Cisco Mesh Access Points, Design and Deployment Guide, Release 7.0

Last revised: May 12, 2011

This document provides design and deployment guidelines for the deployment of secure enterprise, campus, and metropolitan Wi-Fi networks within the Cisco wireless mesh networking solution, a component of the Cisco Unified Wireless Network (CUWN).

Mesh networking employs Cisco 1520 Series outdoor mesh access points and Cisco 1130 and 1240 Series indoor mesh access points along with the Cisco wireless LAN controller, and Cisco Wireless Control System (WCS) to provide scalable, central management, and mobility between indoor and outdoor deployments. Control and Provisioning of Wireless Access Points (CAPWAP) protocol manages the connection of mesh access points to the network.

End-to-end security within the mesh network is supported by employing Advanced Encryption Standard (AES) encryption between the wireless mesh access points and Wi-Fi Protected Access 2 (WPA2) clients. This document also outlines radio frequency (RF) components to consider when designing an outdoor network.

The features described in this document are for the following products:

- Cisco Aironet 1520 (1522, 1524) Series outdoor mesh access points
- Cisco Aironet 1130 and 1240 Series indoor mesh access points
- Mesh features in Cisco wireless LAN controller releases 5.2 and later releases
- Mesh features in Cisco WCS releases 5.2 and later releases

Americas Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

Contents

Mesh Network Components

The Cisco wireless mesh network has four core components:

- Cisco Aironet 1520, 1240, and 1130 Series mesh access points

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

- Cisco wireless LAN controller (hereafter referred to as *controller*)
- Cisco WCS
- Mesh software architecture

Mesh Access Points

This section describes the following:

- Licensing for Mesh Access Points on a 5500 Series Controller, page 5
- Access Point Roles, page 5
- Network Access, page 6
- Network Segmentation, page 7
- Cisco 1130 and 1240 Indoor Mesh Access Points, page 7
- Cisco 1520 Series Outdoor Mesh Access Points, page 7

Licensing for Mesh Access Points on a 5500 Series Controller

To use both mesh and nonmesh access points with a Cisco 5500 Series Controller, only the base license (LIC-CT5508-X) is required from the 7.0 release and later releases. For more information about obtaining and installing licenses, see Chapter 4 of the *Cisco Wireless LAN Controller Configuration Guide, Release 7.0* at

http://www.cisco.rw/en/US/docs/wireless/controller/7.0/configuration/guide/c70ccfg.html

Access Point Roles

Access points within a mesh network operate in one of the following two ways:

1. Root access point (RAP)
2. Mesh access point (MAP)

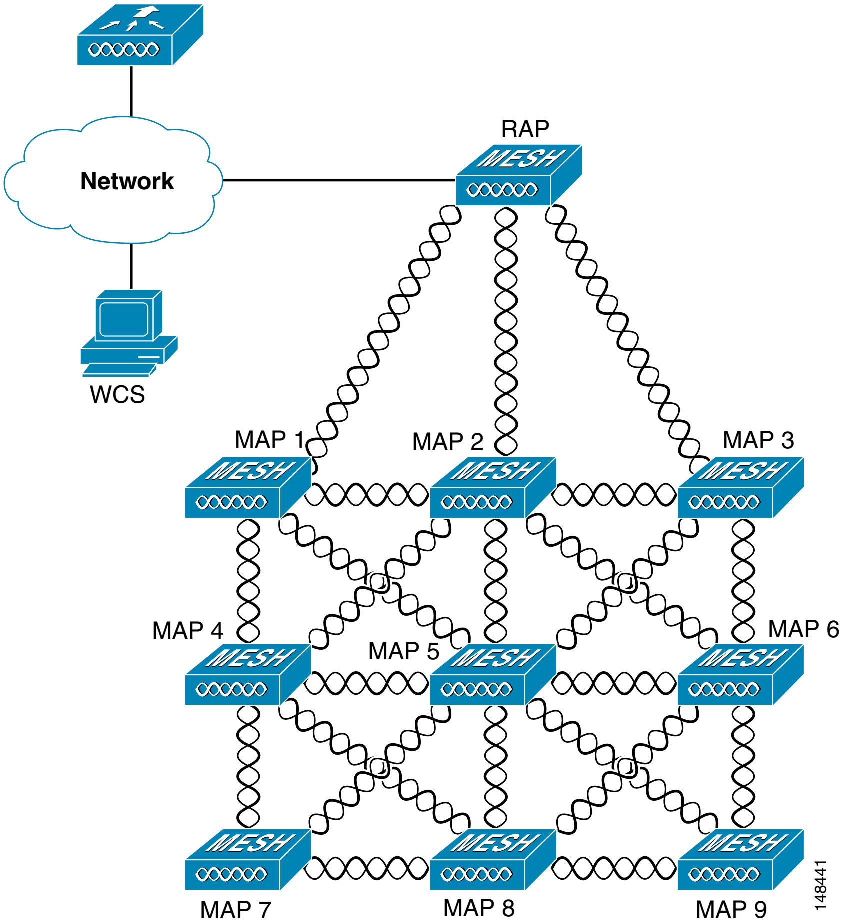
Note All access points are configured and shipped as mesh access points. To use an access point as a root access point, you must reconfigure the mesh access point to a root access point. In all mesh networks, ensure that there is at least one root access point.

While the RAPs have wired connections to their controller, the 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.

Figure 1 shows the relationship between RAPs and MAPs in a mesh network.

Figure 1 Simple Mesh Network Hierarchy



Network Access

Wireless mesh networks can simultaneously carry two different traffic types. They are:

- Wireless LAN client traffic
- 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 the following authentication methods:

- MAC authentication—Mesh access points are added to a database that can be referenced to ensure they are provided access to a given controller and mesh network. See the "Adding Mesh Access Points to the Mesh Network" section on page 62.

- External RADIUS Authentication—Mesh access points can be externally authorized using a RADIUS server such as Cisco ACS (4.1 and later) that supports the client authentication type of Extensible Authentication Protocol-FAST (EAP-FAST) with certificates. See the "Enabling External Authentication of Mesh Access Points - Using the GUI" section on page 74.

Network Segmentation

Membership to the wireless LAN mesh network for mesh access points is controlled by the bridge group names (BGNs). Mesh access points can be placed in similar bridge groups to manage membership or provide network segmentation. See the "Configuring Bridge Group Names" section on page 84.

Cisco 1130 and 1240 Indoor Mesh Access Points

You have a choice of ordering indoor access points (1130 or 1240) directly into the bridge mode, so that these access points can be used directly as mesh access points. If you have these access points in a local mode (nonmesh), then you have to connect these access points to the controller and change the AP mode to the bridge mode (mesh). For more information, see the "Adding Indoor Mesh Access Points to Cisco WCS" section on page 187. This scenario can become cumbersome particularly if the volume of the access points being deployed is large and if the access points are already deployed in the local mode for a traditional nonmesh wireless coverage.

The Cisco 1130 and 1240 are equipped with the following two simultaneously operating radios:

- 2.4-GHz radio used for client access
- 5-GHz radio used for data backhaul

The 5-GHz radio supports the 5.15 GHz, 5.25 GHz, 5.47, and 5.8 GHz bands.

Cisco 1520 Series Outdoor Mesh Access Points

Cisco Aironet 1520 series outdoor mesh access points consist of the 1522 dual-radio mesh access point and the 1524 multi-radio mesh access points. There are two models of the 1524, and one of the 1523, which are the following:

- The public safety model, 1524PS
- The serial backhaul model, 1524SB
- The serial backhaul model, 1523CV

Note In the 6.0 release, the AP1524SB access point was launched in A, C and N domain. In the 7.0 release, the AP1524SB access point is launched also in -E, -M, -K, -S, and -T domains.

Cisco 1520 Series mesh access points (*hereafter referred to in general as AP1520s or specifically as AP1522, AP1524PS* (public safety)*, or AP1524SB and AP1523CV* (serial backhaul access points)) are the core components of the wireless mesh deployment. In the 6.0 release, AP1524SB was launched in A, C, and N domains. In the 7.0 release, AP1524SB is also available in the -E, -M, -K, -S, and -T domains. AP1520s are configured by both the controller (GUI and CLI) and Cisco WCS. In the 7.0 release, AP1523CV is available only in the -A domain. In this document, all the functionality described for AP1524SB is also applicable to AP1523CV. Communication between outdoor mesh access points (MAPs and RAPs) is over the 802.11a radio backhaul. Client traffic is generally transmitted over the 802.11b/g radio (802.11a can also be configured to accept client traffic), and public safety traffic (AP1524PS only) is transmitted over the 4.9-GHz radio.

The mesh access point can also operate as a relay node for other access points not directly connected to a wired network. Intelligent wireless routing is provided by Adaptive Wireless Path Protocol (AWPP). This Cisco protocol enables each mesh access point to identify its neighbors and intelligently choose the optimal path to the wired network by calculating the cost of each path in terms of signal strength and the number of hops required to get to a controller.

AP1520s are manufactured in two different configurations: cable and non-cable.

- The cable configuration has three antenna connectors on top of the unit, can be mounted to a cable strand, and supports power-over-cable (POC).
- The non-cable configuration supports two antennas each on the top and bottom of the unit. It can be mounted to a pole or building wall and supports several power options.

AP1520s are available in a hazardous location hardware enclosure. When configured, the AP1520 complies with safety standards for Class I, Division 2, Zone 2 hazardous locations. For more details, see the "Cisco 1520 Hazardous Location Certification" section on page 28.

Note See the *Cisco Aironet 1520 Series Lightweight Outdoor Access Point Ordering Guide* for power, mounting, antenna, and regulatory support by model: http://www.cisco.com/en/US/prod/collateral/wireless/ps5679/ps8368/product_data_sheet0900aecd8066a157.html

Cisco 1522 Mesh Access Point (Part Nos. AIR–LAP1522AG–X–K9, AIR–LAP1522HZ–X–K9, AIR–LAP1522PC–X–K9)

The AP1522 mesh access point, includes two radios: a 2.4-GHz, and a 4.9 to 5.8-GHz radio. The 2.4-GHz (802.11b/g) radio is for client access and the 5-GHz (802.11a) radio is used as the backhaul.

- Uplinks support includes Gigabit Ethernet (1000BASE-T) and a small form-factor (SFP) slot that can be plugged for a fiber or cable modem interface. Both single mode and multimode SFPs up to 1000BASE-BX are supported. The cable modem is Docsis 2.0 with a cable modem power supply.
- The 5-GHz radio is a 802.11a radio which covers the 4.9- to 5.8-GHz frequency band, and is used as a backhaul. It can also be used for client access if the *universal client access* feature is enabled.
  - For information about the universal access feature, see the "Viewing Global Mesh Parameter Settings" section on page 149.

Note AP1522s with serial numbers *prior* to FTX1150XXXX do **not** support 5- and 10-MHz channels on the 4.9-GHz radio; however, a 20-MHz channel is supported.

Note Those AP1522s with serial numbers *after* FTX1150XXXX support 5-, 10-, and 20-MHz channels.

Cisco 1524PS Mesh Access Point (Part No. AIR–LAP1524PS–X–K9)

The AP1524PS includes three radios: a 2.4-GHz, a 5.8-GHz, and a 4.9-GHz radio. The 2.4-GHz radio is for client access (non-public safety traffic) and the 4.9-GHz radio is for public safety client access traffic only. The 5.8-GHz radio can be used as the backhaul for both public safety and non-public safety traffic.

The 4.9-GHz and 5.8-GHz radios are 802.11a sub-band radios which support a subset of specific 802.11a channels and include a sub-band specific filter designed to lessen interference from other 11a sub-band radios within the same mesh access point.

The 4.9-GHz sub-band radio on the AP1524 supports public safety channels within the 5-MHz (channels 1 to 10), 10-MHz (channels 11-19), and 20-MHz (channels 20-26) bandwidths.

- The data rates supported within the 5-MHz bandwidth are 1.5, 2.25, 3, 4.5, 6, 9, 12, and 13.5 Mbps. The default rate is 6 Mbps.
- The data rates supported within the 10-MHz bandwidth are 3, 4.5, 6, 9, 12, 18, 24, and 27 Mbps. The default rate is 12 Mbps.

Cisco 1524SB Mesh Access Point (Part No. AIR–LAP1524SB–X–K9)

The AP1524SB includes three radios: one 2.4-GHz radio and two 5-GHz radios.

The 2.4-GHz radio is for client access (non-public safety traffic). The two 5-GHz radios serve as serial backhauls: one uplink and one downlink. The AP1524SB is suitable for linear deployments.

In the 6.0 release, the 5-GHz radios in the –A domain could only be operated in the 5.8-GHz band with 5 channels. In the 7.0 release, these radios cover the whole of the 5-GHz band. Each 5-GHz radio backhaul is configured with a different backhaul channel. 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.

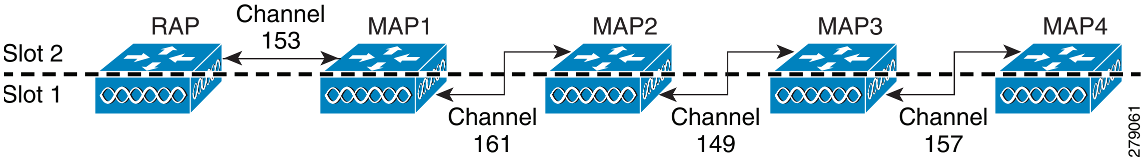
On the RAP, the radio in slot 2 is used to extend the backhaul in the downlink direction; the radio in slot 1 is used only for client access and not mesh.

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.

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 2 shows an example of channel selection when the RAP downlink channel is 153.

Figure 2 Channel Selection Example



Fall Back Mode

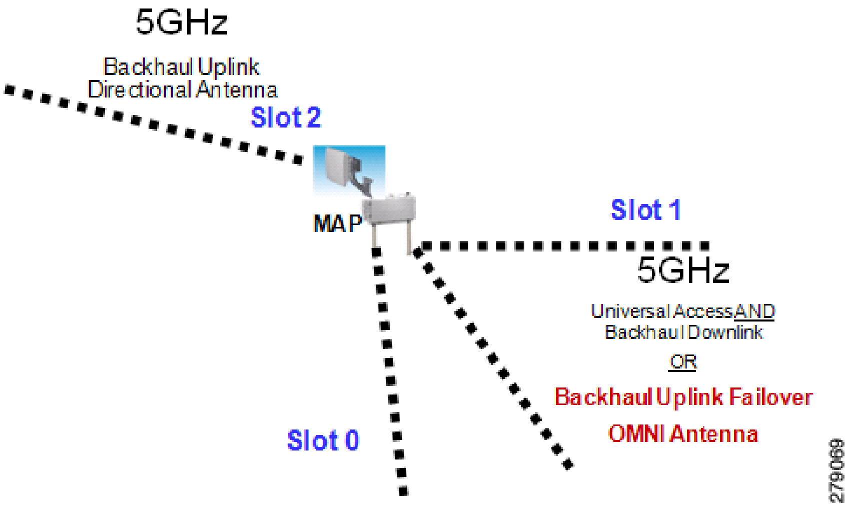
Slot 1 in a 5-GHz radio in a MAP can act as an uplink radio for the backhaul in any one of the following scenarios:

- Slot 2 radio fails.
- Antenna for slot 2 radio goes bad.
- Slot 2 radio is unable to find the uplink because of a bad RF design.
- Interference and long-term fades disturb the uplink to the extent that the slot 2 radio loses its uplink connection.

When a slot 1 radio takes over a slot 2 radio, it is called Fall Back Mode. The slot 2 radio is made inactive on a noninterfering channel. The hardware is reduced to AP1522 (two radios). The slot 1 radio (omni antenna) is extended to the uplink. A period of 15 minutes is set on a timer to attempt a rescan to find a parent on the slot 2 radio again. The timer is similar to the default BGN timer.

Figure 3 shows an example of the Fall Back Mode.

Figure 3 Fall Back Mode



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 1.

Table 1 AP1524SB Antenna Ports

Antenna Port	Radio Slot	Description
1	1	5 GHz–Used for backhaul and universal access. Universal access is configured only on slot 1. **Note** Omni antenna required.
2	0	2 GHz–Used for client access.
3	0	2 GHz–Used for client access.
4	0	2 GHz–Used for client access.
5	—	Not connected.
6	2	5 GHz–Used for backhaul. **Note** Directional antenna required.

Note Depending on the product model, the AP1524SB could have either 5-GHz radios or 5.8-GHz subband 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.

Cisco 1523CV Mesh Access Point (Part No. AIR–LAP1523CV–X–K9)

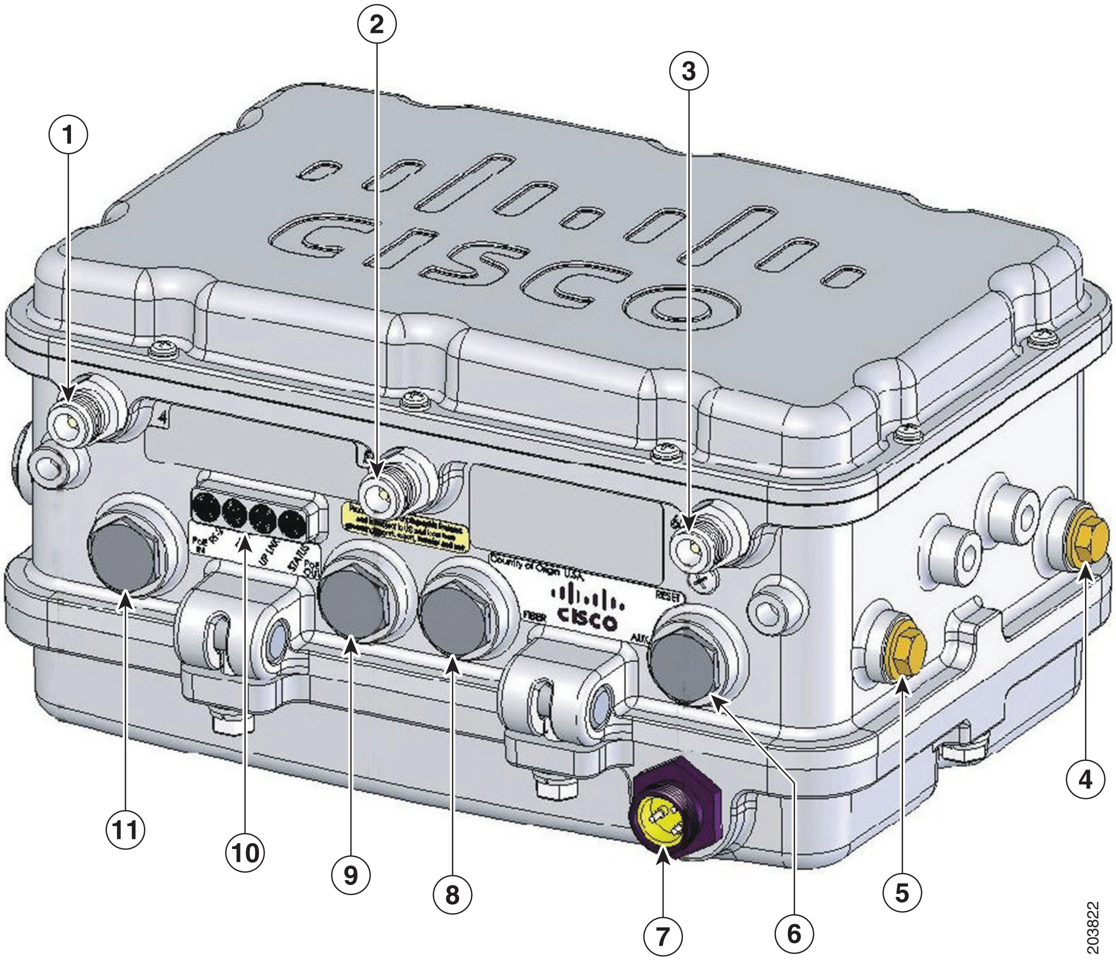
All the functionality described in this document for Cisco 1524SB mesh access points is also applicable to Cisco 1523CV mesh access points, which are available in the 7.0 release. In this document, these two models of the access points are collectively referred to as serial backhaul access points.

Hardware

Figure 4 shows the AP1520 (all models) and its bottom connectors (radio side view).

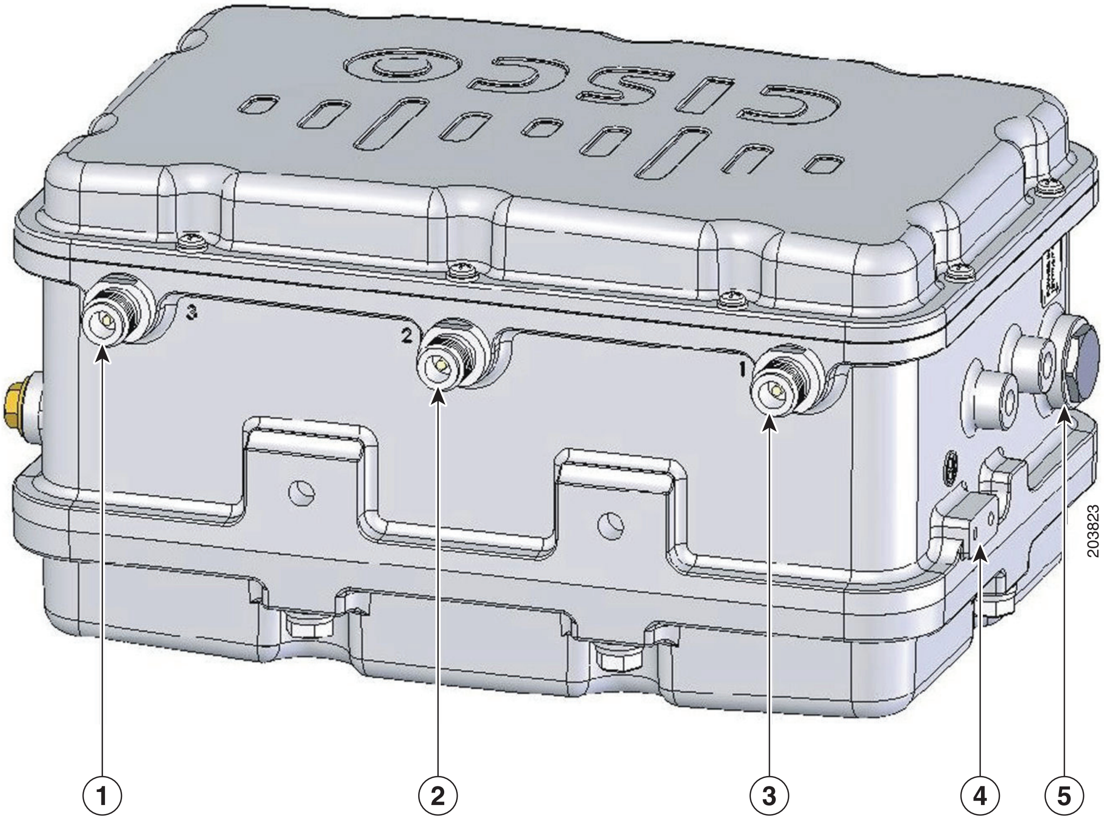
Figure 5 shows the AP1520 (all models) and its top connectors (radio cover view).

Figure 4 Cisco 1520 Series Mesh Access Point (Radio Side View)



1	Antenna port 4	**7**	AC input connector
2	Antenna port 5	**8**	Fiber port
3	Antenna port 6	**9**	PoE out port
4	Fiber port (optional)	**10**	LEDs
5	Cable POC port (optional)	**11**	PoE in port
6	Aux/Console port		

Figure 5 Cisco 1520 Series Mesh Access Point (Radio Cover View)



1	Antenna port 3	**4**	Ground screw holes
2	Antenna port 2	**5**	DC power connector
3	Antenna port 1		

Note For more information about antennas and their selection, see the "Antennas" section on page 21.

Note For more information about power, see the "Multiple Power Options" section on page 13.

Ethernet Ports

AP1520s supports four Gigabit Ethernet interfaces.

- Port 0 (g0) is a Power over Ethernet (PoE) input port–PoE (in)
- Port 1 (g1) is a PoE output port–PoE (out)
- Port 2 (g2) is a cable connection
- Port 3 (g3) is a fiber connection

You can query the status of these four interfaces in the controller CLI and Cisco WCS.

In the controller CLI, the **show mesh env summary** command is used to display the status of the ports.

- The Up or Down (Dn) status of the four ports is reported in the following format:
  - port0(PoE-in):port1(PoE-out):port2(cable):port3(fiber)
- For example, *rap1522.a380* in the display below shows a port status of *UpDnDnDn.* This indicates that:
  - PoE-in port 0 (g0) is Up, PoE-out port 1 (g1) is Down (Dn), Cable port 2 (g2) is Down (Dn), and Fiber port 3 (g3) is Down (Dn).

```
(controller)> show mesh env summary
AP Name       Temperature(C/F) Heater Ethernet Battery
--------      ---------------- -------- ------- -------
rap1242.c9ef    N/A              N/A     UP       N/A
rap1522.a380    29/84            OFF     UpDnDnDn N/A
rap1522.4da8    31/87            OFF     UpDnDnDn N/A
```

Multiple Power Options

Power options include the following:

- 90 to 480 VAC streetlight power
- 12 V DC
- Power-over-cable power supply (40-90VAC)
- PoE using a separate power injection system (48VDC)
  - For more information about the power injection, its specifications, and installation, see http://www.cisco.com/en/US/docs/wireless/access_point/1520/power/guide/1520pwrinj.html
- Internal battery backup power
- 802.3af-compliant PoE out to connect IP devices (such as a video cameras)

Battery Backup Module (Optional)

An optional battery backup module (part no. AIR-1520-BATT-6AH) is available for AP1520s.

The integrated battery can be used for temporary backup power during external power interruptions. The battery run time for AP1520s is as follows:

- 3-hour access point operation using two radios at 77°F (25°C) with PoE output port off
- 2-hour access point operation using two radios at 77°F (25°C) with PoE output port on

The battery pack is not supported on the access point cable configuration.

Note For a complete listing of optional hardware components for AP1520s such as mounting brackets, power injectors, and power tap adapters, see http://www.cisco.com/en/US/prod/collateral/wireless/ps5679/ps8368/product_data_sheet0900aecd8066a157.html

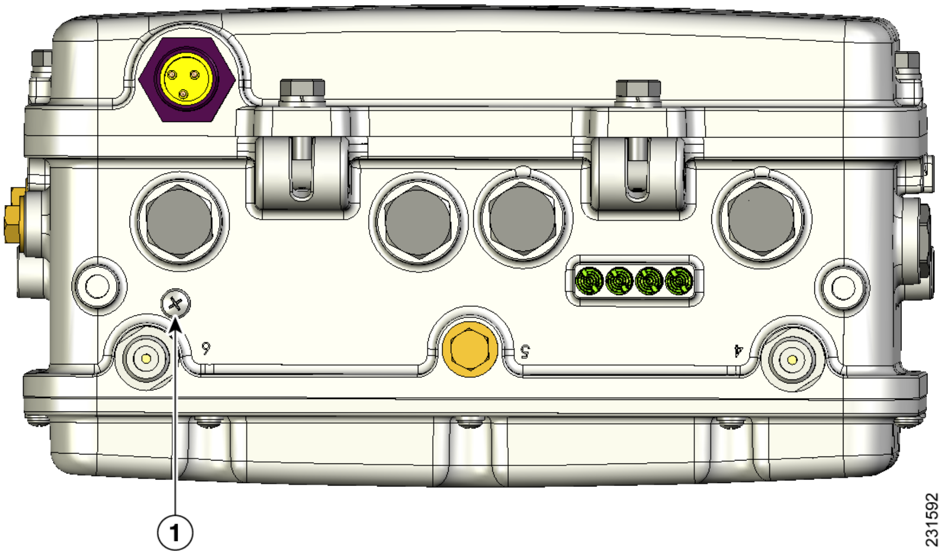
Reset Button

The access point has a reset button located on the bottom of the unit (see Figure 6). The reset button is recessed in a small hole that is sealed with a screw and a rubber gasket. The reset button is used to perform these functions:

- Reset the access point—Press the reset button for less than 10 seconds. LEDs turn off during the reset and then reactivate when the reset is complete.
- Disable battery backup power—Press the reset button for more than 10 seconds. LEDs turn off, then on, and then stay off.
  - You can also disable the battery remotely by entering the following command:

    config mesh battery-state disable *AP_name*
- Switch off LEDs—Press the reset button for more than 10 seconds. LEDs turn off, then on, and then stay off.

Figure 6 Reset Button Location



1	Reset button location

To reset the access point, follow these steps:

Step 1 Use a Phillips screwdriver to remove the reset button screw. Ensure that you do not lose the screw.

Step 2 Use a straightened paperclip, and push the reset button for less than 10 seconds. This causes the access point to reboot (power cycle), all LEDs turn off for approximately 5 seconds, and then the LEDs reactivate.

Step 3 Replace the reset button screw, and use a Phillips screwdriver to tighten to 22 to 24 in. lbs (2.49 to 2.71 nm).

Monitoring LED Status

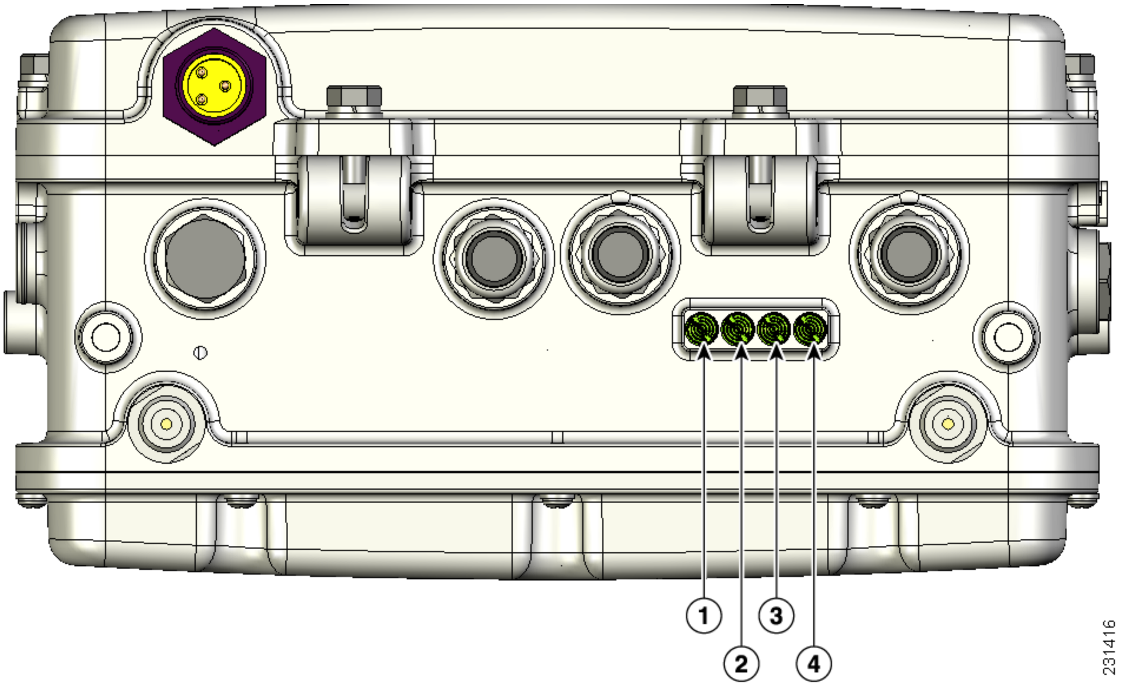
The four-status LEDs on AP1520s are useful during the installation process to verify connectivity, radio status, access point status, and software status. However, once the access point is up and running and no further diagnosis is required, we recommend that you turn off the LEDs to discourage vandalism.

If your access point is not working as expected, see the LEDs at the bottom of the unit. You can use them to quickly assess the unit's status.

Note LEDs are enabled or disabled using the following command:
config ap led-state {**enable** | **disable**} {**cisco_ap_name** | **all**}

There are four LED status indicators on AP1520s. Figure 7 shows the location of the AP1520 LEDs.

Figure 7 Access Point LEDs at the Bottom of the Unit



The table below describes each LED and its status.

1	Status LED—Access point and software status	**3**	RF-1 LED—Status of the radio in slot 0 (2.4-GHz) and slot 2 (5.8-GHz for 1524SB and 4.9-GHz for 1524PS)).
2	Uplink LED—Ethernet, cable, or fiber status	**4**	RF-2 LED—Status of the radio in slot 1 (5.8-GHz) and the radio in slot 3.[1]

[1] Slot 3 is disabled in this release.

Note The RF-1 and RF-2 LEDs monitor two radios simultaneously but do not identify the affected radio. For example, if the RF-1 LED displays a steady red LED, one or both of the radios in slots 0 and 2 have experienced a firmware failure. To identify the failing radio, you must use other means, such as the access point CLI or controller GUI to investigate and isolate the failure.

Table 2 lists the access point LED signals.

Table 2 Access Point LED Signals

LED	Color[1],[2]	Meaning
Status	Off	Access is point is not powered on.
	Green	Access point is operational.
	Blinking green	Download or upgrade of Cisco IOS image file is in progress.
	Amber	Mesh neighbor access point discovery is in progress.
	Blinking amber	Mesh authentication is in progress.
	Blinking red/green/amber	CAPWAP discovery is in progress.
	Red	Firmware failure. Contact your support organization for assistance.
Uplink	Off	No physical connector is present. The uplink port is not operational.
	Green	Uplink network is operational (cable, fiber optic, or Ethernet).
RF-1	Off	Radio is turned off.
Slot 0	Green	Radio is operational.
2.4-GHz radio	Red	Firmware failure. Contact your support organization for assistance.
RF-1	Off	Radio is turned off.
Slot 2	Green	Radio is operational.
802.11a radio	Red	Firmware failure. Contact your support organization for assistance.
RF-2	Off	Radio is turned off.
Slot 1	Green	Radio is operational.
802.11a radio	Red	Firmware failure. Contact your support organization for assistance.

Table 2 Access Point LED Signals (continued)

LED	Color[1],[2]	Meaning
RF-2 Slot 3	Disabled in this release.	—

[1] If all LEDs are off, the access point has no power.

[2] When the access point power supply is initially turned on, all LEDs are amber.

Serial Backhaul Access Point Guidelines for the Rest of the World (ROW)

In the 7.0 release, new 1524 SKUs are released, with both 802.11a radio units supporting the entire 5-GHz band from 4.9 GHz to 5.8 GHz. This release also opens the 5-GHz band for the -A domain as well on the existing hardware. The radios can also operate in UNII-2 (5.25 to 5.35 GHz), UNII-2 plus (5.47 to 5.725 GHz), and the upper ISM (5.725 to 5.850 GHz) bands.

The public safety band (4.94 to 4.99 GHz) is not supported for backhaul and for client access.

For information about the channels and maximum power levels of the AP1520 supported within the world's regulatory domains, see the *Channels and Maximum Power Settings for Cisco Aironet Lightweight Access Points* manual at http://www.cisco.com/en/US/docs/wireless/access_point/channels/lwapp/reference/guide/1520_chp.html

Table 3 provides a complete overview of channels supported in each domain. In addition to 5 channels in the upper ISM band, there are 4 channels in the UNII-2 band and 11 channels in the UNII-2 plus band.

Table 3 Channels Supporter Per Regulatory Domain

Channel ID	Frequency (MHz)	Regulatory Domains								
		-A	-C	-E	-K	-M	-N	-P	-S	-T
4940-5100 MHz										
184	4920							Yes		
188	4949							Yes		
22/192	4960							Yes		
26/196	4980							Yes		
8	5040							Yes		
12	5060							Yes		
5250-5350 MHz										
52	5260									
56	5280	DFS			DFS					
60	5300	DFS			DFS					
64	5320	DFS			DFS					
5470-5725 MHz										

Table 3 Channels Supporter Per Regulatory Domain (continued)

Channel ID	Frequency (MHz)	Regulatory Domains								
		-A	-C	-E	-K	-M	-N	-P	-S	-T
100	5500	DFS		DFS	DFS	DFS				DFS
104	5520	DFS		DFS	DFS	DFS				DFS
108	5540	DFS		DFS	DFS	DFS				DFS
112	5560	DFS		DFS	DFS	DFS				DFS
116	5580	DFS		DFS	DFS	DFS				DFS
120	5580				DFS					DFS
124	5620				DFS					DFS
128	5640									DFS
132	5660	DFS		DFS		DFS				DFS
136	5680	DFS		DFS		DFS				DFS
140	5700	DFS		DFS		DFS				DFS
5725-5850 MHz										
149	5745	Yes	Yes			DFS	Yes		Yes	Yes
153	5765	Yes	Yes			DFS	Yes		Yes	Yes
157	5785	Yes	Yes			DFS	Yes		Yes	Yes
161	5805	Yes	Yes			DFS	Yes		Yes	Yes
165	5825	Yes	Yes				Yes		Yes	Yes

Note Channels marked Yes/DFS are channels supported in that domain.
Channels marked DFS are additional DFS-enabled channels and require checks for radar detection.
This table is for up to 8 dBi antennas. For higher gain antennas, see http://www.cisco.com/en/US/docs/wireless/access_point/channels/lwapp/reference/guide/1520_chp.html.

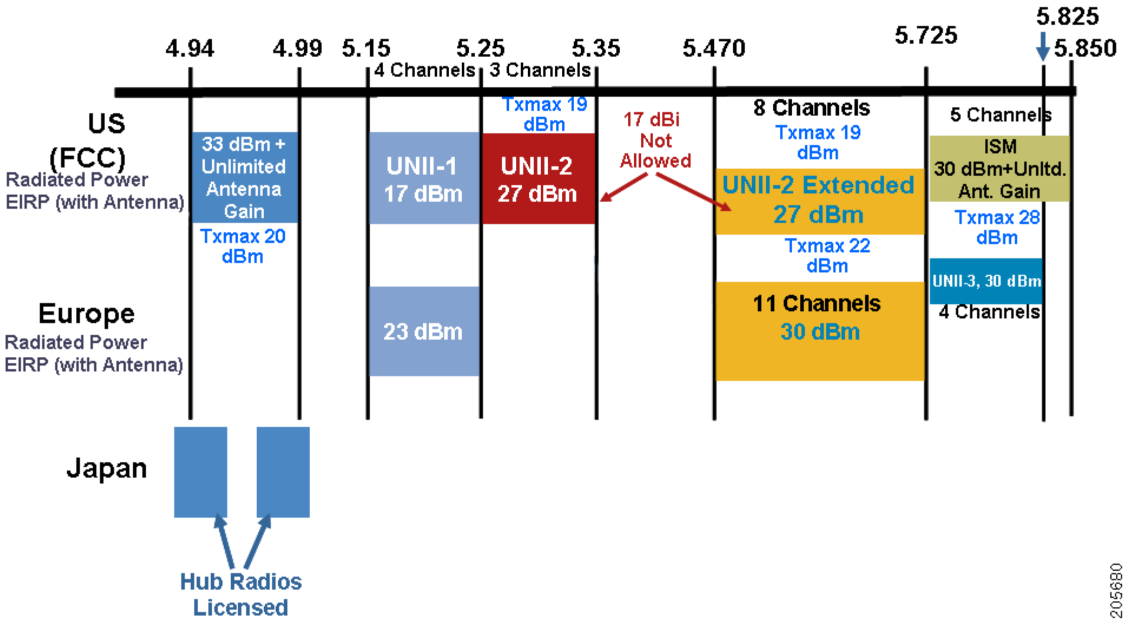
With the expansion of the channel set, DFS-enabled channels are also supported. Radar detection and automatic channel reassignment in case of radar detection on RAP/MAPs are also supported. When there is a channel change, it is also propagated to the corresponding parent/child access point (if applicable) so that the channel change is synchronized between the parent and child so that there is no link downtime. For example, if radar is detected on the uplink radio of a child access point, the parent is informed so that it can change the channel of the downlink radio. The parent in turn informs the child about the channel change, so that the child access point can set the new channel on its uplink radio as well and does not have to scan again to rejoin the parent on the new channel.

For countries in the Middle East such as Saudi Arabia and Kuwait, a new regulatory domain for outdoor APs, the -M domain, has been mandated. With this release, outdoor APs will now support this new -M domain. Earlier, these countries were part of the -E domain, which supported a channel set of 100 to 140. However, in the -M domain, channels 149 to 161 are also supported with the 100 to 140 band (see Table 3 for details). Also, in the -M domain, channels 149 to 161 are DFS enabled, unlike other domains such as -A, -C, -N, and so on, where these channels are non-DFS. Radar detection is also enabled on these channels. Because the countries that are now part of the -M domain (that is, Saudi Arabia and Kuwait) were earlier part of the -E domain, both the -E domain and the -M domain APs are supported, when any of these countries is configured on the controller, which ensures backward compatibility with the existing -E domain APs in these countries. However, you will have to ensure that only a valid set of channels (the channels common to both the -E and the -M domains) is selected as part of the 802.11a DCA list, and that the backhaul channel deselection feature is enabled to ensure correct operation of the -E domain APs, as these APs can support 100 to 140 channels and not the extended list of 149 to 161 channels available in the -M domain.

Frequency Bands

The 2.4-GHz and 5-GHz frequency bands are supported on the AP1130, AP1240, and AP1520 radios. Additionally, the 4.9-GHz public safety band is supported on the AP1524. (See Figure 8.)

Figure 8 Frequency Bands Supported By 802.11a Radios on AP1520s



The 5-GHz band is a conglomerate of three bands in the USA: 5.150 to 5.250 (UNII-1), 5.250 to 5.350 (UNII-2), 5.470 to 5.725 (UNII-2 Extended), and 5.725 to 5.850 (ISM). UNII-1 and the UNII-2 bands are contiguous and are indeed treated by 802.11a as being a continuous swath of spectrum 200-MHz wide, more than twice the size of the 2.4-GHz band. See Table 4.

The 4.9 GHz is a public safety channel within the 5-MHz (channels 1 to 10), 10-MHz (channels 11-19), and 20-MHz (channels 20-26) bandwidths.

Note The frequency depends on the regulatory domain in which the access point is installed. For additional information, see the Channels and Power Levels document at http://www.cisco.com/en/US/docs/wireless/access_point/channels/lwapp/reference/guide/lw_chp2.html

Table 4 Frequency Band

Frequency Band Terms	Description	Model Support
UNII-1[1]	Regulations for UNII devices operating in the 5.15- to 5.25-GHz frequency band. Indoor operation only,	1130, 1240
UNII-2	Regulations for UNII devices operating in the 5.25- to 5.35-GHz frequency band. DFS and TPC are mandatory in this band.	1130, 1240, 1522, 1524SB (A domain), 1523CV (A domain)
UNII-2 Extended	Regulations for UNII-2 devices operating in the 5.470 to 5.725 frequency band.	1130, 1240, 1522, 1524SB (A domain), 1524CV (A domain)
ISM[2]	Regulations for UNII devices operating in the 5.725 to 5.850 GHz frequency band.	1130, 1240, 1522, 1524 (AP1524PS and AP1524SB), and AP1523CV

[1] UNII refers to the Unlicensed National Information Infrastructure.

[2] ISM refers to Industrial Science and Mechanical.

Dynamic Frequency Selection

Previously, devices employing radar operated in frequency sub-bands without other competing services. However, controlling regulatory bodies are attempting to open and share these bands with new services like wireless mesh LANs (IEEE 802.11).

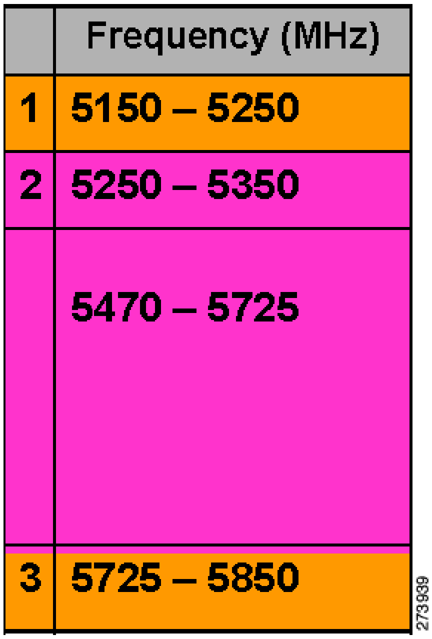
To protect existing radar services, the regulatory bodies require that devices wishing to share the newly opened frequency sub-band behave in accordance with a protocol named Dynamic Frequency Selection (DFS). DFS dictates that to be compliant, a radio devices must be capable of detecting the presence of radar signals. When a radio detects a radar signal, it is required to stop transmitting to for at least 30 minutes to protect that service.The radio then selects a different channel to transmit on but only after monitoring it. If no radar is detected on the projected channel for at least one minute, then the new radio service device may begin transmissions on that channel.

The process for a radio to detect and identify a radar signal is a complicated task that sometimes leads to incorrect detects. Incorrect radar detections can occur due to a large number of factors, including due to uncertainties of the RF environment and the ability of the access point to reliably detect actual on-channel radar.

The 802.11h standard addresses DFS and Transmit Power Control (TPC) as it relates to the 5-GHz band. DFS is to avoid interference with radar and TPC is used to avoid interference with satellite feeder links.

Note DFS is mandatory in the U.S. for 5250 to 5350, and 5470 to 5725 frequency bands. DFS and TPC are mandatory for these same bands in Europe. (See Figure 9.)

Figure 9 DFS and TPC Band Requirements



	Frequency (MHz)
1	5150 – 5250
2	5250 – 5350
	5470 – 5725
3	5725 – 5850

Antennas

Overview

Antenna choice is a vital component of any wireless network deployment. Essentially, there are two broad types of antennas:

- Directional
- Omnidirectional

Each type of antenna has a specific use and is most beneficial in specific types of deployments. Because antennas distribute RF signal in large *lobed* coverage areas determined by antenna design, successful coverage is heavily reliant on antenna choice.

An antenna gives a mesh access point three fundamental properties: gain, directivity, and polarization:

- Gain—A measure of the increase in power. Gain is the amount of increase in energy that an antenna adds to an RF signal.
- Directivity—The shape of the transmission pattern. If the gain of the antenna increases, the coverage area decreases. The coverage area or radiation pattern is measured in degrees. These angles are measured in degrees and are called beamwidths.

Note Beamwidth is defined as a measure of the ability of an antenna to focus radio signal energy towards a particular direction in space. Beamwidth is usually expressed in degrees HB (Horizontal Beamwidth); usually, the most important one is expressed in a VB (Vertical Beamwidth) (up and down) radiation pattern. When viewing an antenna plot or pattern, the angle is usually measured at half-power (3 dB) points of the main lobe when referenced to the peak effective radiated power of the main lobe.

Note An 8-dBi antenna transmits with a horizontal beamwidth of 360 degrees, causing the radio waves to disperse power in all directions. Therefore, radio waves from an 8-dBi antenna do not go nearly as far as those sent from a 17-dBi patch antenna (or a third-party dish) that has a more narrow beamwidth (less than 360 degrees).

- Polarization—The orientation of the electric field of the electromagnetic wave through space. Antennas can be polarized either horizontally or vertically, though other kinds of polarization are available. Both antennas in a link must have the same polarization to avoid additional unwanted loss of signal. To improve the performance, an antenna can sometimes be rotated to alter polarization and thus reduce interference. A general rule of thumb is that vertical polarization is preferable for sending RF waves down concrete *canyons,* and horizontal polarization is generally more preferable for wide area distribution. Polarization can also be harnessed to optimize for RF bleed-over when reducing RF energy to adjacent structures is important. Most omnidirectional antennas ship with vertical polarization as their default.

Antenna Options

A wide variety of antennas are available to provide flexibility when you deploy the mesh access points over various terrains. 5 GHz is used as a backhaul and 2.4 GHz is used for client access.

Table 5 lists the supported external 2.4- and 5-GHz antennas for AP1520s.

Table 5 External 2.4- and 5-GHz Antennas

Part Number	Model	Gain (dBi)
AIR-ANT2450V-N	2.4-GHz compact omnidirectional[1]	5
AIR-ANT2480V-N	2.4-GHz omnidirectional	8.0
AIR-ANT5180V-N	5-GHz compact omnidirectional[2]	8.0
	4.9-GHz compact omnidirectional[3]	7.0
AIR-ANT58G10SSA-N	5-GHz sector	9.5
AIR-ANT5114P-N	4.9- to 5-GHz patch[2]	14.0
AIR-ANT5117S-N	4.9- to 5-GHz 90-degree sector[2]	17.0

[1] The compact omnidirectional antennas mount directly on the access point.

[2] The compact omnidirectional antennas mount directly on the access point.

[3] Use of the 4.9-GHz band requires a license and may be used only by qualified Public Safety operators as defined in section 90.20 of the FCC rules.

See the *Cisco Aironet Antenna and Accessories Reference Guide* on Cisco antennas and accessories at

http://www.cisco.com/en/US/prod/collateral/wireless/ps7183/ps469/product_data_sheet09186a008008883b.html

The deployment and design, limitations and capabilities, and basic theories of antennas as well as installation scenarios, regulatory information, and technical specifications are addressed in detail.

Table 6 summarizes the horizontal and vertical beamwidth for Cisco antennas.

Table 6 Horizontal and Vertical Beamwidth for Cisco Antennas

Antenna	Horizontal Beamwidth (degrees)	Vertical Beamwidth (degrees)
AIR-ANT5180V-N	360	16
AIR-ANT58G10SSA-N	60	60
AIR-ANT5114P-N	25	29
AIR-ANT5117S-N	90	8

N-Connectors

All antennas are equipped with N connectors.

AP1522 has three separate N-connectors to attach two 2.4-GHz antennas, and one N-connector for a 5-GHz antenna.

AP1524PS, AP1524SB, and AP1523CV have five N connectors to attach three 2.4-GHz antennas and two N connectors for 5-GHz/4.9-GHz bands.

Each radio has at least one TX/RX port. Each radio must have an antenna connected to at least one of its available TX/RX ports.

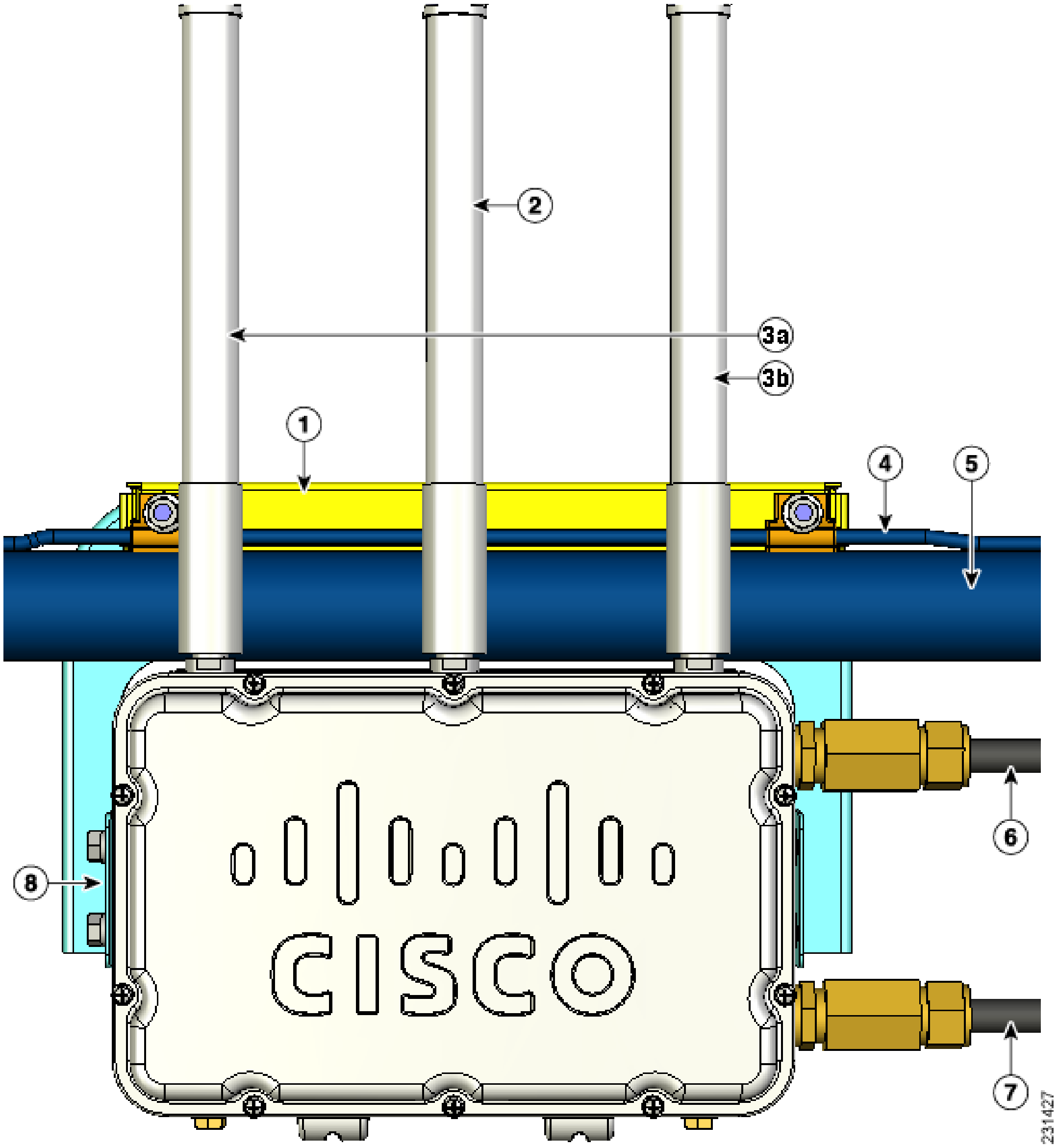
Antenna locations for 5.8 GHz, 4.9 GHz, and 2.4 GHz are fixed and labeled.

Figure 10 shows antenna placement for a two-radio cable mesh access point.

Figure 11 shows antenna placement for a two-radio fiber mesh access point.

Figure 12 shows antenna placement for a three-radio fiber mesh access point.

Figure 10 Two Radio Cable Mesh Access Point Configuration (Hinged-side Facing Forward)



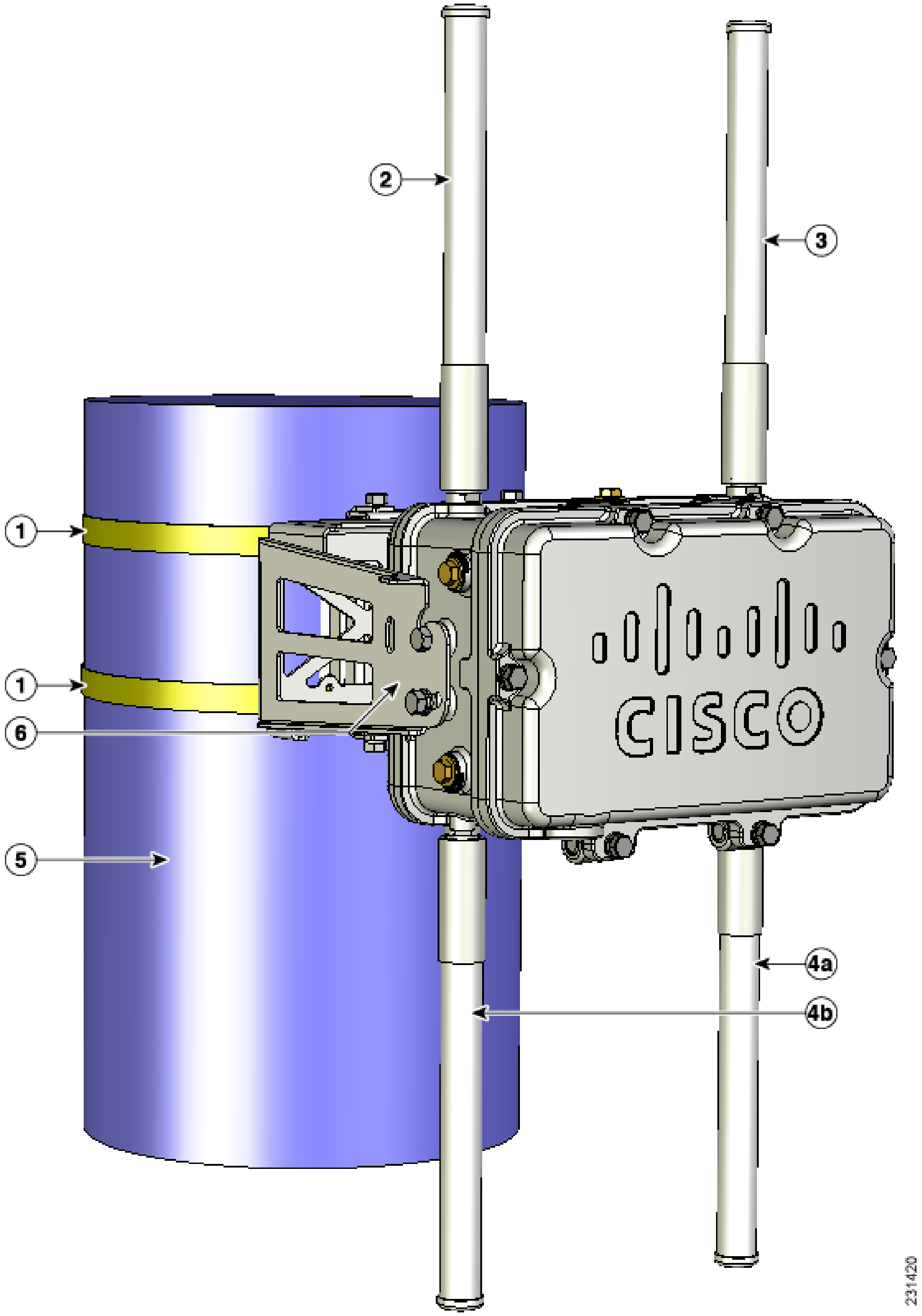
1	Clamp bracket with cable clamps (part of strand mount kit, ordered separately)	**5**	Cable bundle
2	5-GHz antenna[1]	**6**	Fiber-optic connection[2]
3	2.4-GHz antennas[2]	**7**	Cable POC power input[3]
4	Strand support cable	**8**	Strand mount bracket (part of strand mount kit, ordered separately)

[1] Illustration shows antenna for an access point with two radios.

[2] Liquid tight connector not shown.

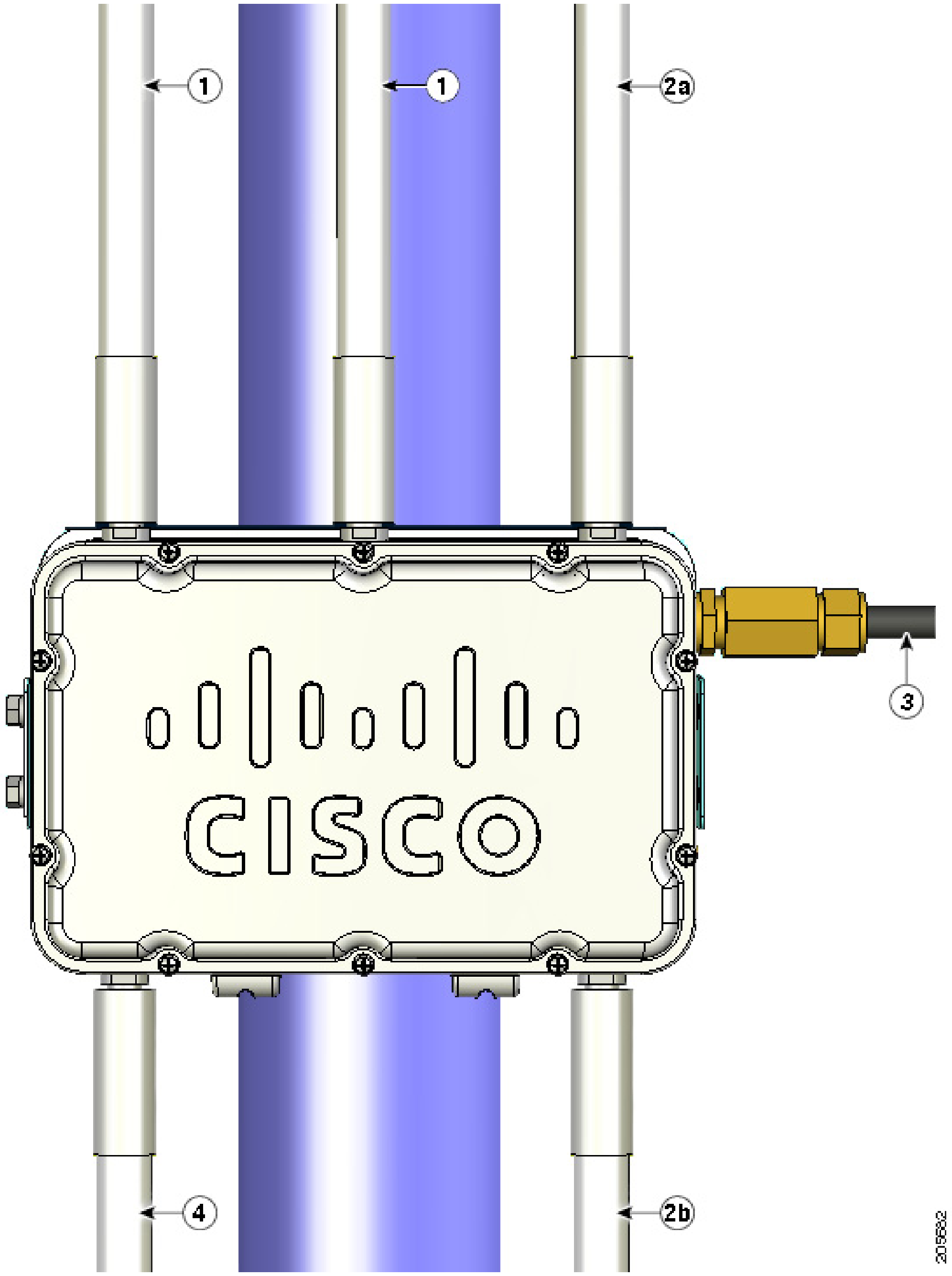
[3] Stinger connector shown is user-supplied.

Figure 11 Two Radio Fiber Mesh Access Point Configuration (Hinged-side Facing Backward)



1	Stainless steel mounting straps (part of pole mount kit)	**4**	2 to 4-GHz antennas
2	2.4-GHz antenna	**5**	Pole (wood, metal, or fiberglass), 2 to 16 in. (5.1 to 40.6 cm) diameter
3	5-GHz antenna	**6**	Mounting bracket (part of pole mount kit)

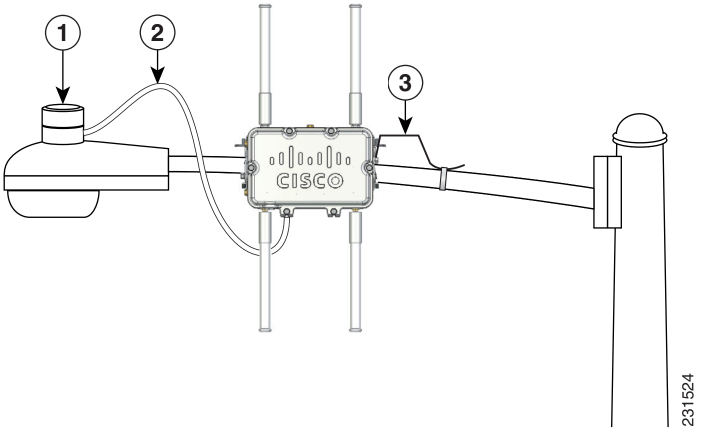
Figure 12 AP1524 Mesh Access Point Pole Mount Configuration (Hinged-side Facing Forward)



1	2.4-GHz antenna (Tx/Rx)	**3**	Fiber-optic connection
2	5-GHz antenna (Tx/Rx)	**4**	4.9-GHz antenna (Tx/Rx)

Figure 13 shows one of the recommended installations of an outdoor AP1520.

Figure 13 Outdoor Pole-top Installation of a Mesh Access Point



1	Outdoor light control	**3**	6-AWG copper grounding wire
2	Streetlight power tap adapter		

Maximum Ratio Combining

AP1520 radios have a much higher transmit power, better receiver sensitivity, and broader outdoor temperature range as compared to AP1510 and AP1505 mesh access points.

- The 5-GHz radio (802.11a) is a Single-in-Single-Out (SISO) architecture and the 2.4-GHz radio (802.11 b/g) is 1x3 Single-in-Multiple-Out (SIMO) architecture.
- The 2.4-GHz radio has one transmitter and three receivers. Output power is configurable to 5 levels. With its 3 receivers enabling maximum-ratio combining (MRC), this radio has better sensitivity and range than a typical SISO 802.11b/g radio for OFDM rates.

When operating with data rates higher than 12 Mbps, you can increase gain on a 2.4-GHz radio to 2.7 dB by adding two antennas and to 4.5 dB, by adding three antennas. For information about RX sensitivities and MRC gain, see Table 7.

Table 7 RX Sensitivities and MRC Gain

	Typical sensitivity (dBM)			**MRC gain**	
Modulation Rate	**One antenna**	**Two antennas MRC**	**Three antennas MRC**	**Two antennas**	**Three antennas**
1	-92.0	-92.0	-92.0	0.0	0.0
2	-91.0	-91.0	-91.0	0.0	0.0
5.5	-90.3	-90.3	-90.3	0.0	0.0
11	-90.0	-90.0	-90.0	0.0	0.0

Table 7 RX Sensitivities and MRC Gain (continued)

	Typical sensitivity (dBM)			MRC gain	
Modulation Rate	One antenna	Two antennas MRC	Three antennas MRC	Two antennas	Three antennas
6	-90.3	-90.3	-90.3	0.0	0.0
9	-90.3	-90.3	-90.3	0.0	0.0
12	-89.0	-89.5	-90.0	0.5	1.0
18	-88.0	-89.5	-90.0	1.5	2.0
24	-84.3	-87.0	-88.3	2.7	4.0
36	-81.3	-84.0	-85.8	2.7	4.5
48	-77.3	-80.0	-81.8	2.7	4.5
54	-76.0	-78.7	-80.5	2.7	4.5

Client Access Certified Antennas (Third-party Antennas)

You can use third-party antennas with AP1520s. However, note the following:

- Cisco does not track or maintain information about the quality, performance, or reliability of the non-certified antennas and cables.
- RF connectivity and compliance is the customer's responsibility.
- Compliance is only guaranteed with Cisco antennas or antennas that are of the same design and gain as Cisco antennas.
- Cisco Technical Assistance Center (TAC) has no training or customer history with regard to non-Cisco antennas and cables.

Cisco 1520 Hazardous Location Certification

The standard AP1520 enclosure is a ruggedized, hardened enclosure that supports the NEMA 4X and IP67 standards for protection to keep out dust, damp and water.

Hazardous Certification (Class 1, Div 2, and Zone 2)

To operate in occasional hazardous environments, such as oil refineries, oil fields, drilling platforms, chemical processing facilities, and open-pit mining, special certification is required and the certification is labeled as Class 1, Div 2, or Zone 2.

Note For USA and Canada, this certification is CSA Class 1, Division 2. For Europe (EU), it is ATEX or IEC Class 1, Zone 2.

Cisco has two Hazardous Certified SKUs for USA and EU: AIR-LAP1522HZ-X-K9 and AIR-LAP1524HZ-X-K9. These SKUs are modified, as per the certification requirements. The hazardous locations certificate requires that all electrical power cables be run through conduit piping to protect against accidental damage to the electrical wiring that could cause a spark and possible explosion. Access points for hazardous locations contain an internal electrical mounting connect that receives discrete wires from a conduit interface coupler entering from the side of the housing. After the electrical wiring is installed, a cover housing is installed over the electrical connector to prevent exposure to the electrical wiring. On the outside of the housing is a hazardous location certification label (CSA, ATEX, or IEC) that identifies the type of certifications and environments that the equipment is approved for operation.

Note Power entry module for CSA (USA & CANADA) is Power Entry Module, Groups A,B,C,D with T5v(120º C) temp code.

Power Entry Module for ATEX (EU) is Power entry module Groups IIC, IIB, IIA with T5 (120º C) temp code.

Hazardous Certification (Div 1 > Div 2 and Zone 1 > Zone 2)

Class 1, Division 1/Zone 1 is for environments with full-time ignitable concentrations of flammable gases, vapors, or liquids. To meet the requirements of the Div 1 > Div 2 and Zone 1 > Zone 2 locations, we recommend a TerraWave Solutions CSA certified protective Wi-Fi enclosure (see Table 8).

Table 8 TerraWave Enclosures

Access Point Model	Enclosure Part No	Description
1240	TerraWave XEP1242	18 x12 x8 Protective Wi-Fi Enclosure that includes the Cisco 1242 Access Point
1522, 1524	TerraWave Part Number: XEP1522	18 x 12 x8 Protective Wi-Fi Enclosure that includes the Cisco 1522 Access Point

For more information about the TerraWave enclosures, see

http://www.tessco.com/yts/partner/manufacturer_list/vendors/terrawave/pdf/terrawavehazardouesenclosuresjan08.pdf

Cisco Wireless LAN Controllers

The wireless mesh solution is supported by Cisco 2100 Series, Cisco 4400 Series Wireless LAN Controllers, and 5500 Series Wireless LAN Controllers. The Cisco 5500 and 4400 Series Controllers (see Figure 14) are recommended for wireless mesh deployments because they can scale to large numbers of access points and can support Layer 3 CAPWAP.

Figure 14 Cisco 5500 Wireless LAN Controller

For more information about the Cisco 5500, 4400, and 2100 Wireless LAN Controllers, see:

http://www.cisco.com/en/US/products/hw/wireless/index.html#,hide-id-trigger-g1-wireless_LAN

and http://www.cisco.com/en/US/products/ps7206/products_installation_and_configuration_guides_list.html

Cisco WCS

The Cisco WCS provides a graphical platform for wireless mesh planning, configuration, and management. Network managers can use Cisco WCS to design, control, and monitor wireless mesh networks from a central location.

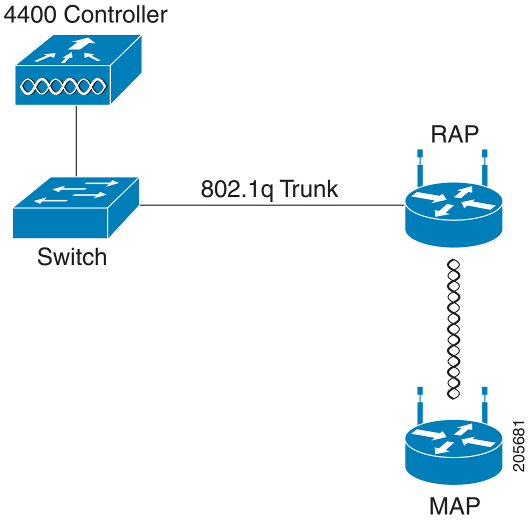
With Cisco WCS, network administrators have a solution for RF prediction, policy provisioning, network optimization, troubleshooting, user tracking, security monitoring, and wireless LAN systems management. Graphical interfaces make wireless LAN deployment and operations simple and cost-effective. Detailed trending and analysis reports make Cisco WCS vital to ongoing network operations.

Cisco WCS runs on a server platform with an embedded database. This provides scalability necessary to allow hundreds of controllers and thousands of Cisco mesh access points to be managed. Controllers can be located on the same LAN as Cisco WCS, on separate routed subnets, or across a wide-area connection.

Multiple, geographically dispersed Cisco WCS management platforms can be cost-effectively and easily managed by the Cisco WCS Navigator. Cisco WCS Navigator supports up to 20 Cisco WCS management platforms with manageability of up to 30,000 mesh access points from a single management console. Together, Cisco WCS and Cisco WCS Navigator provide a wireless LAN management solution for even the largest enterprise environments and outdoor deployments.

Figure 15 shows the interconnections between the controllers, Cisco WCS, and AP1520s.

Figure 15 Interconnections to the Solution



Mesh Deployment Modes

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

- Wireless mesh
- WLAN backhaul

Wireless Mesh Network

In a Cisco wireless outdoor mesh network, multiple mesh access points comprise a network that provides secure, scalable outdoor wireless LAN. Figure 16 shows an example of a simple mesh network deployment composed of mesh access point (MAPs and RAPs), controllers, and Cisco WCS.

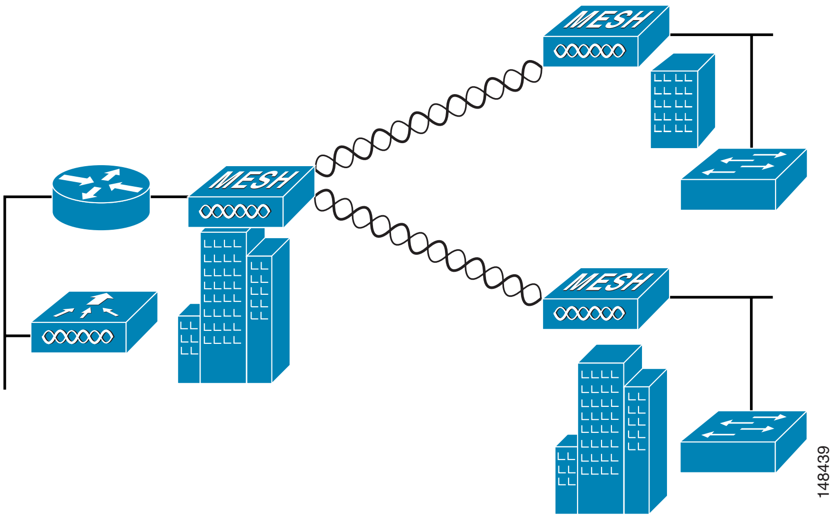
The three RAPs are connected to the wired network at each location and are located on the building roof. All the downstream access points operate as MAPs and communicate using wireless links (not shown).

Both MAPs and RAPs can provide WLAN client access; however, the location of RAP are often not suitable for providing client access. All the three access points in Figure 16 are located on the building roofs and are functioning as RAP. These RAP are connected to the network at each location.

Some of the buildings have onsite controllers to terminate CAPWAP sessions from the mesh access points but it is not a mandatory requirement because CAPWAP sessions can be back hauled to a controller over a wide-area network (WAN). (See Figure 17.)

Note For more details on CAPWAP, see the "Architecture Overview" section on page 32.

Figure 16 Wireless Mesh Deployment



Wireless Backhaul

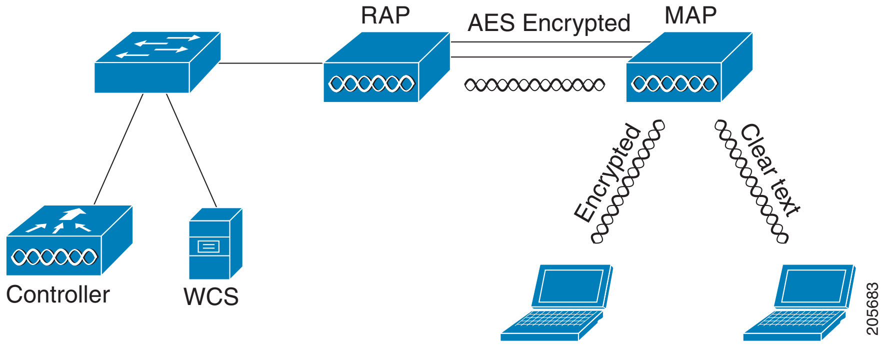
In a Cisco wireless backhaul network, traffic can be bridged between MAPs and RAPs. This traffic can be from wired devices that are being bridged by the wireless mesh or CAPWAP traffic from the mesh access points. This traffic is always AES encrypted when it crosses a wireless mesh link such as a wireless backhaul (Figure 17).

AES encryption is established as part of the mesh access point neighbor relationship with other mesh access points. The encryption keys used between mesh access points are derived during the EAP authentication process.

Universal Access

You can configure the backhaul on mesh access points to accept client traffic over its 802.11a radio. This feature is identified as Backhaul Client Access in the controller GUI (Monitor > Wireless). When this feature is disabled, backhaul traffic is transmitted only over the 802.11a radio and client association is allowed only over the 802.11b/g radio. For more information about the configuration, see the "Universal Client Access on Serial Backhaul Access Points" section on page 102.

Figure 17 Wireless Backhaul



Architecture Overview

This section describes the architecture overview of a mesh network.

CAPWAP

CAPWAP is the provisioning and control protocol used by the controller to manage access points (mesh and non-mesh) in the network. In release 5.2, CAPWAP replaced LWAPP.

Upgrading from an earlier LWAPP release (4.1.x.x or earlier) to release 5.2 is transparent. CAPWAP supports path maximum transmission unit (MTU) discovery and it is configurable on switches and routers in the backbone network.

Note Mesh features are not supported on controller releases 5.0 and 5.1.

CAPWAP is becoming the protocol of choice to manage access points. It significantly reduces capital expenditures (CapEx) and operational expenses (OpEx), enabling the Cisco wireless mesh networking solution to be a cost-effective and secure deployment option in enterprise, campus, and metropolitan networks.

CAPWAP Discovery on a Mesh Network

CAPWAP discovery on a mesh network follows these steps:

1. A mesh access point establishes a link before starting CAPWAP discovery, whereas a non-mesh access point starts CAPWAP discovery using a static IP for the mesh access point, if any.

2. The mesh access point initiates CAPWAP discovery using a static IP for the mesh access point on the Layer 3 network or searches the network for its assigned primary, secondary, or tertiary controller. A maximum of 10 attempts are made to connect.

   Note The mesh access point searches a list of controllers configured on the access point (primed) during setup.

3. If step 2 fails after 10 attempts, the mesh access point falls back to DHCP and attempts to connect in 10 tries.
4. If both steps 2 and 3 fail and there is no successful CAPWAP connection to a controller, then the mesh access point falls back to LWAPP.
5. If there is no discovery after attempting steps 2, 3, and 4, the mesh access point tries the next link.

Dynamic MTU Detection

If the MTU is changed in the network, the access point detects the new MTU value and forwards that to the controller to adjust to the new MTU. After both the access point and the controller are set at the new MTU, all data within their path are fragmented into the new MTU. The new MTU size is used until it is changed. The default MTU on switches and routers is 1500 bytes.

XML Configuration File

Starting from release 5.2, mesh features within the controller's boot configuration file are saved in an XML file in ASCII format. The XML configuration file is saved in the flash memory of the controller.

Note The current release does not support binary configuration files; however, configuration files are in the binary state *immediately* after an upgrade from a mesh release to controller software release 7.0. After reset, the XML configuration file is selected.

Caution Do not edit the XML file. Downloading a modified configuration file onto a controller causes a cyclic redundancy check (CRC) error on boot and the configuration is reset to the default values.

You can easily read and modify the XML configuration file by converting it to CLI format. To convert from XML to CLI format, upload the configuration file to a TFTP or an FTP server. The controller initiates the conversion from XML to CLI during the upload.

Once on the server, you can read or edit the configuration file in CLI format. Then, you can download the file back to the controller. The controller then converts the configuration file back to XML format, saves it to flash memory, and then reboots using the new configuration.

Note The controller does not support uploading and downloading of port configuration CLI commands. If you want to configure the controller ports, enter the relevant commands summarized below:

Note The commands listed below are manually entered after the software upgrade to release 7.0.

- **config port linktrap** {*port* | **all**} {**enable** | **disable**}–Enables or disables the up and down link traps for a specific controller port or for all ports.
- **config port adminmode** {*port* | **all**} {**enable** | **disable**}–Enables or disables the administrative mode for a specific controller port or for all ports.
- **config port multicast appliance** *port* {**enable** | **disable**}–Enables or disables the multicast appliance service for a specific controller port.
- **config port power** {*port* | ***all***} {**enable** | **disable**}–Enables or disables power over Ethernet (PoE) for a specific controller port or for all ports.

CLI commands with known keywords and proper syntax are converted to XML while improper CLI commands are ignored and saved to flash memory. Any field with an invalid value is filtered out and set to a default value by the XML validation engine.Validation occurs during bootup.

To see any ignored commands or invalid configuration values, enter the following command:

show invalid-config

Note You can only execute this command before either the **clear config** or **save config** command. If the downloaded configuration contains a large number of invalid CLI commands, you might want to upload the invalid configuration to the TFTP or FTP server for analysis.

Access passwords are hidden (obfuscated) in the configuration file. To enable or disable access point or controller passwords, enter the following command:

config switchconfig secret-obfuscation {**enable** | **disable**}

AWPP

AWPP is designed specifically for wireless mesh networking to provide ease of deployment, fast convergence, and minimal resource consumption.

AWPP takes advantage of the CAPWAP WLAN, where client traffic is tunneled to the controller and is therefore hidden from the AWPP process. Also, the advance radio management features in the CAPWAP WLAN solution are available to the wireless mesh network and do not have to be built into AWPP.

AWPP enables a remote access point to dynamically find the best path back to a RAP for each MAP that is part of the RAP's bridge group (BGN). Unlike traditional routing protocols, AWPP takes RF details into account.

To optimize the route, a MAP actively solicits neighbor MAP. 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. The path decisions of AWPP are based on link quality and the number of hops.

AWPP automatically determines the best path back to the CAPWAP controller by calculating the cost of each path in terms of signal strength and number of hops. After the path is established, AWPP continuously monitors conditions and changes routes to reflect changes in conditions. AWPP also performs a smoothing function to signal condition information to ensure that the ephemeral nature of RF environments does not impact network stability.

Traffic Flow

The traffic flow within the wireless mesh can be divided into three components:

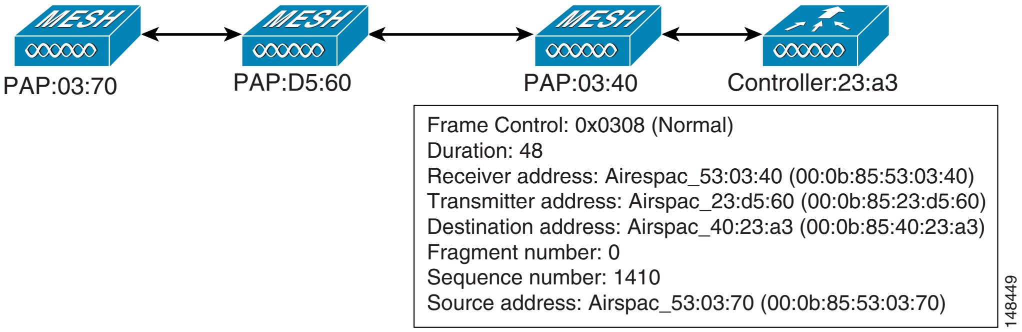
1. Overlay CAPWAP traffic that flows within a standard CAPWAP access point deployment; that is, CAPWAP traffic between the CAPWAP access point and the CAPWAP controller.
2. Wireless mesh data frame flow.
3. AWPP exchanges.

As the CAPWAP model is well known and the AWPP is a proprietary protocol, only the wireless mesh data flow is described. The key to the wireless mesh data flow is the address fields of the 802.11 frames being sent between mesh access points.

An 802.11 data frame can use up to four address fields: receiver, transmitter, destination, and source. The standard frame from a WLAN client to an AP uses only three of these address fields because the transmitter address and the source address are the same. However, in a WLAN bridging network, all four address fields are used because the source of the frame might not the transmitter of the frame, because the frame might have been generated by a device behind the transmitter.

Figure 18 shows an example of this type of framing. The source address of the frame is MAP:03:70, the destination address of this frame is the controller (the mesh network is operating in Layer 2 mode), the transmitter address is MAP:D5:60, and the receiver address is RAP:03:40.

Figure 18 Wireless Mesh Frame



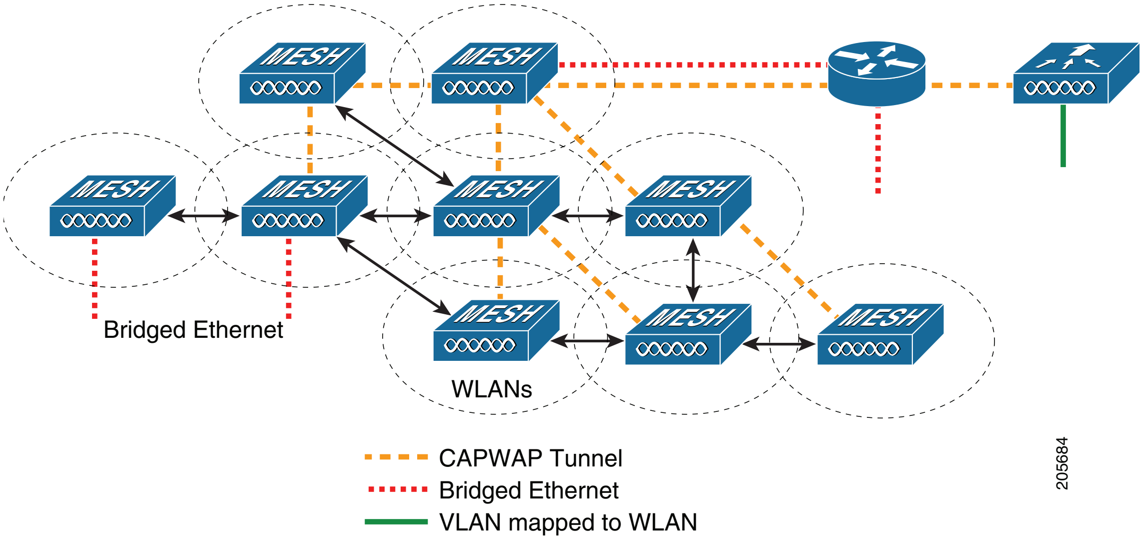
Frame Control: 0x0308 (Normal)
Duration: 48
Receiver address: Airespac_53:03:40 (00:0b:85:53:03:40)
Transmitter address: Airspac_23:d5:60 (00:0b:85:23:d5:60)
Destination address: Airspac_40:23:a3 (00:0b:85:40:23:a3)
Fragment number: 0
Sequence number: 1410
Source address: Airspac_53:03:70 (00:0b:85:53:03:70)

As this frame is sent, the transmitter and receiver addresses change on a hop-by-hop basis. AWPP is used to determine the receiver address at each hop. The transmitter address is known because it is the current mesh access point. The source and destination addresses are the same over the entire path.

If the RAP's controller connection is Layer 3, the destination address for the frame is the default gateway MAC address, because the MAP has already encapsulated the CAPWAP in the IP packet to send it to the controller, and is using the standard IP behavior of using ARP to find the MAC address of the default gateway.

Each mesh access point within the mesh forms an CAPWAP session with a controller. WLAN traffic is encapsulated inside CAPWAP and is mapped to a VLAN interface on the controller. Bridged Ethernet traffic can be passed from each Ethernet interface on the mesh network and does not have to be mapped to an interface on the controller (see Figure 19).

Figure 19 Logical Bridge and WLAN Mapping

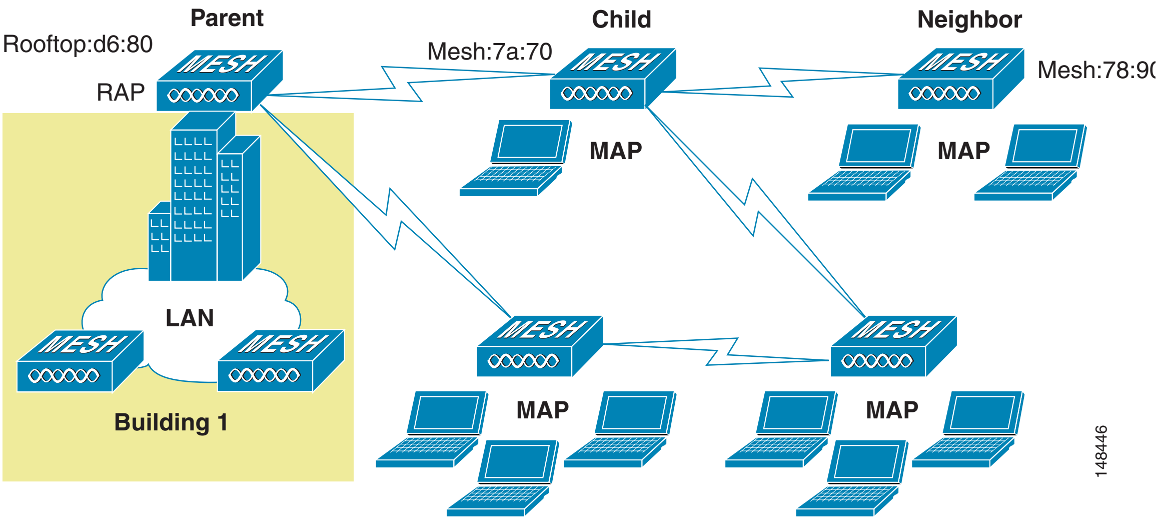


Mesh Neighbors, Parents, and Children

Relationships among mesh access points are as a parent, child, or neighbor (see Figure 20).

- 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 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 20 Parent, Child, and Neighbor Access Points



Choosing the Best Parent

AWPP follows this process in selecting parents for a RAP or MAP with a radio backhaul:

- A list of channels with neighbors is generated by passive scanning in the *scan* state, which is a subset of all backhaul channels.
- The channels with neighbors are sought by actively scanning in the *seek* state and the backhaul channel is changed to the channel with the best neighbor.
- The parent is set to the best neighbor and the parent-child handshake is completed in the *seek* state.
- Parent maintenance and optimization occurs in the *maintain* state.

This algorithm is run at startup and whenever a parent is lost and no other potential parent exists, and is usually followed by CAPWAP network and controller discovery. All neighbor protocol frames carry the channel information.

Parent maintenance occurs by the child node sending a directed NEIGHBOR_REQUEST to the parent and the parent responding with a NEIGHBOR_RESPONSE.

Parent optimization and refresh occurs by the child node sending a NEIGHBOR_REQUEST broadcast on the same channel on which its parent resides, and by evaluating all responses from neighboring nodes on the channel.

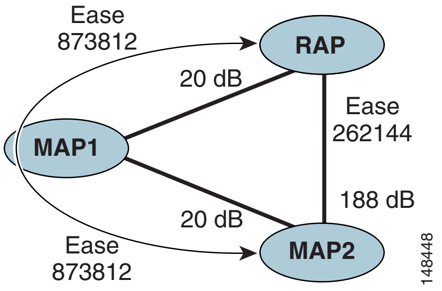
A parent mesh access point provides the best path back to a RAP. AWPP uses ease to determine the best path. Ease can be considered the opposite of cost, and the preferred path is the path with the higher ease.

Ease Calculation

Ease is calculated using the SNR and hop value of each neighbor, and applying a multiplier based on various SNR thresholds. The purpose of this multiplier is to apply a spreading function to the SNRs that reflects various link qualities.

Figure 21 shows parent path selection where MAP2 prefers the path through MAP1 because the adjusted ease of (436906) though this path is greater then the ease value (262144) of the direct path from MAP2 to RAP.

Figure 21 Parent Path Selection



Parent Decision

A parent mesh access point is chosen by using the adjusted ease, which is the ease of each neighbor divided by the number of hops to the RAP:

$$\text{adjusted ease} = \frac{\min(\textit{ease at each hop})}{\text{Hop count}}$$

SNR Smoothing

One of the challenges in WLAN routing is the ephemeral nature of RF. This must be considered when analyzing an optimal path and deciding when a change in path is required. The SNR on a given RF link can change substantially from moment to moment, and changing route paths based on these fluctuations results in an unstable network, with severely degraded performance. To effectively capture the underlying SNR but remove moment-to-moment fluctuations, a smoothing function is applied that provides an adjusted SNR.

In evaluating potential neighbors against the current parent, the parent is given 20% of bonus-ease on top of the parent's calculated ease, to reduce the ping-pong effect between parents. This implies that a potential parent must be significantly better for a child to make a switch. Parent switching is transparent to CAPWAP and other higher-layer functions.

Loop Prevention

To ensure that routing loops are not created, AWPP discards any route that contains its own MAC address. That is, routing information apart from hop information contains the MAC address of each hop to the RAP; therefore, a mesh access point can easily detect and discard routes that loop.

Design Considerations

Each outdoor wireless mesh deployment is unique, and each environment has its own challenges with available locations, obstructions, and available network infrastructure. Design requirements driven by expected users, traffic, and availability needs are also major design criteria. This section describes important design considerations and provides an example of a wireless mesh design.

Wireless Mesh Constraints

The following are a few system characteristics to consider when you design and build a wireless mesh network. Some of these apply to the backhaul network design and others to the CAPWAP controller design:

- We recommend setting the backhaul rate to **auto**.

  When the bridge data rate is set to **auto**, the mesh backhaul chooses the highest rate possible given its link quality and sustainability of that rate. The bridge data rate is set on each access point individually. It is not a global setting.

  - Typically, 24 Mbps is chosen as the optimal backhaul rate because it aligns with the maximum coverage of the WLAN portion of the client WLAN of the MAP; that is, the distance between MAP using 24 Mbps backhaul should allow for seamless WLAN client coverage between the MAP.
  - 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 mesh channel and bridge data rate (mesh backhaul bit rate) is set on each individual access point. It is not a global setting.

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

- The required minimum LinkSNR for backhaul links per data rate is shown in Table 9.

Table 9 Backhaul Data Rates and Minimum LinkSNR Requirements

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

- The required minimum LinkSNR value is driven by the data rate and the following formula: *Minimum SNR + fade margin*.

  Table 10 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 10 Minimum Required LinkSNR Calculations by Data Rate

Date Rate (Mbps)	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 or four primarily to maintain sufficient backhaul throughput, because each mesh access point 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 on 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. For more information, see the "Controller Planning" section.

Controller Planning

The following items affect the number of controllers required in a mesh network:

- Mesh access points (RAPs and MAPs) in the network.

  The wired network that connects the RAP and controllers can affect the total number of access points supported in the network. If this network allows the controllers to be equally available to all access points without any impact on WLAN performance, the access points can be evenly distributed across all controllers for maximum efficiency. If this is not the case, and controllers are grouped into various clusters or PoPs, the overall number of access points and coverage are reduced.

  For example, you can have 72 Cisco 4400 Series Controllers in a mobility group, and each Cisco 4400 Series Controller supports 100 local access points. This gives a total number of 7200 possible access points per mobility group.

- Number of mesh access points (RAPs and MAPs) supported per controller. See Table 11.

  For clarity, nonmesh access points are referred to as *local* access points in this document.

Table 11 Mesh Access Point Support by Controller Model

Controller Model	Local AP Support (non-mesh)[1]	Maximum Possible Mesh AP Support	RAP	MAP	Total Mesh AP Support
5508[2]	500	500	1	499	500
			100	400	500
			150	350	500
			200	300	500
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

Table 11 Mesh Access Point Support by Controller Model (continued)

Controller Model	Local AP Support (non-mesh)[1]	Maximum Possible Mesh AP Support	RAP	MAP	Total Mesh AP Support
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.

Note The Wireless LAN Controller modules NM and NME now support mesh 1520 series access points from Wireless LAN Controller (WLC) software release 5.2 and later releases.

Note Mesh is fully supported on Cisco 5508 Controllers. The Base License (LIC-CT508-Base) is sufficient for indoor and outdoor APs (AP152X). The WPlus License (LIC-WPLUS-SW) is merged with the base license. The WPlus License is not required for indoor mesh APs (1242s/1130s).

Mesh APs (MAPs/RAPs) are counted as full APs on Cisco 5508 Controllers.

With other controller platforms, MAPs are counted as half APs.

Data Plane Transport Layer Security (DTLS) is not supported on mesh access points.

Site Preparation and Planning

This section provides implementation details and configuration examples.

Site Survey

We recommend that you perform a radio site survey before installing the equipment. A site survey reveals problems such as interference, Fresnel zone, or logistics problems. A proper site survey involves temporarily setting up mesh links and taking measurements to determine whether your antenna calculations are accurate. Determine the correct location and antenna before drilling holes, routing cables, and mounting equipment.

Note When power is not readily available, we recommend you to use an unrestricted power supply (UPS) to temporarily power the mesh link.

Pre-Survey Checklist

Before attempting a site survey, determine the following:

- How long is your wireless link?
- Do you have a clear line of sight?
- What is the minimum acceptable data rate within which the link runs?
- Is this a point-to-point or point-to-multipoint link?
- Do you have the correct antenna?
- Can the access point installation area support the weight of the access point?
- Do you have access to both of the mesh site locations?
- Do you have the proper permits, if required?
- Do you have a partner? Never attempt to survey or work alone on a roof or tower.
- Have you configured the 1522 or 1524 before you go onsite? It is always easier to resolve configuration or device problems first.
- Do you have the proper tools and equipment to complete your task?

Note Cellular phones or handheld two-way radios can be helpful to do surveys.

Outdoor Site Survey

Deploying WLAN systems outdoors requires a different skill set to indoor wireless deployments. Considerations such as weather extremes, lightning, physical security, and local regulations need to be taken into account.

When determining the suitability of a successful mesh link, define how far the mesh link is expected to transmit and at what radio data rate. Remember that the data rate is not directly included in the wireless routing calculation, and we recommend that the same data rate is used throughout the same mesh (the recommended rate is 24 Mbps).

Design recommendations for mesh links are as follows:

- MAP deployment cannot exceed 35 feet in height above the street.
- MAPs are deployed with antennas pointed down toward the ground.
- Typical 5-GHz RAP-to-MAP distances are 1000 to 4000 feet.
- RAP locations are typically towers or tall buildings.
- Typical 5-GHz MAP-to-MAP distances are 500 to 1000 feet.
- MAP locations are typically short building tops or streetlights.
- Typical 2.4-GHz MAP-to-client distances are 300 to 500 feet.
- Client locations are typically laptops, CPEs, or professionally house-mounted antennas.

Determining Line of Sight

When you determine the suitability of a successful link, you must define how far the link is expected to transmit and at what radio data rate. Very close links, one kilometer or less, are fairly easy to achieve assuming there is *clear line of sight (LOS)*–a path with no obstructions.

Since mesh radio waves have very high frequency in the 5-GHz band, the radio wavelength is small; therefore, the radio waves do not travel as far as radio waves on lower frequencies, given the same amount of power. This higher frequency range makes the mesh ideal for unlicensed use because the radio waves do not travel far unless a high-gain antenna is used to tightly focus the radio waves in a given direction.

This high-gain antenna configuration is recommended only for connecting RAP to the MAP. To optimize mesh behavior, omnidirectional antennas are used because mesh links are limited to one mile (1.6 km). The curvature of the earth does not impact line-of-sight calculations because the curvature of the earth changes every six miles (9.6 km).

Weather

In addition to free space path loss and line of sight, weather can also degrade a mesh link. Rain, snow, fog, and any high humidity condition can slightly obstruct or affect line of sight, introducing a small loss (sometimes referred to as *rain fade* or *fade margin*), which has little effect on the mesh link. If you have established a stable mesh link, weather should not be a problem; however, if the link is poor to begin with, bad weather can degrade performance or cause loss of link.

Ideally, you need line of sight; a white-out snow storm does not allow line of sight. Also, while storms may make the rain or snow itself appear to be the problem, many times it might be additional conditions caused by the adverse weather. For example, perhaps the antenna is on a mast pipe and the storm is blowing the mast pipe or antenna structure and that movement is causing the link to come and go, or there might be a large build-up of ice or snow on the antenna.

Fresnel Zone

A Fresnel zone is an imaginary ellipse around the visual line of sight between the transmitter and receiver. As radio signals travel through free space to their intended target, they could encounter an obstruction in the Fresnel area, degrading the signal. Best performance and range are attained when there is no obstruction of this Fresnel area. Fresnel zone, free space loss, antenna gain, cable loss, data rate, link distance, transmitter power, receiver sensitivity, and other variables play a role in determining how far your mesh link goes. Links can still occur as long as 60–70 percent of the Fresnel area is unobstructed, as illustrated in Figure 22.

Figure 23 illustrates an obstructed Fresnel zone.

Figure 22 Point-to-Point Link Fresnel Zone

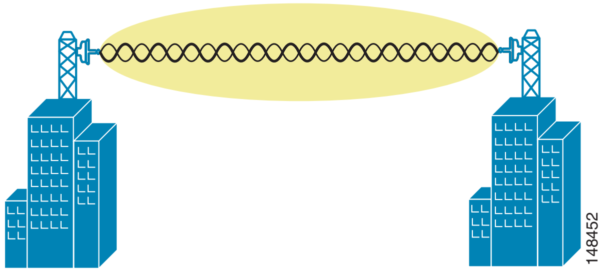
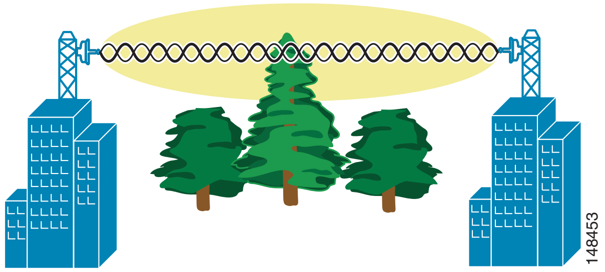


Figure 23 Typical Obstructions in a Fresnel Zone



It is possible to calculate the radius of the Fresnel zone (in feet) at any particular distance along the path using this equation:

F1 = 72.6 X square root (d/4 x f)

where

F1 = the first Fresnel zone radius in feet

D = total path length in miles

F = frequency (GHz)

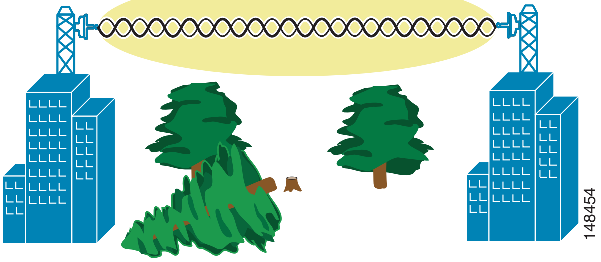
Normally, 60 percent of the first Fresnel zone clearance is recommended, so the above formula for 60 percent Fresnel zone clearance can be expressed as:

0.60 F1= 43.3 x square root (d/4 x f)

These calculations are based on a flat terrain.

Figure 24 shows the removal of an obstruction in the Fresnel zone of the wireless signal.

Figure 24 Removing Obstructions in a Fresnel Zone



Fresnel Zone Size in Wireless Mesh Deployments

To give an approximation of size of the maximum Fresnel zone to be considered, at a possible minimum frequency of 4.9 GHz, the minimum value changes depending on the regulatory domain. The minimum figure quoted is a possible band allocated for public safety in the U.S., and a maximum distance of one mile gives a Fresnel zone of clearance requirement of 9.78 ft = 43.3 x SQR(1/(4*4.9)). This clearance is relatively easy to achieve in most situations. In most deployments, distances are expected to be less than one mile, and the frequency greater than 4.9 GHz, making the Fresnel zone smaller. Every mesh deployment should consider the Fresnel zone as part of its design, but in most cases, it is not expected that meeting the Fresnel clearance requirement is an issue.

Hidden Nodes Interference

The mesh backhaul uses the same 802.11a channel for all nodes in that mesh, and this can introduce hidden nodes into the WLAN backhaul environment, as shown in Figure 25.

Figure 25 Hidden Nodes

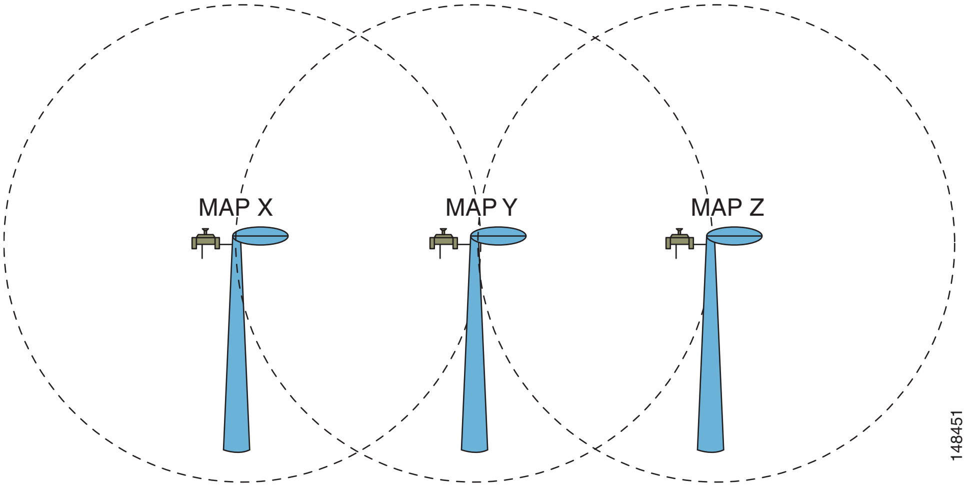


Figure 25 shows the following three MAPs:

- MAP X
- MAP Y
- MAP Z

If MAP X is the route back to the RAP for MAP Y and Z, both MAP X and MAP Z might be sending traffic to MAP Y at the same time. MAP Y can see traffic from both MAP X and Z, but MAP X and Z cannot see each other because of the RF environment. This means that the carrier sense multi-access (CSMA) mechanism does not stop MAP X and Z from transmitting during the same time window; if either of these frames is destined for a MAP, it is corrupted by the collision between frames and requires retransmission.

Although all WLANs at some time can expect some hidden node collisions, the fixed nature of the MAP makes hidden node collisions a persistent feature of the mesh WLAN backhaul under some traffic conditions such as heavy loads and large packet streams.

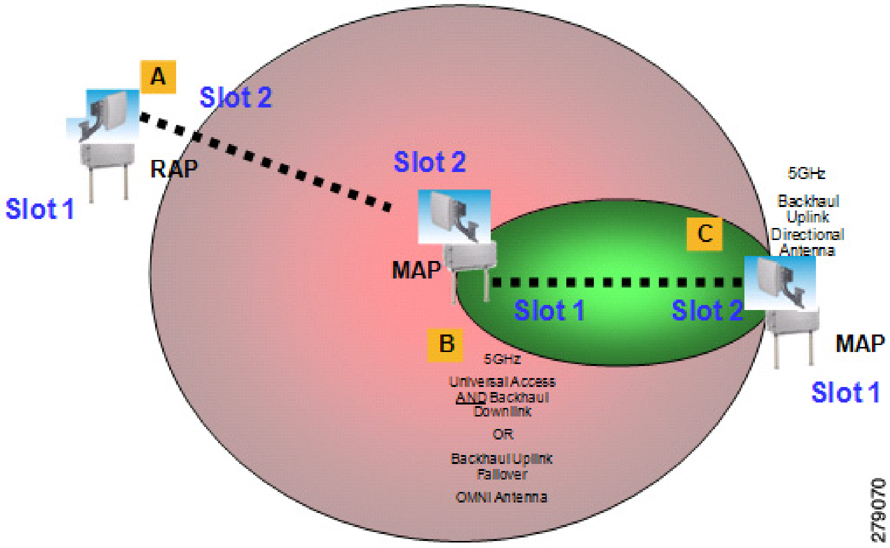
Both the hidden node problem and the exposed node problem are inherent to wireless mesh networks because mesh access points share the same backhaul channel. Because these two problems can affect the overall network performance, the Cisco mesh solution seeks to mitigate these two problems as much as possible. For example, the AP1520s have at least two radios: one for backhaul access on a 5-GHz channel and the other for 2.4-GHz client access. In addition, the radio resource management (RRM) feature enables cell breathing and automatic channel change, which can effectively decrease the collision domains in a mesh network.

There is an additional solution that can help to further mitigate these two problems. To reduce collisions and to improve stability under high load conditions, the 802.11 MAC uses an exponential backoff algorithm, where contending nodes back off exponentially and retransmit packets whenever a perceived collision occurs. Theoretically, the more retries a node has, the smaller the collision probability will be. In practice, when there are only two contending stations and they are not hidden stations, the collision probability becomes negligible after just three retries. Collision probability increases when there are more contending stations. Therefore, when there are many contending stations in the same collision domain, a higher retry limit and a larger maximum contention window are necessary. Further, collision probability does not decrease exponentially when there are hidden nodes in the network. In this case, an RTS/CTS exchange can be used to mitigate the hidden node problem.

Functional Routing of Three Radio MAPs

Because a directional antenna is required to be attached to the slot 2 radios, you should align and RF tune each link to minimize the hidden node effect. For example, a MAP at location C should be aligned to the MAP at location B. The MAP at location C should not be able to see AP at location A (see Figure 26). This can be achieved by first aligning the antennas and then optimizing each link by tuning the RF power. A channel is reused after 4 hops. A maximum number of 8 hops is supported.

Figure 26 Functional Routing Example



Co-Channel Interference

In addition to hidden node interference, co-channel interference can also impact performance. Co-channel interference occurs when adjacent radios on the same channel interfere with the performance of the local mesh network. This interference takes the form of collisions or excessive deferrals by CSMA. In both cases, performance of the mesh network is degraded. With appropriate channel management, co-channel interference on the wireless mesh network can be minimized.

Wireless Mesh Network Coverage Considerations

This section provides a summary of items that must be considered for maximum wireless LAN coverage in an urban or suburban area, to adhere to compliance conditions for respective domains.

The following recommendations assume a flat terrain with no obstacles (green field deployment).

Cisco always recommends a site survey before taking any real estimations for the area and creating a bill of materials.

Cell Planning and Distance

The RAP-to-MAP ratio is the starting point. For general planning purposes, the current ratio is 20 MAPs per RAP.

We recommend the following values for cell planning and distance in non-voice networks:

- RAP-to-MAP ratio—Recommended maximum ratio is 20 MAPs per RAP.
- AP-to-AP distance—A spacing of no more than of 2000 ft between each mesh access point is recommended. When you extend the mesh network on the backhaul (no client access), use a cell radius of 1000 ft.
- Hop count—Three to four hops.
  - One square mile in ft (5280^2), is nine cells and you can cover one square mile with approximately three or four hops. (See Figure 27 and Figure 28.)

- For 2.4 GHz, the local access cell size radius is 600 feet. One cell size is around 1.310 x 10^6, so there are 25 cells per square mile. (See Figure 29 and Figure 30.)

Figure 27 Cell Radius of 1000 Feet and Access Point Placement for Non-Voice Mesh Networks

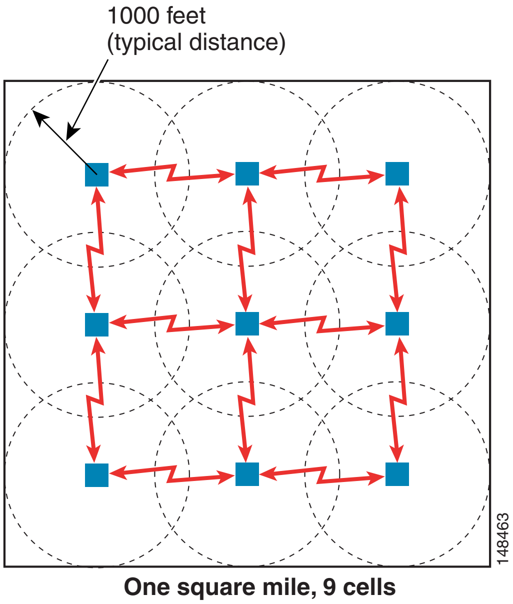


Figure 28 Path Loss Exponent 2.3 to 2.7

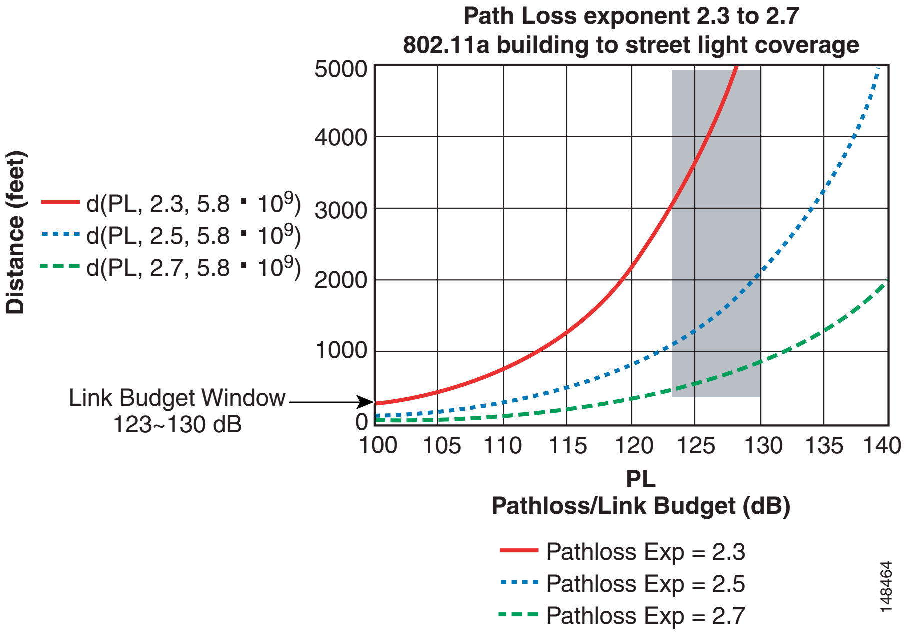


Figure 29 Cell Radius of 600 Feet and Access Point Placement for Non-Voice Mesh Networks

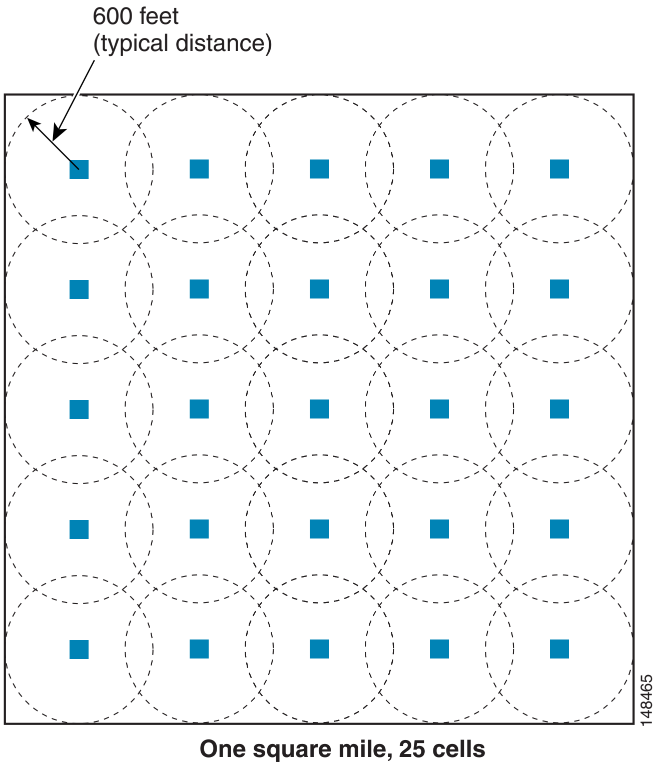


Figure 30 Path Loss Exponent 2.5 to 3.0

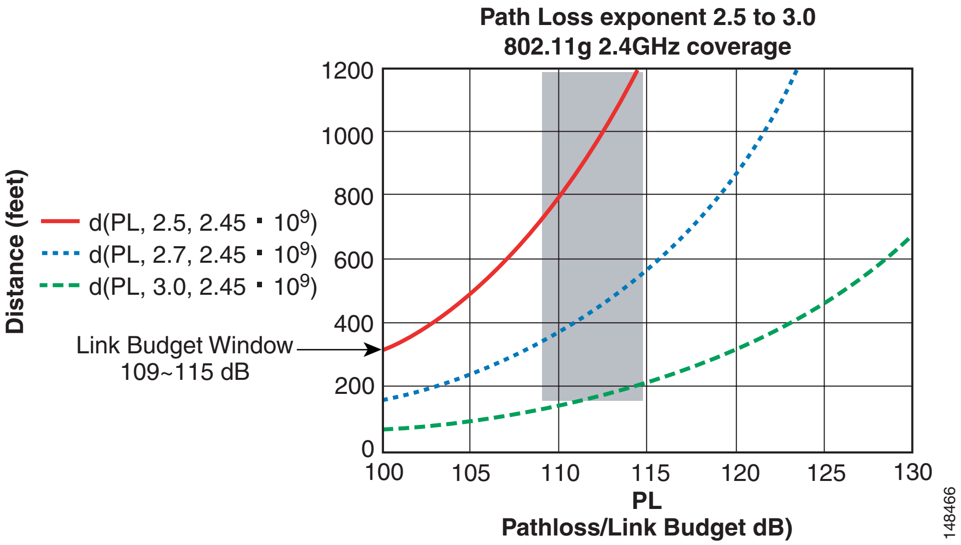
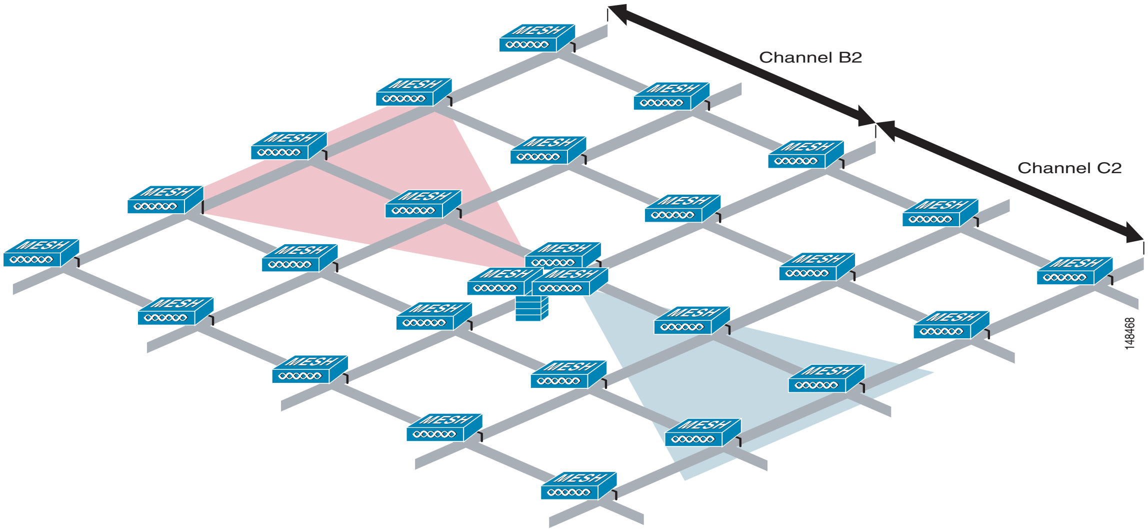


Figure 31 shows a schematic of the wireless mesh layout.

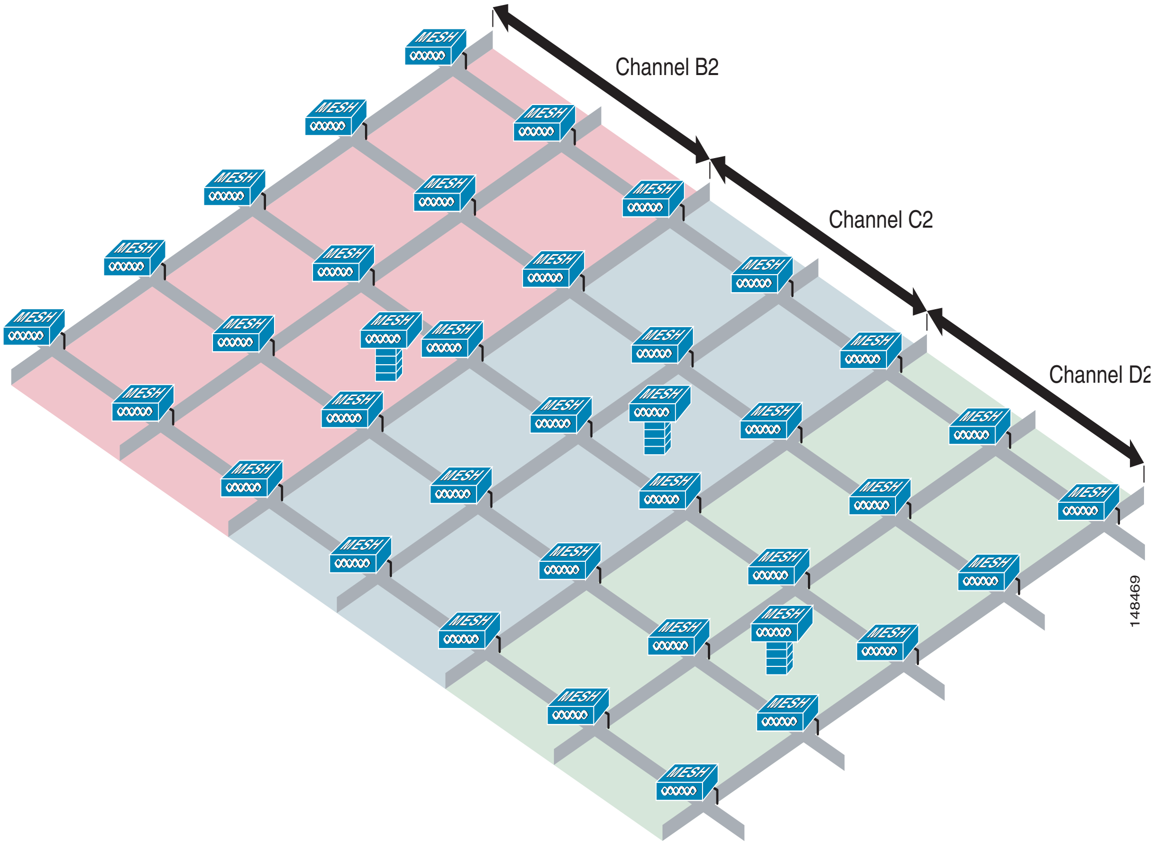
The RAPs shown in Figure 31 are simply a starting point. The goal is to use the RAP location in combination with the RF antenna design to ensure that there is a good RF link to the MAP within the core of the cell. This means that the physical location of the RAPs can be on the edge of the cell, and a directional antenna is used to establish a link into the center of the cell. Therefore, the wired network location of a RAP might play host to the RAP of multiple cells, as shown in Figure 31.

Figure 31 PoP with Multiple RAPs



When the basic cell composition is settled, the cell can be replicated to cover a greater area. When replicating the cells, a decision needs to be made whether to use the same backhaul channel on all cells or to change backhaul channels with each cell. In the example shown in Figure 32, various backhaul channels (B2, C2, and D2) per cell have been chosen to reduce the co-channel interference between cells.

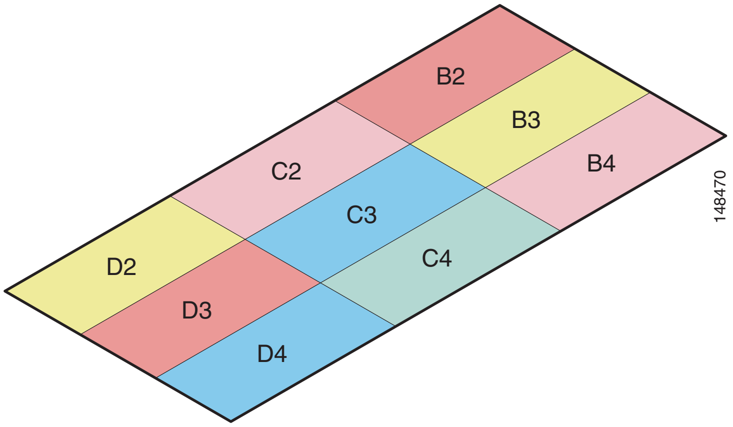
Figure 32 Multiple RAP and MAP Cells



Choosing various channels reduces the co-channel interference at the cell boundaries, at the expense of faster mesh convergence, because MAPs must fall back to seek mode to find neighbors in adjacent cells. In areas of high-traffic density, co-channel interference has the highest impact, and this is likely to be around the RAP. If RAPs are clustered in one location, a different channel strategy is likely to give optimal performance; if RAPs are dispersed among the cells, using the same channel is less likely to degrade performance.

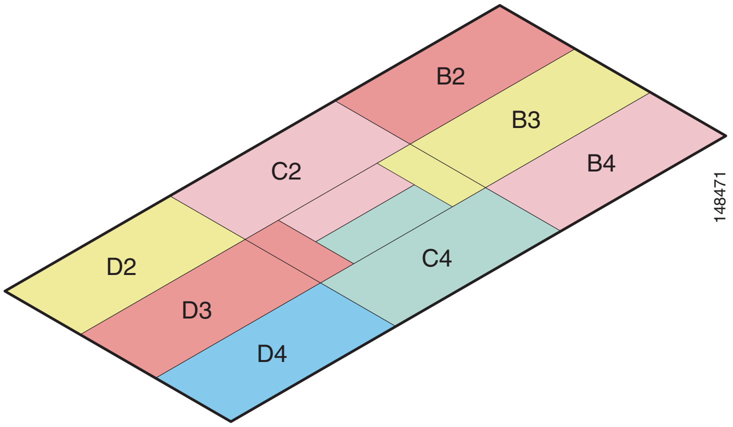
When you lay out multiple cells, use channel planning similar to standard WLAN planning to avoid overlapping channels, as shown in Figure 33.

Figure 33 Laying out Various Cells



If possible, the channel planning should also minimize channel overlap in cases where the mesh has expanded to cover the loss of a RAP connection, as shown in Figure 34.

Figure 34 Failover Coverage



Collocating Mesh Access Points

The following recommendations provide guidelines to determine the required antenna separation when you collocate AP1520s on the same tower. The recommended minimum separations for antennas, transmit powers, and channel spacing are addressed.

The goal of proper spacing and antenna selection is to provide sufficient isolation by way of antenna radiation pattern, free space path loss, and adjacent or alternate adjacent channel receiver rejection to provide independent operation of the collocated units. The goal is to have negligible throughput degradation due to a CCA hold-off, and negligible receive sensitivity degradation due to a receive noise floor increase.

Antenna proximity must be obeyed, and is dependent upon adjacent and alternate adjacent channel usage.

Collocating AP1520s on Adjacent Channels

If two collocated AP1520s operate on adjacent channels such as channel 149 (5745 MHz) and channel 152 (5765 MHz), the minimum vertical separation between the two AP1520s is 40 feet (this is true for mesh access points equipped with either 8 dBi omnidirectional or 17 dBi high-gain directional patch antennas).

If two collocated AP1520s operate on channels 1, 6, or 11 (2412 to 2437 MHz) with a 5.5-dBi omnidirectional antenna, then the minimum vertical separation is 8 feet.

Collocating AP1520s on Alternate Adjacent Channels

If two collocated AP1520s operate on alternate adjacent channels such as channel 149 (5745 MHz) and channel 157 (5785 MHz), the minimum vertical separation between the two AP1520s is 10 feet (This is true for mesh access points equipped with either 8-dBi omnidirectional or 17-dBi high-gain directional patch antennas).

If two collocated AP1520s operate on alternate adjacent channels 1 and 11 (2412 and 2462 MHz) with a 5.5-dBi omnidirectional antenna, then the minimum vertical separation is 2 feet.

In summary, a 5-GHz antenna isolation determines mesh access point spacing requirements and antenna proximity must be obeyed and is dependent upon adjacent and alternate adjacent channel usage.

Special Considerations for Indoor Mesh Networks

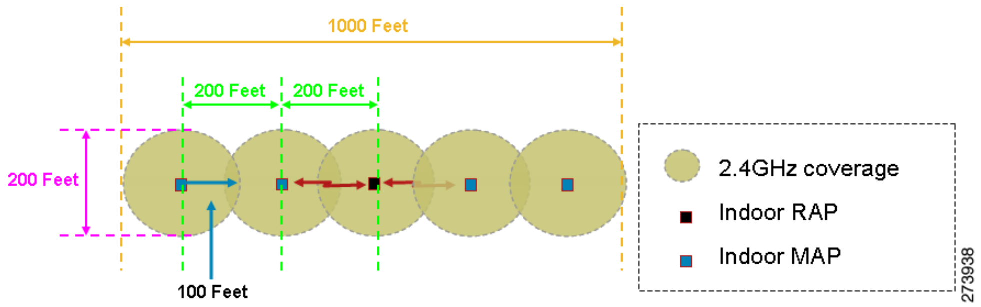
- Voice is supported only on indoor mesh networks in release 5.2, 6.0, and 7.0. For outdoors, voice is supported on a best-effort basis on a mesh infrastructure.
- Quality of Service (QoS) is supported on the local 2.4-GHz client access radio and on the 5-GHz and 4.9-GHz backhauls.
- Cisco also supports static Call Admission Control (CAC) in CCXv4 clients, which provides CAC between the access point and the client.
- RAP-to-MAP ratio—Recommended ratio is 3 to 4 MAPs per RAP.
- AP-to-AP distance—A spacing of no more than of 200 ft between each mesh access point is recommended with a cell radius of 100 ft.
- Hop count—No more than 2 hops.
- RF considerations for client access on voice networks:
  - Coverage hole of 2 to 10 percent
  - Cell coverage overlap of 15 to 20 percent
  - RSSI and SNR values that are at least 15 dB higher than data requirements

    For example, an RSSI of -67 dBm is recommended on an 11 or 12 Mbps link with an SNR of no more than 25 dB. Likewise, an RSSI of -56 dBm is recommended on a 56 Mbps link with an SNR of no more than 40 dB.
  - An RSSI of -62 dBm is recommended on a 24 Mbps 802.11a backhaul when universal access is configured and client traffic is present
  - Packet error rate (PER) configured for a value of one percent or less
  - Channel with the lowest utilization (CU) must be used.

    Check the CU when no traffic is running.
  - Radio resource manager (RRM) can be used to implement the recommended RSSI, PER, CU, cell coverage, and coverage hole settings on the 802.11b/g radio (RRM is not yet enabled on the 802.11a radio).

See Figure 35.

Figure 35 Cell Radius of 1000 Feet and Access Point Placement for Voice Mesh Networks



Note See the "Guidelines For Using Voice On The Mesh Network" section on page 132 for additional voice considerations when configuring voice on your network.

Wireless Propagation Characteristics

Table 12 provides a comparison of the 2.4-GHz and 5-GHz bands.

The 2.4-GHz band does provide better propagation characteristics than 5 GHz, but 2.4 GHz is an unlicensed band and has historically been affected with more noise and interference to date than the 5-GHz band. In addition, because there are only three backhaul channels in 2.4 GHz, co-channel interference would result. Therefore, the best method to achieve comparable capacity is by reducing system gain (that is, transmit power, antenna gain, receive sensitivity, and path loss) to create smaller cells. Keep in mind that these smaller cells require more access points per square mile (greater access point density).

Table 12 Comparison of 2.4-GHz and 5-GHz Bands

2.4-GHz Band Characteristics	5-GHz Band Characteristics
3 channels	20 channels
More prone to co-channel interference	No co-channel interference
Lower power	Higher power
Data rates less than 6 Mbps	Data rates 6 Mbps and greater (up to 54 Mbps).
Lower SNR requirements given lower data rates	Higher SNR requirements given higher data rates
Better propagation characteristics than 5 GHz but more susceptible to noise and interference	Worse propagation characteristics than 2.4 GHz but less susceptible to noise and interference
Unlicensed band. Widely available throughout the world.	Not as widely available in the world as 2.4-GHz. Licenses in some countries.

Therefore, 2.4 GHz has more penetration capability across the obstacles due to larger wavelength. In addition, 2.4 GHz has lower date rates which increases the success of the signal to reach the other end.

Wireless Mesh Mobility Groups

Mobility Group allows controllers to peer with each other to support seamless roaming across controller boundaries. APs learn the IP addresses of the other members of the mobility group after the CAPWAP Join process. A controller can be a member of a single mobility group which can contain up to 24 controllers. Mobility is supported across 72 controllers. There can be up to 72 members (WLCs) in the mobility list with up to 24 members in the same mobility group (or domain) participating in client hand-offs. The IP address of a client does not have to be renewed in the same mobility domain. Renewing the IP address is irrelevant in controller based architecture when you use this feature.

Multiple Controllers

The consideration in distance of the CAPWAP controllers from other CAPWAP controllers in the mobility group, and the distance of the CAPWAP controllers from the RAP, is similar to the consideration of an CAPWAP WLAN deployment in an enterprise.

There are operational advantages to centralizing CAPWAP controllers, and these advantages need to be traded off against the speed and capacity of the links to the CAPWAP APs and the traffic profile of the WLAN clients using these mesh access points.

If the WLAN client traffic is expected to be focused on particular sites, such as the Internet or a data center, centralizing the controllers at the same sites as these traffic focal points gives the operational advantages without sacrificing traffic efficiency.

If the WLAN client traffic is more peer-to-peer, a distributed controller model might be a better fit. It is likely that a majority of the WLAN traffic are clients in the area, with a smaller amount of traffic going to other locations. Given that many peer-to-peer applications can be sensitive to delay and packet loss, it is best to ensure that traffic between peers takes the most efficient path.

Given that most deployments see a mix of client-server traffic and peer-to peer traffic, it is likely that a hybrid model of CAPWAP controller placement is used, where points of presence (PoPs) are created with clusters of controllers placed in strategic locations in the network.

In all cases, remember that the CAPWAP model used in the wireless mesh network is designed for campus networks; that is, it expects a high-speed, low-latency network between the CAPWAP mesh access points and the CAPWAP controller.

Increasing Mesh Availability

In the “Cell Planning and Distance” section on page 47, a wireless mesh cell of one square mile was created and then built upon. This wireless mesh cell has similar properties to the cells used to create a cellular phone network because the smaller cells (rather than the defined maximum cell size) can be created to cover the same physical area, providing greater availability or capacity. This is done by adding a RAP to the cell. Similar to the larger mesh deployment, the decision is whether to use RAP on the same channel, as shown in Figure 36, or to use RAPs placed on different channels, as shown in Figure 37. The addition of RAPs into an area adds capacity and resilience to that area.

Figure 36 Two RAPs per Cell with the Same Channel

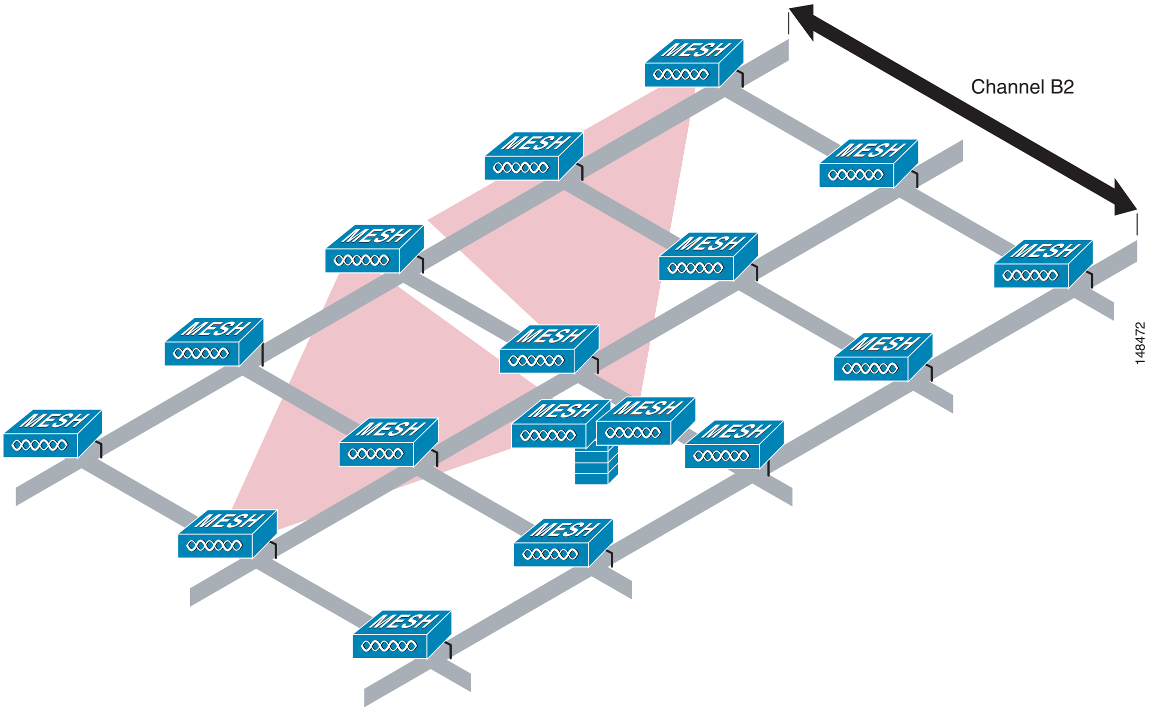
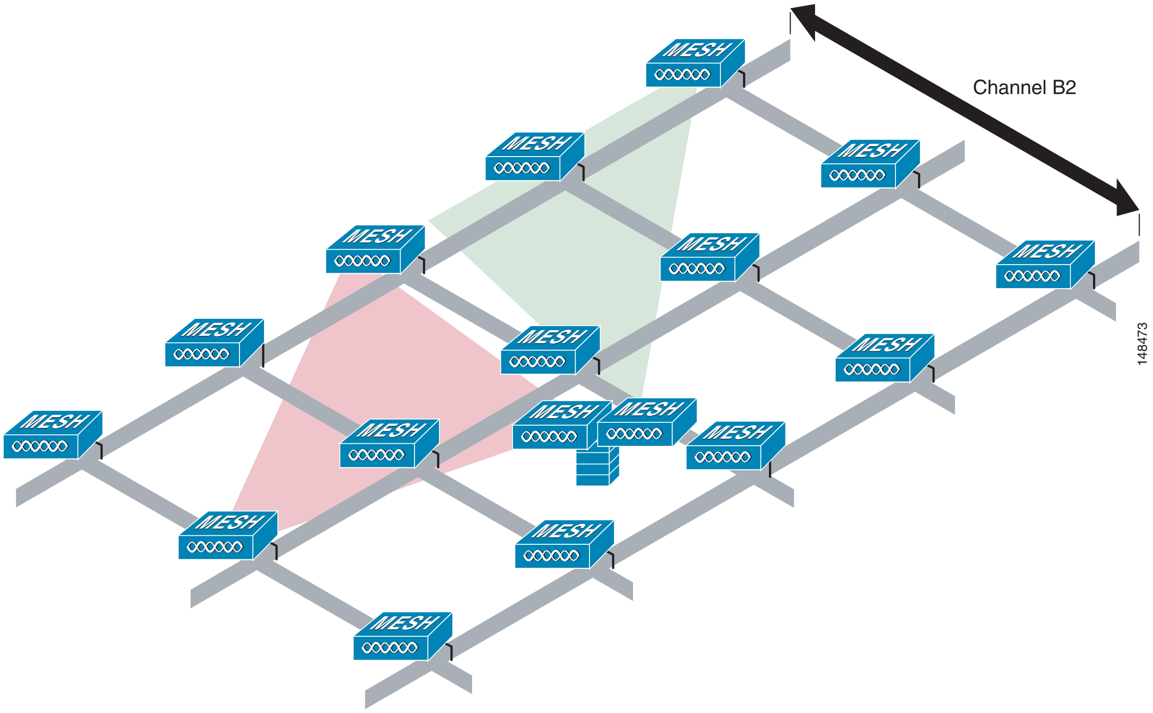


Figure 37 Two RAPs per Cell on Different Channels



Multiple RAPs

If multiple RAPs are to be deployed, the purpose for deploying these RAPs needs to be considered. If the RAPs are being deployed to provide hardware diversity, the additional RAP(s) should be deployed on the same channel as the primary RAP to minimize the convergence time in a scenario where the mesh transfers from one RAP to another. When you plan RAP hardware diversity, the 32 MAPs per RAP limitation should be remembered.

If additional RAPs are deployed to primarily provide additional capacity, then the additional RAPs should be deployed on a different channel than its neighboring RAP to minimize the interference on the backhaul channels.

Adding a second RAP on a different channel also reduces the collision domain through channel planning or through RAP cell splitting. Channel planning allocates different non-overlapping channels to mesh nodes in the same collision domain to minimize the collision probability. RAP cell splitting is a simple, yet effective, way to reduce the collision domain. Instead of deploying one RAP with omnidirectional antennas in a mesh network, two or more RAPs with directional antennas can be deployed. These RAP collocate with each other and operate on different frequency channels, thus dividing a large collision domain into several smaller ones that operate independently.

If the mesh access point bridging features are being used with multiple RAPs, these RAPs should all be on the same subnet to ensure that a consistent subnet is provided for bridge clients.

If you build your mesh with multiple RAPs on different subnets, MAP convergence times increase if a MAP has to failover to another RAP on a different subnet. One way to limit this from happening is to use different BGNs for segments in your network that are separated by subnet boundaries.

Indoor Mesh Interoperability with Outdoor Mesh

Mobility groups can be shared between outdoor mesh networks and indoor WLAN networks. It is also possible for a single controller to control indoor (1130, 1240) and outdoor mesh access points (1522, 1524) simultaneously. The same WLANs are broadcast out of both indoor and outdoor mesh access points.

⚠ **Caution** The 1200 series indoor access points in a third-party outdoor enclosure can be deployed for limited outdoor deployments, such as a simple short haul extension from an indoor WLAN to a hop in a parking lot. The 1200 access point series (1240, 1250, and 1260) in an outdoor enclosure is recommended because of its robust environmental and temperature specifications when compared to 1100 access point series. Additionally 1200 series have connectors to support articulated antennas when the AP is within an outdoor enclosure. Exercise caution with the SNR values as they may not scale and long-term fades may take away the links for these APs when compared to a more optimized outdoor 1520 series access point.

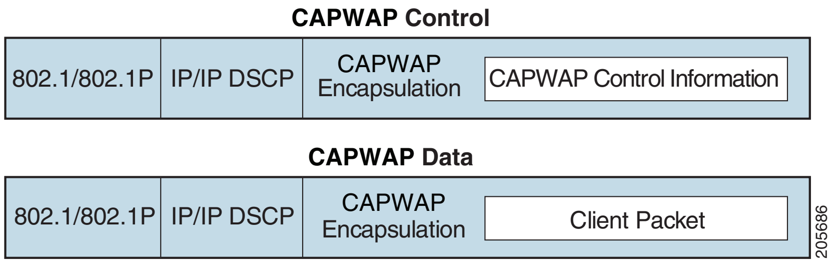
Complete interoperability of indoor mesh access points with the outdoor ones is supported to have coverage from outdoors into the indoors. We recommend 1100 series for indoor use only, and under no circumstances should these access points be deployed outdoors even if they are in enclosures.

Connecting the Cisco 1520 Series Mesh Access Point to Your Network

The wireless mesh terminates on two points on the wired network. The first location is where the RAP attaches to the wired network, and where all bridged traffic connects to the wired network. The second location is where the CAPWAP controller connects to the wired network; this is where WLAN client traffic from the mesh network connects to the wired network. This is shown schematically in Figure 38. The WLAN client traffic from CAPWAP is tunneled at Layer 2, and matching WLANs should terminate on the same switch VLAN as where the controllers are collocated. The security and network configuration for each of the WLANs on the mesh depend on the security capabilities of the network to which the controller is connected.

Note When an HSRP configuration is in operation on a mesh network, we recommend that the In-Out multicast mode be configured. For more details on multicast configuration, see the "Enabling Multicast on the Mesh Network - Using the CLI" section on page 139.

Figure 38 Mesh Network Traffic Termination



Upgrading to the 7.0 Release

This section describes procedures to upgrade to the 7.0 release.

Mesh and Mainstream Releases on the Controller

After controller release 4.1.185.0, all mesh features were extracted from the main software base and a new mesh release software base for the controller was created. This mesh software base remained distinct from the main software base of the controller until release 5.2.

In release 5.2, features developed in the three controller mesh releases, 4.1.190.5, 4.1.191.22M, and 4.1.192.xxM, were merged with the main controller software base.

Figure 39 provides a graphical display of the parallel mesh and main software bases of the controller.

Note We have announced an end of life (EOL) for both the AP1505 and AP1510 mesh access points. The last sale date was November 30, 2008. You are encouraged to migrate your networks to AP1520s.

Note Also with the 7.0 release, a new mesh access point AP1523CV has been introduced. You can order AP1523CV, which has the same hardware as AP1524SB, except that it has a built-in cable modem, similar to the AP1522PC-X-K9 model. AP1522 and AP1523CV can be configured with a cable modem. The AP1524SB and AP1524PS models are not available with cable modem.

AP1523CV is available only in the -A domain with the 7.0 release.

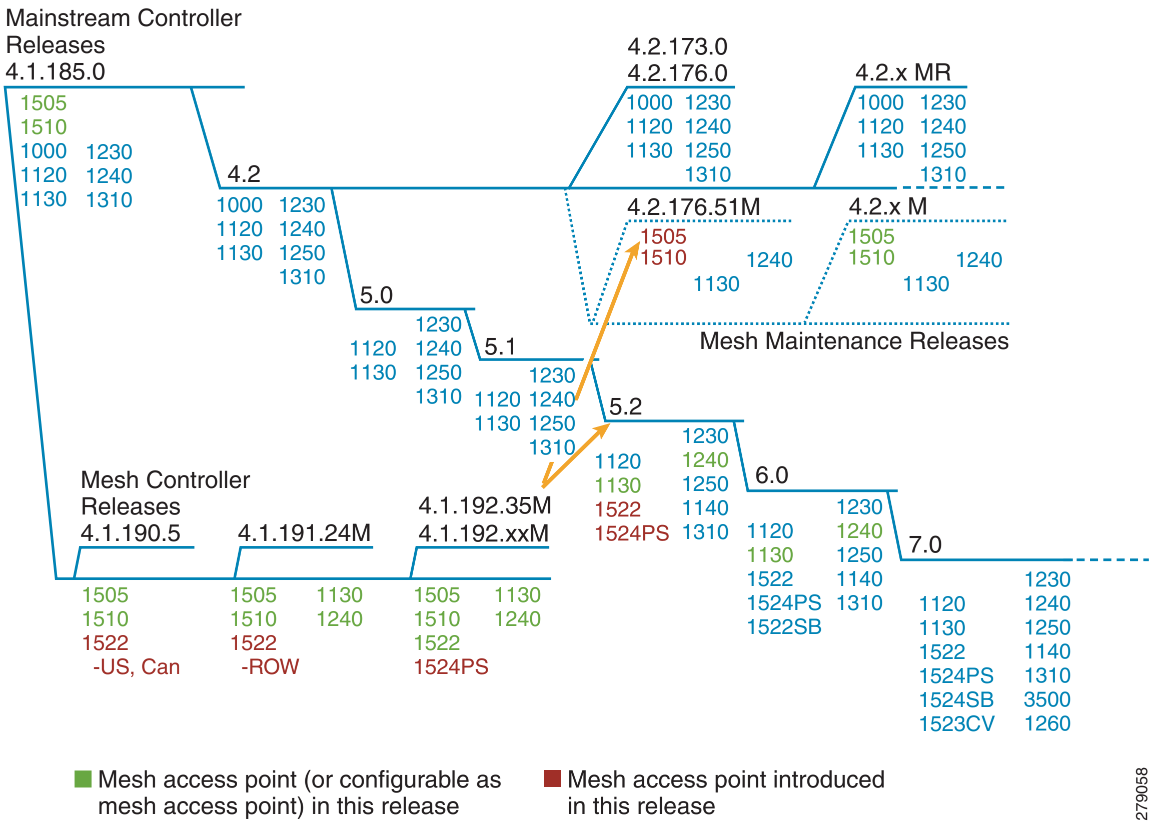
In this document, all the functionality described for AP1524SB is also applicable to AP1523CV.

Note Releases 5.2 and later do not support AP1505 and AP1510. However, the controller mesh maintenance release for 4.2.176.51M and later releases provides continued support for AP1505 and AP1510. No releases beyond 4.2.xM support AP1505 and AP1510 because these products have been discontinued.

If you are using the mesh release, 4.1.192.xxM, we recommend that you upgrade to release 5.2 before upgrading to release 7.0. Upgrading directly to the intermediate release 5.2 from either 4.1.190.05 or 4.1.191.22M is not supported.

Caution We recommend that you save the configuration from the latest mesh release (4.1.192.xxM) before upgrading to controller release 5.2. You can then reapply the configuration if you need to downgrade.

Figure 39 Mesh and Mainstream Controller Software Releases



Software Upgrade Procedure

When you upgrade the controller's software, the software on the controller's associated mesh access points is also automatically upgraded. When a mesh access point is loading software, each of its LED blinks in succession.

Caution Do not power down the controller or any mesh access point during this process; otherwise, the software image may become corrupted. Upgrading a controller with a large number of mesh access points can take around 30 minutes, depending on the size of your network. The mesh access points must remain powered on, and the controller must not be reset during this time.

Caution Controller software release 7.0 is greater than 32 MB; therefore, you must verify that your TFTP server supports files of this size. Two TFTP servers that support files of this size are *tftpd* and the TFTP server within Cisco WCS. If you download the software and your TFTP server does not support files of size greater than 32 MB, then a *TFTP failure while storing in flash* error message appears.

Caution Upgrade to release 5.2 from the latest 4.1.192.xxM mesh release prior to upgrading to release 7.0. Upgrading directly to release 5.2 from either 4.1.190.05 or 4.1.191.22M is not supported. For details on upgrading to the latest version of 4.1.192.xxM from an earlier mesh release, see the "Upgrade Compatibility Matrix" section in the *Release Notes for Cisco Wireless LAN Controllers and Mesh Access Points for Release 4.1.192.35M (or later)* at http://www.cisco.com/en/US/products/ps6366/prod_release_notes_list.html

Note When upgrading to an intermediate software release as part of the 4.1.192.xxM to release 5.2 and then to release 7.0 controller software upgrade, ensure that all mesh access points associated with the controller are at the same intermediate release before preceding to install the next intermediate or final version of software. In large networks, it can take some time to download the software on each mesh access point.

Note If you are upgrading from mesh release 4.1.191.22M to the latest 4.1.192.xxM before upgrading to the release 5.2 (prior to upgrading to release 6.0), you must manually reset the controller immediately after the upgrade without saving the configuration. Ensure to check the RRM configurations after the upgrade to see if all match your earlier configurations.

Caution A backup of your controller configuration file is recommended prior to any software upgrade. Without this backup, you will need to manually reconfigure the controller should the configuration file be lost or corrupted or if you need to downgrade.

To upgrade the mesh controller software using the controller GUI, follow these steps:

Step 1 Upload your controller configuration files to a backup server.

Step 2 Follow these steps to obtain the mesh controller software and the associated boot images from the Software Center on Cisco.com:

- **a.** Click this URL to go to the Software Center:

  http://www.cisco.com/cisco/software/navigator.html
- **b.** Click **Wireless Software**.
- **c.** Click Wireless LAN Controllers.
- **d.** Click **Standalone Controllers**, **Wireless Integrated Routers**, or **Wireless Integrated Switches.**
- **e.** Click the controller product name.
- **f.** Click **Wireless LAN Controller Software**.
- **g.** Click a controller software release.

Note Verify that the software release is 6.0.

- **h.** Click the filename (*filename*.aes).
- **i.** Click **Download**.
- **j.** Read Cisco's End User Software License Agreement and then click **Agree**.
- **k.** Save the file to your hard drive.

Step 3 Copy the controller software file (*filename*.aes) and the boot image to the default directory on your TFTP server.

Step 4 Choose **Commands** > **Download File** to open the Download File to Controller page.

Step 5 From the File Type drop-down list, choose **Code**.

Step 6 In the IP Address field, specify the IP address of the TFTP server.

Step 7 The default values of 10 retries and 6 seconds for the Maximum Retries and Timeout fields should work without any adjustment. However, you can change these values. To do so, specify the maximum number of times that the TFTP server attempts to download the software in the Maximum Retries field and the amount of time (in seconds) that the TFTP server attempts to download the software in the Timeout field.

Step 8 In the File Path field, specify the directory path of the controller software.

Step 9 In the File Name field, specify the name of the software file (*filename*.aes).

Step 10 Click **Download** to download the software to the controller. A message appears indicating the status of the download.

Step 11 Disable any WLANs on the controller.

Step 12 After the download is complete, click **Reboot**.

Step 13 If prompted to save your changes, click **Save and Reboot**.

Step 14 Click **OK** to confirm your decision to reboot the controller.

Step 15 After the controller reboots, re-enable the WLAN.

Step 16 If desired, reload your latest configuration file to the controller.

Step 17 To verify that the release 6.0 controller software is installed on your controller, click **Monitor** on the controller GUI and look at the Software Version field under Controller Summary.

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.

Note Controller ports that the mesh access points connect to should be untagged.

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

1. Add the MAC address of the mesh access point to the controller's MAC filter. See the "Adding MAC Addresses of Mesh Access Points to MAC Filter" section on page 63.
2. Define the role (RAP or MAP) for the mesh access point. See the "Defining Mesh Access Point Role" section on page 65.
3. Verify that Layer 3 is configured on the controller. See the "Verifying Layer 3 Configuration" section on page 66.
4. Configure a primary, secondary, and tertiary controller for each mesh access point. See the "Configuring Multiple Controllers Using DHCP 43 and DHCP 60" section on page 67.
   a. Configure a backup controller. See the "Configuring Backup Controllers" procedure on page 67.
5. 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 73.
6. Configure global mesh parameters. See the "Configuring Global Mesh Parameters" section on page 76.
7. Configure local mesh parameters. See the "Configuring Local Mesh Parameters" section on page 82.
8. Configure antenna parameters. See the "Configuring Antenna Gain" section on page 92.
9. Configure channels for serial backhaul. This is applicable only to serial backhaul access points. See the "Backhaul Channel Deselection on Serial Backhaul Access Point" section on page 94.
10. Configure the DCA channels for the mesh access points. See the "Configuring Dynamic Channel Assignment" section on page 99 for details.
11. Configure universal client access. See the "Universal Client Access on Serial Backhaul Access Points" section on page 102.
12. Configure mobility groups (if desired) and assign controllers. See Chapter 12, "Configuring Mobility Groups" in the *Cisco Wireless LAN Controller Configuration Guide, Release 5.2* at:

    http://www.cisco.com/en/US/products/ps6366/products_installation_and_configuration_guides_list.html
13. Configure Ethernet bridging (if desired). See the "Configuring Ethernet Bridging" section on page 82.
14. Configure advanced features such as Ethernet VLAN tagging network, video, and voice. See the "Configuring Advanced Features" section on page 106.

Adding MAC Addresses of Mesh Access Points to MAC Filter

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 addresses need to be configured. If the access point has an SSC and has been added to the AP Authorization List, then the MAC address of the AP need not be added to the MAC Filtering List.

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

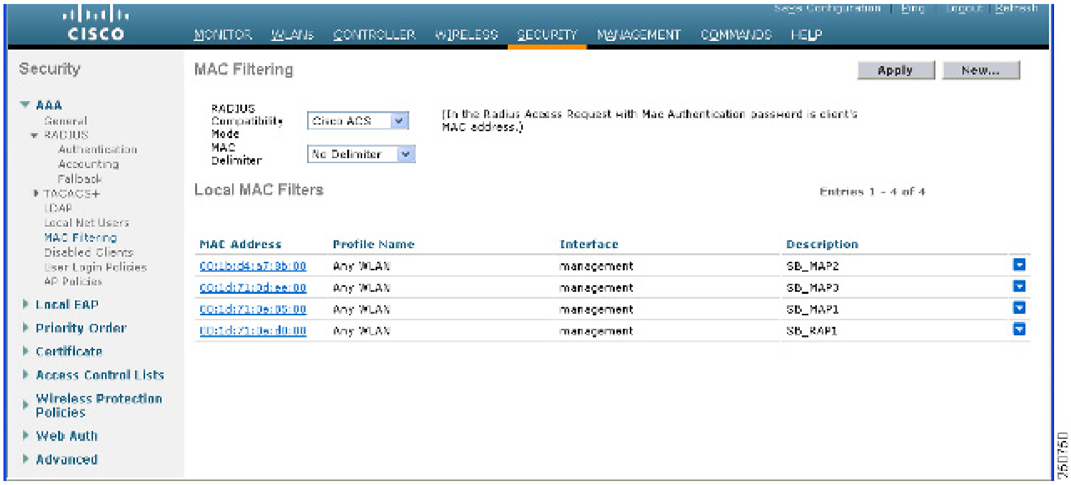
Note You can also download the list of mesh access point MAC addresses and push them to the controller using Cisco WCS. See the *Cisco Wireless Control System Configuration Guide, Release 7.0*: http://www.cisco.com/en/US/docs/wireless/wcs/7.0/configuration/guide/WCS70cg.html

Adding the MAC Address of the Mesh Access Point to the Controller Filter List - Using the GUI

To add a MAC filter entry for the mesh access point on the controller using the controller GUI, follow these steps.

Step 1 Choose **Security** > **AAA** > **MAC Filtering**. The MAC Filtering page appears (see Figure 40).

Figure 40 MAC Filtering Page



MAC Filtering

RADIUS Compatibility Mode: Cisco ACS (In the Radius Access Request with Mac Authentication password is client's MAC address.)

MAC Delimiter: No Delimiter

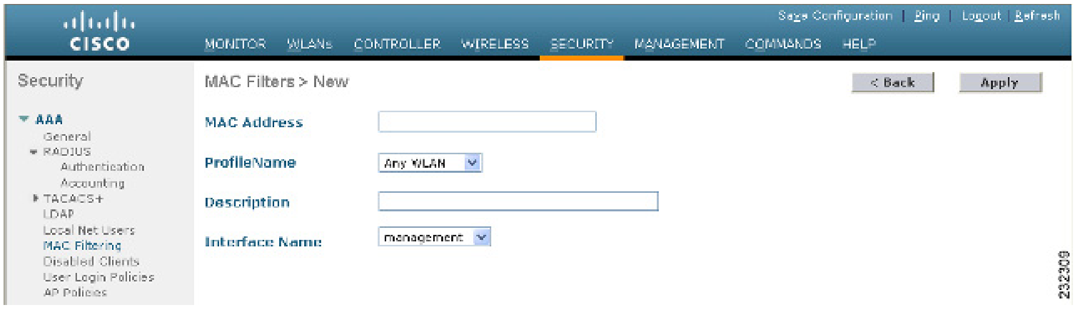
Local MAC Filters

Entries 1 - 4 of 4

MAC Address	Profile Name	Interface	Description
00:1b:d4:a7:8b:00	Any WLAN	management	SB_MAP2
00:1d:71:0d:ee:00	Any WLAN	management	SB_MAP3
00:1d:71:0e:05:00	Any WLAN	management	SB_MAP1
00:1d:71:0e:d0:00	Any WLAN	management	SB_RAP1

Step 2 Click **New**. The MAC Filters > New page appears (see Figure 41).

Figure 41 MAC Filters > New Page



MAC Filters > New

MAC Address

Profile Name: Any WLAN

Description

Interface Name: management

Step 3 Enter the MAC address of the mesh access point.

Note For 1522, 1524PS, and serial backhaul outdoor mesh access points, specify 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. If the required MAC address does not appear on the exterior of the mesh access point, enter the following command at the access point console to display the BVI and Ethernet MAC addresses: *sh int | i Hardware*.

Step 4 From the Profile Name drop-down list, select **Any WLAN**.

Step 5 In the Description field, specify a description of the mesh 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 r*oof top*, *pole top*, or its cross streets.

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

Step 7 Click **Apply** to commit your changes. The mesh 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 mesh access points to the list.

Adding the MAC Address of the Mesh Access Point to the Controller Filter List - Using the CLI

To add a MAC filter entry for the mesh access point on the controller using the controller CLI, follow these steps:

Step 1 To add the MAC address of the mesh 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

Defining Mesh Access Point Role

By default, AP1520s are shipped with a radio role set to MAP. You must reconfigure a mesh access point to act as a RAP.

General Notes about MAP and RAP Association With The Controller

The general notes are as follows:

- A MAP always sets the Ethernet port as the *primary backhaul* if it is UP, and secondarily the 802.11a radio. This gives the network administrator time to reconfigure the mesh access point as a RAP, initially. For faster convergence on the network, we recommend that you do not connect any Ethernet device to the MAP until it has joined the mesh network.
- A MAP that fails to connect to a controller on a UP Ethernet port, sets the 802.11a radio as the primary backhaul. If a MAP fails to find a neighbor or fails to connect to a controller through a neighbor, the Ethernet port is set as the primary backhaul again.
- A MAP connected to a controller over an Ethernet port does not build a mesh topology (unlike a RAP).
- A RAP always sets the Ethernet port as the primary backhaul.
- If the Ethernet port is DOWN on a RAP, or a RAP fails to connect to a controller on a UP Ethernet port, the 802.11a radio is set as the primary backhaul for 15 minutes. Failing to find a neighbor or failing to connect to a controller via any neighbor on the 802.11a radio causes the primary backhaul to go into the *scan* state. The primary backhaul begins its scan with the Ethernet port.

Configuring the AP Role - Using the GUI

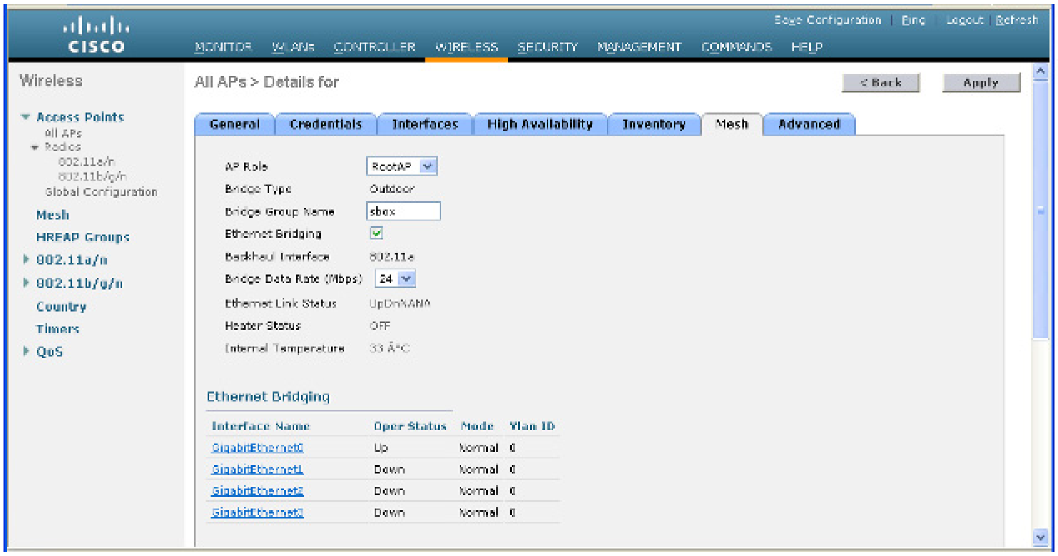
To configure the role of a mesh access point using the GUI, follow these steps:

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 (see Figure 42).

Figure 42 All APs > Details for (Mesh) Page



All APs > Details for

AP Role: RootAP
Bridge Type: Outdoor
Bridge Group Name: sbox
Ethernet Bridging: ☑
Backhaul Interface: 802.11a
Bridge Data Rate (Mbps): 24
Ethernet Link Status: UpDnNANA
Heater Status: OFF
Internal Temperature: 33 Â°C

Ethernet Bridging

Interface Name	Oper Status	Mode	Vlan ID
GigabitEthernet0	Up	Normal	0
GigabitEthernet1	Down	Normal	0
GigabitEthernet2	Down	Normal	0
GigabitEthernet3	Down	Normal	0

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

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

Configuring the AP Role - Using the CLI

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

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

Verifying Layer 3 Configuration

Verify that the initial controller that the mesh access point is to associate with is at Layer 3.

To verify that the controller is configured for Layer 3, follow these steps:

Step 1 Open your web-browser and enter the IP address of your controller. Be sure to precede the IP address with *https://*. A login page appears.

Step 2 Specify your username and password.

The default case-sensitive username and password are *admin* and *admin*. The summary page appears.

Step 3 From the top menu bar, click **Controller**. The controller general page appears.

Step 4 Verify that the LWAPP Transport Modes is set to Layer 3. If it is not, change it to Layer 3 and click **Apply**.

Step 5 Save the changes, if any.

Step 6 From the menu bar, click **Monitor** to return to the Monitor summary page.

Step 7 See the "Configuring Multiple Controllers Using DHCP 43 and DHCP 60" section on page 67 to assign a primary, secondary, and tertiary controller.

Configuring Multiple Controllers Using DHCP 43 and DHCP 60

To configure DHCP Option 43 and 60 for mesh access points in the embedded Cisco IOS DHCP server, follow these steps:

Step 1 Enter configuration mode at the Cisco IOS CLI.

Step 2 Create the DHCP pool, including the necessary parameters such as the default router and name server. The commands used to create a DHCP pool are as follows:

```
ip dhcp pool pool name
network IP Network Netmask
default-router Default router
dns-server DNS Server
```

where:

```
pool name is the name of the DHCP pool, such as AP1520
IP Network is the network IP address where the controller resides, such as 10.0.15.1
Netmask is the subnet mask, such as 255.255.255.0
Default router is the IP address of the default router, such as 10.0.0.1
DNS Server is the IP address of the DNS server, such as 10.0.10.2
```

Step 3 Add the option 60 line using the following syntax:

```
option 60 ascii "VCI string"
For the VCI string, use one of the values below. The quotation marks must be included.
    For Cisco 1520 series access points, enter "Cisco AP c1520"
    For Cisco 1240 series access points, enter "Cisco AP c1240"
    For Cisco 1130 series access points, enter "Cisco AP c1130"
```

Step 4 Add the option 43 line using the following syntax:

```
option 43 hex hex string
```

The hex string is assembled by concatenating the TLV values shown below:

Type + *Length* + *Value*

Type is always f1(hex). *Length* is the number of controller management IP addresses times 4 in hex. *Value* is the IP address of the controller listed sequentially in hex.

For example, suppose that there are two controllers with management interface IP addresses, 10.126.126.2 and 10.127.127.2. The type is *f1(hex)*. The length is *2 * 4 = 8 = 08 (hex)*. The IP addresses translate to *0a7e7e02* and *0a7f7f02*. Assembling the string then yields *f1080a7e7e020a7f7f02*.

The resulting Cisco IOS command added to the DHCP scope is listed below:

```
option 43 hex f1080a7e7e020a7f7f02
```

Configuring Backup Controllers

A single controller at a centralized location can act as a backup for mesh access points when they lose connectivity with the primary controller in the local region. Centralized and regional controllers need not be in the same mobility group. Using the controller GUI or CLI, you can specify the IP addresses of the backup controllers, which allows the mesh access points to fail over to controllers outside of the mobility group.

You can also configure primary and secondary backup controllers (which are used if primary, secondary, or tertiary controllers are not specified or are not responsive) for all access points connected to the controller as well as various timers, including the heartbeat timer and discovery request timers.

Note The fast heartbeat timer is not supported on mesh access points. The fast heartbeat timer is only configured on access points in local and hybrid-REAP modes.

The mesh access point maintains a list of backup controllers and periodically sends primary discovery requests to each entry on the list. When the mesh access point receives a new discovery response from a controller, the backup controller list is updated. Any controller that fails to respond to two consecutive primary discovery requests is removed from the list. If the mesh access point's local controller fails, it chooses an available controller from the backup controller list in this order: primary, secondary, tertiary, primary backup, secondary backup. The mesh access point waits for a discovery response from the first available controller in the backup list and joins the controller if it receives a response within the time configured for the primary discovery request timer. If the time limit is reached, the mesh access point assumes that the controller cannot be joined and waits for a discovery response from the next available controller in the list.

Note When a mesh access point's primary controller comes back online, the mesh access point disassociates from the backup controller and reconnects to its primary controller. The mesh access point falls back to its primary controller and not to any secondary controller for which it is configured. For example, if a mesh access point is configured with primary, secondary, and tertiary controllers, it fails over to the tertiary controller when the primary and secondary controllers become unresponsive and waits for the primary controller to come back online so that it can fall back to the primary controller. The mesh access point does not fall back from the tertiary controller to the secondary controller if the secondary controller comes back online; it stays connected to the tertiary controller until the primary controller comes back up.

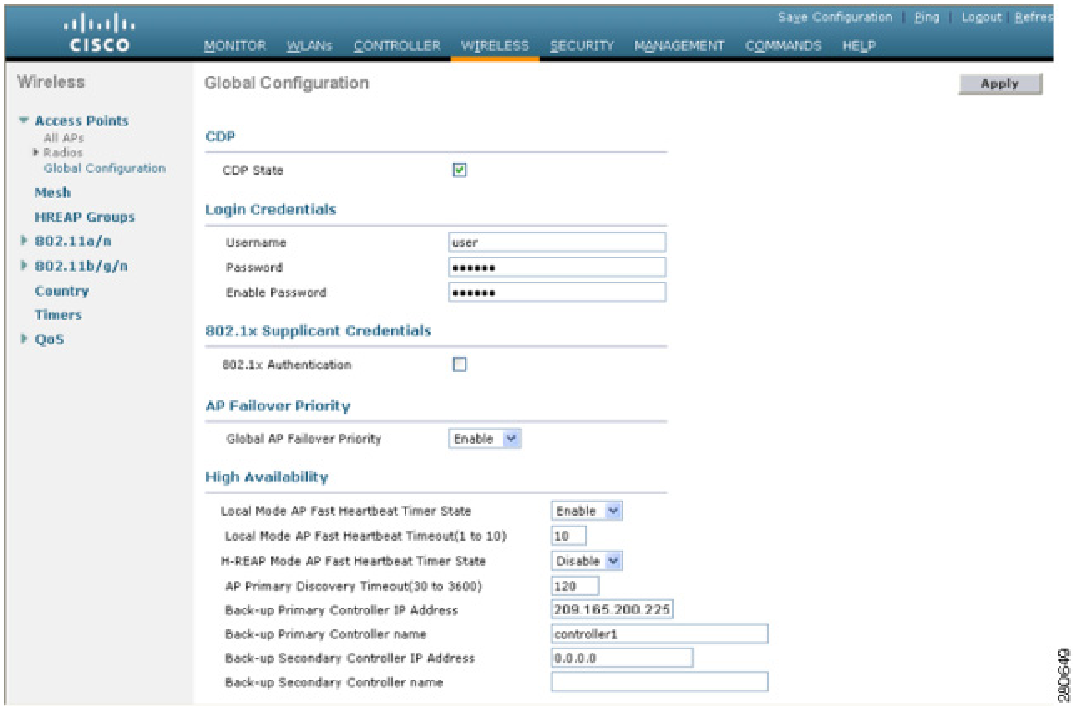
Note If you inadvertently configure a controller that is running software release 6.0 with a failover controller that is running a different software release (such as 4.2, 5.0, 5.1, or 5.2), the mesh access point might take a long time to join the failover controller because the mesh access point starts the discovery process in LWAPP and then changes to CAPWAP discovery.

Configuring Backup Controllers - Using the GUI

Using the controller GUI, follow these steps to configure primary, secondary, and tertiary controllers for a specific mesh access point and to configure primary and secondary backup controllers for all mesh access points.

Step 1 Choose **Wireless** > **Access Points** > **Global Configuration** to open the Global Configuration page. (See Figure 43.)

Figure 43 Global Configuration Page



Global Configuration

CDP

CDP State ☑

Login Credentials

Username	user
Password	••••••
Enable Password	••••••

802.1x Supplicant Credentials

802.1x Authentication □

AP Failover Priority

Global AP Failover Priority	Enable

High Availability

Local Mode AP Fast Heartbeat Timer State	Enable
Local Mode AP Fast Heartbeat Timeout(1 to 10)	10
H-REAP Mode AP Fast Heartbeat Timer State	Disable
AP Primary Discovery Timeout(30 to 3600)	120
Back-up Primary Controller IP Address	209.165.200.225
Back-up Primary Controller name	controller1
Back-up Secondary Controller IP Address	0.0.0.0
Back-up Secondary Controller name	

Note The fast heartbeat timer is not supported on mesh access points.

Step 2 In the AP Primary Discovery Timeout field, enter a value between 30 and 3600 seconds (inclusive) to configure the access point primary discovery request timer. The default value is 120 seconds.

Step 3 If you want to specify a primary backup controller for all access points, specify the IP address of the primary backup controller in the Back-up Primary Controller IP Address field and the name of the controller in the Back-up Primary Controller Name field.

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

Step 4 If you want to specify a secondary backup controller for all access points, specify the IP address of the secondary backup controller in the Back-up Secondary Controller IP Address field and the name of the controller in the Back-up Secondary Controller Name field.

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

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

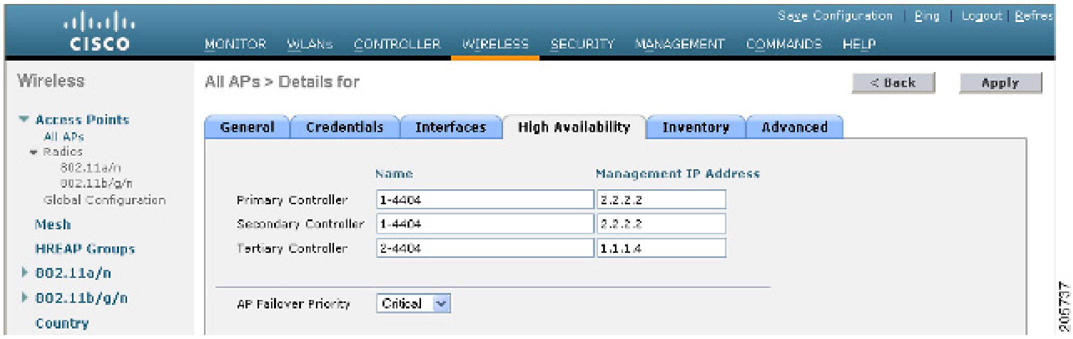
Step 6 If you want to configure primary, secondary, and tertiary backup controllers for a specific point, follow these steps:

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

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

c. Click the **High Availability** tab. (See Figure 44.)

Figure 44 All APs > Details for (High Availability) Page



	Name	Management IP Address
Primary Controller	1-4404	2.2.2.2
Secondary Controller	1-4404	2.2.2.2
Tertiary Controller	2-4404	1.1.1.4

AP Failover Priority: Critical

d. If desired, specify the name and IP address of the primary backup controller for this access point in the Primary Controller fields.

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

e. If desired, specify the name and IP address of the secondary backup controller for this mesh access point in the Secondary Controller fields.

f. If desired, specify the name and IP address of the tertiary backup controller for this mesh access point in the Tertiary Controller fields.

g. No change is required to the AP Failover Priority value. The default value for mesh access points is *critical* and it cannot be modified.

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

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

Configuring Backup Controllers - Using the CLI

Using the controller CLI, follow these steps to configure primary, secondary, and tertiary controllers for a specific mesh access point and to configure primary and secondary backup controllers for all mesh access points.

Step 1 To configure a primary controller for a specific mesh access point, enter this command:

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

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

Step 2 To configure a secondary controller for a specific mesh access point, enter this command:

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

Step 3 To configure a tertiary controller for a specific mesh access point, enter this command:

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

Step 4 To configure a primary backup controller for all mesh access points, enter this command:

config advanced backup-controller primary *backup_controller_name backup_controller_ip_address*

Step 5 To configure a secondary backup controller for all mesh access points, enter this command:

config advanced backup-controller secondary *backup_controller_name backup_controller_ip_address*

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

Step 6 To configure the mesh access point primary discovery request timer, enter this command:

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

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

Step 7 To configure the mesh access point discovery timer, enter this command:

config advanced timers ap-discovery-timeout *interval*

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

Step 8 To configure the 802.11 authentication response timer, enter this command:

config advanced timers auth-timeout *interval*

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

Step 9 To save your changes, enter this command:

save config

Step 10 To view a mesh access point's configuration, enter these commands:

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

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

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

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

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

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

```
Authentication Response Timeout (seconds)........ 10
Rogue Entry Timeout (seconds).................... 1300
AP Heart Beat Timeout (seconds).................. 30
AP Discovery Timeout (seconds)................... 10
AP Primary Discovery Timeout (seconds)........... 120
```

Information similar to the following appears for the **show mesh config** command:

```
Mesh Range....................................... 12000
Backhaul with client access status............... disabled
Background Scanning State........................ enabled
Mesh Security
Security Mode................................. EAP
External-Auth................................. disabled
Use MAC Filter in External AAA server......... disabled
Force External Authentication................. disabled
Mesh Alarm Criteria
Max Hop Count................................. 4
Recommended Max Children for MAP.............. 10
Recommended Max Children for RAP.............. 20
Low Link SNR.................................. 12
High Link SNR................................. 60
Max Association Number........................ 10
Association Interval.......................... 60 minutes
Parent Change Numbers......................... 3
Parent Change Interval........................ 60 minutes
Mesh Multicast Mode.............................. In-Out
Mesh Full Sector DFS............................. enabled
Mesh Ethernet Bridging VLAN Transparent Mode..... enabled
```

Configuring External Authentication and Authorization Using a RADIUS Server

External authorization and authentication of mesh access points using a RADIUS server such as Cisco ACS (4.1 and later) is supported in release 5.2 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, ensure that you make these changes:

- 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.
- Add the mesh access point configured for external authorization and authentication to the user list of the RADIUS server.
  - For additional details, see the "Adding a Username to a RADIUS Server" section on page 74.
- 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 about installing and trusting the CA certificates, see the "Configuring RADIUS Servers" section on page 73.

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

To install and trust the CA certificates on the RADIUS server, follow these steps:

Step 1 Download the CA certificates for Cisco Root CA 2048 from the following locations:

- 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 **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. Select 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, see the following:

- http://www.cisco.com/en/US/products/sw/secursw/ps2086/products_installation_and_configuration_guides_list.html (Windows)
- http://www.cisco.com/en/US/products/sw/secursw/ps4911/
(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 Cisco 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 Cisco 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.

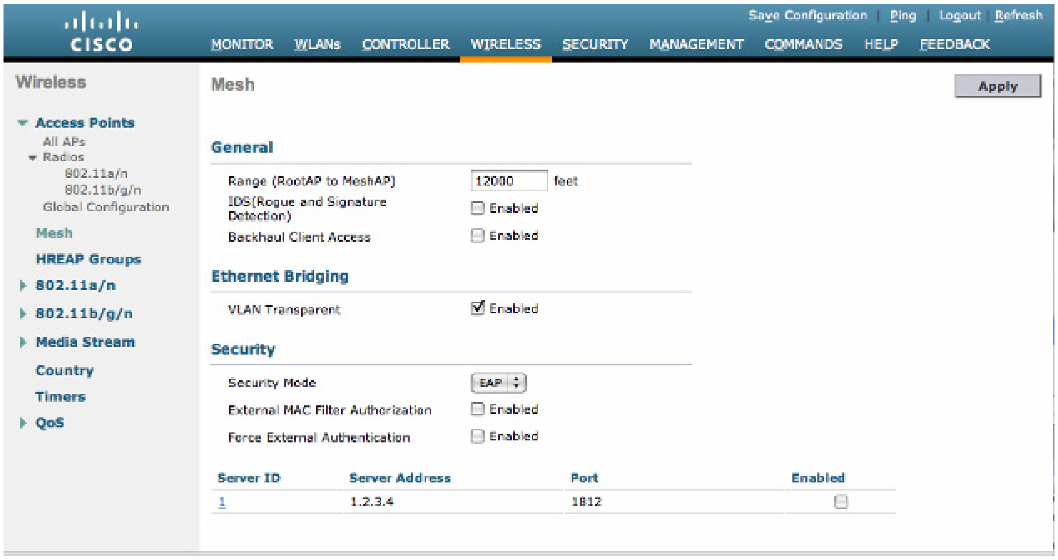
Note The password must match the username (for example, *c1520-001122334455).*

Enabling External Authentication of Mesh Access Points - Using the GUI

To enable external authentication for a mesh access point using the GUI, follow these steps:

Step 1 Choose **Wireless > Mesh**. The Mesh page appears (see Figure 45).

Figure 45 Mesh Page



Mesh

General

Range (RootAP to MeshAP) 12000 feet

IDS(Rogue and Signature Detection) □ Enabled

Backhaul Client Access □ Enabled

Ethernet Bridging

VLAN Transparent ☑ Enabled

Security

Security Mode EAP

External MAC Filter Authorization □ Enabled

Force External Authentication □ Enabled

Server ID	Server Address	Port	Enabled
1	1.2.3.4	1812	□

Step 2 In the security section, select the **EAP** option from the Security Mode drop-down list.

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

Step 4 Click **Apply**.

Step 5 Click **Save Configuration**.

Enable External Authentication of Mesh Access Points - Using the CLI

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

1. **config mesh security eap**
2. **config macfilter mac-delimiter colon**
3. **config mesh security rad-mac-filter enable**
4. **config mesh radius-server** ***index*** **enable**
5. **config mesh security force-ext-auth enable** (Optional)

View Security Statistics - Using the CLI

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

show mesh security-stats *Cisco_AP*

Use this command to display 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 Global Mesh Parameters

This section provides instructions to configure the mesh access point to establish a connection with the controller including:

- Setting the maximum range between RAP and MAP (not applicable to AP1130 and AP1240).
- Enabling a backhaul to carry client traffic.
- Defining if 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).

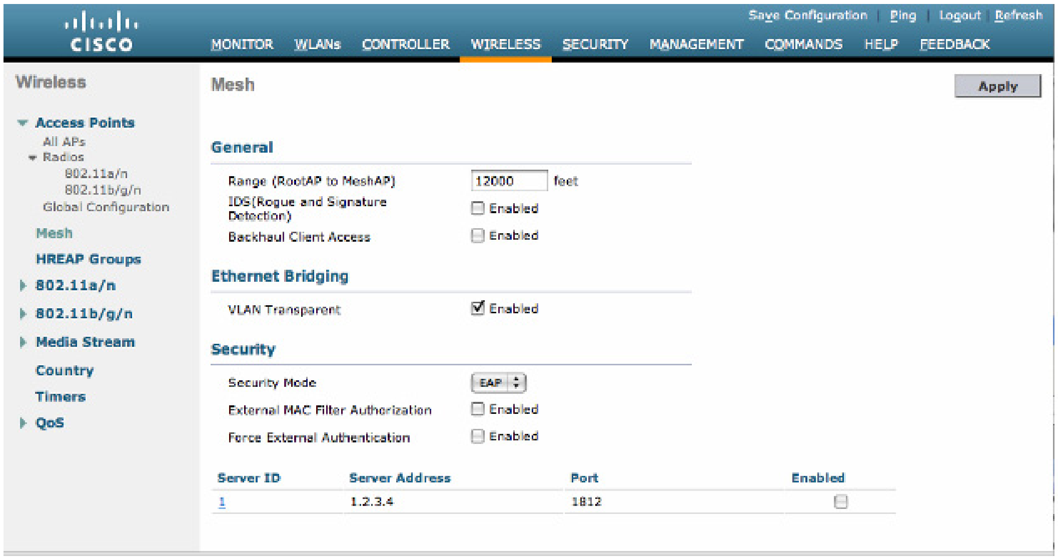
You can configure the necessary mesh parameters using either the GUI or the CLI. All parameters are applied globally.

Configuring Global Mesh Parameters - Using the GUI

To configure global mesh parameters using the controller GUI, follow these steps:

Step 1 Choose **Wireless** > **Mesh** (see Figure 46).

Figure 46 Mesh Page



Mesh

General

Range (RootAP to MeshAP) 12000 feet

IDS(Rogue and Signature Detection) □ Enabled

Backhaul Client Access □ Enabled

Ethernet Bridging

VLAN Transparent ☑ Enabled

Security

Security Mode EAP

External MAC Filter Authorization □ Enabled

Force External Authentication □ Enabled

Server ID	Server Address	Port	Enabled
1	1.2.3.4	1812	□

Step 2 Modify the mesh parameters as appropriate. Table 13 describes each parameter.

Table 13 Global Mesh Parameters

Parameter	Description
Range (RootAP to MeshAP)	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 mesh access points when they join the controller and all existing mesh access points in the network. **Range:** 150 to 132,000 feet **Default:** 12,000 feet After this feature is enabled, all mesh access points reboot.
IDS (Rogue and Signature Detection)	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. **Note** IDS reporting is disabled by default for all outdoor mesh access points.
Backhaul Client Access	**Note** This parameter applies to mesh access points with two or more radios (1524SB, 1523CV, 1522, 1240 and 1130) *excluding* the 1524PS. When this feature is enabled, it allows wireless client association over the 802.11a radio. This implies that a 802.11a can carry both backhaul traffic and 802.11a client traffic over the same 802.11a radio. When this feature is disabled, only backhaul traffic is sent over the 802.11a radio and client association is only over the 802.11b/g radio. **Default:** Disabled **Note** After this feature is enabled, all mesh access points reboot.

Table 13 Global Mesh Parameters (continued)

Parameter	Description
VLAN Transparent	This feature determines how a mesh access point handles VLAN tags for Ethernet bridged traffic. **Note** See the "Configuring Advanced Features" section on page 106 for overview and additional configuration details. If VLAN Transparent is enabled, then VLAN tags are not handled and packets are bridged as untagged packets. **Note** No configuration of Ethernet ports is required when VLAN transparent is enabled. The Ethernet port passes both tagged and untagged frames without interpreting the frames. If VLAN Transparent is disabled, then all packets are handled according to the VLAN configuration on the port (trunk, access, or normal mode). **Note** If the Ethernet port is set to Trunk mode, then Ethernet VLAN tagging must be configured. See the "Enabling Ethernet Bridging - Using the GUI" section on page 83. **Note** For an overview of normal, access, and trunk Ethernet port use, see the "Ethernet Port Notes" section on page 107. **Note** To use VLAN tagging, you must deselect the VLAN Transparent check box. **Note** VLAN Transparent is enabled as a default to ensure a smooth software upgrade from 4.1.192.xxM releases to release 5.2. Release 4.1.192.xxM does not support VLAN tagging (see Figure 46). **Default:** 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 deselected). **Options:** PSK or EAP **Default:** EAP

Table 13 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 mesh access points that are not defined on the external server from joining. Before employing 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 Cisco IOS-based mesh access points (1130, 1240, 1522, 1524), the platform name of the mesh access point is located in front of its Ethernet address within the certificate; therefore, their username for external RADIUS servers is *platform_name_string–Ethernet MAC address* such as *c1520-001122334455*. • The certificates must be installed and EAP-FAST must be configured on the RADIUS server. **Note** When this capability is not enabled, by default, 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, external authorization and authentication of mesh access points is done by default by an external RADIUS server (such as Cisco 4.1 and later). 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.

Configuring Global Mesh Parameters - Using the CLI

To configure global mesh parameters including authentication methods using the controller CLI, follow these steps.

Note See the "Configuring Global Mesh Parameters - Using the GUI" section on page 76 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 mesh 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 Mbps) 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 a mesh 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 the 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

Viewing Global Mesh Parameter Settings - Using the CLI

Use these commands to obtain information on global mesh 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 config**–Displays global configuration settings.

```
(Cisco Controller) > show mesh config
Mesh Range....................................... 12000
Mesh Statistics update period.................... 3 minutes
Backhaul with client access status............... disabled
Background Scanning State........................ enabled
Backhaul Amsdu State............................. disabled

Mesh Security
    Security Mode................................. EAP
    External-Auth................................. disabled
    Use MAC Filter in External AAA server......... disabled
    Force External Authentication................. disabled

Mesh Alarm Criteria
    Max Hop Count................................. 4
    Recommended Max Children for MAP.............. 10
    Recommended Max Children for RAP.............. 20
    Low Link SNR.................................. 12
    High Link SNR................................. 60
    Max Association Number........................ 10
    Association Interval.......................... 60 minutes
    Parent Change Numbers......................... 3
    Parent Change Interval....................... 60 minutes

Mesh Multicast Mode............................ In-Out
Mesh Full Sector DFS........................... enabled

Mesh Ethernet Bridging VLAN Transparent Mode..... enabled
```

Configuring Local Mesh Parameters

After configuring global mesh parameters, you must configure the following local mesh parameters for these specific features if in use in your network:

- Ethernet Bridging. See the "Configuring Ethernet Bridging" section on page 82.
- Bridge Group Name. See the"Configuring Ethernet Bridging" section on page 82.
- Workgroup Bridge. See the "Configuring Workgroup Bridges" section on page 115.
- Public Safety Band Settings. See the "Configuring Public Safety Band Settings" section on page 86.
- Cisco 3200 Series Association and Interoperability. See the "Configuring Interoperability with the Cisco 3200" section on page 125.
- Power and Channel Setting. See the"Configuring Power and Channel Settings" section on page 89.
- Antenna Gain Settings. See the "Configuring Antenna Gain" section on page 92.
- Dynamic Channel Assignment. See the "Configuring Dynamic Channel Assignment" section on page 99.

Configuring Ethernet Bridging

For security reasons, the Ethernet port on all MAPs is disabled by default. It can be enabled only by configuring Ethernet bridging on the root and its respective MAP.

Note Exceptions are allowed for a few protocols even though Ethernet bridging is disabled. For example, following are some of the protocols that are allowed:

1. Spanning Tree Protocol (STP)
2. Address Resolution Protocol (ARP)
3. Control And Provisioning of Wireless Access Points (CAPWAP)
4. Bootstrap Protocol (BOOTP) packets

Due to the exceptions and to prevent loop issues, we recommend that you do not connect two MAPs to each other over their Ethernet ports, unless they are configured as Trunk ports on different Native VLANs, and each is connected to a similarly configured switch.

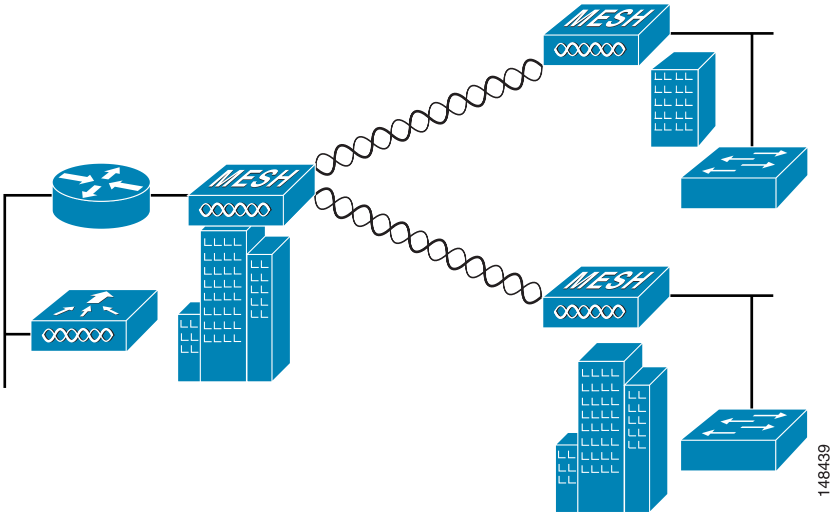
Ethernet bridging has to be enabled for two scenarios:

1. When you want to use the Mesh nodes as bridges. (See Figure 47.)

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

2. When you want to connect any Ethernet device such as a video camera on the MAP using its Ethernet port. This is the first step to enable VLAN tagging.

Figure 47 Point-to-Multipoint Bridging



Enabling Ethernet Bridging - Using the GUI

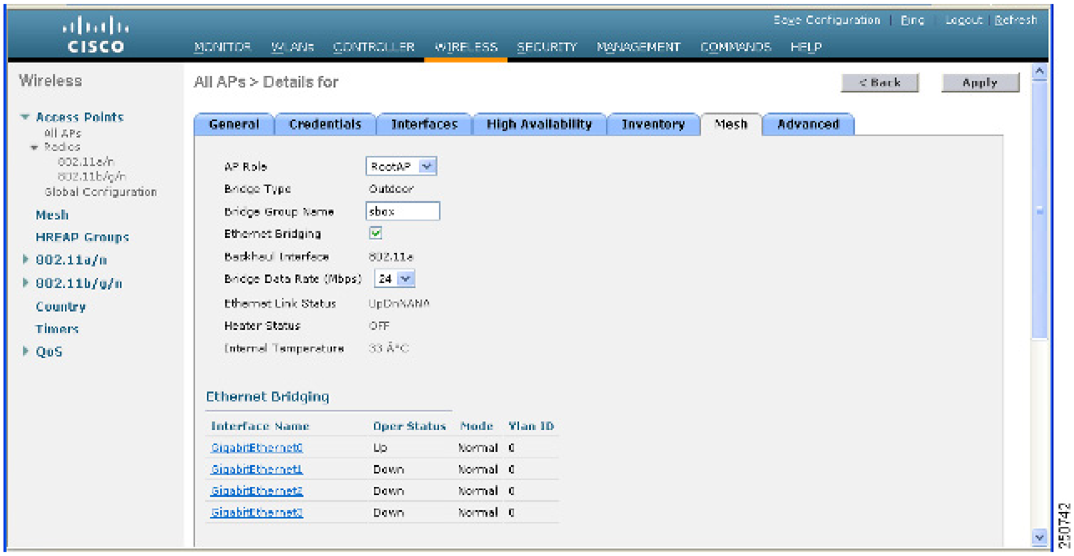
To enable Ethernet bridging on a RAP or MAP using the GUI, follow these steps:

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

Step 2 Click the AP name link of the mesh access point on which you want to enable Ethernet bridging.

Step 3 At the details page, select the **Mesh** tab. (See Figure 48.)

Figure 48 All APs > Details for (Mesh) Page



All APs > Details for

AP Role: RootAP
Bridge Type: Outdoor
Bridge Group Name: sbox
Ethernet Bridging: ☑
Backhaul Interface: 802.11a
Bridge Data Rate (Mbps): 24
Ethernet Link Status: UpDnNANA
Heater Status: OFF
Internal Temperature: 33 Â°C

Ethernet Bridging

Interface Name	Oper Status	Mode	Vlan ID
GigabitEthernet0	Up	Normal	0
GigabitEthernet1	Down	Normal	0
GigabitEthernet2	Down	Normal	0
GigabitEthernet3	Down	Normal	0

Step 4 Select either **RootAP** or **MeshAP** from the AP Role drop-down list, if not already selected.

- **MeshAP**—Select this option if the AP1520 has a wireless connection to the controller. This is the default setting.
- **RootAP**—Select this option if the AP1520 has a wired connection to the controller.

Note At least one mesh access point must be set to RootAP in the mesh network.

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

Step 6 Select the **Ethernet Bridging** check box to enable Ethernet bridging or deselect 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. We recommend setting the backhaul rate to **auto**.

When the bridge data rate is set to **auto**, the mesh backhaul chooses the highest rate possible given its link quality and the ability to sustain of that rate.

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.

Configuring Bridge Group Names

Bridge group names (BGNs) control the association of mesh access points. BGNs can logically group radios to avoid two networks on the same channel from communicating with each other. The setting is also useful if you have more than one RAP in your network in the same sector (area). BGN is a string of 10 characters maximum.

A BGN of *NULL VALUE* is assigned by default by manufacturing. Although not visible to you, it allows a mesh access point to join the network prior to your assignment of your network-specific BGN.

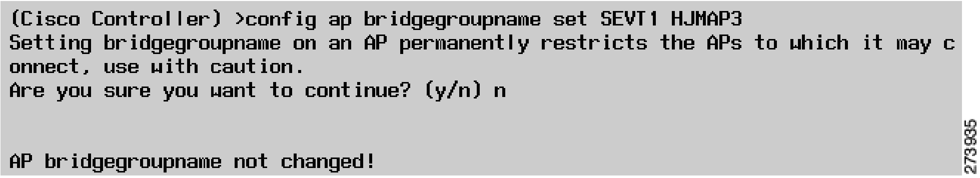
If you have two RAPs in your network in the same sector (for more capacity), we recommend that you configure the two RAPs with the same BGN, but on different channels.

Configuring BGN - Using the CLI

To configure a BGN, follow these steps:

Step 1 Using the CLI, enter the following command:

T



```
(Cisco Controller) >config ap bridgegroupname set SEVT1 HJMAP3
Setting bridgegroupname on an AP permanently restricts the APs to which it may c
onnect, use with caution.
Are you sure you want to continue? (y/n) n


AP bridgegroupname not changed!
```

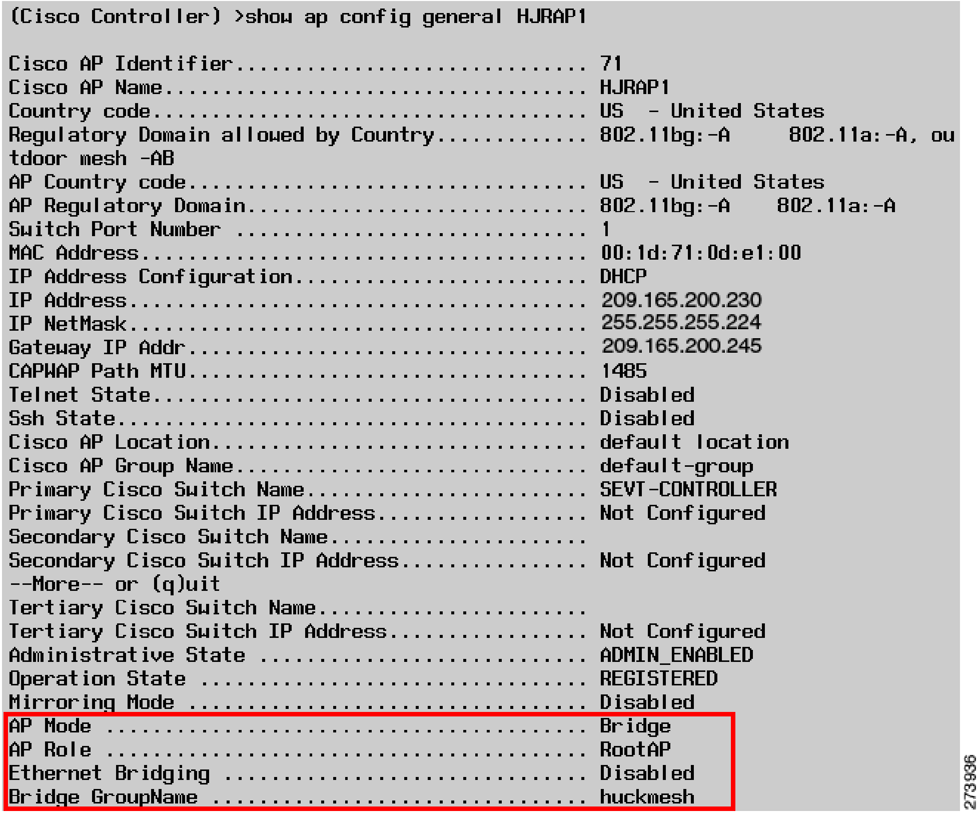
Note The mesh access point reboots after a BGN configuration.

Caution Exercise caution when you configure a BGN on a live network. Always start a BGN assignment from the farthest-most node (last node, bottom of mesh tree) and move up towards the RAP. This ensures that no mesh access points are dropped due to mixed BGNs (old and new BGNs) within the same network.

Step 2 To verify the BGN, enter the following command:

(Cisco controller) > **show ap config general** *AP_Name*

Information similar to the following is displayed.



```
(Cisco Controller) >show ap config general HJRAP1

Cisco AP Identifier.............................. 71
Cisco AP Name.................................... HJRAP1
Country code..................................... US  - United States
Regulatory Domain allowed by Country............. 802.11bg:-A     802.11a:-A, ou
tdoor mesh -AB
AP Country code.................................. US  - United States
AP Regulatory Domain............................. 802.11bg:-A    802.11a:-A
Switch Port Number .............................. 1
MAC Address...................................... 00:1d:71:0d:e1:00
IP Address Configuration......................... DHCP
IP Address....................................... 209.165.200.230
IP NetMask....................................... 255.255.255.224
Gateway IP Addr.................................. 209.165.200.245
CAPWAP Path MTU.................................. 1485
Telnet State..................................... Disabled
Ssh State........................................ Disabled
Cisco AP Location................................ default location
Cisco AP Group Name.............................. default-group
Primary Cisco Switch Name........................ SEVT-CONTROLLER
Primary Cisco Switch IP Address.................. Not Configured
Secondary Cisco Switch Name......................
Secondary Cisco Switch IP Address................ Not Configured
--More-- or (q)uit
Tertiary Cisco Switch Name.......................
Tertiary Cisco Switch IP Address................. Not Configured
Administrative State ............................ ADMIN_ENABLED
Operation State ................................. REGISTERED
Mirroring Mode .................................. Disabled
AP Mode ......................................... Bridge
AP Role ......................................... RootAP
Ethernet Bridging ............................... Disabled
Bridge GroupName ................................ huckmesh
```

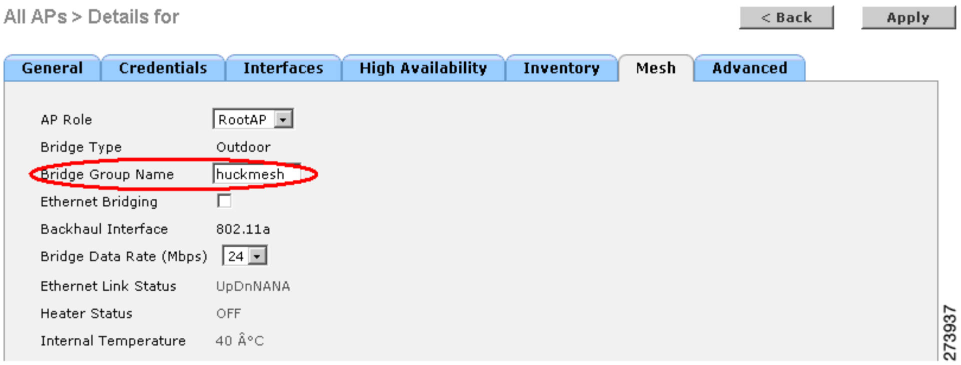
Verifying BGN - Using the GUI

To verify BGN using the GUI, follow these steps:

Step 1 Click **Wireless > Access Points >** *AP Name*. the details page for the selected mesh access point appears.

Step 2 Click the Mesh tab. Details for the mesh access point including the BGN appears. (See Figure 49.)

Figure 49 AP Name > Mesh



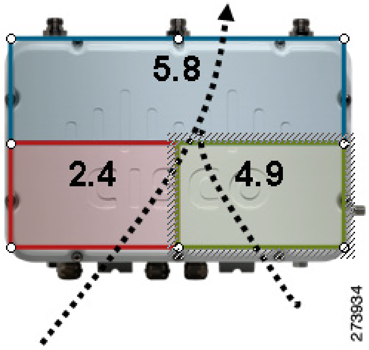
All APs > Details for

AP Role: RootAP
Bridge Type: Outdoor
Bridge Group Name: huckmesh
Ethernet Bridging: ☐
Backhaul Interface: 802.11a
Bridge Data Rate (Mbps): 24
Ethernet Link Status: UpDnNANA
Heater Status: OFF
Internal Temperature: 40 Â°C

Configuring Public Safety Band Settings

A public safety band (4.9 GHz) is supported on the AP1522 and AP1524PS. (See Figure 50.)

Figure 50 AP 1524PS Diagram Showing Radio Placement



- For the AP1524PS, the 4.9-GHz radio is independent of the 5-GHz radio and is not used for the backhaul. On the AP1524PS, the 4.9-GHz band is enabled by default.
  - In Japan, 4.9 GHz is enabled by default as 4.9 GHz is unlicensed.
- For AP1522s, you can enable the 4.9 GHz public safety band on the backhaul. This can only be done at the global level and cannot be done on per mesh access point basis.
  - For client access on the 4.9 GHz band on the AP1522, you have to enable the feature *universal client access*.
- For public safety only deployments, the AP1522 and the AP1524PS must each be connected to its own separate RAP-based tree. For such deployments, the 1522 must use the 4.9-GHz backhaul and the 1524PS must be in its own RAP tree and use the 5.8-GHz backhaul.
- In some parts of the world including the U.S., you can only have public safety traffic on the 4.9-GHz backhaul. Check the destination countries compliance before installing.

The 4.9-GHz sub-band radio on the AP1524PS supports public safety channels within the 5-MHz (channels 1 to 10), 10-MHz (channels 11-19), and 20-MHz (channels 20-26) bandwidths.

- The following data rates are supported within the 5 MHz bandwidth: 1.5, 2.25, 3, 4.5, 6, 9, 12, and 13.5 Mbps. *The default rate is 6 Mbps.*
- The following data rates are supported within the 10 MHz bandwidth: 3, 4.5, 6, 9, 12, 18, 24, and 27 Mbps. *The default rate is 12 Mbps.*

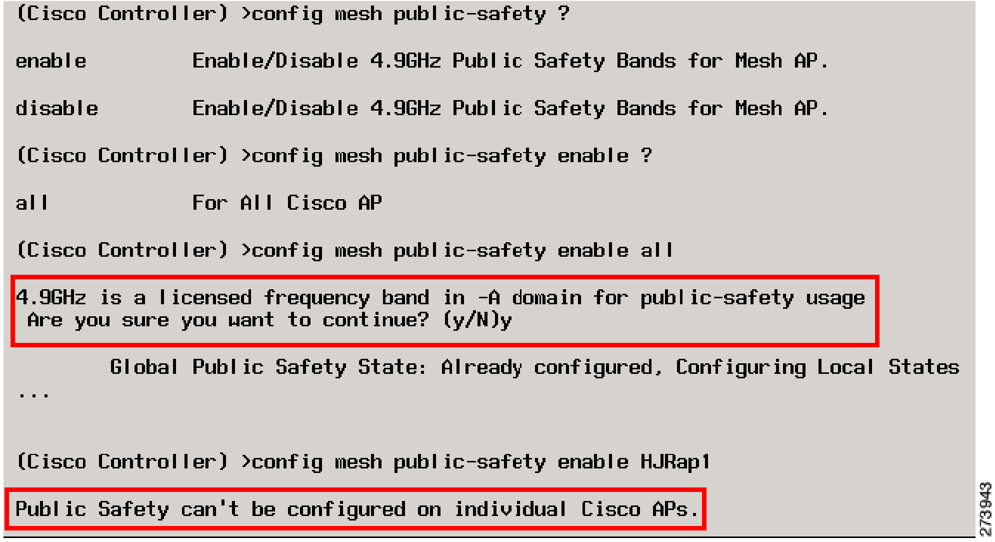
Note

- Those AP1522s with serial numbers *prior* to FTX1150XXXX do **not** support 5 and 10 MHz channels on the 4.9-GHz radio; however, a 20-MHz channel is supported.
- Those AP1522s with serial numbers *after* FTX1150XXXX support 5, 10, and 20 MHz channels.

Enabling the 4.9-GHz Band

When you attempt to enable the 4.9-GHz band, you get a warning that the band is a licensed band in most parts of the world. (See Figure 51.)

Figure 51 Public Safety Warning During Configuration



```
(Cisco Controller) >config mesh public-safety ?

enable         Enable/Disable 4.9GHz Public Safety Bands for Mesh AP.

disable        Enable/Disable 4.9GHz Public Safety Bands for Mesh AP.

(Cisco Controller) >config mesh public-safety enable ?

all            For All Cisco AP

(Cisco Controller) >config mesh public-safety enable all

4.9GHz is a licensed frequency band in -A domain for public-safety usage
 Are you sure you want to continue? (y/N)y

        Global Public Safety State: Already configured, Configuring Local States
...

(Cisco Controller) >config mesh public-safety enable HJRap1

Public Safety can't be configured on individual Cisco APs.
```

- To verify that a public safety band is on the mesh access point using the CLI, enter:

```
(Cisco controller) show mesh public-safety
Global Public Safety status: enabled
```

- To verify that a public safety band is on the mesh access point using the GUI:

  Wireless > Access Points > 802.11a radio > *Configure* (from Antenna drop-down menu)

Enabling AP1522 and AP1524PS to Associate with Cisco 3200 - Using the GUI

To enable AP1522 and AP1524PS to associate with Cisco 3200, follow these steps:

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

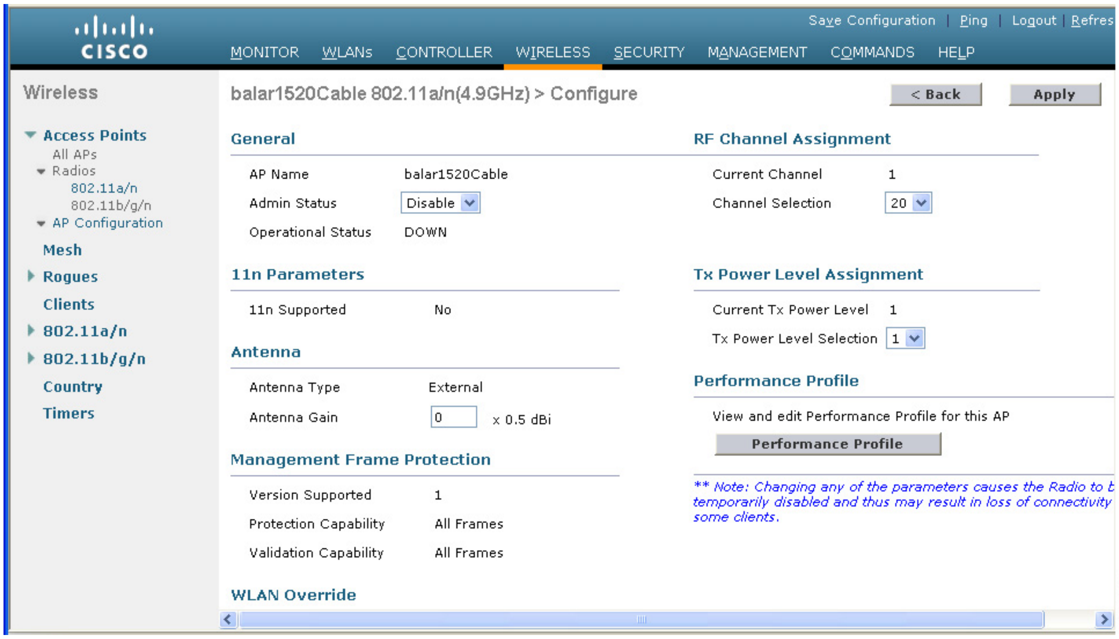
Step 2 Select the Backhaul Client Access **Enabled** check box to allow wireless client association over the 802.11a radio. Click **Apply**.

Note You are prompted with a message to allow reboot of all the mesh access points to enable Backhaul Client Access on a network. Click **OK**.

Step 3 To assign the channel to use for the backhaul (channels 20 through 26), click **Wireless > Access Points > Radio** and select **802.11a/n** from the Radio subheading. A summary page for all 802.11a radios displays.

Step 4 At the Antenna drop-down menu for the appropriate RAP, select **Configure.** The page seen in Figure 52 displays.

Figure 52 Wireless > Access Points > Radio > 802.11 a/n > Configure Page



balar1520Cable 802.11a/n(4.9GHz) > Configure

General

AP Name balar1520Cable

Admin Status Disable

Operational Status DOWN

11n Parameters

11n Supported No

Antenna

Antenna Type External

Antenna Gain 0 x 0.5 dBi

Management Frame Protection

Version Supported 1

Protection Capability All Frames

Validation Capability All Frames

WLAN Override

RF Channel Assignment

Current Channel 1

Channel Selection 20

Tx Power Level Assignment

Current Tx Power Level 1

Tx Power Level Selection 1

Performance Profile

View and edit Performance Profile for this AP

*** Note: Changing any of the parameters causes the Radio to b temporarily disabled and thus may result in loss of connectivity some clients.*

Step 5 At the RF Backhaul Channel Assignment section, select the **Custom** option for the Assignment Method option and select any channel between 1 and 26.

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

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

Enabling 1522 and 1524PS Association with Cisco 3200 - Using the CLI

To enable an AP1522 or AP1524PS to associate with Cisco 3200, follow these steps:

Step 1 To enable client access mode on the AP1522 and AP1524, enter this command:

config mesh client-access enable

Step 2 To enable the 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:

a. On the AP1522, enter these commands:

config 802.11a disable *Cisco_MAP*

config 802.11a channel ap *Cisco_MAP channel number*

config 802.11a enable *Cisco_MAP*

b. On the AP1524PS, 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 AP1522 and AP1524PS, *channel number* is equal to any value 1 to 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 (1522 only)

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

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

Configuring Power and Channel Settings

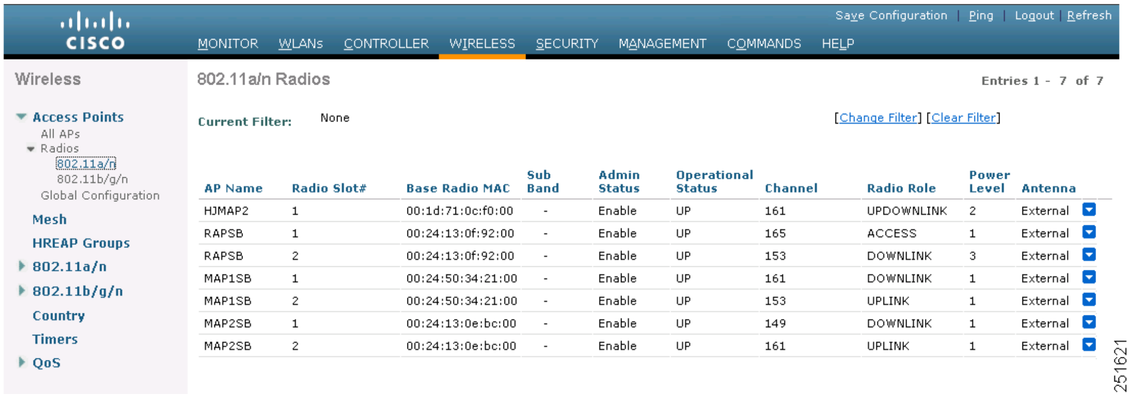
The backhaul channel (802.11a/n) can be configured on a RAP. MAPs tune to the RAP channel. The local access can be configured independently for MAP.

Configuring Power and Channel Settings - Using the GUI

To configure power and channel using the controller GUI, follow these steps:

Step 1 Choose **Wireless > Access Points > 802.11a/n** (see Figure 53).

Figure 53 Access Points > 802.11a/n Radios Page


Save Configuration | Ping | Logout | Refresh
CISCO
MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP
Wireless
Access Points
All APs
Radios
802.11a/n
802.11b/g/n
Global Configuration
Mesh
HREAP Groups
802.11a/n
802.11b/g/n
Country
Timers
QoS
[Change Filter] [Clear Filter]
251621

802.11a/n Radios

Entries 1 - 7 of 7

Current Filter: None

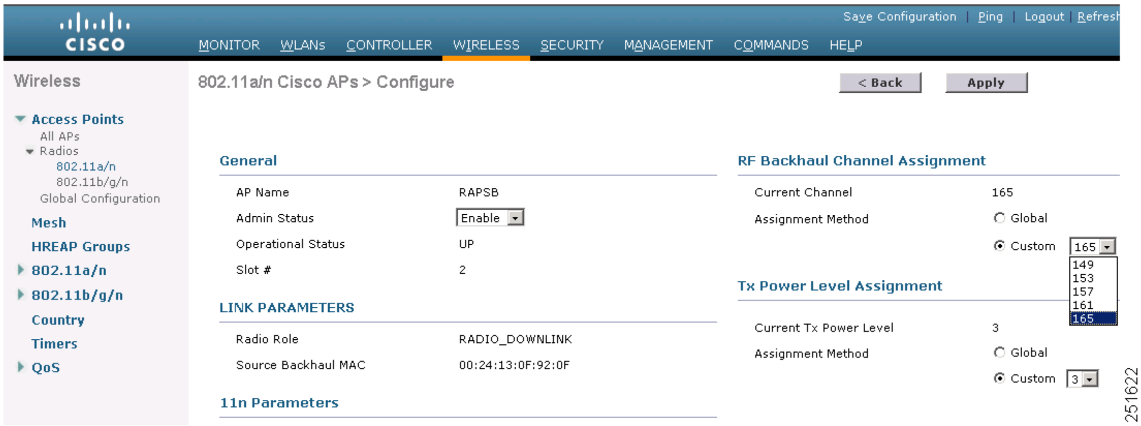
AP Name	Radio Slot#	Base Radio MAC	Sub Band	Admin Status	Operational Status	Channel	Radio Role	Power Level	Antenna
HJMAP2	1	00:1d:71:0c:f0:00	-	Enable	UP	161	UPDOWNLINK	2	External
RAPSB	1	00:24:13:0f:92:00	-	Enable	UP	165	ACCESS	1	External
RAPSB	2	00:24:13:0f:92:00	-	Enable	UP	153	DOWNLINK	3	External
MAP1SB	1	00:24:50:34:21:00	-	Enable	UP	161	DOWNLINK	1	External
MAP1SB	2	00:24:50:34:21:00	-	Enable	UP	153	UPLINK	1	External
MAP2SB	1	00:24:13:0e:bc:00	-	Enable	UP	149	DOWNLINK	1	External
MAP2SB	2	00:24:13:0e:bc:00	-	Enable	UP	161	UPLINK	1	External

Note In Figure 53, radio slots are displayed for each radio. For an AP1524SB, the 802.11a radio will display for slots 1 and 2 that operate in the 5-GHz band. For an AP1524PS, the 802.11a radio will display for slots 1 and 2, operating in the 5-GHz and 4.9-GHz bands respectively.

Step 2 Select **configure** from the antenna drop-down list for the 802.11 a/n radio. The configure page appears (see Figure 54).

Note For the 1524SB, select the antenna drop-down list for a RAP with a radio role of downlink.

Figure 54 802.11a/n Cisco APs > Configure Page



802.11a/n Cisco APs > Configure

General

AP Name	RAPSB
Admin Status	Enable
Operational Status	UP
Slot #	2

LINK PARAMETERS

Radio Role	RADIO_DOWNLINK
Source Backhaul MAC	00:24:13:0F:92:0F

11n Parameters

RF Backhaul Channel Assignment

Current Channel	165
Assignment Method	○ Global
	● Custom 165

Tx Power Level Assignment

Current Tx Power Level	3
Assignment Method	○ Global
	● Custom 3

Step 3 Assign a channel (assignment methods of global and custom) for the radio.

Note When you assign a channel to the AP1524SB, choose the **Custom** assignment method, and select one of the supported channels for the 5-GHz band.

Step 4 Assign Tx power levels (global and custom) for the radio.

There are five selectable power levels for the 802.11a backhaul for AP1520s.

- AP1522 supports ISM, UNII-2 band and UNII-2 Extended bands.
- AP1524 supports the 5-GHz band.

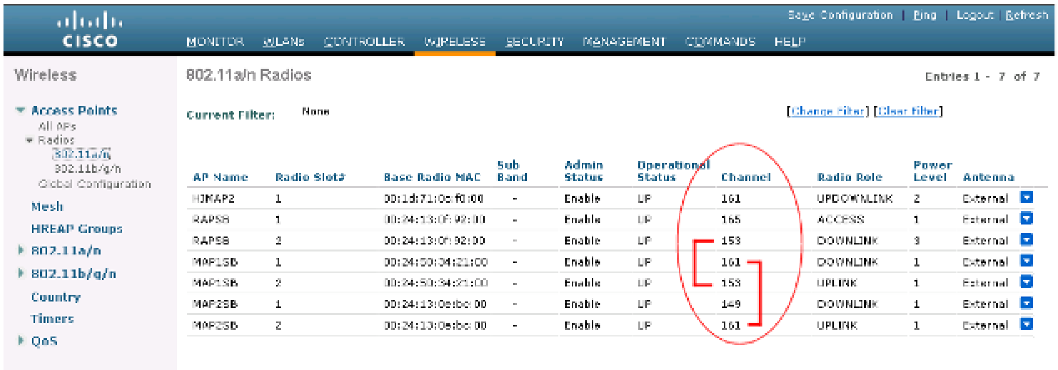
Note The default Tx power level on the backhaul is the highest power level (Level 1).

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

Step 5 Click **Apply** when power and channel assignment are complete.

Step 6 From the 802.11 a/n Radios page, verify that channel assignments were made correctly (see Figure 55).

Figure 55 Channel Assignment



802.11a/n Radios

Entries 1 - 7 of 7

Current Filter: None

AP Name	Radio Slot#	Base Radio MAC	Sub Band	Admin Status	Operational Status	Channel	Radio Role	Power Level	Antenna
HJMAP2	1	00:1d:71:0c:f0:00	-	Enable	UP	161	UPDOWNLINK	2	External
RAPSB	1	00:24:13:0f:92:00	-	Enable	UP	165	ACCESS	1	External
RAPSB	2	00:24:13:0f:92:00	-	Enable	UP	153	DOWNLINK	3	External
MAP1SB	1	00:24:50:34:21:00	-	Enable	UP	161	DOWNLINK	1	External
MAP1SB	2	00:24:50:34:21:00	-	Enable	UP	153	UPLINK	1	External
MAP2SB	1	00:24:13:0e:bc:00	-	Enable	UP	149	DOWNLINK	1	External
MAP2SB	2	00:24:13:0e:bc:00	-	Enable	UP	161	UPLINK	1	External

Configuring the Channels on the Serial Backhaul - Using the CLI

To configure channels on the serial backhaul of the RAP using the controller CLI, follow these steps:

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 Antenna Gain

You must configure the antenna gain for the mesh access point to match that of the antenna installed using the controller GUI or controller CLI.

Note See Table 5 on page 22 for details on supported antennas and their gains.

Configuring Antenna Gain - Using the GUI

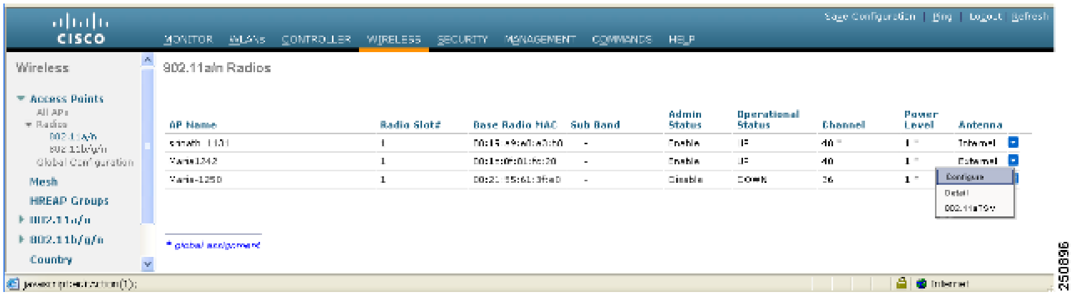
To configure antenna parameters using the controller GUI, follow these steps:

Step 1 Choose **Wireless > Access Points > Radio > 802.11a/n** to open the 802.11a/n Radios page.

Step 2 For the mesh access point antenna you want to configure, hover the mouse over the blue arrow (far right) to display antenna options. Choose **Configure**. (See Figure 56.)

Note Only external antennas have configurable gain settings.

Figure 56 802.11a/n Radios Page



802.11a/n Radios

AP Name	Radio Slot#	Base Radio MAC	Sub Band	Admin Status	Operational Status	Channel	Power Level	Antenna
sinath_1131	1	00:15:[illegible]	-	Enable	UP	40 *	1 *	Internal
Varia1242	1	00:1e:0f:01:fc:20	-	Enable	UP	40	1 *	External
Varia-1250	1	00:21:55:61:3f:a0	-	Disable	DOWN	36	1 *	

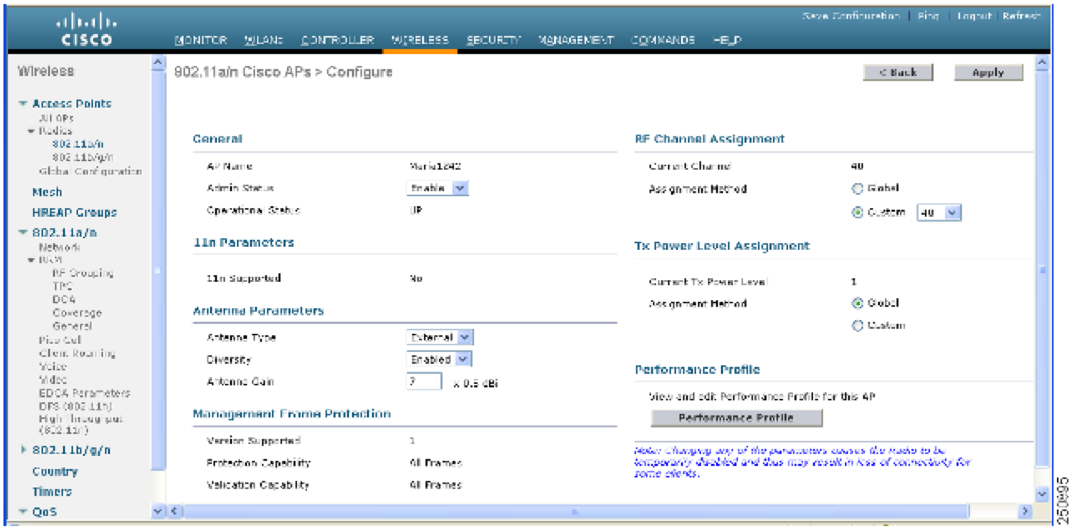
* global assignment

Step 3 In the Antenna Parameters section, enter the antenna gain.

The gain is entered in 0.5 dBm units. For example, 2.5 dBm = 5. (See Figure 57.)

Note The entered gain value must match that value specified by the vendor for that antenna.

Figure 57 802.11 a/n Cisco APs > Configure Page



802.11a/n Cisco APs > Configure

General

AP Name	Varia1242
Admin Status	Enable
Operational Status	UP

11n Parameters

11n Supported	No

Antenna Parameters

Antenna Type	External
Diversity	Enabled
Antenna Gain	7 x 0.5 dBi

Management Frame Protection

Version Supported	1
Protection Capability	All Frames
Validation Capability	All Frames

RF Channel Assignment

Current Channel	40
Assignment Method	○ Global ● Custom 40

Tx Power Level Assignment

Current Tx Power Level	1
Assignment Method	● Global ○ Custom

Performance Profile

View and edit Performance Profile for this AP

Note: Changing any of the parameters causes the Radio to be temporarily disabled and thus may result in loss of connectivity for some clients.

Step 4 Click **Apply** and **Save Configuration** to save the changes.

Configuring Antenna Gain - Using the CLI

Enter this command to configure the antenna gain for the 802.11a backhaul radio using the controller CLI.

config 802.11a antenna extAntGain *antenna_gain AP_name*

where gain is entered in 0.5 dBm units (for example, 2.5 dBm =5).

Backhaul Channel Deselection on Serial Backhaul Access Point

The backhaul channel deselection feature helps you to restrict the set of channels available to be assigned for the serial backhaul MAPs and RAPs. Because 1524 MAP channels are automatically assigned, this feature helps in regulating the set of channels that get assigned to mesh access points. For example, if you do not want channel 165 to get assigned to any of the 1524 mesh access points, you need to remove channel 165 from the DCA list and enable this feature.

When you remove certain channels from the DCA list and enable the **mesh backhaul dca-channel** command, those channels will not be assigned to any serial backhaul access points in any scenario. Even if a radar is detected on all channels within the DCA list channels, the radio will be shut down rather than moved to channels outside it. A trap message is sent to the WCS, and the message is displayed showing that the radio has been shut down because of DFS. You will not be able to assign channels to serial backhaul RAP outside of the DCA list with the **config mesh backhaul dca-channels enable** command enabled. However, this is not case for 1522/1524PS APs. For these APs, you can assign any channel outside of the DCA list for a RAP, and the controller/AP can also select a channel outside of the DCA list if no radar-free channel is available from the list.

This feature is best suited in an interoperability scenario with indoor mesh access points or workgroup bridges that support a channel set that is different from outdoor access points. For example, channel 165 is supported by outdoor access points but not by indoor access points in the -A domain. By enabling the backhaul channel deselection feature, you can restrict the channel assignment to only those channels that are common to both indoor and outdoor access points.

Note Channel deselection is applicable to 7.0 and later releases.

In some scenarios, there may be two linear tracks or roads for mobility side by side. Because channel selection of MAPs happens automatically, there can be a hop at a channel, which is not available on the autonomous side, or the channel has to be skipped when the same or adjacent channel is selected in a neighborhood access point that belongs to a different linear chain.

Configuring Backhaul Channel Deselection - Using the Controller GUI

To configure the backhaul channel deselection, follow these steps:

Step 1 Choose **Controller > Wireless > 802.11a/n > RRM > DCA**

The Dynamic Channel Assignment Algorithm page appears.

Step 2 Select one or more channels to include in the DCA list.

The channels included in the DCA list will not be assigned to the access points associated to this controller during automatic channel assignment.

Step 3 Choose **Wireless > Mesh**

The Mesh page appears.

Step 4 Select the Mesh DCA Channels check box to enable the backhaul channel deselection using the DCA list. This option is applicable for serial backhaul access points.

Step 5 After you enable the backhaul deselection option, choose **Wireless > Access Points > Radios > 802.11a/n** to configure the channel for the RAP downlink radio.

Step 6 From the list of access points, click on the Antenna drop-down list for a RAP and choose **Configure**.

The Configure page appears.

Step 7 In the RF Backhaul Channel assignment section, choose **Custom**.

Step 8 Select a channel for the RAP downlink radio from the drop-down list, which appears when you choose **Custom**.

Step 9 Click **Apply** to save and apply the configuration changes.

Configuring Backhaul Channel Deselection - Using the Controller CLI

To configure backhaul channel deselection using CLI, follow these steps:

Step 1 From the controller prompt, enter the **show advanced 802.11a channel** command to review the channel list already configured in the DCA list.

```
(Controller) > show advanced 802.11a channel
Automatic Channel Assignment
  Channel Assignment Mode....................... AUTO
  Channel Update Interval....................... 600 seconds
  Anchor time (Hour of the day)................. 0
  Channel Update Contribution................... SNI..
  CleanAir Event-driven RRM option.............. Enabled
  CleanAir Event-driven RRM sensitivity......... Medium
  Channel Assignment Leader..................... 09:2b:16:28:00:03
  Last Run...................................... 286 seconds ago
  DCA Sensitivity Level......................... MEDIUM (15 dB)
  DCA 802.11n Channel Width..................... 20 MHz
  DCA Minimum Energy Limit...................... -95 dBm
  Channel Energy Levels
    Minimum..................................... unknown
    Average..................................... unknown
    Maximum..................................... unknown
  Channel Dwell Times
    Minimum..................................... 0 days, 17 h 02 m 05 s
    Average..................................... 0 days, 17 h 46 m 07 s
    Maximum..................................... 0 days, 18 h 28 m 58 s
  802.11a 5 GHz Auto-RF Channel List

--More-- or (q)uit
    Allowed Channel List........................ 36,40,44,48,52,56,60,64,116,
                                                 140
    Unused Channel List......................... 100,104,108,112,120,124,128,
                                                 132,136
  DCA Outdoor AP option......................... Disabled
```

Step 2 To add a channel to the DCA list, enter the **config advanced 802.11a channel add** *channel number* command, where *channel number* is the channel number that you want to add to the DCA list.

You can also delete a channel from the DCA list by entering the **config advanced 802.11a channel delete** *channel number* command, where *channel number* is the channel number that you want to delete from the DCA list.

Before you add or delete a channel to or from the DCA list, ensure that the 802.11a network is disabled.

- To disable the 802.11a network, enter the following command:

  config 802.11a disable network

- To enable the 802.11a network, enter the following command:

  config 802.11a enable network

You cannot directly delete a channel from the DCA list if it is assigned to any 1524 RAP. To delete a channel assigned to a RAP, you must first change the channel assigned to the RAP and then enter the **config advanced 802.11a channel delete** *channel number* command from the controller.

The following is a sample output of the add and delete channel commands:

```
(Controller) > config 802.11a disable network

Disabling the 802.11a network may strand mesh APs. Are you sure you want to continue?
(y/n)y


(Controller) > config advanced 802.11a channel add 132


(Controller) > config advanced 802.11a channel delete 116

802.11a 5 GHz Auto-RF:
Allowed Channel List......................... 36,40,44,48,52,56,60,64,116,
                                                  132,140
DCA channels for cSerial Backhaul Mesh APs is enabled.
DCA list should have at least 3 non public safety channels supported by Serial Backhaul
Mesh APs.
Otherwise, the Serial Backhaul Mesh APs can get stranded.
Are you sure you want to continue? (y/N)y


Failed to delete channel.
Reason: Channel 116 is configured for one of the Serial Backhaul RAPs.
Disable mesh backhaul dca-channels or configure a different channel for Serial Backhaul
RAPs.

(Controller) > config advanced 802.11a channel delete 132

  802.11a 5 GHz Auto-RF:
Allowed Channel List..................... 36,40,44,48,52,56,60,64,116,132,140
DCA channels for Serial Backhaul Mesh APs is enabled.
DCA list should have at least 3 non public safety channels supported by Serial Backhaul
Mesh APs.
Otherwise, the Serial Backhaul Mesh APs can get stranded.
Are you sure you want to continue? (y/N)y

(Controller) > config 802.11a enable network
```

Step 3 After a suitable DCA list has been created, enter the **config mesh backhaul dca-channels enable** command to enable the backhaul channel deselection feature for mesh access points.

You can enter the **config mesh backhaul dca-channels disable** command if you want to disable the backhaul channel deselection feature for mesh access points.

It is not required to disable 802.11a network to enable or disable this feature.

The following is a sample output:

```
(Controller) > config mesh backhaul dca-channels enable
```

```
  802.11a 5 GHz Auto-RF:
    Allowed Channel List......................... 36,40,44,48,52,56,60,64,116,
                                                  140
Enabling DCA channels for c1524 mesh APs will limit the channel set to the DCA channel
list.
DCA list should have at least 3 non public safety channels supported by Serial Backhaul
Mesh APs.
Otherwise, the Serial Backhaul Mesh APs can get stranded.
Are you sure you want to continue? (y/N)y

(Controller) > config mesh backhaul dca-channels disable
```

Step 4 To check the current status of the backhaul channel deselection feature, enter the **show mesh config** command.

The following is a sample output:

```
(Controller) > show mesh config

Mesh Range....................................... 12000
Mesh Statistics update period.................... 3 minutes
Backhaul with client access status............... enabled
Background Scanning State........................ enabled
Backhaul Amsdu State............................. disabled

Mesh Security
   Security Mode................................. PSK
   External-Auth................................. enabled
      Radius Server 1............................ 209.165.200.240
   Use MAC Filter in External AAA server......... disabled
   Force External Authentication................. disabled

Mesh Alarm Criteria
   Max Hop Count................................. 4
   Recommended Max Children for MAP.............. 10
   Recommended Max Children for RAP.............. 20
   Low Link SNR.................................. 12
   High Link SNR................................. 60
   Max Association Number........................ 10
   Association Interval.......................... 60 minutes
   Parent Change Numbers......................... 3

--More-- or (q)uit
   Parent Change Interval........................ 60 minutes


Mesh Multicast Mode.............................. In-Out
Mesh Full Sector DFS............................. enabled


Mesh Ethernet Bridging VLAN Transparent Mode..... enabled

Mesh DCA channels for Serial Backhaul APs................ disabled
```

Step 5 Enter the **config slot** *slot number* **channel ap** *ap-name channel number* command to assign a particular channel to 1524 RAP downlink radio.

- *slot number* refers to the slot of the downlink radio to which the channel is assigned.
- *ap-name* refers to the name of the access point on which the channel is configured.
- *channel number* refers to the channel that is assigned to a slot on the access point.

The slot 2 of 1524 RAP acts as a downlink radio. If backhaul channel deselection is enabled, you can assign only those channels that are available in the DCA list the access point.

The following is a sample output:

```
(Controller) > config slot 2 channel ap Controller-RAP2-1524 136
Mesh backhaul dca-channels is enabled. Choose a channel from the DCA list.
(Controller) > config slot 2 channel ap Controller-RAP2-1524 140
```

Backhaul Channel Deselection Guidelines

Follow these guidelines when configuring backhaul channel deselection:

- Channels for serial backhaul RAP 11a access radio and both 11a radios of serial backhaul MAPs are assigned automatically. You cannot configure these channels.
- Look out for trap logs on the controller. In case of radar detection and subsequent channel change, messages similar to below appear:

  ```
  Channel changed for Base Radio MAC: 00:1e:bd:19:7b:00 on 802.11a
  radio. Old channel: 132. New Channel: 116. Why: Radar. Energy
  before/after change: 0/0. Noise before/after change: 0/0.
  Interference before/after change: 0/0.

  Radar signals have been detected on channel 132 by 802.11a radio
  with MAC: 00:1e:bd:19:7b:00 and slot 2
  ```

- For every serial backhaul AP, channels on downlink and uplink radios should always be noninterfering (for example, if the uplink is channel 104, the 100, 104, and 108 channels cannot be assigned for a downlink radio on that AP). An alternate adjacent channel is also selected for an 11a access radio on RAP.
- If radar signals are detected on all channels except the uplink radio channel, the downlink radio will be shut down and the uplink radio will act as both an uplink and a downlink (that is, the behavior is similar to 1522 APs in this case).
- Radar detection is cleared after 30 minutes. Any radio that is shut down because of radar detection should be back up and operational after this duration.
- There is a 60-second silent period immediately after moving to a DFS-enabled channel (irrespective of whether the channel change is because of radar detection or user configured in case of a RAP) during which the AP scans for radar signals without transmitting anything. A small period (60 seconds) of downtime may occur because of radar detection, if the new channel is also DFS-enabled. If radar detection occurs again on the new channel during the silent period, the parent changes its channel without informing the child AP because it is not allowed to transmit during the silent period. In this case, the child AP dissociates and goes back to scan mode, rediscovers the parent on the new channel and then joins back, which causes a slightly longer (approximately 3 minutes) downtime.
- In case of a RAP, the channel for the downlink radio is always selected from within the DCA list, irrespective of whether the backhaul channel deselection feature is enabled or not. The behavior is different for a MAP because the MAP can pick any channel that is allowed for that domain, unless the backhaul channel deselection feature is enabled. We recommend that you have quite a few channels added to the 802.11a DCA channel list to prevent any radios getting shut down because of a lack of channels even if the backhaul channel deselection feature is not in use.
- Because the DCA list that was used for the RRM feature is also used for mesh APs through the backhaul channel deselection feature, keep in mind that any addition or deletion of channels from the DCA list will affect the channel list input to the RRM feature for nonmesh access points as well. RRM is off for mesh.

- For -M domain APs, a slightly longer time interval (25 to 50 percent more time than usual) may be required for the mesh network to come up because there is a longer list of DFS-enabled channels in the -M domain, which each AP scans before joining the parent.

Configuring Dynamic Channel Assignment

Using the controller GUI, follow these steps to specify the channels that the dynamic channel assignment (DCA) algorithm considers when selecting the channels to be used for RRM scanning. This functionality is helpful when you know that the clients do not support certain channels because they are legacy devices or they have certain regulatory restrictions.

The steps outlined in this section are only relevant to mesh networks.

Step 1 To disable the 802.11a or 802.11b/g network, follow these steps:

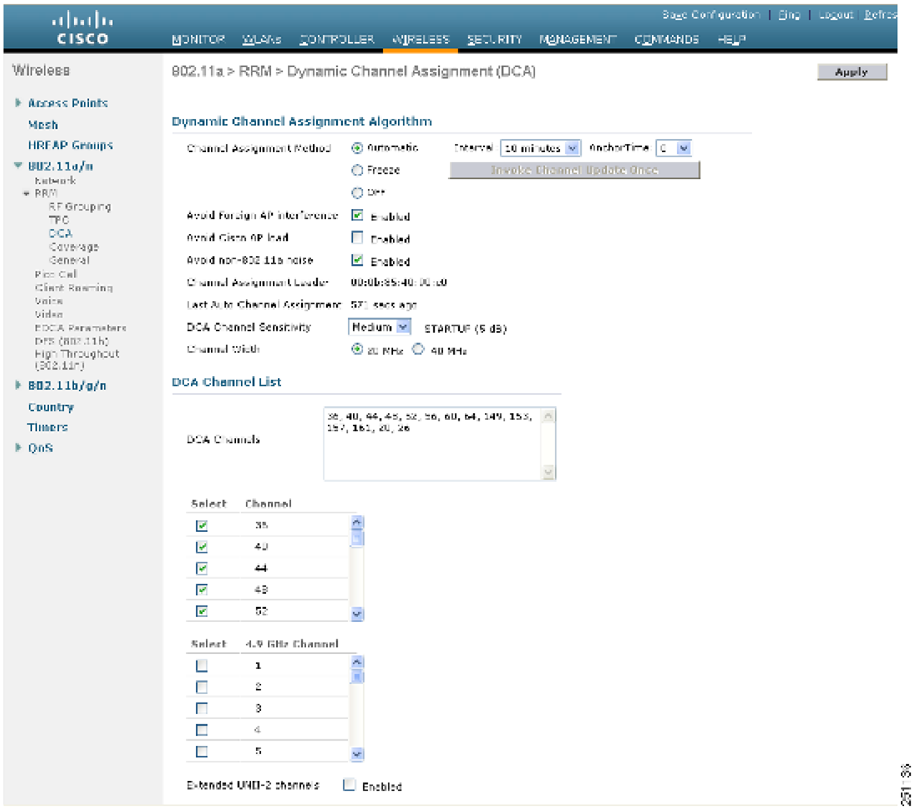
a. Choose **Wireless** > **802.11a/n** or **802.11b/g/n** > **Network** to open the 802.11a (or 802.11b/g) Global Parameters page.

b. Deselect the **802.11a** (or **802.11b/g**) **Network Status** check box.

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

Step 2 Choose **Wireless** > **802.11a/n** or **802.11b/g/n** > **RRM** > **DCA** to open the 802.11a (or 802.11b/g) > RRM > Dynamic Channel Assignment (DCA) page. (See Figure 58.)

Figure 58 ***802.11a > RRM > Dynamic Channel Assignment (DCA) Page***



802.11a > RRM > Dynamic Channel Assignment (DCA)

Dynamic Channel Assignment Algorithm

Channel Assignment Method ● Automatic Interval 10 minutes AnchorTime 0
○ Freeze
○ Off

Avoid Foreign AP interference ☑ Enabled

Avoid Cisco AP load ☐ Enabled

Avoid non-802.11a noise ☑ Enabled

Channel Assignment Leader 00:0b:85:40:00:a0

Last Auto Channel Assignment 571 secs ago

DCA Channel Sensitivity Medium STARTUP (5 dB)

Channel Width ● 20 MHz ○ 40 MHz

DCA Channel List

DCA Channels 36, 40, 44, 48, 52, 56, 60, 64, 149, 153, 157, 161, 20, 26

Select	Channel
☑	36
☑	40
☑	44
☑	48
☑	52

Select	4.9 GHz Channel
☐	1
☐	2
☐	3
☐	4
☐	5

Extended UNII-2 channels ☐ Enabled

Step 3 Choose one of the following options from the Channel Assignment Method drop-down list to specify the controller's DCA mode:

- **Automatic**—Causes the controller to periodically evaluate and, if necessary, update the channel assignment for all joined mesh access points. This is the default value.
- **Freeze**—Causes the controller to evaluate and update the channel assignment for all joined mesh access points, if necessary, but only when you click **Invoke Channel Update Once**.

Note The controller does not evaluate and update the channel assignment immediately after you click **Invoke Channel Update Once**. It waits for the next interval to elapse.

- **OFF**—Turns off DCA and sets all mesh access point radios to the first channel of the band, which is the default value. If you choose this option, you must manually assign channels on all radios.

Step 4 From the Interval drop-down list, choose one of the following options to specify how often the DCA algorithm is allowed to run: 10 minutes, 1 hour, 2 hours, 3 hours, 4 hours, 6 hours, 8 hours, 12 hours, or 24 hours. The default value is 10 minutes.

Step 5 From the AnchorTime drop-down list, choose a number to specify the time of day when the DCA algorithm is to start. The options are numbers between 0 and 23 (inclusive) representing the hour of the day from 12:00 a.m. to 11:00 p.m.

Step 6 Select the **Avoid Foreign AP Interference** check box to cause the controller's RRM algorithms to consider 802.11 traffic from foreign access points (those not included in your wireless network) when assigning channels to lightweight access points, or deselect it to disable this feature. For example, RRM may adjust the channel assignment to have access points avoid channels close to foreign access points. The default value is checked.

Step 7 Select the **Avoid Cisco AP Load** check box to cause the controller's RRM algorithms to consider 802.11 traffic from Cisco lightweight access points in your wireless network when assigning channels, or deselect it to disable this feature. For example, RRM can assign better reuse patterns to access points that carry a heavier traffic load. The default value is deselected.

Step 8 Select the **Avoid Non-802.11a (802.11b) Noise** check box to cause the controller's RRM algorithms to consider noise (non-802.11 traffic) in the channel when assigning channels to lightweight access points, or deselect it to disable this feature. For example, RRM may have access points avoid channels with significant interference from non-access point sources, such as microwave ovens. The default value is checked.

Step 9 From the DCA Channel Sensitivity drop-down list, choose one of the following options to specify how sensitive the DCA algorithm is to environmental changes such as signal, load, noise, and interference when determining whether to change channels:

- **Low**—The DCA algorithm is not particularly sensitive to environmental changes.
- **Medium**—The DCA algorithm is moderately sensitive to environmental changes.
- **High**—The DCA algorithm is highly sensitive to environmental changes.

The default value is *Medium*. The DCA sensitivity thresholds vary by radio band, as noted in Table 14.

Table 14 DCA Sensitivity Thresholds

Option	2.4-GHz DCA Sensitivity Threshold	5-GHz DCA Sensitivity Threshold
High	5 dB	5 dB
Medium	15 dB	20 dB
Low	30 dB	35 dB

Step 10 For 802.11a/n networks only, choose one of the following Channel Width options to specify the channel bandwidth supported for all 802.11n radios in the 5-GHz band:

- **20 MHz**—The 20-MHz channel bandwidth (default)

Note To override the globally configured DCA channel width setting, you can statically configure an access point's radio for 20-MHz mode on the 802.11a/n Cisco APs > Configure page. If you ever then change the static RF channel assignment method to Global on the access point radio, the global DCA configuration overrides the channel width configuration that the access point was previously using.

This page also shows the following non-configurable channel parameter settings:

- **Channel Assignment Leader**—The MAC address of the RF group leader, which is responsible for channel assignment.
- **Last Auto Channel Assignment**—The last time RRM evaluated the current channel assignments.

Step 11 In the DCA Channel List section, the DCA Channels field shows the channels that are currently selected. To choose a channel, select its check box in the Select column. To exclude a channel, deselect its check box.

Range:
802.11a—36, 40, 44, 48, 52, 56, 60, 64, 100, 104, 108, 112, 116, 132, 136, 140, 149, 153, 157, 161, 165, 190, 196
802.11b/g—1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11

Default:
802.11a—36, 40, 44, 48, 52, 56, 60, 64, 100, 104, 108, 112, 116, 132, 136, 140, 149, 153, 157, 161
802.11b/g—1, 6, 11

Note These extended UNII-2 channels in the 802.11a band do not appear in the channel list: 100, 104, 108, 112, 116, 132, 136, and 140. If you have Cisco Aironet 1520 series mesh access points in the -E regulatory domain, you must include these channels in the DCA channel list before you start operation. If you are upgrading from a previous release, verify that these channels are included in the DCA channel list. To include these channels in the channel list, select the **Extended UNII-2 Channels** check box.

Step 12 If you are using AP1520s in your network, you need to set the 4.9-GHz channels in the 802.11a band on which they are to operate. The 4.9-GHz band is for public safety client access traffic only. To choose a 4.9-GHz channel, select its check box in the Select column. To exclude a channel, deselect its check box.

Range:
802.11a—1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26

Default:
802.11a—20, 26

Step 13 Click **Apply** to commit your changes.

Step 14 To re-enable the 802.11a or 802.11b/g network, follow these steps:

a. Click **Wireless** > **802.11a/n** or **802.11b/g/n** > **Network** to open the 802.11a (or 802.11b/g) Global Parameters page.

b. Select the **802.11a** (or **802.11b/g**) **Network Status** check box.

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

Step 15 Click **Save Configuration** to save your changes.

Note To see why the DCA algorithm changed channels, click **Monitor** and then **View All** under Most Recent Traps. The trap provides the MAC address of the radio that changed channels, the previous channel and the new channel, the reason why the change occurred, the energy before and after the change, the noise before and after the change, and the interference before and after the change.

Universal Client Access on Serial Backhaul Access Points

With universal client access, you can have client access on the backhaul 802.11a radios in addition to the backhaul functionality. This feature is available on AP1522 and the serial backhaul access points AP1524SB & AP1523CV.

The dual 5-GHz Universal Client Access feature is intended for the serial backhaul access point platform, which has three radio slots. The radio in slot 0 operates in the 2.4-GHz band and is used for client access. The radios in slot 1 and slot 2 operate in the 5-GHz band and are primarily used for backhaul. However, with the Universal Client Access feature, clients were allowed to associate over the slot 1 radio. But slot 2 radio was used only for backhaul. With the 7.0 release, client access over the slot 2 radio is allowed with this Dual 5-GHz Universal Access feature.

By default, client access is disabled over both the backhaul radios. Follow the guidelines to enable or disable client access on the radio slots that constitute 5-GHz radios, irrespective of the radios being used as downlinks or uplinks:

- You can enable client access on slot 1 even if client access on slot 2 is disabled.
- You can enable client access on slot 2 only when client access on slot 1 is enabled.
- If you disable client access on slot 1, client access on slot 2 is automatically disabled on the CLI.
- To disable only the extended client access (on the slot 2 radio), use the GUI.
- All the mesh access points reboot whenever client access is enabled or disabled.

The two 802.11a backhaul radios use the same MAC address. There may be instances where a WLAN maps to the same BSSID on more than one slot. Client access on the slot 2 radio is referred to as Extended Universal Access (EUA) in this document.

You can configure Extended Universal Access using one of the following methods:

- "Configuring Extended Universal Access - Using the Controller GUI" section on page 102
- "Configuring Extended Universal Access - Using the Controller CLI" section on page 105
- "Configuring Extended Universal Access from Wireless Control System (WCS)" section on page 106

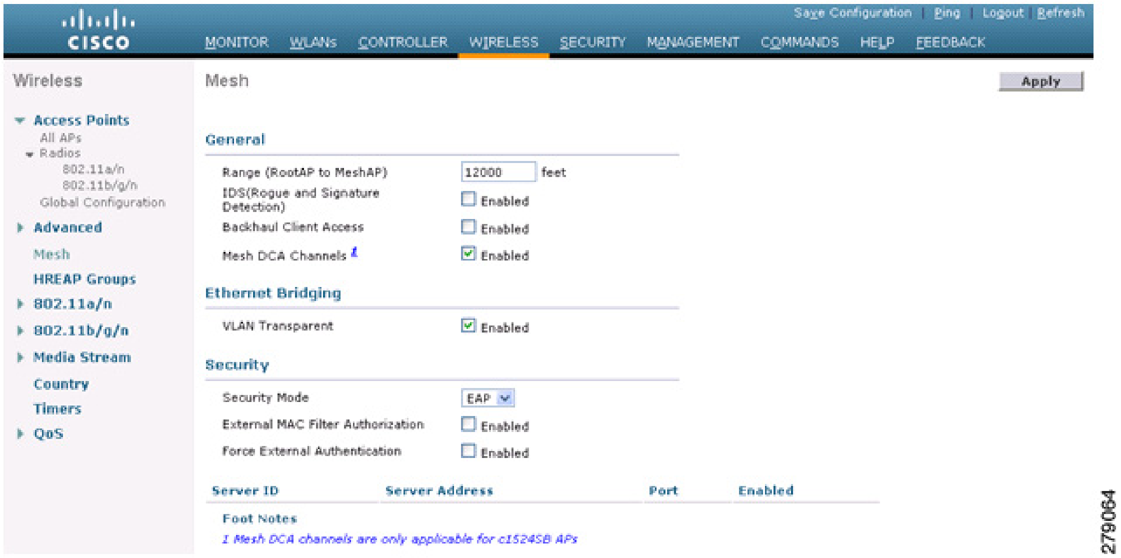
Configuring Extended Universal Access - Using the Controller GUI

To configure the Extended Universal Access, follow these steps:

Step 1 Choose **Controller > Wireless > Mesh**.

The Controller GUI when Backhaul Client Access is disabled page appears as shown in Figure 59.

Figure 59 *Advanced Controller Settings for Mesh Page*



Mesh

General

Range (RootAP to MeshAP) 12000 feet

IDS(Rogue and Signature Detection) □ Enabled

Backhaul Client Access □ Enabled

Mesh DCA Channels [1] ☑ Enabled

Ethernet Bridging

VLAN Transparent ☑ Enabled

Security

Security Mode EAP

External MAC Filter Authorization □ Enabled

Force External Authentication □ Enabled

Server ID	Server Address	Port	Enabled

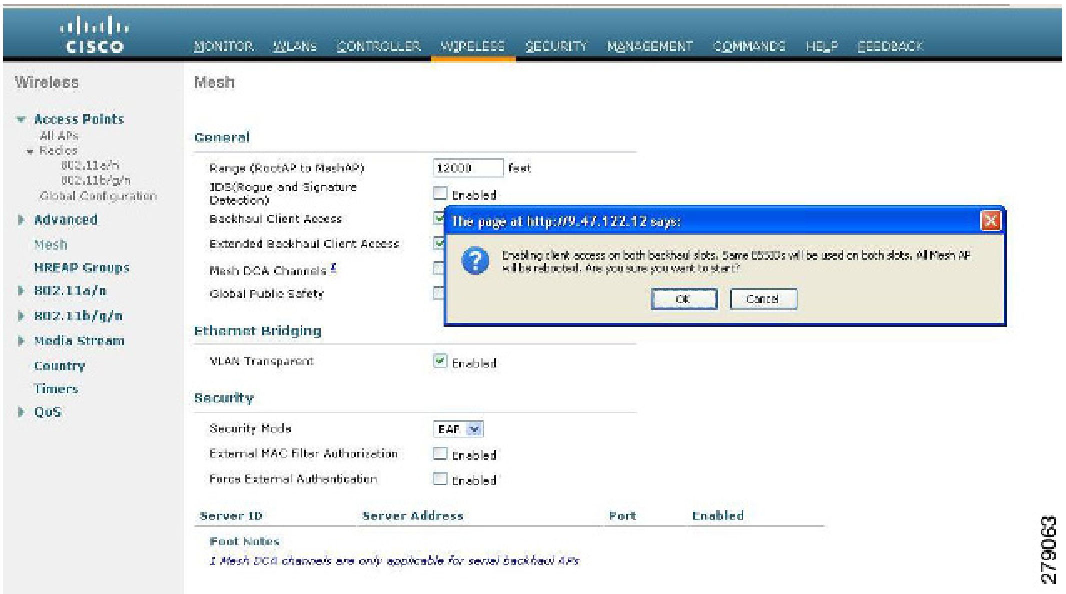
Foot Notes

1 Mesh DCA channels are only applicable for c1524SB APs

Step 2 Select the **Backhaul Client Access** check box to display the Extended Backhaul Client Access check box.

Step 3 Select the **Extended Backhaul Client Access** check box and click **Apply**. A message appears as shown in Figure 60.

Figure 60 *Advanced Controller Settings for Mesh Page*



Mesh

General

Range (RootAP to MeshAP) 12000 feet

IDS(Rogue and Signature Detection) □ Enabled

Backhaul Client Access ☑

Extended Backhaul Client Access ☑

Mesh DCA Channels [1] □

Global Public Safety □

The page at http://9.47.122.12 says:

Enabling client access on both backhaul slots. Same BSSIDs will be used on both slots. All Mesh AP will be rebooted. Are you sure you want to start?

Ethernet Bridging

VLAN Transparent ☑ Enabled

Security

Security Mode EAP

External MAC Filter Authorization □ Enabled

Force External Authentication □ Enabled

Server ID	Server Address	Port	Enabled

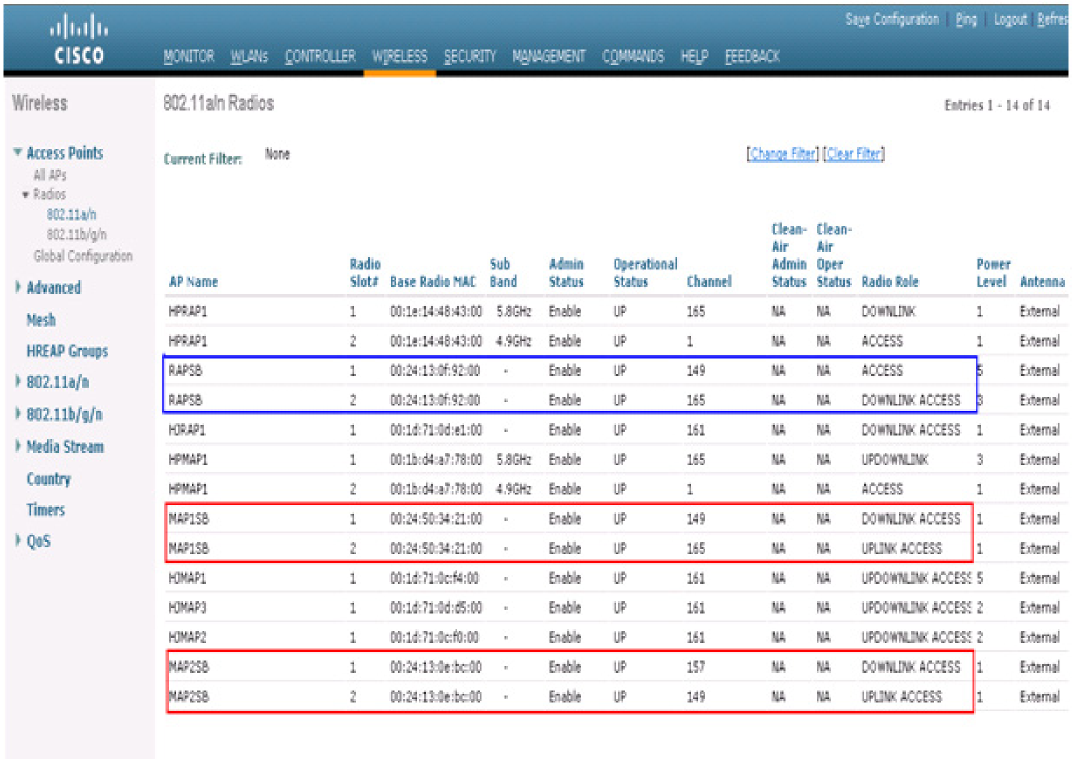
Foot Notes

1 Mesh DCA channels are only applicable for serial backhaul APs

Step 4 Click **OK**.

After EUA is enabled, 802.11a radios are displayed as shown in Figure 61.

Figure 61 802.11a Radios after EUA is Enabled



802.11a/n Radios

Entries 1 - 14 of 14

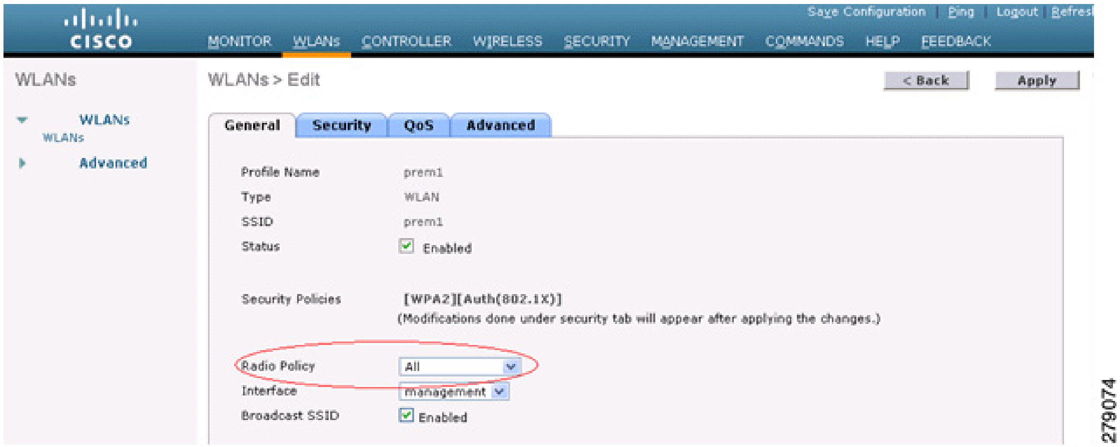
Current Filter: None

AP Name	Radio Slot#	Base Radio MAC	Sub Band	Admin Status	Operational Status	Channel	Clean-Air Admin Status	Clean-Air Oper Status	Radio Role	Power Level	Antenna
HPRAP1	1	00:1e:14:48:43:00	5.8GHz	Enable	UP	165	NA	NA	DOWNLINK	1	External
HPRAP1	2	00:1e:14:48:43:00	4.9GHz	Enable	UP	1	NA	NA	ACCESS	1	External
RAPSB	1	00:24:13:0f:92:00	-	Enable	UP	149	NA	NA	ACCESS	5	External
RAPSB	2	00:24:13:0f:92:00	-	Enable	UP	165	NA	NA	DOWNLINK ACCESS	3	External
HORAP1	1	00:1d:71:0d:e1:00	-	Enable	UP	161	NA	NA	DOWNLINK ACCESS	1	External
HPMAP1	1	00:1b:d4:a7:78:00	5.8GHz	Enable	UP	165	NA	NA	UPDOWNLINK	3	External
HPMAP1	2	00:1b:d4:a7:78:00	4.9GHz	Enable	UP	1	NA	NA	ACCESS	1	External
MAP1SB	1	00:24:50:34:21:00	-	Enable	UP	149	NA	NA	DOWNLINK ACCESS	1	External
MAP1SB	2	00:24:50:34:21:00	-	Enable	UP	165	NA	NA	UPLINK ACCESS	1	External
HOMAP1	1	00:1d:71:0c:f4:00	-	Enable	UP	161	NA	NA	UPDOWNLINK ACCESS	5	External
HOMAP3	1	00:1d:71:0d:d5:00	-	Enable	UP	161	NA	NA	UPDOWNLINK ACCESS	2	External
HOMAP2	1	00:1d:71:0c:f0:00	-	Enable	UP	161	NA	NA	UPDOWNLINK ACCESS	2	External
MAP2SB	1	00:24:13:0e:bc:00	-	Enable	UP	157	NA	NA	DOWNLINK ACCESS	1	External
MAP2SB	2	00:24:13:0e:bc:00	-	Enable	UP	149	NA	NA	UPLINK ACCESS	1	External

Slot 2 in the 5-GHz radio in the RAPSB (serial backhaul) that is used to extend the backhaul in the DOWNLINK direction is displayed as DOWNLINK ACCESS, where slot 1 in the 5-GHz radio in the RAPSB that is used for client access is displayed as ACCESS. Slot 2 in the 5-GHz radio in the MAPSB that is used for the UPLINK is displayed as UPLINK ACCESS, and slot 1 in the MAPSB is used for the DOWNLINK ACCESS with an omnidirectional antenna that also provides the client access.

Create WLAN on the WLC with the appropriate SSID mapped to the correct interface (VLAN). After you create a WLAN, it is applied to all the radios by default. If you want to enable client access only on 802.11a radios, then choose only the appropriate radio policy from the list shown in Figure 62.

Figure 62 Radio Policy Selection


cisco
Save Configuration | Ping | Logout | Refresh
MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK
WLANs
WLANs
WLANs
Advanced
WLANs > Edit
< Back
Apply
General
Security
QoS
Advanced
279074

Profile Name prem1
Type WLAN
SSID prem1
Status ☑ Enabled

Security Policies [WPA2][Auth(802.1X)]
(Modifications done under security tab will appear after applying the changes.)

Radio Policy All
Interface management
Broadcast SSID ☑ Enabled

Configuring Extended Universal Access - Using the Controller CLI

- Go to the Controller prompt and enter the **config mesh client-access enable extended** command.

  The following message is displayed:

  ```
  Enabling client access on both backhaul slots
  Same BSSIDs will be used on both slots
  All Mesh Serial Backhaul APs will be rebooted
  Are you sure you want to start? (y/N)
  ```

- Enter the **show mesh client-access** command to know the status of the backhaul with client access and the backhaul with client access extended.

  The status is displayed as follows:

  ```
  Backhaul with client access status: enabled
  Backhaul with client access extended status(3 radio AP): enabled
  ```

- There is no explicit command to disable client access only on slot 2 (EUA). You have to disable client access on both the backhaul slots by entering the following command:

  config mesh client-access disable

  The following message is displayed:

  ```
  All Mesh APs will be rebooted
  Are you sure you want to start? (y/N)
  ```

- You can disable EUA from the GUI without disturbing client access on the slot 1 radio, but all 1524SB access points will be rebooted.

  It is possible to enable client access only on slot 1 and not on slot 2 by entering the following command:

  config mesh client-access enable

  The following message is displayed:

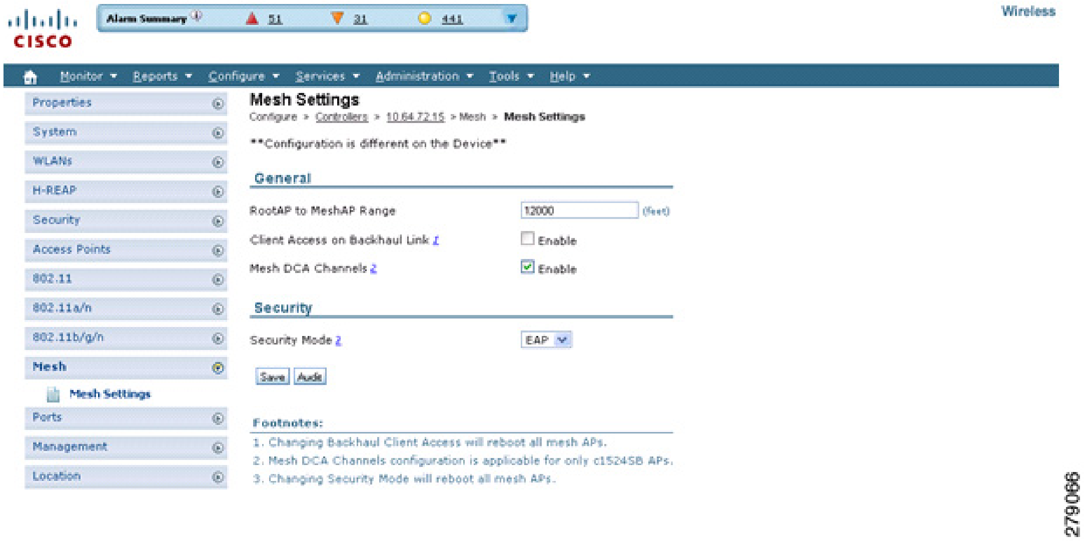
  ```
  All Mesh APs will be rebooted
  Are you sure you want to start? (y/N)
  ```

Configuring Extended Universal Access from Wireless Control System (WCS)

Step 1 Choose **Controllers** > *Controller IP Address* > **Mesh** > **Mesh Settings**.

The WCS Mesh page when Backhaul Client Access is disabled appears as shown in Figure 63.

Figure 63 Mesh Settings Page



Mesh Settings

Configure > Controllers > 10.64.72.15 > Mesh > **Mesh Settings**

Configuration is different on the Device

General

RootAP to MeshAP Range 12000 (feet)

Client Access on Backhaul Link 1 □ Enable

Mesh DCA Channels 2 ☑ Enable

Security

Security Mode 3 EAP

Footnotes:

1. Changing Backhaul Client Access will reboot all mesh APs.
2. Mesh DCA Channels configuration is applicable for only c1524SB APs.
3. Changing Security Mode will reboot all mesh APs.

Step 2 Select the **Client Access on Backhaul Link** check box to display the Extended Backhaul Client Access check box.

Step 3 Select the **Extended Backhaul Client Access** check box and click **Apply**. A message appears indicating the possible results of enabling the Extended Backhaul Client Access.

Step 4 Click **OK** to continue.

Configuring Advanced Features

See the following sections:

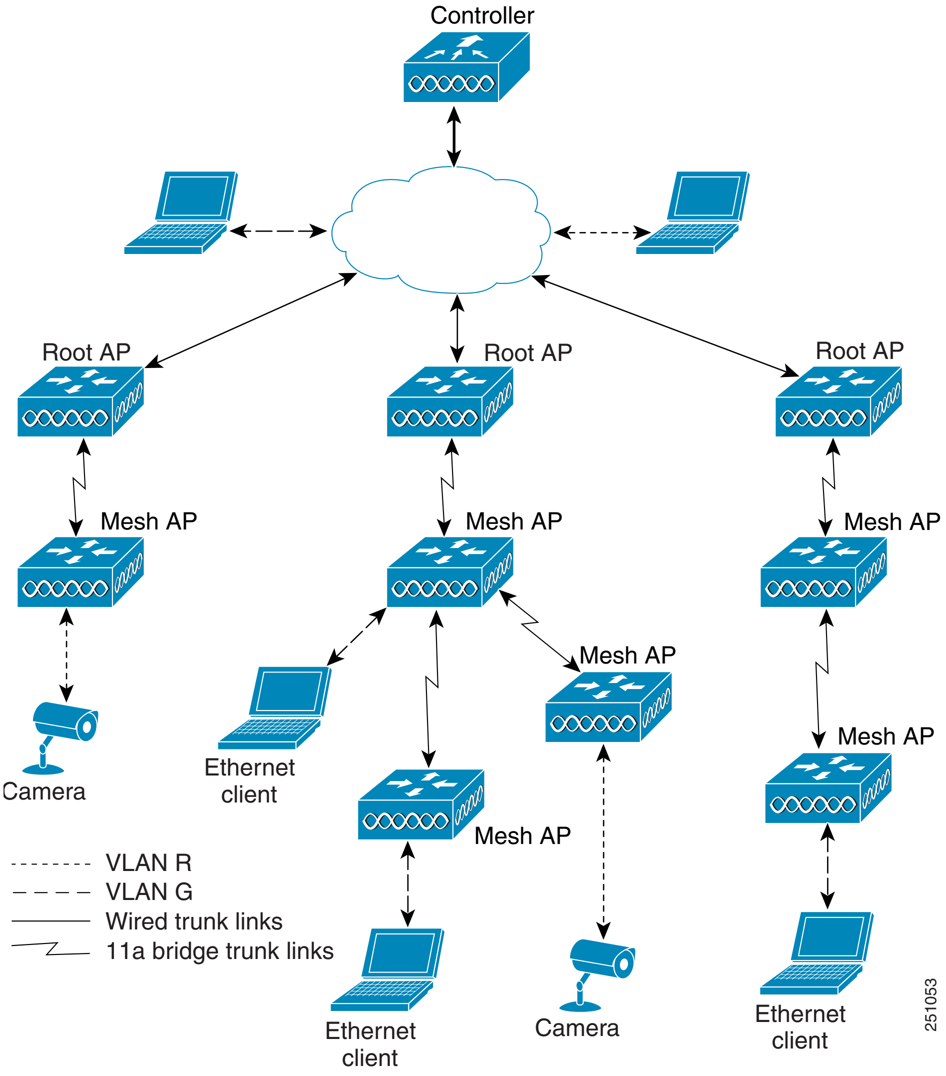
- Configuring Ethernet VLAN Tagging, page 106
- Workgroup Bridge Interoperability with Mesh Infrastructure, page 114
- Client Roaming, page 124
- Configuring Voice Parameters in Indoor Mesh Networks, page 127
- Enabling Mesh Multicast Containment for Video, page 138

Configuring Ethernet VLAN Tagging

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 that uses Ethernet VLAN tagging is the 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 64).

Figure 64 Ethernet VLAN Tagging



Ethernet Port Notes

- Ethernet VLAN tagging allows Ethernet ports to be configured as normal, access, or trunk in both indoor and outdoor implementations.

Note When VLAN Transparent is disabled, the default Ethernet port mode is normal. VLAN Transparent must be disabled for VLAN tagging to operate and to allow configuration of Ethernet ports. To disable VLAN Transparent, a global parameter, see the "Configuring Global Mesh Parameters" section on page 76.

- Normal mode–In this mode, the Ethernet port does not accept or send any tagged packets. Tagged frames from clients are dropped.

  Use the normal mode in applications when only a single VLAN is in use or there is no need to segment traffic in the network across multiple VLANs.
- Access Mode–In this mode, only untagged packets are accepted. All incoming packets are tagged with user-configured VLANs called access-VLAN.

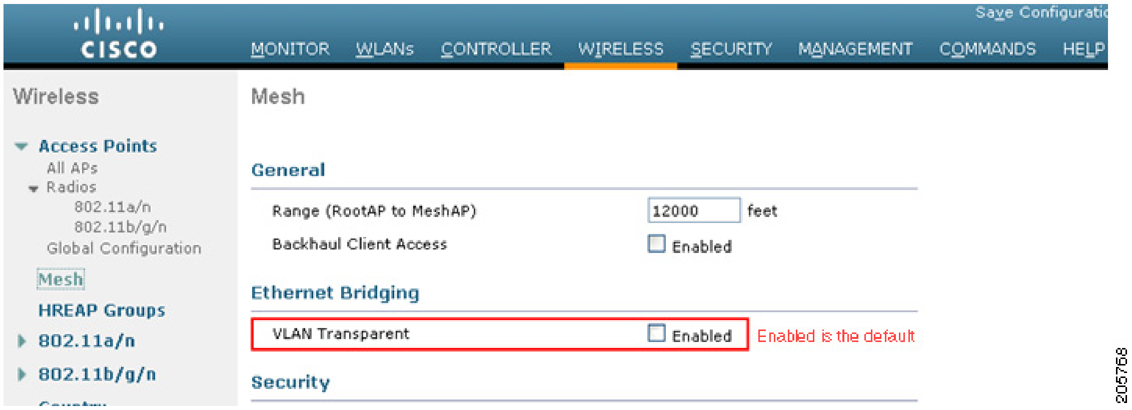
  Use the access mode for applications in which information is collected from devices connected to the MAP such as cameras or PCs and then forwarded to the RAP. The RAP then applies tags and forwards traffic to a switch on the wired network.
- Trunk mode–This mode requires the user to configure a native VLAN and an allowed VLAN list (no defaults). In this mode, both tagged and untagged packets are accepted. Untagged packets are 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.
- Use the trunk mode for bridging applications such as forwarding traffic between two MAPs resident on separate buildings within a campus.

- Ethernet VLAN tagging operates on Ethernet ports that are not used as backhauls.

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 mesh 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). See the "Configuring Global Mesh Parameters - Using the CLI" section on page 80.
  - VLAN transparent is enabled by default. To set as non-VLAN transparent, you must deselect the VLAN transparent option in the global mesh parameters page (see Figure 65).

Figure 65 Wireless > Mesh Page



Mesh

General

Range (RootAP to MeshAP) 12000 feet

Backhaul Client Access ☐ Enabled

Ethernet Bridging

VLAN Transparent ☐ Enabled

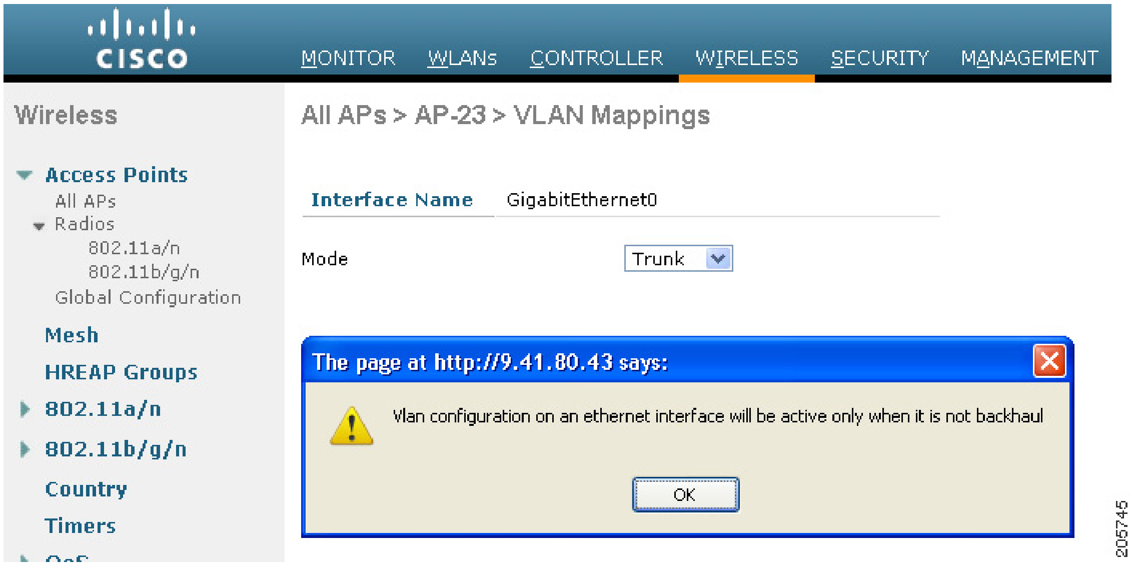
Enabled is the default

- VLAN tagging can only be configured on Ethernet interfaces.
  - On AP1520s, 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.
- For indoor mesh networks (AP1130, AP1240), the VLAN tagging feature functions as it does for outdoor mesh networks. Any access port that is not acting as a backhaul is *secondary* and can be used for VLAN tagging.
- VLAN tagging cannot be implemented on RAPs because the RAPs do not have a secondary Ethernet port, and the primary port is used as a backhaul. However, VLAN tagging can be enabled on MAPs with a single Ethernet port because the Ethernet port on a MAP does not function as a backhaul and is therefore a secondary port.
- No configuration changes are applied to any Ethernet interface acting as a backhaul. A warning displays if you attempt to modify the backhaul's configuration. The configuration is only applied after the interface is no longer acting as backhaul (see Figure 66).

Figure 66 Warning Message Displays for Backhaul Configuration Attempts



All APs > AP-23 > VLAN Mappings

Interface Name GigabitEthernet0

Mode Trunk

The page at http://9.41.80.43 says:

Vlan configuration on an ethernet interface will be active only when it is not backhaul

- 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 AP1520s. VLANs can be configured on ports 0 (PoE-in), 1 (PoE-out), and 3 (fiber).
- Up to 16 VLANs are supported on each sector. Therefore, the cumulative number of VLANs supported by a RAP's children (MAP) cannot exceed 16.
- The switch port connected to the RAP must be a trunk.

  - The trunk port on the switch and the RAP trunk port must match.
  - 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.
  - 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 VLANs, other than those destined for the mesh sector, should be configured on the switch trunk port.
- A configured VLAN on a MAP Ethernet port cannot function as a Management VLAN.
- Configuration is effective only when an mesh access point is in CAPWAP RUN state and VLAN-Transparent mode is disabled.
- Whenever there is a case of roaming or CAPWAP restart, an attempt is made to apply configuration again.

VLAN Registration

To support a VLAN on a mesh access point, all the uplink mesh access points must also support the same VLAN to allow segregation of traffic that belongs to different VLANs. The activity by which an mesh access point communicates its requirements for a VLAN and gets response from a parent is known as VLAN registration.

Note VLAN registration occurs automatically. No user intervention is required.

The steps of VLAN registration are summarized below:

1. Whenever an Ethernet port on a mesh access point is configured with a VLAN, the port requests its parent to support that VLAN.
2. If the parent is able to support the request, it creates a bridge group for the VLAN and propagates the request to its parent. This propagation continues until the RAP is reached.
3. When the request reaches the RAP, it checks whether it is able to support the VLAN request. If yes, the RAP creates a bridge group and a sub-interface on its uplink Ethernet interface to support the VLAN request.
4. If the mesh access point is not able to support the VLAN request by its child, at any point, the mesh access point replies with a negative response. This response is propagated to downstream mesh access points until the mesh access point which requested the VLAN is reached.
5. Upon receiving the negative response from its parent, the requesting mesh access point defers the configuration of the VLAN. However, the configuration is stored for future attempts. Given the dynamic nature of mesh, another parent and its uplink mesh access points might be able to support it in the case of roaming or a CAPWAP reconnect.

Using the GUI to Enable Ethernet VLAN Tagging

You must enable Ethernet bridging before you can configure VLAN tagging. See the "Configuring Ethernet Bridging" procedure on page 82.

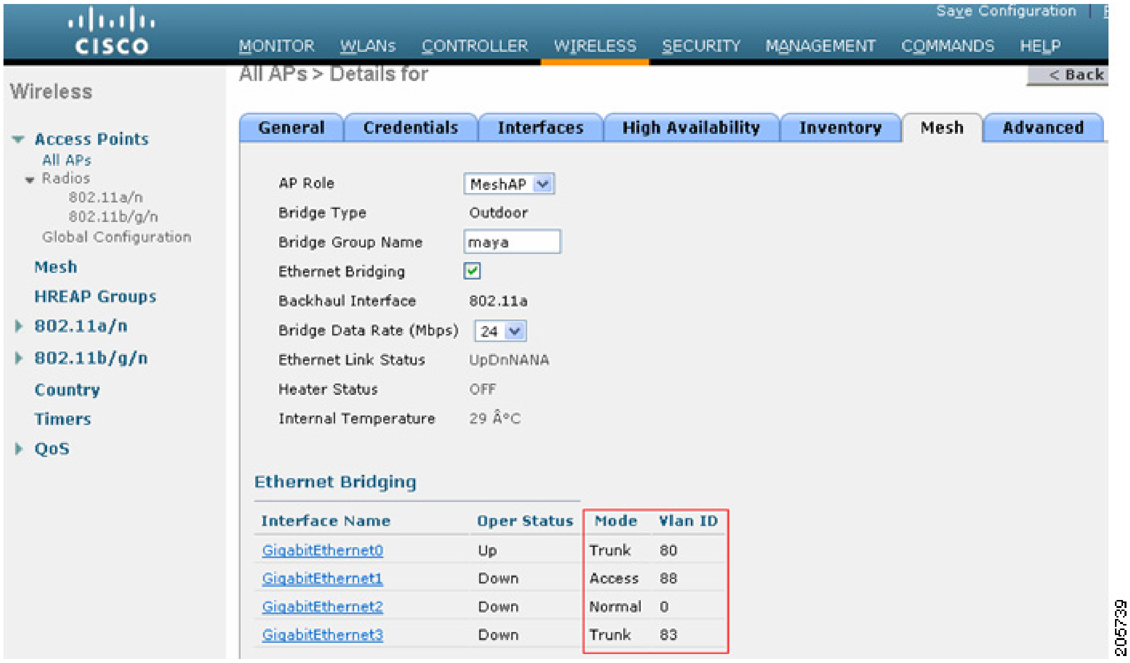
To enable VLAN tagging on a RAP or MAP using the GUI, follow these steps:

Step 1 After enabling Ethernet bridging, choose **Wireless > All APs**.

Step 2 Click the AP name link of the mesh access point on which you want to enable VLAN tagging.

Step 3 On the details page, select the **Mesh** tab. (See Figure 67.)

Figure 67 All APs > Details for (Mesh) Page



AP Role: MeshAP
Bridge Type: Outdoor
Bridge Group Name: maya
Ethernet Bridging: ☑
Backhaul Interface: 802.11a
Bridge Data Rate (Mbps): 24
Ethernet Link Status: UpDnNANA
Heater Status: OFF
Internal Temperature: 29 Â°C

Ethernet Bridging

Interface Name	Oper Status	Mode	Vlan ID
GigabitEthernet0	Up	Trunk	80
GigabitEthernet1	Down	Access	88
GigabitEthernet2	Down	Normal	0
GigabitEthernet3	Down	Trunk	83

Step 4 Select the **Ethernet Bridging** check box to enable the feature and click **Apply**.

An Ethernet Bridging section appears at the bottom of the page listing each of the four Ethernet ports of the mesh access point.

- If configuring a MAP *access* port, click, for example, **gigabitEthernet1** (port 1-PoE out).

  a. Select **access** from the mode drop-down list. (See Figure 68.)

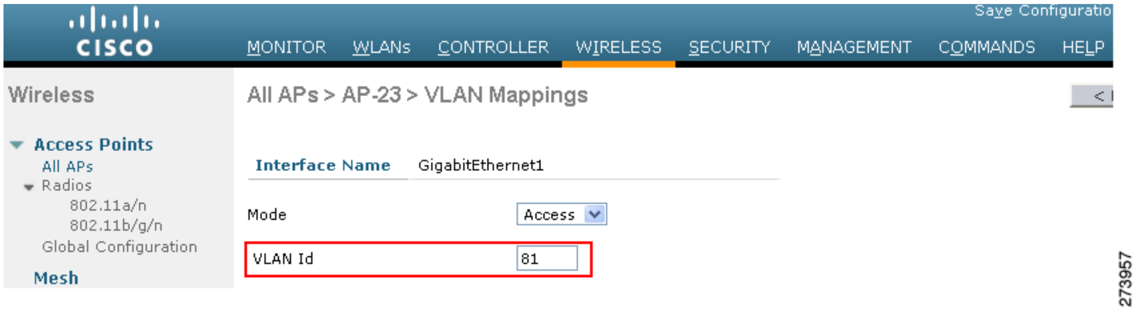
  b. Enter a VLAN ID. The VLAN ID can be any value between 1 and 4095.

  c. Click **Apply**.

Note VLAN ID 1 is not reserved as the default VLAN.

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

Figure 68 VLAN Access Mode



All APs > AP-23 > VLAN Mappings

Interface Name GigabitEthernet1

Mode Access

VLAN Id 81

- If configuring a RAP or MAP *trunk* port, click **gigabitEthernet0** (port 0-PoE in).

   a. Select **trunk** from the mode drop-down menu. (See Figure 69.)

   b. Specify a native VLAN ID for *incoming* traffic. The native VLAN ID can be any value between 1 and 4095. Do not assign any value assigned to a user-VLAN (access).

   c. Click **Apply**.

   A trunk VLAN ID field and a summary of configured VLANs appears at the bottom of the screen. The trunk VLAN ID field is for outgoing packets.

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

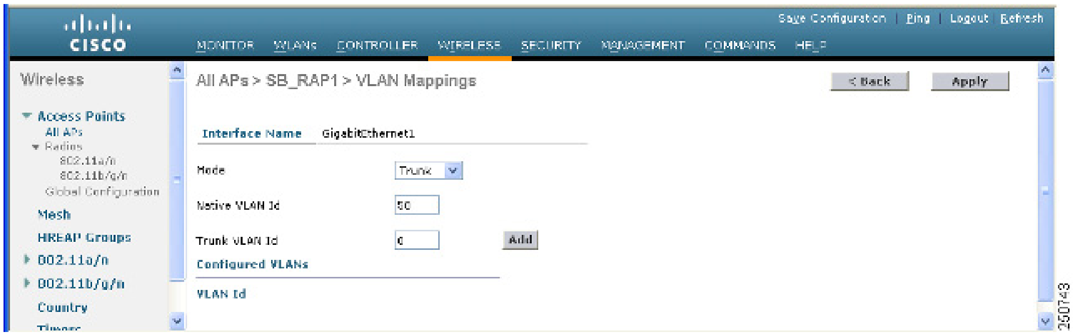
   If forwarding *untagged* packets, do not change the default trunk VLAN ID value of zero. (MAP-to-MAP bridging, campus environment)

   If forwarding *tagged* packets, enter a VLAN ID (1 to 4095) that is not already assigned. (RAP to switch on wired network).

   e. 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 page.

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

Figure 69 All APs > AP > VLAN Mappings Page



All APs > SB_RAP1 > VLAN Mappings

Interface Name GigabitEthernet1

Mode Trunk

Native VLAN Id 50

Trunk VLAN Id 0

Configured VLANs

VLAN Id

Step 5 Click **Apply**.

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

Using the CLI to Configure Ethernet VLAN Tagging

- 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 *AP_name* 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 *AP_name* and *60* is the variable *native_vlan ID*

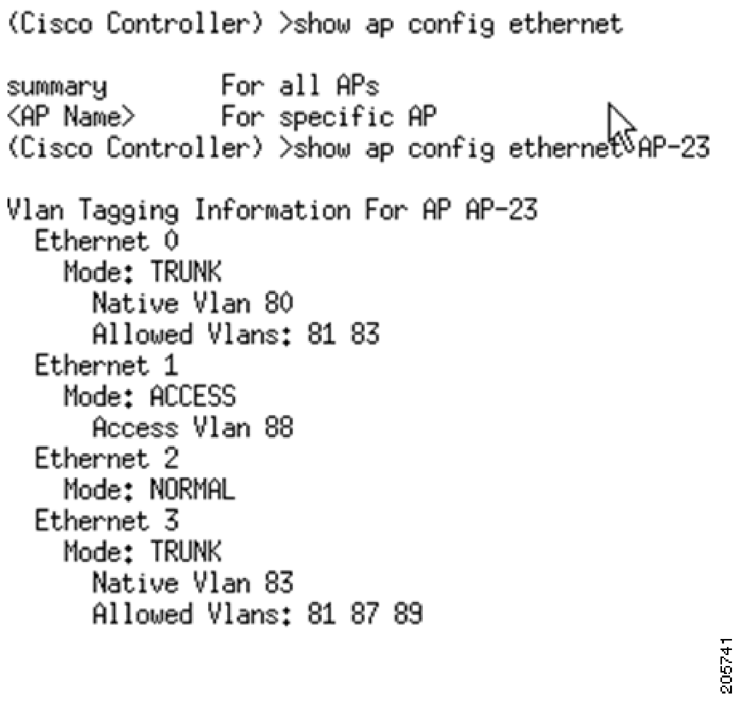
  - To add a VLAN to the VLAN allowed list of the native VLAN, enter this command:

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

    where *AP1522-MAP 3* is the variable *AP_name* and *65* is the variable *VLAN ID*

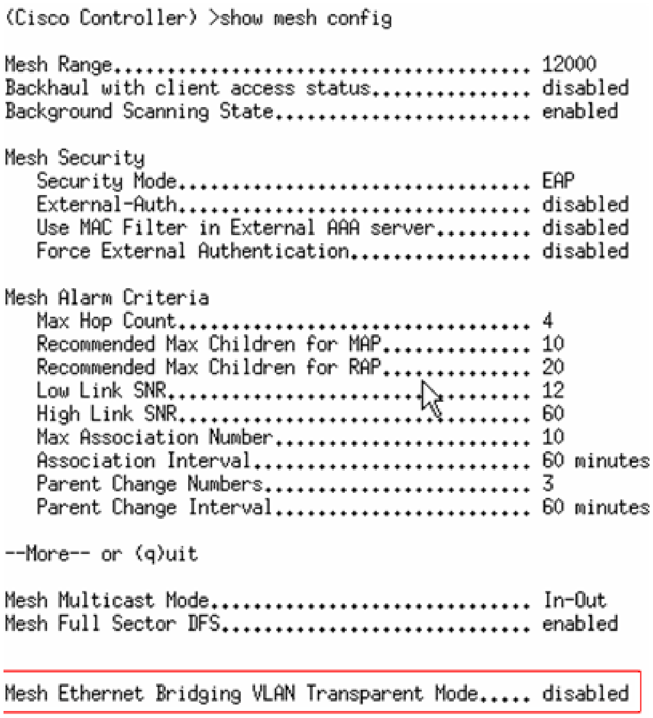
Using the CLI to View Ethernet VLAN Tagging Configuration Details

- To view VLAN configuration details for Ethernet interfaces on a specific mesh access point (*AP Name*) or all mesh access points (*summary*), enter one of the following commands:



```
(Cisco Controller) >show ap config ethernet

summary        For all APs
<AP Name>      For specific AP
(Cisco Controller) >show ap config ethernet AP-23

Vlan Tagging Information For AP AP-23
  Ethernet 0
    Mode: TRUNK
      Native Vlan 80
      Allowed Vlans: 81 83
  Ethernet 1
    Mode: ACCESS
      Access Vlan 88
  Ethernet 2
    Mode: NORMAL
  Ethernet 3
    Mode: TRUNK
      Native Vlan 83
      Allowed Vlans: 81 87 89
```

- To see if VLAN transparent mode is enabled or disabled, enter the following command:



```
(Cisco Controller) >show mesh config

Mesh Range....................................... 12000
Backhaul with client access status............... disabled
Background Scanning State........................ enabled

Mesh Security
   Security Mode................................. EAP
   External-Auth................................. disabled
   Use MAC Filter in External AAA server......... disabled
   Force External Authentication................. disabled

Mesh Alarm Criteria
   Max Hop Count................................. 4
   Recommended Max Children for MAP.............. 10
   Recommended Max Children for RAP.............. 20
   Low Link SNR.................................. 12
   High Link SNR................................. 60
   Max Association Number........................ 10
   Association Interval.......................... 60 minutes
   Parent Change Numbers......................... 3
   Parent Change Interval........................ 60 minutes

--More-- or (q)uit

Mesh Multicast Mode.............................. In-Out
Mesh Full Sector DFS............................. enabled

Mesh Ethernet Bridging VLAN Transparent Mode..... disabled
```

205742

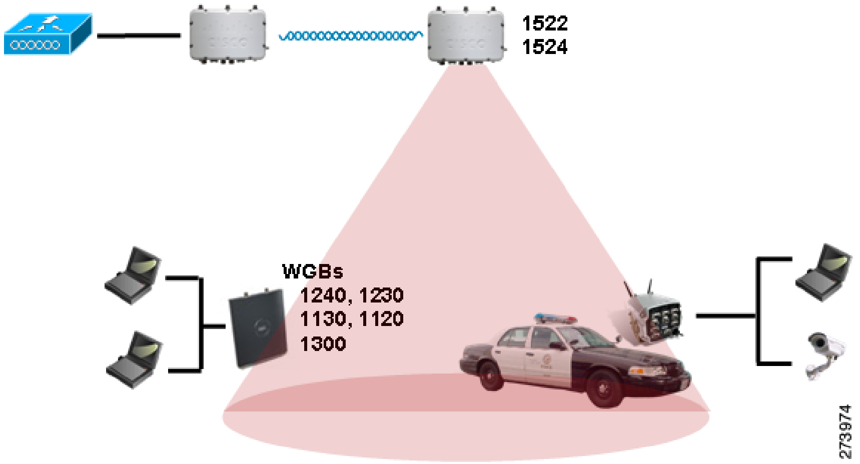
Workgroup Bridge Interoperability with Mesh Infrastructure

A workgroup bridge (WGB) is a small stand-alone unit that can provide a wireless infrastructure connection for Ethernet-enabled devices. Devices that do not have a wireless client adapter to connect to the wireless network can be connected to the WGB through the Ethernet port. The WGB is associated with the root AP through the wireless interface. Thus, wired clients get access to the wireless network.

A WGB is used to connect wired networks over a single wireless segment. This is accomplished by informing the mesh access point of all the clients that the WGB has on its wired segment via IAPP messages. The data packets for WGB clients contain an additional MAC address in the 802.11 header (4 MAC header, versus the normal 3 MAC data headers). The additional MAC in the header is the address of the WGB itself. This additional MAC address is used to route the packet to and from the clients.

WGB association is supported on all radios of every mesh access point (see Figure 70).

Figure 70 WGB Example



In the current architecture, while an autonomous AP functions as a workgroup bridge, only one radio interface is used for controller connectivity, Ethernet interface for wired client connectivity, and other radio interface for wireless client connectivity. dot11radio 1 (5 GHz) can be used to connect to a controller (using the mesh infrastructure) and Ethernet interface for wired clients. dot11radio 0 (2.4 GHz) can be used for wireless client connectivity. Depending on the requirement, dot11radio 1 or dot11radio 0 can be used for client association or controller connectivity.

With the 7.0 release, the wireless clients on the second radio of the WGB are not dissociated by the WGB upon losing its uplink to a wireless infrastructure or in a roaming scenario.

With two radios, one radio can be used for client access and the other radio can be used for accessing the access points. Having two independent radios performing two independent functions provides you better control and lowers the latency. Also, wireless clients on the second radio for the WGB do not get disassociated by the WGB when an uplink is lost or in a roaming scenario. One radio has to be configured as Root AP (radio role) and the second radio has to be configured as a WGB (radio role).

Note If one radio is configured as a WGB, then the second radio cannot be a WGB or a repeater.

The following features are not supported for use with a WGB:

- Hybrid REAP
- Idle timeout
- Web authentication — If a WGB associates to a web-authentication WLAN, the WGB is added to the exclusion list, and all of the WGB wired clients are deleted (Web-authentication WLAN is another name for a guest WLAN).
- For wired clients behind the WGB, MAC filtering, link tests, and idle timeout

Configuring Workgroup Bridges

A workgroup bridge (WGB) is used to connect wired networks over a single wireless segment. It does this by informing the mesh access point of all the clients that the WGB has on its wired segment via IAPP messages. In addition to the IAPP control messages, the data packets for WGB clients contain an extra

MAC address in the 802.11 header (4 MAC header, versus the normal 3 MAC data headers). The extra MAC in the header is the address of the workgroup bridge itself. This extra MAC address is used to route the packet to and from the clients.

WGB association is supported on both the 2.4-GHz (802.11b/g) and 5-GHz (802.11a) radios on the AP1522, and the 2.4-GHz (802.11b) and 4.9-GHz (public safety) radios on the AP1524PS;

Supported platforms are autonomous WGBs AP1130, AP1240, AP1310, and the Cisco 3200 Mobile Router (*hereafter* referred to as Cisco 3200) which configured as WGB can associate with a mesh access point. See the “Cisco Workgroup Bridges” section in Chapter 7 of the *Cisco Wireless LAN Controller Configuration Guide, Release 6.0* for configuration steps at:
http://www.cisco.com/en/US/products/ps6366/products_installation_and_configuration_guides_list.html

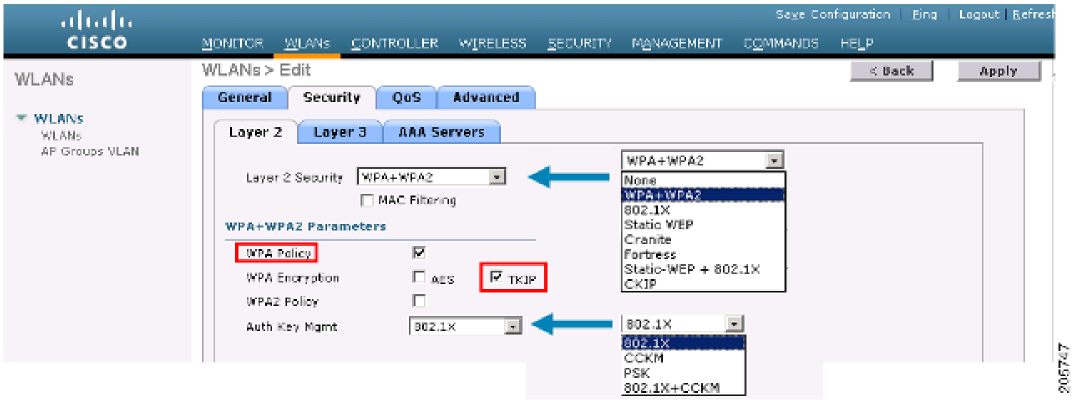
Supported Workgroup Bridge Modes and Capacities

- The 1130, 1240, and 1310 autonomous mesh access points 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. We recommend that you disable the second radio. Workgroup bridge mode is not supported on access points with three radios such as the AP1524.

- Client mode WGB (BSS) is supported; however, infrastructure WGB is not supported. The client mode WGB is not able to trunk VLAN as in an infrastructure WGB.
- Multicast traffic is not reliably transmitted to WGB because no ACKs are returned by the client. Multicast traffic is unicast to infrastructure WGB, and ACKs are received back.
- If one radio is configured as WGB in a Cisco IOS access point, then the second radio cannot be a WGB or a repeater.
- Mesh access points can support up to 200 clients including wireless clients, WGB, and wired clients behind the associated WGB.
- WGB 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):
  - Figure 71 displays WPA security settings for WGB (controller GUI).
  - Figure 72 displays WPA-2 security settings for WGB (controller GUI).

Figure 71 WPA Security Settings for WGB



WLANs > Edit

Layer 2 Security: WPA+WPA2

☐ MAC Filtering

WPA+WPA2 Parameters

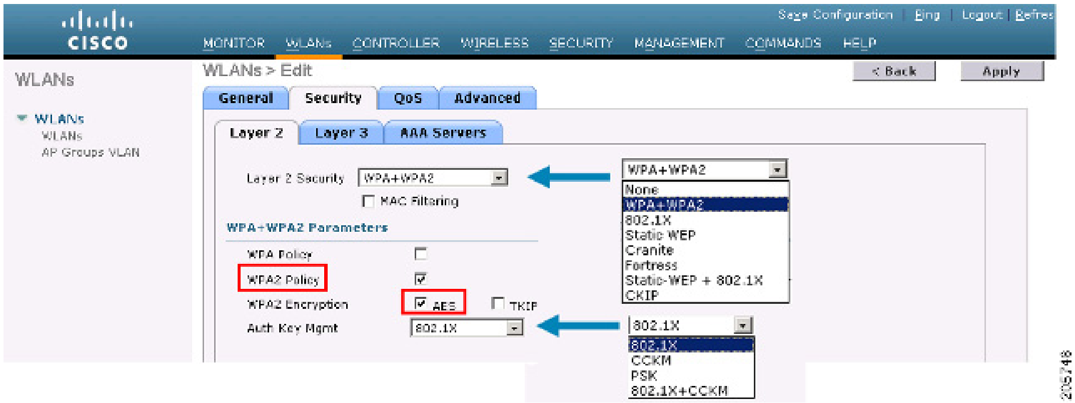
WPA Policy ☑

WPA Encryption ☐ AES ☑ TKIP

WPA2 Policy ☐

Auth Key Mgmt: 802.1X

Figure 72 WPA-2 Security Settings for WGB



WLANs > Edit

Layer 2 Security: WPA+WPA2

☐ MAC Filtering

WPA+WPA2 Parameters

WPA Policy ☐

WPA2 Policy ☑

WPA2 Encryption ☑ AES ☐ TKIP

Auth Key Mgmt: 802.1X

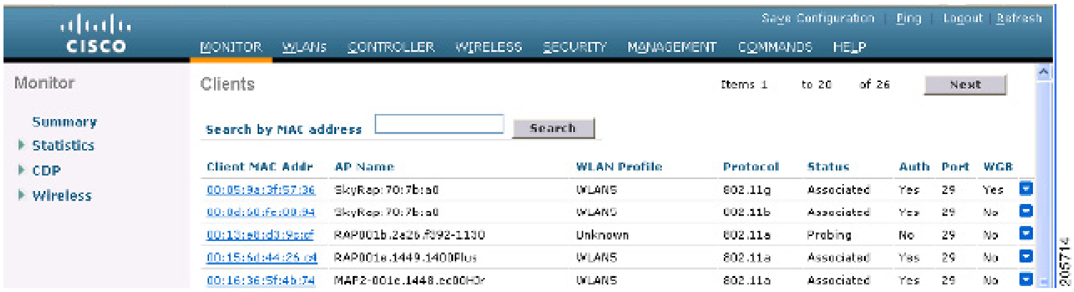
To view the status of a WGB client, follow these steps:

Step 1 Choose **Monitor > Clients**.

Step 2 On the client summary page, click on the MAC address of the client or search for the client using its MAC address.

Step 3 In the page that appears, note that the client type is identified as *WGB* (far right). (See Figure 73.)

Figure 73 Clients are Identified as WGB


CISCO
Save Configuration | Ping | Logout | Refresh
MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP
Monitor
Summary
Statistics
CDP
Wireless
Next
Search
206714

Clients

Items 1 to 20 of 26

Search by MAC address

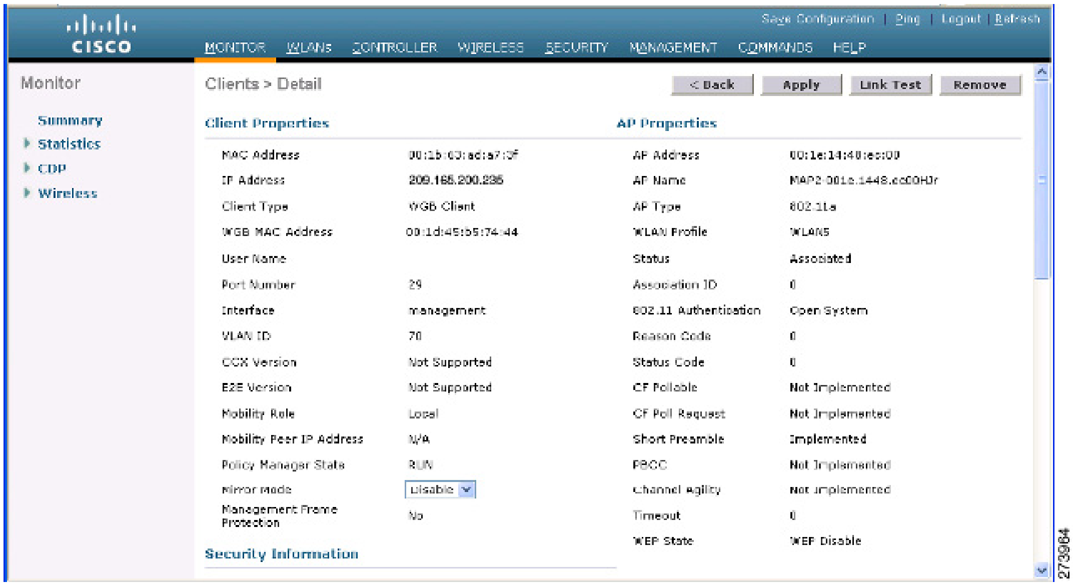
Client MAC Addr	AP Name	WLAN Profile	Protocol	Status	Auth	Port	WGB
00:05:9a:3f:57:36	SkyRap:70:7b:a0	WLANS	802.11g	Associated	Yes	29	Yes
00:0d:60:fe:00:94	SkyRap:70:7b:a0	WLANS	802.11b	Associated	Yes	29	No
00:13:e8:d3:9c:cf	RAP001b.2a26.f392-1130	Unknown	802.11a	Probing	No	29	No
00:15:6d:44:26:cd	RAP001e.1449.1400Plus	WLANS	802.11a	Associated	Yes	29	No
00:16:36:5f:4b:74	MAP2-001e.1448.ec00HDr	WLANS	802.11a	Associated	Yes	29	No

Step 4 Click on the MAC address of the client to view configuration details.

- For a wireless client, the page seen in Figure 74 appears.

- For a wired client, the page seen in Figure 75 appears.

Figure 74 Monitor > Clients > Detail Page (Wireless WGB Client)


Save Configuration | Ping | Logout | Refresh
CISCO
MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP
Monitor
Summary
Statistics
CDP
Wireless
< Back
Apply
Link Test
Remove
273964

Clients > Detail

Client Properties

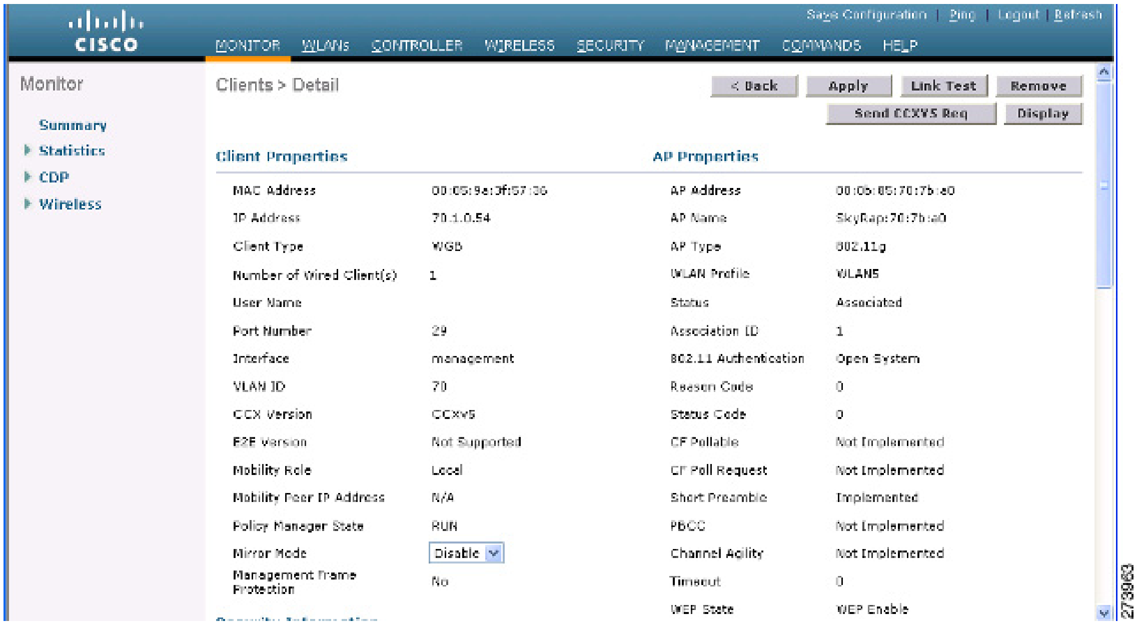
MAC Address	00:1b:d3:ad:a7:3f
IP Address	209.165.200.236
Client Type	WGB Client
WGB MAC Address	00:1d:45:55:74:44
User Name	
Port Number	29
Interface	management
VLAN ID	70
CCX Version	Not Supported
E2E Version	Not Supported
Mobility Role	Local
Mobility Peer IP Address	N/A
Policy Manager State	RUN
Mirror Mode	Disable
Management Frame Protection	No

AP Properties

AP Address	00:1e:14:48:ec:00
AP Name	MAP2-001e.1448.ec00HJr
AP Type	802.11a
WLAN Profile	WLAN5
Status	Associated
Association ID	0
802.11 Authentication	Open System
Reason Code	0
Status Code	0
CF Pollable	Not Implemented
CF Poll Request	Not Implemented
Short Preamble	Implemented
PBCC	Not Implemented
Channel Agility	Not Implemented
Timeout	0
WEP State	WEP Disable

Security Information

Figure 75 Monitor > Clients > Detail Page (Wired WGB Client)


Save Configuration | Ping | Logout | Refresh
CISCO
MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP
Monitor
Summary
Statistics
CDP
Wireless
< Back
Apply
Link Test
Remove
Send CCXV5 Req
Display
273963

Clients > Detail

Client Properties

MAC Address	00:05:9a:3f:57:36
IP Address	70.1.0.54
Client Type	WGB
Number of Wired Client(s)	1
User Name	
Port Number	29
Interface	management
VLAN ID	70
CCX Version	CCXv5
E2E Version	Not Supported
Mobility Role	Local
Mobility Peer IP Address	N/A
Policy Manager State	RUN
Mirror Mode	Disable
Management Frame Protection	No

AP Properties

AP Address	00:0b:85:70:7b:a0
AP Name	SkyRap:70:7b:a0
AP Type	802.11g
WLAN Profile	WLAN5
Status	Associated
Association ID	1
802.11 Authentication	Open System
Reason Code	0
Status Code	0
CF Pollable	Not Implemented
CF Poll Request	Not Implemented
Short Preamble	Implemented
PBCC	Not Implemented
Channel Agility	Not Implemented
Timeout	0
WEP State	WEP Enable

Guidelines for Configuration

- We recommend using a 5-GHz radio for the uplink to Mesh AP infrastructure so you can take advantage of a strong client access on two 5-GHz radios available on mesh access points. A 5-GHz band allows more Effective Isotropic Radiated Power (EIRP) and is less polluted. In a two-radio WGB, configure 5-GHz radio (radio 1) mode as WGB. This radio will be used to access the mesh infrastructure. Configure the second radio 2.4-GHz (radio 0) mode as Root for client access.
- On the Autonomous access points, only one SSID can be assigned to the native VLAN. You cannot have multiple VLANs in one SSID on the autonomous side. SSID to VLAN mapping should be unique because this is the way to segregate traffic on different VLANs. In a unified architecture, multiple VLANs can be assigned to one WLAN (SSID).
- Only one WLAN (SSID) for wireless association of the WGB to the access point infrastructure is supported. This SSID should be configured as an infrastructure SSID and should be mapped to the native VLAN.
- A dynamic interface should be created in the controller for each VLAN configured in the WGB.
- A second radio (2.4-GHz) on the access point should be configured for client access. You have to use the same SSID on both radios and map to the native VLAN. If you create a separate SSID, then it is not possible to map it to a native VLAN, due to the unique VLAN/SSID mapping requirements. If you try to map the SSID to another VLAN, then you do not have multiple VLAN support for wireless clients.
- All Layer 2 security types are supported for the WLANs (SSIDs) for wireless client association in WGB.
- This feature does not depend on the AP platform. On the controller side, both mesh and non-mesh APs are supported.
- There is a limitation of 20 clients in the WGB. The 20-client limitation includes both wired and wireless clients. If the WGB is talking to autonomous access points, then the client limit is very high.
- The controller treats the wireless and wired clients behind WGB in the same manner. Features such as MAC filtering and link test are not supported for wireless WGB clients from the controller.
- If required, you can run link tests for a WGB wireless client from autonomous AP.
- Multiple VLANs for wireless clients associated to WGB are not supported.
- Up to 16 multiple VLANs are supported for wired clients behind WGB from the 7.0 release and later releases.
- Roaming is supported for wireless and wired clients behind WGB. The wireless clients on the other radio will not be dissociated by the WGB when an uplink is lost or in a roaming scenario.

We recommend that you configure radio 0 (2.4 GHz) as a Root (one of the mode of operations for Autonomous AP) and radio 1 (5 GHz) as WGB.

Configuration Example

When you configure from the CLI, the following are mandatory:

- dot11 SSID (security for WLAN can be decided based on the requirement)
- Map the subinterfaces in both the radios to a single bridge group.

Note Native VLAN is always mapped to Bridge Group 1 by default. For other VLANs, Bridge Group number matches VLAN number; for example, for VLAN 46, Bridge Group is 46.

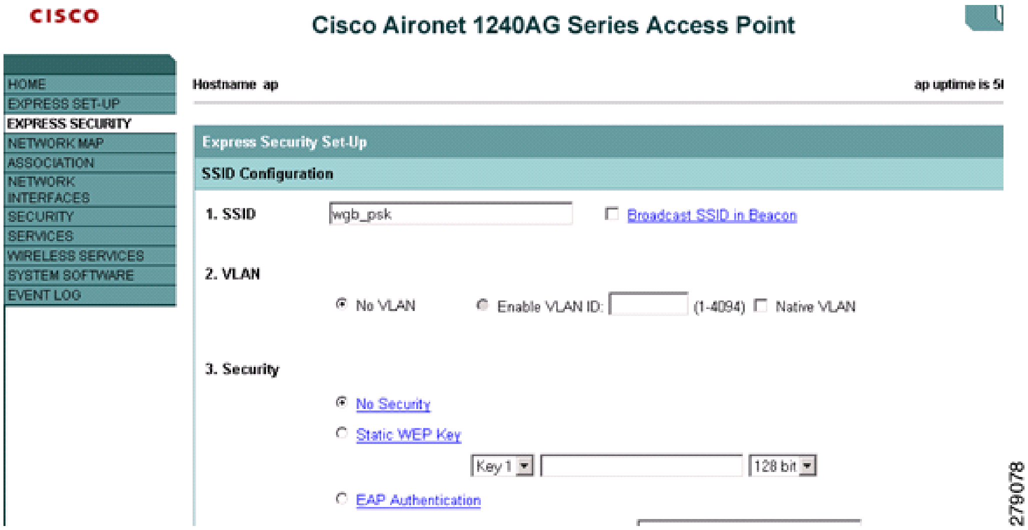
- Map the SSID to the radio interfaces and define the role of the radio interfaces.

In the following example, one SSID (WGBTEST) is used in both radios, and the SSID is infrastructure SSID mapped to NATIVE VLAN 51. All radio interfaces are mapped to bridge group -1.

```
WGB1#config t
WGB1(config)#interface Dot11Radio1.51
WGB1(config-subif)#encapsulation dot1q 51 native
WGB1(config-subif)#bridge-group 1
WGB1(config-subif)#exit
WGB1(config)#interface Dot11Radio0.51
WGB1(config-subif)#encapsulation dot1q 51 native
WGB1(config-subif)#bridge-group 1
WGB1(config-subif)#exit
WGB1(config)#dot11 ssid WGBTEST
WGB1(config-ssid)#VLAN 51
WGB1(config-ssid)#authentication open
WGB1(config-ssid)#infrastructiure-ssid
WGB1(config-ssid)#exit
WGB1(config)#interface Dot11Radio1
WGB1(config-if)#ssid WGBTEST
WGB1(config-if)#station-role workgroup-bridge
WGB1(config-if)#exit
WGB1(config)#interface Dot11Radio0
WGB1(config-if)#ssid WGBTEST
WGB1(config-if)#station-role root
WGB1(config-if)#exit
```

You can also use the GUI of an autonomous AP for configuration (see Figure 76). From the GUI, subinterfaces are automatically created after the VLAN is defined.

Figure 76 SSID Configuration Page



Hostname ap   ap uptime is 5l

Express Security Set-Up

SSID Configuration

1. SSID wgb_psk   □ Broadcast SSID in Beacon

2. VLAN

● No VLAN   ○ Enable VLAN ID: (1-4094) □ Native VLAN

3. Security

● No Security

○ Static WEP Key

Key 1   128 bit

○ EAP Authentication

WGB Association Check

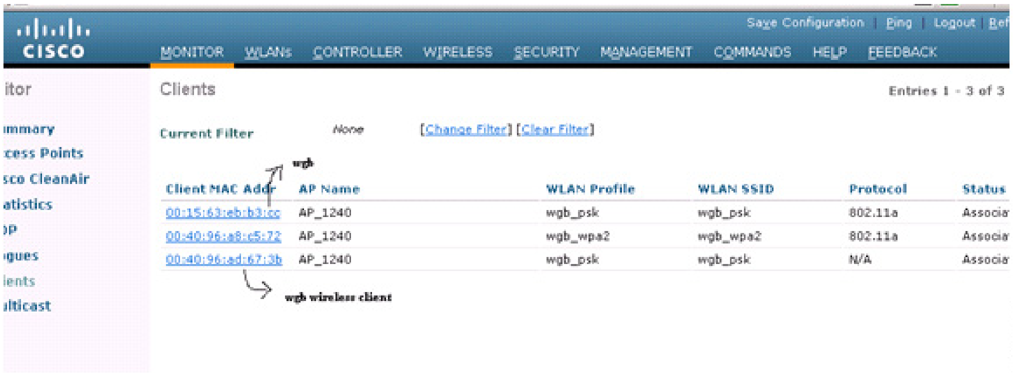
Both the WGB association to the controller and the wireless client association to WGB can be verified by entering the **show dot11 associations client** command in autonomous AP.

```
WGB#show dot11 associations client
```

```
802.11 Client Stations on Dot11Radio1:

SSID [WGBTEST] :

MAC Address        IP Address    Device        Name          Parent        State
0024.130f.920e     209.165.200   LWAPP-Paren   RAPSB         -             Assoc
                   .225          t
```

From the controller, choose **Monitor** > **Clients**. The WGB and the wireless/wired client behind WGB are updated and the wireless/wired client are shown as WGB client, as shown in Figure 77, Figure 78, and Figure 79.

Figure 77 Updated WGB Clients



Save Configuration | Ping | Logout | Ref
MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK
itor
mmary
cess Points
sco CleanAir
atistics
DP
gues
ients
ulticast

Clients

Entries 1 - 3 of 3

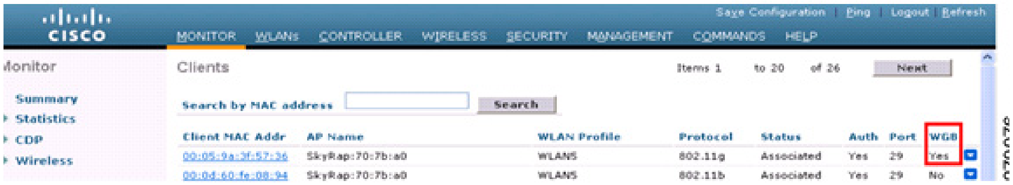
Current Filter None [Change Filter] [Clear Filter]

wgb

Client MAC Addr	AP Name	WLAN Profile	WLAN SSID	Protocol	Status
00:15:63:eb:b3:cc	AP_1240	wgb_psk	wgb_psk	802.11a	Associa
00:40:96:a8:c5:72	AP_1240	wgb_wpa2	wgb_wpa2	802.11a	Associa
00:40:96:ad:67:3b	AP_1240	wgb_psk	wgb_psk	N/A	Associa

wgb wireless client

Figure 78 Updated WGB Clients



Save Configuration | Ping | Logout | Refresh
MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP
Monitor
Summary
Statistics
CDP
Wireless

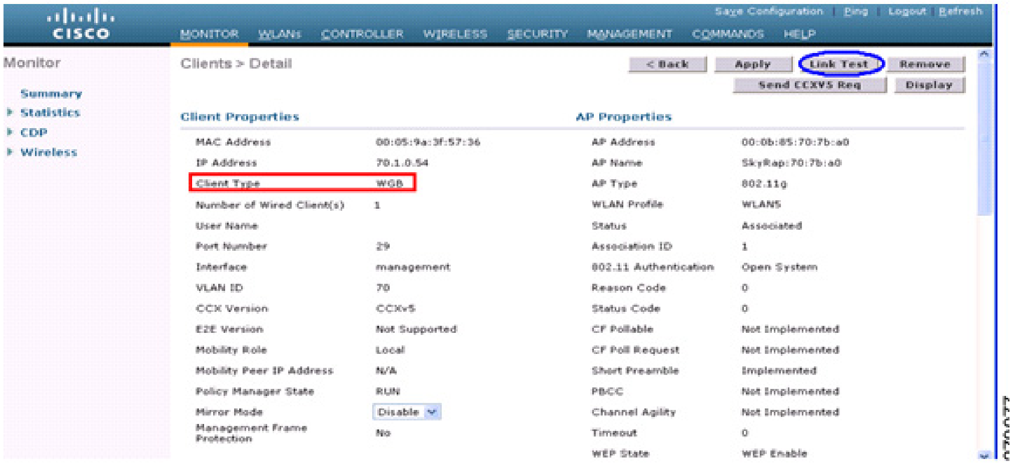
Clients

Items 1 to 20 of 26 Next

Search by MAC address Search

Client MAC Addr	AP Name	WLAN Profile	Protocol	Status	Auth	Port	WGB
00:05:9a:3f:57:36	SkyRap:70:7b:a0	WLANS	802.11g	Associated	Yes	29	Yes
00:0d:60:fe:08:94	SkyRap:70:7b:a0	WLANS	802.11b	Associated	Yes	29	No

Figure 79 Updated WGB Clients



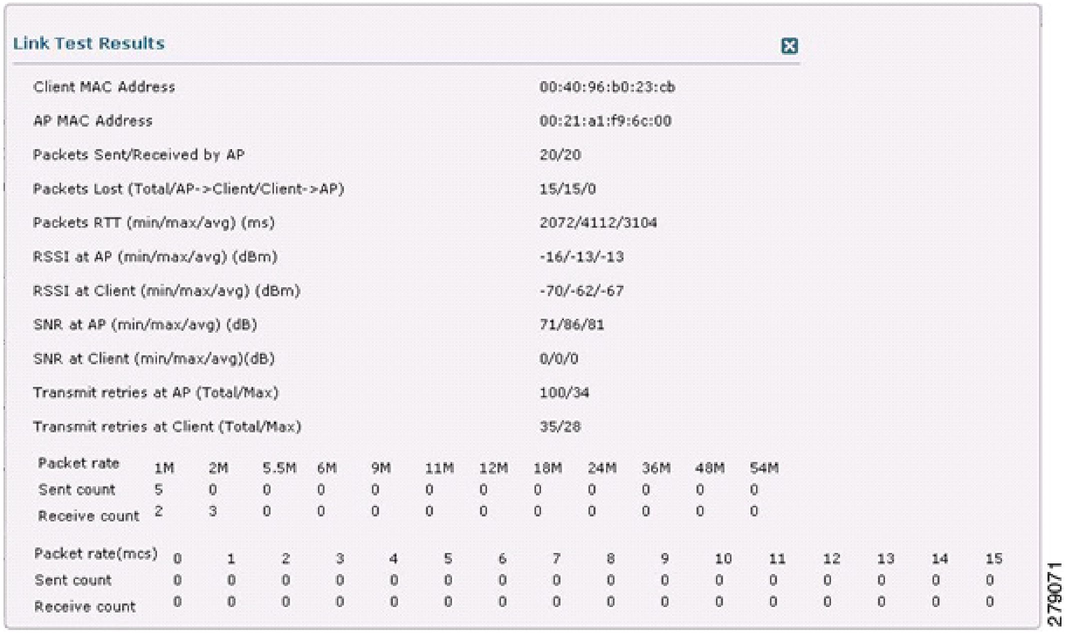
Clients > Detail

Client Properties		AP Properties	
MAC Address	00:05:9a:3f:57:36	AP Address	00:0b:85:70:7b:a0
IP Address	70.1.0.54	AP Name	SkyRap:70:7b:a0
Client Type	WGB	AP Type	802.11g
Number of Wired Client(s)	1	WLAN Profile	WLAN5
User Name		Status	Associated
Port Number	29	Association ID	1
Interface	management	802.11 Authentication	Open System
VLAN ID	70	Reason Code	0
CCX Version	CCXv5	Status Code	0
E2E Version	Not Supported	CF Pollable	Not Implemented
Mobility Role	Local	CF Poll Request	Not Implemented
Mobility Peer IP Address	N/A	Short Preamble	Implemented
Policy Manager State	RUN	PBCC	Not Implemented
Mirror Mode	Disable	Channel Agility	Not Implemented
Management Frame Protection	No	Timeout	0
		WEP State	WEP Enable

Link Test Result

Figure 80 shows the link test results.

Figure 80 Link Test Results



Link Test Results

Client MAC Address	00:40:96:b0:23:cb
AP MAC Address	00:21:a1:f9:6c:00
Packets Sent/Received by AP	20/20
Packets Lost (Total/AP->Client/Client->AP)	15/15/0
Packets RTT (min/max/avg) (ms)	2072/4112/3104
RSSI at AP (min/max/avg) (dBm)	-16/-13/-13
RSSI at Client (min/max/avg) (dBm)	-70/-62/-67
SNR at AP (min/max/avg) (dB)	71/86/81
SNR at Client (min/max/avg)(dB)	0/0/0
Transmit retries at AP (Total/Max)	100/34
Transmit retries at Client (Total/Max)	35/28

Packet rate	1M	2M	5.5M	6M	9M	11M	12M	18M	24M	36M	48M	54M
Sent count	5	0	0	0	0	0	0	0	0	0	0	0
Receive count	2	3	0	0	0	0	0	0	0	0	0	0

Packet rate(mcs)	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Sent count	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Receive count	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

A link test can also be run from the controller CLI using the following command:

```
(Cisco Controller) > linktest client mac address
```

Link tests from the controller are only limited to the WGB, and they cannot be run beyond the WGB from the controller to a wired or wireless client connected to the WGB. You can run link tests for the wireless client connected to the WGB from the WGB itself using the following command:

```
ap#dot11 dot11Radio 0 linktest target client mac
Start linktest to 0040.96b8.d462, 100 512 byte packets
```

```
ap#

   POOR (4% lost)    Time (msec)   Strength (dBm)     SNR Quality        Retries

                                 In       Out      In       Out      In       Out

Sent: 100           Avg. 22      -37      -83      48       3        Tot. 34  35

Lost to Tgt: 4      Max. 112     -34      -78      61       10       Max. 10  5

Lost to Src: 4      Min. 0       -40      -87      15       3


Rates (Src/Tgt)     24Mb 0/5  36Mb 25/0  48Mb 73/0  54Mb 2/91
Linktest Done in 24.464 msec
```

WGB Wired/Wireless Client

You can also use the following commands:

```
(Cisco Controller) > show wgb summary
Number of WGBs................................. 2

MAC Address        IP Address       AP Name  Status   WLAN  Auth  Protocol  Clients

00:1d:70:97:bd:e8  209.165.200.225  c1240    Assoc    2     Yes   802.11a   2

00:1e:be:27:5f:e2  209.165.200.226  c1240    Assoc    2     Yes   802.11a   5


(Cisco Controller) > show client summary

Number of Clients.............................. 7

MAC Address        AP Name  Status      WLAN/Guest-Lan  Auth  Protocol  Port    Wired

00:00:24:ca:a9:b4  R14      Associated  1               Yes   N/A       29      No

00:24:c4:a0:61:3a  R14      Associated  1               Yes   802.11a   29      No

00:24:c4:a0:61:f4  R14      Associated  1               Yes   802.11a   29      No

00:24:c4:a0:61:f8  R14      Associated  1               Yes   802.11a   29      No

00:24:c4:a0:62:0a  R14      Associated  1               Yes   802.11a   29      No

00:24:c4:a0:62:42  R14      Associated  1               Yes   802.11a   29      No

00:24:c4:a0:71:d2  R14      Associated  1               Yes   802.11a   29      No


(Cisco Controller) > show wgb detail 00:1e:be:27:5f:e2

Number of wired client(s): 5

MAC Address        IP Address        AP Name     Mobility   WLAN  Auth

00:16:c7:5d:b4:8f  Unknown           c1240       Local      2     No
```

```
00:21:91:f8:e9:ae  209.165.200.232   c1240       Local      2     Yes

00:21:55:04:07:b5  209.165.200.234   c1240       Local      2     Yes

00:1e:58:31:c7:4a  209.165.200.236   c1240       Local      2     Yes

00:23:04:9a:0b:12  Unknown           c1240       Local      2     No
```

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 AP1522s and AP1524s. An example application 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.

For more information, see the Enterprise Mobility Design Guide at http://www.cisco.com/en/US/docs/solutions/Enterprise/Mobility/emob41dg/eMob4.1.pdf

WGB Roaming Guidelines

Follow these guidelines for WGB roaming:

- Configuring a WGB for roaming—If a WGB is mobile, you can configure it to scan for a better radio connection to a parent access point or bridge. Use this command to configure the workgroup bridge as a mobile station:

  ap(config-if)#**mobile station period 3 threshold 50**

  When you enable this setting, the WGB scans for a new parent association when it encounters a poor Received Signal Strength Indicator (RSSI), excessive radio interference, or a high frame-loss percentage. Using these criteria, a WGB configured as a mobile station searches for a new parent association and roams to a new parent before it loses its current association. When the mobile station setting is disabled (the default setting), a WGB does not search for a new association until it loses its current association.

- Configuring a WGB for Limited Channel Scanning—In mobile environments such as railroads, a WGB instead of scanning all the channels will be restricted to scan only a set of limited channels to reduce the hand-off delay when the WGB roams from one access point to another. By limiting the number of channels, the WGB scans to only those required; the mobile WGB achieves and maintains a continuous wireless LAN connection with fast and smooth roaming. This limited channel set is configured using the following command:

  ap(config-if)#**mobile station scan** *set of channels*

  This command invokes scanning to all or specified channels. There is no limitation on the maximum number of channels that can be configured. The maximum number of channels that can be configured is restricted only by the number of channels that a radio can support. When executed, the WGB scans only this limited channel set. This limited channel feature also affects the known channel list that the WGB receives from the access point to which it is currently associated. Channels are added to the known channel list only if they are also part of the limited channel set.

Configuration Example

The following example shows how to configure a roaming configuration:

```
ap(config)#interface dot11radio 1
ap(config-if)#ssid outside
ap(config-if)#packet retries 16
ap(config-if)#station role workgroup-bridge
ap(config-if)#mobile station
ap(config-if)#mobile station period 3 threshold 50
ap(config-if)#mobile station scan 5745 5765
```

Use the **no mobile station scan** command to restore scanning to all the channels.

Configuring Interoperability with the Cisco 3200

Cisco AP1522 and AP1524PS can interoperate with the Cisco 3200 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.

This section provides configuration guidelines and step-by-step instructions for configuring interoperability between the Cisco 3200 and the AP1522 and the AP1524PS.

For specific interoperability details between series 1130, 1240, and 1520 (1522, 1524PS) mesh access points and Cisco 3200, see Table 15.

Table 15 Mesh Access Points and Cisco 3200 Interoperability

Mesh Access Point Model	Cisco 3200 Model
1522[1]	c3201[2], c3202[3], c3205[4]
1524PS	c3201, c3202
1524SB, 1523CV, 1130, 1240	c3201, c3205

1. Universal access must be enabled on the AP1522 if connecting to a Cisco 3200 on the 802.11a radio or 4.9-GHz band.
2. Model c3201 is a Cisco 3200 with a 802.11b/g radio (2.4-GHz).
3. Model c3202 is a Cisco 3200 with a 4-9-GHz sub-band radio.
4. Model c3205 is a Cisco 3200 with a 802.11a radio (5.8-GHz sub-band).

Table 16 identifies mesh access points and their respective frequency bands that support WGB.

Table 16 WGB Interoperability Chart

RAP/MAP	**WGB**								
	MAR3200			1240/1250		1130		1310	
Backhaul	4.9 GHz (5, 10, 20 MHz)	5 GHz	2.4 GHz	5 GHz	2.4 GHz	5 GHz	2.4 GHz	5 GHz	2.4 GHz
1524SB/1524SB	No	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes
1524PS/1524PS	Yes	No	Yes	No	Yes	No	Yes	No	Yes
1522/1522	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes
1524SB/1522	No	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes
1524PS/1522	No	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes
1522/1524SB	No	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes
1522/1524PS	Yes	No	Yes	No	Yes	No	Yes	No	Yes
1240/1130	No	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes

Configuration Guidelines for Public Safety 4.9-GHz Band

For the AP1522 or AP1524PS and Cisco 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). This feature is not supported on the AP1524PS.
- Public safety must be enabled globally on all mesh access points (MAPs) in the mesh network.
- Channel number assignment on the AP1522 or AP1524PS must match those on the Cisco 3200 radio interfaces.
  - Channels 20 (4950 GHz) through 26 (4980 GHz) and sub-band channels 1-19 (5 and 10 MHz) are used for Cisco 3200 interoperability. This configuration change is made on the controller. No changes are made to the mesh access point configuration.
  - Channel assignments are only made to the RAP. Updates to the MAP are propagated by the RAP.

The default channel width for Cisco 3200s is 5 MHz. You must *either* change the channel width to 10 or 20-MHz to enable WGBs to associate with the AP1522 and AP1524PS *or* change the channel on the AP1522 or AP1524PS to a channel in the 5-MHz (channels 1 to 10) or 10-MHz band (channels 11 to 19).

- Radio (802.11a) must be disabled when configuring channels and then re-enabled when using the CLI.
  - When using the GUI, enabling and disabling of the 802.11a radio for channel configuration is not required.
- Cisco 3200s can scan channels *within* but not across the 5, 10 or 20-MHz bands.

Troubleshooting Tips

If a wireless client is not associated with a WGB, use the following steps to troubleshoot the problem:

1. Verify the client configuration and ensure that client configuration is correct.
2. Check the **show bridge** command output in autonomous AP, and confirm that the AP is reading the client MAC address from the right interface.
3. Confirm that the subinterfaces corresponding to specific VLANs in different interfaces are mapped to the same bridge group.
4. If required, clear the bridge entry using the **clear bridge** command (remember that this command will remove all wired and wireless clients associated in WGB and make them associate again).
5. Check the **show dot11 association** command output and confirm that the WGB is associated with the controller.
6. Ensure that the WGB has not exceeded its 20-client limitation.

In a normal scenario, if the **show bridge** and **show dot11 association** command outputs are as expected, wireless client association should be successful.

Configuring Voice Parameters in Indoor Mesh Networks

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

The indoor mesh access points (1130 and 1240) are 802.11e capable, and QoS is supported on the local 2.4-GHz access radio and the 5-GHz backhaul radio. CAC is supported on the backhaul and the CCXv4 clients (which provides CAC between the mesh access point and the client).

Note Voice is supported only on indoor mesh networks. Voice is supported on a best-effort basis in the outdoors in a mesh network.

CAC

CAC enables a mesh 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, to maintain QoS under differing network loads, CAC in CCXv4 or later is required.

Note CAC is supported in Cisco Compatible Extensions (CCX) v4 or later. See Chapter 6 of the *Cisco Wireless LAN Controller Configuration Guide, Release 7.0* at http://www.cisco.com/en/US/docs/wireless/controller/7.0/configuration/guide/c70sol.html

Two types of CAC are available for access points: bandwidth-based CAC and load-based CAC. All calls on a mesh network are bandwidth-based, so mesh access points use only bandwidth-based CAC.

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 is capable of accommodating a particular call by looking at the bandwidth available and compares it against the bandwidth required for the call. If there is not enough bandwidth available to maintain the maximum allowed number of calls with acceptable quality, the mesh access point rejects the call.

QoS and DSCP Marking

Cisco supports 802.11e on the local access and on the backhaul. Mesh access points prioritize user traffic based on classification, and therefore all user traffic is treated on a best-effort basis.

Resources available to users of the mesh vary, according to the location within the mesh, and a configuration that provides a bandwidth limitation in one point of the network can result in an oversubscription in other parts of the network.

Similarly, limiting clients on their percentage of RF is not suitable for mesh clients. The limiting resource is not the client WLAN, but the resources available on the mesh backhaul.

Similar to wired Ethernet networks, 802.11 WLANs employ Carrier Sense Multiple Access (CSMA), but instead of using collision detection (CD), WLANs use collision avoidance (CA). This means that instead of each station trying to transmit as soon as the medium is free, WLAN devices will use a collision avoidance mechanism to prevent multiple stations from transmitting at the same time.

The collision avoidance mechanism uses two values, called CWmin and CWmax. CW stands for *contention window*. The CW determines what additional amount of time an endpoint should wait, after the interframe space (IFS), to attend to transmit a packet. Enhanced distributed coordination function (EDCF) is a model that allows end devices that have delay-sensitive multi-media traffic to modify their CWmin and CWmax values to allow for statically greater (and more frequent) access to the medium.

Cisco access points support EDCF-like QoS. This provides up to eight queues for QoS.

These queues can be allocated in several different ways, as follows:

- Based on TOS / DiffServ settings of packets
- Based on Layer 2 or Layer 3 access lists
- Based on VLAN
- Based on dynamic registration of devices (IP phones)

AP1520s, in conjunction with Cisco controllers, provides a minimal integrated services capability at the controller, in which client streams have maximum bandwidth caps, and a more robust differentiated services (diffServ) capability based on the IP DSCP values and QoS WLAN overrides.

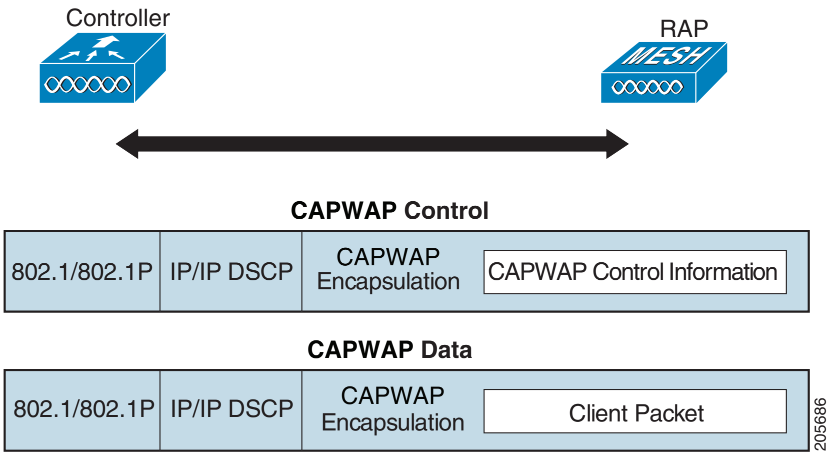
When the queue capacity has been reached, additional frames are dropped (tail drop).

Encapsulations

There are several encapsulations used by the mesh system. These include CAPWAP control and data between the controller and RAP, over the mesh backhaul, and between the mesh access point and its client(s). The encapsulation of bridging traffic (non-controller traffic from a LAN) over the backhaul is the same as the encapsulation of CAPWAP data.

There are two encapsulations between the controller and the RAP. The first is for CAPWAP control, and the second for CAPWAP data. In the control instance, CAPWAP is used as a container for control information and directives. In the instance of CAPWAP data, the entire packet, including the Ethernet and IP headers, is sent in the CAPWAP container (see Figure 81).

Figure 81 Encapsulations

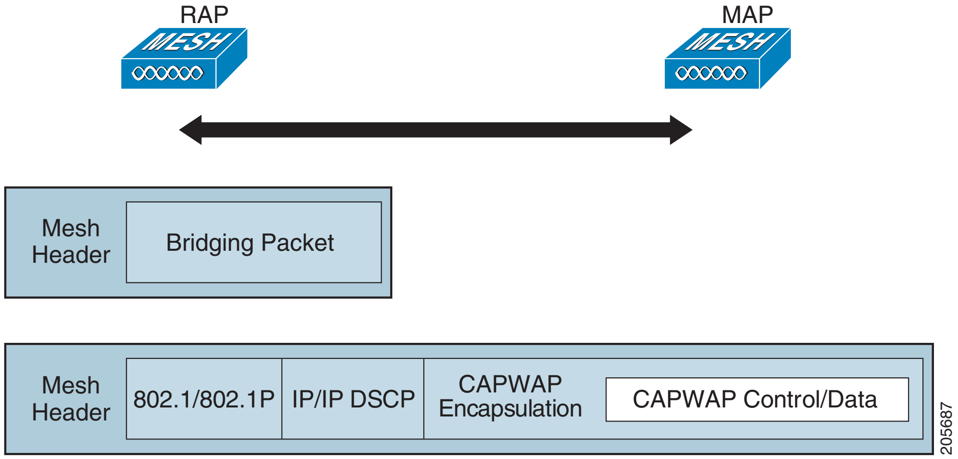


For the backhaul, there is only one type of encapsulation, encapsulating MESH traffic. However, two types of traffic are encapsulated: bridging traffic and CAPWAP control and data traffic. Both types of traffic are encapsulated in a proprietary mesh header.

In the case of bridging traffic, the entire packet Ethernet frame is encapsulated in the mesh header (see Figure 82).

All backhaul frames are treated identically, regardless of whether they are MAP to MAP, RAP to MAP, or MAP to RAP.

Figure 82 Encapsulating Mesh Traffic



Queuing on the Mesh Access Point

The mesh access point uses a high speed CPU to process ingress frames, Ethernet, and wireless on a first-come first-serve basis. These are queued for transmission to the appropriate output device, either Ethernet or wireless. Egress frames can be destined for either the 802.11 client network, the 802.11 backhaul network, or Ethernet.

AP1520s support four FIFOs for wireless client transmissions. These FIFOs correspond to the 802.11e platinum, gold, silver, and bronze queues, and obey the 802.11e transmission rules for those queues. The FIFOs have a user configurable queue depth.

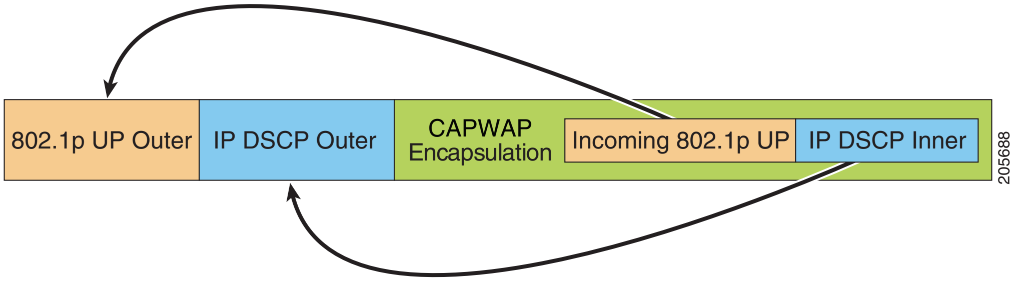
Likewise, the backhaul (frames destined for another outdoor mesh access point) uses four FIFOs, though user traffic is limited to gold, silver, and bronze. The platinum queue is used exclusively for CAPWAP control traffic and Voice, and has been reworked from the standard 802.11e parameters for CWmin, CWmax, and so on, to provide more robust transmission but higher latencies.

Similarly, the 802.11e parameters for CWmin, CWmax, and so on, for the gold queue have been reworked to provide lower latency at the expense of slightly higher error rate and aggressiveness. The purpose of these changes is to provide a channel more conducive to video applications.

Frames destined for Ethernet are queued as FIFO, up to the maximum available transmit buffer pool (256 frames). There is support for a Layer 3 IP Differentiated Services Code Point (DSCP), so marking of the packets is there as well.

In the controller to RAP path for the data traffic, the outer DSCP value is set to the DSCP value of the incoming IP frame. If the interface is in tagged mode, the controller sets the 802.1Q VLAN ID, and derives the 802.1p UP (outer) from 802.1p UP incoming and the WLAN default priority ceiling. Frames with VLAN ID 0 are not tagged (see Figure 83).

Figure 83 Controller to RAP Path



For CAPWAP control traffic the IP DSCP value is set to 46, and the 802.1p user priority is set to 7. Prior to transmission of a wireless frame over the backhaul, regardless of node pairing (RAP/MAP) or direction, the DSCP value in the outer header is used to determine a backhaul priority. The following sections describe the mapping between the four backhaul queues the mesh access point uses and the DSCP values shown in Backhaul Path QoS (see Table 17).

Table 17 Backhaul Path QoS

DSCP Value	Backhaul Queue
2, 4, 6, 8 to 23	Bronze
26, 32 to 63	Gold
46 to 56	Platinum
All others including 0	Silver

Note The platinum backhaul queue is reserved for CAPWAP control traffic, IP control traffic, and voice packets. DHCP, DNS and ARP requests are also transmitted at the platinum QoS level. The mesh software inspects each frame to determine whether it is an CAPWAP control or IP control frame in order to protect the platinum queue from use by non-CAPWAP applications.

For a MAP to the client path, there are two different procedures, depending on whether the client is a WMM client or a normal client. If the client is a WMM client, the DSCP value in the outer frame is examined, and the 802.11e priority queue is used (see Table 18).

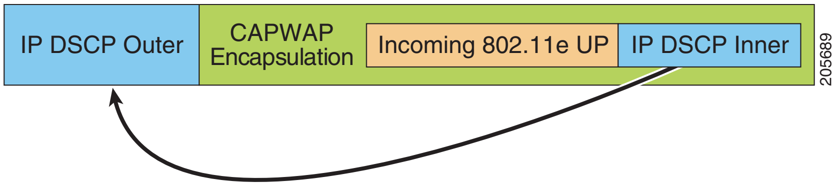
Table 18 MAP to Client Path QoS

DSCP Value	Backhaul Queue
2, 4, 6, 8 to 23	Bronze
26, 32 to 45, 47	Gold
46, 48 to 63	Platinum
All others including 0	Silver

If the client is not a WMM client, the WLAN override (as configured at the controller) determines the 802.11e queue (bronze, gold, platinum, or silver), on which the packet is transmitted.

For a client of a mesh access point, there are modifications made to incoming client frames in preparation for transmission on the mesh backhaul or Ethernet. For WMM clients, a MAP illustrates the way in which the outer DSCP value is set from an incoming WMM client frame (see Figure 84).

Figure 84 MAP to RAP Path



The minimum of the incoming 802.11e user priority and the WLAN override priority is translated using the information listed in Table 19 to determine the DSCP value of the IP frame. For example, if the incoming frame has as its value a priority indicating the gold priority, but the WLAN is configured for silver priority, the minimum priority of silver is used to determine the DSCP value.

Table 19 DSCP to Backhaul Queue Mapping

DSCP Value	802.11e UP	Backhaul Queue	Packet Types
2, 4, 6, 8 to 23	1, 2	Bronze	Lowest priority packets, if any
26, 32 to 34	4, 5	Gold	Video packets
46 to 56	6, 7	Platinum	CAPWAP control, AWPP, DHCP/DNS, ARP packets, voice packets
All others including 0	0, 3	Silver	Best effort, CAPWAP data packets

In the event that there is no incoming WMM priority, the default WLAN priority is used to generate the DSCP value in the outer header. In the event that the frame is an originated CAPWAP control frame, the DSCP value of 46 is placed in the outer header.

With the 5.2 code enhancements, DSCP information is preserved in an AWPP header.

All wired client traffic is restricted to a maximum 802.1p UP value of 5, except DHCP/DNS and ARP packets, which go through the platinum queue.

The non-WMM wireless client traffic gets the default QoS priority of its WLAN. While, the WMM wireless client traffic may have a maximum 802.11e value of 6, but it must be below the QoS profile configured for its WLAN. If admission control is configured, WMM clients must use TSPEC signaling and get admitted by CAC.

The CAPWAPP data traffic carries wireless client traffic and has the same priority and treatment as wireless client traffic.

Now that the DSCP value is determined, the rules described earlier for the backhaul path from the RAP to the MAP are used to further determine the backhaul queue on which the frame is transmitted. Frames transmitted from the RAP to the controller are not tagged. The outer DSCP values are left intact, as they were first constructed.

Bridging Backhaul Packets

Bridging services are treated a little differently from regular controller-based services. There is no outer DSCP value in bridging packets because they are not CAPWAP encapsulated. Therefore, the DSCP value in the IP header as it was received by the mesh access point is used to index into the table as described in the path from the mesh access point to the mesh access point (backhaul).

Bridging Packets from and to a LAN

Packets received from a station on a LAN are not modified in any way. There is no override value for the LAN priority. Therefore, in bridging mode the LAN must be properly secured. The only protection offered to the mesh backhaul is that non-CAPWAP control frames that map to the platinum queue are demoted to the gold queue.

Packets are transmitted to the LAN precisely as they are received on the Ethernet ingress at entry to the mesh.

The only way to integrate QoS between Ethernet ports on AP1520 and 802.11a is by tagging Ethernet packets with DSCP. AP1520s will take the Ethernet packet with DSCP and place it in the appropriate 802.11e queue.

AP1520s do not tag DSCP itself:

- On the ingress port, the 1520 sees a DSCP tag, encapsulates the Ethernet frame, and applies the corresponding 802.11e priority.
- On the egress port, the AP1520 decapsulates the Ethernet frame, and places it on the wire with an untouched DSCP field.

Ethernet devices such as video cameras, should have the capability to mark the bits with DSCP value to take advantage of QoS.

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

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.
- RF considerations for voice networks:
  - Coverage hole of 2 to 10 percent

  - Cell coverage overlap of 15 to 20 percent
  - RSSI and SNR values that are at least 15 dB higher than data requirements. For example, we recommend an RSSI of -67 dBm for an 11 or 12 Mbps link and an SNR of no more than 25 dB. Likewise, an RSSI of -56 dBm for a 56 Mbps link is recommended with an SNR of no more than 40 dB.
  - An RSSI of -62 dBm is recommended on a 24 Mbps 802.11a backhaul when universal access is configured and client traffic is present.
  - Packet error rate (PER) must be configured for a value of one percent or less.
  - Channel with the lowest utilization (CU) must be used. Check the CU when no traffic is running.
  - Radio resource manager (RRM) can be used to implement the recommended RSSI, PER, CU, cell coverage and coverage hole settings on the 802.11 b/g radio. RRM is not supported on the 802.11a radio.

- On the 802.11a or 802.11b/g/n > *Global* parameters page:
  - 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 page:
  - 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 page:
  - Set the EDCA profile for the interface as voice optimized
  - Disable low latency MAC
- On the QoS > *Profile* page:
  - Create a voice profile and select 802.1Q as the wired QoS protocol type
- On the WLANs > *Edit* > *QoS* page:
  - 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* page:
  - Select CCKM for authorization (*auth*) key management (*mgmt*) if you want to support fast roaming. See the "Client Roaming" section on page 124.
- On the **x** > ***y*** page:
  - Disable voice active detection (VAD)

Voice Call Support in a Mesh Network

Table 20 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 21 shows the actual calls in a clean, ideal environment.

Table 20 Theoretical 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 Mbps with 50% of the bandwidth reserved for voice calls.

[2] Bandwidth of 1076 Mbps with 50% of the bandwidth reserved for voice calls.

Table 21 Actual Calls Possible In a Clean, Ideal Environment[1]

No of calls	802.11a radio	802.11b radio
RAP	12	12
MAP1	7	10
MAP2	4	8

[1] Traffic was bidirectional 64K voice flows. VoCoder type: G.711, PER <= 1%. Network setup was daisy-chained with no calls traversing more than 2 hops. No external interference.

While making a call, observe the MOS score of the call on the 7921 phone (see Table 22). A MOS score between 3.5 and 4 is acceptable.

Table 22 MOS Ratings

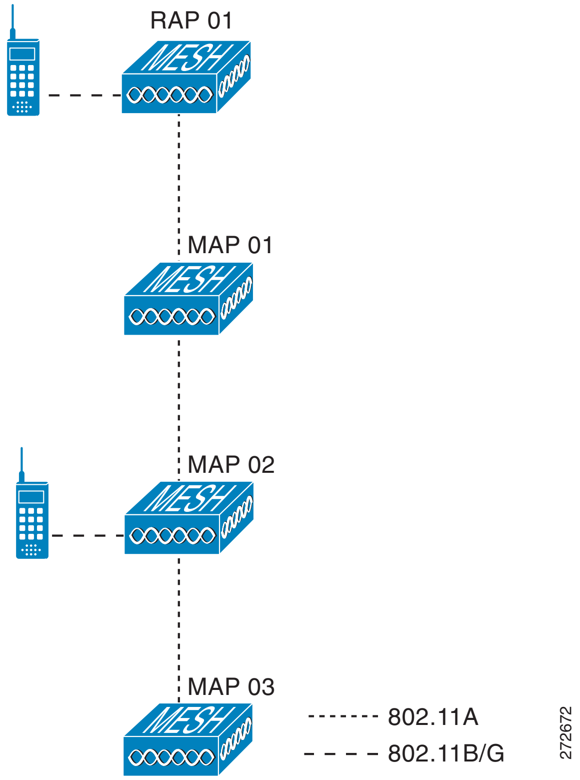
MOS rating	User satisfaction
> 4.3	Very satisfied
4.0	Satisfied
3.6	Some users dissatisfied
3.1	Many users dissatisfied
< 2.58	—

Using the CLI to View Voice Details for Mesh Networks

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

Note See Figure 85 when using the CLI commands and viewing their output.

Figure 85 Mesh Network Example



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

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

  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 MAP is from its RAP.

  Note When the radio type is the same, the backhaul bandwidth utilization (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 mesh access point radio, enter this command:

  show mesh cac access *AP_name*

  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 a mesh 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 *AP_name*

  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 mesh access point radio due to insufficient bandwidth, and the corresponding mesh access point radio where the rejection occurred, enter this command:

  show mesh cac rejected *AP_name*

  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, enter this command. The peak and average length of each queue are shown as well as the overflow count.

  show mesh queue-stats *AP_name*

  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 due to 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 MAP and RAP 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 RAP and MAP.
- **In-only 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.

Note When an HSRP configuration is in operation on a mesh network, we recommend the In-Out multicast mode be configured.

- **In-out mode**—The RAP and MAP both multicast but in a different manner:
  - In-out mode is the default mode.
  - If multicast packets are received at a MAP over Ethernet, they are sent to the RAP; however, they are not sent to other MAP over Ethernet, 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).

Enabling Multicast on the Mesh Network - Using the CLI

- 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.

IGMP Snooping

IGMP snooping delivers improved RF usage through selective multicast forwarding, and optimizes packet forwarding in voice and video applications.

A mesh access point transmits multicast packets only if a client is associated with the mesh access point that is subscribed to the multicast group. So, when IGMP snooping is enabled, only that multicast traffic relevant to given hosts is forwarded.

To enable IGMP snooping on the controller, enter:

configure network multicast igmp snooping enable

A client sends an IGMP *join* which travels through the mesh access point to the controller. The controller intercepts the *join* and creates a table entry for the client in the multicast group. The controller then proxies the IGMP *join* through the upstream switch or router.

You can query the status of the IGMP groups on a router by entering the following command:

```
router# show ip gmp groups
IGMP Connected Group Membership

Group Address     Interface   Uptime  Expires    Last Reporter
233.0.0.1         Vlan119     3w1d    00:01:52   10.1.1.130
```

For Layer 3 roaming, an IGMP query is sent to the client's WLAN. The controller modifies the client's response before forwarding, and changes the source IP address to the controller's dynamic interface IP address.

The network hears the controller's request for the multicast group and forwards the multicast to the new controller.

Locally Significant Certificates for Mesh APs

Currently, mesh APs support only the Manufactured Installed Certificate (MIC) to authenticate and get authenticated by controllers to join the controller. You may want to have your own public key infrastructure (PKI) to control CAs, to define policies, to define validity periods, to define restrictions and usages on the certificates that are generated, and get these certificates installed on the APs and controllers. After these customer generated or locally significant certificates (LSCs) are present on the APs and controllers, the devices should start using these LSCs, to join, authenticate, and derive a session key. Cisco supports normal APs from the 5.2 release and later releases and is extending the support for mesh APs as well from the 7.0 release.

Guidelines for Configuration

Follow these guidelines when using LSCs for mesh APs:

- This feature does not remove any preexisting certificates from an AP. It is possible for an AP to have both LSC and MIC certificates.
- After an AP is provisioned with an LSC, it does not read in its MIC certificate on boot-up. A change from an LSC to an MIC will require the AP to reboot. APs do it for fallback if they cannot be joined with LSC.
- Provisioning LSC on an AP does not require an AP to turn off its radios, which is vital for mesh APs, which may get provisioned over-the-air.
- Because mesh APs need a dot1x authentication, a CA and ID certificate is required on the server (in the controller or third-party server depending on the configuration).
- LSC provisioning will be supported only over Ethernet. You have to connect the mesh AP to the controller through Ethernet and get the LSC certificate provisioned. After the LSC becomes the default, AP can be connected over-the-air to the controller using the LSC certificate.

Differences Between LSCs for Mesh APs and Normal APs

CAPWAP APs use LSC for DTLS setup during JOIN irrespective of the AP mode. Mesh APs also use the certificate for mesh security. This involves a dot1x authentication with the controller (or an external AAA server), through the parent AP. After the mesh APs are provisioned with an LSC, they need to use the LSC for this purpose because MIC will not be read-in.

Mesh APs use a statically configured dot1x profile to authenticate.

This profile is hardcoded to use "cisco" as the certificate issuer. This needs to be made configurable so that vendor certificates can be used for mesh authentication (Enter the **config local-auth eap-profile cert-issuer vendor "prfMaP1500LlEAuth93"** command).

You must enter the **config mesh lsc enable/disable** command to enable or disable an LSC for mesh APs. This command will cause all the mesh APs to reboot.

Note LSC on mesh is open for very specific Oil and Gas customers with the 7.0 release. Initially, it is a hidden feature. The **config mesh lsc enable/disable** is a hidden command. Also, the **config local-auth eap-profile cert-issuer vendor "prfMaP1500LlEAuth93"** command is a normal command, but the "prfMaP1500LlEAuth93" profile is a hidden profile, and is not stored on the controller and is lost after the controller reboot.

Certificate Verification Process in LSC AP

LSC-provisioned APs have both LSC and MIC certificates, but the LSC certificate will be the default one. The verification process consists of the following two steps:

1. The controller sends the AP the MIC device certificate, which the AP verifies with the MIC CA.
2. The AP sends the LSC device certificate to the controller, which the controller verifies with the LSC CA.

Configuring LSC

To configure LSC, follow these steps:

Step 1 Enable LSC and provision the LSC CA certificate in the controller.

Step 2 Enter the following command:

config local-auth eap-profile cert-issuer vendor "prfMaP1500LlEAuth93"

Step 3 Turn on the feature by entering the following command:

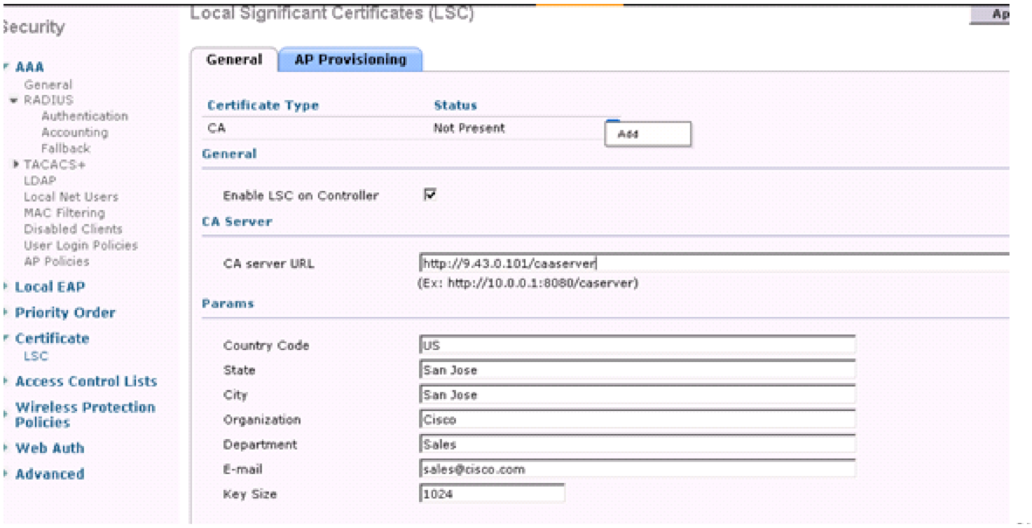
config mesh lsc enable/disable

Step 4 Install the CA and ID cert on the controller (or any other authentication server) from the same certificate server.

Step 5 Connect the mesh AP through Ethernet and provision for an LSC certificate.

Step 6 Let the Mesh AP get a certificate and join the controller using the LSC certificate. See Figure 86 and Figure 87.

Figure 86 Local Significant Certificate



Local Significant Certificates (LSC)

Certificate Type	Status
CA	Not Present

General

Enable LSC on Controller ☑

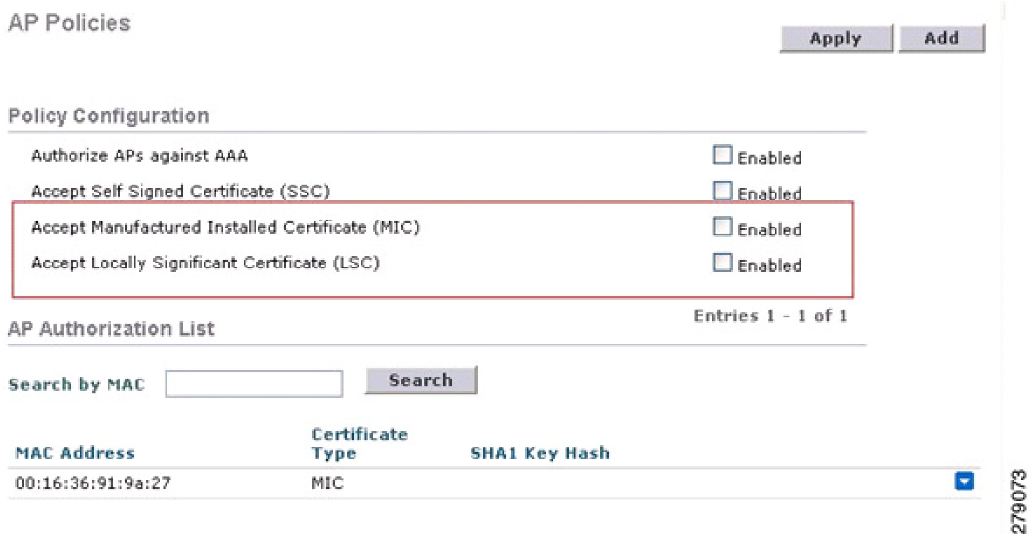
CA Server

CA server URL http://9.43.0.101/caaserver
(Ex: http://10.0.0.1:8080/caserver)

Params

Country Code	US
State	San Jose
City	San Jose
Organization	Cisco
Department	Sales
E-mail	sales@cisco.com
Key Size	1024

Figure 87 AP Policy Configuration



AP Policies

Policy Configuration

Authorize APs against AAA	☐ Enabled
Accept Self Signed Certificate (SSC)	☐ Enabled
Accept Manufactured Installed Certificate (MIC)	☐ Enabled
Accept Locally Significant Certificate (LSC)	☐ Enabled

AP Authorization List

Entries 1 - 1 of 1

Search by MAC

MAC Address	Certificate Type	SHA1 Key Hash
00:16:36:91:9a:27	MIC	

LSC-Related Commands

The following commands are related to LSCs:

- **config certificate lsc <enable/disable>**
  - **enable**—To enable an LSC on the system.
  - **disable**—To disable an LSC on the system. Use this keyword to remove the LSC device certificate and send a message to an AP, to do the same and disable an LSC, so that subsequent joins could be made using the MIC/SSC. The removal of the LSC CA cert on the WLC should be done explicitly by using the CLI to accommodate any AP that has not transitioned back to the MIC/SSC.
- **config certificate lsc ca-server "URL-Path"**

  This command configures the URL to the CA server for getting the certificates. The URL contains either the domain name or the IP address, port number (typically=80), and the CGI-PATH. The following format is an example:

  http://<ipaddr>:<port>/<cgi-path>

  Only one CA server is allowed to be configured. The CA server has to be configured to provision an LSC.
- **config certificate lsc ca-server delete**

  This command deletes the CA server configured on the WLC.
- **config certificate lsc ca-cert add/delete**

  This command adds or deletes the LSC CA certificate into/from the WLC's CA certificate database.
  - **add**—Queries the configured CA server for a CA certificate using the SSCEP getca operation, and gets into the WLC and installs it permanently into the WLC database. If installed, this CA certificate is used to validate the incoming LSC device certificate from the AP.
  - **delete**—Deletes the LSC CA certificate from the WLC database.
- **config certificate lsc subject-params <Country> <State> <City> <Orgn> <Dept> <Email>**

This command configures the parameters for the device certificate that will be created and installed on the controller and the AP.

All of these strings have 64 bytes, except for the Country that has a maximum of 3 bytes. The Common Name will be autogenerated using its Ethernet MAC address. This should be given prior to the creation of the controller device certificate request.

The above parameters are sent as an LWAPP payload to the AP, so that the AP can use these parameters to generate the certReq. The CN is autogenerated on the AP using the current MIC/SSC "Cxxxx-MacAddr" format, where xxxx is the product number.

- **config certificate lsc other-params *keysize validity***

  The keysize and validity configurations have defaults. Therefore, it is not mandatory to configure them.

  1. The keysize can be from 360 to 2048 (the default is 2048 bits).
  2. The validity period can be configured from 1 to 20 years (the default is 10 years).

- **config certificate lsc ap-provision enable/disable**

  This command enables or disables the provisioning of the LSCs on the APs if the APs just joined using the SSC/MIC. If enabled, all APs that join and do not have the LSC will get provisioned.

  If disabled, no more automatic provisioning will be done. This command does not affect the APs, which already have LSCs in them.

- **config certificate lsc ra-cert add/delete**

  This command is recommended when the CA server is a Cisco IOS CA server. The WLC can use the RA to encrypt the certificate requests and make communication more secure. RA certificates are not currently supported by other external CA servers, such as MSFT.

  - **add**—Queries the configured CA server for an RA certificate using the SCEP operation and installs it into the WLC Database. This is used to get the certReq signed by the CA.
  - **delete**—Deletes the LSC RA certificate from the WLC database.

- **config auth-list ap-policy lsc enable/disable**

  After getting the LSC, an AP tries to join WLC. Before the AP tries to join the WLC, this command must be executed on the WLC console. Execution of this command is mandatory. By default, the **config auth-list ap-policy lsc** command is in disabled state, and in the disabled state, the APs are not allowed to join WLC using the LSC.

- **config auth-list ap-policy mic enable/disable**

  After getting the MIC, an AP tries to join WLC. Before the AP tries to join the WLC, this command must be executed on the WLC console. Execution of this command is mandatory. By default, the **config auth-list ap-policy mic** command is in enabled state. If an AP cannot join because of the enabled state, a log message is added in the WLC side saying “LSC/MIC AP is not allowed to join by config”.

WLC CLI show Commands

The following are the **show** commands:

- **show certificate lsc summary**

  This command displays the LSC certificates installed on the WLC. It would be CA certificate, device certificate and optionally an RA certificate if RA certificate has also been installed. It also indicates if LSC is enabled or not.

- **show certificate lsc ap-provision**

This command displays in brief the status of the provisioning of AP, whether it is enabled or disabled, and whether a provision list is present or not.

- **show certificate lsc ap-provision details**

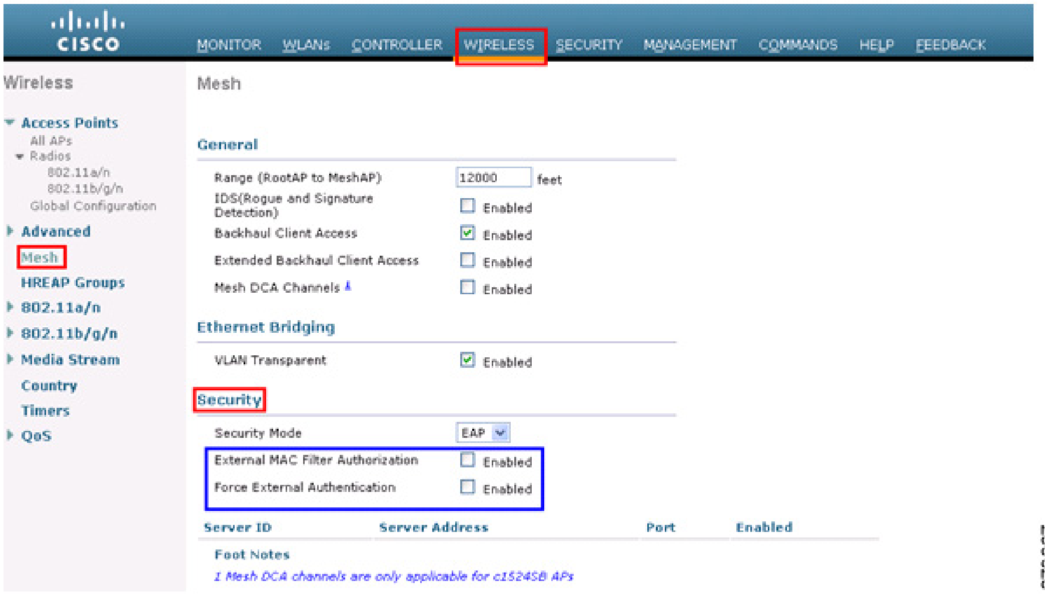
  This command displays the list of MAC addresses present in the AP provisioning lists.

Controller GUI Security Settings

Although the settings are not directly related to the feature, it may help you in achieving the desired behavior with respect to APs provisioned with LSC.

Figure 88 shows three possible cases for Mesh AP MAC authorization and EAP.

Figure 88 Possible Cases for Mesh AP MAC Authorization and EAP



Mesh

General

Range (RootAP to MeshAP) 12000 feet

IDS(Rogue and Signature Detection) □ Enabled

Backhaul Client Access ☑ Enabled

Extended Backhaul Client Access □ Enabled

Mesh DCA Channels [1] □ Enabled

Ethernet Bridging

VLAN Transparent ☑ Enabled

Security

Security Mode EAP

External MAC Filter Authorization □ Enabled

Force External Authentication □ Enabled

Server ID	Server Address	Port	Enabled

Foot Notes

1 Mesh DCA channels are only applicable for c1524SB APs

- Case 1—Local MAC Authorization and Local EAP Authentication

  Add the MAC address of RAP/MAP to the controller MAC Filter list.

  Example:

```
(Cisco Controller) > config macfilter mac-delimiter colon
(Cisco Controller) > config macfilter add 00:0b:85:60:92:30 0 management
```

- Case 2—External MAC Authorization and Local EAP Authentication

  Enter the following command on the WLC:

```
(Cisco Controller) > config mesh security rad-mac-filter enable
```

  or

  Check only the external MAC filter authorization on the GUI page and follow these guidelines:

  – Do not add the MAC address of the RAP/MAP to the controller MAC filter list.

  – Configure the external Radius server details on the WLC.

  – Enter the **config macfilter mac-delimiter colon** command configuration on the WLC.

- Add the MAC address of the RAP/MAP in the external Radius server in the following format:

  User name: 11:22:33:44:55:66   Password : 11:22:33:44:55:66

- Case 3—External EAP Authentication

  Configure the external radius server details on the WLC and apply the following configuration on the controller:

```
(Cisco Controller) > config mesh radius-server index enable
(Cisco Controller) > config mesh security force-ext-auth enable
```

  Add the user ID and password on the AAA server in the *(<platform name string>-<Ethernet mac address hex string>)* format for EAP Authentication.

  If it is a Cisco IOS AP, it should be in the following format:

  username: c1240-112233445566 and password: c1240-112233445566 for 1240 platform APs

  username: c1520-112233445566 and password: c1520-112233445566 for 1520 platform APs

  For 1510 VxWorks-based AP, it should be in the following format:

  username: 112233445566 and password: 112233445566

Deployment Guidelines

Follow these guidelines during deployment:

- When using local authorization, the controller should be installed with the vendor's CA and device certificate.
- When using an external AAA server, the controller should be installed with the vendor’s CA and device certificate.
- Mesh security should be configured to use ‘vendor’ as the cert-issuer.
- MAPs cannot move from an LSC to an MIC when they fallback to a backup controller.

The **config mesh lsc enable/disable** command is required to enable or disable LSC for Mesh APs. This command causes all the Mesh APs to reboot. Currently, disabling this command may also reboot nonmesh APs.

Checking the Health of the Network

This section describes how to check the health of your network.

Show Mesh Commands

The show mesh commands are grouped under the following sections:

- “Viewing General Mesh Network Details” section on page 146
- “Viewing Mesh Access Point Details” section on page 148
- “Viewing Public Safety Setting” section on page 150
- “Viewing Security Settings and Statistics” section on page 150

To view a summary of possible **show mesh** commands, enter this command:

```
(Cisco Controller) > show mesh ?

env             Show mesh environment.
backhaul        Show mesh AP backhaul info.
neigh           Show AP neigh list.
path            Show AP path.
astools         show mesh astools list
stats           Show AP stats.
secbh-stats     Show Mesh AP secondary backhaul stats.
per-stats       Show AP Neighbor Packet Error Rate stats.
queue-stats     Show AP local queue stats.
security-stats  Show AP security stats.
ap              Show mesh ap summary
config          Show mesh configurations.
secondary-backhaul Show mesh secondary-backhaul
ids-state       Show mesh ids-state
client-access   Show mesh backhaul with client access.
public-safety   Show mesh public safety.
background-scanning Show mesh background-scanning state.
cac             Show mesh cac.
```

Viewing General Mesh Network Details

- **show mesh env** {**summary** | *AP_name*}—Shows the temperature, heater status, and Ethernet status for either all access points (summary) or a specific access point (*AP_name*). 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 The battery status appears as N/A (not applicable) in the **show mesh env** *AP_name* 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
```

- **show mesh ap summary**: Revised to show the CERT MAC field which shows a MAC address within an AP certificate that can be used to assign a username for external authentication.

```
(Cisco Controller) > show mesh ap summary
AP Name AP Model           BVI MAC            CERT MAC          Hop Bridge Group Name
------- ---------------    -----------------  ---------------- ---- -----------------
R1      LAP1520            00:0b:85:63:8a:10  00:0b:85:63:8a:10 0    y1
R2      LAP1520            00:0b:85:7b:c1:e0  00:0b:85:7b:c1:e0 1    y1
H2      AIR-LAP1522AG-A-K9 00:1a:a2:ff:f9:00  00:1b:d4:a6:f4:60 1
Number of Mesh APs.............................. 3
Number of RAP................................. 2
Number of MAP................................. 1
```

- **show mesh path**—Displays MAC addresses, access point roles, SNR ratios (dBs) for uplink and downlink (SNRUp, SNRDown) and link SNR for a particular path.

```
(Cisco Controller) > show mesh path mesh-45-rap1
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.
```

- **show mesh neighbor summary**—Displays summary information about mesh neighbors. Neighbor information includes MAC addresses, parent-child relationships, and uplink and downlink (SNRUp, SNRDown).

```
(Cisco Controller) > show mesh neighbor summary ap1500:62:39:70
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
```

Note After review of the **show mesh...** commands above, you should be able to see the relationships between the nodes of your network and verify the RF connectivity by seeing the SNR values for every link.

- **show mesh ap tree**: Displays mesh access points within a tree structure (hierarchy).

```
(Cisco Controller) > show mesh ap tree
R1(0,y1)
|-R2(1,y1)
|-R6(2,y1)
|-H2(1,default)
Number of Mesh APs.............................. 4
Number of RAP................................. 1
Number of MAP................................. 3
```

Viewing Mesh Access Point Details

To view a mesh access point's configuration, enter these commands:

- **show ap config general** *Cisco_AP*–Displays system specifications for a mesh access point.

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

- **show mesh astools stats** [Cisco_AP] **–**Displays anti-stranding statistics for all outdoor mesh access points or a specific mesh access point.

```
(Cisco Controller) > show mesh astools stats

Total No of Aps stranded : 0
> (Cisco Controller) > show mesh astools stats sb_map1

Total No of Aps stranded : 0
```

- **show advanced backup-controller–**Displays configured primary and secondary backup controllers.

```
(Cisco Controller) > show advanced backup-controller
AP primary Backup Controller .................. controller1 10.10.10.10
AP secondary Backup Controller ............... 0.0.0.0
```

- **show advanced timer—**Displays setting for system timers.

```
(Cisco Controller) > show advanced timer
Authentication Response Timeout (seconds)........ 10
Rogue Entry Timeout (seconds)................... 1300
AP Heart Beat Timeout (seconds)................. 30
AP Discovery Timeout (seconds).................. 10
AP Primary Discovery Timeout (seconds).......... 120
```

- **show ap slots**–Displays slot information for mesh access points.

```
(Cisco Controller) > show ap slots
Number of APs.................................. 3
AP Name Slots AP Model            Slot0    Slot1   Slot2    Slot3
------------------------------  ------  -------  ------   ------
R1       2    LAP1520            802.11A  802.11BG
H1       3    AIR-LAP1521AG-A-K9 802.11BG 802.11A  802.11A
H2       4    AIR-LAP1521AG-A-K9 802.11BG 802.11A  802.11A 802.11BG
```

Viewing Global Mesh Parameter Settings

Use this command to obtain information on global mesh settings:

- **show mesh config**—Displays global mesh configuration settings.

```
(Cisco Controller) > show mesh config
Mesh Range..................................... 12000
Backhaul with client access status.............. disabled
Background Scanning State....................... enabled
Mesh Security
Security Mode............................... EAP
External-Auth............................... disabled
Use MAC Filter in External AAA server......... disabled
Force External Authentication................ disabled
Mesh Alarm Criteria
Max Hop Count............................... 4
Recommended Max Children for MAP............. 10
Recommended Max Children for RAP............. 20
Low Link SNR................................ 12
High Link SNR............................... 60
Max Association Number....................... 10
Association Interval......................... 60 minutes
Parent Change Numbers........................ 3
Parent Change Interval....................... 60 minutes
Mesh Multicast Mode............................ In-Out
Mesh Full Sector DFS........................... enabled
Mesh Ethernet Bridging VLAN Transparent Mode..... enabled
```

Viewing Bridge Group Settings

- **show mesh forwarding table**—Shows all configured bridges and their MAC table entries.
- **show mesh forwarding interfaces**—Displays bridge groups and the interfaces within each bridge group. Useful for troubleshooting bridge group membership.

Viewing VLAN Tagging Settings

- **show mesh forwarding VLAN mode**—Shows the configured VLAN Transparent mode (enabled or disabled).
- **show mesh forwarding VLAN statistics**—Displays statistics for the VLAN and the path.
- **show mesh forwarding vlans**—Displays supported VLANs.
- **show mesh ethernet VLAN statistics**—Displays statistics for the Ethernet interface.

Viewing DFS Details

- **show mesh dfs history**—Displays a history of radar detections by channels and resulting outages.

```
(Cisco Controller) > show mesh dfs history
ap1520#show mesh dfs history
Channel 100 detects radar and is unusable (Time Elapsed: 18 day(s), 22 hour(s), 10
minute(s), 24 second(s)).
Channel is set to 136 (Time Elapsed: 18 day(s), 22 hour(s), 10 minute(s), 24
second(s)).
Channel 136 detects radar and is unusable (Time Elapsed: 18 day(s), 22 hour(s), 9
minute(s), 14 second(s)).
Channel is set to 161 (Time Elapsed: 18 day(s), 22 hour(s), 9 minute(s), 14
second(s)).
Channel 100 becomes usable (Time Elapsed: 18 day(s), 21 hour(s), 40 minute(s), 24
second(s)).
Channel 136 becomes usable (Time Elapsed: 18 day(s), 21 hour(s), 39 minute(s), 14
second(s)).
Channel 64 detects radar and is unusable (Time Elapsed: 0 day(s), 1 hour(s), 20
minute(s), 52 second(s)).
Channel 104 detects radar and is unusable (Time Elapsed: 0 day(s), 0 hour(s), 47
minute(s), 6 second(s)).
Channel is set to 120 (Time Elapsed: 0 day(s), 0 hour(s), 47 minute(s), 6 second(s)).
```

- **show mesh dfs channel** *channel number*—Displays a history of radar detections and outages for a specified channel.

```
(Cisco Controller) > show mesh dfs channel 104
ap1520#show mesh dfs channel 104
Channel 104 is available
Time elapsed since radar last detected: 0 day(s), 0 hour(s), 48 minute(s), 11
second(s).
```

Viewing Public Safety Setting

- **show mesh public-safety**—Verifies that the 4.8-GHz public safety band is enabled.

```
(Cisco controller) show mesh public-safety
Global Public Safety status: enabled
```

Viewing Security Settings and Statistics

- **show mesh security-stats** *AP_name*—Shows packet error statistics and a count of failures, timeouts, and successes with respect to associations and authentications as well as reassociations and reauthentications for the specified access point and its child.

```
(Cisco controller) > show mesh security-stats ap417

AP MAC : 00:0B:85:5F:FA:F0
Packet/Error Statistics:
-----------------------------
Tx 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
```

Viewing Mesh Statistics for a Mesh Access Point

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

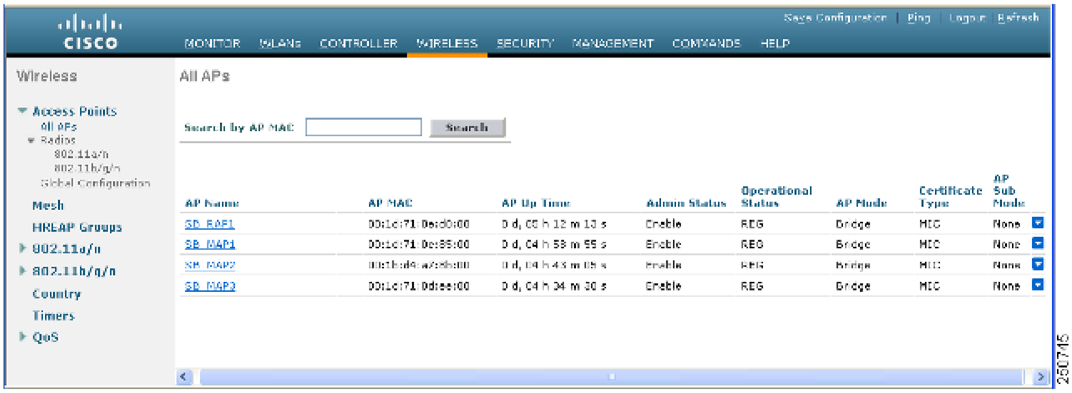
Note You can modify the Statistics Timer interval setting on the All APs > Details page of the controller GUI.

Viewing Mesh Statistics for a Mesh Access Point - Using the GUI

To view mesh statistics for a specific mesh access point using the controller GUI, follow these steps:

Step 1 Choose **Wireless** > **Access Points** > **All APs** to open the All APs page. (See Figure 89.)

Figure 89 All APs Page



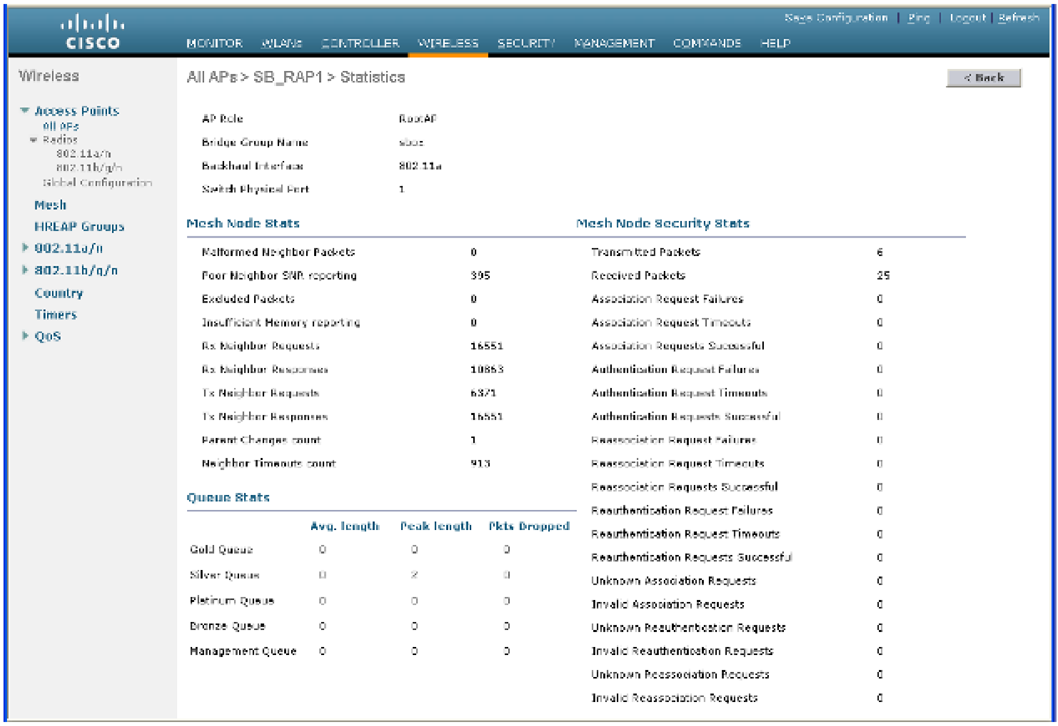
All APs

Search by AP MAC

AP Name	AP MAC	AP Up Time	Admin Status	Operational Status	AP Mode	Certificate Type	AP Sub Mode
SB_RAP1	00:1c:71:0e:d0:00	0 d, 05 h 12 m 13 s	Enable	REG	Bridge	MIC	None
SB_MAP1	00:1c:71:0e:85:00	0 d, 04 h 53 m 55 s	Enable	REG	Bridge	MIC	None
SB_MAP2	00:1b:d4:a7:8b:00	0 d, 04 h 43 m 05 s	Enable	REG	Bridge	MIC	None
SB_MAP3	00:1c:71:0d:ee:00	0 d, 04 h 34 m 30 s	Enable	REG	Bridge	MIC	None

Step 2 To view statistics for a specific mesh access point, hover the mouse over the blue drop-down arrow for the desired mesh access point and choose **Statistics**. The **All APs >** *AP Name* **> Statistics** page for the selected mesh access point appears. (See Figure 90.)

Figure 90 All APs > Access Point Name > Statistics Page



All APs > SB_RAP1 > Statistics

AP Role	RootAP
Bridge Group Name	sbox
Backhaul Interface	802.11a
Switch Physical Port	1

Mesh Node Stats

Malformed Neighbor Packets	0
Poor Neighbor SNR reporting	395
Excluded Packets	0
Insufficient Memory reporting	0
Rx Neighbor Requests	16551
Rx Neighbor Responses	10863
Tx Neighbor Requests	6371
Tx Neighbor Responses	16551
Parent Changes count	1
Neighbor Timeouts count	913

Queue Stats

	Avg. length	Peak length	Pkts Dropped
Gold Queue	0	0	0
Silver Queue	0	2	0
Platinum Queue	0	0	0
Bronze Queue	0	0	0
Management Queue	0	0	0

Mesh Node Security Stats

Transmitted Packets	6
Received Packets	25
Association Request Failures	0
Association Request Timeouts	0
Association Requests Successful	0
Authentication Request Failures	0
Authentication Request Timeouts	0
Authentication Requests Successful	0
Reassociation Request Failures	0
Reassociation Request Timeouts	0
Reassociation Requests Successful	0
Reauthentication Request Failures	0
Reauthentication Request Timeouts	0
Reauthentication Requests Successful	0
Unknown Association Requests	0
Invalid Association Requests	0
Unknown Reauthentication Requests	0
Invalid Reauthentication Requests	0
Unknown Reassociation Requests	0
Invalid Reassociation Requests	0

This page shows the role of the mesh access point in the mesh network, the name of the bridge group to which the mesh 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 mesh access point. Table 23 describes each of the statistics.

Table 23 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 23 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 23 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.

Viewing Mesh Statistics for an Mesh Access Point - Using the CLI

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

- To view packet error statistics; a count of failures, timeouts, and successes with respect to associations and authentications; and reassociations and reauthentications for a specific mesh access point, enter this command:

  show mesh security-stats *AP_name*

  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 *AP_name*

  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 due to 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 Mesh Access Point

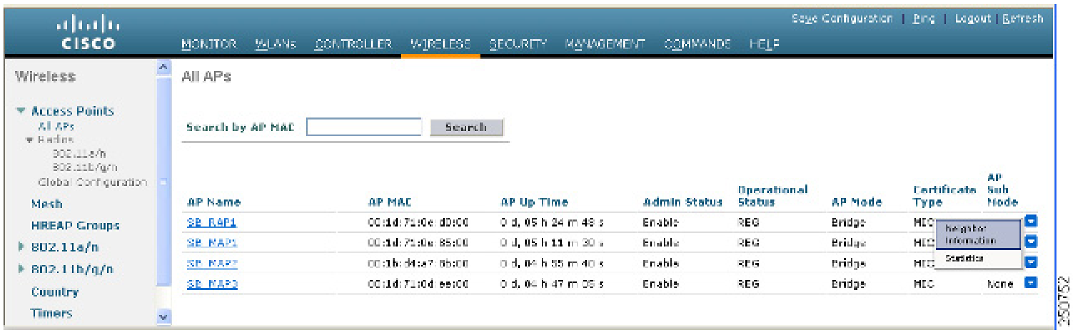
This section explains how to use the controller GUI or CLI to view neighbor statistics for a selected mesh access point. It also describes how to run a link test between the selected mesh access point and its parent.

Viewing Neighbor Statistics for a Mesh Access Point - Using the GUI

To view neighbor statistics for a specific mesh access point using the controller GUI, follow these steps:

Step 1 Choose **Wireless** > **Access Points** > **All APs** to open the All APs page. (See Figure 91.)

Figure 91 All APs Page



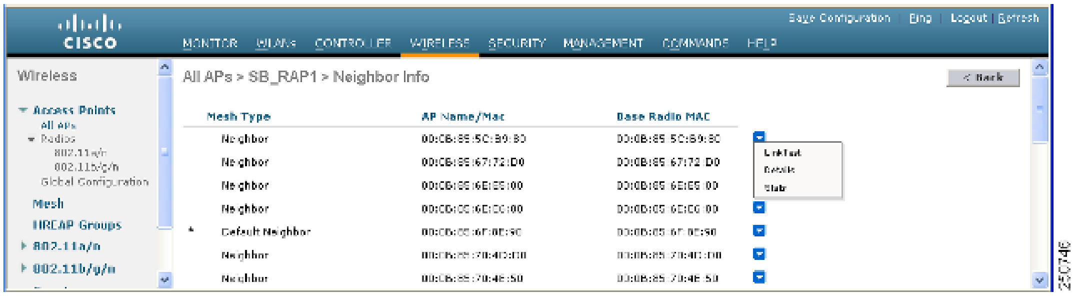
All APs

Search by AP MAC

AP Name	AP MAC	AP Up Time	Admin Status	Operational Status	AP Mode	Certificate Type	AP Sub Mode
SB_RAP1	00:1d:71:0e:d0:00	0 d, 05 h 24 m 48 s	Enable	REG	Bridge	MIC	
SB_MAP1	00:1d:71:0e:85:00	0 d, 05 h 11 m 30 s	Enable	REG	Bridge	MIC	
SB_MAP2	00:1b:d4:a7:8b:00	0 d, 04 h 55 m 40 s	Enable	REG	Bridge	MIC	
SB_MAP3	00:1d:71:0d:ee:00	0 d, 04 h 47 m 06 s	Enable	REG	Bridge	MIC	None

Step 2 To view neighbor statistics for a specific mesh access point, hover the mouse over the blue drop-down arrow for the desired mesh access point and choose **Neighbor Information**. The All APs > *Access Point Name* > Neighbor Info page for the selected mesh access point appears (see Figure 92).

Figure 92 All APs > Access Point Name > Neighbor Info Page



All APs > SB_RAP1 > Neighbor Info

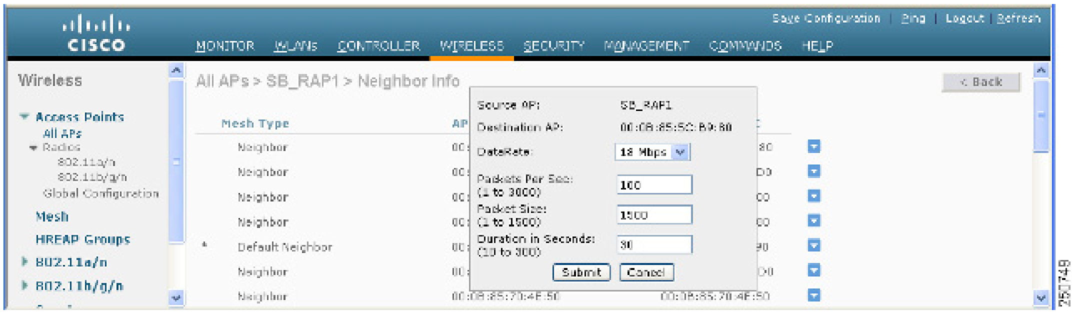
	Mesh Type	AP Name/Mac	Base Radio MAC
	Neighbor	00:0B:85:5C:B9:80	00:0B:85:5C:B9:80
	Neighbor	00:0B:85:67:72:D0	00:0B:85:67:72:D0
	Neighbor	00:0B:85:6E:E5:00	00:0B:85:6E:E5:00
	Neighbor	00:0B:85:6E:C0:00	00:0B:85:6E:C0:00
*	Default Neighbor	00:0B:85:6F:0E:90	00:0B:85:6F:0E:90
	Neighbor	00:0B:85:70:4D:D0	00:0B:85:70:4D:D0
	Neighbor	00:0B:85:70:4E:50	00:0B:85:70:4E:50

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

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

a. Hover the mouse over the blue drop-down arrow of the parent or desired child and choose **LinkTest**. A pop-up window appears (see Figure 93).

Figure 93 Link Test Page



All APs > SB_RAP1 > Neighbor Info

Source AP: SB_RAP1

Destination AP: 00:0B:85:5C:B9:80

DataRate: 18 Mbps

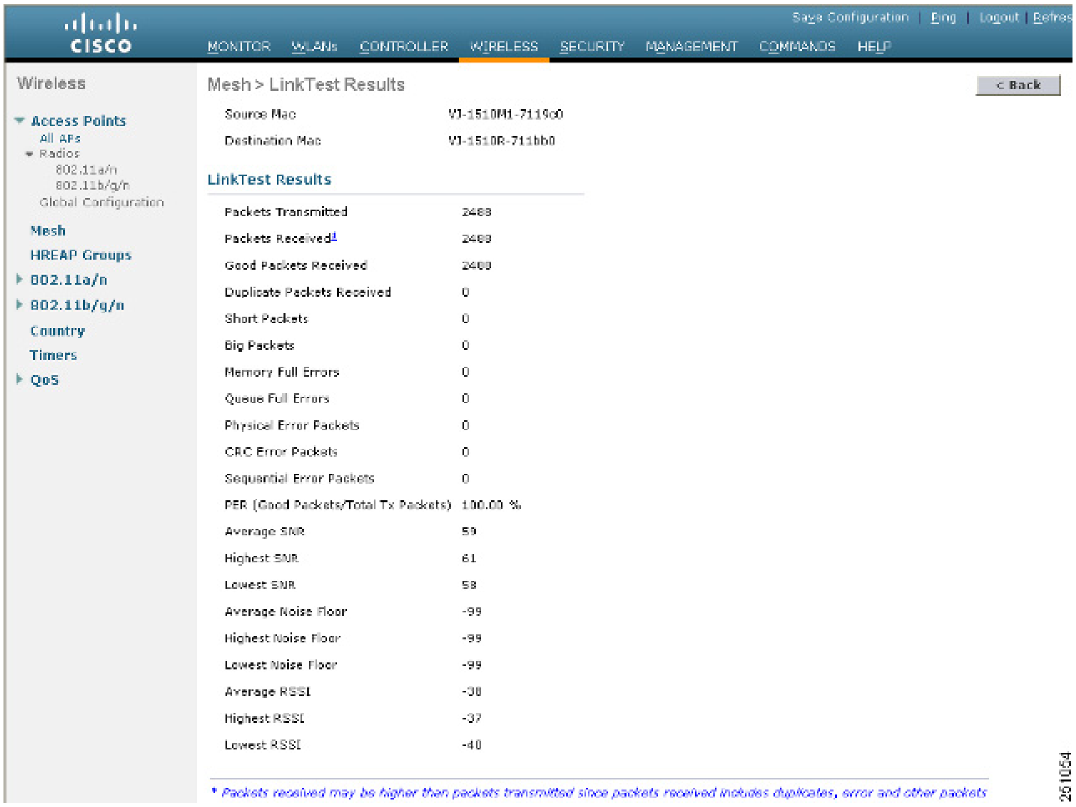
Packets Per Sec: (1 to 3000) 100

Packet Size: (1 to 1500) 1500

Duration in Seconds: (10 to 300) 30

b. Click **Submit** to start the link test. The link test results appear on the Mesh > LinkTest Results page (see Figure 94).

Figure 94 Mesh > LinkTest Results Page



Mesh > LinkTest Results

Source Mac	VJ-1510M1-7119c0
Destination Mac	VJ-1510R-711bb0

LinkTest Results

Packets Transmitted	2488
Packets Received[1]	2488
Good Packets Received	2488
Duplicate Packets Received	0
Short Packets	0
Big Packets	0
Memory Full Errors	0
Queue Full Errors	0
Physical Error Packets	0
CRC Error Packets	0
Sequential Error Packets	0
PER (Good Packets/Total Tx Packets)	100.00 %
Average SNR	59
Highest SNR	61
Lowest SNR	58
Average Noise Floor	-99
Highest Noise Floor	-99
Lowest Noise Floor	-99
Average RSSI	-38
Highest RSSI	-37
Lowest RSSI	-40

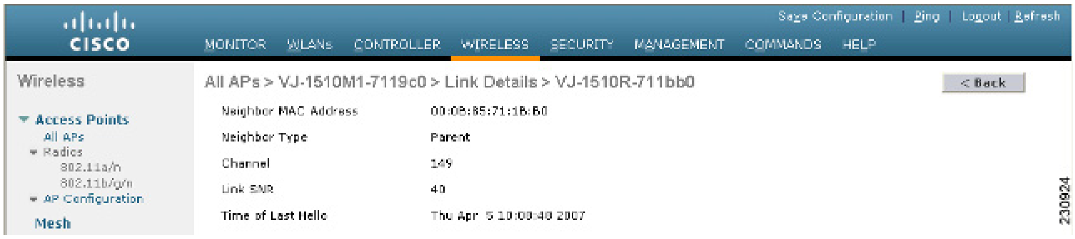
* Packets received may be higher than packets transmitted since packets received includes duplicates, error and other packets

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 mesh access points on this page, follow these steps:

a. Hover the mouse over the blue drop-down arrow for the desired mesh access point and choose **Details**. The **All APs >** *Access Point Name* **> Link Details >** *Neighbor Name* page appears (see Figure 95).

Figure 95 All APs > Access Point Name > Link Details > Neighbor Name page



All APs > VJ-1510M1-7119c0 > Link Details > VJ-1510R-711bb0

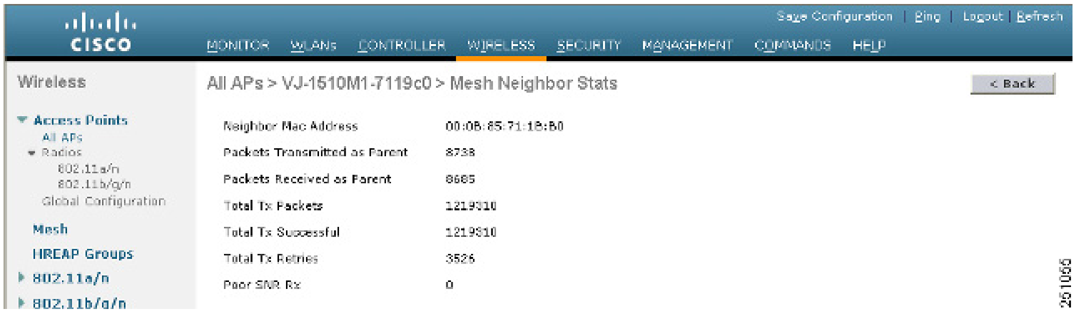
Neighbor MAC Address	00:0B:85:71:1B:B0
Neighbor Type	Parent
Channel	149
Link SNR	40
Time of Last Hello	Thu Apr 5 10:08:40 2007

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

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

a. Hover the mouse over the blue drop-down arrow for the desired mesh access point and choose **Stats**. The **All APs >** ***Access Point Name*** **> Mesh Neighbor Stats** page appears (see Figure 96).

Figure 96 All APs > Access Point Name > Mesh Neighbor Stats Page



All APs > VJ-1510M1-7119c0 > Mesh Neighbor Stats

Neighbor Mac Address	00:0B:85:71:18:B0
Packets Transmitted as Parent	8738
Packets Received as Parent	8685
Total Tx Packets	1219310
Total Tx Successful	1219310
Total Tx Retries	3526
Poor SNR Rx	0

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

Using the CLI to View Neighbor Statistics for a Mesh Access Point

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

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

  show mesh neigh {detail | summary} *AP_Name*

  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 a mesh access point and its neighbor, enter this command:

  show mesh path *AP_Name*

  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 *AP_Name*

  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).

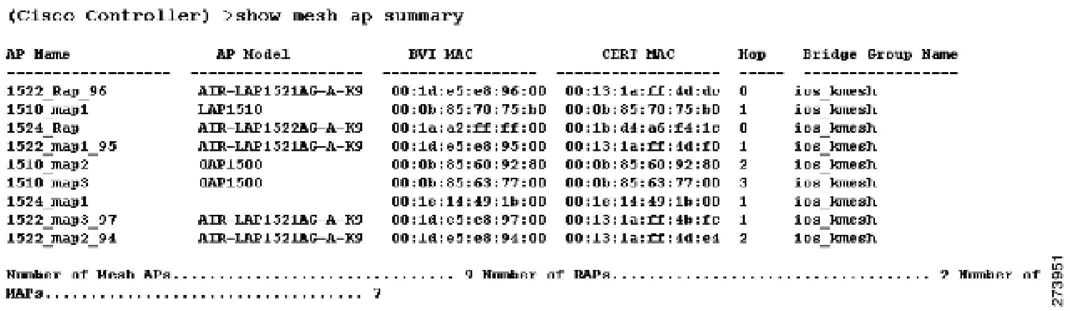
Troubleshooting

This section provides troubleshooting information.

Installation and Connections

1. Connect the mesh access point that you want to be the RAP to the controller.
2. Deploy the radios (MAP) at the desired locations.
3. Using the CLI, enter the **show mesh ap summary** command to see all MAPs and RAPs on the controller. (See Figure 97.)

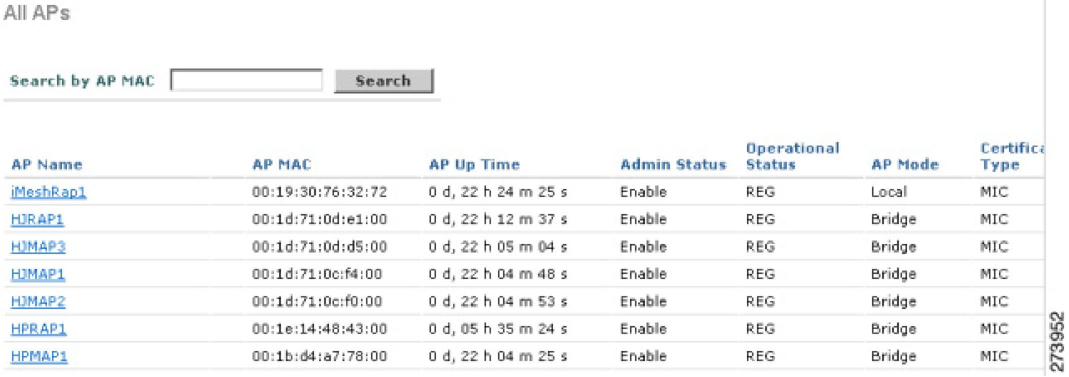
Figure 97 Show Mesh AP Summary Page



```
(Cisco Controller) >show mesh ap summary

AP Name             AP Model             BVI MAC            CERT MAC            Hop    Bridge Group Name
------------------  -------------------  -----------------  ------------------  -----  -----------------
1522_Rap_96         AIR-LAP1521AG-A-K9   00:1d:e5:e8:96:00  00:13:1a:ff:4d:dc   0      ios_kmesh
1510 map1           LAP1510              00:0b:85:70:75:b0  00:0b:85:70:75:b0   1      ios kmesh
1524_Rap            AIR-LAP1522AG-A-K9   00:1a:a2:ff:ff:00  00:1b:d4:a6:f4:1c   0      ios_kmesh
1522_map1_95        AIR-LAP1521AG-A-K9   00:1d:e5:e8:95:00  00:13:1a:ff:4d:f0   1      ios_kmesh
1510 map2           OAP1500              00:0b:85:60:92:80  00:0b:85:60:92:80   2      ios kmesh
1510 map3           OAP1500              00:0b:85:63:77:00  00:0b:85:63:77:00   3      ios kmesh
1524 map1                                00:1e:14:49:1b:00  00:1e:14:49:1b:00   1      ios_kmesh
1522_map3_97        AIR LAP1521AG A K9   00:1d:c5:c8:97:00  00:13:1a:ff:4b:fc   1      ios_kmesh
1522_map2_94        AIR-LAP1521AG-A-K9   00:1d:e5:e8:94:00  00:13:1a:ff:4d:e1   2      ios_kmesh

Number of Mesh APs.............................. 9 Number of RAPs.................................. 2 Number of
MAPs.................................. 7
```

4. From the controller GUI, click **Wireless** to see the mesh access point (RAP and MAP) summary. (See Figure 98.)

Figure 98 All APs Summary Page



All APs

AP Name	AP MAC	AP Up Time	Admin Status	Operational Status	AP Mode	Certifica Type
iMeshRap1	00:19:30:76:32:72	0 d, 22 h 24 m 25 s	Enable	REG	Local	MIC
HJRAP1	00:1d:71:0d:e1:00	0 d, 22 h 12 m 37 s	Enable	REG	Bridge	MIC
HJMAP3	00:1d:71:0d:d5:00	0 d, 22 h 05 m 04 s	Enable	REG	Bridge	MIC
HJMAP1	00:1d:71:0c:f4:00	0 d, 22 h 04 m 48 s	Enable	REG	Bridge	MIC
HJMAP2	00:1d:71:0c:f0:00	0 d, 22 h 04 m 53 s	Enable	REG	Bridge	MIC
HPRAP1	00:1e:14:48:43:00	0 d, 05 h 35 m 24 s	Enable	REG	Bridge	MIC
HPMAP1	00:1b:d4:a7:78:00	0 d, 22 h 04 m 25 s	Enable	REG	Bridge	MIC

5. Click **AP Name** to see the details page and then select the **Interfaces** tab to see the active radio interfaces.

   The radio slot in use, radio type, sub-band in use, and operational status (UP or DOWN) are summarized.

   - AP1524 supports 3 radio slots: slot 0 – 2.4 GHz, slot 1-5.8 GHz, and slot 2- 4.9 GHz
   - AP1522 supports 2 radio slots: slot 0 - 2.4 GHz, and slot 1 – 4.9 to 5.8 GHz

   If you have more than one controller connected to the same mesh network, then you must specify the name of the primary controller using global configuration for every mesh access point or specify the primary controller on every node, otherwise the least loaded controller is the preferred. If the mesh access points were previously connected to a controller, they already have learned a controller's name.

   After configuring the controller name, the mesh access point reboots.

6. Click **Wireless > AP Name** to check the mesh access point's primary controller on the AP details page.

Debug Commands

The following two commands are very helpful to see the messages being exchanged between mesh access points and the controller.

```
(Cisco Controller) > debug capwap events enable
(Cisco Controller) > debug disable-all
```

You can use the **debug** command to see the flow of packet exchanges that occur between the mesh access point and the controller. The mesh access point initiates the discovery process. An exchange of credentials takes place during the Join phase to authenticate that the mesh access point is allowed to join the mesh network.

Upon a successful join completion, the mesh access point sends a CAPWAP configuration request. The controller responds with a configuration response. When a Configure Response is received from the controller, the mesh access point evaluates each configuration element and then implements them.

Remote Debug Commands

You can log on to the mesh access point console for debugging either through a direct connection to the AP console port or through the remote debug feature on the controller.

To invoke remote debug on the controller, enter the following commands:

```
(Cisco controller) > debug ap enable ap name
(Cisco controller) > debug ap command "command" ap name
```

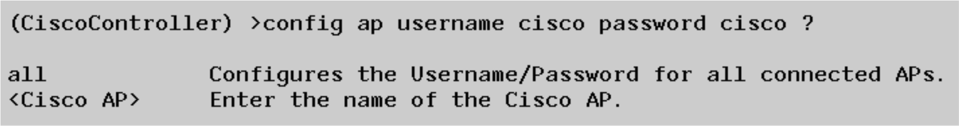
AP Console Access

AP1520s have a console port. A console cable is not shipped with the mesh access point. You must open the hinged side of the mesh access point to access the console port and then bring the cable outside from the Aux port to connect it to the laptop.

Note For details on opening the mesh access point, see the *Cisco Aironet 1520 Series Outdoor Mesh Access Point Mounting Instructions* document at http://www.cisco.com/en/US/docs/wireless/access_point/1520/mounting/installation/guide/1520mountInst.html#wp40299

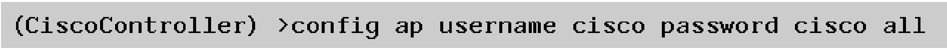
The AP1520s have console access security embedded in the code to prevent unauthorized access on the console port and provide enhanced security.

The *login ID* and *password* for console access are configured from the controller. You can use the following commands to push the username/password combination to the specified mesh access point or all access points.



```
(CiscoController) >config ap username cisco password cisco ?

all            Configures the Username/Password for all connected APs.
<Cisco AP>     Enter the name of the Cisco AP.
```

273953



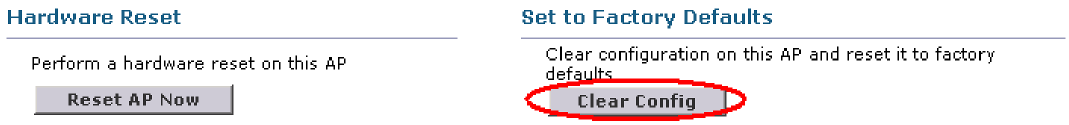
```
(CiscoController) >config ap username cisco password cisco all
```

273954

You must verify whether the username/password pushed from the controller is used as *user-id* and *password* on the mesh access point. It is a non-volatile setting. Once set, a *login ID* and *password* is saved in the private config of the mesh access point.

Once you have a successful login, the trap is sent to Cisco WCS. If a user fails to log in 3 times consecutively, login failure traps are sent to the controller and Cisco WCS.

Caution A mesh access point must be reset to the Factory Default settings before moving from one location to another.



Hardware Reset

Perform a hardware reset on this AP

Set to Factory Defaults

Clear configuration on this AP and reset it to factory defaults

205711

Cable Modem Serial Port Access From an AP

Commands can be sent to the cable modem from the privileged mode of the CLI. Use the command to take a text string and send it to the cable modem UART interface. The cable modem interprets the text string as one of its own commands. The cable modem response is captured and displayed on the IOS console. Up to 9600 characters are displayed from the cable modem. Any text that is greater than 4800 characters is truncated.

The modem commands are only operational on Mesh APs that have devices connected to the UART port originally intended for the cable modem. If the commands are used on a Mesh AP that does not have a cable modem (or any other device connected to the UART), the commands will be accepted, however, but will not produce any returned output. No errors will be explicitly flagged.

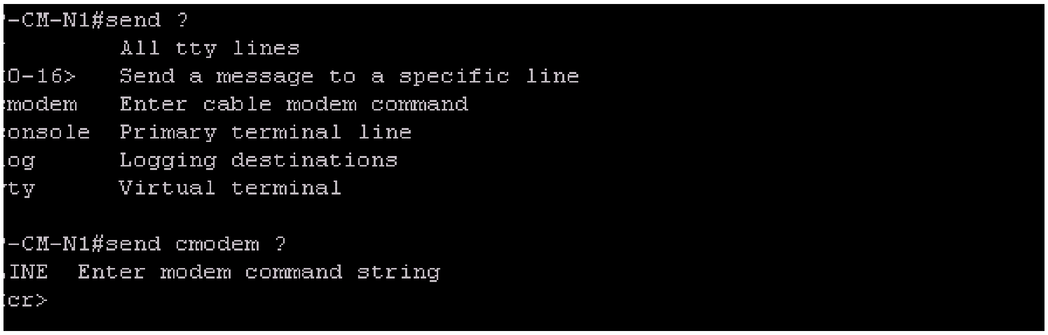
Configuration

Enter the following command from the privileged mode of the MAP:

```
AP#send cmodem <timeout value> <modem command>
```

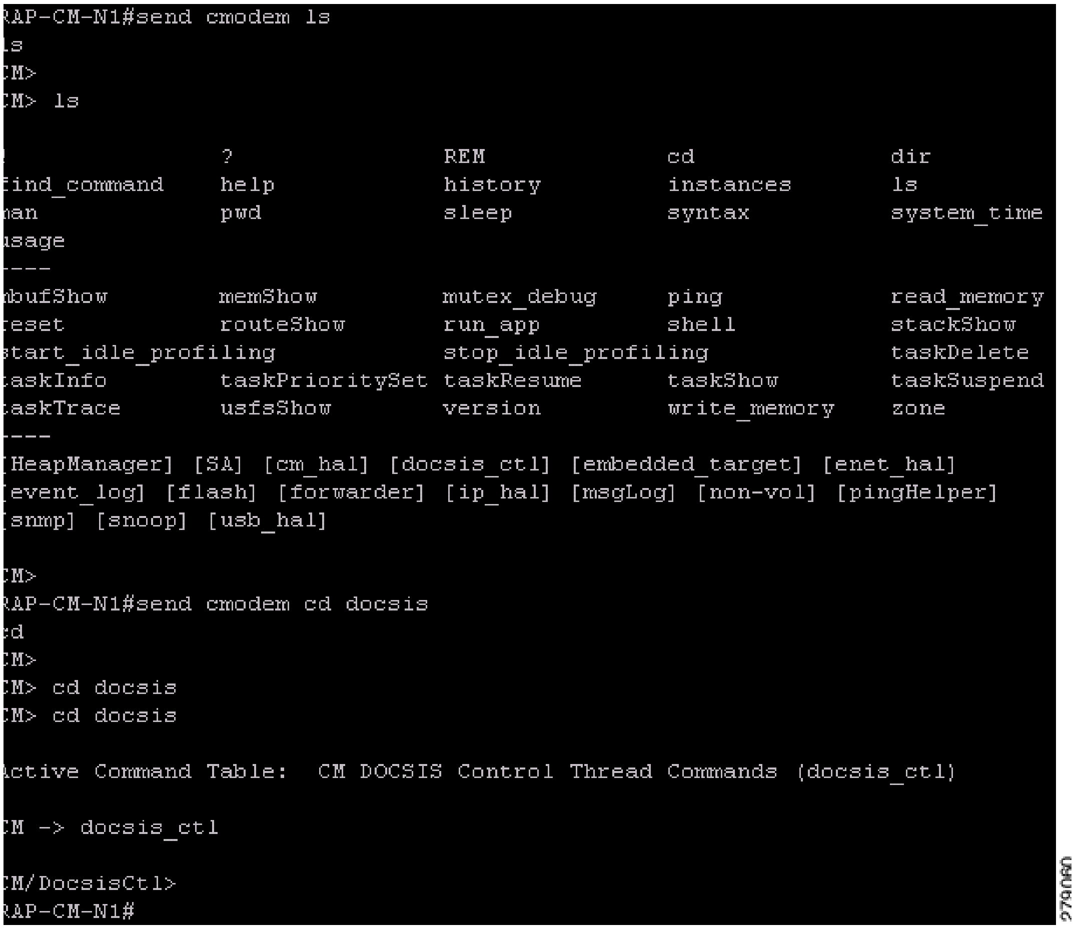
The *modem command* is any command or text to send to the cable modem. The range of *timeout value* is 1 to 300 seconds. However, if the captured data equals 9600 characters, any text beyond that is truncated and the response, irrespective of the timeout value, is immediately displayed on the AP console. See Figure 99 and Figure 100.

Figure 99 Cable Modem Console Access Command



```
-CM-N1#send ?
        All tty lines
0-16>   Send a message to a specific line
modem   Enter cable modem command
onsole  Primary terminal line
og      Logging destinations
ty      Virtual terminal

-CM-N1#send cmodem ?
INE  Enter modem command string
cr>
```

Figure 100 Cable Modem Console Access Command

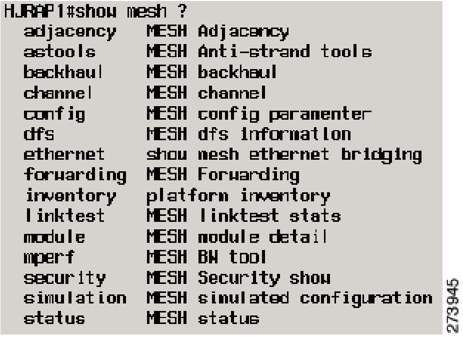


```
AP-CM-N1#send cmodem ls
ls
M>
M> ls

                ?               REM             cd              dir
ind_command     help            history         instances       ls
an              pwd             sleep           syntax          system_time
sage
---
bufShow         memShow         mutex_debug     ping            read_memory
eset            routeShow       run_app         shell           stackShow
tart_idle_profiling             stop_idle_profiling             taskDelete
askInfo         taskPrioritySet taskResume      taskShow        taskSuspend
askTrace        usfsShow        version         write_memory    zone
---
HeapManager] [SA] [cm_hal] [docsis_ctl] [embedded_target] [enet_hal]
event_log] [flash] [forwarder] [ip_hal] [msgLog] [non-vol] [pingHelper]
snmp] [snoop] [usb_hal]

M>
AP-CM-N1#send cmodem cd docsis
d
M>
M> cd docsis
M> cd docsis

ctive Command Table:  CM DOCSIS Control Thread Commands (docsis_ctl)

M -> docsis_ctl

M/DocsisCtl>
AP-CM-N1#
```

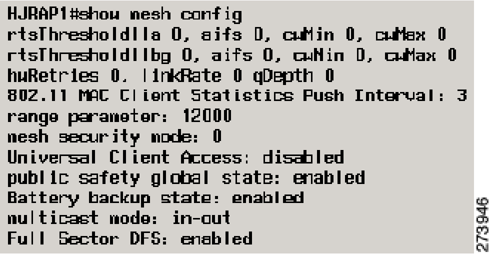
Caution The question mark (?) and the exclamation point (!) should not be used in the **send cmodem** command. These characters have immediate interpreted use in the Cisco IOS CLI. Therefore, they cannot be sent to the modem.

Mesh Access Point CLI Commands

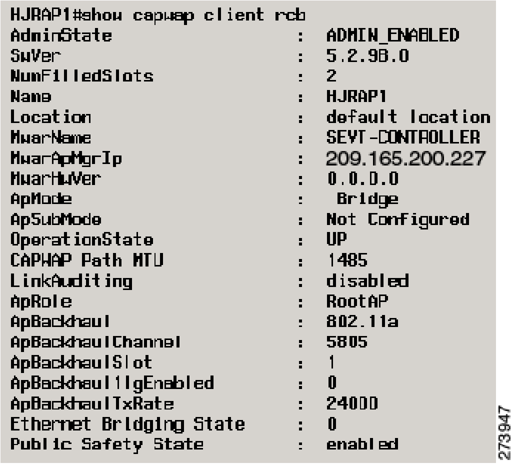
You can enter these commands directly on the mesh access point using the AP console port or you can use the remote debug feature from the controller.



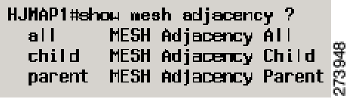
```
HJRAP1#show mesh ?
  adjacency   MESH Adjacency
  astools     MESH Anti-strand tools
  backhaul    MESH backhaul
  channel     MESH channel
  config      MESH config parameter
  dfs         MESH dfs information
  ethernet    show mesh ethernet bridging
  forwarding  MESH Forwarding
  inventory   platform inventory
  linktest    MESH linktest stats
  module      MESH module detail
  mperf       MESH BW tool
  security    MESH Security show
  simulation  MESH simulated configuration
  status      MESH status
```



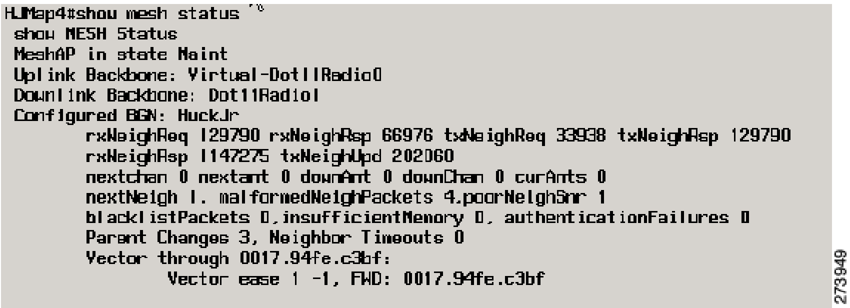
```
HJRAP1#show mesh config
rtsThreshold11a 0, aifs 0, cwMin 0, cwMax 0
rtsThreshold11bg 0, aifs 0, cwMin 0, cwMax 0
hwRetries 0, linkRate 0 qDepth 0
802.11 MAC Client Statistics Push Interval: 3
range parameter: 12000
mesh security mode: 0
Universal Client Access: disabled
public safety global state: enabled
Battery backup state: enabled
multicast mode: in-out
Full Sector DFS: enabled
```



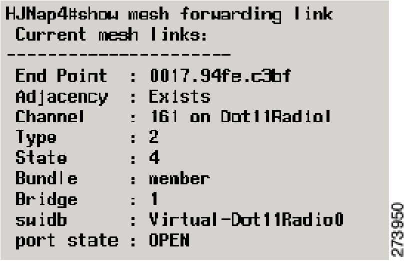
```
HJRAP1#show capwap client rcb
AdminState                  :  ADMIN_ENABLED
SwVer                       :  5.2.98.0
NumFilledSlots              :  2
Name                        :  HJRAP1
Location                    :  default location
MwarName                    :  SEVT-CONTROLLER
MwarApMgrIp                 :  209.165.200.227
MwarHwVer                   :  0.0.0.0
ApMode                      :   Bridge
ApSubMode                   :  Not Configured
OperationState              :  UP
CAPWAP Path MTU             :  1485
LinkAuditing                :  disabled
ApRole                      :  RootAP
ApBackhaul                  :  802.11a
ApBackhaulChannel           :  5805
ApBackhaulSlot              :  1
ApBackhaul11gEnabled        :  0
ApBackhaulTxRate            :  24000
Ethernet Bridging State     :  0
Public Safety State         :  enabled
```



```
HJMAP1#show mesh adjacency ?
  all     MESH Adjacency All
  child   MESH Adjacency Child
  parent  MESH Adjacency Parent
```



```
HJMap4#show mesh status
 show MESH Status
 MeshAP in state Maint
 Uplink Backbone: Virtual-Dot11Radio0
 Downlink Backbone: Dot11Radio1
 Configured BGN: HuckJr
        rxNeighReq 129790 rxNeighRsp 66976 txNeighReq 33938 txNeighRsp 129790
        rxNeighRsp 1147275 txNeighUpd 202060
        nextchan 0 nextant 0 downAnt 0 downChan 0 curAnts 0
        nextNeigh 1, malformedNeighPackets 4,poorNeighSnr 1
        blacklistPackets 0,insufficientMemory 0, authenticationFailures 0
        Parent Changes 3, Neighbor Timeouts 0
        Vector through 0017.94fe.c3bf:
                Vector ease 1 -1, FWD: 0017.94fe.c3bf
```



```
HJNap4#show mesh forwarding link
 Current mesh links:
----------------------
 End Point   : 0017.94fe.c3bf
 Adjacency   : Exists
 Channel     : 161 on Dot11Radio1
 Type        : 2
 State       : 4
 Bundle      : member
 Bridge      : 1
 swidb       : Virtual-Dot11Radio0
 port state : OPEN
```

Mesh Access Point Debug Commands

You can enter these commands directly on the mesh access point using the AP console port or you can use the remote debug feature from the controller.

- **debug mesh ethernet bridging**—Debugs Ethernet bridging.
- **debug mesh ethernet config**—Debugs access and trunk port configuration associated with VLAN tagging.
- **debug mesh ethernet registration**—Debugs VLAN registration protocol. Associated with VLAN tagging.
- **debug mesh forwarding table**—Debugs the forwarding table containing bridge groups.
- **debugs mesh forwarding packet bridge-group**—Debugs bridge group configuration.

Mesh Access Point Roles

By default, the AP1520s are shipped with a radio role set to MAP. Therefore, you must change the radio role on a mesh access point for it to function as RAP.

You can change this configuration on the mesh access point by statically setting them as rooftop access points or mesh access points with the following command:

(Cisco Controller) > **config ap role** {*rootAP* | *mesh AP* | *default*}

To change the radio role can also be changed using the GUI, follow these steps:

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

Step 2 Click the name of the mesh access point that you want to change. Click the **Mesh** tab.

Step 3 From the AP Role drop-down list, choose **MeshAP** or **RootAP** to specify this mesh access point as a MAP or RAP, respectively.

Step 4 Click **Apply** to commit your changes. The mesh access point reboots.

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

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

Backhaul Algorithm

A *backhaul* is used to create only the wireless connection between mesh access points.

The backhaul interface by default is 802.11a. You cannot change the backhaul interface to 802.11b/g.

The 24 Mbps data rate is selected by default for AP1520s.

The backhaul algorithm has been designed to fight against stranded mesh access point conditions. This also adds a high-level of resiliency for each mesh node.

The algorithm can be summarized as follows:

- A MAP always sets the Ethernet port as the *primary backhaul* if it is UP, otherwise it is the 802.11a radio. (This gives the network administrator the ability to configure it as a RAP the first time and recover it in-house). For fast convergence of the network, we recommend that you not connect any Ethernet device to the MAP for its initial joining to the mesh network.
- A MAP failing to connect to a WLAN controller on an Ethernet port that is UP, sets the 802.11a radio as the *primary backhaul*. Failing to find a neighbor or failing to connect to a WLAN controller via any neighbor on the 802.11a radio causes the *primary backhaul* to be UP on the Ethernet port again. A MAP will give preference to the *parent* which has the same BGN.
- A MAP connected to a controller over an Ethernet port does not build a mesh topology (unlike a RAP).
- A RAP always sets the Ethernet port as the *primary backhaul*.
- If the Ethernet port on a RAP is DOWN, or a RAP fails to connect to a controller on an Ethernet port that is UP, the 802.11a radio is set as the *primary backhaul*. Failing to find a neighbor or failing to connect to a controller via any neighbor on the 802.11a radio will make the RAP go to SCAN state after 15 minutes and starts with the Ethernet port first.

Keeping the roles of mesh nodes distinct using the above algorithm greatly helps avoid a mesh access point from being in an unknown state and becoming stranded in a live network.

Passive Beaconing (Anti-Stranding)

When enabled, passive beaconing allows a stranded mesh access point to broadcast its debug messages over-the-air using a 802.11b/g radio. A neighboring mesh access point that is listening to the stranded mesh access point and has a connection to a controller, can pass those messages to the controller over CAPWAP. Passive beaconing prevents a mesh access point that has no wired connection from being stranded.

Debug logs can also be sent as distress beacons on a non-backhaul radio so that a neighboring mesh access point can be dedicated to listen for the beacons.

The following steps are automatically initiated at the controller when a mesh access point loses its connection to the controller:

- Identifies the MAC address of a stranded mesh access point
- Finds a nearby neighbor that is CAPWAP connected
- Sends commands through remote debug
- Cycles channels to follow the mesh access point

You only have to know the MAC address of the stranded AP to make use of this feature.

A mesh access point is considered stranded if it goes through a lonely timer reboot. When the lonely timer reboot is triggered, the mesh access point, which is now stranded, enables passive beaconing, the anti-stranding feature.

This feature can be divided into three parts:

- Strand detection by stranded mesh access point
- Beacons sent out by stranded mesh access point
  - Latch the 802.11b radio to a channel (1,6,11)
  - Enable debugs
  - Broadcast the standard debug messages as distress beacons
  - Send Latest Crash info file
- Receive beacons. (Neighboring mesh access point with remote debugging enabled).

Deployed mesh access points constantly look for stranded mesh access points. Periodically, mesh access points send a list of stranded mesh access points and SNR information to the controller. The controller maintains a list of the stranded mesh access points within its network.

When the **debug mesh astools troubleshoot** *mac-addr* **start** command is entered, the controller runs through the list to find the MAC address of the stranded mesh access point.

A message is sent to the best neighbor to start listening to the stranded access point. The listening mesh access point gets the distress beacons from the stranded mesh access point and sends it to the controller.

Once a mesh access point takes the role of a listener, it will not purge the stranded mesh access point from its internal list, until it stops listening to the stranded mesh access point. While a stranded mesh access point is being debugged, if a neighbor of that mesh access point reports a better SNR to the controller than the current listener by some percentage, then the listener of the stranded mesh access point is changed to the new listener (with better SNR) immediately.

End-user commands are as follows:

- **config mesh astools** [**enable/disable**]: Enables or disables the astools on the mesh access points. If disabled, APs no longer sends a stranded AP list to the controller.
- **show mesh astools stats**: Shows the list of stranded APs and their listeners if they have any.
- **debug mesh astools troubleshoot** *mac-addr* **start**: Sends a message to the best neighbor of the <mac-addr> to start listening.
- **debug mesh astools troubleshoot** *mac-addr* **stop**: Sends a message to the best neighbor of the <mac-addr> to stop listening.
- **clear mesh stranded** [**all/***mac of b/g radio*]: Clears stranded AP entries.

The controller console is swamped with debug messages from stranded APs for 30 minutes.

DFS

DFS in RAP

The RAP performs the following steps as a response to radar detection:

1. The RAP sends a message to the controller that the channel is infected with radar. The channel is marked as infected on the RAP and on the controller.
2. The RAP blocks the channel for 30 minutes. This 30-minute period is called *non-occupancy period***.**
3. The Controller sends the TRAP, indicating that the radar has been detected on the channel. TRAP remains until the non-occupancy period expires.
4. The RAP has 10 seconds to move away from the channel. This is called *channel move time.* This is defined as the time for the system to clear the channel and is measured from the end of the radar burst to the end of the final transmission on the channel.
5. The RAP enters the *quiet mode.* In the quiet mode, the RAP stops data transmissions. Beacons are still generated and probe responses are still delivered. The quiet mode exists until the channel move time is over (10 seconds).
6. The Controller picks up a new random channel and sends the channel information to the RAP.
7. The RAP receives the new channel information and sends channel change frames (unicast, encrypted) to the MAP, and each MAP sends the same information to its lower children down the sector. Each mesh access point sends the channel change frames once every 100 msecs for a total of five times.
8. The RAP tunes to the new channel and enters into the *silent mode*. During the silent mode, only the receiver is ON. The RAP keeps scanning the new channel for any radar presence for 60 seconds. This is called *channel availability check* (CAC)**.**
9. The MAP tunes to the new channel and enters into the silent mode. During the silent mode, only the receiver is ON. The MAP keeps scanning the new channel for any radar presence for 60 seconds.
10. If radar is not detected, the RAP resumes full functionality on this new channel and the whole sector tunes to this new channel.

DFS in MAP

The MAP performs the following steps as a response to radar detection:

1. The MAP sends a radar seen indication to the parent and ultimately to the RAP indicating that the channel is infected. The RAP sends this message to the controller. The message will appear to be coming from the RAP. The MAP, RAP, and controller mark the channel as infected for 30 minutes.
2. The MAP blocks the channel for 30 minutes. This 30-minute period is called *non-occupancy period***.**
3. The Controller sends the TRAP, indicating that the radar has been detected on the channel. The TRAP remains until the non-occupancy period expires.
4. The MAP has 10 seconds to move away from the channel. This is called *channel move time.* This is defined as the time for the system to clear the channel and is measured from the end of the radar burst to the end of the final transmission on the channel.
5. The MAP enters the quiet mode. In the quiet mode, the MAP stops data transmissions. Beacons are still generated and probe responses are still delivered. The quiet mode exists until the channel move time is over (10 seconds).
6. The Controller picks up a new random channel and sends the channel to the RAP.

7. The RAP receives the new channel information and sends channel change frames (unicast, encrypted) to a MAP, and each MAP sends the same information to its lower children down the sector. Each mesh access point sends the channel change frames once every 100 msecs for a total of five times.
8. Each mesh access point tunes to the new channel and enters into the *silent mode*. During the silent mode, only the receiver is ON. There is no packet transmission happening. AP keeps scanning the new channel for any radar presence for 60 seconds. This is called the *channel availability check (CAC)***.** The MAP should not disconnect from the controller. The network should remain stable during this one minute period.

DFS functionality allows a MAP that detects a radar signal to transmit that up to the RAP, which then acts as if it has experienced radar and moves the sector. This is termed the *coordinated channel change*. This functionally can be turned on or off on the controller. Coordinated channel change is enabled by default.

To enable DFS, enter:

```
(Cisco Controller) > config mesh full-sector-dfs enable
```

To verify that DFS is enabled on the network, enter:

```
(Cisco Controller) > show network
```

Note A MAP that detects radar should send a message to the RAP, unless the parent has a different BGN, in which case it does not send messages for a coordinated sector change. Instead the MAP reenters the SCAN state and searches on non-radar seen channels for a new parent.

Note Ensure that none of your mesh access points are using a default BGN.

Note A repeated radar event on the MAP (radar triggers once, then almost immediately again), will cause the MAP to disconnect.

Preparation in a DFS Environment

- To verify that your controller is set to the correct country domain, enter:

  ```
  (Cisco Controller) > show country
  ```

- To check the mesh access point country and the channel setting on controller, enter:

  ```
  (Cisco Controller)> show ap config 802.11a ap name
  ```

- To identify channels available for mesh, enter:

  ```
  (Cisco Controller)> show ap config 802.11a ap name
  ```

  Look for the allowed channel list.

  ```
  Allowed Channel List...................... 100,104,108,112,116,120,124,
  ........................................ 128,132,136,140
  ```

- To identify channels available for mesh on the AP console (or using remote debug from the controller, enter:

```
ap1520-rap # show mesh channels

HW: Dot11Radio1, Channels:
100, 104, 108, 112, 116, 120, 124, 128, 132, 136, 140
```

An asterisk next to a channel indicates that radar has been seen on the channel.

Do a spot check on the mesh access points for radar information using the following remote debug commands from the controller:

- To invoke remote debug:

```
(Cisco Controller) > debug ap enable <ap name>
(Cisco Controller) > debug ap command <command> <ap name>
```

- Debug commands to see radar detection and past radar detections on the DFS channel are:

```
show mesh dfs channel <channel number>
show mesh dfs history
```

Information similar to this example appears.

```
ap1520-rap # show mesh dfs channel 132
```

```
Channel 132 is available
Time elapsed since radar last detected: 0 day(s), 7 hour(s), 6 minute(s), 51
second(s).
```

The RAP should then be run through the channels to determine whether there is active radar on each of the channels.

```
ap1520-rap # show mesh dfs channel 132

Radar detected on channel 132, channel becomes unusable (Time Elapsed: 0 day(s), 7
hour(s), 7 minute(s), 11 second(s)).
Channel is set to 100 (Time Elapsed: 0 day(s), 7 hour(s), 7 minute(s), 11 second(s)).
Radar detected on channel 116, channel becomes unusable (Time Elapsed: 0 day(s), 7
hour(s), 6 minute(s), 42 second(s)).
Channel is set to 64 (Time Elapsed: 0 day(s), 7 hour(s), 6 minute(s), 42 second(s)).
Channel 132 becomes usable (Time Elapsed: 0 day(s), 6 hour(s), 37 minute(s), 10
second(s)).
Channel 116 becomes usable (Time Elapsed: 0 day(s), 6 hour(s), 36 minute(s), 42
second(s)).
```

Monitoring DFS

The DFS history should be run every morning or more frequently to detect the radar. This information does not get erased and is stored on the mesh access point flash. Therefore, you only need to match up times.

```
ap1520-rap # show controller dot11Radio 1
```

Information similar to this displays:

```
interface Dot11Radio1
Radio Hammer 5, Base Address 001c.0e6c.9c00, BBlock version 0.00, Software version
0.05.30
Serial number: FOC11174XCW
Number of supported simultaneous BSSID on Dot11Radio1: 16
Carrier Set: ETSI (OFDM) (EU) (-E)
Uniform Spreading Required: Yes
Current Frequency: 5540 MHz Channel 108 (DFS enabled)
```

```
Allowed Frequencies: *5500(100) *5520(104) *5540(108) *5560(112) *5580(116) *560
0(120) *5620(124) *5640(128) *5660(132) *5680(136) *5700(140)
* = May only be selected by Dynamic Frequency Selection (DFS)
Listen Frequencies: 5180(36) 5200(40) 5220(44) 5240(48) 5260(52) 5280(56) 5300(6
0) 5320(64) 5500(100) 5520(104) 5540(108) 5560(112) 5580(116) 5660(132) 5680(136
) 5700(140) 5745(149) 5765(153) 5785(157) 5805(161) 5825(165) 4950(20) 4955(21)
4960(22) 4965(23) 4970(24) 4975(25) 4980(26)
```

Note An asterisk indicates that this channel has DFS enabled.

Frequency Planning

Use alternate adjacent channels in adjacent sectors. If you have two RAPs deployed at the same location, you must leave one channel in between.

Weather radars operate within the band 5600 to 5650 MHz, which means that channel 124 and 128 might be affected, but also channels 120 and 132 might suffer from weather radar activity.

If the mesh access point does detect radar, the controller and the mesh access point both will retain the channel as the configured channel. The controller retains it in volatile memory associated with the mesh access point, and the mesh access point has it stored in its flash as configuration. After the 30 minute quiet period, the controller returns the mesh access point to the static value, regardless of whether the mesh access point has been configured with a new channel or not. In order to overcome this, configure the mesh access point with a new channel, and reboot the mesh access point.

Once radar is reliably detected on a channel, that channel, and the two surrounding channels, should be added to the RRM exclusion list, as follows:

```
(Cisco Controller) > config advanced 802.11a channel delete <channel>
```

A mesh access point will go to a new channel as picked by RRM, and it will not consider excluded channels.

In the case where radar is detected on channel 124, for instance, channels 120, 124, and 128 should be added to the exclusion list. In addition, do not configure RAP to operate on those channels.

Good SNRs

For European installations, the minimum recommendation is increased to 20 dB of SNR. The extra dBs are used to mitigate the effects of radar interference with packet reception, which is not observed in non DFS environments.

AP Placement

Collocated mesh access points should have a minimum of 10 feet of vertical separation or 100 feet of horizontal separation.

Check Packet Error Rate

Mesh access points that have an high error rate, greater than 1%, should have mitigation applied to them, by changing the channels used in the case of noise and interference, by adding additional mesh access points in the transmission path, moving the mesh access points to different sectors, or by adding additional mesh access points.

Misconfiguration of BGN

A mesh access point can be wrongly provisioned with a *bridgegroupname* and placed in a group other than it was intended. Depending on the network design, this mesh access point might or might not be able to reach out and find its correct sector or tree. If it cannot reach a compatible sector, the mesh access point can become stranded.

In order to recover such a stranded mesh access point, the concept of default bridgegroupname has been introduced in the software. Therefore, when a mesh access point is unable to connect to any other mesh access point with its configured bridgegroupname, it attempts to connect with the bridgegroupname of *default*.

The algorithm of detecting this strand condition and recovery is as follows:

1. Passively scan and find all neighbor nodes, regardless of their bridgegroupname.
2. The mesh access point attempts to connect to the neighbors heard with *my own bridgegroupname* using AWPP.
3. If Step 2 fails, attempt connecting with default bridgegroupname using AWPP.
4. For each failed attempt in Step 3, exclusion-list the neighbor and attempt to connect the next best neighbor.
5. If the AP fails to connect with all neighbors in Step 4, reboot the mesh access point.
6. If connected with a *default* bridgegroupname for 15 minutes, the mesh access point will go into a scan state.

When an mesh access point is able to connect with the default bridgegroupname, the parent node reports the mesh access point as a default child/node/neighbor entry on the controller, so that a network administrator is Cisco WCS. Such a mesh access point behaves as a normal (non-mesh) access point and accepts any client, other mesh nodes as its children, and it can pass any data traffic through.

Note Do not confuse an unassigned BGN (null value) with DEFAULT, which is a mode the access point uses to connect when it cannot find its own BGN.

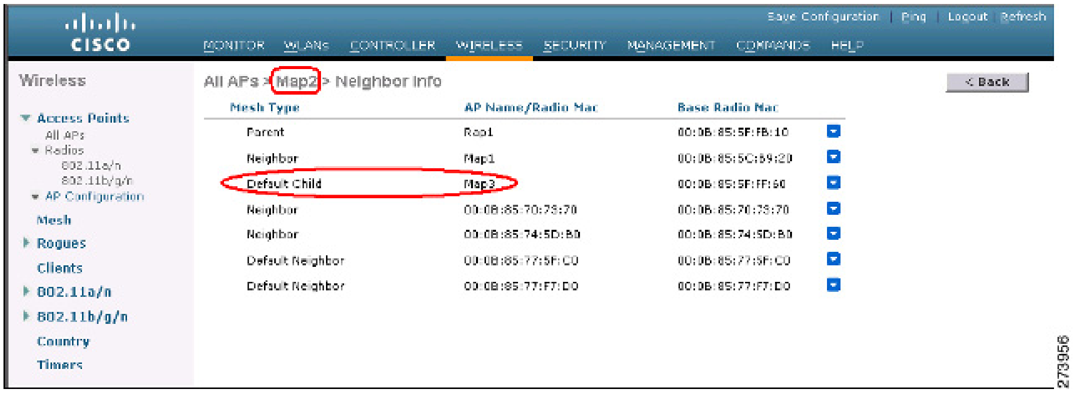
To check the current state of a mesh access point's BGN, enter this command (CLI):

```
(Cisco Controller)> show mesh path Map3:5f:ff:60
00:0B:85:5F:FA:60 state UPDATED NEIGH PARENT DEFAULT (106B), snrUp 48, snrDown 48, linkSnr
49
00:0B:85:5F:FB:10 state UPDATED NEIGH PARENT BEACON (86B) snrUp 72, snrDown 63, linkSrn 57
00:0B:85:5F:FA:60 is RAP
```

To check the current state of a mesh access point's BGN, check neighbor information for the mesh access point (GUI):

Choose **Wireless > All APs >** *AP Name* **>** *Neighbor info* (see Figure 101 and Figure 102).

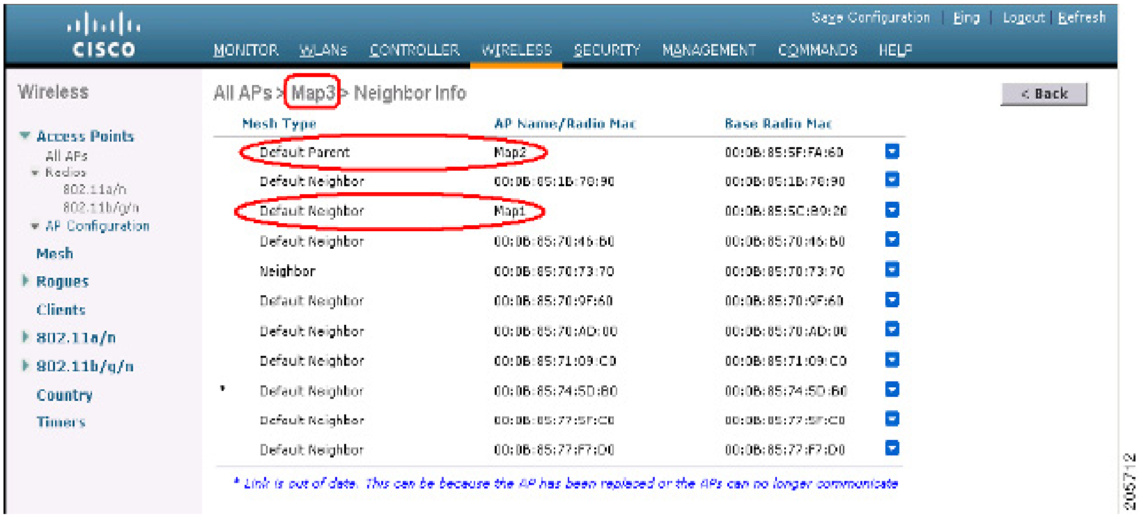
Figure 101 Neighbor Information for Child



All APs > Map2 > Neighbor Info

Mesh Type	AP Name/Radio Mac	Base Radio Mac
Parent	Rap1	00:0B:85:5F:FB:10
Neighbor	Map1	00:0B:85:5C:69:20
Default Child	Map3	00:0B:85:5F:FF:60
Neighbor	00:0B:85:70:73:70	00:0B:85:70:73:70
Neighbor	00:0B:85:74:5D:B0	00:0B:85:74:5D:B0
Default Neighbor	00:0B:85:77:5F:C0	00:0B:85:77:5F:C0
Default Neighbor	00:0B:85:77:F7:D0	00:0B:85:77:F7:D0

Figure 102 Neighbor Information for Parent



All APs > Map3 > Neighbor Info

	Mesh Type	AP Name/Radio Mac	Base Radio Mac
	Default Parent	Map2	00:0B:85:5F:FA:60
	Default Neighbor	00:0B:85:1D:70:90	00:0B:85:1D:70:90
	Default Neighbor	Map1	00:0B:85:5C:80:20
	Default Neighbor	00:0B:85:70:46:B0	00:0B:85:70:46:B0
	Neighbor	00:0B:85:70:73:70	00:0B:85:70:73:70
	Default Neighbor	00:0B:85:70:9F:60	00:0B:85:70:9F:60
	Default Neighbor	00:0B:85:70:AD:00	00:0B:85:70:AD:00
	Default Neighbor	00:0B:85:71:09:C0	00:0B:85:71:09:C0
*	Default Neighbor	00:0B:85:74:5D:B0	00:0B:85:74:5D:B0
	Default Neighbor	00:0B:85:77:5F:C0	00:0B:85:77:5F:C0
	Default Neighbor	00:0B:85:77:F7:D0	00:0B:85:77:F7:D0

* Link is out of date. This can be because the AP has been replaced or the APs can no longer communicate

Misconfiguration of the Mesh Access Point IP Address

Although most practical Layer 3 networks are deployed using DHCP IP address management, manual IP address management and allocating IP addresses statically to each mesh node might be preferred by some network administrators. Manual mesh access point IP address management can be a nightmare for large networks, but it might make sense in small to medium size networks (approx. 10-100 mesh nodes) given the number of mesh nodes are relatively small compared to client hosts.

Statically configuring the IP address on a mesh node has the possibility of putting a MAP on a wrong network, such as a subnet or VLAN. This could prevent a mesh access point from successfully resolving the IP gateway, eventually failing to discover a WLAN controller. In such a scenario, the mesh access point falls back to its DHCP mechanism and automatically attempts to find a DHCP server and obtains an IP address from it. This fallback mechanism prevents a mesh node from being potentially stranded from a wrongly configured static IP address and allows it to obtain a correct address from a DHCP server on the network.

When you are manually allocating IP addresses, we recommend that you make IP addressing changes from the furthest mesh access point child first and then work your way back to the RAP. This also applies if you relocate equipment. For example, if you uninstall a mesh access point and redeploy it in another physical location of the mesh network that has a different addressed subnet.

Another option is to take a controller in Layer 2 mode with a RAP to the location with the misconfigured MAP. Set the bridge group name on the RAP to match the MAP that needs the configuration change. Add the MAP's MAC address to the controller. When the misconfigured MAP comes up in the mesh access point summary detail, configure it with an IP address.

Misconfiguration of DHCP

Despite the DHCP fallback mechanism, there is still a possibility that a mesh access point can become stranded, if any of the following conditions exist:

- There is no DHCP server on the network.
- There is a DHCP server on the network, but it does not offer an IP address to the AP, or if it gives a wrong IP address to the AP (for example, on a wrong VLAN or subnet).

These conditions can strand a mesh access point that is configured with or without a wrong static IP address or with DHCP. Therefore, it is necessary to ensure that when a mesh access point is unable to connect after exhausting all DHCP discovery attempts or DHCP retry counts or IP gateway resolution retry counts, it attempts to find a controller in Layer 2 mode. In other words, a mesh access point attempts to discover a controller in Layer 3 mode first and in this mode, attempts with both static IP (if configured) or DHCP (if possible). The AP then attempts to discover a controller in Layer 2 mode. After finishing a number of Layer 3 and Layer 2 mode attempts, the mesh access point changes its parent node and re-attempts DHCP discovery. Additionally, the software exclusion-lists notes the parent node through which it was unable to obtain the correct IP address.

Identifying the Node Exclusion Algorithm

Depending on the mesh network design, it is entirely possible that a node finds another node "best" according to its routing metric (even recursively true), yet it is unable to provide the node with a connection to the correct controller or correct network. It is the typical *honeypot* access point scenario caused by either misplacement, provisioning, design of the network, or by the dynamic nature of an RF environment exhibiting conditions that optimize the AWPP routing metric for a particular link in a persistent or transient manner. Such conditions are generally difficult to recover from in most networks and could blackhole or sinkhole a node completely, taking it out from the network. Possible symptoms include, but are not limited to:

- A node connects to the honeypot, but cannot resolve the IP gateway when configured with static IP address, or cannot obtain the correct IP address from DHCP server, or cannot connect to a WLAN controller.
- A node ping-pongs between a few honeypots or circles between many honeypots (in worst-case scenarios).

Cisco mesh software tackles this difficult scenario using a sophisticated node exclusion-listing algorithm. This node exclusion-listing algorithm uses an exponential backoff and advance technique much like TCP sliding window or 802.11 MAC.

The basic idea relies on the following five major steps:

1. Honeypot detection—The honeypots are first detected via the following steps.

   A parent node is set by the AWPP module, by:

   – A static IP attempt in CAPWAP module.

   – A DHCP attempt in the DHCP module.

   – A CAPWAP attempt to find and connect to a controller fails.

2. Honeypot conviction—When a honeypot is detected, it is placed in a exclusion-list database with its conviction period to remain on the list. The default is 32 minutes. Other nodes are then attempted as parents in the following order, falling back to the next, upon failing the current mechanism:

   – On the same channel.

   – Across different channels (first with its own bridgegroupname and then with default).

   – Another cycle, by clearing conviction of all current exclusion-list entries.

   – Rebooting the AP.

3. Non-honeypot credit—It is often possible that a node is not a really a honeypot, but appears to be due to some transient backend condition, such as:

   – The DHCP server is either not up-and-running yet, has failed temporarily, or requires a reboot.

   – The WLAN controller is either not up-and-running yet, has failed temporarily, or requires a reboot.

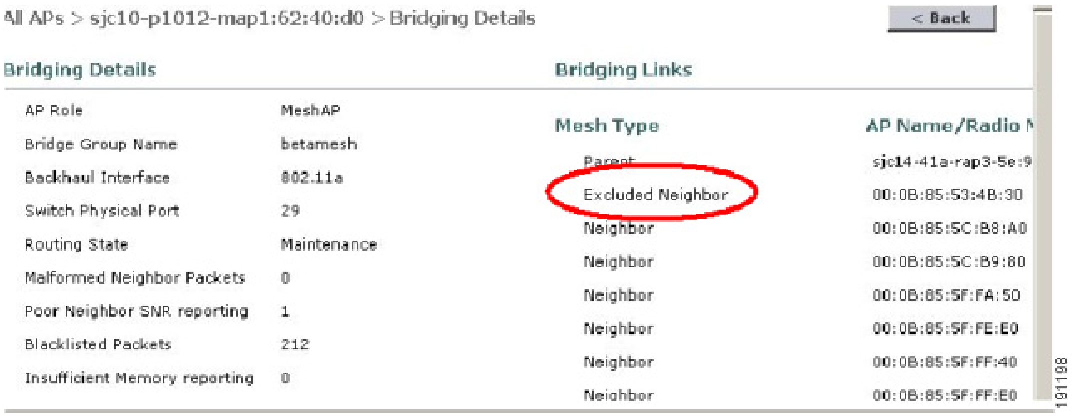
   – The Ethernet cable on the RAP was accidentally disconnected.

   Such non-honeypots must be credited properly from their serving times so that a node can come back to them as soon as possible.

4. Honeypot expiration—Upon expiration, an exclusion-list node must be removed from the exclusion-list database and return to normal state for future consideration by AWPP.

5. Honeypot reporting—Honeypots are reported to the controller via an LWAPP mesh neighbor message to the controller, which shows these on the Bridging Information page. A message is also displayed the first-time an exclusion-listed neighbor is seen. In subsequent software release, an SNMP trap will be generated on the controller for this condition so that Cisco WCS can record the occurrence. Figure 103 shows the bridging details.

Figure 103 Excluded Neighbor



All APs > sjc10-p1012-map1:62:40:d0 > Bridging Details

Bridging Details

AP Role	MeshAP
Bridge Group Name	betamesh
Backhaul Interface	802.11a
Switch Physical Port	29
Routing State	Maintenance
Malformed Neighbor Packets	0
Poor Neighbor SNR reporting	1
Blacklisted Packets	212
Insufficient Memory reporting	0

Bridging Links

Mesh Type	AP Name/Radio M
Parent	sjc14-41a-rap3-5e:9
Excluded Neighbor	00:0B:85:53:4B:30
Neighbor	00:0B:85:5C:B8:A0
Neighbor	00:0B:85:5C:B9:80
Neighbor	00:0B:85:5F:FA:50
Neighbor	00:0B:85:5F:FE:E0
Neighbor	00:0B:85:5F:FF:40
Neighbor	00:0B:85:5F:FF:E0

Because there could be many nodes attempting to join or re-join the network after an expected or unexpected event, a hold-off time of 16 minutes is implemented. This means that no nodes are exclusion-listed during this period of time after system initialization.

This exponential backoff and advance algorithm is unique and has the following useful properties:

- It allows a node to correctly identify the parent nodes whether it is a true honeypot or is just experiencing temporary outage conditions.
- It credits the good parent nodes according to the time it has enabled a node to stay connected with the network and the crediting requires lesser and lesser time over period in order to bring the exclusion-list conviction period to be very low for real transient conditions and not so low for transient to moderate outages.
- It has built-in hysteresis for encountering the initial condition issue where many nodes try to discover each other only to find that those are not really meant to be in the same network.
- It has built-in memory for nodes that can appear as neighbors sporadically so they are not accidentally considered as parents if they were, or are supposed to be, on the exclusion-list database.

The node exclusion-listing algorithm is constructed to guard the mesh network against serious stranding, which was observed in customers' networks. It integrates into AWPP in such a way that a node can quickly (re-)converge and find the correct network under many kinds of adversities.

Throughput Analysis

Throughput depends on packet error rate and hop count.

Throughput is calculated as:

*Throughput = BR * 0.5 * 1/n * PSR*

BR = Raw backhaul rate, i.e. 18, 24 Mbps

n = Backhaul hop count

PSR = Packet success rate = (1.0-PER) = (0.0 .. 1.0)

Two assumptions apply to this calculation:

- There is no other traffic on the mesh
- 1/n factor is based on all hops hearing each other.

Generally, the throughput numbers per hop are as shown in Table 24.

Table 24 Throughput Numbers Per Hop

Hops	Throughput
One	Approximately 14 Mbps
Two	Approximately 8 Mbps
Three	Approximately 3 Mbps
Four	Approximately up to 1 Mbps

Capacity and throughput are orthogonal concepts. Throughput is one user's experience at node *N* and total area capacity is calculated over the entire sector of *N*-nodes and is based on the number of ingress and egress RAP, assuming separate non-interfering channels.

For example, 4 RAPs at 10 Mbps each deliver 40 Mbps total capacity. So, one user at 2 hops out, logically under each RAP, could get 5 Mbps each of TPUT, but consume 40 Mbps of backhaul capacity.

With the Cisco Mesh solution, the per-hop latency is less than 10 msecs, and the typical latency numbers per hop range from 1~3 msecs. Overall jitter is also less than 3 msecs.

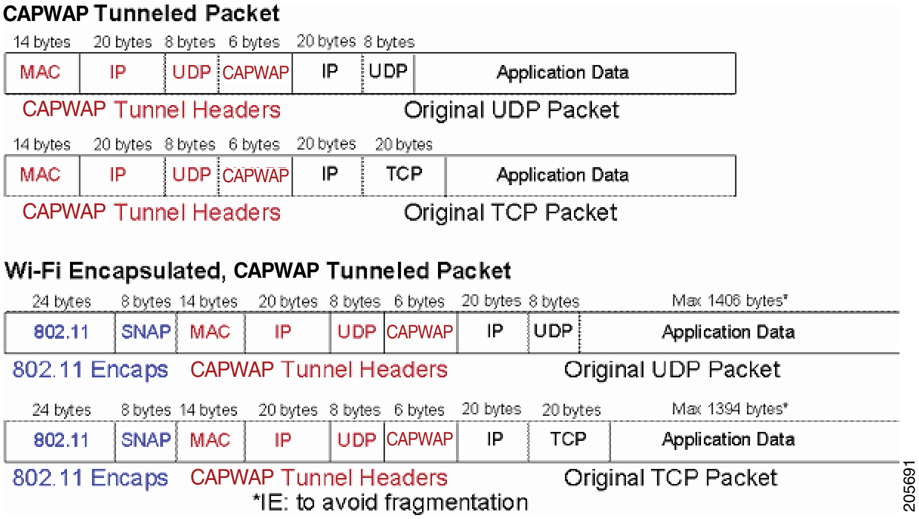
Throughput depends on the type of traffic being passed through the network. Traffic can be User Datagram Protocol (UDP) or Transmission Control Protocol (TCP). UDP sends a packet over Ethernet with a source and destination address and a UDP protocol header. It does not expect an acknowledgement (ACK). There is no assurance that the packet is delivered at the application layer.

TCP is similar to UDP but it is a reliable packet delivery mechanism. There are packet acknowledgments and a sliding window technique is used to allow the sender to transmit multiple packets before waiting for an ACK. There is a maximum amount of data the client will transmit (called a TCP socket buffer window) before it stops sending data. Sequence numbers are used to track packets sent and to ensure that they arrive in the correct order. TCP uses cumulative ACKs and the receiver reports how much of the current stream has been received. An ACK might cover any number of packets, up to the TCP window size.

TCP uses slow start and multiplicative decrease to respond to network congestion or packet loss. When a packet is lost, the TCP window will be cut in half and the back-off retransmission timer will be increased exponentially. Wireless is subject to packet loss due to interference issues and TCP will react to this packet loss. There is also a slow start recovery algorithm that is used to avoid swamping a connection when recovering from packet loss. The natural effect of these algorithms in a lossy network environment is to lessen the overall throughput of a traffic stream.

By default, the maximum segment size (MSS) of TCP is 1460 bytes, which results in a 1500-byte IP datagram. Therefore, TCP fragments any data packet that is larger than 1460 bytes, which can cause at least 30% throughput drop. In addition, the Cisco controller encapsulates IP datagrams in the 48-byte CAPWAP tunnel header as illustrated in Figure 104. Therefore, any data packet that is longer than 1394 bytes is also fragmented by the controller, which results in up to 15% throughput decrease.

Figure 104 CAPWAP Tunneled Packets



Adding and Managing Mesh Access Points with Cisco WCS

To configure and monitor mesh networks from Cisco WCS, you must first import campus and outdoor maps into Cisco WCS and add buildings. Thereafter, you can add mesh access points to the map and configure and monitor mesh access points from Cisco WCS.

See the following sections for details:

- "Adding Campus Maps, Outdoor Areas, and Buildings with Cisco WCS"
- "Adding Mesh Access Points to Maps with Cisco WCS"
- "Monitoring Mesh Access Points Using Google Earth"
- "Adding Indoor Mesh Access Points to Cisco WCS"
- "Managing Mesh Access Points with Cisco WCS"
- "Monitoring WGBs"
- "Workgroup Bridge Interoperability with Mesh Infrastructure"
- "Locally Significant Certificates for Mesh APs"
- "Cable Modem Serial Port Access From an AP"
- "Viewing AP Last Reboot Reason"

Adding Campus Maps, Outdoor Areas, and Buildings with Cisco WCS

For mesh networks, maps and items on those maps (buildings and mesh access points) are added to Cisco WCS in the following order:

1. Add campus map
2. Add outdoor area map
3. Add buildings
4. Add mesh access points

Detailed steps for adding these maps and components are noted below.

Adding Campus Maps

To add a single campus map to the Cisco WCS database, follow these steps:

Step 1 Save the map in .PNG, .JPG, .JPEG, or .GIF format.

Note The map can be any size because Cisco WCS automatically resizes the map to fit its working areas.

Step 2 Browse to and import the map from anywhere in your file system.

Step 3 Choose **Monitor** > **Maps** to display the Maps page.

Step 4 From the Select a command drop-down menu, choose **New Campus** and click **GO**.

Step 5 On the Maps > New Campus page, enter the campus name and campus contact name.

Step 6 Browse to and choose the image filename containing the map of the campus and click **Open**.

Step 7 Select the **Maintain Aspect Ratio** check box to prevent length and width distortion when Cisco WCS resizes the map.

Step 8 Enter the horizontal and vertical span of the map in feet.

Note The horizontal and vertical span should be larger than any building or floor plan to be added to the campus.

Step 9 Click OK to add this campus map to the Cisco WCS database. Cisco WCS displays the Maps page, which lists maps in the database, map types, and campus status.

Adding Outdoor Areas

To add an outdoor area to a campus map, follow these steps:

Note You can add outdoor areas to a campus map in the Cisco WCS database regardless of whether you outdoor area maps are in the database.

Step 1 If you want to add a map of the outdoor area to the database, save the map in .PNG, .JPG, .JPEG, or .GIF format. Then browse to and import the map from anywhere in your file system.

Note You do not need a map to add an outdoor area. You can simply define the dimensions of the area to add it to the database. The map can be any size because Cisco WCS automatically resizes the map to fit the workspace.

Step 2 Choose **Monitor** > **Maps** to display the Maps page.

Step 3 Click the desired campus. Cisco WCS displays the Maps > *Campus Name* page.

Step 4 From the Select a command drop-down menu, choose **New Outdoor Area** and click **GO**.

Step 5 On the *Campus Name* > New Outdoor Area page, follow these steps to create a manageable outdoor area:

a. Enter the outdoor area name.

b. Enter the outdoor area contact name.

c. If desired, enter or browse to the filename of the outdoor area map.

d. Enter an approximate outdoor horizontal span and vertical span (width and depth on the map) in feet.

Tip You can also use **Ctrl-click** to resize the bounding area in the upper left corner of the campus map. As you change the size of the bounding area, the Horizontal Span and Vertical Span parameters of the outdoor area change to match your actions.

e. Click **Place** to put the outdoor area on the campus map. Cisco WCS creates an outdoor area rectangle scaled to the size of the campus map.

f. Click on the outdoor area rectangle and drag it to the desired position on the campus map.

g. Click **Save** to save this outdoor area and its campus location to the database. Cisco WCS saves the outdoor area name in the outdoor area rectangle on the campus map.

Note A hyperlink associated with the outdoor area takes you to the corresponding Map page

Step 6 Click **Save**.

Adding a Building to a Campus Map

You can add buildings to the Cisco WCS database regardless of whether you have added campus maps to the database. This section explains how to add a building to a campus map or a standalone building (one that is not part of a campus) to the Cisco WCS database.

To add a building to a campus map in the Cisco WCS database, follow these steps:

Step 1 Choose **Monitor > Maps** to display the Maps page.

Step 2 Click the desired campus. Cisco WCS displays the Maps > *Campus Name* page.

Step 3 From the Select a command drop-down menu, choose **New Building** and click **GO**.

Step 4 On the *Campus Name* > New Building page, follow these steps to create a virtual building in which to organize related floor plan maps:

a. Enter the building name.

b. Enter the building contact name.

c. Enter the number of floors and basements.

d. Enter an approximate building horizontal span and vertical span (width and depth on the map) in feet.

Tip The horizontal and vertical span should be larger than or the same size as any floors that you might add later.You can also use Ctrl-click to resize the bounding area in the upper left corner of the campus map. As you change the size of the bounding area, the Horizontal Span and Vertical Span parameters of the building change to match your actions.

e. Click **Place** to put the building on the campus map. Cisco WCS creates a building rectangle scaled to the size of the campus map.

f. Click on the building rectangle and drag it to the desired position on the campus map.

Note After adding a new building, you can move it from one campus to another without having to recreate it.

g. Click **Save** to save this building and its campus location to the database. Cisco WCS saves the building name in the building rectangle on the campus map.

Note A hyperlink associated with the building takes you to the corresponding Map page.

Step 5 Click **Save**.

Adding Mesh Access Points to Maps with Cisco WCS

After you add the .PNG, .JPG, .JPEG, or .GIF format floor plan and outdoor area maps to the Cisco WCS database, you can position mesh access point icons on the maps to show where they are installed in the buildings.

To add mesh access points to floor plan and outdoor area maps, follow these steps:

Step 1 Click the desired floor plan or outdoor area map in the Coverage Areas component of the General tab. Cisco WCS displays the associated coverage area map.

Step 2 From the Select a command drop-down menu, choose **Add Access Points** and click **GO**.

Step 3 On the Add Access Points page, choose the mesh access points to add to the map.

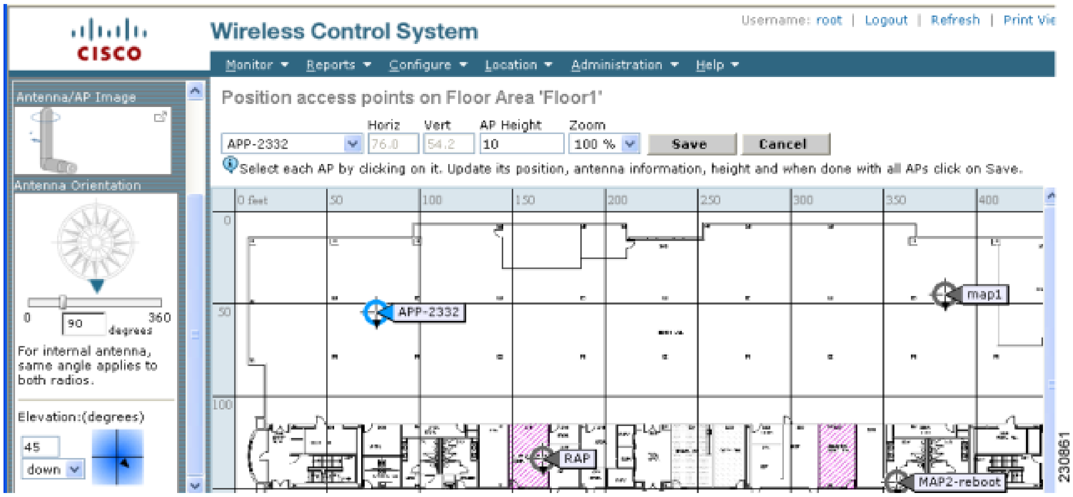
Step 4 Click **OK** to add the mesh access points to the map and display the Position Access Points map.

Note The mesh access point icons appear in the upper left area of the map.

Step 5 Click and drag the icons to indicate their physical locations.

Step 6 Click each icon and choose the antenna orientation in the sidebar (see Figure 105).

Figure 105 Antenna Sidebar



Position access points on Floor Area 'Floor1'

APP-2332 | Horiz 76.0 | Vert 54.2 | AP Height 10 | Zoom 100 %

Select each AP by clicking on it. Update its position, antenna information, height and when done with all APs click on Save.

Antenna orientation: 90 degrees

For internal antenna, same angle applies to both radios.

Elevation:(degrees) 45 down

The antenna angle is relative to the map's X axis. Because the origin of the X (horizontal) and Y (vertical) axes is in the upper left corner of the map, 0 degrees points side A of the mesh access point to the right, 90 degrees points side A down, 180 degrees points side A to the left, and so on. The antenna elevation is used to move the antenna vertically, up or down, to a maximum of 90 degrees.

Make sure each mesh access point is in the correct location on the map and has the correct antenna orientation. Accurate mesh access point positioning is critical when you use the maps to find coverage holes and rogue access points.

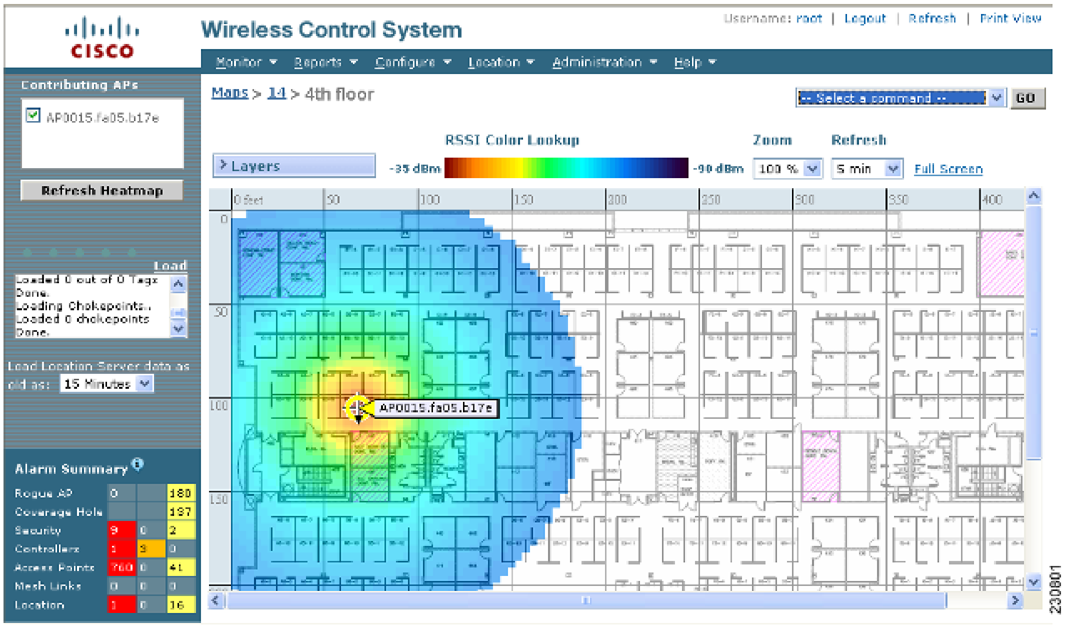
See this location for further information about the antenna elevation and azimuth patterns:

http://www.cisco.com/en/US/products/hw/wireless/ps469/tsd_products_support_series_home.html

Step 7 Click **Save** to store the mesh access point locations and orientations. Cisco WCS computes the RF prediction for the coverage area. These RF predictions are popularly known as *heat maps* because they show the relative intensity of the RF signals on the coverage area map. Figure 106 shows an RF prediction heat map.

Note This display is only an approximation of the actual RF signal intensity because it does not take into account the attenuation of various building materials, such as drywall or metal objects, nor does it display the effects of RF signals bouncing off obstructions.

Figure 106 RF Prediction Heat Map



☑ AP0015.fa05.b17e

Zoom: 100 %

Refresh: 5 min

```
Loaded 0 out of 0 Tags
Done.
Loading Chokepoints..
Loaded 0 chokepoints
Done.
```

Load Location Server data as old as: 15 Minutes

Alarm Summary			
Rogue AP	0		180
Coverage Hole			197
Security	9	0	2
Controllers	1	3	0
Access Points	760	0	41
Mesh Links	0	0	0
Location	1	0	16

Monitoring Mesh Access Points Using Google Earth

Cisco WCS supports both Google Earth Map Plus or Pro and displays, when present, mesh access points and their links.

Launching Google Earth in Cisco WCS

Cisco WCS supports both Google Earth Map Plus or Pro and displays, when present, mesh access points and their links.

To launch Google Earth maps, follow these steps:

Step 1 Launch Google Earth plus or pro and add a new folder.

Step 2 Create a mesh access points placemark on Google Earth plus or pro.

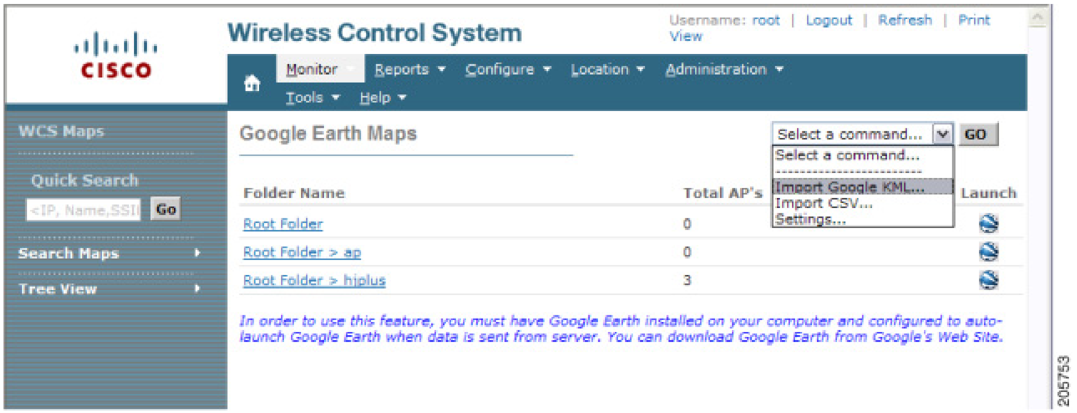
Note You must use the exact name of the mesh access point when creating the placement mark to ensure Cisco WCS can recognize these mesh access points.

Step 3 Place the mesh access point placemarks in the new folder. Save the folder as a .KML file.

Step 4 In Cisco WCS, choose **Monitor > Google Earth Maps**. Select Import Google KML from the Select a command drop-down list.

Step 5 Import the new Google KML folder (see Figure 107). It displays in the folder name summary.

Figure 107 Importing New Folder into Google Earth



Folder Name	Total AP's	Launch
Root Folder	0	
Root Folder > ap	0	
Root Folder > hiplus	3	

In order to use this feature, you must have Google Earth installed on your computer and configured to auto-launch Google Earth when data is sent from server. You can download Google Earth from Google's Web Site.

Step 6 Click the launch icon next to the new folder to launch the Google Earth map from Cisco WCS.

Viewing Google Earth Maps

You can view campus maps, mesh access point and link information using Google maps.

To view Google Earth maps, follow these steps:

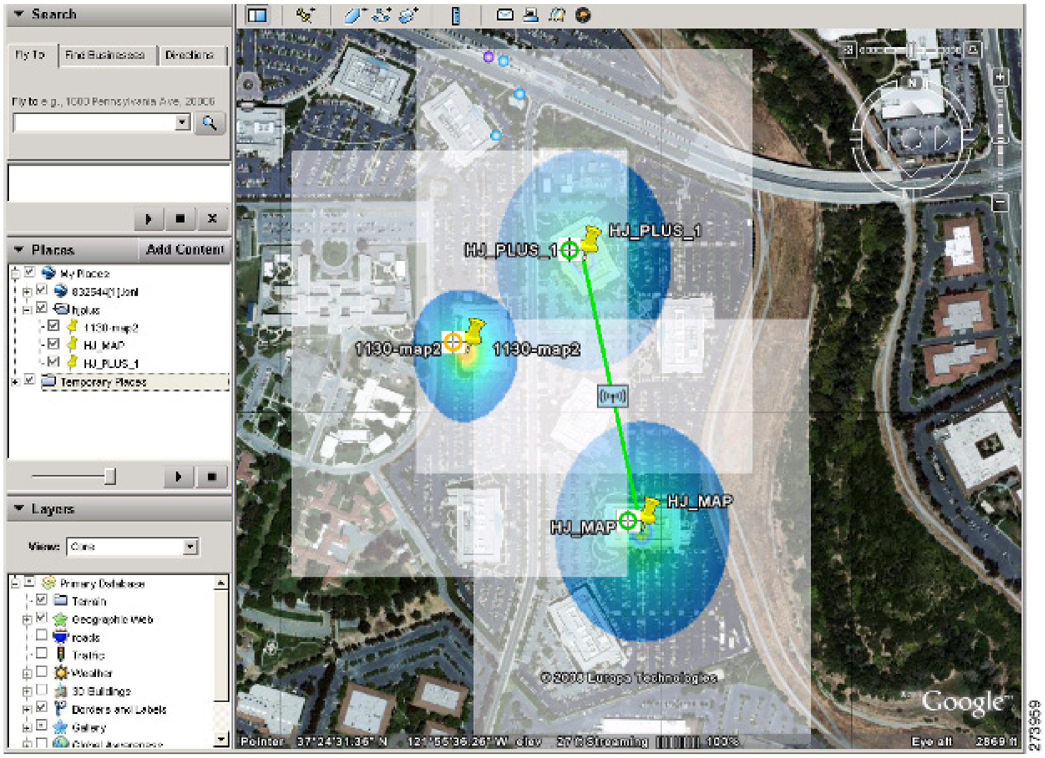
Step 1 Log on to Cisco WCS.

Step 2 Choose **Monitor > Google Earth Maps**. The Google Earth Maps page displays all folders and the number of mesh access points included within each folder.

Step 3 Click **Launch** for the map you want to view. Google Earth opens in a separate window and displays the location and its mesh access points. (see Figure 108.)

Note To use this feature, you must have Google Earth installed on your computer and configured to auto-launch when data is sent from the server. You can download Google Earth from Google's website.

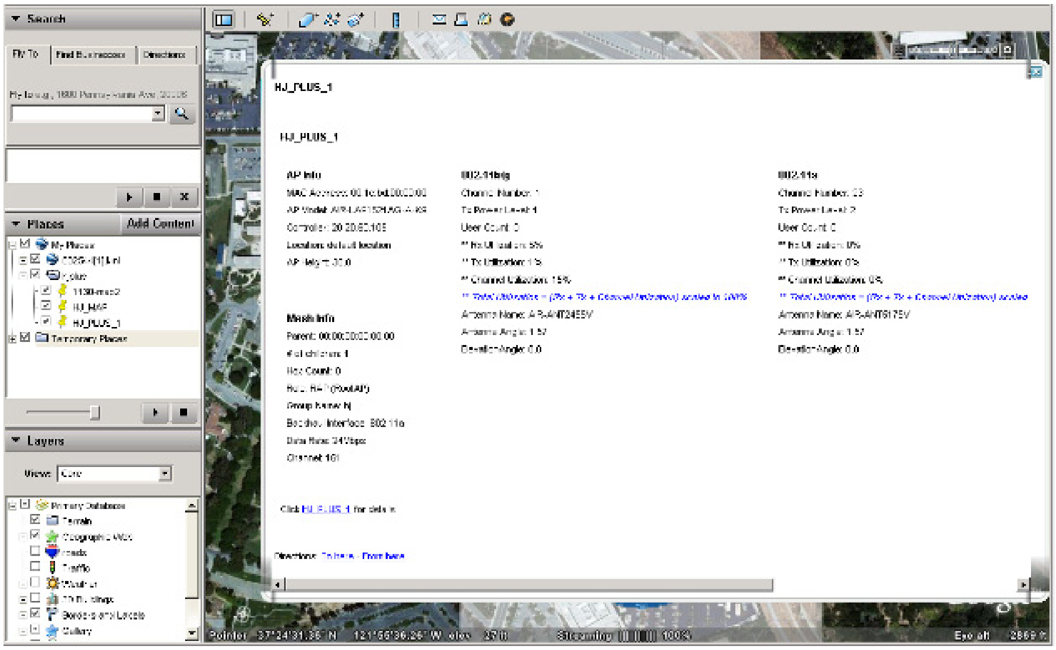
Figure 108 Google Earth Map Page



Step 4 Click **Launch** for the map you want to view (see Figure 109 and Figure 110). Google Earth opens in a separate window and displays the location and its mesh access points.

Note To use this feature, you must have Google Earth installed on your computer and configured to auto-launch when data is sent from the server. You can download Google Earth from Google's website.

Figure 109 Google Earth Map With Mesh Access Point Details



HJ_PLUS_1

HJ_PLUS_1

AP Info
MAC Address: 00:1c:b1:00:00:00
AP Model: AIR-LAP1521AG-A-K9
Controller: 20.20.60.105
Location: default location
AP Height: 30.0

Mesh Info
Parent: 00:00:00:00:00:00
# of children: 1
Hop Count: 0
Role: RAP (RootAP)
Group Name: hj
Backhaul Interface: 802.11a
Data Rate: 24Mbps
Channel: 161

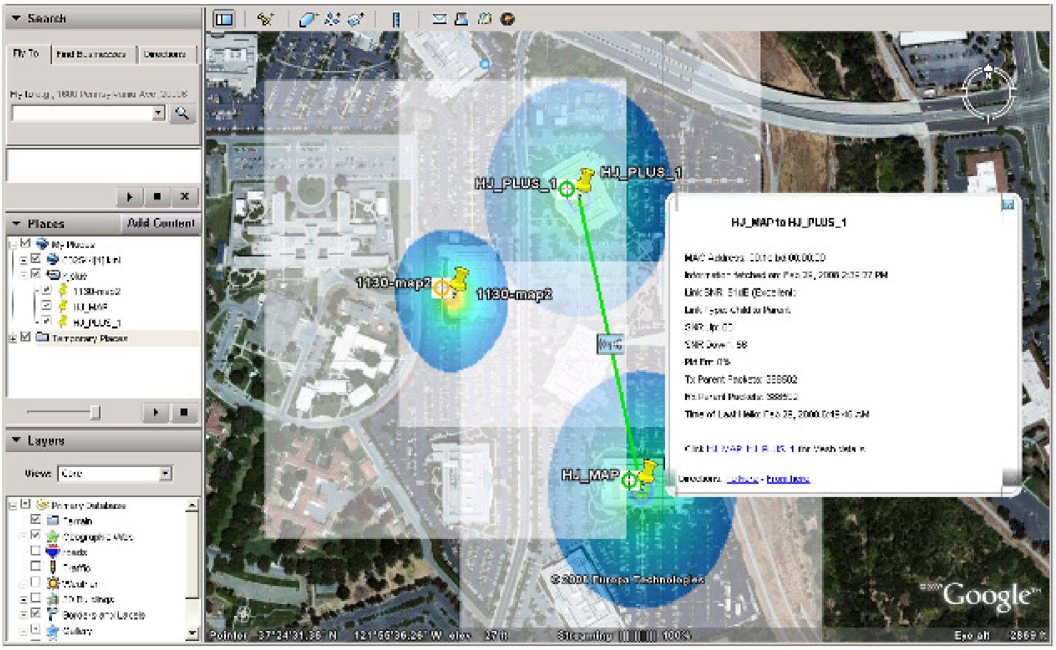
802.11b/g
Channel Number: 1
Tx Power Level: 1
User Count: 0
** Rx Utilization: 5%
** Tx Utilization: 1%
** Channel Utilization: 15%
*** Total Utilization = (Rx + Tx + Channel Utilization) scaled to 100%*
Antenna Name: AIR-ANT2455V
Antenna Angle: 1.57
Elevation Angle: 0.0

802.11a
Channel Number: 23
Tx Power Level: 2
User Count: 0
** Rx Utilization: 0%
** Tx Utilization: 0%
** Channel Utilization: 0%
*** Total Utilization = (Rx + Tx + Channel Utilization) scaled*
Antenna Name: AIR-ANT5175V
Antenna Angle: 1.57
Elevation Angle: 0.0

Click HJ_PLUS_1 for details

Directions: To here - From here

Figure 110 Google Earth Map With Mesh Link Details



HJ_MAP to HJ_PLUS_1

MAC Address: 00:1c:b0:00:00:00
Information fetched on: Feb 29, 2008 2:39:37 PM
Link SNR: 51dB (Excellent)
Link Type: Child to Parent
SNR Up: 60
SNR Down: 58
Pkt Err: 0%
Tx Parent Packets: 388502
Rx Parent Packets: 388502
Time of Last Hello: Feb 28, 2008 6:45:46 AM

Click HJ_MAP_HJ_PLUS_1 for Mesh details

Directions: To here - From here

To view details for a Google Earth Map folder, follow these steps:

Step 1 From the Google Earth Map page, click the folder name to open the details page for this folder. The Google Earth Details page provides the mesh access point names and MAC or IP addresses.

Note To delete a mesh access point, select the applicable check box and click **Delete**.
To delete the entire folder, select the check box next to **Folder Name** and click **Delete**. Deleting a folder also deletes all subfolders and mesh access points inside the folder.

Step 2 Click **Cancel** to close the details page.

Adding Indoor Mesh Access Points to Cisco WCS

You have a choice of ordering indoor access points (1130 or 1240) directly into the bridge mode, so that these access points can be used directly as mesh access points. If you have these access points in a local mode (nonmesh), then you have to connect these access points to the controller and change the radio role to the bridge mode (mesh). This can become cumbersome particularly if the volume of the access points being deployed is large and if the access points are already deployed in the local mode for a traditional nonmesh wireless coverage.

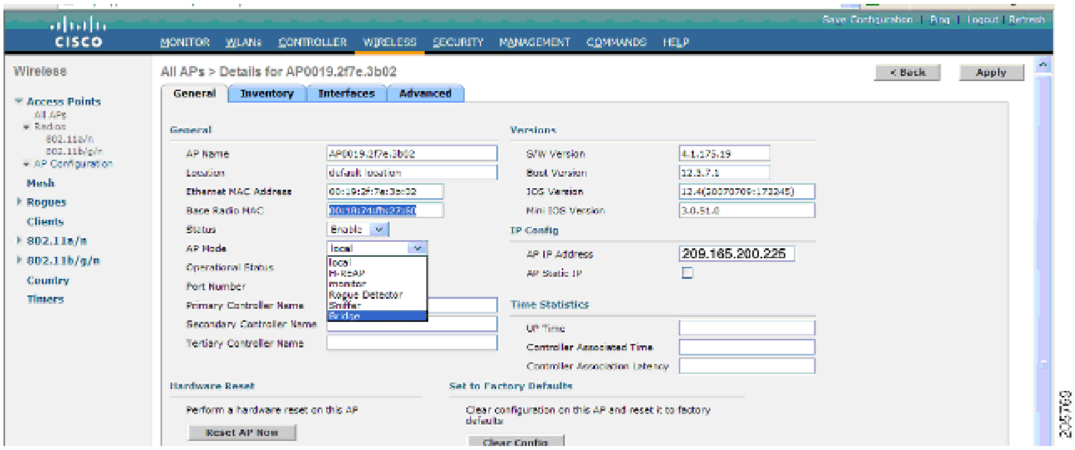
For local mode indoor access points prior to a mesh installation, you must first connect all indoor mesh access points to the controller and change the mode to *bridge* mode.

To do so, connect all the indoor access points (AP1130, AP1240) to the Layer 3 network on the same subnet as the Management IP address.

Add the MAC address of the indoor mesh access points into the MAC filter list on the controller. All indoor access points will then join the controller in local mode.

You can then change local mode to bridge mode in the controller for every indoor access point (see Figure 111).

Figure 111 All APs > AP Details Controller Page



All APs > Details for AP0019.2f7e.3b02

General

AP Name	AP0019.2f7e.3b02
Location	default location
Ethernet MAC Address	00:19:2f:7e:3b:02
Base Radio MAC	[illegible]
Status	Enable
AP Mode	local
Operational Status	
Port Number	
Primary Controller Name	
Secondary Controller Name	
Tertiary Controller Name	

Versions

S/W Version	4.1.175.19
Boot Version	12.3.7.1
IOS Version	12.4(20070709:172245)
Mini IOS Version	3.0.51.0

IP Config

AP IP Address	209.165.200.225
AP Static IP	□

Time Statistics

UP Time	
Controller Associated Time	
Controller Association Latency	

Hardware Reset

Perform a hardware reset on this AP

Set to Factory Defaults

Clear configuration on this AP and reset it to factory defaults

After changing the indoor access points to bridge mode on the controller, add these indoor mesh access points into Cisco WCS.

You cannot initially configure AP1130 and AP1240 into bridge mode from Cisco WCS.

Managing Mesh Access Points with Cisco WCS

Cisco WCS is a complete platform for enterprise-wide WLAN systems management. It provides a wide range of tools for visualizing and controlling the mesh, including histograms of signal-to-noise ratio, mesh detail information, mesh access point neighbor and link information, seven-day temporal link information, and tools to identify and avoid RF interference.

This section addresses the following Cisco WCS monitoring capabilities:

- "Monitoring Mesh Networks Using Maps" section on page 188
- "Monitoring Mesh Health" section on page 195
- "Mesh Statistics for a Mesh Access Point" section on page 199
- "Viewing the Mesh Network Hierarchy" section on page 204
- "Using Mesh Filters to Modify Map Display of Maps and Mesh Links" section on page 205

Monitoring Mesh Networks Using Maps

You can access and view details for the following elements from a mesh network map in Cisco WCS:

- Mesh Link Statistics
- Mesh Access Points
- Mesh Access Point Neighbors

Details on how this information is accessed and the information displayed for each of these items is detailed in the following sections.

Monitoring Mesh Link Statistics Using Maps

You can view the SNR for a specific mesh network link, view the number of packets transmitted and received on that link, and initiate a link test from the Monitor > Maps display.

To view details on a specific mesh link between two mesh access points or a mesh access point and a root access point, follow these steps:

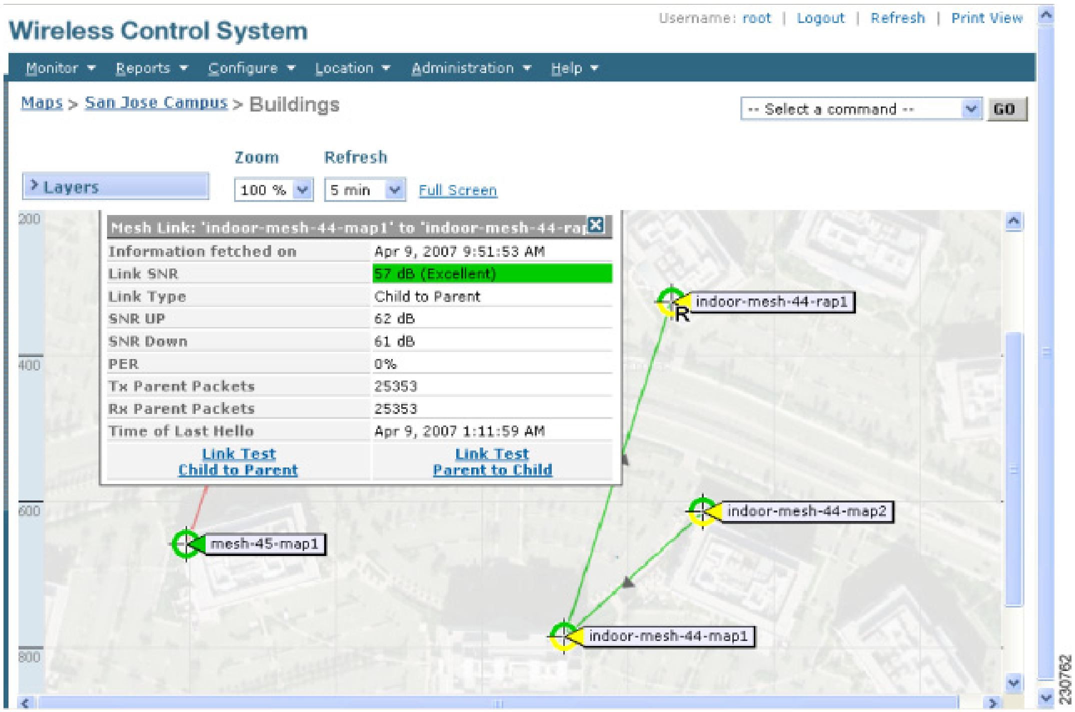
Step 1 In Cisco WCS, choose **Monitor > Maps**.

Step 2 Click the **Map Name** that corresponds to the outdoor area, campus, building, or floor you want to monitor.

Step 3 Move the cursor over the link arrow for the target link (see Figure 112). A Mesh Link page appears.

Note The AP Mesh Info check box under the Layers drop-down list must be selected for links to appear on the map.

Figure 112 Mesh Link Details Page


Wireless Control System
Username: root | Logout | Refresh | Print View
Monitor ▾ Reports ▾ Configure ▾ Location ▾ Administration ▾ Help ▾
Maps > San Jose Campus > Buildings
-- Select a command -- GO
Zoom Refresh
Layers
100 % 5 min Full Screen
200
400
600
800
indoor-mesh-44-rap1
R
indoor-mesh-44-map2
mesh-45-map1
indoor-mesh-44-map1
230762

Mesh Link: 'indoor-mesh-44-map1' to 'indoor-mesh-44-rap

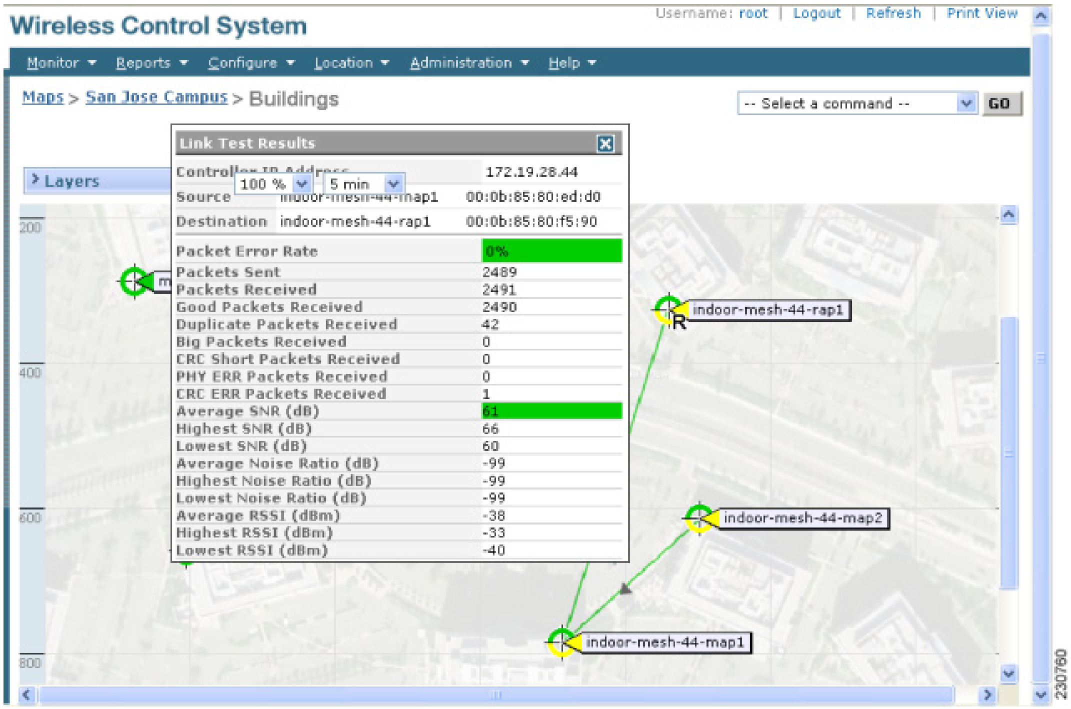
Information fetched on	Apr 9, 2007 9:51:53 AM
Link SNR	57 dB (Excellent)
Link Type	Child to Parent
SNR UP	62 dB
SNR Down	61 dB
PER	0%
Tx Parent Packets	25353
Rx Parent Packets	25353
Time of Last Hello	Apr 9, 2007 1:11:59 AM
Link Test Child to Parent	Link Test Parent to Child

Step 4 Click either **Link Test**, **Child to Parent or Link Test**, or **Parent to Child**. After the link test is complete, a results page appears (see Figure 113).

Note A link test runs for 30 seconds.

Note You cannot run link tests for both links (child-to-parent and parent-to-child) at the same time.

Figure 113 Link Test Results


Wireless Control System
Username: root | Logout | Refresh | Print View
Monitor ▾ Reports ▾ Configure ▾ Location ▾ Administration ▾ Help ▾
Maps > San Jose Campus > Buildings
-- Select a command --
GO
Layers
100 %
5 min
200
400
600
800
indoor-mesh-44-rap1
R
indoor-mesh-44-map2
indoor-mesh-44-map1
230760

Link Test Results

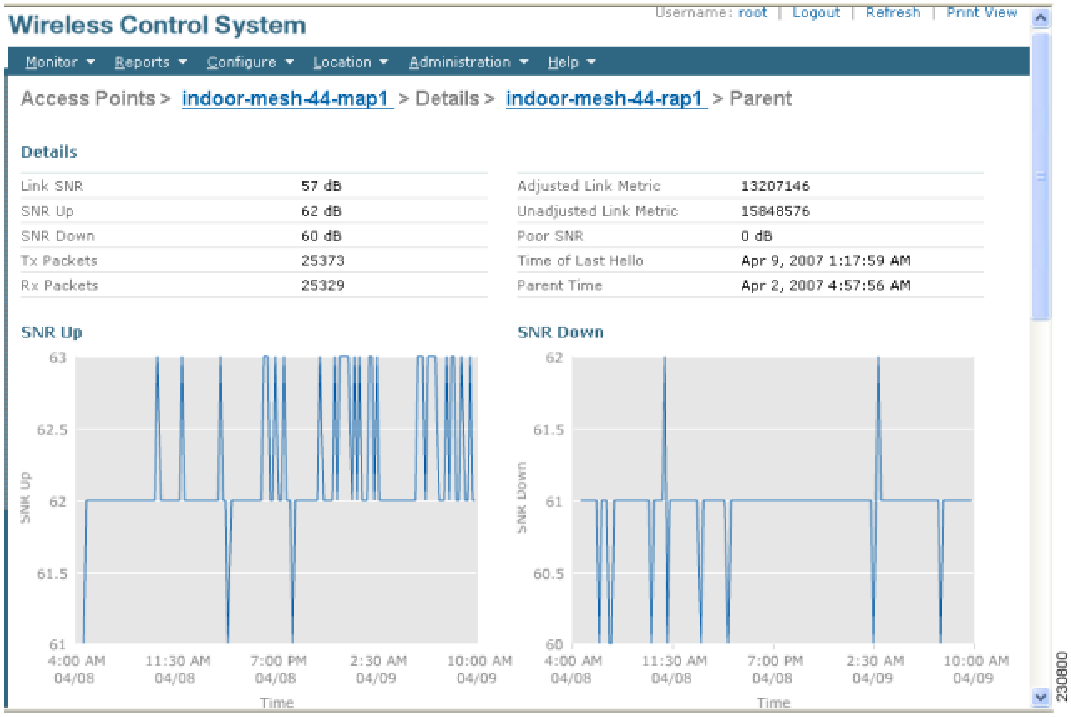
Controller IP Address		172.19.28.44
Source	indoor-mesh-44-map1	00:0b:85:80:ed:d0
Destination	indoor-mesh-44-rap1	00:0b:85:80:f5:90
Packet Error Rate		0%
Packets Sent		2489
Packets Received		2491
Good Packets Received		2490
Duplicate Packets Received		42
Big Packets Received		0
CRC Short Packets Received		0
PHY ERR Packets Received		0
CRC ERR Packets Received		1
Average SNR (dB)		61
Highest SNR (dB)		66
Lowest SNR (dB)		60
Average Noise Ratio (dB)		-99
Highest Noise Ratio (dB)		-99
Lowest Noise Ratio (dB)		-99
Average RSSI (dBm)		-38
Highest RSSI (dBm)		-33
Lowest RSSI (dBm)		-40

Step 5 To view a graphical representation of SNR statistics over a period of time, click the arrow on the link. A page with multiple SNR graphs appears (see Figure 114).

The following graphs are displayed for the link:

- SNR Up—Plots the RSSI values of the neighbor from the perspective of the mesh access point.
- SNR Down—Plots the RSSI values that the neighbor reports to the mesh access point.
- Link SNR—Plots a weighed and filtered measurement based on the SNR Up value.
- The Adjusted Link Metric —Plots the value used to determine the least cost path to the root mesh access point. This value is the ease to get to the rooftop access point and accounts for the number of hops. The lower the ease value, the less likely the path is used.
- The Unadjusted Link Metric —Plots the least cost path to get to the root access point unadjusted by the number of hops. The higher the value for the unadjusted link, the better the path.

Figure 114 Mesh SNR Graphs page (Top)



Details

Link SNR	57 dB	Adjusted Link Metric	13207146
SNR Up	62 dB	Unadjusted Link Metric	15848576
SNR Down	60 dB	Poor SNR	0 dB
Tx Packets	25373	Time of Last Hello	Apr 9, 2007 1:17:59 AM
Rx Packets	25329	Parent Time	Apr 2, 2007 4:57:56 AM

Monitoring Mesh Access Points Using Maps

You can view the following summary information for a mesh access point from a mesh network map:

- Parent
- Number of children
- Hop count
- Role
- Group name
- Backhaul interface
- Data Rate
- Channel

Note This information is in addition to the information shown for all mesh access points (MAC address, mesh access point model, controller IP address, location, height of mesh access point, mesh access point up time, and CAPWAP up time).

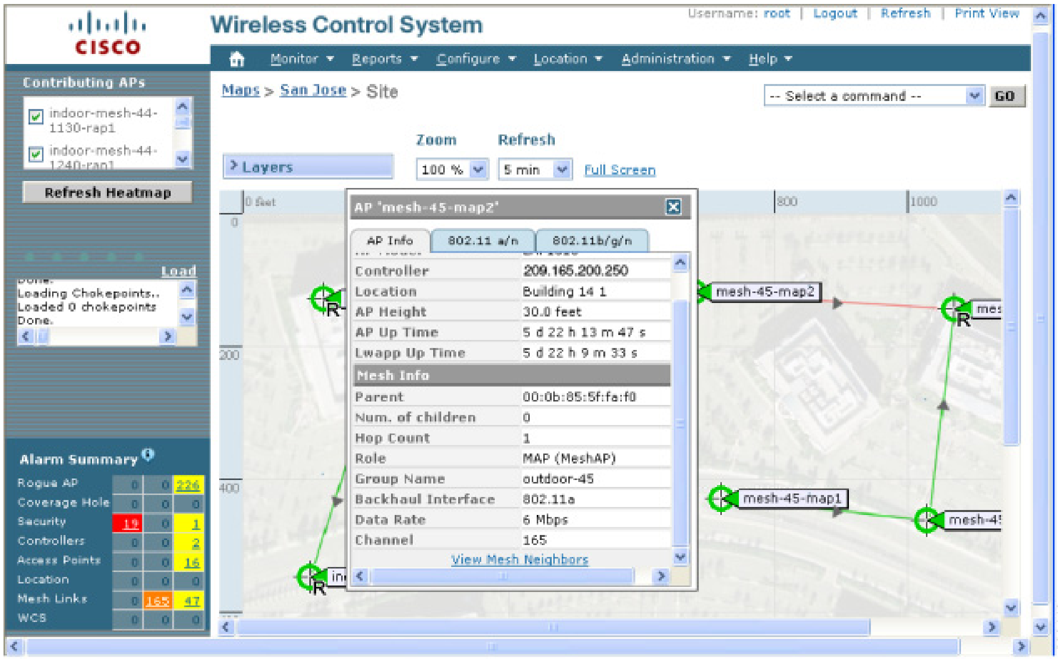
To view summary and detailed configuration information for a mesh access point from a mesh network map, follow these steps:

Step 1 In Cisco WCS, choose **Monitor > Maps**.

Step 2 Click the **Map Name** that corresponds to the outdoor area, campus, building, or floor location of the mesh access point you want to monitor.

Step 3 To view summary configuration information for a mesh access point, move the cursor over the mesh access point that you want to monitor. A page with configuration information for the selected mesh access point appears (see Figure 115).

Figure 115 Mesh AP Summary Panel



AP 'mesh-45-map2'

AP Info | 802.11 a/n | 802.11b/g/n

Controller	209.165.200.250
Location	Building 14 1
AP Height	30.0 feet
AP Up Time	5 d 22 h 13 m 47 s
Lwapp Up Time	5 d 22 h 9 m 33 s
Mesh Info	
Parent	00:0b:85:5f:fa:f0
Num. of children	0
Hop Count	1
Role	MAP (MeshAP)
Group Name	outdoor-45
Backhaul Interface	802.11a
Data Rate	6 Mbps
Channel	165

View Mesh Neighbors

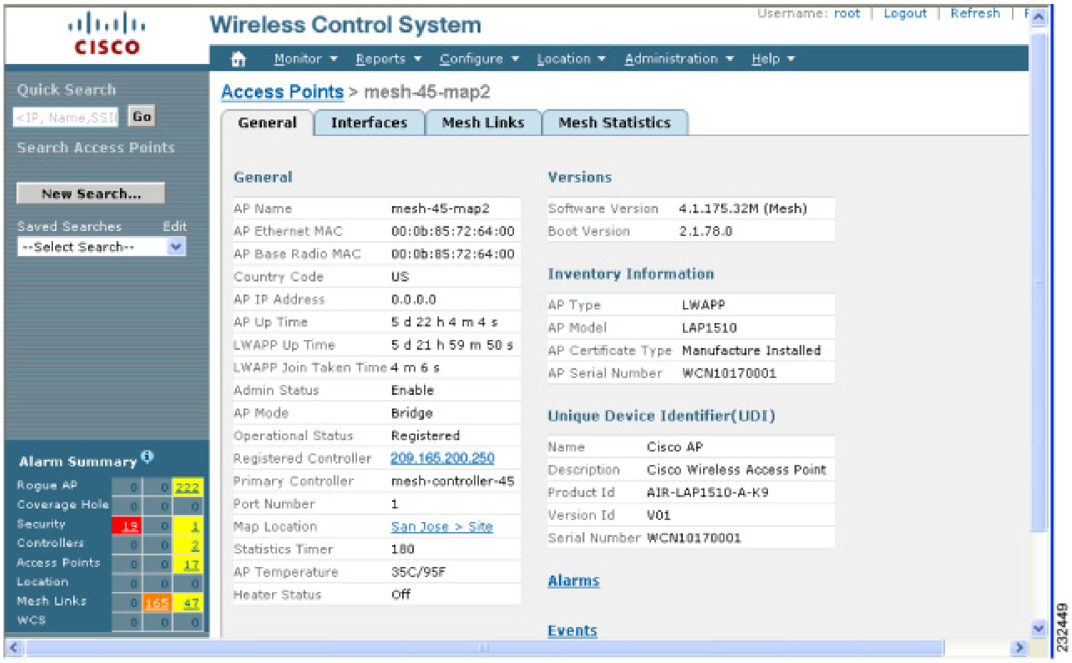
Alarm Summary

Rogue AP	0	0	226
Coverage Hole	0	0	0
Security	19	0	1
Controllers	0	0	2
Access Points	0	0	16
Location	0	0	0
Mesh Links	0	165	47
WCS	0	0	0

Step 4 To view detailed configuration information for a mesh access point, click the arrow portion of the mesh access point label. The configuration details for the mesh access point appears (see Figure 116).

Note For more details on the View Mesh Neighbors link in the mesh access point panel above, see the "Monitoring Mesh Access Point Neighbors Using Maps" section on page 193. If the mesh access point has an IP address, a Run Ping Test link is also visible at the bottom of the mesh access point panel.

Figure 116 Mesh AP Detail Page



Alarm Summary

Rogue AP	0	0	222
Coverage Hole	0	0	0
Security	19	0	1
Controllers	0	0	2
Access Points	0	0	17
Location	0	0	0
Mesh Links	0	165	47
WCS	0	0	0

General

AP Name	mesh-45-map2
AP Ethernet MAC	00:0b:85:72:64:00
AP Base Radio MAC	00:0b:85:72:64:00
Country Code	US
AP IP Address	0.0.0.0
AP Up Time	5 d 22 h 4 m 4 s
LWAPP Up Time	5 d 21 h 59 m 50 s
LWAPP Join Taken Time	4 m 6 s
Admin Status	Enable
AP Mode	Bridge
Operational Status	Registered
Registered Controller	209.165.200.250
Primary Controller	mesh-controller-45
Port Number	1
Map Location	San Jose > Site
Statistics Timer	180
AP Temperature	35C/95F
Heater Status	Off

Versions

Software Version	4.1.175.32M (Mesh)
Boot Version	2.1.78.0

Inventory Information

AP Type	LWAPP
AP Model	LAP1510
AP Certificate Type	Manufacture Installed
AP Serial Number	WCN10170001

Unique Device Identifier(UDI)

Name	Cisco AP
Description	Cisco Wireless Access Point
Product Id	AIR-LAP1510-A-K9
Version Id	V01
Serial Number	WCN10170001

Alarms

Events

Step 5 On the Access Point configuration page, follow these steps to view configuration details for the mesh access point:

a. Choose the **General** tab to view the overall configuration of the mesh access point such as AP name, MAC address, AP Up time, associated controllers (registered and primary) operational status, and software version.

Note The software version for mesh access points is appended the letter *m* and the word *mesh* in parentheses.

b. Choose the **Interface** tab to view configuration details for the interfaces supported on the mesh access point. Interface options are radio and Ethernet.

c. Choose the **Mesh Links** tab to view parent and neighbors' details (name, MAC address, packet error rate, and link details) for the mesh access point. You can also initiate link tests from this panel.

d. Choose the **Mesh Statistics** tab to view details on the bridging, queue, and security statistics for the mesh access point. For more details on mesh statistics, see the "Mesh Statistics for a Mesh Access Point" section.

Monitoring Mesh Access Point Neighbors Using Maps

To view details on neighbors of a mesh access point from a mesh network map, follow these steps:

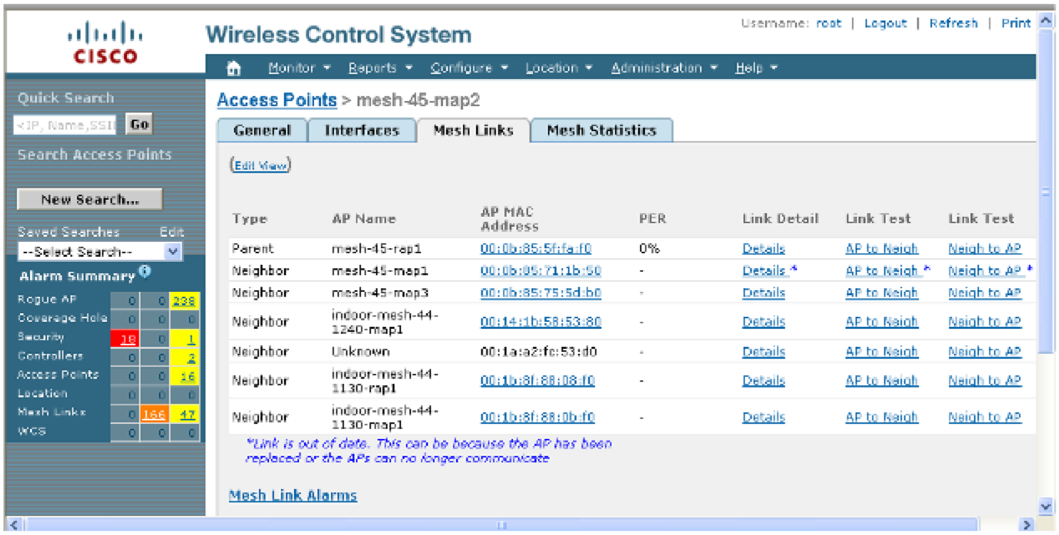
Step 1 Choose **Monitor > Maps**.

Step 2 Click the **Map Name** that corresponds to the outdoor area, campus, building, or floor you want to monitor.

Step 3 To view detailed information on mesh links for a mesh access point, click the arrow portion of the access point label. The Access Points screen appears.

Step 4 Click the **Mesh Links** tab (see Figure 117).

Figure 117 Access Points > Mesh Links Panel



Access Points > mesh-45-map2

Alarm Summary

Rogue AP	0	0	238
Coverage Hole	0	0	0
Security	18	0	1
Controllers	0	0	2
Access Points	0	0	16
Location	0	0	0
Mesh Links	0	166	47
WCS	0	0	0

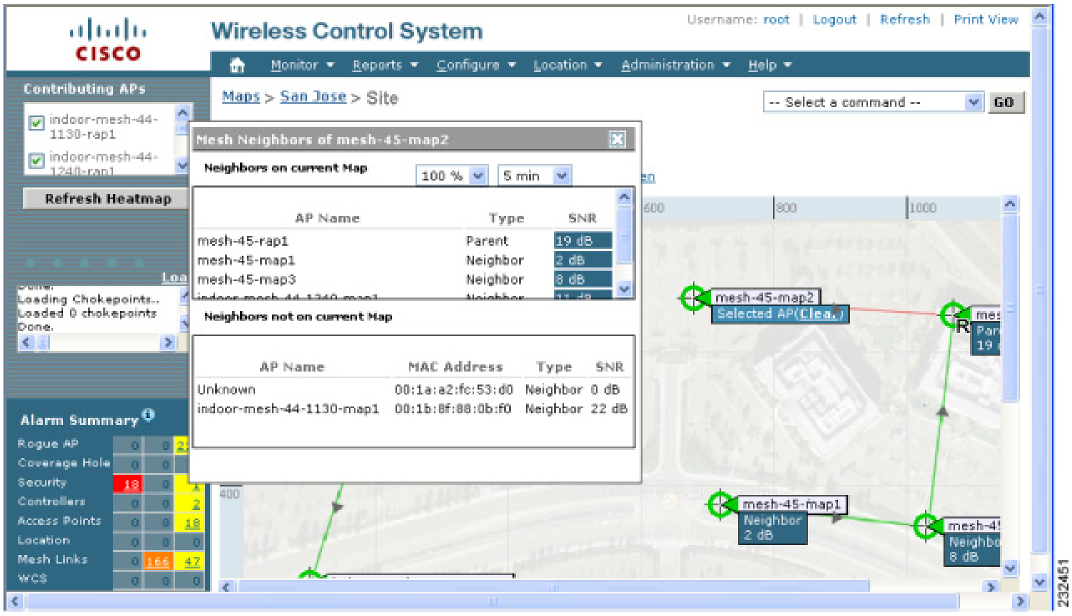
Type	AP Name	AP MAC Address	PER	Link Detail	Link Test	Link Test
Parent	mesh-45-rap1	00:0b:85:5f:fa:f0	0%	Details	AP to Neigh	Neigh to AP
Neighbor	mesh-45-map1	00:0b:05:71:1b:50	-	Details *	AP to Neigh *	Neigh to AP *
Neighbor	mesh-45-map3	00:0b:85:75:5d:b0	-	Details	AP to Neigh	Neigh to AP
Neighbor	indoor-mesh-44-1240-map1	00:14:1b:58:53:80	-	Details	AP to Neigh	Neigh to AP
Neighbor	Unknown	00:1a:a2:fc:53:d0	-	Details	AP to Neigh	Neigh to AP
Neighbor	indoor-mesh-44-1130-rap1	00:1b:8f:88:08:f0	-	Details	AP to Neigh	Neigh to AP
Neighbor	indoor-mesh-44-1130-map1	00:1b:8f:88:0b:f0	-	Details	AP to Neigh	Neigh to AP

*Link is out of date. This can be because the AP has been replaced or the APs can no longer communicate

Note You can also mesh link details for neighbors of a selected mesh access point by clicking on the View Mesh Neighbors link on the mesh access point configuration summary panel that displays when you mouse over a mesh access point on a map. (See Figure 118.)

Note Signal-to-noise (SNR) only appears on the View Mesh Neighbors panel. (See Figure 118.)

Figure 118 View Mesh Neighbors Panel



Loading Chokepoints..
Loaded 0 chokepoints
Done.

Mesh Neighbors of mesh-45-map2

Neighbors on current Map — 100 % — 5 min

AP Name	Type	SNR
mesh-45-rap1	Parent	19 dB
mesh-45-map1	Neighbor	2 dB
mesh-45-map3	Neighbor	8 dB

Neighbors not on current Map

AP Name	MAC Address	Type	SNR
Unknown	00:1a:a2:fc:53:d0	Neighbor	0 dB
indoor-mesh-44-1130-map1	00:1b:8f:88:0b:f0	Neighbor	22 dB

Note In addition to listing the current and past neighbors in the panel that displays, labels are added to the mesh access points map icons to identify the selected mesh access point, the neighbor mesh access point, and the child mesh access point. Select the **clear** link of the selected mesh access point to remove the relationship labels from the map.

Note The drop-down lists at the top of the mesh neighbors page indicate the resolution of the map (100%) displayed and how often the information displayed is updated (5 minutes). You can modify these default values.

Monitoring Mesh Health

Mesh Health monitors the overall health of outdoor and indoor mesh access points, except as noted. Tracking this environmental information is particularly critical for mesh access points that are deployed outdoors. The following factors are monitored:

- Temperature: Displays the internal temperature of the mesh access point in Fahrenheit and Celsius (AP1520s only).
- Heater status: Displays the heater as on or off (AP1520s only).
- AP Up time: Displays how long the mesh access point has been active to receive and transmit.
- CAPWAP Join Taken Time: Displays how long it took to establish the CAPWAP connection.
- CAPWAP Up Time: Displays how long the CAPWAP connection has been active.

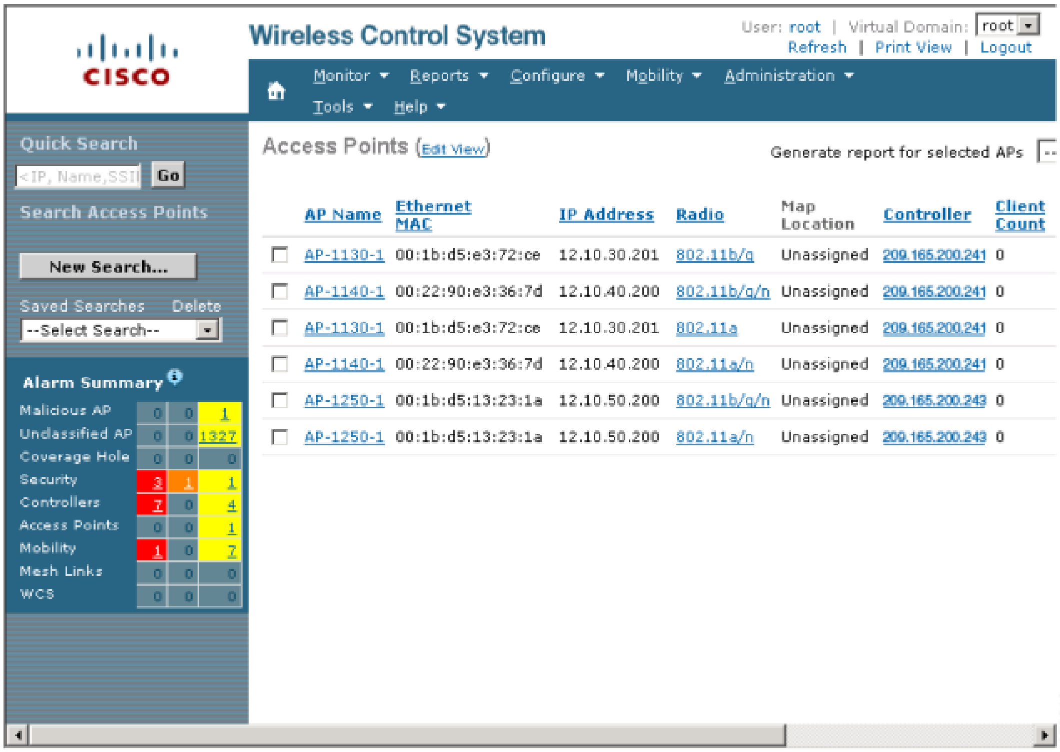
Mesh Health information is displayed in the General Properties panel for mesh access points.

To view the mesh health details for a specific mesh access point, follow these steps:

Step 1 Choose **Monitor > Access Points**. A listing of access points appears (see Figure 119).

Note You can also use the New Search button to display the mesh access point summary shown below. With the New Search option, you can further define the criteria of the access points that display. Search criteria include AP Type, AP Mode, Radio Type, and 802.11n Support.

Figure 119 Monitor > Access Points



Alarm Summary

Malicious AP	0	0	1
Unclassified AP	0	0	1327
Coverage Hole	0	0	0
Security	3	1	1
Controllers	7	0	4
Access Points	0	0	1
Mobility	1	0	7
Mesh Links	0	0	0
WCS	0	0	0

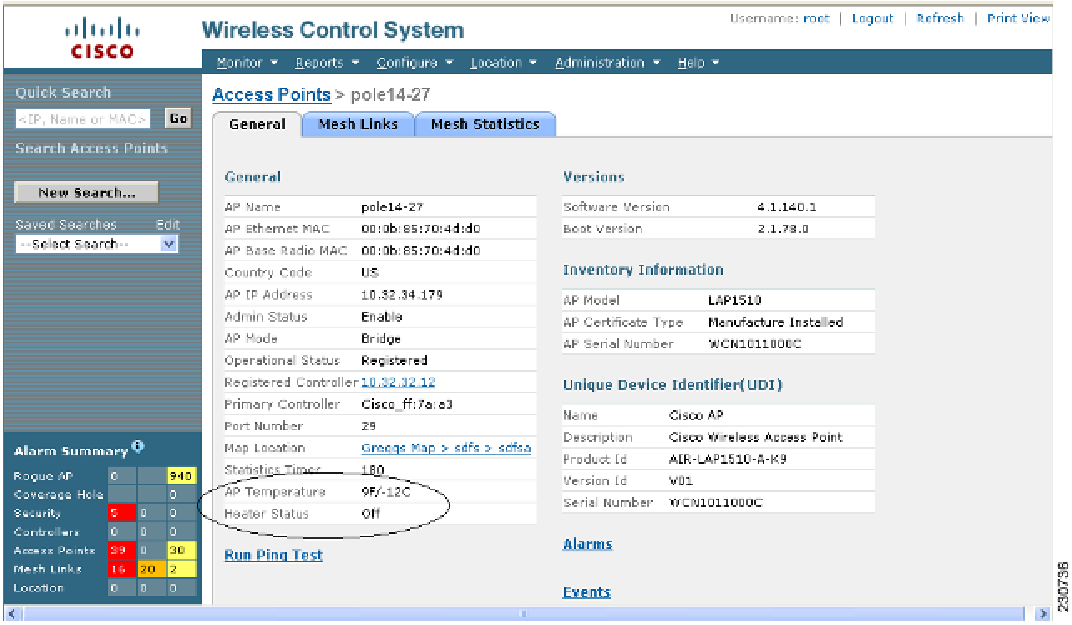
Access Points (Edit View)

	AP Name	Ethernet MAC	IP Address	Radio	Map Location	Controller	Client Count
□	AP-1130-1	00:1b:d5:e3:72:ce	12.10.30.201	802.11b/g	Unassigned	209.165.200.241	0
□	AP-1140-1	00:22:90:e3:36:7d	12.10.40.200	802.11b/g/n	Unassigned	209.165.200.241	0
□	AP-1130-1	00:1b:d5:e3:72:ce	12.10.30.201	802.11a	Unassigned	209.165.200.241	0
□	AP-1140-1	00:22:90:e3:36:7d	12.10.40.200	802.11a/n	Unassigned	209.165.200.241	0
□	AP-1250-1	00:1b:d5:13:23:1a	12.10.50.200	802.11b/g/n	Unassigned	209.165.200.243	0
□	AP-1250-1	00:1b:d5:13:23:1a	12.10.50.200	802.11a/n	Unassigned	209.165.200.243	0

Step 2 Click the AP Name link to display details for that mesh access point. The General Properties panel for that mesh access point appears (see Figure 120).

Note You can also access the General properties panel for a mesh access point from a Cisco WCS map page. To display the panel, click the arrow portion of the mesh access point label. A tabbed panel appears and displays the General properties panel for the selected access point.

Figure 120 AP Name > General Properties Page



Alarm Summary

Rogue AP	0		940
Coverage Hole			0
Security	5	0	0
Controllers	0	0	0
Access Points	39	0	30
Mesh Links	16	20	2
Location	0	0	0

General

AP Name	pole14-27
AP Ethernet MAC	00:0b:85:70:4d:d0
AP Base Radio MAC	00:0b:85:70:4d:d0
Country Code	US
AP IP Address	10.32.34.179
Admin Status	Enable
AP Mode	Bridge
Operational Status	Registered
Registered Controller	10.32.32.12
Primary Controller	Cisco_ff:7a:a3
Port Number	29
Map Location	Greggs Map > sdfs > sdfsa
Statistics Timer	180
AP Temperature	9F/-12C
Heater Status	Off

Versions

Software Version	4.1.140.1
Boot Version	2.1.78.0

Inventory Information

AP Model	LAP1510
AP Certificate Type	Manufacture Installed
AP Serial Number	WCN1011000C

Unique Device Identifier(UDI)

Name	Cisco AP
Description	Cisco Wireless Access Point
Product Id	AIR-LAP1510-A-K9
Version Id	V01
Serial Number	WCN1011000C

To add, remove, or reorder columns in the table, click the Edit View link. Table 25 displays optional access point parameters available from the Edit View page.

Table 25 ***Monitor Access Points Additional Search Results Parameters***

Column	Options
AP Type	Indicates the type of access point (unified or autonomous).
Antenna Azim. Angle	Indicates the horizontal angle of the antenna.
Antenna Diversity	Indicates if antenna diversity is enabled or disabled. Antenna diversity refers to the access point sampling the radio signal from two integrated antenna ports in order to choose the preferred antenna.
Antenna Elev. Angle	Indicates the elevation angle of the antenna.
Antenna Gain	The peak gain of the dBi of the antenna for directional antennas and the average gain in dBi for omnidirectional antennas connected to the wireless network adapter. The gain is in multiples of 0.5 dBm. An integer value 4 means 4 x 0.5 - 2 dBm of gain.
Antenna Mode	Indicates the antenna mode such as omni, directional, or non-applicable.
Antenna Name	Indicates the antenna name or type.
Antenna Type	Indicates whether the antenna is internal or external.
Audit Status	Indicates one of the following audit statuses: • Mismatch—Config differences were found between Cisco WCS and controller during the last audit. • Identical—No config differences were found during the last audit. • Not Available—Audit status is unavailable.
Bridge Group Name	Indicates the name of the bridge group used to group the access points, if applicable.
CDP Neighbors	Indicates all directly connected Cisco devices.
Channel Control	Indicates whether the channel control is automatic or custom.
Channel Number	Indicates the channel on which the Cisco radio is broadcasting.
Controller Port	Indicates the number of controller ports.
Node Hops	Indicates the number of hops between access point.
POE Status	Indicates the Power-over-Ethernet status of the access point. The possible values include: • Low—The access point draws low power from the Ethernet. • Lower than 15.4 volts—The access point draws lower than 15.4 volts from the Ethernet. • Lower than 16.8 volts—The access point draws lower than 16.8 volts from the Ethernet. • Normal—The power is high enough for the operation of the access point. • Not Applicable—The power source is not from the Ethernet.
Primary Controller	Indicates the name of the primary controller for this access point.

Table 25 Monitor Access Points Additional Search Results Parameters (continued)

Column	Options
Radio MAC	Indicates the radio's MAC address.
Reg. Domain Supported	Indicates whether or not the regulatory domain is supported.
Serial Number	Indicates the access point's serial number.
Slot	Indicates the slot number.
Tx Power Control	Indicates whether the transmission power control is automatic or custom.
Tx Power Level	Indicates the transmission power level.
Up Time	Indicates how long the access point has been up in days, hours, minutes, and seconds.
WLAN Override Names	Indicates the WLAN override profile names.
WLAN Override	Indicates whether WLAN Override is enabled or disabled. Each access point is limited to 16 WLAN profiles. Each access point broadcasts all WLAN profiles unless the WLAN override feature is enabled. The WLAN override feature allows you to disable any of the 16 WLAN profiles per access point.

Mesh Statistics for a Mesh Access Point

Mesh Statistics are reported when a child mesh access point authenticates or associates with a parent mesh access point.

Security entries are removed and no longer displayed when the child mesh access point disassociates from the controller.

The following mesh security statistics are displayed for mesh access points:

- Bridging
- Queue
- Security

To view the mesh statistics for a specific mesh access point, follow these steps:

Step 1 Choose **Monitor > Access Points**. A listing of access points appears. (See Figure 121.)

Note You can also use the New Search button to display the access point summary. With the New Search option, you can further define the criteria of the access points that display. Search criteria include AP Name, IP address, MAC address, Controller IP or Name, Radio type, and Outdoor area.

Step 2 Click the **AP Name** link of the target mesh access point.

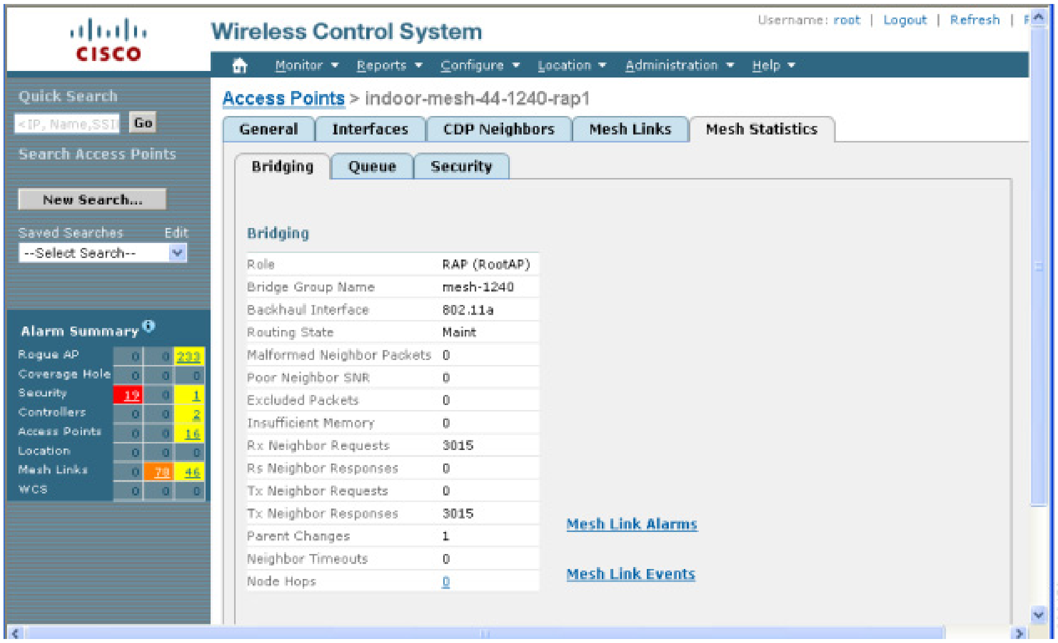
A tabbed panel appears and displays the General Properties page for the selected mesh access point.

Step 3 Click the **Mesh Statistics** tab (see Figure 121). A three-tabbed Mesh Statistics panel appears.

Note The Mesh Statistics tab and its subordinate tabs (Bridging, Queue and Security) only appear for mesh access points. The Mesh Link Alarms and Mesh Link Events links are accessible from each of the three tabbed panels.

Note You can also access the Mesh Securities panel for a mesh access point from a Cisco WCS map. To display the panel, click the arrow portion of the mesh access point label.

Figure 121 ***Monitor > Access Points > AP Name > Mesh Statistics***



Bridging

Role	RAP (RootAP)
Bridge Group Name	mesh-1240
Backhaul Interface	802.11a
Routing State	Maint
Malformed Neighbor Packets	0
Poor Neighbor SNR	0
Excluded Packets	0
Insufficient Memory	0
Rx Neighbor Requests	3015
Rs Neighbor Responses	0
Tx Neighbor Requests	0
Tx Neighbor Responses	3015
Parent Changes	1
Neighbor Timeouts	0
Node Hops	0

Summaries of the Bridging, Queue and Security Statistics and their definitions are provided in Table 26, Table 27, and Table 28 respectively.

Table 26 ***Bridging Mesh Statistics***

Parameter	**Description**
Role	The role of the mesh access point. Options are mesh access points (MAPs) and root access points (RAPs).
Bridge Group Name (BGN)	The name of the bridge group to which the MAP or RAP is a member. Assigning membership in a BGN is recommended. If one is not assigned, a MAP is by default assigned to a default BGN.
Backhaul Interface	The radio backhaul for the mesh access point.
Routing State	The state of parent selection. Values that display are seek, scan, and maint. Maint displays when parent selection is complete.

Table 26 Bridging Mesh Statistics (continued)

Parameter	Description
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	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	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	The number of times a mesh access point (child) moves to another parent.
Neighbor Timeouts	The number of neighbor timeouts.
Node Hops	The number of hops between the MAP and the RAP. Click the value link to display a sub-panel which enables you to configure details of what is reported, how often the node hop value is updated, and view a graphical representation of the report.

Table 27 Queue Mesh Statistics

Parameter	Description
Silver Queue	The average and peak number of packets waiting in the silver (best effort) queue during the defined statistics time interval. Packets dropped and queue size is also summarized.
Gold Queue	The average and peak number of packets waiting in the gold (video) queue during the defined statistics time interval. Packets dropped and queue size is also summarized.
Platinum Queue	The average and peak number of packets waiting in the platinum (voice) queue during the defined statistics time interval. Packets dropped and queue size is also summarized.

Table 27 Queue Mesh Statistics (continued)

Parameter	Description
Bronze Queue	The average and peak number of packets waiting in the bronze (background) queue during the defined statistics time interval. Packets dropped and queue size is also summarized.
Management Queue	The average and peak number of packets waiting in the management queue during the defined statistics time interval. Packets dropped and queue size is also summarized.

Table 28 Security Mesh Statistics

Parameter	Description
Association Request Failures	Summarizes the total number of association request failures that occur between the selected mesh access point and its parent.
Association Request Success	Summarizes the total number of successful association requests that occur between the selected mesh access point and its parent.
Association Request Timeouts	Summarizes the total number of association request time outs that occur between the selected mesh access point and its parent.
Authentication Request Failures	Summarizes the total number of failed authentication requests that occur between the selected mesh access point and its parent.
Authentication Request Success	Summarizes the total number of successful authentication requests between the selected mesh access point and its parent mesh node.
Authentication Request Timeouts	Summarizes the total number of authentication request timeouts that occur between the selected mesh access point and its parent.
Invalid Association Request	Summarizes the total number of invalid association requests received by the parent mesh access point from the selected child mesh access point. This state might occur when the selected child is a valid neighbor but is not in a state that allows association.
Invalid Reassociation Request	Summarizes the total number of invalid reassociation requests received by the parent mesh access point from a child. This might happen when a child is a valid neighbor but is not in a proper state for reassociation.

Table 28 Security Mesh Statistics (continued)

Parameter	Description
Invalid Reauthentication Request	Summarizes the total number of invalid reauthentication requests received by the parent mesh access point from a child. This may happen when a child is a valid neighbor but is not in a proper state for reauthentication.
Packets Received	Summarizes the total number of packets received during security negotiations by the selected mesh access point.
Packets Transmitted	Summarizes the total number of packets transmitted during security negotiations by the selected mesh access point.
Reassociation Request Failures	Summarizes the total number of failed reassociation requests between the selected mesh access point and its parent.
Reassociation Request Success	Summarizes the total number of successful reassociation requests between the selected mesh access point and its parent.
Reassociation Request Timeouts	Summarizes the total number of reassociation request timeouts between the selected mesh access point and its parent.
Reauthentication Request Failures	Summarizes the total number of failed reauthentication requests between the selected mesh access point and its parent.
Reauthentication Request Success	Summarizes the total number of successful reauthentication requests that occurred between the selected mesh access point and its parent.
Reauthentication Request Timeouts	Summarizes the total number of reauthentication request timeouts that occurred between the selected mesh access point and its parent.
Unknown Association Requests	Summarizes the total 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.
Unknown Reassociation Request	Summarizes the total number of unknown reassociation requests received by the parent mesh access point from a child. This might happen when a child mesh access point is an unknown neighbor.
Unknown Reauthentication Request	Summarizes the total number of unknown reauthentication requests received by the parent mesh access point node from its child. This might occur when a child mesh access point is an unknown neighbor.

Viewing the Mesh Network Hierarchy

You can view the parent-child relationship of mesh access points within a mesh network in an easily navigable display. You can also filter which mesh access points display on the Map view, by selecting only mesh access points of interest.

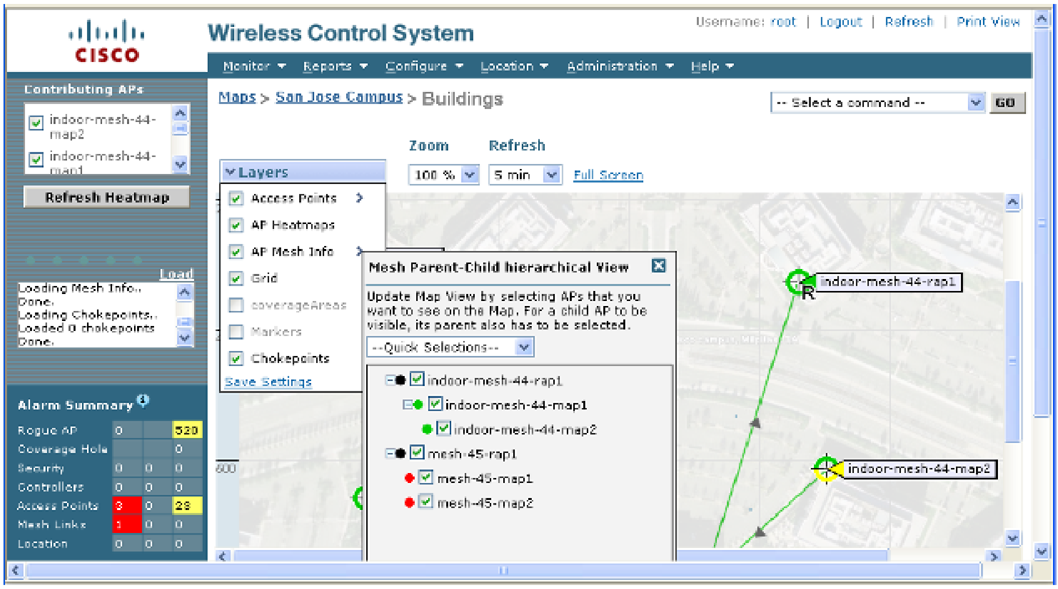
To view the mesh network hierarchy for a selected network, follow these steps:

Step 1 Choose **Monitor** > **Maps**.

Step 2 Select the map you want to display.

Step 3 Click the **Layers** arrow to expand that menu. (See Figure 122.)

Figure 122 Monitor > Maps > Selected Map



Wireless Control System
Username: root | Logout | Refresh | Print View
Monitor ▾ Reports ▾ Configure ▾ Location ▾ Administration ▾ Help ▾
Maps > San Jose Campus > Buildings
-- Select a command -- GO
Zoom
Refresh
Full Screen
Contributing APs
Refresh Heatmap
Load
Layers
Save Settings
Alarm Summary
indoor-mesh-44-rap1
indoor-mesh-44-map2
600
230767

Contributing APs: ☑ indoor-mesh-44-map2, ☑ indoor-mesh-44-map1

Zoom: 100 % | Refresh: 5 min

Loading Mesh Info..
Done.
Loading Chokepoints..
Loaded 0 chokepoints
Done.

Layers:
- ☑ Access Points
- ☑ AP Heatmaps
- ☑ AP Mesh Info
- ☑ Grid
- □ coverageAreas
- □ Markers
- ☑ Chokepoints

Mesh Parent-Child hierarchical View

Update Map View by selecting APs that you want to see on the Map. For a child AP to be visible, its parent also has to be selected.

--Quick Selections--

```
⊟● ☑ indoor-mesh-44-rap1
    ⊟● ☑ indoor-mesh-44-map1
        ● ☑ indoor-mesh-44-map2
⊟● ☑ mesh-45-rap1
    ● ☑ mesh-45-map1
    ● ☑ mesh-45-map2
```

Alarm Summary			
Rogue AP	0		520
Coverage Hole			0
Security	0	0	0
Controllers	0	0	0
Access Points	3	0	28
Mesh Links	1	0	0
Location	0	0	0

Step 4 Select the **AP Mesh Info** check box if it is not already checked.

Note The AP Mesh Info check box can be selected only if mesh access points are present on the map. It must be checked to view the mesh hierarchy.

Step 5 Click the **AP Mesh Info** arrow to display the mesh parent-child hierarchy.

Step 6 Click the **plus (+)** sign next to a mesh access point to display its children.

All subordinate mesh access points are displayed when a negative (-) sign displays next to the parent mesh access point entry. For example, in Figure 122, the mesh access point, *indoor-mesh-45-rap2*, has only one child, *indoor-mesh-44-map2*.

Step 7 Move the cursor over the colored dot next to each mesh access point child to view details on the link between it and its parent. Table 29 summarizes the parameters that display.

The color of the dot also provides a quick reference point of the SNR strength.

- A green dot represents a high SNR (above 25 dB).
- An amber dot represents an acceptable SNR (20-25 dB).

- A red dot represents a low SNR (below 20 dB).
- A black dot indicates a root access point.

Table 29 Bridging Link Information

Parameter	Description
Information fetched on	Date and time that information was compiled.
Link SNR	Link signal-to-noise ratio (SNR).
Link Type	Hierarchical link relationship.
SNR Up	Signal-to-noise radio for the uplink (dB).
SNR Down	Signal-to-noise radio for the downlink (dB).
PER	The packet error rate for the link.
Tx Parent Packets	The TX packets to a node while acting as a parent.
Rx Parent Packets	The RX packets to a node while acting as a parent.
Time of Last Hello	Date and time of last hello.

Using Mesh Filters to Modify Map Display of Maps and Mesh Links

In the mesh hierarchical page, you can also define mesh filters to determine which mesh access points display on the map based on hop values as well as what labels display for mesh links.

Mesh access points are filtered by the number of hops between them and their root access point.

To use mesh filtering, follow these steps:

Step 1 To modify what label and color displays for a mesh link, follow these steps:

a. In the Mesh Parent-Child Hierarchical View, select an option from the Link Label drop-down menu. Options are None, Link SNR, and Packet Error Rate.

b. In the Mesh Parent-Child Hierarchical View, select an option from the Link Color drop-down menu to define which parameter (Link SNR or Packet Error Rate) determines the color of the mesh link on the map.

Note The color of the link provides a quick reference point of the SNR strength or Packet Error Rate. See Table 30.

Table 30 Definition for SNR and Packet Error Rate Link Color

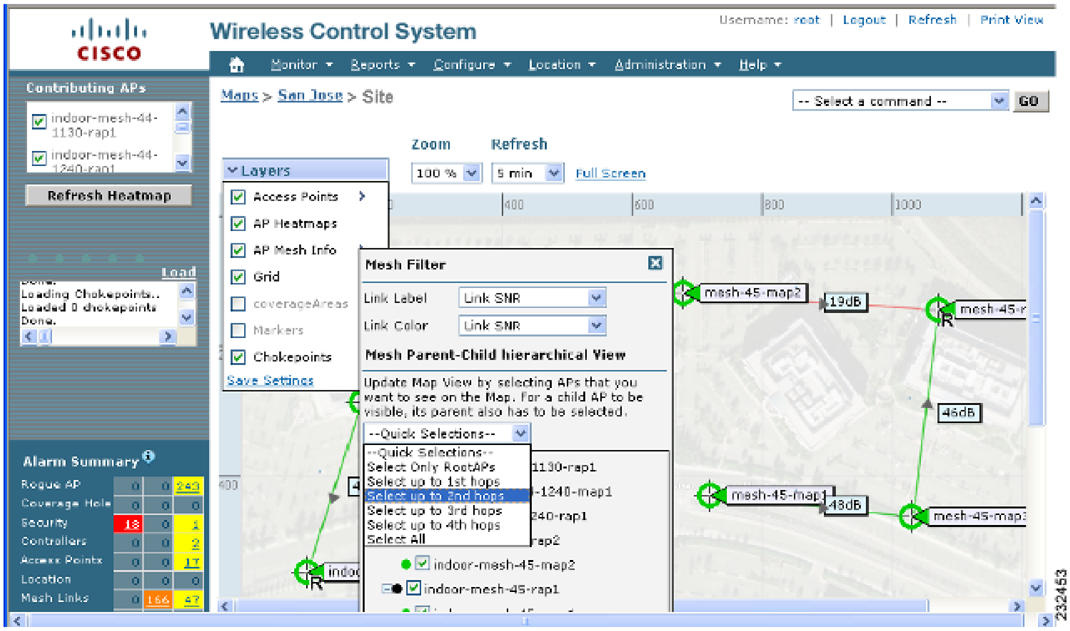
Link Color	Link SNR	Packet Error Rate (PER)
Green	Represents a SNR above 25 dB (high value)	Represents a PER of one percent (1%) or lower

Table 30 Definition for SNR and Packet Error Rate Link Color

Link Color	Link SNR	Packet Error Rate (PER)
Amber	Represents a SNR between 20 and 25 dB (acceptable value)	Represents a PER that is less than ten percent (10%) and greater than one percent (1%)
Red	Represents a SNR below 20 dB (low value)	Represents a PER that is greater than ten percent (10%)

Note The Link label and color settings are reflected on the map immediately (see Figure 123). You can display both SNR and PER values simultaneously.

Figure 123 Mesh Filter and Hope Count Configuration Panel



Mesh Filter

Link Label: Link SNR

Link Color: Link SNR

Mesh Parent-Child hierarchical View

Update Map View by selecting APs that you want to see on the Map. For a child AP to be visible, its parent also has to be selected.

--Quick Selections--
- --Quick Selections--
- Select Only RootAPs
- Select up to 1st hops
- Select up to 2nd hops
- Select up to 3rd hops
- Select up to 4th hops
- Select All

1130-rap1
-1240-map1
240-rap1
rap2
● ☑ indoor-mesh-45-map2
● ☑ indoor-mesh-45-rap1

Step 2 To modify which mesh access points display based on the number of hops between them and their parents, do the following:

a. In the Mesh Parent-Child Hierarchical View, click the **Quick Selections** drop-down menu.

b. Select the appropriate option from the menu. A description of the options is provided in Table 31.

Table 31 Quick Selection Options

Parameter	Description
Select only Root APs	Choose this setting if you want the map view to display root access points only.
Select up to 1st hops	Choose this setting if you want the map view to display 1st hops only.

Table 31 Quick Selection Options (continued)

Select up to 2nd hops	Choose this setting if you want the map view to display 2nd hops only.
Select up to 3rd hops	Choose this setting if you want the map view to display 3rd hops only.
Select up to 4th hops	Choose this setting if you want the map view to display 4th hops only.
Select All	Select this setting if you want the map view to display all access points.

c. Click **Update Map View** to refresh the screen and redisplay the map view with the selected options.

Note Map view information is retrieved from the Cisco WCS database and is updated every 15 minutes.

Note You can also select or deselect the check boxes of mesh access points in the mesh hierarchical view to modify which mesh access points are displayed. For a child access point to be visible, the parent access point to root access point must be selected.

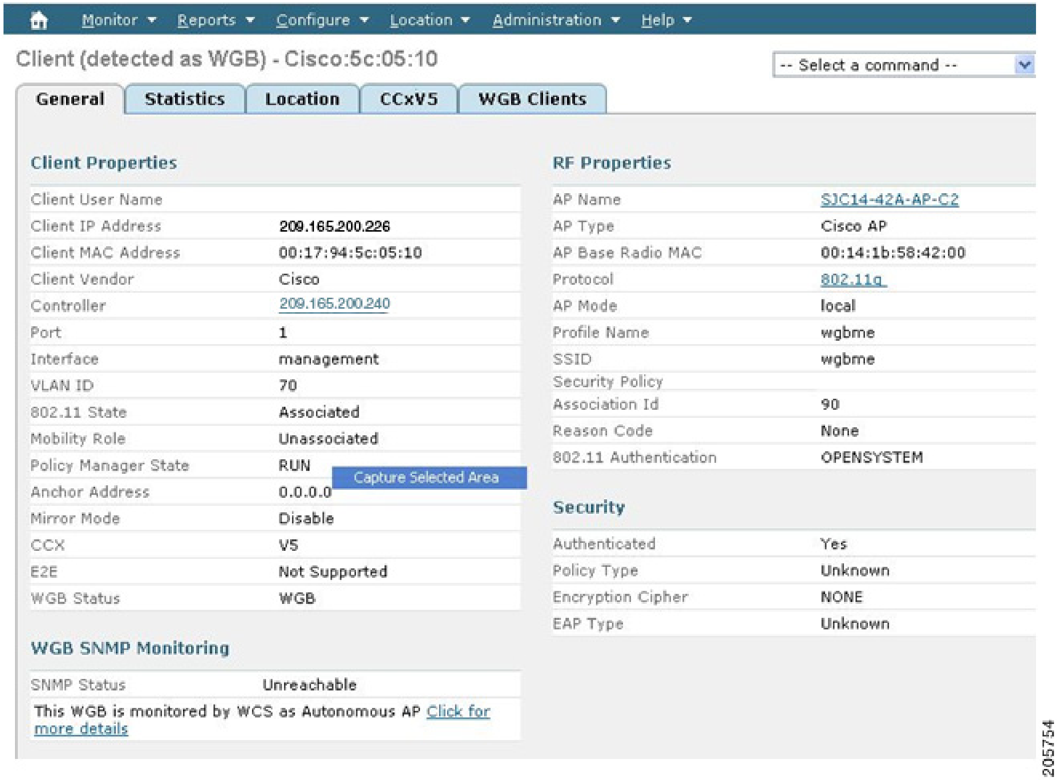
Monitoring WGBs

You can monitor WGB clients separately.

To view details on WGB clients, follow these steps:

Step 1 In Cisco WCS, choose **Monitor > WGBs**. The following page appears (see Figure 124).

Figure 124 Monitor > WGBs



Client (detected as WGB) - Cisco:5c:05:10

Client Properties

Client User Name	
Client IP Address	209.165.200.226
Client MAC Address	00:17:94:5c:05:10
Client Vendor	Cisco
Controller	209.165.200.240
Port	1
Interface	management
VLAN ID	70
802.11 State	Associated
Mobility Role	Unassociated
Policy Manager State	RUN
Anchor Address	0.0.0.0
Mirror Mode	Disable
CCX	V5
E2E	Not Supported
WGB Status	WGB

RF Properties

AP Name	SJC14-42A-AP-C2
AP Type	Cisco AP
AP Base Radio MAC	00:14:1b:58:42:00
Protocol	802.11g
AP Mode	local
Profile Name	wgbme
SSID	wgbme
Security Policy	
Association Id	90
Reason Code	None
802.11 Authentication	OPENSYSTEM

Security

Authenticated	Yes
Policy Type	Unknown
Encryption Cipher	NONE
EAP Type	Unknown

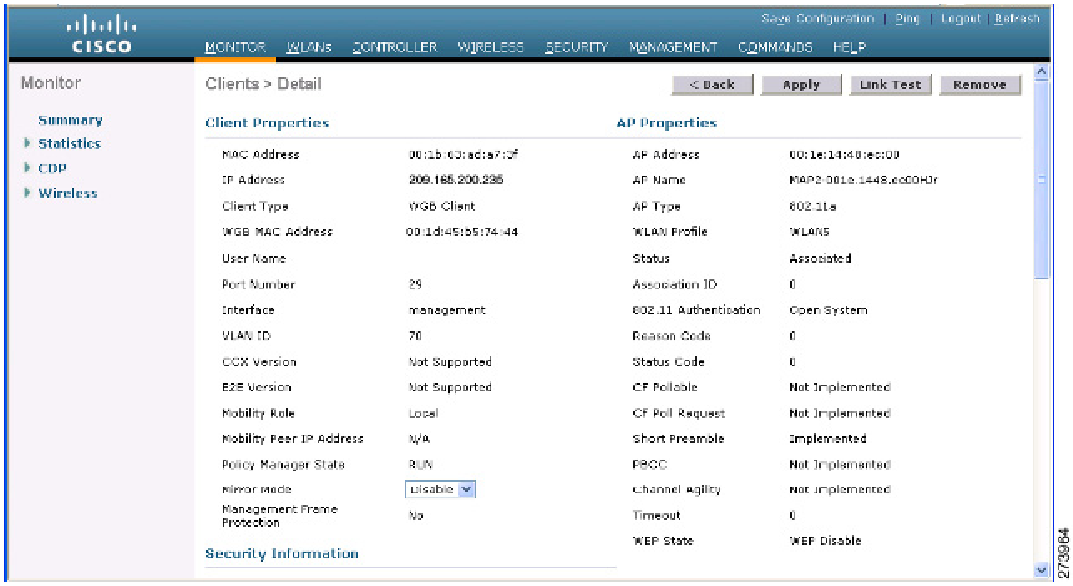
WGB SNMP Monitoring

SNMP Status	Unreachable

This WGB is monitored by WCS as Autonomous AP Click for more details

Step 2 Click the **WGB Clients** tab to see a summary of WGB clients. (See Figure 125.)

Figure 125 Monitor > WGBs > WGB Clients Panel



Clients > Detail

Client Properties

MAC Address	00:1b:63:ad:a7:3f
IP Address	209.165.200.235
Client Type	WGB Client
WGB MAC Address	00:1d:45:55:74:44
User Name	
Port Number	29
Interface	management
VLAN ID	70
CCX Version	Not Supported
E2E Version	Not Supported
Mobility Role	Local
Mobility Peer IP Address	N/A
Policy Manager State	RUN
Mirror Mode	Disable
Management Frame Protection	No

AP Properties

AP Address	00:1e:14:48:ec:00
AP Name	MAP2-001e.1448.ec00HJr
AP Type	802.11a
WLAN Profile	WLAN5
Status	Associated
Association ID	0
802.11 Authentication	Open System
Reason Code	0
Status Code	0
CF Pollable	Not Implemented
CF Poll Request	Not Implemented
Short Preamble	Implemented
PBCC	Not Implemented
Channel Agility	Not Implemented
Timeout	0
WEP State	WEP Disable

Security Information

Multiple VLAN and QoS Support for WGB Wired Clients

A WGB is a small stand-alone unit that can provide a wireless infrastructure connection for Ethernet-enabled devices. Devices that do not have a wireless client adapter to connect to the wireless network can be connected to the WGB through the Ethernet port. The WGB associates with the root AP through the wireless interface. Thus, wired clients get access to the wireless network.

This feature provides the segregation of traffic based on VLANs for different applications running on different devices connected to a switch behind a WGB. Traffic from WGB clients are sent in the right priority queue in the mesh backhaul based on DSCP/dot1p values.

Note You need a special autonomous image on the autonomous access points being used as a WGB for interoperability with the Unified CAPWAP infrastructure. This image will be merged with the next official autonomous release.

The WGB informs the WLC about the wired-client VLAN information in an IAPP association message. The WGB removes the 802.1Q header from the packet while sending to the WLC. The WLC sends the packet to the WGB without the 802.1Q tag and the WGB adds 802.1Q header to packets that go to the wired switch based on the destination MAC address.

The WLC treats the WGB client as a VLAN client and forwards the packet in the right VLAN interface based on the source MAC address.

You must enable the WGB unified client for multiple VLAN support on the WGB by entering the **WGB(config)#workgroup-bridge unified-VLAN-client** command. This WGB unified client is disabled by default.

You have to configure subinterfaces on the WGB that corresponds to the VLANs on the switch ports to which the wired clients are connected.

WGB Guidelines

Follow these guidelines when configuring WGBs:

- A dynamic interface should be created in the controller for each VLAN that is configured in the WGB.
- Only one WLAN (SSID) for a wireless association of the WGB to the access point infrastructure is supported. This SSID should be configured as an infrastructure SSID and should be mapped to the native VLAN. The WGB drops everything that is not in the native VLAN in the mesh infrastructure.
- We recommend that you configure the same native VLAN in the switch that connects the WLC, WGB, and in the switch behind the WGB.

  All native VLAN clients on the WGB Ethernet side are part of the same VLAN in which the WGB is associated. The WGB is part of the VLAN to which the WLAN (in which the WGB has associated) is mapped.

  For example, if in the WGB, the 5-GHz radio (dot11radio 1) is mapped to a native VLAN 184, and the switch behind WGB has wired clients only in VLAN 185 and 186, then you may not require the native VLAN to be identical to the native VLAN on the WGB (VLAN 184).

  But, if you add one wired client in VLAN 184 and this VLAN client in the WGB belongs to a native VLAN, you must define the same native VLAN on the switch.
- Intersubnet mobility is supported with this feature for VLAN clients behind the WGB with a limitation that the dynamic interface for all VLANs of the WGB should be configured in all the controllers.
- Interoperability with a VLAN-pooling feature is not supported. When the VLAN-pooling feature is enabled, the WGB and its native VLAN clients become part of the same VLAN.
- AAA-override for WGB clients is not supported. But, AAA-override for the WGB is supported.
- Only Layer 3 multicast is provided for WGB VLAN clients and there is no support for Layer 2 multicast.
- There is a 20-client limitation in WGB that includes wireless clients.
- Link testing for WGB wired clients is not supported.
- Roaming is supported for wireless and wired clients behind WGB.
- Multicast is supported for wired clients behind WGB.
- Broadcast is supported.

Configuring VLAN and QoS Support - Using CLI

In the following example, VLANs 184 and 185 exist on the wired switch behind WGB. WGB’s native VLAN is 184. SSID is auto-wgb mapped to native VLAN 184. Radio 1 (5 GHz) radio is used to connect to the CAPWAP infrastructure using this SSID.

```
ap#config t
ap(config)#workgroup-bridge unified-VLAN-client
ap(config)#int FastEthernet0.184
ap(config-subif)#encapsulation dot1q 184 native
ap(config-subif)#bridge-group 1
ap(config-subif)#exit
ap(config)#int FastEthernet0.185
ap(config-subif)#encapsulation dot1q 185
ap(config-subif)#bridge-group 185
ap(config-subif)#exit
ap(config)#int Dot11Radio 1.185
ap(config-subif)#encapsulation dot1q 185
ap(config-subif)#bridge-group 185
ap(config-subif)#exit
ap(config)#int Dot11Radio 1.184
ap(config-subif)#encapsulation dot1q 184 native
ap(config-subif)#bridge-group 1
ap(config-subif)#exit
ap(config)#dot11 ssid auto-wgb
ap(config-ssid)#authentication open
ap(config-ssid)#infrastructure-ssid
ap(config-ssid)#VLAN 184
ap(config-ssid)#exit
ap(config)#int Dot11Radio 1
ap(config-if)#station-role workgroup-bridge
ap(config-if)#ssid auto-wgb
ap(config-if)#exit
ap(config)#bridge irb
ap(config)#hostname WGB
```

The **bridge irb** command is used to enable integrated routing and bridging, which the Auto AP code has retained from other higher end platforms.

You have to create dynamic interfaces 184 and 185 on the WLC for the above configuration to work. The WGB updates the WLC about the wired-client VLAN information in the IAPP association message. The WLC treats the WGB client as a VLAN-client and forwards the packet in the right VLAN interface based on the source MAC address. In the upstream direction, the WGB removes the 802.1Q header from the packet and sends it to the WLC. In the downstream direction, the WLC sends the packet to the WGB without the 802.1Q tag and the WGB adds the 802.1Q header based on the destination MAC address, while forwarding the packet to the switch that connects the wired client.

WGB Bridge Output

Enter the following command:

```
WGB#sh bridge
Total of 300 station blocks, 292 free
Codes: P - permanent, S - self

Bridge Group 1:

Address          Action     Interface   Age          RX count    TX count


0023.049a.0b12   forward    Fa0.184     0            2           0

0016.c75d.b48f   forward    Fa0.184     0            21          0

0021.91f8.e9ae   forward    Fa0.184     0            110         16

0017.59ff.47c2   forward    Vi0.184     0            23          22

0021.5504.07b5   forward    Fa0.184     0            18          6

0021.1c7b.38e0   forward    ViO.184     0            6           0
```

```
Bridge Group 185:

0016.c75d.b48f      forward      Fa0.185      0            10           0

001e.5831.c74a      forward      Fa0.185      0            9            0
```

WGB Detail on Controller

Enter the following command:

```
(Cisco Controller) > show wgb summary
Number of WGBs................................. 2

MAC Address        IP Address        AP Name  Status    WLAN   Auth  Protocol  Clients


00:1d:70:97:bd:e8  209.165.200.225  c1240    Assoc     2      Yes   802.11a   2

00:1e:be:27:5f:e2  209.165.200.226  c1240    Assoc     2      Yes   802.11a   5


Cisco Controller) > show client summary
Number of Clients.............................. 7

MAC Address        AP Name   Status      WLAN/Guest-Lan  Auth  Protocol  Port     Wired


00:00:24:ca:a9:b4  R14      Associated  1               Yes   N/A       29       No

00:24:c4:a0:61:3a  R14      Associated  1               Yes   802.11a   29       No

00:24:c4:a0:61:f4  R14      Associated  1               Yes   802.11a   29       No

00:24:c4:a0:61:f8  R14      Associated  1               Yes   802.11a   29       No

00:24:c4:a0:62:0a  R14      Associated  1               Yes   802.11a   29       No

00:24:c4:a0:62:42  R14      Associated  1               Yes   802.11a   29       No

00:24:c4:a0:71:d2  R14      Associated  1               Yes   802.11a   29       No


(Cisco Controller) > show wgb detail 00:1e:be:27:5f:e2
Number of wired client(s): 5

MAC Address        IP Address        AP Name     Mobility   WLAN  Auth


00:16:c7:5d:b4:8f  Unknown           c1240       Local      2     No

00:21:91:f8:e9:ae  209.165.200.232   c1240       Local      2     Yes

00:21:55:04:07:b5  209.165.200.234   c1240       Local      2     Yes

00:1e:58:31:c7:4a  209.165.200.236   c1240       Local      2     Yes

00:23:04:9a:0b:12  Unknown           c1240       Local      2     No
```

```
WGB_1#sh ip int brief
Interface                IP Address        OK?         Method     Status     Protocol
BVI1                     209.165.200.225   YES         DHCP       up         up
Dot11Radio0              unassigned        YES         unset      admindown  down
Dot11Radio1              unassigned        YES         TFTP       up         up
Dot11Radio1.184          unassigned        YES         other      up         up
Dot11Radio1.185          unassigned        YES         unset      up         up
FastEthernet0            unassigned        YES         other      up         up
FastEthernet0.184        unassigned        YES         unset      up         up
FastEthernet0.185        unassigned        YES         unset      up         up
Virtual-Dot11Radio0      unassigned        YES         TFTP       up         up
Virtual-Dot11Radio0.184  unassigned        YES         unset      up         up
Virtual-Dot11Radio0.185  unassigned        YES         unset      up         up
```

Troubleshooting Tips

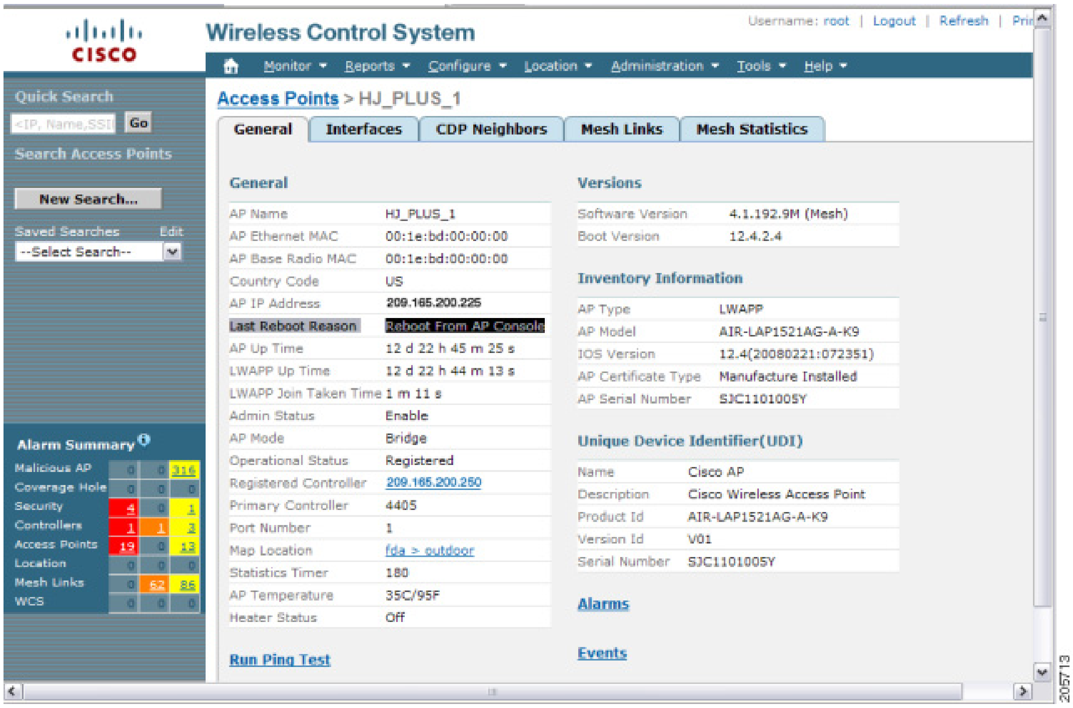
If a WGB client does not associate with the WGB, note these tips to troubleshoot the problem:

1. The native VLAN that is configured on the WGB needs to be the same VLAN on the switch to which the WGB is connected. The switch port connected to the WGB should be Trunk.
2. Verify the client configuration and ensure that the client configuration is correct.
3. Check the **show bridge** command output in the autonomous AP and confirm that the AP is reading the client MAC address in the right interface.
4. Confirm that the subinterfaces that correspond to specific VLANs and different subinterfaces are mapped to the bridge group.
5. WGB reads the switch port behind as a client in its MAC address table.
6. If required, clear the bridge entry using the **clear bridge** command (remember that this command will remove all the wired and wireless clients associated with the WGB and make them associated again).
7. Ensure that the WGB has not exceeded its 20-client limitation.

Viewing AP Last Reboot Reason

Cisco WCS now reports the reason for the most recent reboot on the general panel of the access point details page (**Monitor > Access Points >** *AP Name*). (See Figure 126.)

Figure 126 Access Point > AP Name



Access Points > HJ_PLUS_1

Alarm Summary

Malicious AP	0	0	316
Coverage Hole	0	0	0
Security	4	0	1
Controllers	1	1	3
Access Points	19	0	13
Location	0	0	0
Mesh Links	0	62	86
WCS	0	0	0

General

AP Name	HJ_PLUS_1
AP Ethernet MAC	00:1e:bd:00:00:00
AP Base Radio MAC	00:1e:bd:00:00:00
Country Code	US
AP IP Address	209.165.200.225
Last Reboot Reason	Reboot From AP Console
AP Up Time	12 d 22 h 45 m 25 s
LWAPP Up Time	12 d 22 h 44 m 13 s
LWAPP Join Taken Time	1 m 11 s
Admin Status	Enable
AP Mode	Bridge
Operational Status	Registered
Registered Controller	209.165.200.250
Primary Controller	4405
Port Number	1
Map Location	fda > outdoor
Statistics Timer	180
AP Temperature	35C/95F
Heater Status	Off

Versions

Software Version	4.1.192.9M (Mesh)
Boot Version	12.4.2.4

Inventory Information

AP Type	LWAPP
AP Model	AIR-LAP1521AG-A-K9
IOS Version	12.4(20080221:072351)
AP Certificate Type	Manufacture Installed
AP Serial Number	SJC1101005Y

Unique Device Identifier(UDI)

Name	Cisco AP
Description	Cisco Wireless Access Point
Product Id	AIR-LAP1521AG-A-K9
Version Id	V01
Serial Number	SJC1101005Y

Listed below is a summary of each of the possible Last Reboot Reasons that might be reported and its definition:

- none–Access point reported a reboot reason unknown to the controller
- dot11gModeChange–Change of 802.11g mode change occurred
- ipAddressSet–Set of static IP address
- ip AddressReset–Reset of static IP address
- rebootFromController–Reboot of access point initiated from the controller
- dhcpFallbackFail–Fallback to DHCP did not occur
- discoveryFail–Discovery was not sent
- noJoinResponse–Join response was not received
- denyJoin–Join attempt at the controller was denied
- noConfigResponse–Config Response was not received
- configController–Configured or master controller found
- imageUpgrade Success–Upgrade of image successful
- imageOpcodeInvalid–Invalid image data opcode
- imageCheckSumInvalid–Invalid image md 5 checksum
- imageDataTimeout–Image data message timed-out
- configFileInvalid–Invalid config file
- imageDownloadError–Process error during the image download
- rebootFromConsole–Reboot command initiated from AP console

- rapOverAir–Root access point (RAP) is connected over the air
- brownout–Power failure caused reboot
- powerLow–Low power caused a reboot
- crash–Software failure caused crash
- powerHigh–Power spike caused reboot
- powerLoss–Power loss caused reboot
- powerCharge–Change in power source caused reboot
- componentFailure–Component failure caused reboot
- watchdog–Watch dog timer reset caused reboot

Obtaining Documentation and Submitting a Service Request

For information about obtaining documentation, submitting a service request, and gathering additional information, see the monthly *What's New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation, at:

http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html

Subscribe to the *What's New in Cisco Product Documentation* as a Really Simple Syndication (RSS) feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service and Cisco currently supports RSS Version 2.0.