Controlling Mesh Access Points

This chapter contains these sections:

Information About Cisco Aironet Mesh Access Points

Mesh networking employs Cisco Aironet 1500 Series outdoor mesh access points and indoor mesh access points (Cisco Aironet 1040, 1130, 1140, 1240, 1250, 1260, series 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.

Controller software release 7.0.116.0 and later releases support these Cisco Aironet mesh access points:

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

  Note AP1130 and AP1240 must be converted to operate as indoor mesh access points. See the "Converting Indoor Access Points to Mesh Access Points" section on page 10-123.

- Cisco Aironet 1550 series outdoor mesh access points consist of four models:

- 1552E
- 1552C
- 1552I
- 1552H

In the 7.0.98.0 release, indoor mesh is available on dual band Cisco Aironet 1130 and 1240 series access points. In the 7.0.116.0 release, indoor mesh is also available on dual band 11n access points (Cisco Aironet 1040, 1140, 1250, 1260, 3500 and 3600 series access points). Indoor mesh is not supported with 802.11b/g only access points because 5 GHz is required for mesh backhaul access.

Guidelines and Limitations

- All features discussed in this chapter apply to indoor (1040, 1140, 1250, 1260, 3500, 3600) and outdoor mesh access points (1500 series) unless noted otherwise. *Mesh access point* or *MAP* is hereafter used to refer to both indoor and outdoor mesh access points.
- Cisco Aironet 1505 and 1510 access points are not supported in this release.

Additional References

Related Topic	Document Title
Physical installation and initial configuration of the mesh access points	*Cisco Aironet 1520 Series Outdoor Mesh Access Point Hardware Installation Guide* http://www.cisco.com/en/US/products/ps8368/tsd_products_support_series_home.html
Converting indoor access points to operate as mesh access points	"Converting Indoor Access Points to Mesh Access Points" section on page 10-123
More information about Cisco Aironet 1550 series outdoor mesh access points	http://www.cisco.com/en/US/docs/wireless/technology/mesh/7.0MR1/design/guide/MeshAP_70MR1.html
Mesh feature summary, important notes, and software upgrade steps to migrate from 4.1.19x.xx mesh releases to controller release 7.0.116.0	*Release Notes for Cisco Wireless LAN controllers and Lightweight Access Points for Release 7.0.116.0* http://www.cisco.com/en/US/products/ps6366/prod_release_notes_list.html

Access Point Roles

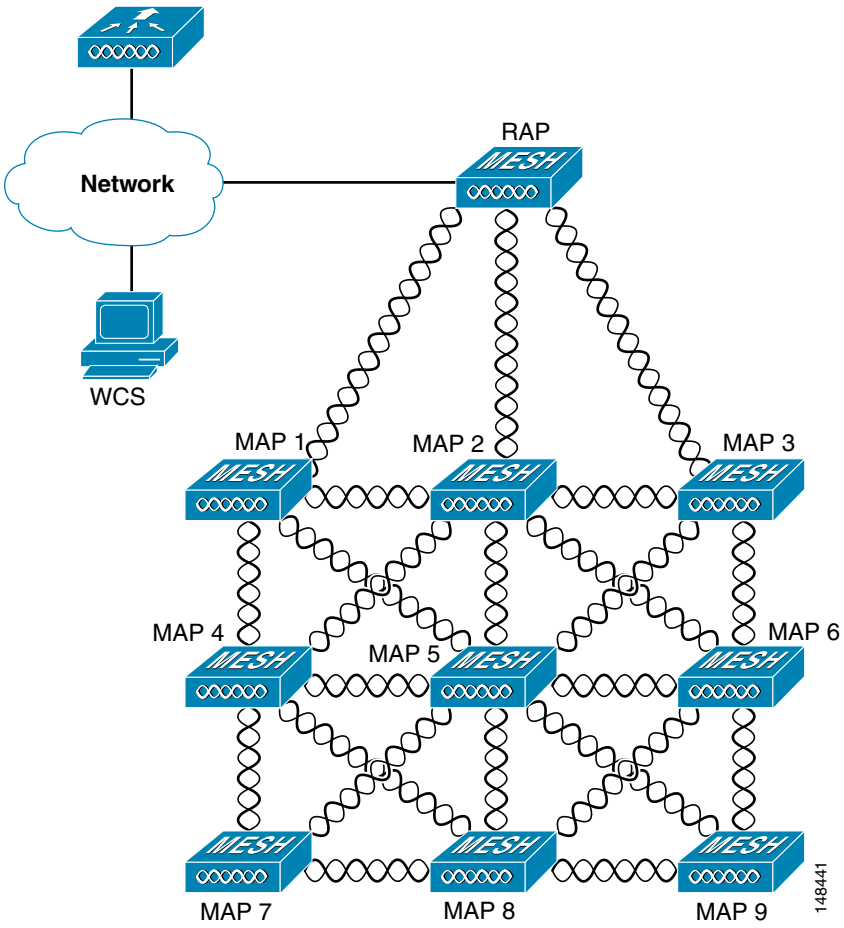
Access points within a mesh network operate as either a Root Access Point (RAP) or a Mesh Access Point (MAP).

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

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

All the possible paths between the MAPs and RAPs form the wireless mesh network. Figure 10-1 shows the relationship between RAPs and MAPs in a mesh network.

Figure 10-1 Simple Mesh Network Hierarchy



Network Access

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

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

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

- MAC authentication—Mesh access points are added to a database to ensure that they are allowed access to a given controller and the mesh network. See the "Converting Indoor Access Points to Mesh Access Points" section on page 10-123.
- External RADIUS authentication—Mesh access points can be externally authorized to use a RADIUS server such as Cisco ACS 4.1 and later releases that support the client authentication type of EAP-FAST with certificates. See the "Configuring RADIUS Servers" section on page 10-28.

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 Antenna Gain (GUI)" section on page 10-54.

Cisco Indoor Mesh Access Points

With the 7.0.116.0 release, indoor mesh is also available on 802.11n access points (Cisco Aironet 1040, 1140, 1250, 1260, 3500, and 3600 series access points).

With the 7.0 release, indoor mesh is available on Cisco Aironet 1130 and 1240 series access points.

Enterprise 11n mesh is an enhancement added to the CUWN feature to work with the 802.11n access points. Enterprise 11n mesh features are compatible with non-802.11n mesh but adds higher backhaul and client access speeds. The 802.11n indoor access points are two-radio Wi-Fi infrastructure devices for select indoor deployments. One radio can be used for local (client) access for the access point and the other radio can be configured for wireless backhaul. The backhaul is supported only on the 5-GHz radio. Enterprise 11n mesh supports P2P, P2MP, and mesh types of architectures.

You have a choice of ordering indoor access points 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). 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 indoor mesh access points 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 GHz, and 5.8 GHz bands.

Cisco Outdoor Mesh Access Points

Cisco outdoor mesh access points comprise of the Cisco Aironet 1500 series access points. The 1500 series includes 1552 11n outdoor mesh access points, 1522 dual-radio mesh access points, and 1524 multi-radio mesh access points. There are two models of the 1524, which are the following:

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

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

Cisco 1500 series mesh access points are the core components of the wireless mesh deployment. AP1500s are configured by both the controller (GUI and CLI) and Cisco WCS. Communication between outdoor mesh access points (MAPs and RAPs) is over the 802.11a/n radio backhaul. Client traffic is generally transmitted over the 802.11b/g/n radio (802.11a/n 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 the 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 the signal strength and the number of hops required to get to a controller.

AP1500s are manufactured in two different configurations: cable and noncable.

- The cable configuration can be mounted to a cable strand and supports power-over-cable (POC).
- The noncable configuration supports multiple antennas. It can be mounted to a pole or building wall and supports several power options.

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 can be DOCSIS 2.0 or DOCSIS/EuroDOCSIS 3.0 depending upon the type of mesh access point.

AP1500s are available in a hazardous location hardware enclosure. When configured, the AP1500 complies with safety standards for Class I, Division 2, Zone 2 hazardous locations.

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

Mesh Deployment Modes

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

- Wireless mesh
- Wireless backhaul
- Point-to-Multipoint Wireless Bridging
- Point-to-Point Wireless Bridging

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 10-2 shows an example of a simple mesh network deployment composed of mesh access point (MAPs and RAPs), controllers, and Cisco WCS.

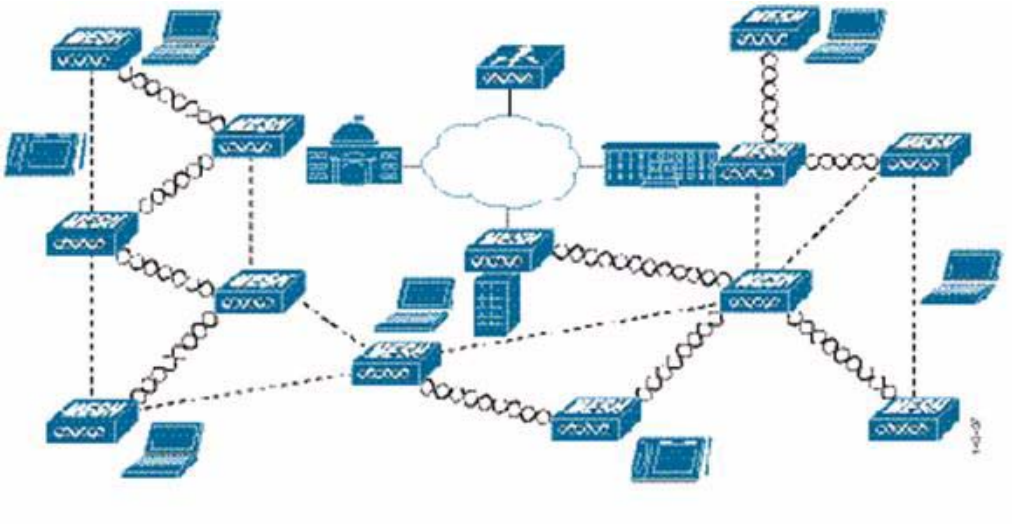
The three RAPs are connected to the wired network at each location and are located on the building roof. All the downstream access points operate as MAPs and communicate using wireless links (not shown).

Both MAPs and RAPs can provide WLAN client access; however, the location of RAPs are often not suitable for providing client access. All the three access points in Figure 10-2 are located on the building roofs and are functioning as RAPs. These RAPs 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).

Note For more details on CAPWAP, see the "Architecture Overview" section on page 10-11.

Figure 10-2 Wireless Mesh Deployment



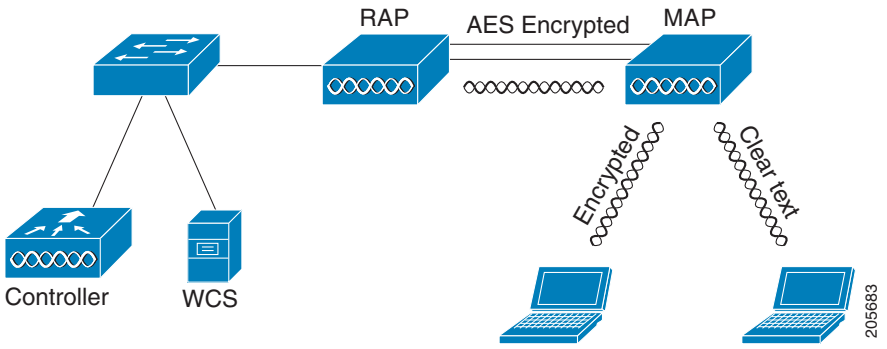
Wireless Backhaul

In a Cisco wireless backhaul network, traffic can be bridged between MAPs and RAPs. Outdoor Mesh AP and indoor AP converted to MAP mode are supported if CAPWAP over CAPWAP using ethernet bridging is supported. Both, local and flexconnect modes are support in MAP using ethernet bridging. 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 (see Figure 10-3).

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.

Only 5 GHz backhaul is possible on all mesh access points except 1522 in which either 2.4 or 5 GHz radio can be configured as a backhaul radio (see the "Configuring Advanced Features" section on page 10-63).

Figure 10-3 Wireless Backhaul



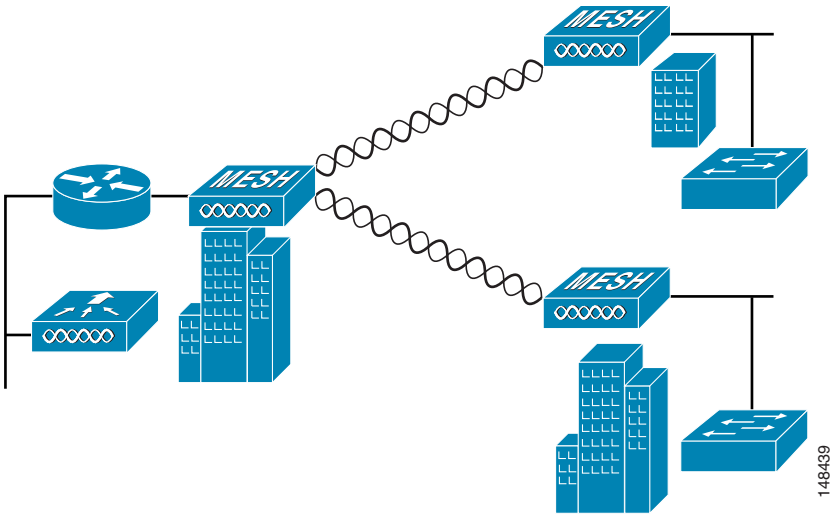
Universal Access

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 or 802.11a/n radio and client association is allowed only over the 802.11b/g or 802.11b/g/n radio. For more information about the configuration, see the "Configuring Advanced Features" section on page 10-63.

Point-to-Multipoint Wireless Bridging

In the point-to-multipoint bridging scenario, a RAP acting as a root bridge connects multiple MAPs as nonroot bridges with their associated wired LANs. By default, this feature is disabled for all MAPs. If Ethernet bridging is used, you must enable it on the controller for the respective MAP and for the RAP. Figure 10-4 shows a simple deployment with one RAP and two MAPs, but this configuration is fundamentally a wireless mesh with no WLAN clients. Client access can still be provided with Ethernet bridging enabled, although if bridging between buildings, MAP coverage from a high rooftop might not be suitable for client access.

Figure 10-4 Point-to-Multipoint Bridging Example

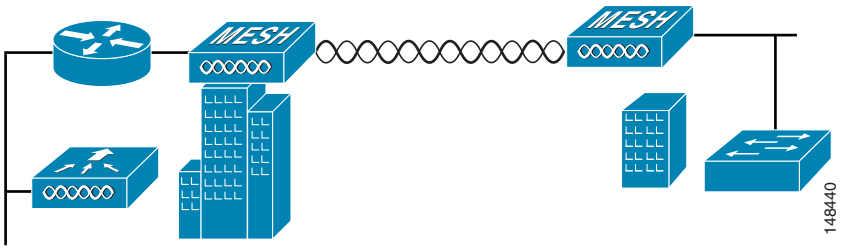


Point-to-Point Wireless Bridging

In a point-to-point bridging scenario, a 1500 Series Mesh AP can be used to extend a remote network by using the backhaul radio to bridge two segments of a switched network (see Figure 10-5). This is fundamentally a wireless mesh network with one MAP and no WLAN clients. Just as in point-to-multipoint networks, client access can still be provided with Ethernet bridging enabled, although if bridging between buildings, MAP coverage from a high rooftop might not be suitable for client access.

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

Figure 10-5 Point-to-Point Bridging Example



For security reasons the Ethernet port on the MAPs is disabled by default. It can be enabled only by configuring Ethernet Bridging on the Root and the respective MAPs (see Figure 10-6).

Ethernet bridging has to be enabled for the following two scenarios:

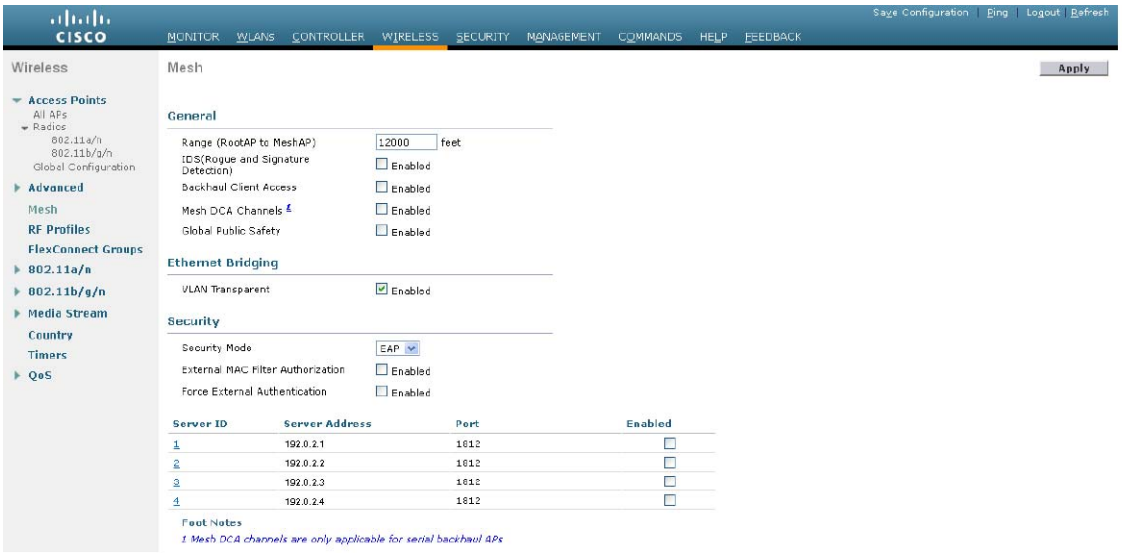
1. When you want to use the mesh nodes as bridges.
2. When you want to connect Ethernet devices such as a video camera on the MAP using its Ethernet port.

Figure 10-6 Wireless > All APs > Details

Ensure that you enable Ethernet bridging for every parent mesh AP taking the path from the mesh AP in question to the controller. For example, if you enable Ethernet bridging on MAP2 in Hop 2, then you must also enable Ethernet bridging on MAP1 (parent MAP), and on the RAP connecting to the controller.

Range Parameters have to be configured for longer links under the **Wireless > Mesh** tab. Optimum distance (in feet) should exist between the root access point (RAP) and the farthest mesh access point (MAP). Range from the RAP bridge to the MAP bridge has to be mentioned in feet.

Figure 10-7 Configuring Range Parameters



The following 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

Configuring Mesh Range (CLI)

- To configure the distance between the nodes doing the bridging, enter this commands:

  config mesh range *range-in-feet*

- To get the mesh range, enter the following command:

  show mesh config

  Information similar to the following:

```
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
```

Note APs reboot after you specify the range.

To estimate the range, you can use range calculators that are available at:

- Cisco 1520 Series Outdoor Mesh Range Calculation Utility: http://www.cisco.com/en/US/products/ps8368/products_implementation_design_guides_list.html
- Range Calculator for 1550 Series Outdoor Mesh Access Points: http://www.cisco.com/en/US/partner/products/ps11451/products_implementation_design_guides_list.html

Assumptions for the AP1522 Range Calculator

- The AP1522 Range Calculator has been edited to stay within limitations for Tx power and EIRP under the listed regulatory domains. There may be cases where it exceeds the limitations. You must verify that the installation is within the laws of the location in which it is being installed.
- When you use the AP1522 Range Calculator, available power levels change based upon the regulatory domain, the antenna (or antenna gain) selected, the modulation mode, which is based on the data rate selected (OFDM requires a lower power level in some domains). You must verify all parameters after making any parameter changes.
- Rx sensitivity in 2.4 GHz is the composite sensitivity of all three Rx paths. That is, MRC is included in 2.4 GHz. There is only one Rx for 5 GHz.
- You can choose only the channels that the access point is certified for.
- You can select only valid power levels.

Assumptions for the AP1552 Range Calculator

- The AP1552 Range Calculator has been edited to stay within limitations for Tx power and EIRP under the listed regulatory domains. There may be cases where it exceeds the limitations. You must verify that the installation is within the laws of the location in which it is being installed.
- All three antenna ports must be used for external antenna models of 1552 for effective performance. Otherwise, range is significantly compromised. 1552 radios have two Tx paths and three Rx paths.
- The Tx power is the total composite power of both Tx paths.
- Rx sensitivity is the composite sensitivity of all three Rx paths. That is, MRC is included.
- The AP1552 Range Calculator assumes that ClientLink (Beamforming) is switched on.
- When you use the AP1552 Range Calculator, available power levels change based upon the regulatory domain, the antenna (or antenna gain) selected, and the data rate selected. You must verify all parameters after making any parameter changes.
- You can select a different antenna than the two that are available by default. If you enter a high gain antenna and choose a power that goes over the EIRP limit, then you get a warning and the range equals 0.
- You can choose only the channels that the access point is certified for.
- You can only select only valid power levels.

Architecture Overview

This section contains the following sections:

Control And Provisioning of Wireless Access Points (CAPWAP)

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

Cisco Adaptive Wireless Path Protocol Wireless Mesh Routing

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

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

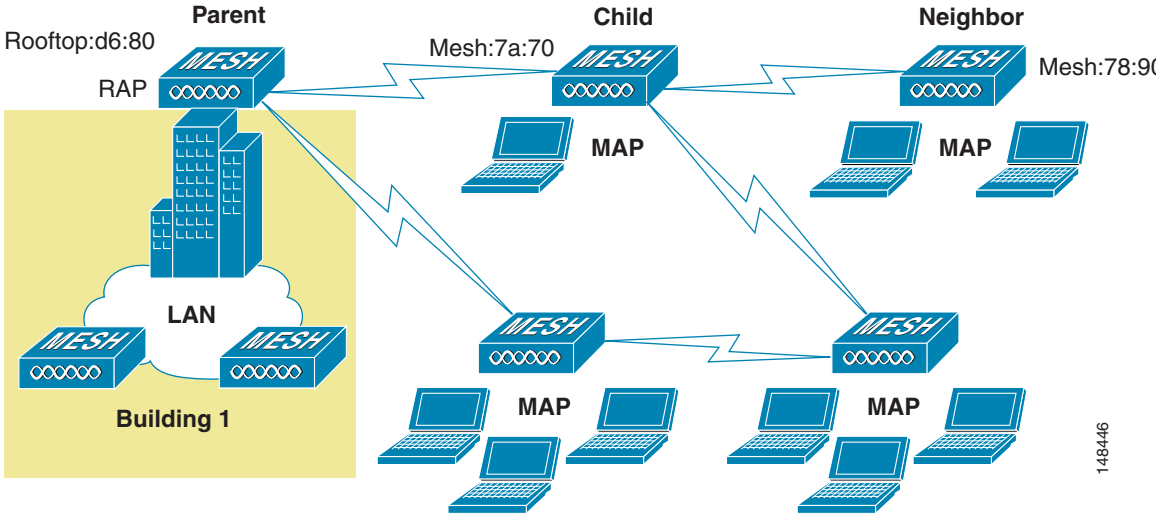
The goal of AWPP is to find the best path back to a RAP for each MAP that is part of the RAP's bridge group. To do this, the MAP actively solicits for neighbor MAPs. During the solicitation, the MAP learns all of the available neighbors back to a RAP, determines which neighbor offers the best path, and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

Mesh Neighbors, Parents, and Children

Relationships among access points with the mesh network are labeled as parent, child, or neighbor (see Figure 10-8) as follows:

- 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, an access point with a higher ease value is selected.
- A child access point selects the parent access point as its best route back to the RAP.
- A neighbor access point is within the radio frequency (RF) range of another access point but is not selected as its parent or a child because its *ease* values are lower than that of the parent.

Figure 10-8 Parent, Child, and Neighbor Access Points



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 characteristics apply to the backhaul network design and others to the CAPWAP controller design.

Wireless Backhaul Data Rate

Backhaul is used to create only the wireless connection between the access points. The backhaul interface by default is 802.11a or 802.11a/n depending upon the access point. The rate selection is important for effective use of the available RF spectrum. The rate can also affect the throughput of client devices, and throughput is an important metric used by industry publications to evaluate vendor devices.

Dynamic Rate Adaptation (DRA) introduces a process to estimate optimal transmission rate for packet transmissions. It is important to select rates correctly. If the rate is too high, packet transmissions fail resulting in communication failure. If the rate is too low, the available channel bandwidth is not used, resulting in inferior products, and the potential for catastrophic network congestion and collapse.

Data rates also affect the RF coverage and network performance. Lower data rates, for example 6 Mbps, can extend farther from the access point than can higher data rates, for example 300 Mbps. As a result, the data rate affects cell coverage and consequently the number of access points required. Different data rates are achieved by sending a more redundant signal on the wireless link, allowing data to be easily recovered from noise. The number of symbols sent out for a packet at the 1-Mbps data rate is higher than

the number of symbols used for the same packet at 11 Mbps. Therefore, sending data at the lower bit rates takes more time than sending the equivalent data at a higher bit rate, resulting in reduced throughput.

A lower bit rate might allow a greater distance between MAPs, 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 MAPs or results in a reduced SNR between MAPs, limiting mesh reliability and interconnection. For more information about configuring wireless backhaul data rate, see the "Configuring Wireless Backhaul Data Rate" section on page 10-38.

Note The data rate can be set on the backhaul on a per AP basis. It is not a global command.

The required minimum Link SNR for backhaul links per data rate is shown in Table 10-1.

Table 10-1 Backhaul Data Rates and Minimum Link SNR Requirements

802.11a Data Rate (Mbps)	Minimum Required Link SNR (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 10-2 summarizes the calculation by data rate.

  - Minimum SNR refers to an ideal state of noninterference, nonnoise, and a system packet error rate (PER) of no more than 10 percent.
  - Typical fade margin is approximately 9 to 10 dB.

Table 10-2 Minimum Required Link SNR Calculations by Data Rate

802.11n Date Rate (Mbps)	Minimum SNR (dB) +	Fade Margin =	Minimum Required Link SNR (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

- If you take into account the effect of MRC for calculating Minimum Required Link SNR. Table 10-3 shows the required Link SNR for 802.11a/g (2.4 GHz and 5 GHz) for AP1552 and 1522 with 3 Rx antennas (MRC gain).

  LinkSNR = Minimum SNR - MRC + Fade Margin (9 dB)

Table 10-3 Required Link SNR Calculations for 802.11a/g

802.11a/g MCS (Mbps)	Modulation	Minimum SNR (dB)	MRC Gain from 3 RXs (dB)	Fade Margin (dB)	Required Link SNR (dB)
6	BPSK 1/2	5	4.7	9	9.3
9	BPSK 3/4	6	4.7	9	10.3
12	QPSK 1/2	7	4.7	9	11.3
18	QPSK 3/4	9	4.7	9	13.3
24	16QAM 1/2	13	4.7	9	17.3
36	16QAM 3/4	17	4.7	9	21.3
48	64QAM 2/3	20	4.7	9	24.3
54	64QAM 3/4	22	4.7	9	26.3

If you consider only 802.11n rates, Table 10-4 shows Link SNR requirements with AP1552 for 2.4 and 5 GHz.

Table 10-4 Requirements for Link SNR with AP1552 for 2.4 and 5 GHz

No. of Spatial Streams	11n MCS	Modulation	Minimum SNR (dB)	MRC Gain from 3 RXs (dB)	Fade Margin (dB)	Link SNR (dB)
1	MCS 0	BPSK 1/2	5	4.7	9	9.3
1	MCS 1	QPSK 1/2	7	4.7	9	11.3
1	MCS 2	QPSK 3/4	9	4.7	9	13.3
1	MCS 3	16QAM 1/2	13	4.7	9	17.3
1	MCS 4	16QAM 3/4	17	4.7	9	21.3
1	MCS 5	64QAM 2/3	20	4.7	9	24.3
1	MCS 6	64QAM 3/4	22	4.7	9	26.3
1	MCS 7	64QAM 5/6	23	4.7	9	27.3
2	MCS 8	BPSK 1/2	5	1.7	9	12.3
2	MCS 9	QPSK 1/2	7	1.7	9	14.3
2	MCS 10	QPSK 3/4	9	1.7	9	16.3
2	MCS 11	16QAM 1/2	13	1.7	9	20.3
2	MCS 12	16QAM 3/4	17	1.7	9	24.3
2	MCS 13	64QAM 2/3	20	1.7	9	27.3
2	MCS 14	64QAM 3/4	22	1.7	9	29.3
2	MCS 15	64QAM 5/6	23	1.7	9	30.3

Note With two spatial streams, the MRC gain is halved, that is the MRC gain is reduced by 3 dB. This is because the system has 10 log (3/2 SS) instead of 10 log (3/1 SS). If there were to have been 3 SS with 3 RX, then the MRC gain would have been zero.

- Number of backhaul hops is limited to eight but we recommend three to four hops.

  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, which 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 the number 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.

ClientLink Technology

Many networks still support a mix of 802.11a/g and 802.11n clients. Because 802.11a/g clients (legacy clients) operate at lower data rates, the older clients can reduce the capacity of the entire network. Cisco ClientLink can help solve problems related to adoption of 802.11n in mixed-client networks by ensuring that 802.11a/g clients operate at the best possible rates, especially when they are near cell boundaries.

Advanced signal processing has been added to the Wi-Fi chipset. Multiple transmit antennas are used to focus transmissions in the direction of the 802.11a/g client, increasing the downlink signal-to-noise ratio and the data rate over range, thereby reducing coverage holes and enhancing the overall system performance. This technology learns the optimum way to combine the signal received from a client and then uses this information to send packets in an optimum way back to the client. This technique is also referred to as MIMO (multiple-input multiple-output) beamforming, transmit beamforming, or cophasing, and it is the only enterprise-class and service provider-class solution in the market that does not require expensive antenna arrays.

The 802.11n systems take advantage of multipath by sending multiple radio signals simultaneously. Each of these signals, called a spatial stream, is sent from its own antenna using its own transmitter. Because there is some space between these antennas, each signal follows a slightly different path to the receiver, a situation called spatial diversity. The receiver has multiple antennas as well, each with its own radio that independently decodes the arriving signals, and each signal is combined with signals from the other receiver radios which results in multiple data streams receiving at the same time. This enables a higher throughput than previous 802.11a/g systems, but requires an 802.11n capable client to decipher the signal. Therefore, both AP and client need to support this capability. Due to the complexity of issues, in the first generation of mainstream 802.11n chipsets, neither the AP nor client chipsets implemented 802.11n transmit beamforming. Therefore, the 802.11n standard transmit beamforming will be available eventually, but not until the next generation of chipsets take hold in the market.

For the current generation of 802.11n APs, while the second transmit path was being well utilized for 802.11n clients (to implement spatial diversity), it was not being fully used for 802.11a/g clients. For 802.11 a/g clients, some of the capabilities of the extra transmit path was lying idle. In addition, for many networks, the performance of the installed 802.11 a/g client base would be a limiting factor on the network.

Cisco ClientLink uses advanced signal processing techniques and multiple transmit paths to optimize the signal received by 802.11a/g clients in the downlink direction without requiring feedback. Because no special feedback is required, Cisco ClientLink works with all existing 802.11a/g clients.

Cisco ClientLink technology effectively enables the access point to optimize the SNR exactly at the position where the client is placed. Cisco ClientLink provides a gain of almost 4 dB in the downlink direction. Improved SNR yields many benefits, such as a reduced number of retries and higher data rates. For example, a client at the edge of the cell that might previously have been capable of receiving packets at 12 Mbps could now receive them at 36 Mbps. Typical measurements of downlink performance with Cisco ClientLink show as much as 65 percent greater throughput for 802.11a/g clients. By allowing the Wi-Fi system to operate at higher data rates and with fewer retries, Cisco ClientLink increases the overall capacity of the system, which means an efficient use of spectrum resources.

Cisco ClientLink in the 1552 access points is based on Cisco ClientLink capability available in AP3500s. Therefore, the access point has the ability to beamform well to nearby clients and to update beamforming information on 802.11ACKs. Even if there is no dedicated uplink traffic, the Cisco ClientLink works well, which is beneficial to both TCP and UDP traffic streams. There are no RSSI watermarks, which the client has to cross to take advantage of this beamforming with Cisco 802.11n access points.

Cisco ClientLink can beamform to 15 clients at a time. Therefore, the host must select the best 15 if the number of legacy clients exceeds 15 per radio. AP1552 has two radios, which means that up to 30 clients can be beamformed in time domain.

Although ClientLink is applied to legacy OFDM portions of packets, which refers to 11a/g rates (not 11b) for both indoor and outdoor 802.11n access points, there is one difference between ClientLink for indoor 11n and ClientLink for outdoor 11n. For indoor 11n access points, the SW limits the affected rates to 24, 36, 48, and 54 Mbps. To avoid clients sticking to a far away AP in an indoor environment. SW also does not allow ClientLink to work for those rates for 11n clients because the throughput gain is so minimal. However, there is a demonstrable gain for pure legacy clients. For outdoor 11n access points, three more additional legacy data rates lower than 24 Mbps have been added. ClientLink for outdoors is applicable to legacy data rates of 9, 12, 18, 24, 36, 48, and 54 Mbps.

Configuring Cisco ClientLink (CLI)

Note From the 7.2 release onwards, it is not possible to configure ClientLink (beamforming) using the controller GUI.

Step 1 Disable the 802.11a or 802.11b/g network by entering this command:

config {802.11a | 802.11b} disable network

Step 2 Reenable the network by entering this command:

config {802.11a | 802.11b} enable network

Step 3 Save your changes by entering this command:

save config

Commands Related to Cisco ClientLink

- The following commands are to be entered in the AP console:
  - To find a client in the AP rbf table, enter the **show interface dot110** command.
- The following commands on the AP console are used for troubleshooting:
  - To show that ClientLink is enabled on a radio, enter the **show controllers | inc Beam** command.

    The output is displayed as follows:

```
Legacy Beamforming: Configured Yes, Active Yes, RSSI Threshold -50 dBm
Legacy Beamforming: Configured Yes, Active Yes, RSSI Threshold -60 dBm
```

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, which gives a total number of 7200 possible access points per mobility group.
- Number of mesh access points supported per controller. See Table 10-5.

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

Table 10-5 Mesh Access Point Support by Controller Models

Controller Model	Local AP Support (nonmesh)[1]	Maximum Possible Mesh AP Support
5508	500	500
4404	100	150
2504	50	50
2106	6	11
2112	12	12
2125	25	25
WiSM	300	375
WiSM2	500	500

1. Local AP support is the total number of nonmesh APs supported on the controller model.

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.

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.

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

Ensure that you 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 the MAC Filter" section on page 10-19.
2. Define the role (RAP or MAP) for the mesh access point. See the "Defining Mesh Access Point Role" section on page 10-20.

Note CAPWAP supports only layer3 mode and it does not support layer2 mode.

3. 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 10-21.
4. Configure a backup controller. See the "Configuring Backup Controllers" procedure on page 10-22.
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 10-27.
6. Configure global mesh parameters. See the "Configuring Global Mesh Parameters" section on page 10-31.
7. Configure universal client access. Configuring universal client access is part of the Configuring Advanced Features section. See the "Universal Client Access" section on page 10-66.
8. Configure local mesh parameters. See the "Configuring Local Mesh Parameters" section on page 10-38.
9. Configure mobility groups (if desired) and assign controllers. See Chapter 12, Configuring Mobility Groups.

Adding MAC Addresses of Mesh Access Points to the MAC Filter

You must enter the radio 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 does not need to be added to the MAC Filtering List.

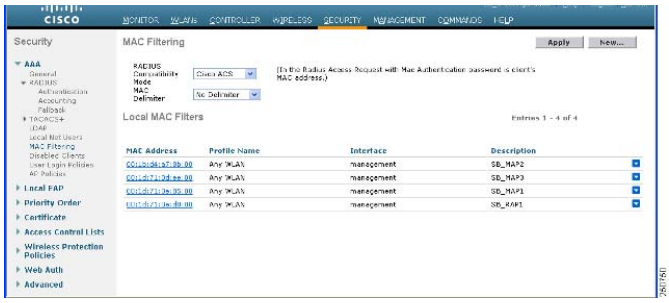
You can add the mesh access point using either the GUI or the CLI.

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 7.0.172.0*: http://www.cisco.com/en/US/docs/wireless/wcs/7.0MR1/configuration/guide/WCS70MR1.html

Adding the MAC Address of the Mesh Access Point to the Controller Filter List (GUI)

Step 1 Choose **Security > AAA > MAC Filtering**. The MAC Filtering page appears.

Figure 10-9 MAC Filtering Page



Step 2 Click **New**. The MAC Filters > New page appears.

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

Note For 1500 series outdoor mesh access points, specify the BVI MAC address of the mesh access point into the controller as a MAC filter. For 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, choose **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 *roof 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 (CLI)

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, AP1500s are shipped with a radio role set to MAP. You must reconfigure a mesh access point to act as a RAP.

Information About MAP and RAP Association With the Controller

- A MAP always sets the Ethernet port as the *primary backhaul* if it is UP, and secondarily the 802.11a/n 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/n 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/n 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/n radio causes the primary backhaul to go into the *scan* state. The primary backhaul begins its scan with the Ethernet port.

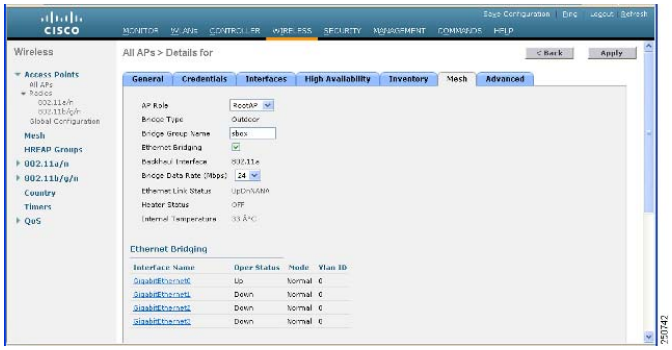
Configuring the AP Role (GUI)

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

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

Step 3 Click the **Mesh** tab.

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



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 (CLI)

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

Configuring Multiple Controllers Using DHCP 43 and DHCP 60

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 1550 series access points, enter *Cisco AP c1550*
- 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 as follows:

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 as follows:

```
option 43 hex f1080a7e7e020a7f7f02
```

Configuring Backup Controllers

This section contains the following topics:

Information About 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.

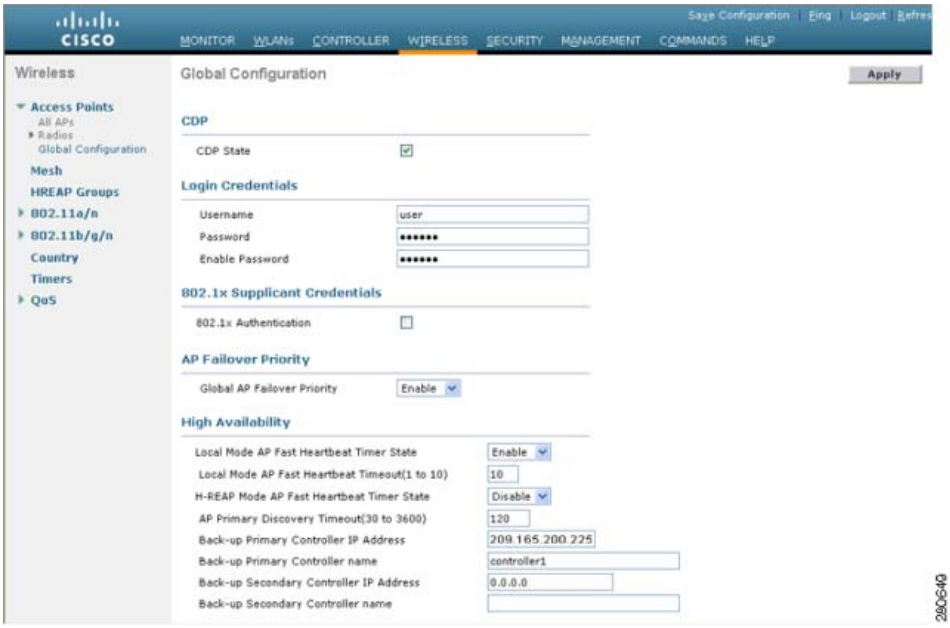
Guidelines and Limitations

- The fast heartbeat timer is not supported on mesh access points. The fast heartbeat timer is only configured on access points in local and flexconnect 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, and 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.
- 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.
- 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 (GUI)

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

Figure 10-11 Global Configuration Page



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.

Figure 10-12 All APs > Details for (High Availability) Page

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 (CLI)

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 releases. 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 10-28.
- 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 10-28.

Note If mesh access points connect to a 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

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 as follows:

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 as follows:

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, in addition to adding the MAC address to the user list, you need to enter the *platform_name_string–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–MAC_address* string as the username.

Example: RADIUS Server Username Entry

For each mesh access point, two entries must be added to the RADIUS server, the *platform_name_string-MAC_address* string, then a hyphen delimited MAC Address. For example:

- platform_name_string-MAC_address

  User: c1520-aabbccddeeff

  Password: cisco
- Hyphen Delimited MAC Address

  User: aa-bb-cc-dd-ee-ff

  Password: aa-bb-cc-dd-ee-ff

Note The platform AP1552 uses a platform name of c1520.

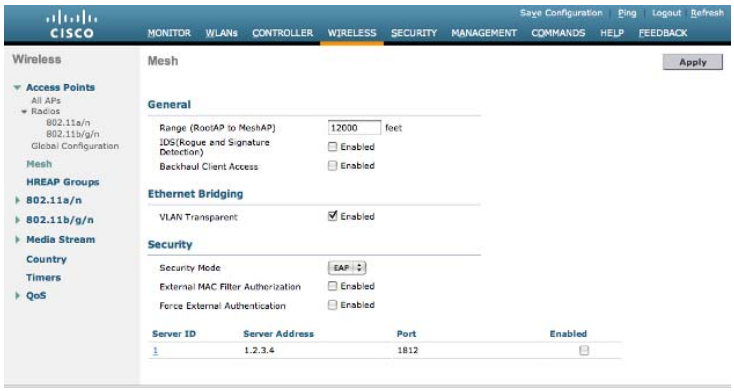
Enabling External Authentication of Mesh Access Points

This section contains the following topics:

Enabling External Authentication of Mesh Access Points (GUI)

Step 1 Choose **Wireless > Mesh**. The Mesh page appears.

Figure 10-13 Mesh Page



Step 2 In the security section, choose 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 (CLI)

Step 1 **config mesh security eap**

Step 2 **config macfilter mac-delimiter colon**

Step 3 **config mesh security rad-mac-filter enable**

Step 4 **config mesh radius-server** *index* **enable**

Step 5 **config mesh security force-ext-auth enable** (Optional)

Viewing Security Statistics

To view security statistics for mesh access points using the CLI, enter this 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 contains the following topics:

Information About Configuring Global Mesh Parameters

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

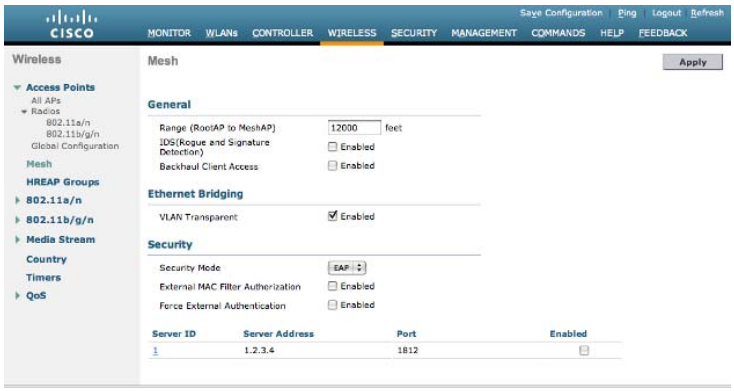
- Setting the maximum range between RAP and MAP (not applicable to indoor MAPs).
- Enabling a backhaul to carry client traffic.
- Defining if VLAN tags are forwarded or not.
- Defining the authentication mode (EAP or PSK) and method (local or external) for mesh access points including security settings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

Step 1 Choose **Wireless > Mesh**.

Figure 10-14 Mesh Page



Step 2 Modify the mesh parameters as appropriate.

Table 10-6 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 **Note** 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 client access only and not on the backhaul. When you disable this feature, no IDS reports are generated, which preserves bandwidth on the backhaul. You have to use the following command to enable or disable it on the mesh APs: **config mesh ids-state** {**enable** | **disable**} **Note** 2.4GHz IDS is activated with the global IDS settings on the controller.

Table 10-6 Global Mesh Parameters (continued)

Parameter	Description
Backhaul Client Access	**Note** This parameter applies to mesh access points with two or more radios (1552, 1524SB, 1522, 1240, 1130, and 11n indoor mesh APs) *excluding* the 1524PS. When Universal Client Access is enabled, it allows wireless client association over the backhaul radio. Generally, backhaul radio is a 5-GHz radio for most of the mesh access points except for 1522 where backhaul can be 2.4 GHz. This means that a backhaul radio can carry both backhaul traffic and client traffic. When Universal Client Access is disabled, only backhaul traffic is sent over the backhaul radio and client association is only over the second radio(s). **Default:** Disabled **Note** After this feature is enabled, all mesh access points reboot.

Table 10-6 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 10-63 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, Ethernet VLAN tagging must be configured. See "Enabling Ethernet Bridging (GUI)" section on page 10-44. **Note** For an overview of normal, access, and trunk Ethernet port use, see "Ethernet Port Notes" section on page 10-72. **Note** To use VLAN tagging, you must uncheck 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 10-14). **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 unchecked). **Options:** PSK or EAP **Default:** EAP

Table 10-6 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 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 (CLI)

Note See the "Configuring Global Mesh Parameters (GUI)" section on page 10-31 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 the **show mesh range** command.

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 (CLI)

- **show mesh client-access**—When Universal Client Access is enabled, it allows wireless client association over the backhaul radio. Generally, backhaul radio is a 5-GHz radio for most of the mesh access points except for 1522 where backhaul can be 2.4 GHz. This means that a backhaul radio can carry both backhaul traffic and client traffic.

  When Universal Client Access is disabled, only backhaul traffic is sent over the backhaul radio and client association is only over the second radio(s).

  Example:

  show mesh client-access

  ```
  Backhaul with client access status: enabled
  ```

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

  Example:

  show mesh ids-state

  ```
  Outdoor Mesh IDS(Rogue/Signature Detect): .... Disabled
  ```

- **show mesh config**—Displays global configuration settings.

  Example:

  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:

- Backhaul Data Rate. See the "Configuring Wireless Backhaul Data Rate" section on page 10-38.
- Ethernet Bridging. See the "Configuring Ethernet Bridging" section on page 10-43.
- Bridge Group Name. See the"Configuring Ethernet Bridging" section on page 10-43.
- Workgroup Bridge. See the "Configuring Workgroup Bridges" section on page 10-82.
- Public Safety Band Settings. See the "Configuring Public Safety Band Settings" section on page 10-46.
- Cisco 3200 Series Association and Interoperability. See the "Table 10-10 identifies mesh access points and their respective frequency bands that support WGB." section on page 10-91.
- Power and Channel Setting. See the"Configuring Power and Channel Settings" section on page 10-51.
- Antenna Gain Settings. See the "Configuring Antenna Gain" section on page 10-54.
- Backhaul channel deselection on serial backhaul access point. See the "Backhaul Channel Deselection on Serial Backhaul Access Point" section on page 10-55.
- Dynamic Channel Assignment. See the "Configuring Dynamic Channel Assignment (GUI)" section on page 10-60.

Configuring Wireless Backhaul Data Rate

Backhaul is used to create only the wireless connection between the access points. The backhaul interface by default is 802.11a or 802.11a/n depending upon the access point. The rate selection is important for effective use of the available RF spectrum. The rate can also affect the throughput of client devices, and throughput is an important metric used by industry publications to evaluate vendor devices.

Dynamic Rate Adaptation (DRA) introduces a process to estimate optimal transmission rate for packet transmissions. It is important to select rates correctly. If the rate is too high, packet transmissions fail resulting in communication failure. If the rate is too low, the available channel bandwidth is not used, resulting in inferior products, and the potential for catastrophic network congestion and collapse.

Data rates also affect the RF coverage and network performance. Lower data rates, for example 6 Mbps, can extend farther from the access point than can higher data rates, for example 300 Mbps. As a result, the data rate affects cell coverage and consequently the number of access points required. Different data rates are achieved by sending a more redundant signal on the wireless link, allowing data to be easily recovered from noise. The number of symbols sent out for a packet at the 1-Mbps data rate is higher than the number of symbols used for the same packet at 11 Mbps. Therefore, sending data at the lower bit rates takes more time than sending the equivalent data at a higher bit rate, resulting in reduced throughput.

In the controller release 5.2, the default data rate for the mesh 5-GHz backhaul is 24 Mbps. It remains the same with 6.0 and 7.0 controller releases.

With the 6.0 controller release, mesh backhaul can be configured for ‘Auto’ data rate. Once configured, the access point picks the highest rate where the next higher rate cannot be used because of conditions not being suitable for that rate and not because of conditions that affect all rates. That is, once configured, each link is free to settle down to the best possible rate for its link quality.

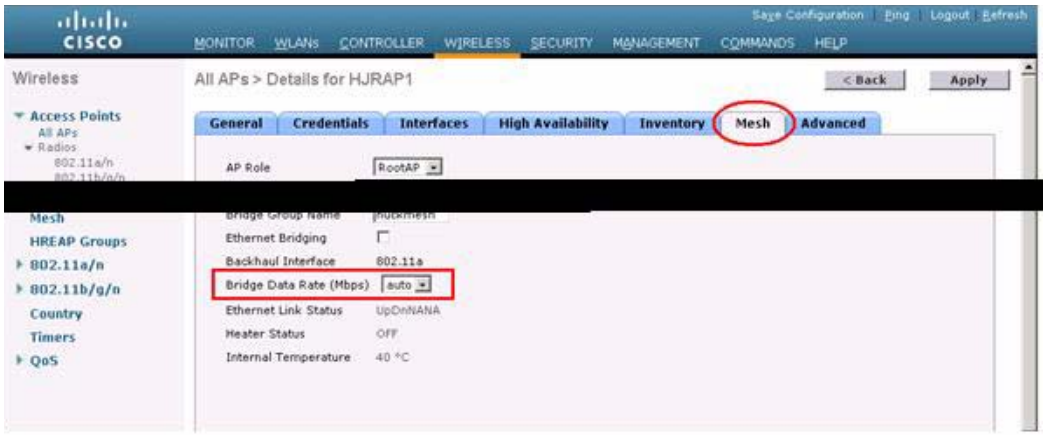
We recommend that you configure the mesh backhaul to Auto.

For example, if mesh backhaul chose 48 Mbps, then this decision is taken after ensuring that we cannot use 54 Mbps as there is not enough SNR for 54 and not because some just turned the microwave oven on which affects all rates.

A lower bit rate might allow a greater distance between MAPs, 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 MAPs or results in a reduced SNR between MAPs, limiting mesh reliability and interconnection.

Figure 10-15 shows the RAP using the "auto" backhaul data rate, and it is currently using 54 Mbps with its child MAP.

Figure 10-15 Bridge Rate Set to Auto



Note The data rate can be set on the backhaul on a per-AP basis. It is not a global command.

Related Commands

Use these commands to obtain information about backhaul:

- **config ap bhrate**—Configures the Cisco Bridge backhaul Tx rate.

  Syntax:

  config ap bhrate *backhaul-rate ap-name*

Note Preconfigured data rates for each AP (RAP=18 Mbps, MAP1=36 Mbps) are preserved after the upgrade to 6.0 or later software releases.

Before you upgrade to the 6.0 release, if you have the backhaul data rate configured to any data rate, then the configuration is preserved.

This example shows how to configure a backhaul rate of 36000 Kbps on a RAP:

```
config ap bhrate 36000 HPRAP1
```

- **show ap bhrate**—Displays the Cisco Bridge backhaul rate.

  Syntax:

  ```
  show ap bhrate ap-name
  ```

- **show mesh neigh summary**—Displays the link rate summary including the current rate being used in backhaul

  Example:

  ```
  show mesh neigh summary HPRAP1

  AP Name/Radio    Channel     Rate     Link-Snr     Flags      State
  ---------------- --------   --------   -------     -----      -----
  00:0B:85:5C:B9:20 0          auto        4       0x10e8fcb8   BEACON
  00:0B:85:5F:FF:60 0          auto        4       0x10e8fcb8   BEACON DEFAULT
  00:0B:85:62:1E:00 165        auto        4       0x10e8fcb8   BEACON
  OO:0B:85:70:8C:A0 0          auto        1       0x10e8fcb8   BEACON
  HPMAP1            165        54          40      0x36         CHILD BEACON
  HJMAP2            0          auto        4       0x10e8fcb8   BEACON
  ```

Backhaul capacity and throughput depends upon the type of the AP, that is, if it is 802.11a/n or only 802.11a, number of backhaul radios it has, and so on.

In AP1524 SB, Slot 2 in the 5-GHz radio in the RAP is used to extend the backhaul in the downlink direction, whereas Slot 2 in the 5-GHz radio in the MAP is used for backhaul in the uplink. We recommend using a directional antenna with the Slot 2 radio. MAPs extend Slot 1 radio in the downlink direction with Omni or directional antenna also providing client access. Client access can be provided on the Slot 2 radio from the 7.0 release onwards.

AP1524SB provides you with better throughput, and throughput rarely degrades after the first hop. The performance of AP1524SB is better than AP1522 and AP1524PS because these APs have only a single radio for the backhaul uplink and downlink (see Figure 10-16, Figure 10-17, Figure 10-18, and Figure 10-19).

Figure 10-16 1524SB TCP Downstream Rate Auto

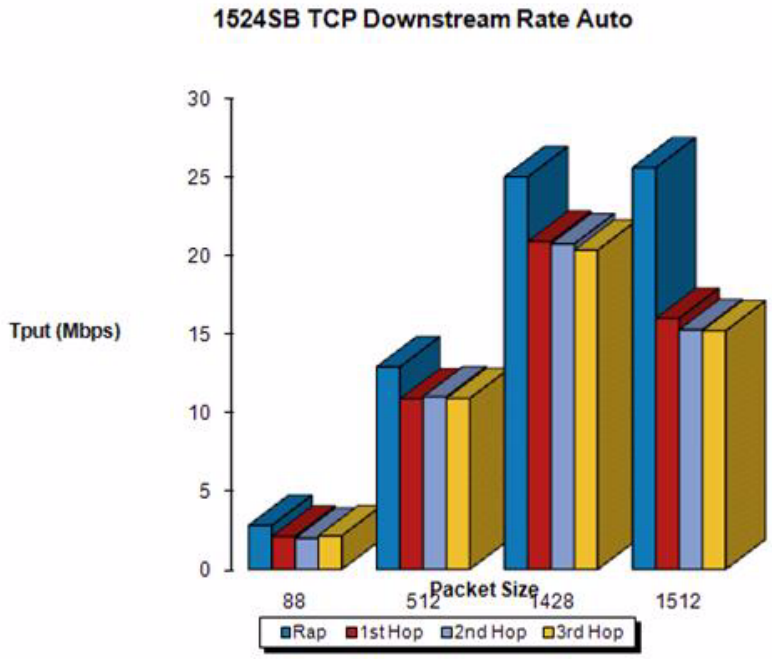
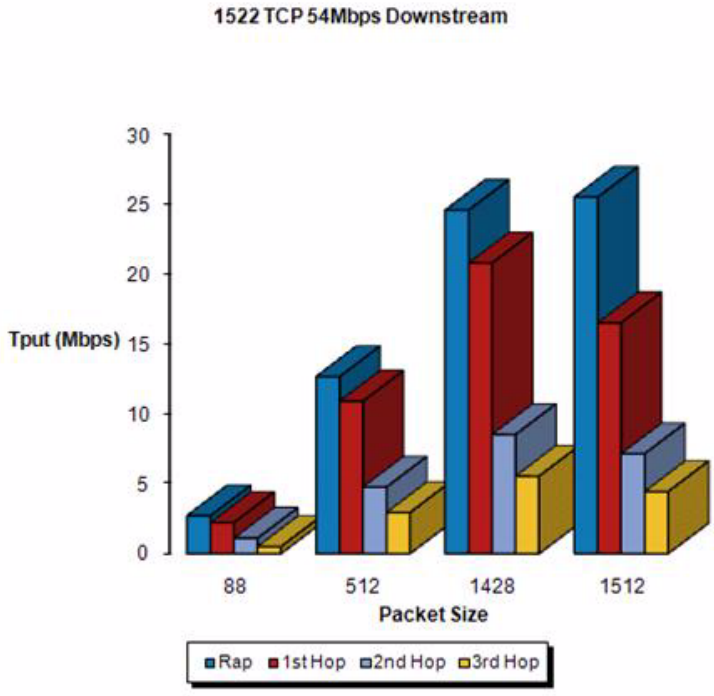


Figure 10-17 1522 TCP 54 Mbps Downstream



Note With DRA, each hop uses the best possible data rate for the backhaul. The data rate can be changed on a per-AP basis.

Figure 10-18 1524SB TCP Downstream Rate Auto

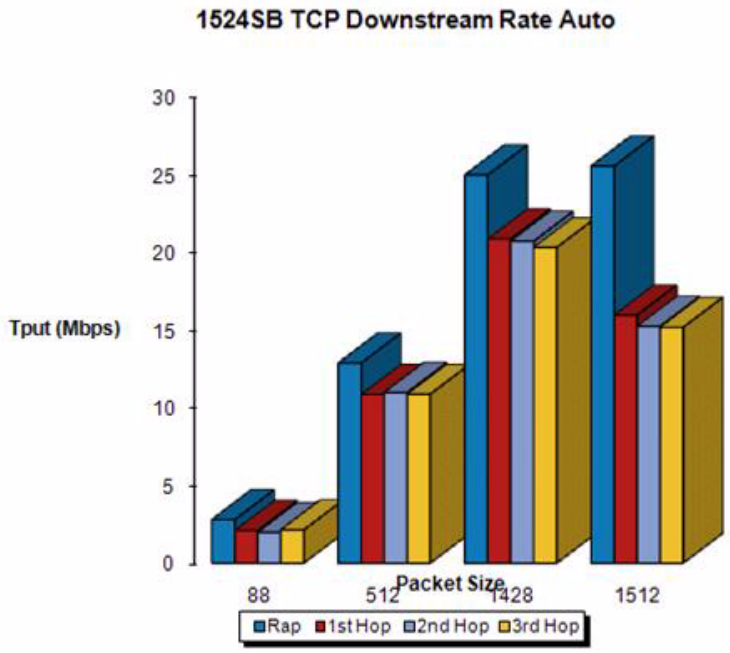
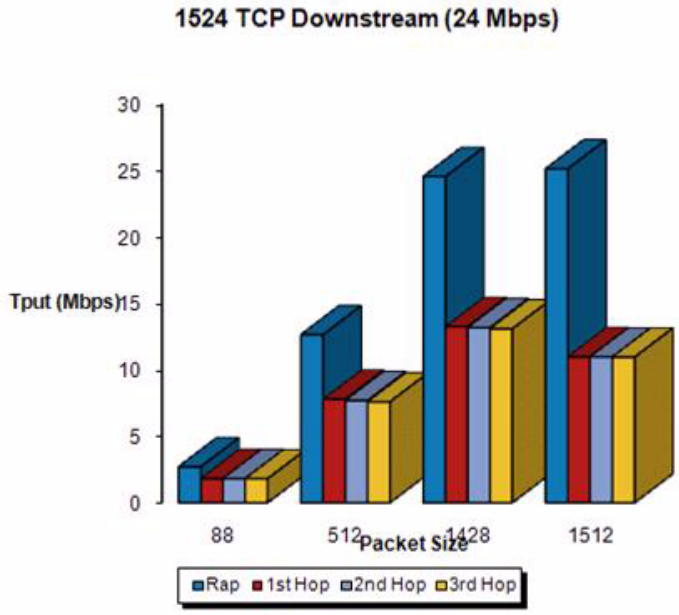


Figure 10-19 1524 TCP Downstream (24 Mbps)



Note Using 1552 802.11n provides you higher throughput and more capacity. It offers a very fat backhaul pipe to start with from the RAP.

Figure 10-20 AP1552 Backhaul Throughput

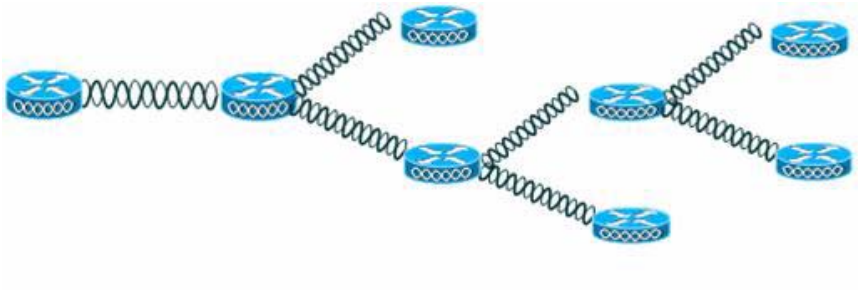


Table 10-7 AP1552 Backhaul Capacity

HOPS	RAP	One	Two	Three	Four
Maximum Throughput (20 MHz BH)	112 Mbps	83 Mbps	41 Mbps	25 Mbps	15 Mbps
Maximum Throughput (40 MHz BH)	206 Mbps	111 Mbps	94 Mbps	49 Mbps	35 Mbps

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, the following protocols are allowed:

– Spanning Tree Protocol (STP)
– Address Resolution Protocol (ARP)
– Control And Provisioning of Wireless Access Points (CAPWAP)
– 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.

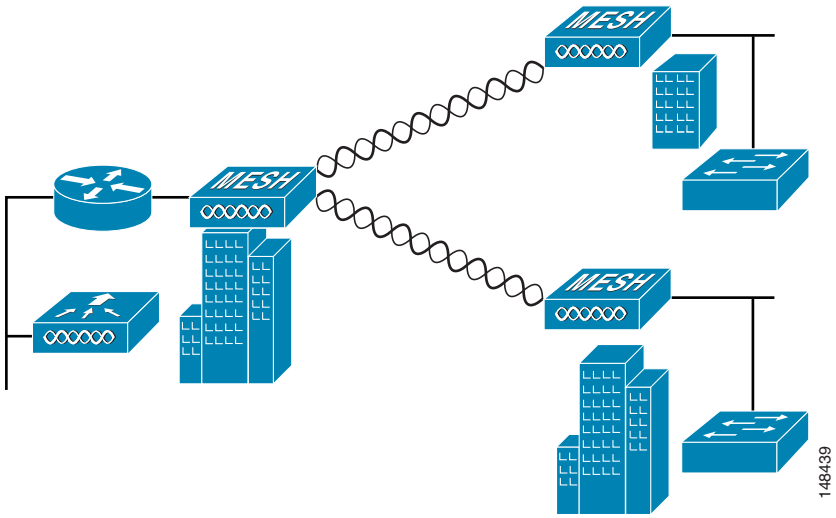
Ethernet bridging has to be enabled for two scenarios:

1. When you want to use the mesh nodes as bridges. (See Figure 10-21.)

   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 10-21 Point-to-Multipoint Bridging



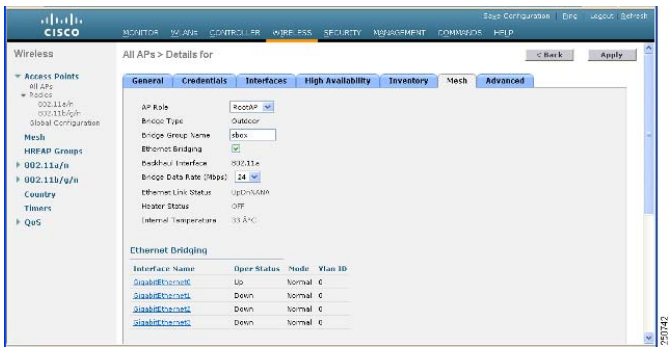
Enabling Ethernet Bridging (GUI)

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 click the **Mesh** tab.

Figure 10-22 All APs > Details for (Mesh) Page



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

Step 5 Select the **Ethernet Bridging** check box to enable Ethernet bridging or deselect it to disable this feature.

Step 6 Click **Apply** to commit your changes. An Ethernet Bridging section appears at the bottom of the page listing each of the Ethernet ports of the mesh access point.

Step 7 Ensure that you enable Ethernet bridging for every parent mesh AP taking the path from the mesh AP in question to the controller. For example, if you enable Ethernet bridging on MAP2 in Hop 2, then you must also enable Ethernet bridging on MAP1 (parent MAP), and on the RAP connecting to the controller.

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 Bridge Group Names (CLI)

- Using the CLI, enter the following command:

  config ap bridgegroupname set *bridge-group-name*

  Infomation similar to the following appears:

```
Setting bridgegroupname on an AP permanently restricts the APs to which it may
connect, use with caution.
Are you sure you want to continue? (y/n) n

AP bridgegroupname not changed!
```

  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 toward the RAP to ensure that no mesh access points are dropped due to mixed BGNs (old and new BGNs) within the same network.

Verifying Bridge Group Names (CLI)

- To verify the BGN, enter the following command:

  show ap config general *AP_Name*

  Information similar to the following is displayed.

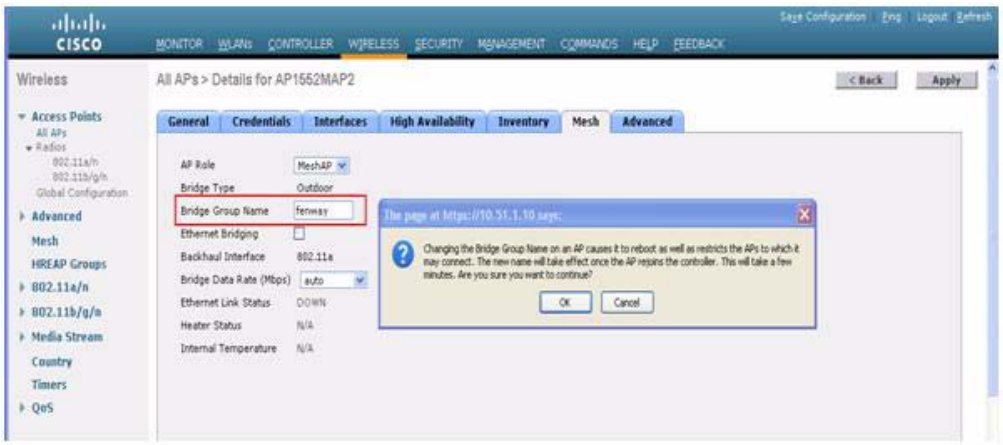
```
(Cisco Controller 1) >show ap config general AP1552RAP1

Cisco AP Identifier.............................. 122
Cisco AP Name.................................... AP1552RAP1
Country code..................................... US  - United States
Regulatory Domain allowed by Country............. 802.11bg:-A     802.11a:-A, outdoor mesh -AB
AP Country code.................................. US  - United States
AP Regulatory Domain............................. 802.11bg:-A     802.11a:-A
Switch Port Number .............................. 1
MAC Address...................................... 58:bc:27:c5:53:00
IP Address Configuration......................... DHCP
IP Address....................................... 10.51.1.68
IP NetMask....................................... 255.255.255.0
Gateway IP Addr.................................. 10.51.1.1
NAT External IP Address.......................... None
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.................. 10.51.1.10
Secondary Cisco Switch Name......................
Secondary Cisco Switch IP Address................ Not Configured
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 ................................ fenway
Public Safety ................................... Enabled
```

Verifying Bridge Group Names (GUI)

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.

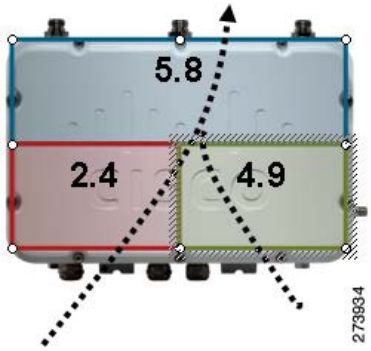
Figure 10-23 AP Name > Mesh



Configuring Public Safety Band Settings

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

Figure 10-24 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 backhaul. The 5.8 GHz is used only for backhaul, and there is no client access possible on it. 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 step can only be done at the global level and cannot be done on a 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 USA, you can only have public safety traffic on the 4.9-GHz backhaul. Check the destination countries compliance before installing.

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

Figure 10-25 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 this command:

  show mesh public-safety

  The following appears:

  ```
  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 the Antenna drop-down list)

Configuring Interoperability with 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 feature 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 the table below.

Table 10-8 Mesh Access Points and Cisco 3200 Interoperability

Mesh Access Point Model	Cisco 3200 Model
1552, 1522[1]	c3201[2], c3202[3], c3205[4]
1524PS	c3201, c3202
1524SB, 1130, 1240, Indoor 802.11n mesh access points	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 an 802.11b/g radio (2.4-GHz).
3. Model c3202 is a Cisco 3200 with a 4-9-GHz subband radio.
4. Model c3205 is a Cisco 3200 with a 802.11a radio (5.8-GHz subband.

Configuration Guidelines for Public Safety 4.9-GHz Band

- 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.
- The 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 subband channels 1 through 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 band (channels 1 to 10) or 10-MHz band (channels 11 to 19).

- Radio (802.11a) must be disabled when configuring channels and then reenabled 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.

Enabling AP1522 to Associate with Cisco 3200 (GUI)

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

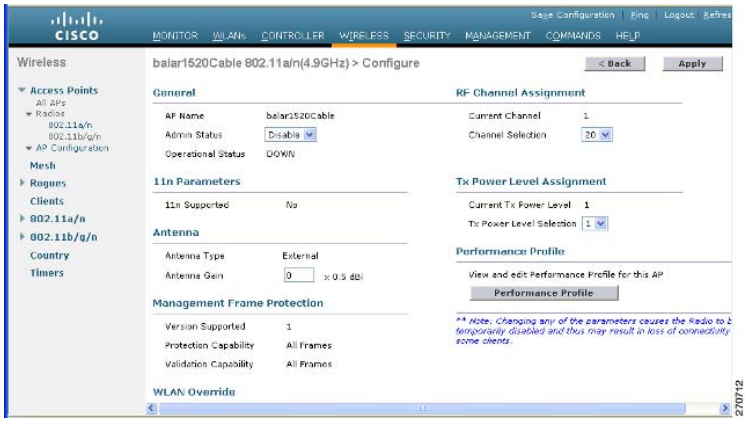
Step 2 Select the Backhaul Client Access **Enabled** check box to allow wireless client association over the 802.11a radio. Click **Apply**.

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 appears.

Step 4 At the Antenna drop-down list for the appropriate RAP, select **Configure**. The Configure page appears.

Figure 10-26 Wireless > Access Points > Radio > 802.11 a/n > Configure Page



Step 5 At the RF Channel Assignment section, choose the **WLC Controlled** option for the Assignment Method option and choose 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 (CLI)

Step 1 To enable client access mode on the AP1522, 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 the **config 802.11–a58 enable** *Cisco_MAP* command 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 the **show config 802.11-a58 summary** command to display configuration details for a 5.8-GHz radio.

Configuring Power and Channel Settings

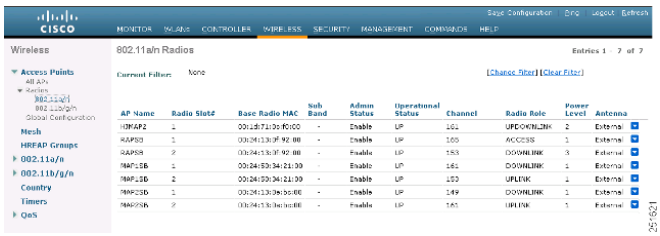
The backhaul channel (802.11a/n) can be configured on a RAP. MAPs tune to the RAP channel. The local access can be configured independently for MAP.

Configuring Power and Channel Settings (GUI)

Step 1 Choose **Wireless > Access Points > 802.11a/n**.

The Access Points > 802.11a/n Radios page appears.

Figure 10-27 Access Points > 802.11a/n Radios Page

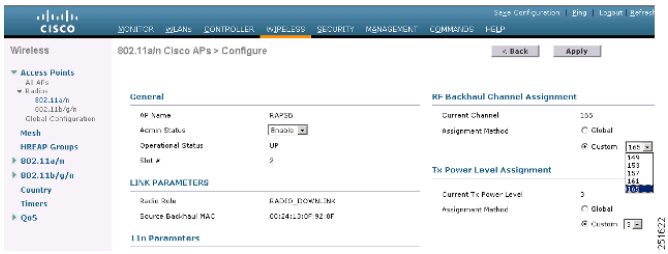


Note In Figure 10-27, radio slots are displayed for each radio. For an AP1524SB, the 802.11a radio will display for slots 1 and 2 that operate in the 5-GHz band. For an AP1524PS, the 802.11a radio will display for slots 1 and 2, operating in the 5-GHz and 4.9-GHz bands respectively.

Step 2 From the Antenna drop-down list for the 802.11a/n radio, choose **configure**. The Configure page appears.

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

Figure 10-28 802.11a/n Cisco APs > Configure Page



Step 3 Assign a channel (assignment methods of AP Controlled and WLC Controlled) for the radio.

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

Step 4 Assign Tx power levels (AP Controlled and WLC Controlled) for the radio.

There are five selectable power levels for the 802.11a backhaul for AP1500s.

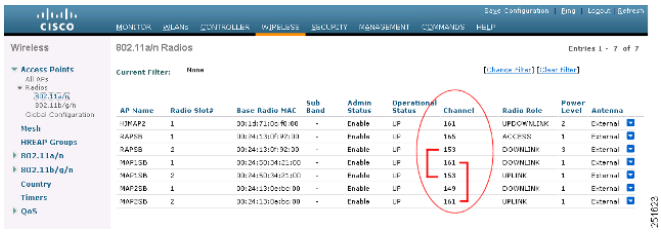
Note The default Tx power level on the backhaul is the highest power level (Level 1).

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 802.11a/n Radios page, verify that channel assignments were made correctly.

Figure 10-29 Channel Assignment



Configuring the Channels on the Serial Backhaul (CLI)

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

config slot 2 channel ap *Cisco_RAPSB channel*

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

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

config slot 2 txPower ap *Cisco_RAPSB power*

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

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

- **show mesh path** *MAP*

  Information similar to the following appears:

```
AP Name/Radio   Channel   Rate    Link-Snr     Flags        State
MAP1SB          161       auto    60           0x10ea9d54   UPDATED NEIGH PARENT BEACON
RAPSB           153       auto    51           0x10ea9d54   UPDATED NEIGH PARENT BEACON

RAPSB is a Root AP.
```

- **show mesh backhaul** *RAPSB*

  Information similar to the following appears:

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

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

Basic Attributes for Slot 2
    Radio Type.............................. RADIO_TYPE_80211a
    Radio Role.............................. RADIO_DOWNLINK
    Administrative State ................... ADMIN_ENABLED
    Operation State ........................ UP
    Current Tx Power Level ................. 3
    Current Channel ........................ 153
```

```
Antenna Type.............................. EXTERNAL_ANTENNA
External Antenna Gain (in .5 dBm units)...... 0
```

- **show ap channel** *MAP1SB*

  Information similar to the following appears:

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

Configuring 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.

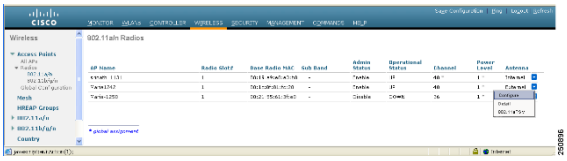
Configuring Antenna Gain (GUI)

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**.

Note Only external antennas have configurable gain settings.

Figure 10-30 802.11a/n Radios Page

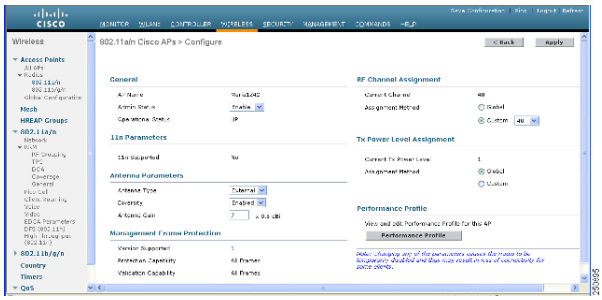


Step 3 In the Antenna Parameters section, enter the antenna gain.

The gain is entered in 0.5 dBm units. For example, 2.5 dBm = 5.

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

Figure 10-31 802.11 a/n Cisco APs > Configure Page



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

Configuring Antenna Gain (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

This feature is applicable to mesh APs with two 5-GHz radios, such as 1524SB (serial backhaul).

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 1524SB 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 1524SB 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 the serial backhaul RAP outside of the DCA list with the **config mesh backhaul dca-channels enable** command enabled. However, this is not case for the APs with one 5-GHz radio such as 1552, 1522, and 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 (GUI)

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 apply and save the backhaul channel deselection configuration changes.

Configuring Backhaul Channel Deselection (CLI)

Step 1 To review the channel list already configured in the DCA list, enter this command:

show advanced 802.11a channel

Information similar to the following appears:

```
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 this command:

  config 802.11a disable network

- To enable the 802.11a network, enter this 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 channel** 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 that you disable 802.11a network to enable or disable this feature.

Information similar to the following appears:

```
(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.

Information similar to the following appears:

```
(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 the 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.

Slot 2 of the 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

- 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 the following 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.
- For 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 (GUI)

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.

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

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

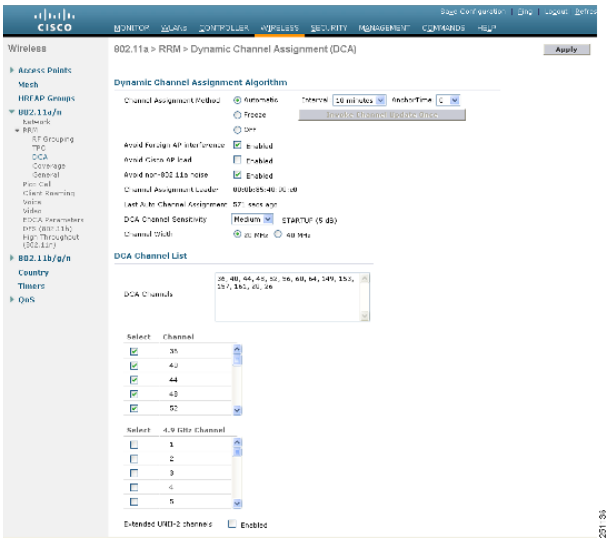
a. Choose **Wireless > 802.11a/n or 802.11b/g/n > Network** to open the 802.11a (or 802.11b/g) Global Parameters page.

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.

Figure 10-32 802.11a > RRM > Dynamic Channel Assignment (DCA) Page



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 access points 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 nonaccess 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 10-9.

Table 10-9 DCA Sensitivity Thresholds

Option	2.4-GHz DCA Sensitivity Threshold	5-GHz DCA Sensitivity Threshold
High	5 dB	5 dB
Medium	10 dB	15 dB
Low	20 dB	20 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 change the static RF channel assignment method to WLC Controlled 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 nonconfigurable 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 1500 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 AP1500s in your network, you must 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 reenable 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.

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.

Configuring Advanced Features

This section includes the following topics:

Using the 2.4-GHz Radio for Backhaul

Until the 7.0 release, mesh used the 5-GHz radio for backhaul, and the 2.4-GHz radio was used only for client access. The reasons for using only the 5-GHz radio for backhaul are as follows:

- More channels are available
- More EIRP is available
- Less interference occurs
- Most of the client access occurs over the 2.4-GHz band

However, under certain conditions, such as dense foliage areas, you might have needed to use the 2.4-GHz band for a backhaul because it has better penetration.

With the 7.0.116.0 release, you can configure an entire mesh network to use a single backhaul that can be either 5 GHz or 2.4 GHz.

Caution This feature is available only for AP1522 (two radios). This feature should be used only after exploring the 5-GHz backhaul option.

Caution We recommend that you use 5 GHz as the first option and use 2.4 GHz only if the 5-GHz option does not work.

Changing the Backhaul from 5 GHz to 2.4 GHz

When you specify only the RAP name as an argument to the command, the whole mesh sector changes to 2.4 GHz or 5 GHz backhaul. The warning messages indicate the change in backhaul, whether it is from 2.4 GHz to 5 GHz or vice versa.

Note The 2.4-GHz backhaul cannot be configured using the controller user interface, but only through the CLI.

Step 1 To change the backhaul, enter this command:

config mesh backhaul slot 0 enable *RAP*

A message similar to the following appears:

```
Warning! Changing backhaul slot will bring down the mesh for renegotiation!!!
After backhaul is changed, 5 GHz client access channels need to be changed manually

Are you sure you want to continue? (y/N)
```

Step 2 Press **y**.

Note When you change the 5-GHz backhaul to local client access, the 5-GHz client access frequencies on all the APs are the same, because the backhaul frequency is ported on these 5-GHz radios for client access. You need to configure these channels for a better frequency planning.

Changing the Backhaul from 2.4 GHz to 5 GHz

Step 1 To change the backhaul, enter the following command:

config mesh backhaul slot 1 enable *RAP*

A message similar to the following appears:

```
Warning! Changing backhaul slot will bring down the mesh for renegotiation!!!
Are you sure you want to continue? (y/N)
```

Step 2 Press **y**.

Note You cannot configure the 2.4-GHz backhaul using the controller GUI, but you can configure the 2.4-GHz backhaul using the CLI.

Verifying the Current Backhaul in Use

To verify the current backhaul in use, enter the command:

show mesh backhaul *AP_name*

Note For a 5-GHz backhaul, dynamic frequency selection (DFS) occurs only on 5 GHz and not on 2.4 GHz. The mechanism, which differs for RAP and MAP, is called a coordinated change mechanism.

When 5 GHz is converted to client access from the backhaul or 2.4 GHz is being used as backhaul, DFS works similar to how it works for a local mode AP. DFS is detected on a 5-GHz client access, and the request is sent to the controller for a new channel. Mesh adjacency is not affected for the 2.4-GHz backhaul.

Note Universal client access is available on the 2.4-GHz backhaul.

Universal Client Access

When Universal Client Access is enabled, it allows wireless client association over the backhaul radio. Generally, backhaul radio is a 5-GHz radio for most of the mesh access points except for 1522 where backhaul can be 2.4 GHz. This means that a backhaul radio can carry both backhaul traffic and client traffic.

When Universal Client Access is disabled, only backhaul traffic is sent over the backhaul radio and client association is only over the second radio(s).

Note Universal Client Access is disabled by default.

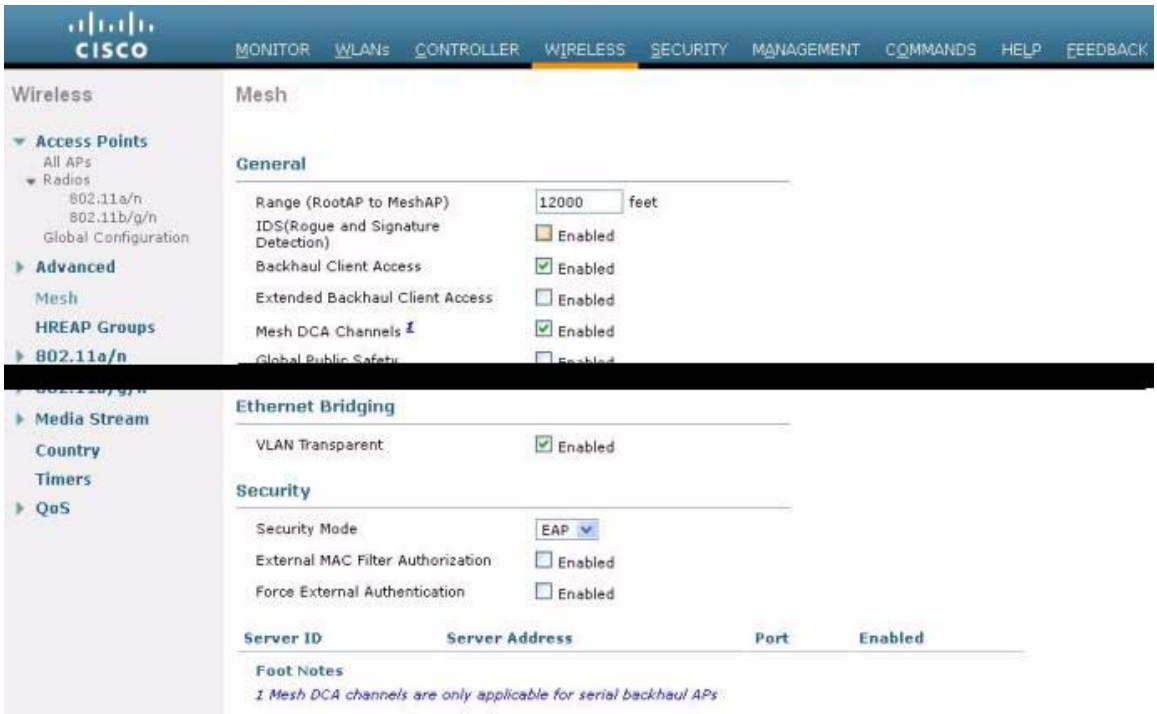
After this feature is enabled, all mesh access points reboot.

This feature is applicable to mesh access points with two or more radios (1552, 1524SB, 1522, Indoor APs in mesh mode) excluding the 1524PS.

Configuring Universal Client Access (GUI)

You will be prompted that the AP will reboot if you enable Universal Client Access.

Figure 10-33 Configuring Universal Client Access Using the GUI



Configuring Universal Client Access (CLI)

Use the following command to enable Universal Client Access:

```
config mesh client-access enable
```

A message similar to the following appears:

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

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 applicable to mesh access points with two or more radios (1552, 1524SB, 1522, Indoor APs in mesh mode) excluding the 1524PS.

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:

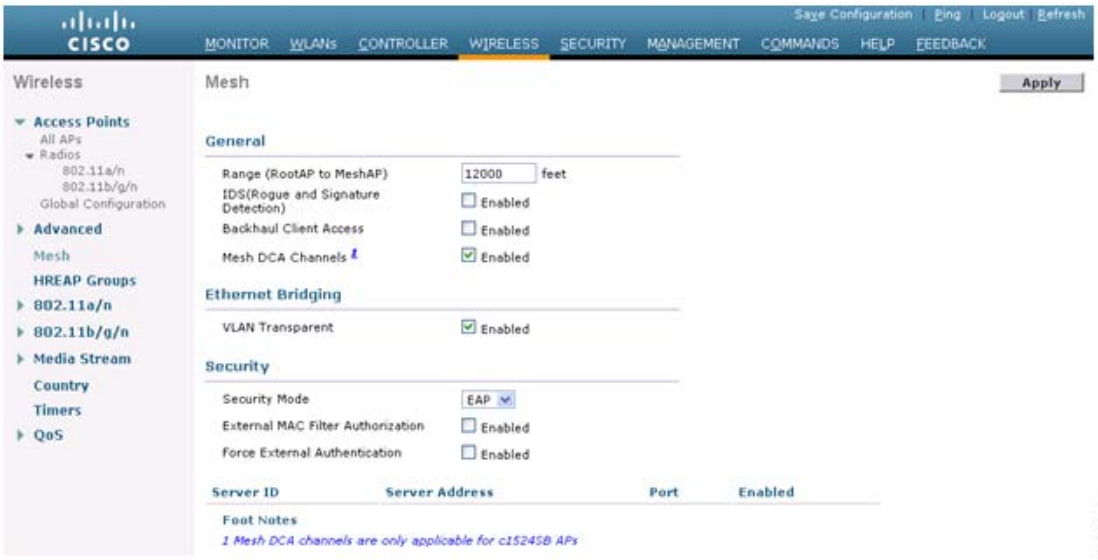
- Configuring Extended Universal Access (GUI), page 10-67
- Configuring Extended Universal Access (CLI), page 10-70
- Configuring Extended Universal Access from the Wireless Control System (WCS), page 10-71

Configuring Extended Universal Access (GUI)

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

The Controller GUI when Backhaul Client Access is disabled page appears.

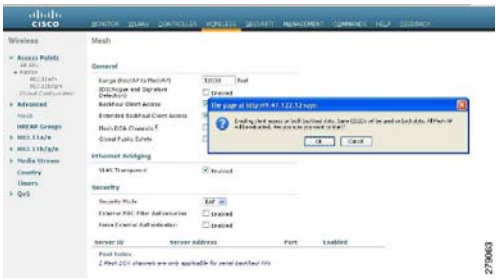
Figure 10-34 Advanced Controller Settings for Mesh Page



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**.

Figure 10-35 Advanced Controller Settings for Mesh Page

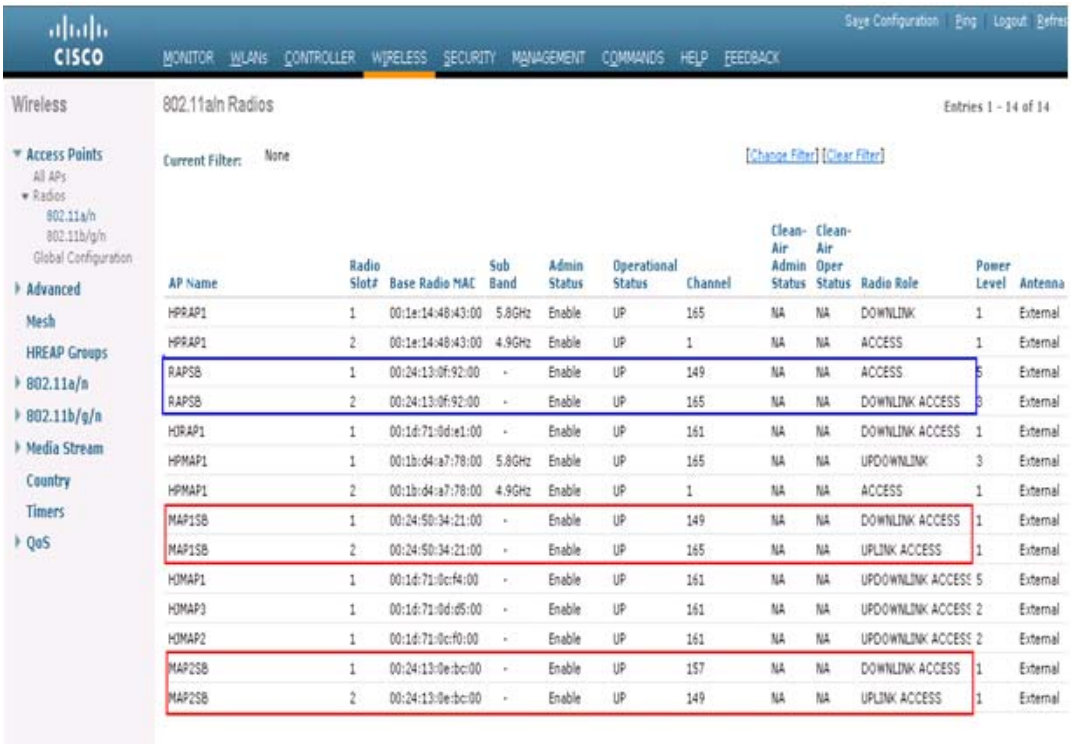


Step 4 Click **OK**.

Post-Configuration

After EUA is enabled, 802.11a radios are displayed.

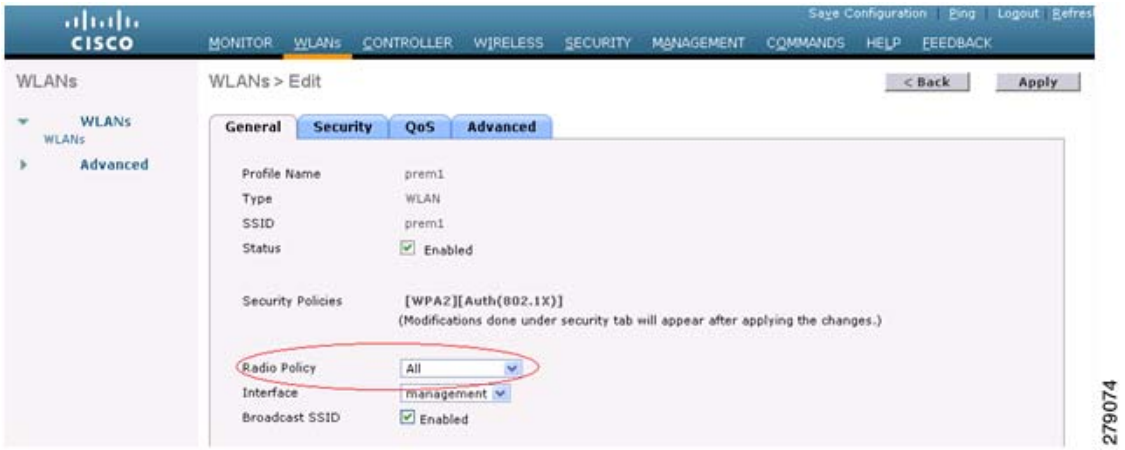
Figure 10-36 802.11a Radios after EUA is Enabled



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, choose only the appropriate radio policy from the list.

Figure 10-37 Radio Policy Selection



Configuring Extended Universal Access (CLI)

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

  A message similar to the following appears:

  ```
  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.

  A message similar to the following appears:

  ```
  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 this command:

  config mesh client-access disable

  A message similar to the following appears:

  ```
  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 this command:

  config mesh client-access enable

  A message similar to the following appears:

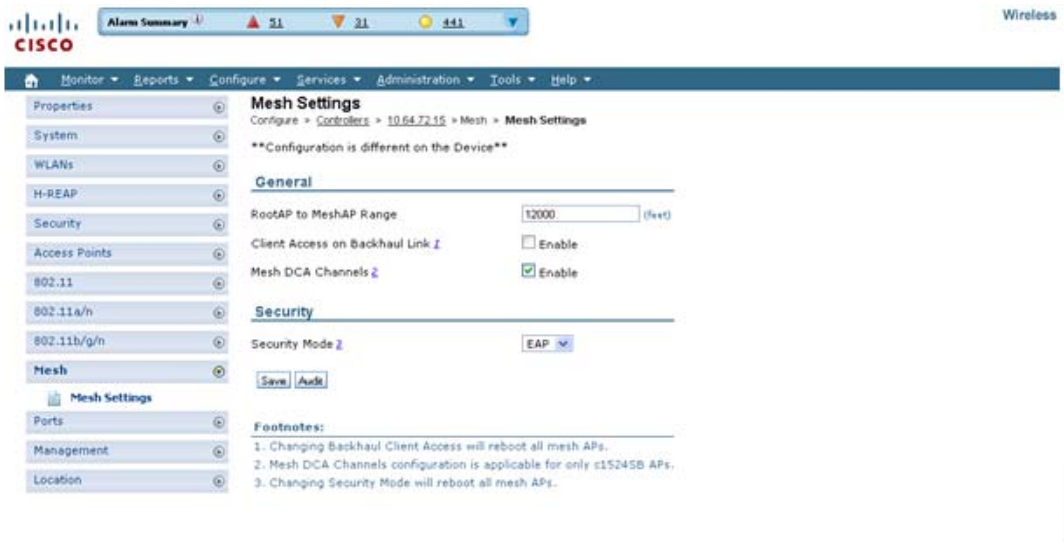
  ```
  All Mesh APs will be rebooted
  Are you sure you want to start? (y/N)
  ```

Configuring Extended Universal Access from the Wireless Control System (WCS)

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

The WCS Mesh page when Backhaul Client Access is disabled.

Figure 10-38 Mesh Settings Page



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.

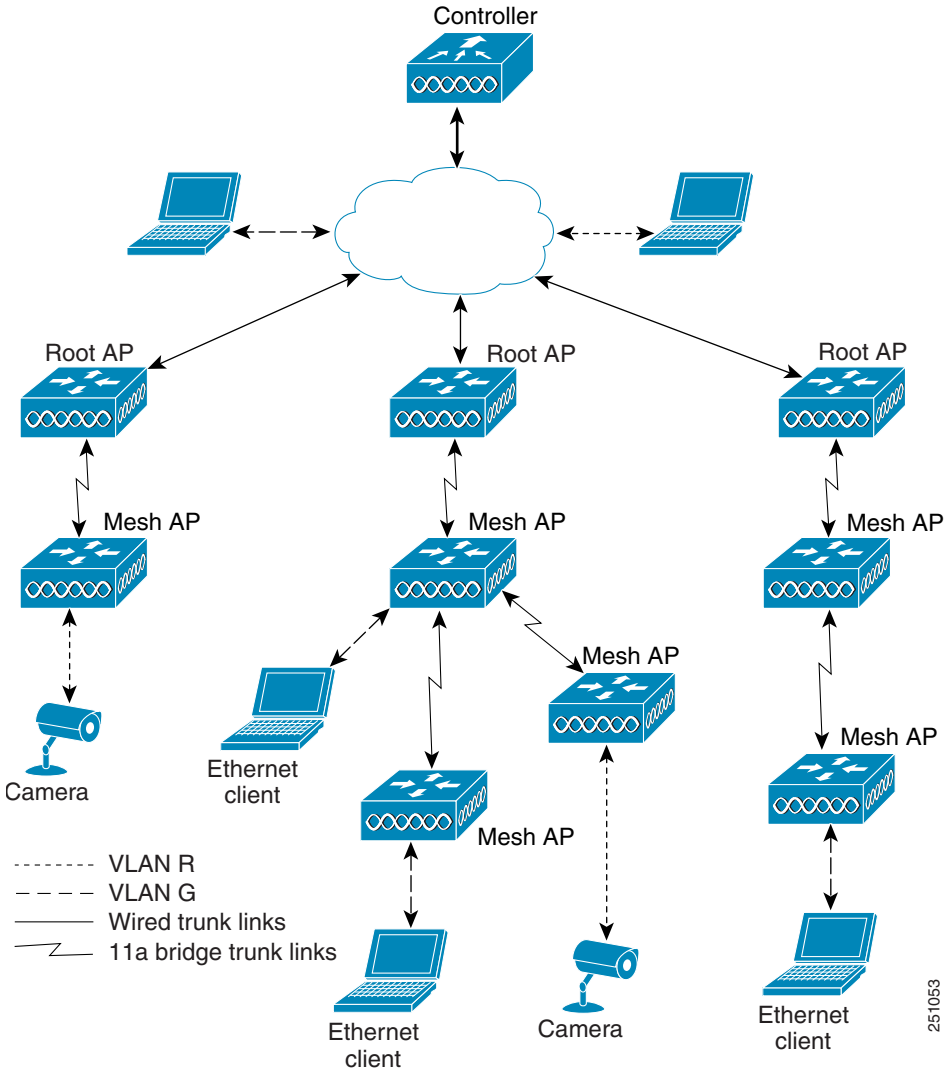
Step 4 Click **OK** to continue.

Configuring 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.

Figure 10-39 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, which is a global parameter, see the "Configuring Global Mesh Parameters" section on page 10-31.

- 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-VLANs.

  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 that reside on separate buildings within a campus.

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

Note In the controller releases prior to 7.2, the Root Access Point (RAP) native VLAN is forwarded out of Mesh Access Point (MAP) Ethernet ports with Mesh Ethernet Bridging and VLAN Transparent enabled.

In the 7.2 and later controller releases, the Root Access Point (RAP) native VLAN is not forwarded out of Mesh Access Point (MAP) Ethernet ports with Mesh Ethernet Bridging and VLAN Transparent enabled.

This change in behavior increases reliability and minimizes the possibility of forwarding loops on Mesh Backhauls.

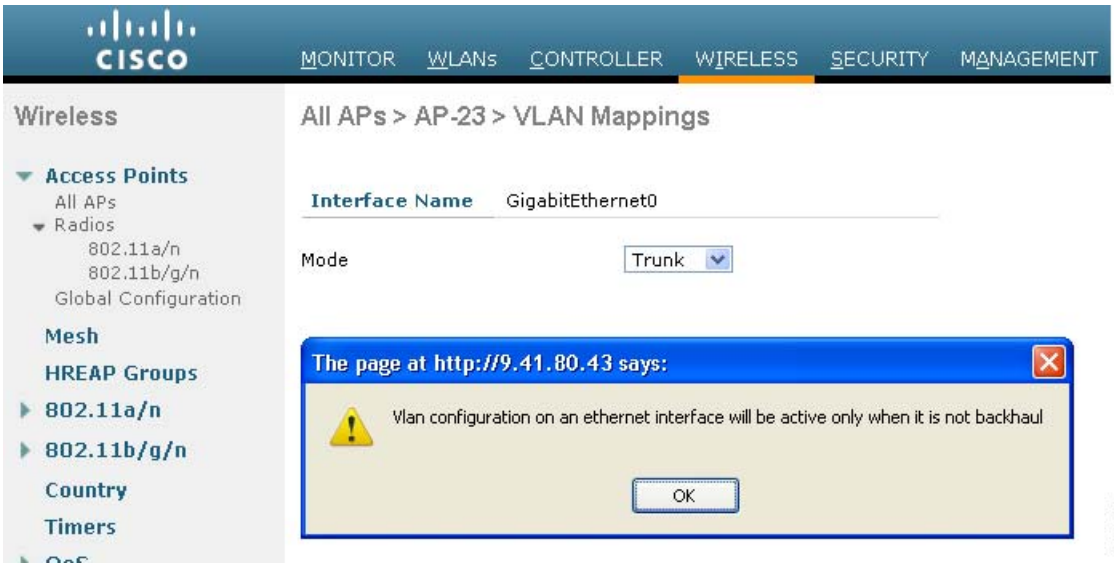
Ethernet VLAN Tagging Guidelines

- 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 (CLI)" section on page 10-36. 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.

Figure 10-40 Wireless > Mesh Page

- VLAN tagging can only be configured on Ethernet interfaces as follows:
  - On AP1500s, 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, 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 a backhaul.

Figure 10-41 Warning Message Displays for Backhaul Configuration Attempts



- No configuration is required to support VLAN tagging on any 802.11a backhaul Ethernet interface within the mesh network as follows:
  - This includes the RAP uplink Ethernet port. The required configuration occurs 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 AP1500s (wherever applicable). VLANs can be configured on ports 0 (PoE-in), 1 (PoE-out), and 3 (fiber).
- Up to 16 VLANs are supported on each sector. 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 a mesh access point is in the CAPWAP RUN state and VLAN-Transparent mode is disabled.
- Whenever there roaming or a 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 a 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.

VLAN registration is 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 subinterface 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 that requested the VLAN is reached.
5. Upon receiving 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.

Enabling Ethernet VLAN Tagging (GUI)

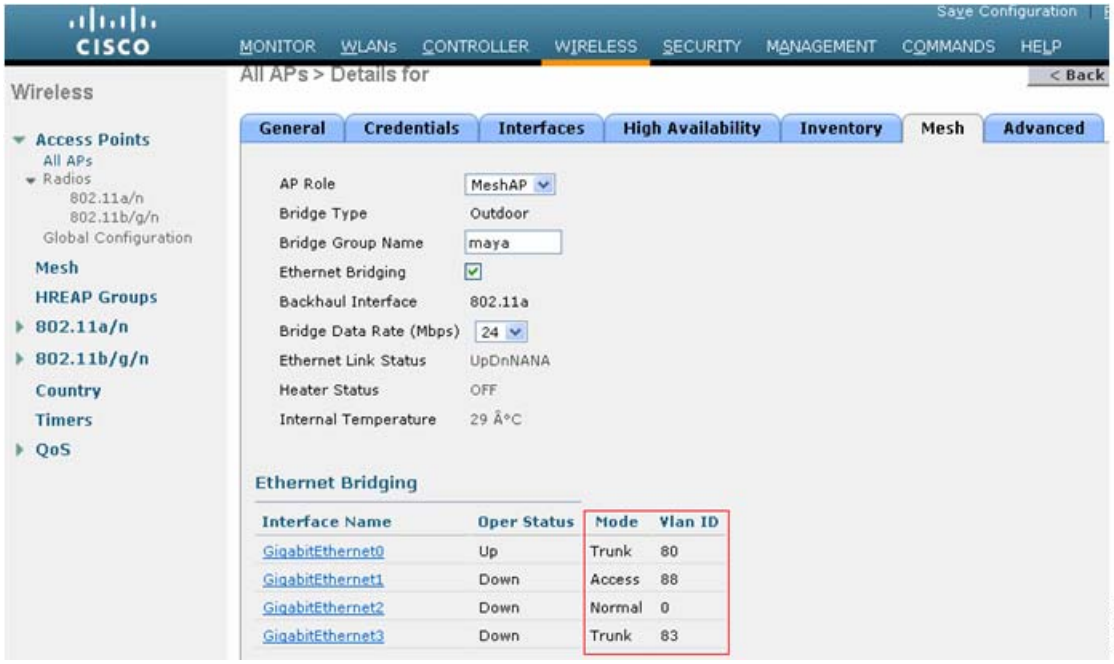
You must enable Ethernet bridging before you can configure VLAN tagging. See the "Configuring Ethernet Bridging" procedure on page 10-43.

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.

Figure 10-42 All APs > Details for (Mesh) Page



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. Choose **access** from the mode drop-down list.
  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 10-43 VLAN Access Mode

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

a. From the mode drop-down list, choose **trunk** . (See Figure 10-44.)

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:

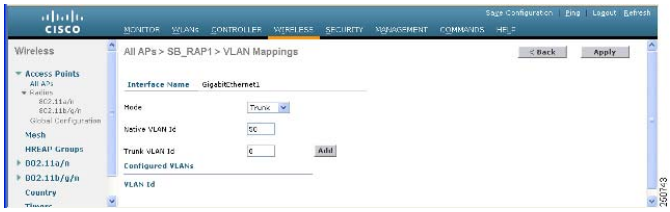
If forwarding *untagged* packets, do not change the default trunk VLAN ID value of zero. (MAP-to-MAP bridging, campus environment)

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 10-44 All APs > AP > VLAN Mappings Page



Step 5 Click **Apply**.

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

Configuring Ethernet VLAN Tagging (CLI)

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

config ap ethernet 1 mode access enable *AP1500-MAP 50*

where *AP1500-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 *AP1500-MAP 60*

where *AP1500-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 *AP1500-MAP3 65*

where *AP1500-MAP 3* is the variable *AP_name* and *65* is the variable *VLAN ID*

Viewing Ethernet VLAN Tagging Configuration Details (CLI)

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 these 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
```

205741

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

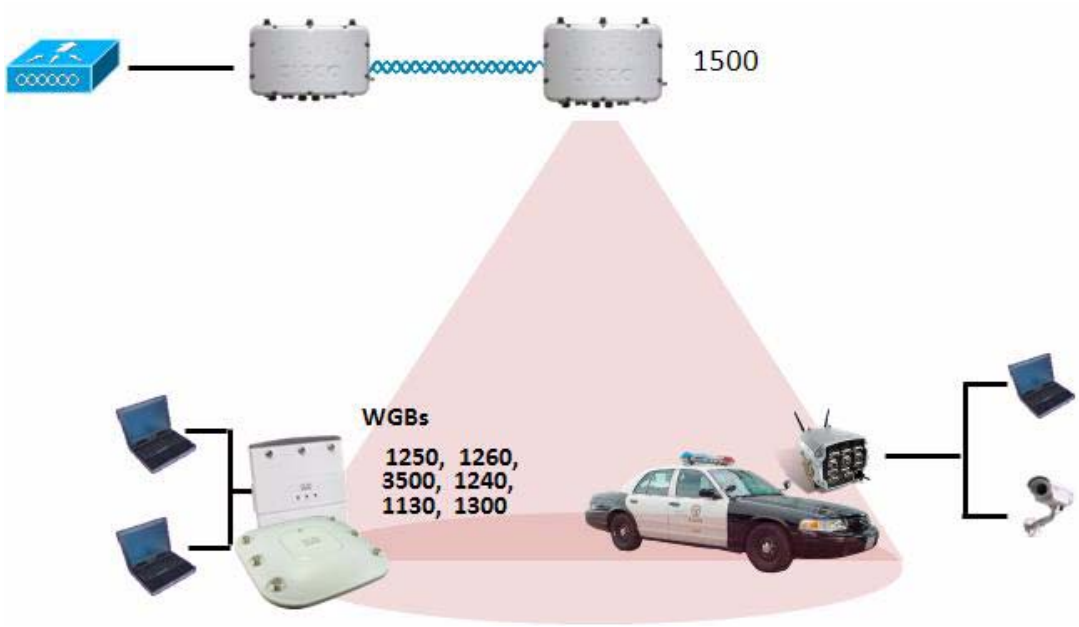
Workgroup Bridge Interoperability with Mesh Infrastructure

A workgroup bridge (WGB) is a small standalone 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, which means that wired clients get access to the wireless network.

A WGB is used to connect wired networks over a single wireless segment 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 headers, 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.

Figure 10-45 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, a wireless client on the second radio of the WGB is 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 a 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:

- FlexConnect
- 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 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 headers, 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, AP 1140, AP1240, AP1310, and the Cisco 3200 Mobile Router (hereafter referred to as Cisco 3200) which are configured as WGBs 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 7.0.116.0* 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 supported WGB modes and capacities are as follows:

- The autonomous access points configured as WGBs must be running Cisco IOS release 12.4.25d-JA or later.

  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 AP1524SB.

- 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 a 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.
- Non-Cisco workgroup bridges are supported on Mesh access points.
- A WGB 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 10-46 displays WPA security settings for WGB (controller GUI).
  - Figure 10-47 displays WPA-2 security settings for WGB (controller GUI).

Figure 10-46 WPA Security Settings for a WGB

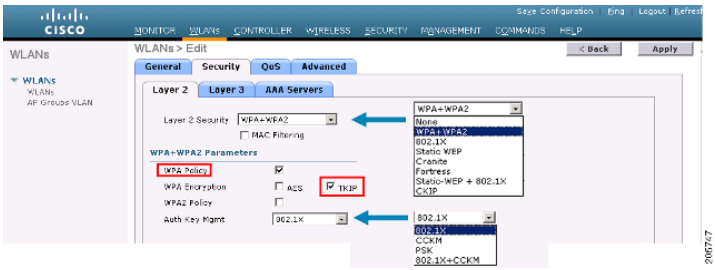
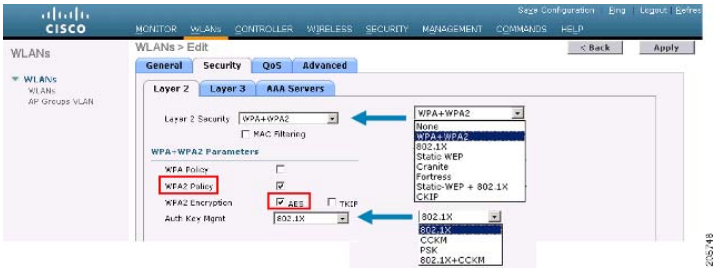


Figure 10-47 WPA-2 Security Settings for a WGB



To view the status of a WGB client, follow these steps:

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

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 a WGB (far right).

Figure 10-48 Clients are Identified as a WGB

Step 4 Click on the MAC address of the client to view configuration details:

- For a wireless client, the page seen in Figure 10-49 appears.
- For a wired client, the page seen in Figure 10-50 appears.

Figure 10-49 Monitor > Clients > Detail Page (Wireless WGB Client)

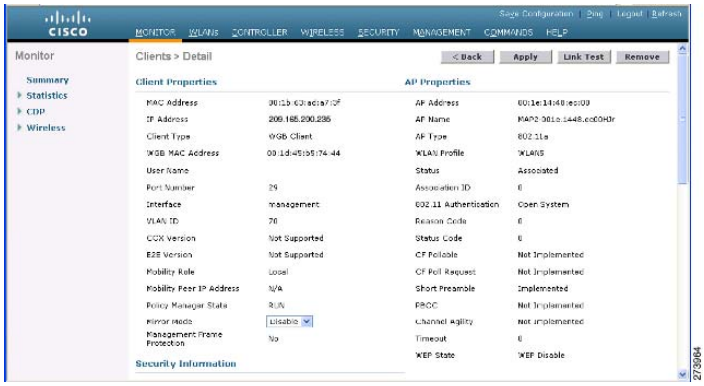


Figure 10-50 Monitor > Clients > Detail Page (Wired WGB Client)

Guidelines and Limitations

- 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 nonmesh 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 a 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 an autonomous AP.
- Multiple VLANs for wireless clients associated to a WGB are not supported.
- Up to 16 multiple VLANs are supported for wired clients behind a WGB from the 7.0 release and later releases.
- Roaming is supported for wireless and wired clients behind a 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.
- Non-Cisco workgroup bridges are supported on Mesh access points.

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 a WGB.

Example—Configuration of a Workgroup Bridge

When you configure from the CLI, the following are mandatory:

- dot11 SSID (security for a WLAN can be decided based on the requirement).
- Map the subinterfaces in both the radios to a single bridge group.

Note A native VLAN is always mapped to bridge group 1 by default. For other VLANs, the bridge group number matches the VLAN number; for example, for VLAN 46, the bridge group is 46.

- Map the SSID to the radio interfaces and define the role of the radio interfaces.

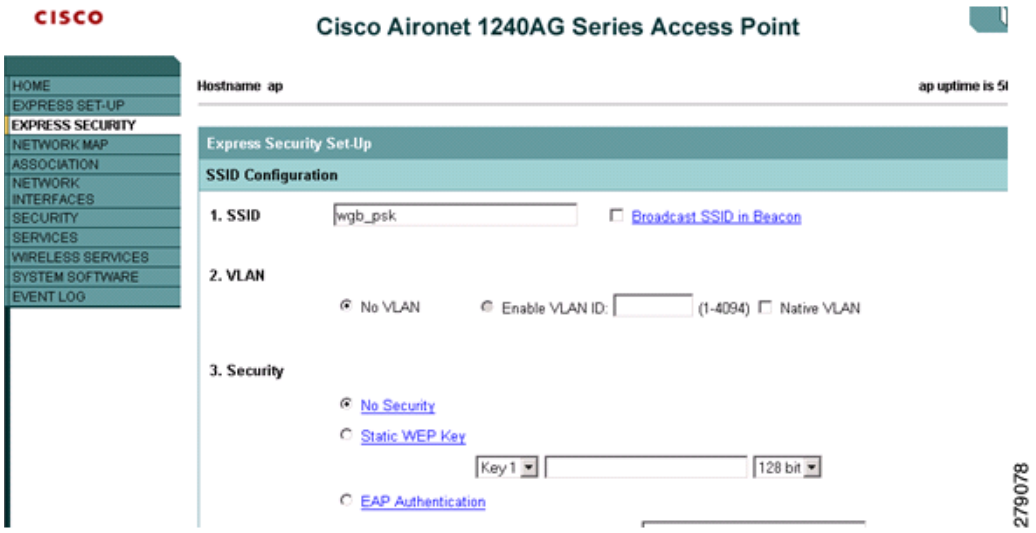
In the following example, one SSID (WGBTEST) is used in both radios, and the SSID is the infrastructure SSID mapped to NATIVE VLAN 51. All radio interfaces are mapped to bridge group -1.

```
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. From the GUI, subinterfaces are automatically created after the VLAN is defined.

Figure 10-51 SSID Configuration Page



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.

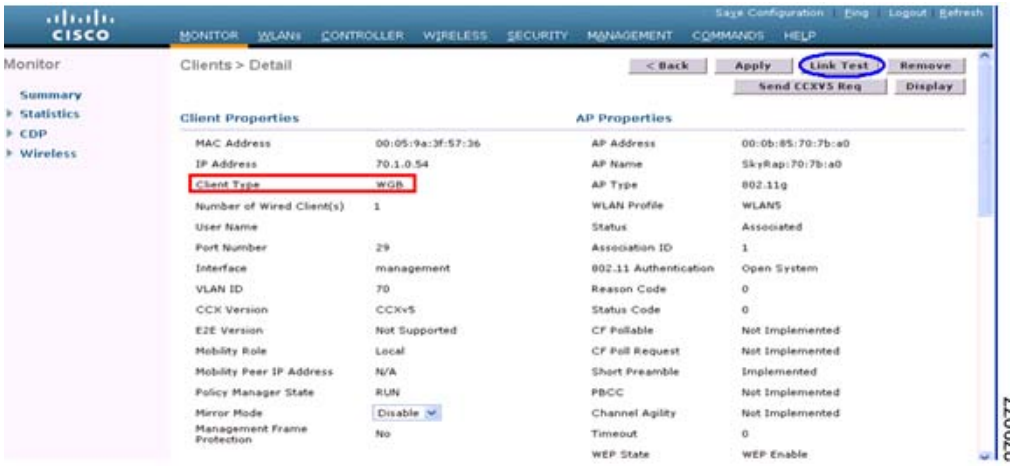
```
WGB# show dot11 associations client

802.11 Client Stations on Dot11Radio1:

SSID [WGBTEST] :

MAC Address          IP Address       Device          Name            Parent          State
0024.130f.920e       209.165.200.225  LWAPP-Parent    RAPSB             -             Assoc
```

From the controller, choose **Monitor > Clients**. The WGB and the wireless/wired client behind the WGB are updated and the wireless/wired client are shown as the WGB client, as shown in Figure 10-52, Figure 10-53, and Figure 10-54.

Figure 10-52 Updated WGB Clients

Figure 10-53 Updated WGB Clients

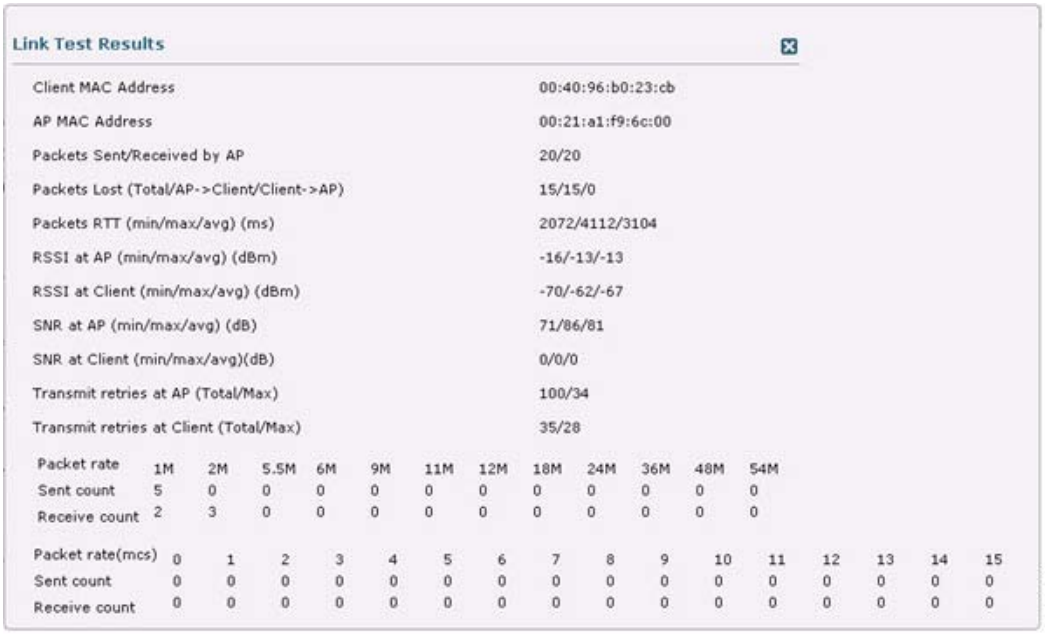
Figure 10-54 Updated WGB Clients



Link Test Result

Figure 10-55 shows the link test results.

Figure 10-55 Link Test Results



A link test can also be run from the controller CLI using this command:

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 to know the summary of WGBs and clients associated associated with a Cisco lightweight access point:

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
```

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
```

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 miles per hour 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—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—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—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

- 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 the **mobile station period 3 threshold 50** command to configure the workgroup bridge as a mobile station.

  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 is 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 only those required channels; the mobile WGB achieves and maintains a continuous wireless LAN connection with fast and smooth roaming. This limited channel set is configured using the 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

This 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.

Table 10-10 identifies mesh access points and their respective frequency bands that support WGB.

Table 10-10 WGB Interoperability Chart

RAP/MAP	WGB								
	MAR3200			802.11n Indoor APs		1130/1240		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
1552/1552	No	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes
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

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 the 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 (this command will remove all wired and wireless clients associated in a 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 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), which 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 multimedia 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)

AP1500s, with Cisco controllers, provide a minimal integrated services capability at the controller, in which client streams have maximum bandwidth limits, and a more robust differentiated services (diffServ) capability based on the IP DSCP values and QoS WLAN overrides.

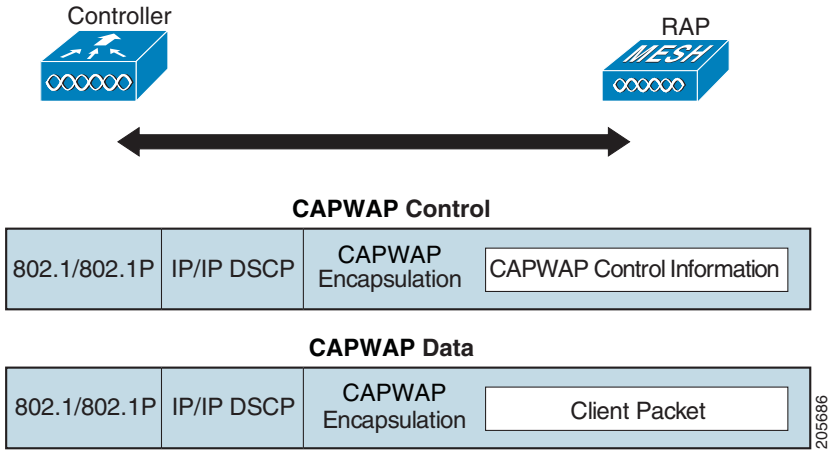
When the queue capacity has been reached, additional frames are dropped (tail drop).

Encapsulations

Several encapsulations are used by the mesh system. These encapsulations 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 (noncontroller 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 is 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.

Figure 10-56 Encapsulations

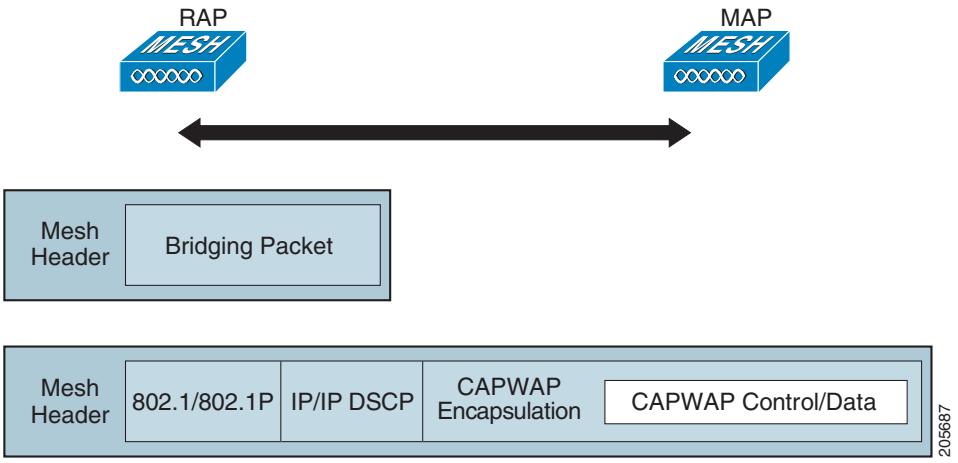


For the backhaul, there is only one type of encapsulation, encapsulating MESH traffic. However, two types of traffic are encapsulated: bridging traffic and CAPWAP control and data traffic. Both types of traffic are encapsulated in a proprietary mesh header.

In the case of bridging traffic, the entire packet Ethernet frame is encapsulated in the mesh header (see Figure 10-57).

All backhaul frames are treated identically, regardless of whether they are MAP to MAP, RAP to MAP, or MAP to RAP.

Figure 10-57 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 frames 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.

AP1500s 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.

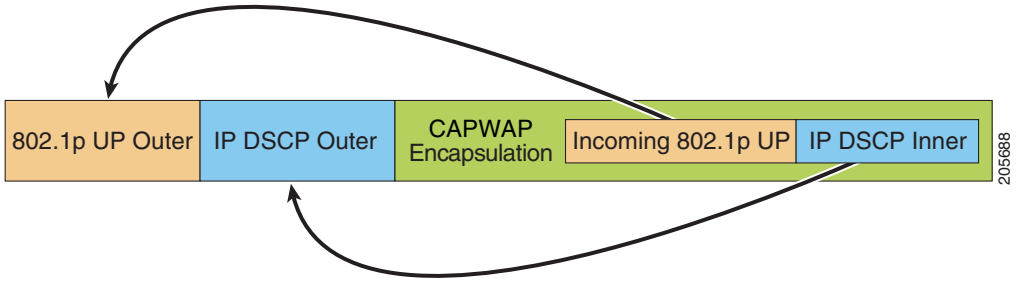
The backhaul (frames destined for another outdoor mesh access point) uses four FIFOs, although user traffic is limited to gold, silver, and bronze. The platinum queue is used exclusively for CAPWAP control traffic and voice, and has been reworked from the standard 802.11e parameters for CWmin, CWmax, and so on, to provide more robust transmission but higher latencies.

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 that is more conducive to video applications.

Frames that are 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.

Figure 10-58 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 10-11).

Table 10-11 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 a 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 10-12).

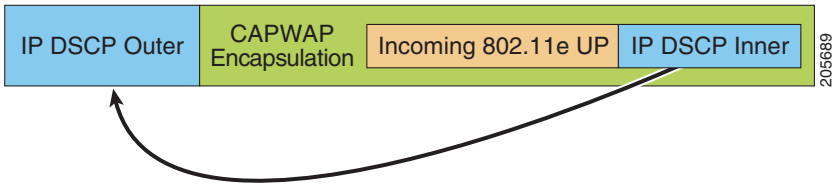
Table 10-12 MAP to Client Path QoS

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 10-59).

Figure 10-59 MAP to RAP Path



The minimum value of the incoming 802.11e user priority and the WLAN override priority is translated using the information listed in Table 10-13 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 the silver priority, the minimum priority of silver is used to determine the DSCP value.

Table 10-13 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

If there is no incoming WMM priority, the default WLAN priority is used to generate the DSCP value in the outer header. If 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. 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, the LAN must be properly secured in bridging mode. 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 AP1500 and 802.11a is by tagging Ethernet packets with DSCP. AP1500s take the Ethernet packet with DSCP and places it in the appropriate 802.11e queue.

AP1500s do not tag DSCP itself:

- On the ingress port, the AP1500 sees a DSCP tag, encapsulates the Ethernet frame, and applies the corresponding 802.11e priority.
- On the egress port, the AP1500 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 supported only on indoor mesh networks in release 5.2, 6.0, 7.0, and 7.0.116.0. For outdoors, voice is supported on a best-effort basis on a mesh infrastructure.
- 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 are as follows:
  - Coverage hole of 2 to 10 percent
  - Cell coverage overlap of 15 to 20 percent
  - Voice needs RSSI and SNR values that are at least 15 dB higher than data requirements
  - RSSI of -67 dBm for all data rates should be the goal for 11b/g/n and 11a/n
  - SNR should be 25 dB for the data rate used by client to connect to the AP
  - Packet error rate (PER) should be configured for a value of one percent or less
  - Channel with the lowest utilization (CU) must be used
- On the 802.11a/n (or 802.11b/g/n) > *Global* parameters page, you should do the following:
  - Enable dynamic target power control (DTPC).
  - Disable all data rates less than 11 Mbps.
- On the 802.11a/n or 802.11b/g/n > *Voice* parameters page, you should do the following:
  - 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 percent.
  - Set the reserved roaming bandwidth to 6 percent.
  - Enable traffic stream metrics.
- On the 802.11a/n or 802.11b/g/n > *EDCA* parameters page, you should do the following:
  - Set the EDCA profile for the interface as voice optimized.
  - Disable low latency MAC.
- On the QoS > *Profile* page, you should do the following:
  - Create a voice profile and select 802.1Q as the wired QoS protocol type.
- On the WLANs > *Edit* > QoS page, you should do the following:
  - 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, you should do the following:
  - Select CCKM for authorization (*auth*) key management (*mgmt*) if you want to support fast roaming. See the "Client Roaming" section on page 10-90.
- On the x > y page, you should do the following:
  - Disable voice active detection (VAD).

Voice Call Support in a Mesh Network

Table 10-14 shows the actual calls in a clean, ideal environment.

Table 10-14 Calls Possible with 1520 Series in 802.11a and 802.11b/g Radios[1]

No. of Calls	802.11a Radio	802.11b/g 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.

Table 10-15 shows the actual calls in a clean, ideal environment.

Table 10-15 Calls Possible with 1550 Series in 802.11a/n 802.11b/g/n Radios[1]

No. of Calls	802.11a/n Radio 20 MHz	802.11a/n Radio 40 MHz	802.11b/g/n Backhaul Radio 20 MHz	802.11b/g/n Backhaul Radio 40 MHz
RAP	20	35	20	20
MAP1 (First Hop)	10	20	15	20
MAP2 (Second Hop)	8	15	10	15

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 10-16). A MOS score between 3.5 and 4 is acceptable.

Table 10-16 MOS Ratings

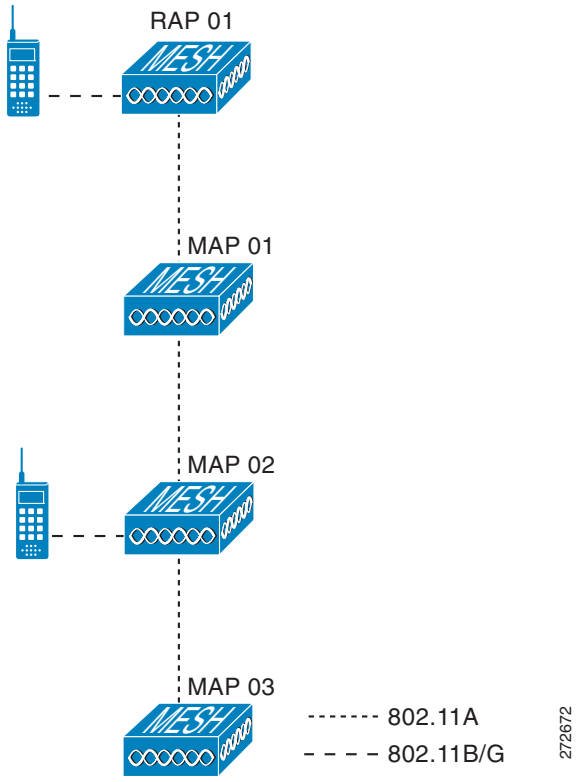
MOS rating	User satisfaction
> 4.3	Very satisfied
4.0	Satisfied
3.6	Some users dissatisfied
3.1	Many users dissatisfied
< 2.58	—

Viewing the Voice Details for Mesh Networks (CLI)

Use the commands in this section to view details on voice and video calls on the mesh network:

Note See Figure 10-60 when using the CLI commands and viewing their output.

Figure 10-60 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 as follows:

- 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** command).

Enabling Multicast on a Mesh Network (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 this command:

configure network multicast igmp snooping enable

A client sends an IGMP *join* that 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 this 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.

For more information about video, see the following:

- Video Surveillance over Mesh Deployment Guide: http://www.cisco.com/en/US/tech/tk722/tk809/technologies_tech_note09186a0080b02511.shtml
- Cisco Unified Wireless Network Solution: VideoStream Deployment Guide: http://www.cisco.com/en/US/products/ps10315/products_tech_note09186a0080b6e11e.shtml

Locally Significant Certificates for Mesh APs

Until the 7.0 release, mesh APs supported only the Manufactured Installed Certificate (MIC) to authenticate and get authenticated by controllers to join the controller. You might have had 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 start using these LSCs, to join, authenticate, and derive a session key. Cisco supported normal APs from the 5.2 release and later releases and extended the support for mesh APs as well from the 7.0 release.

With the 7.0.116.0 release, the following functionality has been added:

- Graceful fallback to MIC if APs are unable to join the controller with LSC certificates—Local APs try to join a controller with an LSC for the number of times that are configured on the controller (the default value is 3). After these trials, the AP deletes the LSC and tries to join a controller with an MIC.

  Mesh APs try to join a controller with an LSC until its lonely timer expires and the AP reboots. The lonely timer is set for 40 minutes. After the reboot, the AP tries to join a controller with an MIC. If the AP is again not able to join a controller with an MIC in 40 minutes, the AP reboots and then tries to join a controller with an LSC.

Note An LSC in mesh APs is not deleted. An LSC is deleted in mesh APs only when the LSC is disabled on the controller, which causes the APs to reboot.

- Over the air provisioning of MAPs.

Guidelines and Limitations

- 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 a fallback if they cannot be joined with an LSC.
- Provisioning an 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 can happen over Ethernet and over-the-air in case of MAPs. You must connect the mesh RAP to the controller through Ethernet and get the LSC certificate provisioned. After the RAP gets the LSC certificate, MAPs connected to this RAP are provisioned with LSC certificates over the air. After the LSC becomes the default, an 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 a JOIN irrespective of the AP mode. Mesh APs also use the certificate for mesh security, which 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 profile 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 An 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 an LSC (CLI)

Step 1 Enable LSC and provision the LSC CA certificate in the controller.

Step 2 Enter this command:

config local-auth eap-profile cert-issuer vendor *prfMaP1500LlEAuth93*

Step 3 Turn on the feature by entering this 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 10-61 and Figure 10-62.

Figure 10-61 Local Significant Certificate

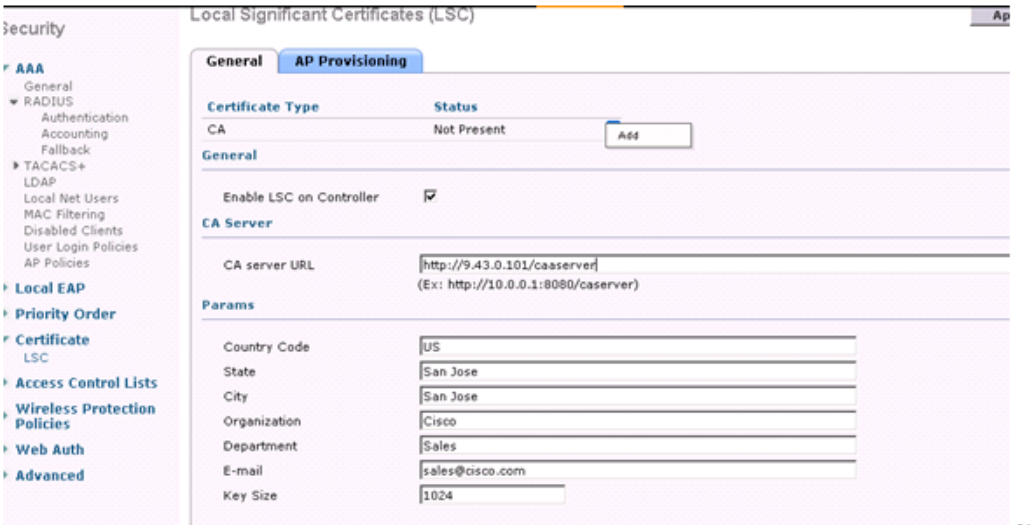


Figure 10-62 AP Policy Configuration

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 as follows:

  - **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 keyword 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 the 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 the disabled state, and in the disabled state, the APs are not allowed to join the WLC using the LSC.

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

  After getting the MIC, an AP tries to join the 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 the enabled state. If an AP cannot join because of the enabled state, this log message in the WLC side is displayed: LSC/MIC AP is not allowed to join by config.

Controller CLI show Commands

The following are the WLC **show** commands:

- **show certificate lsc summary**

  This command displays the LSC certificates installed on the WLC. It would be the CA certificate, device certificate, and optionally, an RA certificate if the RA certificate has also been installed. It also indicates if an LSC is enabled or not.

- **show certificate lsc ap-provision**

  This command displays the status of the provisioning of the AP, whether it is enabled or disabled, and whether a provision list is present or not.

- **show certificate lsc ap-provision details**

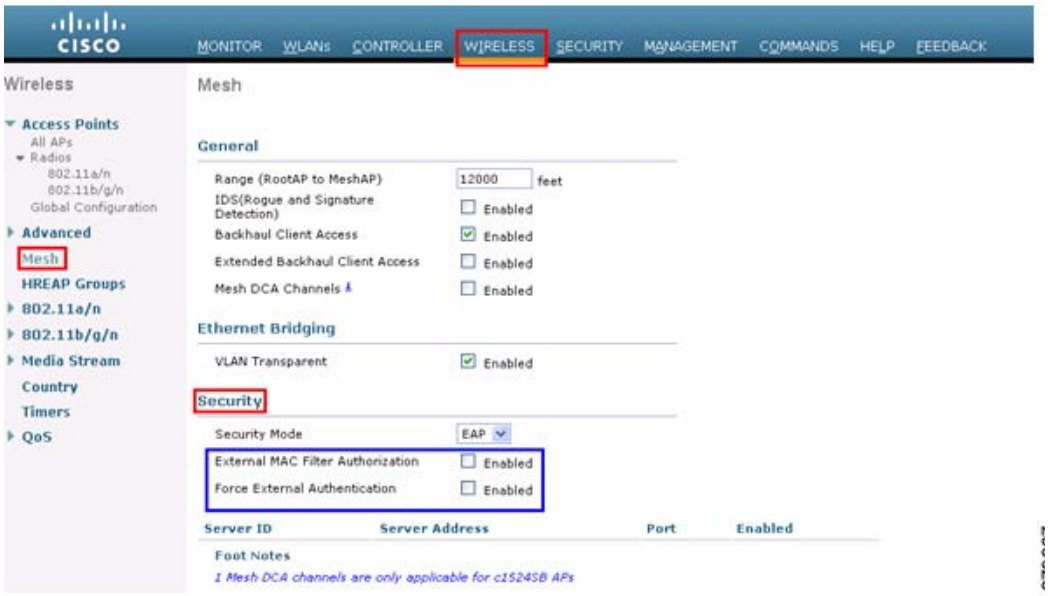
  This command displays the list of MAC addresses present in the AP provisioning lists.

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 an LSC.

Figure 10-63 shows three possible cases for mesh AP MAC authorization and EAP.

Figure 10-63 Possible Cases for Mesh AP MAC Authorization and EAP



- Case 1—Local MAC Authorization and Local EAP Authentication

  Add the MAC address of RAP/MAP to the controller MAC filter list.

  Example:

  ```
  config macfilter mac-delimiter colon
  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:

  ```
  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:

  ```
  config mesh radius-server index enable
  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

- 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 fall back to a backup controller.
- The **config mesh lsc** {**enable** | **disable**} command is required to enable or disable an LSC for mesh APs. This command causes all the mesh APs to reboot. Currently, disabling this command may also reboot nonmesh APs.

Slot Bias Options

This section contains the following topics:

Information About Slot Bias Options

When a 1524SB AP is switched on, either slot 1 or slot 2 can be used for an uplink depending on the strength of the signal. AWPP treats both slots equally. For a MAP, slot 2 is the preferred (biased) uplink slot, that is, the slot that is used to connect to the parent AP. Slot 1 is the preferred downlink slot. When both radio slots are available for use and if slot 1 is used for an uplink backhaul, a 15-minute timer is started. At the end of 15 minutes, the AP scans for a channel in slot 2 so that slot 2 might be used for an uplink backhaul again. This process is called slot bias.

We recommend that you use a directional antenna on slot 2 for a proper linear functionality. We also recommend that you ensure that slot 2 is selected for a strong uplink. However, there may be some scenarios where directional antennas are used on both the backhaul radios for mobility. When the AP is powered on, the parent can be selected in either direction. If slot 1 is selected, the AP should not go to the scanning mode after 15 minutes, that is, you should disable the slot bias.

Disabling Slot Bias

You can use the **config mesh slot-bias disable** to disable slot bias so that the APs can be stable on slot 1.

To disable slot bias, enter this command:

```
config mesh slot-bias disable
```

Note The slot bias is enabled by default.

Guidelines and Limitations

- The **config mesh slot-bias disable** command is a global command and is applicable to all 1524SB APs associated with the same controller.
- Slot bias is applicable only when both slot 1 and slot 2 are usable. If a slot radio does not have a channel that is available because of dynamic frequency selection (DFS), the other slot takes up both the uplink and downlink roles.
- If slot 2 is not available because of hardware issues, slot bias functions normally. Take corrective action by disabling the slot bias or fixing the antenna.
- A 15-minute timer is initiated (slot bias) only when slot 1 and slot 2 are usable (have channels to operate).
- The 15-minute timer is not initiated if slot 2 cannot find any channels because of DFS, which results in slot 1 taking over the uplink and the downlink.
- Slot 2 takes over slot 1 if slot 1 does not have any channels to operate because of DFS.
- If slot 2 has a hardware failure, then slot bias is initiated, and slot 1 is selected for uplinking.
- Disabling slot bias enables you to take preventive action for a smooth operation.

Commands Related to Slot Bias

- To see which slot is being used for an uplink or a downlink, enter this command:

```
show mesh config

Mesh Range..................................... 12000
Mesh Statistics update period.................. 3 minutes
Backhaul with client access status............. enabled
Backhaul with extended client access status..... disabled
Background Scanning State...................... enabled
Backhaul Amsdu 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
Mesh DCA channels for serial backhaul APs....... disabled
Mesh Slot Bias................................. disabled
```

- To verify that slot 1 is being used for an uplink, do the following:
  a. Enable debugging on the AP by entering this command in the controller:

     debug ap enable *AP_name*

  b. Enter these commands in the controller:

     debug ap command show mesh config *AP_name*
     debug ap command show mesh adjacency parent *AP_name*

Preferred Parent Selection

You can configure a preferred parent for a MAP. This feature gives more control to you and enables you to enforce a linear topology in a mesh environment. You can skip AWPP and force a parent to go to a preferred parent.

Guidelines and Limitations

- The preferred parent is the best parent.
- The preferred parent has a link SNR of at least 20 dB (other parents, however good, are ignored).
- The preferred parent has a link SNR in the range of 12 dB and 20 dB, but no other parent is significantly better (that is, the SNR is more than 20 percent better). For an SNR lower than 12 dB, the configuration is ignored.
- The preferred parent is not in a blocked list.
- The preferred parent is not in silent mode because of dynamic frequency selection (DFS).
- The preferred parent is in the same bridge group name (BGN). If the configured preferred parent is not in the same BGN and no other parent is available, the child joins the parent AP using the default BGN.

Note Slot bias and preferred parent selection features are independent of each other. However, with the preferred parent configured, the connection is made to the parent using slot 1 or slot 2, whichever the AP sees first. If slot 1 is selected for the uplink in a MAP, then slot bias occurs. We recommend that you disable slot bias if you already know that slot 1 is going to be selected.

Configuring a Preferred Parent

To configure a preferred parent, enter this command:

config mesh parent preferred *AP_name MAC*

where:

- *AP_name* is the name of the child AP that you have to specify.
- *MAC* is the MAC address of the preferred parent that you have to specify.

Note When you configure a preferred parent, ensure that you specify the MAC address of the actual mesh neighbor for the desired parent. This MAC address is the base radio MAC address that has the letter f as the final character. For example, if the base radio MAC address is 00:24:13:0f:92:00, then you must specify 00:24:13:0f:92:0f as the preferred parent. This is the actual MAC address that is used for mesh neighbor relationships.

This example shows how to configure the preferred parent for the MAP1SB access point, where 00:24:13:0f:92:00 is the preferred parent's MAC address:

config mesh parent preferred *MAP1SB 00:24:13:0f:92:0f*

Related Commands

These commands are related to preferred parent selection:

- To clear a configured parent, enter the following command:

  config mesh parent preferred *AP_name* **none**

- To get information about the AP that is configured as the preferred parent of a child AP, enter this command:

  show ap config general *AP_name*

This example shows how to get the configuration information for the MAP1SB access point, where 00:24:13:0f:92:00 is the MAC address of the preferred parent:

show ap config general *MAP1SB*

```
Cisco AP Identifier.............................. 9
Cisco AP Name.................................... MAP1SB
Country code..................................... US - United States
Regulatory Domain allowed by Country............. 802.11bg:-A 802.11a:-A
AP Country code.................................. US - United States
AP Regulatory Domain............................. 802.11bg:-A 802.11a:-A
Switch Port Number .............................. 1
MAC Address...................................... 12:12:12:12:12:12
IP Address Configuration......................... DHCP
IP Address....................................... 209.165.200.225
IP NetMask....................................... 255.255.255.224
CAPWAP Path MTU.................................. 1485
Domain.......................................
Name Server...................................
Telnet State..................................... Disabled
Ssh State........................................ Disabled
Cisco AP Location................................ default location
Cisco AP Group Name.............................. default-group
Primary Cisco Switch Name........................ 4404
Primary Cisco Switch IP Address.................. 209.165.200.230
Secondary Cisco Switch Name.....................
Secondary Cisco Switch IP Address................ Not Configured
Tertiary Cisco Switch Name....................... 4404
Tertiary Cisco Switch IP Address................. 3.3.3.3
Administrative State ............................ ADMIN_ENABLED
Operation State ................................. REGISTERED
Mirroring Mode .................................. Disabled
AP Mode ......................................... Local
Public Safety ................................... Global: Disabled, Local: Disabled
AP subMode ...................................... WIPS
Remote AP Debug ................................. Disabled
S/W  Version .................................... 5.1.0.0
```

```
Boot  Version ................................. 12.4.10.0
Mini IOS Version .............................. 0.0.0.0
Stats Reporting Period ........................ 180
LED State...................................... Enabled
PoE Pre-Standard Switch........................ Enabled
PoE Power Injector MAC Addr.................... Disabled
Power Type/Mode................................ PoE/Low Power (degraded mode)
Number Of Slots................................ 2
AP Model....................................... AIR-LAP1252AG-A-K9
IOS Version.................................... 12.4(10:0)
Reset Button................................... Enabled
AP Serial Number............................... serial_number
AP Certificate Type............................ Manufacture Installed
Management Frame Protection Validation........... Enabled (Global MFP Disabled)
AP User Mode................................... CUSTOMIZED
AP username.................................... maria
AP Dot1x User Mode............................. Not Configured
AP Dot1x username.............................. Not Configured
Cisco AP system logging host................... 255.255.255.255
AP Up Time..................................... 4 days, 06 h 17 m 22 s
AP LWAPP Up Time............................... 4 days, 06 h 15 m 00 s
Join Date and Time............................. Mon Mar 3 06:19:47 2008

Ethernet Port Duplex........................... Auto
Ethernet Port Speed............................ Auto
AP Link Latency................................ Enabled
 Current Delay................................. 0 ms
 Maximum Delay................................. 240 ms
 Minimum Delay................................. 0 ms
 Last updated (based on AP Up Time)............ 4 days, 06 h 17 m 20 s
Rogue Detection................................ Enabled
AP TCP MSS Adjust.............................. Disabled
Mesh preferred parent.......................... 00:24:13:0f:92:00
```

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.

Viewing Mesh Statistics for a Mesh Access Point

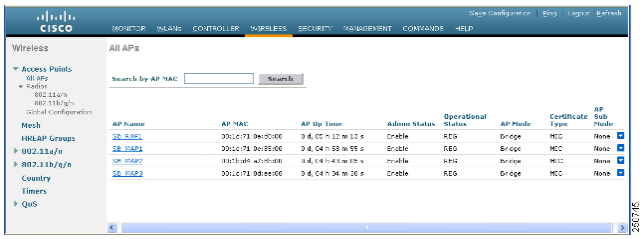
This section describes how to use the controller GUI or CLI to view mesh statistics for specific mesh access points.

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 (GUI)

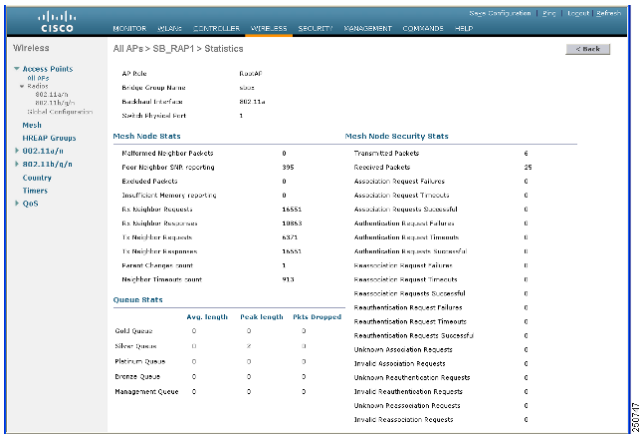
Step 1 Choose **Wireless > Access Points > All APs** to open the All APs page.

Figure 10-64 All APs Page



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.

Figure 10-65 All APs > Access Point Name > Statistics Page



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 10-17 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 10-17 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 10-17 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 (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 a Mesh Access Point

This section describes 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.

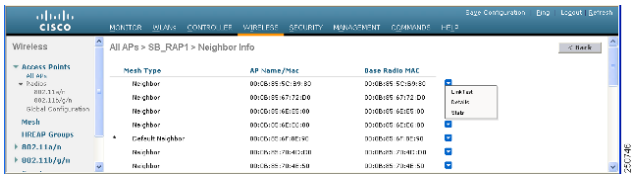
Viewing Neighbor Statistics for a Mesh Access Point (GUI)

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

Figure 10-66 All APs Page

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.

Figure 10-67 All APs > Access Point Name > Neighbor Info Page



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.

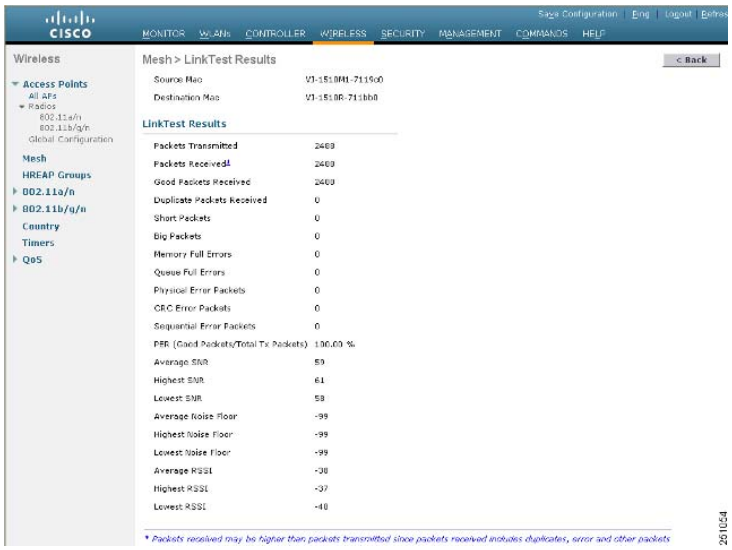
Step 3 To perform a link test between the mesh access point and its parent or children, follow these steps:

a. Hover the mouse over the blue drop-down arrow of the parent or desired child and choose **LinkTest**. A pop-up window appears.

Figure 10-68 Link Test Page

b. Click **Submit** to start the link test. The link test results appear on the Mesh > LinkTest Results page.

Figure 10-69 Mesh > LinkTest Results Page



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

Step 4 To view the details for any of the 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.

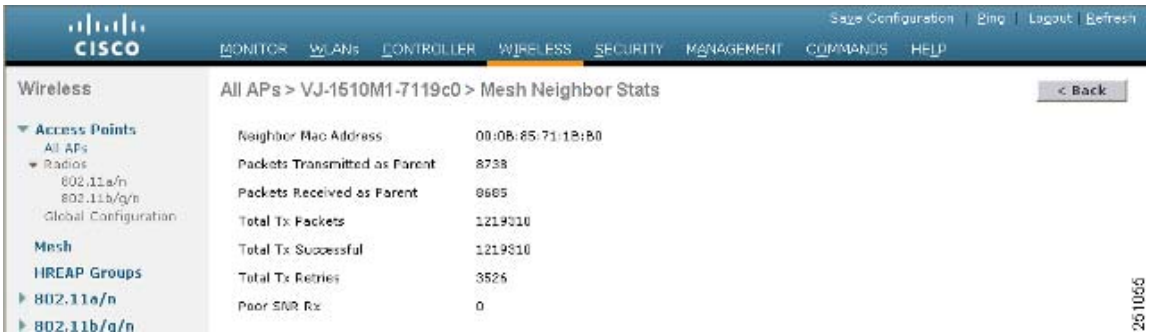
Figure 10-70 All APs > Access Point Name > Link Details > Neighbor Name page

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

Step 5 To view statistics for any of the 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.

Figure 10-71 All APs > Access Point Name > Mesh Neighbor Stats Page



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

Viewing the Neighbor Statistics for a Mesh Access Point (CLI)

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
```

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

Converting Indoor Access Points to Mesh Access Points

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

For information about this process, see this URL: http://cisco-images.cisco.com/en/US/docs/wireless/access_point/conversion/lwapp/upgrade/guide/lwapnote.html.

Step 2 Convert the lightweight access point to either a mesh access point (MAP) or root access point (RAP) as follows:

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

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

    config ap mode bridge *Cisco_AP*

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

    config ap mode bridge *Cisco_AP*

    config ap role rootAP *Cisco_AP*

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

     The access point reboots.
  c. At the Mesh panel, choose either **RootAP** or **MeshAP** from the AP Role drop-down list.
  d. Click **Apply to commit your changes.**
  e. Click **Save Configuration** to save your changes.

Changing MAP and RAP Roles for Indoor Mesh Access Points

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

Changing MAP and RAP Roles for Indoor Mesh Access Points (GUI)

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

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

Step 3 Click the **Mesh** tab.

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

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

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

Note We recommend that you use a Fast Ethernet connection between the MAP and controller when changing from a MAP to RAP.

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

Note We recommend that your power source for MAPs is either a power supply or power injector. We do not recommend that you use PoE as a power source for MAPs.

Changing MAP and RAP Roles for Indoor Mesh Access Points (CLI)

Step 1 Change the role of an indoor access point from MAP to RAP or from RAP to MAP by entering this command:

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

The access point reboots after you change the role.

Step 2 Save your changes by entering this command:

save config

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

The access point reboots after you enter the conversion commands in the controller CLI or perform the steps on the controller or the Cisco WCS.

Note We recommend that you use a Fast Ethernet connection to the controller for the conversion from a mesh (bridge) to nonmesh (local) access point. If the backhaul is a radio, after the conversion, you must enable Ethernet and then reload the access image.

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

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

  config ap mode local *Cisco_AP*

  The access point reloads.

- To convert an indoor mesh access point (MAP or RAP) to a nonmesh lightweight access point using the GUI, follow these steps:
  a. Choose **Wireless** and click on the AP Name link for the 1130 or 1240 indoor access point you want to convert.
  b. At the General Properties panel, choose **Local** from the AP Mode drop-down list.
  c. Click **Apply to apply changes.**
  d. Click **Save Configuration** to save your changes.
- To convert an indoor mesh access point (MAP or RAP) to a nonmesh lightweight access point using Cisco WCS, follow these steps:
  a. Choose **Configure > Access Points** and click on the AP Name link for the 1130 or 1240 indoor access point you want to convert.
  b. At the General Properties panel, choose **Local** as the AP Mode (left side).
  c. Click **Save**.

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

Outdoor access points (1522, 1524PS) can interoperate with the Cisco 3200 Series Mobile Access Router (MAR) on the public safety channel (4.9 GHz) as well as the 2.4-GHz access and 5-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. Data that is collected from in-vehicle deployments, such

as a police car can be integrated into the overall wireless infrastructure. For specific interoperability details between series 1130, 1240, and 1520 mesh access points and series 3200 mobile access routers, see Table 10-18.

Table 10-18 Mesh Access Points and MAR 3200 Interoperability

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

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

Guidelines and Limitations

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

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

- Change the channel width to 10 or 20 MHz to enable WGBs to associate with series 1520 mesh access points.
- Change the channel on the 1522 or 1524PS to a channel in the 5-MHz (channels 1 to 10) or 10-MHz band (channels 11 through 19) as follows:
  - When using the controller CLI, you must disable the 802.11a radio prior to configuring its channels. You reenable the radio after the channels are configured.
  - When using the GUI, enabling and disabling the 802.11a radio for channel configuration is not required.
  - Cisco MAR 3200s can scan channels within but not across the 5-, 10-, or 20-MHz bands.

Enabling Mesh Access Points to Operate with Cisco 3200 Series Mobile Access Routers (GUI)

Step 1 Enable the backhaul for client access by choosing **Wireless > Mesh** to open the Mesh page.

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

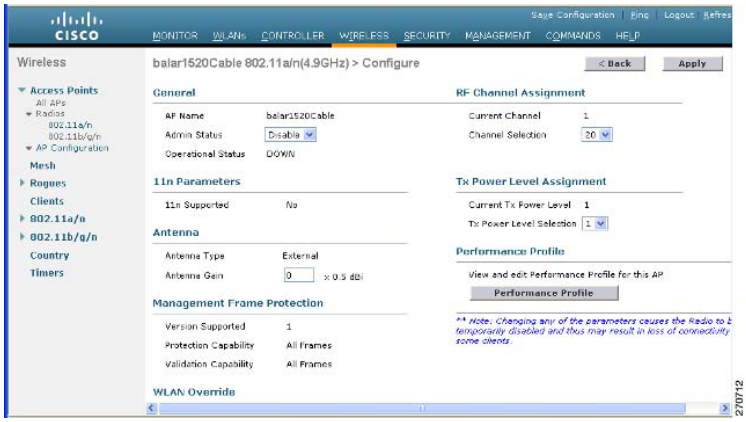
Step 3 Click **Apply** to commit your changes.

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

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

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

Figure 10-72 802.11 a/n (4.9GHz) > Configure Page



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

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

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

Enabling Mesh Access Points to Operate with Cisco 3200 Series Mobile Access Routers (CLI)

Step 1 Enable client access mode on the 1522 and 1524PS mesh access points by entering this command:

config mesh client-access enable

Step 2 Enable public safety on a global basis by entering this command:

config mesh public-safety enable *all*

Step 3 Enable the public safety channels by entering these commands:

- For the 1522 access point, enter these commands:

  config 802.11a disable *Cisco_MAP*

config 802.11a channel ap *Cisco_MAP channel_number*

config 802.11a enable *Cisco_MAP*

- For the 1524PS, enter these commands:

  config 802.11–a49 disable *Cisco_MAP*

  config 802.11–a49 channel ap *Cisco_MAP channel_number*

  config 802.11–a49 enable *Cisco_MAP*

Note Enter the **config 802.11–a58 enable** *Cisco_MAP* command to enable a 5-GHz radio.

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

Step 4 Save your changes by entering this command:

save config

Step 5 Verify your configuration by entering these commands:

show mesh public-safety

show mesh client-access

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

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

Note Enter the **show config 802.11-a58 summary** command to view configuration details for a 5-GHz radio.