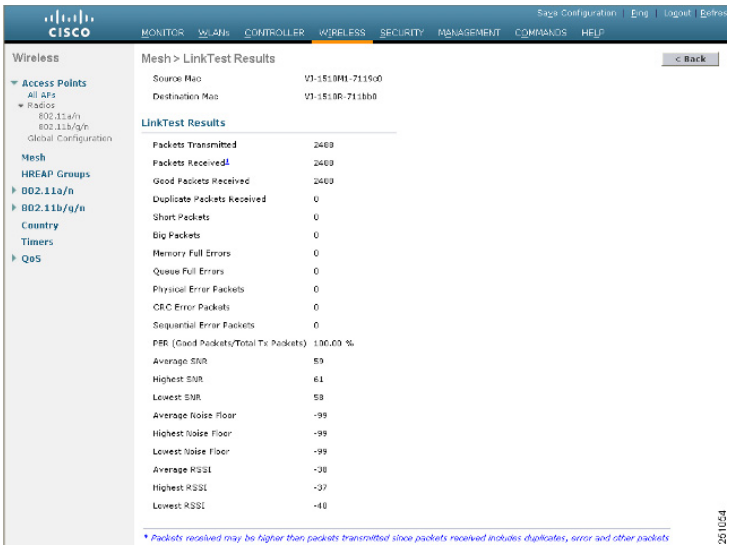
a. Hover your cursor over the blue drop-down arrow of the parent or child and choose **LinkTest**. A pop-up window appears (see Figure 8-27).

Figure 8-27 Link Test Window



b. Click **Submit** to start the link test. The link test results appear on the Mesh > LinkTest Results page (see Figure 8-28).

Figure 8-28 Mesh > LinkTest Results Page



c. Click **Back** to return to the All APs > *Access Point Name* > Neighbor Info page.

Step 4 To view the details for any of the access points on this page, follow these steps:

a. Hover your cursor over the blue drop-down arrow for the desired access point and choose **Details**. The All APs > *Access Point Name* > Link Details > *Neighbor Name* page appears (see Figure 8-29).

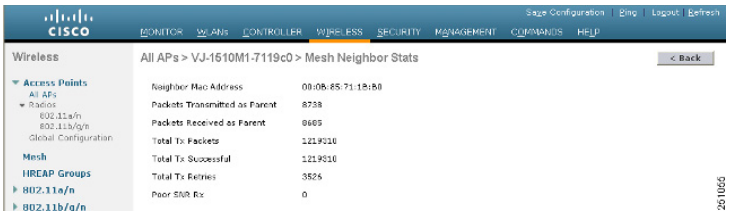
Figure 8-29 All APs > Access Point Name > Link Details > Neighbor Name Page

b. Click **Back** to return to the All APs > *Access Point Name* > Neighbor Info page.

Step 5 To view statistics for any of the access points on this page, follow these steps:

a. Hover your cursor over the blue drop-down arrow for the desired access point and choose **Stats**. The All APs > *Access Point Name* > Mesh Neighbor Stats page appears (see Figure 8-30).

Figure 8-30 All APs > Access Point Name > Mesh Neighbor Stats Page



b. Click **Back** to return to the All APs > *Access Point Name* > Neighbor Info page.

Using the CLI to View Neighbor Statistics for an Access Point

Use these commands to view neighbor statistics for a specific access point.

- To view the mesh neighbors for a specific access point, enter this command:

  show mesh neigh {detail | summary} {*Cisco_AP* **| all}**

  Information similar to the following appears when you request a summary display:

```
AP Name/Radio Mac  Channel Snr-Up Snr-Down Link-Snr Flags State
-----------------  ------- ------ -------- -------- ------ -------
mesh-45-rap1       165     15     18       16       0x86b  UPDATED NEIGH PARENT BEACON
00:0B:85:80:ED:D0  149      5      6        5       0x1a60 NEED UPDATE BEACON DEFAULT
00:17:94:FE:C3:5F  149      7      0        0       0x860     BEACON
```

- To view the channel and signal-to-noise ratio (SNR) details for a link between an access point and its neighbor, enter this command:

  show mesh path *Cisco_AP*

  Information similar to the following appears:

```
AP Name/Radio Mac  Channel Snr-Up Snr-Down Link-Snr Flags State
-----------------  ------- ------ -------- -------- ------ -------
mesh-45-rap1       165     15     18       16       0x86b UPDATED NEIGH PARENT BEACON
mesh-45-rap1 is a Root AP.
```

- To view the percentage of packet errors for packets transmitted by the neighbor mesh access point, enter this command:

  show mesh per-stats {*Cisco_AP* **| all**}

  Information similar to the following appears:

```
Neighbor MAC Address 00:0B:85:5F:FA:F0
Total Packets transmitted: 104833
Total Packets transmitted successfully: 104833
Total Packets retried for transmission: 33028
Neighbor MAC Address 00:0B:85:80:ED:D0
Total Packets transmitted: 0
Total Packets transmitted successfully: 0
Total Packets retried for transmission: 0
```

```
Neighbor MAC Address 00:17:94:FE:C3:5F
Total Packets transmitted: 0
Total Packets transmitted successfully: 0
Total Packets retried for transmission: 0
```

Note Packet error rate percentage = 1 – (number of successfully transmitted packets/number of total packets transmitted).

Converting Indoor Access Points to Mesh Access Points (1130AG, 1240AG)

Before you can install an 1130AG or 1240AG indoor access point into an indoor mesh deployment, you must do the following.

1. Convert the autonomous access point (k9w7 image) to a lightweight access point.

   A detailed explanation of this process is located at:

   http://www.cisco.com/en/US/products/hw/wireless/ps430/prod_technical_reference09186a00804fc3dc.html

2. Convert the lightweight access point to either a mesh access point (MAP) or root access point (RAP).

   Indoor mesh access points (1130 and 1240) can function as either a RAP or a MAP. By default, all are configured as MAPs.

   At least one access point within a mesh network must be configured to function as a RAP.

   - To convert the access point to a mesh access point using the CLI, perform one of the following:
     - To convert from a lightweight access point to a mesh access point, enter the following CLI commands:

       config ap mode bridge *Cisco_AP*

       The mesh access point reloads.
     - To convert from a lightweight access point to a RAP, enter the following CLI commands:

       config ap mode bridge *Cisco_AP*

       config ap role rootAP *Cisco_AP*

       The mesh access point reloads and is configured to operate as a RAP.
   - To convert the access point to a mesh access point using the GUI, follow these steps:
     a. Choose **Wireless** and click on the AP Name link for the 1130 or 1240 indoor access point you want to convert.
     b. At the General Properties panel, choose **Bridge** from the AP Mode drop-down menu.

        The access point reboots.
     c. At the Mesh panel, select either RootAP or MeshAP from the AP Role drop- down menu.
     d. Click **Apply** and **Save Configuration**.

Changing MAP and RAP Roles for Indoor Mesh Access Points (1130AG, 1240AG)

Cisco 1130 and 1240 series indoor mesh access points can function as either RAPs or MAPs.

Using the GUI to Change MAP and RAP Roles for Indoor Mesh Access Points

Using the controller GUI, follow these steps to change an indoor mesh access point from one role to another.

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

Step 2 Click the name of the 1130 or 1240 series access point that you want to change.

Step 3 Click the **Mesh** tab.

Step 4 From the AP Role drop-down box, choose **MeshAP** or **RootAP** to specify this access point as a MAP or RAP, respectively.

Step 5 Click **Apply** to commit your changes. The access point reboots.

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

Note Cisco recommends a Fast Ethernet connection between the MAP and controller when changing from a MAP to RAP.

Note After a RAP-to-MAP conversion, the MAP's connection to the controller is a wireless backhaul rather than a Fast Ethernet connection. It is the responsibility of the user to ensure that the Fast Ethernet connection of the RAP being converted is disconnected before the MAP starts up so that the MAP can join over the air.

Note The recommended power source for MAPs is either a power supply or power injector. PoE is not a recommended power source for MAPs.

Using the CLI to Change MAP and RAP Roles for Indoor Mesh Access Points

Using the controller CLI, follow these steps to change an indoor mesh access point from one role to another.

Step 1 To change the role of an indoor access point from MAP to RAP or from RAP to MAP, enter this command:

config ap role {**rootAP** | **meshAP**} *Cisco_AP*

The access point reboots after you change the role.

Step 2 To save your changes, enter this command:

save config

Converting Indoor Mesh Access Points to Non-Mesh Lightweight Access Points (1130AG, 1240AG)

The access point reboots after entry of the conversion commands (noted below).

Note A Fast Ethernet connection to the controller for the conversion from a mesh (bridge) to non-mesh (local) access point is recommended. If the backhaul is a radio, after the conversion you must enable Ethernet and then reload the access image. After the reload and reboot the backhaul is Fast Ethernet.

Note When a root access point is converted back to a lightweight access point, all of its subordinate mesh access points lose connectivity to the controller. Consequently, a mesh access point is unable to service its clients until the mesh access point is able to connect to a different root access point in the vicinity. Likewise, clients might connect to a different mesh access point in the vicinity to maintain connectivity to the network.

- To convert an indoor mesh access point (MAP or RAP) to a non-mesh lightweight access point using the CLI, enter the following command.

  config ap mode local *Cisco_AP*

  The access point reloads.

- To convert an indoor mesh access point (MAP or RAP) to a non-mesh lightweight access point using the GUI, follow these steps:

  a. Click **Wireless** and click on the AP Name link for the 1130 or 1240 indoor access point you want to convert.

  b. At the General Properties panel, select **Local** from the AP Mode drop-down menu.

  c. Click **Apply** and **Save Configuration**.

- To convert an indoor mesh access point (MAP or RAP) to a non-mesh lightweight access point using Cisco WCS, follow these steps:

  a. Click **Configure > Access Points** and click on the AP Name link for the 1130 or 1240 indoor access point you want to convert.

  b. At the General Properties panel, select **Local** as the AP Mode (left side).

  c. Click **Save**.

Configuring Mesh Access Points to Operate with Cisco 3200 Series Mobile Access Routers

Outdoor access points (1522, 1524PS) can interoperate with the Cisco 3200 Series Mobile Access Router (MAR) on the public safety channel (4.9 GHz) as well as the 2.4-GHz access and 5.8-GHz backhaul.

The Cisco 3200 creates an *in-vehicle network* in which devices such as PCs, surveillance cameras, digital video recorders, printers, PDAs, and scanners can share wireless networks such as cellular or WLAN-based services back to the main infrastructure. This allows data collected from in-vehicle deployments such as a police cars to be integrated into the overall wireless infrastructure. For specific interoperability details between series 1130, 1240, and 1520 mesh access points and series 3200 mobile access routers, refer to Table 8-9.

Table 8-9 Mesh Access Points and MAR 3200 Interoperability

Mesh Access Point Model	MAR Model
1522[1]	c3201[2], c3202[3], c3205[4]
1524PS	c3201, c3202
1130, 1240 configured as indoor mesh access points with universal access	c3201, c3205

1. Universal access must be enabled on the 1522 if connecting to a MAR on the 802.11a radio or 4.9-GHz band.
2. Model c3201 is a MAR with a 802.11b/g radio (2.4 GHz).
3. Model c3202 is a MAR with a 4-9-GHz sub-band radio.
4. Model c3205 is a MAR with a 802.11a radio (5.8-GHz sub-band).

Configuration Guidelines

For the 1522 or 1524PS mesh access point and Cisco MAR 3200 to interoperate on the public safety network, the following configuration guidelines must be met:

- Client access must be enabled on the backhaul (Mesh global parameter).
- Public Safety must be enabled globally on all mesh access points (MAPs) in the mesh network.
- Channel number assignments on the 1522 or 1524PS must match those on the Cisco 3200 radio interfaces.
  - Channels 20 (4950 GHz) through 26 (4980 GHz) and sub-band channels 1 through 19 (5 and 10 MHz) are used for MAR interoperability. This configuration change is made on the controller. No changes are made to the access point configuration.
  - Channel assignments are made only to the RAP. Updates to the MAP are propagated by the RAP.

The default channel width for MAR 3200s is 5 MHz. You must do one of the following:

- Change the channel width to 10 or 20 MHz to enable WGBs to associate with series 1520 mesh access points
- Change the channel on the 1522 or 1524PS to a channel in the 5-MHz (channels 1 to 10) or 10-MHz band (channels 11 through 19).
  - When using the CLI, you must disable the 802.11a radio prior to configuring its channels. You re-enable the radio after the channels are configured.

- When using the GUI, enabling and disabling of the 802.11a radio for channel configuration is not required.
- Cisco MAR 3200s can scan channels *within* but not across the 5-, 10-, or 20-MHz bands.

Using the GUI to Enable Mesh Access Points to Operate with Cisco 3200 Series Mobile Access Routers

Using the controller GUI, follow these steps to enable the 1522 and 1524PS mesh access points to associate to the Cisco 3200 series MAR.

Step 1 To enable the backhaul for client access, click **Wireless > Mesh** to open the Mesh page.

Step 2 Check the **Backhaul Client Access** check box to allow wireless client association over the 802.11a radio.

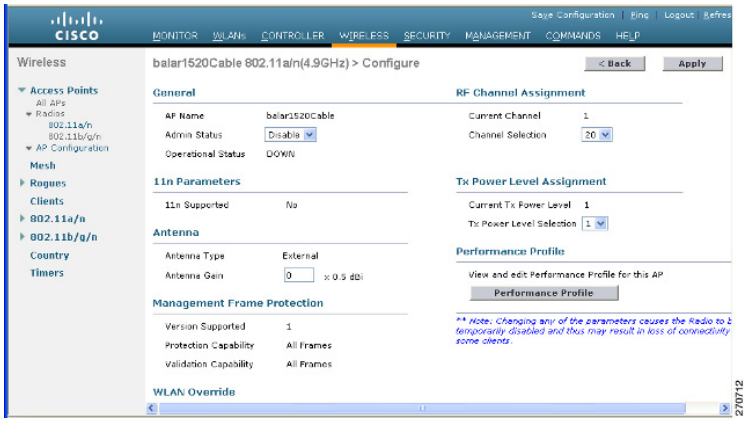
Step 3 Click **Apply** to commit your changes.

Step 4 When prompted to allow a reboot of all the mesh access points on the network, click **OK**.

Step 5 Click **Wireless > Access Points > Radios > 802.11a/n** to open the 802.11a/n Radios page.

Step 6 Hover your cursor over the blue drop-down arrow for the appropriate RAP and choose **Configure**. The 802.11a/n (4.9 GHz) > Configure page appears (see Figure 8-31).

Figure 8-31 802.11 a/n (4.9GHz) > Configure Page



Step 7 Under the RF Channel Assignment section, choose the **Custom** option for Assignment Method and select a channel between 1 and 26.

Step 8 Click **Apply** to commit your changes.

Step 9 Click **Save Configuration** to save your changes.

Using the CLI to Enable Mesh Access Points to Operate with Cisco 3200 Series Mobile Access Routers

Using the controller CLI, follow these steps to enable the 1522 and 1524PS mesh access points to associate to the Cisco 3200 series MAR.

Step 1 To enable client access mode on the 1522 and 1524PS mesh access points, enter this command:

config mesh client-access enable

Step 2 To enable public safety on a global basis, enter this command:

config mesh public-safety enable *all*

Step 3 To enable the public safety channels, enter these commands:

- For the 1522 access point, enter these commands:

  config 802.11a disable *Cisco_MAP*

  config 802.11a channel ap *Cisco_MAP channel_number*

  config 802.11a enable *Cisco_MAP*

- For the 1524PS, enter these commands:

  config 802.11–a49 disable *Cisco_MAP*

  config 802.11–a49 channel ap *Cisco_MAP channel_number*

  config 802.11–a49 enable *Cisco_MAP*

Note Enter **config 802.11–a58 enable** *Cisco_MAP* to enable a 5.8-GHz radio.

Note For both the 1522 and 1524PS mesh access points, valid values for the channel number is 1 through 26.

Step 4 To save your changes, enter this command:

save config

Step 5 To verify your configuration, enter these commands:

show mesh public-safety

show mesh client-access

show ap config 802.11a summary (for 1522 access points only)

show ap config 802.11–a49 summary (for 1524PS access points only)

Note Enter **show config 802.11-a58 summary** to view configuration details for a 5.8-GHz radio.