Cisco Wireless Mesh Networking

This chapter provides design and deployment guidelines for the deployment of secure enterprise, campus, and metropolitan Wi-Fi networks within the Cisco Wireless Mesh Networking solution, a component of the Cisco Unified Wireless Network solution.

Note For more detailed information about Cisco Wireless Mesh Networking, including configuration and deployment, refer to the Cisco Mesh Access Points, Design and Deployment Guide, Release 8.0.

Mesh networking employs Cisco Aironet 1500 Series outdoor mesh access points (APs) and indoor mesh APs (Cisco Aironet 1040, 1130, 1140, 1240, 1250, 1260, 2600, 3500e, 3500i, 3600e, 3600i and 3700i series) along with the Cisco Wireless LAN Controller (WLC), and Cisco Prime Infrastructure to provide scalable, central management and mobility between indoor and outdoor deployments. The Control and Provisioning of Wireless Access Points (CAPWAP) protocol manages the connection of the mesh APs to the network.

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

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

- Cisco Aironet 1570 (1572) Series outdoor 802.11ac mesh APs
- Cisco Aironet 1550 (1552) Series outdoor 802.11n mesh APs
- Cisco Aironet 1520 (1522, 1524) Series outdoor mesh APs
- Cisco Aironet 1040, 1130, 1140, 1240, 1250, 1260, 1700, 2600, 3500e, 3500i, 3600e, 3600i and 3700i series indoor mesh APs333
- Mesh features in Cisco Wireless LAN Controller
- Mesh features in Cisco Prime Infrastructure

Note The Cisco Aironet 1505, 1510 and 1520 mesh APs are not supported because of their End-of-Life status.

Mesh Access Points

Access Point Roles

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

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

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

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

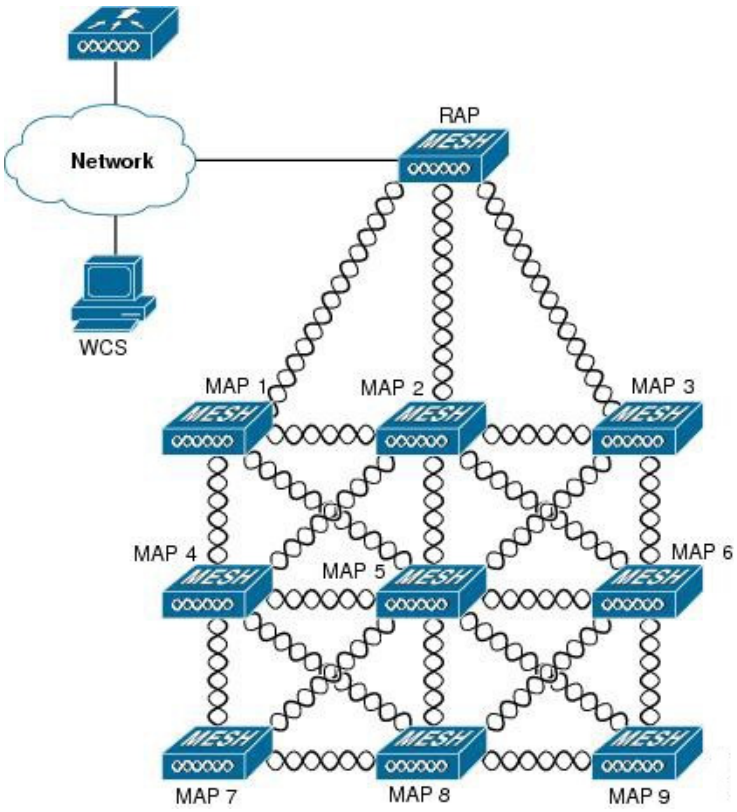
MAPs communicate among themselves and back to the RAP using wireless connections over the 802.11a/n radio backhaul. MAPs use the Cisco Adaptive Wireless Path Protocol (AWPP) to determine the best path through the other mesh access points to the controller.

Bridge mode access points support CleanAir in mesh backhaul at 5GHz frequency and provides only the interference device report (IDR) and Air Quality Index (AQI) reports.

Note The RAP or MAP does not generate Bridge Protocol Data Unit (BPDU) itself. However, the RAP or MAP forwards the BPDU to upstream devices if the RAP or MAP received the BPDU from its connected wired or wireless interface across the network.

Figure 8-1 shows the relationship between RAPs and MAPs in a mesh network.

Figure 8-1 Simple Mesh Network Hierarchy



Network Access

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

- Wireless LAN client traffic
- MAP Ethernet port traffic

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

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

- MAC authentication—Mesh access points are added to a database that can be referenced to ensure they are provided access to a given controller and mesh network.
- External RADIUS Authentication—Mesh access points can be externally authorized using a RADIUS server such as Cisco ACS (4.1 and later) that supports the client authentication type of Extensible Authentication Protocol-FAST (EAP-FAST) with certificates.

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.

Cisco Indoor Mesh Access Points

Indoor mesh is available on the following access points:

- 802.11n
  - 1040
  - 1140
  - 1260
- 802.11n+CleanAir
  - 1600
  - 2600
  - 3500e
  - 3500i
  - 3600
- 802.11ac+CleanAir
  - 1700
  - 2700
  - 3700

Note For more information about controller software support for access points, see the Cisco Wireless Solutions Software Compatibility Matrix.

Enterprise 11n/ac mesh is an enhancement added to the CUWN feature to work with the 802.11n/ac access points. Enterprise 11ac mesh features are compatible with non-802.11ac mesh but adds higher backhaul and client access speeds. The 802.11ac 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. If Universal Backhaul Access is enabled, the 5-GHz radio can be used for local (client) access as well as a backhaul.

Enterprise 11ac mesh supports P2P, P2MP, and mesh types of architectures.

The 802.11ac provides enterprise-class reliability and wired network like performance. It supports three spatial streams and 80 MHz wide channels for a maximum data rate of 1.3 Gbps. This is three times the maximum data rate of today's high-end enterprise 802.11n access point.

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 (non-mesh), 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 non-mesh 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 and client access if Universal Backhaul Access is enabled

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 1572 11ac outdoor access points, 1552 11n outdoor mesh access points, and 1532 dual radio mesh access points.

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 Prime Infrastructure. The communication between outdoor mesh access points (MAPs and RAPs) is over the 802.11a/n/ac radio backhaul. Client traffic is generally transmitted over the 802.11b/g/n radio (802.11a/n/ac can also be configured to accept client traffic).

The mesh access point can also operate as a relay node for other access points that are 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 terms9 of the signal strength and the number of hops required to get to a controller.

AP1500s are manufactured in two different configurations:

- Cable—This configuration can be mounted to a cable strand and supports power-over-cable (POC).
- Non-cable—This 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 Pluggable(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.

The mesh access points, can operate, apart from the mesh mode, in the following modes:

- Local mode—In this mode, the AP can handle clients on its assigned channel or while monitoring all channels on the band over a 180-second period. During this time, the AP listens on each channel for 50 milliseconds for rogue client beacons, noise floor measurements, interference, and IDS events. The AP also scans for CleanAir interference on the channel.
- FlexConnect mode—FlexConnect is a wireless solution for branch office and remote office deployments. The FlexConnect mode enables you to configure and control access points in a branch or remote office from the corporate office through a WAN link without having to deploy a controller in each office. The FlexConnect mode can switch client data traffic locally and perform client authentication locally when the connection to the controller is lost. When connected to the controller, the FlexConnect mode can also tunnel traffic back to the controller.

- Monitor mode—In this mode, the AP radios are in the receive state. The AP scans all the channels every 12 seconds for rogue client beacons, noise floor measurements, interference, IDS events, and CleanAir intruders.
- Rogue Detector mode—In this mode, the AP radio is turned off, and the AP listens only to the wired traffic. The controller passes the APs that are configured as rogue detectors as well as lists of suspected rogue clients and AP MAC addresses. The rogue detector listens for ARP packets and can be connected to all broadcast domains through a trunk link.
- Sniffer mode—In this mode, the AP captures and forwards all packets on a channel to a remote device that decodes the packets with packet analyzer software such as Wireshark.
- Bridge mode—In this mode, the AP is configured to build a wireless mesh network where wired network cabling is not available.
- Flex+Bridge mode—In this mode, both the Flexconnect and Bridge mode configuration options are available on the access point.

Note You can configure these modes using both the GUI and CLI. For configuration instructions, see the Cisco Wireless LAN Controller Configuration Guide.

Note MAPs can only be configured in Bridge / Flex+Bridge mode regardless of their wired or wireless backhaul. If the MAPs have a wired backhaul, you must change their AP role to RAP before you change the AP Mode.

Cisco Aironet 1570 Series Access Points

The Cisco Aironet 1570 series outdoor access point is ideal for both enterprise and carrier-class network operators looking to extend Wi-Fi coverage outdoors. It is the industry's highest performing outdoor AP and supports the latest Wi-Fi standard, 802.11ac, with data connection speeds up to 1.3 Gbps. This industrial-grade AP supports 4x4 multiple input and multiple output (MIMO) smart antenna technology and three spatial streams for optimum performance. The Aironet 1570 provides higher throughput over a larger area with more pervasive coverage. The AP is also well suited to high-density environments where many users in close proximity generate RF interference that needs to be managed. The 1572 highlights include:

- Most advanced carrier-grade outdoor Wi-Fi AP
- Dual-band 2.4 GHz and 5 GHz with 802.11ac Wave 1 support on the integrated 5 GHz radio
- Maximum radiated RF power allowed by law
- High Density Experience (HDX)
- Cisco CleanAir 2.0 technology provides integrated spectrum intelligence for a self configuring and self-healing network on 80 MHz channels.
- ClientLink 3.0 improves reliability and coverage for legacy, 802.11n and 802.11ac data rates
- Optimized roaming to allow clients to join the most optimal access point
- Turbo performance which uses Cisco ASIC design to maximize radio performance
- Improved 802.11ac range and performance with 4x4:3 multiple input and multiple output (MIMO) technology
- 1.3 Gbps (5 GHz) 802.11ac data rates

- Cisco Flexible Antenna Port technology
- DOCSIS 3.0/EuroDOCSIS/JapanDOCSIS 3.0, 24x8 hybrid fiber-coaxial (HFC) cable modem option
- Improved radio sensitivity and range performance with four antenna MIMO and three spatial streams
- Multiple uplink options (Gigabit Ethernet-10/100/1000 BaseT, Fiber SFP, Cable modem)
- Power: AC, DC, Cable, UPOE, PoE-Out (802.3at)
- 4G LTE coexistence
- NEMA Type 4X certified enclosure
- Module option: Investment protection and future proofing
- Low visual profile design
- Unified or autonomous operation

AP1572IC

The AP1572IC has the following features:

- Two radios (2.4 GHz and 5 GHz):
  - 2 GHz: 4x4:3
  - 5 GHz: 4x4:3
- Power options:
  - 40 - 90 VAC, 50 - 60 Hz, quasi-square wave, Power over Cable
  - 10 - 16 VDC
- Console Port
- LTE and WIMAX Signal Rejection (2.1/2.3 GHz; 30 dB; 2.5 GHz; 35 dB)
- DOCSIS and EuroDOCSIS 3.0 24x8
- GPS option

AP1572EC

The AP1572EC has the following features:

- Two radios (2.4 GHz and 5 GHz):
  - 2 GHz: 4x4:3
  - 5 GHz: 4x4:3
- Power options:
  - 40 - 90 VAC, 50 - 60 Hz, quasi-square wave, Power over Cable
  - 10 - 16 VDC
  - 802.3at PoE Out Capable
- Console Port
- LTE and WIMAX Signal Rejection (2.1/2.3 GHz; 30 dB; 2.5 GHz; 35 dB)
- GPS option

AP1572EAC

The AP1572EAC has the following features:

- Two radios (2.4 GHz and 5 GHz):
  - 2 GHz: 4x4:3
  - 5 GHz: 4x4:3
- Power options:
  - 100 - 277 VAC, 50 - 60 Hz
  - 10 - 16 VDC
  - UPoE
  - PoE with AIR-PWRINJ1550-2
  - 802.3at PoE Out Capable when powered via AC/DC power
- Console Port
- LTE and WIMAX Signal Rejection (2.1/2.3 GHz; 30 dB; 2.5 GHz; 35 dB)
- GPS option

Note For more information, see Aironet 1572 Deployment Guide

Cisco Aironet 1530 Series Access Points

The Cisco Aironet 1530 Series Access Points are designed to support a wide variety of applications. With a sleek profile, the access points can be deployed wherever coverage is needed and still meet the requirements of the particular deployment.

The following are the main features:

- Ultra Low—Profile, Outdoor AP
- 802.11n Dual-band (2.4 GHz and 5 GHz)
- Models—Internal (1532I) or External (1532E) antenna.
  - Flexible Antenna Port—Software configure ports for single-band or dual-band antennas
- Unified or Autonomous Modes—New boot logic allows AP to boot Unified or Autonomous from the same Hardware PID
- Bridging on 2.4 GHz or 5 GHz—Point-to-point or point-to-multipoint topology
- Daisy Chaining—Serial backhaul or enhanced universal access

For detailed information and other supporting documentation, see Cisco Aironet 1530 Series.

AP1532I

The AP1532I has the following features:

- Two radios (2.4 GHz and 5 GHz)
  - 2 GHz—3x3:3
  - 5 GHz—2x3:2
- UPoE and DC power (48 V)

- Console Port
- Weight: 2.3 kilograms (5.07 pounds)
- LTE and WIMAX Signal Rejection (2.1/2.3 GHz; 30 dB; 2.5 GHz; 35 dB)
- 23 x 17 x 10 cm (9 x 7 x 4inch); < 3.0 Liters

AP1532E

The AP1532E has the following features:

- Two radios (2.4 GHz and 5 GHz)
  - 2 GHz—2x2:2
  - 5 GHz—2x2:2
- PoE+ (802.3at) and DC power (48 V)
- Console Port
- Weight: 2.5 kilograms (5.5 pounds)
- LTE and WIMAX Signal Rejection (2.1/2.3 GHz; 30 dB; 2.5 GHz; 35 dB)
- Autonomous Bridging Functionality (Replacement for the 1310 and 1410 product lines)
- 26 x 17 x 10 cm (10 x 7 x 4inch); 3.0 Liters

Note For more information, see the 1532 Deployment Guide.

Cisco Aironet 1552 Mesh Access Point

The Cisco Aironet 1550 Series Outdoor Mesh Access Point is a modularized wireless outdoor 802.11n access point designed for use in a mesh network. The access point supports point-to-multipoint mesh wireless connectivity and wireless client access simultaneously. The access point can also operate as a relay node for other access points that are not directly connected to a wired network. Intelligent wireless routing is provided by the Adaptive Wireless Path Protocol (AWPP). This enables the access point to identify its neighbors and intelligently choose the optimal path to the wired network by calculating the cost of each path in terms of signal strength and the number of hops required to get to a controller.

The 1550 series access points leverage 802.11n technology with integrated radio and internal/external antennas. The 1552 outdoor platform consists of Multiple Input Multiple Output (MIMO) WLAN radios. It offers 2x3 MIMO with two spatial streams, beamforming, and comes with integrated spectrum intelligence (CleanAir).

CleanAir provides full 11n data rates while detecting, locating, classifying, and mitigating radio frequency (RF) interference to provide the best client experience possible. The CleanAir technology on the outdoor 11n platform mitigates Wi-Fi and non-Wi-Fi interference on 2.4 GHz radios.

The 1550 series access points have two radios-2.4 GHz and 5 GHz MIMO radios. While the 2.4 GHz radios are used primarily for local access, the 5 GHz radios are used for both local access and wireless backhaul in mesh mode.

Note The wIPS submode is not supported on the Cisco 1532, 1552, and 1572 Series Mesh Access Points.

Note The 2.4 GHz radios cannot be used for backhaul in 1552 APs.

The 2 GHz b/g/n radio has the following features:

- Operates in the 2.4 GHz ISM band.
- Supports channels 1-11 in the United States, 1-13 in Europe, and 1-13 in Japan.
- Has two transmitters for 802.11b/g/n operation.
- You can configure the output power for 5 power levels.
- The radio has three receivers that enable maximum-ratio combining (MRC).

The 5 GHz a/n radio has the following feature:

- Operates in the UNII-2 band (5.25 to 5.35 GHz), UNII-2 Extended/ETSI band (5.47 to 5.725 GHz), and the upper ISM band (5.725 to 5.850 GHz).
- Has two transmitters for 802.11a operation.
- Power settings can change depending on the regulatory domain. You can configure the output power for 5 power levels in 3 dB steps.
- The radio has three receivers that enable maximum-ratio combining (MRC).

The 1550 series access points have the following features:

- Can interoperate with legacy clients and offers enhanced backhaul performance
- Multicast VideoStream is supported when the AP is configured in Local mode.
- HotSpot 2.0 is supported when the AP is configured in Local / FlexConnect / Mesh mode.
- AP1552 is QoS capable of supporting quality VoWLAN calls.
- Band Select, which notifies a connected client to roam from 2.4 GHz to 5 GHz, is supported.
- DTLS support allows AP1552 to encrypt data in all supported AP modes except Bridge mode.
- You can enable CleanAir on the 5 GHz radio by navigating to **Wireless > Radios > 802.11a > Configure** on the controller GUI.
- If AP1552 is in Bridge mode, CleanAir Advisor becomes operational. CleanAir Advisor generates CleanAir reports and identifies interference. The event driven RRM is disabled. Therefore, the radio does not change the transmission power level or channel.

The models can be classified as models with external antennas and models with built-in antennas. The 1552C model is configured with an integrated DOCSIS/EuroDOCSIS 3.0 cable modem. The DOCSIS 3.0 cable modem provides 8 DS and 4 US (8x4), 304x108 Mbps. The EuroDOCSIS 3.0 cable modem provides 4 US and 4 DS (4x4), 152x108 Mbps. While a DOCSIS 2.0 cable modem could provide throughput of up to 40 Mbps only, a DOCSIS 3.0 cable modem can provide a DS throughput of 290 Mbps and a US throughput of 100 Mbps.

The 1552 Access Point is available in these models and defined below:

- 1552E
- 1552C
- 1552I
- 1552H
- 1552EU
- 1552CU

For more information, see Cisco 1550 Series Access Points.

1552E

The Cisco Aironet 1552E Outdoor Access Point is the standard model, dual-radio system with dual-band radios that are compliant with IEEE 802.11a/n (5 GHz) and 802.11b/g/n standards (2.4 GHz). The 1552E has three external antenna connections for three dual-band antennas. It has Ethernet and fiber SFP backhaul options, along with the option of a battery backup. This model also has a PoE-out port and can power a video surveillance camera. A highly flexible model, the Cisco Aironet 1552E is well equipped for municipal and campus deployments, video surveillance applications, mining environments, and data offload.

The 1552E model has the following features:

- Weighs 17.3 lbs (7.9 kg) excluding external antennas
- Two radios (2.4 GHz and 5 GHz)
- Three external dual-band omnidirectional antennas with 4 dBi in 2.4 GHz and 7 dBi in 5 GHz
- Vertical beamwidth: 29° at 2.4 GHz, 15° at 5 GHz
- Aligned console port
- Higher equivalent isotropically radiated power (EIRP)
- Multiple uplinks with Ethernet and fiber
- An optional SFP fiber module that can be ordered with the AP. The AP can use SFP fiber or copper module.
- 802.3af-compliant PoE-Out option to connect IP devices (such as video cameras)
- AC Powered (100 to 480 VAC)
- PoE-In using Power Injector
- Battery backup option (6 AH)

Note The 1552E model has no cable modem. The 1552E battery cannot be used for 1552H.

- AP1552E can be ordered with an Ethernet Passive Optical Network SFP as an add-on. The EPON SFP provides Gigabit data rates.

Note The EPON SFP feature must be ordered separately and installed.

- The AP1552 can be ordered with a GPS module as an add-on. The GPS module provides GPS that coordinates every 5 minutes and automatically updates location in the Cisco Prime Infrastructure Street Maps.

Note The AP1552E with a GPS Module must be powered using AC or DC power. The GPS module will be disabled if the AP is powered by PoE or battery backup.

1552C

Where service providers have already invested in a broadband cable network, the Cisco next-generation outdoor wireless mesh can seamlessly extend network connectivity with the Cisco Aironet 1552C access point by connecting to its integrated cable modem interface. The Cisco Aironet 1552C Outdoor Mesh Access Point is a dual-radio system with DOCSIS 3.0/EuroDOCSIS 3.0 (8x4 HFC) cable modem for power and backhaul. It has dual-band radios that are compliant with IEEE 802.11a/n (5 GHz) and 802.11b/g/n standards (2.4 GHz). The 1552C has an integrated, three- element, dual-band antenna and easily fits within the 30 cm height restriction for service providers. This model is suitable for 3G data offload applications and public Wi-Fi.

The 1552C model has the following features:

- Lightweight (14 lbs or 6.4 kg), low-profile AP
- Two radios (2.4 GHz and 5 GHz)
- DOCSIS/EuroDOCSIS 3.0 cable modem
- Aligned console port
- Supports cable modem backhaul
- Has an integrated 3-element array antenna with 2 dBi in 2.4 GHz and 4 dBi in 5 GHz
- Input module, power-over-cable supply (40 to 90 VAC)
- Stamped cover with two convenient holes to tighten the seizure screw for stringer connector (RF/Power Input) and to adjust the fuse pad to attenuate the signal

Note The 1552C model has no battery backup, no fiber SFP support, no PoE Out, no PoE In using Power Injector or Ethernet port, and no AC power option.

- The AP1552 can be ordered with a GPS module as an add-on. The GPS module provides GPS coordinates every 5 minutes and automatically updates location in the Cisco Prime Infrastructure Street Maps.

1552I

The Cisco Aironet 1552I Outdoor Access Point is a low-profile, lighter weight model. The smaller size and sleeker look helps to blend with the surrounding environment. The smaller power supply also makes it an energy efficient product. The 1552I does not have PoE-Out or a fiber SFP port.

The 1552I model has the following features:

- Lightweight (14 lbs or 6.4 kg), low-profile version
- Two radios (2.4 GHz and 5 GHz)
- Aligned console port
- AC powered (100 to 277 VAC)
- Stamped cover with no holes
- Supports street light power TAP

Note The 1552I model has no battery backup, no fiber SFP support, no cable modem, and no PoE Out.

1552H

This access point is designed for hazardous environments like oil and gas refineries, chemical plants, mining pits, and manufacturing factories. The Cisco Aironet 1552H Outdoor Access Point is Class 1, Div 2/Zone 2 hazardous location certified. The features are similar to the 1552E model, with the exception of the battery backup.

The 1552H model has the following features:

- Weighs 14 lbs (6.4 kg)
- Two radios (2.4 GHz and 5 GHz)
- Hazardous Location (Haz Loc) version.
- Power-over-Ethernet (PoE) input using Power Injector
- Aligned console port
- Three dual-band external omni-directional antennas
- AC entry module with terminal block
- AC powered (100 to 240 VAC, as per ATEX certification requirement)
- Fiber SFP backhaul option
- 802.3af-compliant PoE Out option to connect IP devices (such as video cameras)
- Battery backup option (special battery for hazardous locations)

For more information, see the Cisco Aironet 1552 Mesh Access Point Hardware and Installation Instructions.

1552CU

The 1552CU model has the following features:

- Two radios (2.4 GHz and 5 GHz)
- Aligned console port
- AC powered (40 to 90 VAC)
- Stamped cover with no holes
- External high-gain antennas (13 dBi in 2.4 GHz, 14 dBi in 5 GHz)
- Cable modem
- The AP1552 can be ordered with a GPS module as an add-on. The GPS module provides GPS that coordinates every 5 minutes and automatically updates location in the Cisco Prime Infrastructure Street Maps.

1552EU

The 1552EU model has the following features:

- Two radios (2.4 GHz and 5 GHz)
- Aligned console port
- AC powered (90 to 480 VAC)
- PoE 802.3af
- External high-gain antennas (13 dBi in 2.4 GHz, 14 dBi in 5 GHz)

- Battery
- AP1552EU can be ordered with an Ethernet Passive Optical Network SFP as an add-on. The EPON SFP provides Gigabit data rates.

Note The EPON SFP feature must be ordered separately and installed.

- The AP1552 can be ordered with a GPS module as an add-on. The GPS module provides GPS that coordinates every 5 minutes and automatically updates location in the Cisco Prime Infrastructure Street Maps.

Note The AP1552EU with a GPS Module must be powered using AC or DC power. The GPS module will be disabled if the AP is powered by PoE or battery backup.

Ethernet Ports

AP1500s support four Gigabit Ethernet interfaces.

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

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

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

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

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

Multiple Power Options

For the 1550 Series

Power options include the following:

- Power over Ethernet (PoE)-In
  - 56 VDC using a Power Injector (1552E and 1552H)
  - PoE-In is not 802.3af and does not work with PoE 802.3af-capable Ethernet switch

- AC Power
  - 100 to 480 VAC (47-63 Hz)—Connecting AC or Streetlight Power (1552E)
  - 100 to 240 VAC—Connecting AC or Streetlight Power (1552H)
- External Supply
  - 12 VDC—Connecting DC Power Cable (All Models)
- Internal Battery Backup (1552E and 1552H)
- Power over Cable (PoC)
  - 40 to 90 VAC—Connecting Cable PoC (1552C)
- PoE-Out 802.3af compliant to connect IP devices such as Video Cameras (1552E and 1552H)
  - (PoE-Out) is not available when using Power Injector (PoE-In) as the power source
- 802.3af compliant PoE-Out to connect IP devices such as video cameras (1552E and 1552H)

  This port also performs Auto-MDIX, which enables to connect crossover or straightthrough cables.

The 1550 series access points can be connected to more than one power source. The access points detect the available power sources and switch to the preferred power source using the following default prioritization:

- AC power or PoC power
- External 12-VDC power
- Power injector PoE power
- Internal battery power

Table 8-1 lists the power options available for the 1552 access point models.

Table 8-1 Power Options in 1552 Models

Power Option	1552E	1552H	1552C	1552I
AC	100 to 480 VAC 80W	100 to 240 VAC 80W	—	100 to 277 VAC 50W
Power over Cable	—	—	40 to 90 V (quasi- square wave) 45 W	—
PoE (using Power Injector)	56 V +/- 10%	56 V +/- 10%	—	—
DC (nominal 12 VDC)	11.4 to 15 V	11.4 to 15 V	11.4 to 12.6 V	11.4 to 15 V
Battery Backup	80 W-hr	35 W-hr	—	—

Battery Backup Module (Optional)

Battery backup six-ampere hour module is available for the following:

- AIR-1550-BATT-6AH for only the AIR-CAP-1552E-x-K9 model

The integrated battery can be used for temporary backup power during external power interruptions. The battery run time for AP1550s is as follows:

- 2-hour access point operation using two radios at 77oF (25oC) with PoE output port off
- 1.5-hour access point operation using two radios at 77oF (25oC) with PoE output port on

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

Note For a complete listing of optional hardware components for AP1520s such as mounting brackets, power injectors, and power tap adapters, see Cisco Aironet 1520 Series Lightweight Outdoor Access Point Ordering Guide.

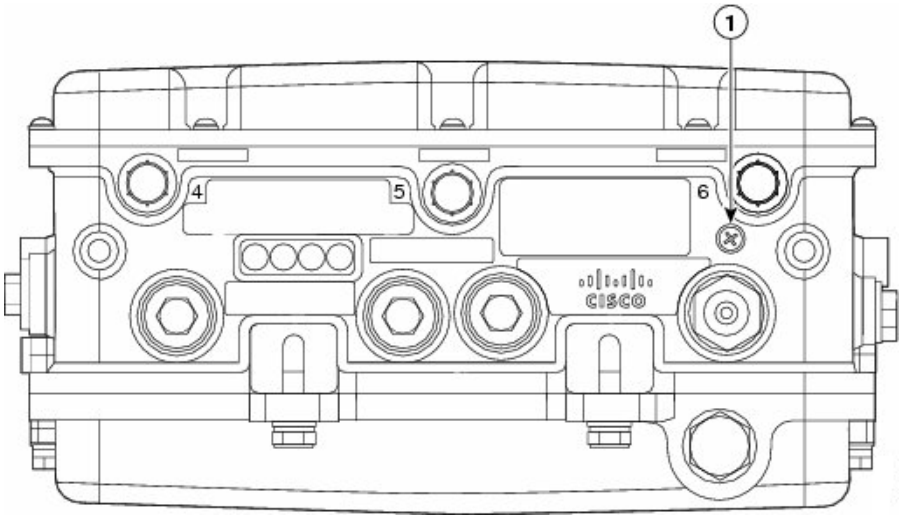
1550 Reset Button

A 1500 series access point has a reset button located on the bottom of the unit. The reset button is recessed in a small hole that is sealed with a screw and a rubber gasket. The reset button can be used to perform the following functions:

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

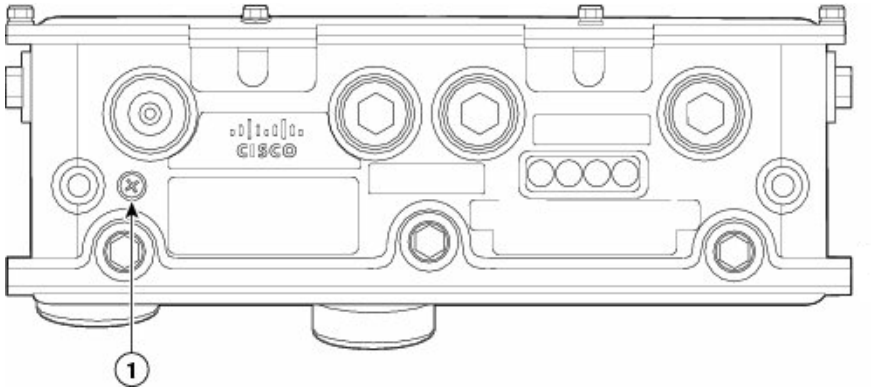
    config mesh battery-state disable *AP_name*
- Switch off LEDs—Press the reset button for more than 10 seconds, and the LEDs turn off, then on, and then stay off.

Figure 8-2 Reset Button Location - Models AIR-CAP1552E-x-K9 and AIR-CAP1552H-x-K9



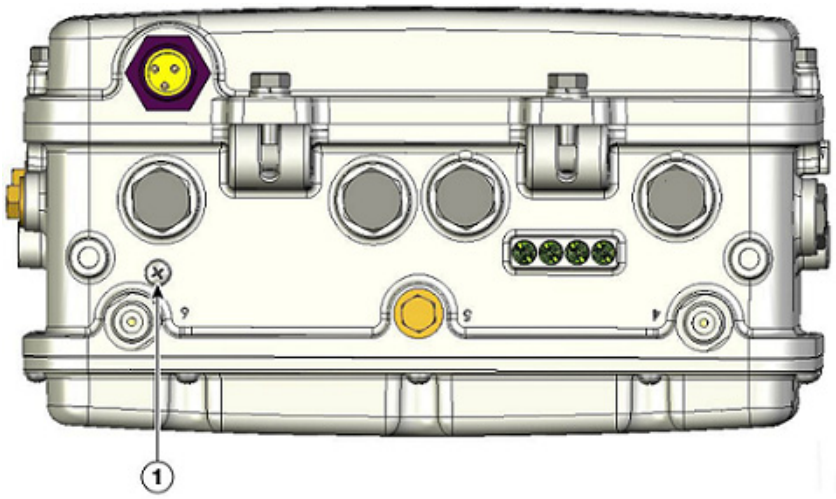
1	Reset Button

Figure 8-3 Reset Button Location - Models AIR-CAP1552C-x-K9 and AIR-CAP1552I-x-K9



1	Reset Button

Figure 8-4 Reset Button Location for 1520 Series



1	Reset Button

Resetting 1550 Access Point

To reset the access point, follow these steps:

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

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

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

Monitoring the 1550s LED Status

The four-status LEDs on AP1550s are useful during the installation process to verify connectivity, radio status, access point status, and software status. However, once the access point is up and running and no further diagnosis is required, we recommend that you turn off the LEDs to discourage damage.

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

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

There are four LED status indicators on AP1550s.

Figure 8-5 shows the location of the AP1550 LEDs.

Figure 8-5 Access Point LEDs at the Bottom of the Unit

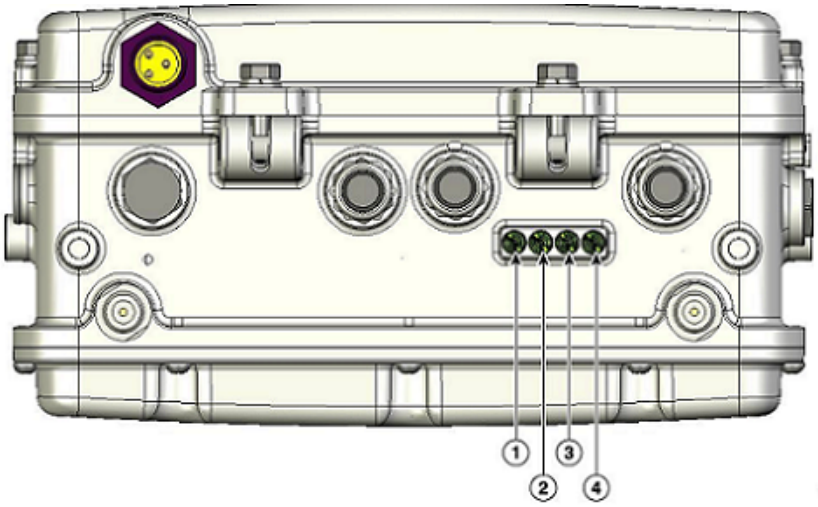


Table 8-2 below describes each LED and its status.

Table 8-2 LED and its Status

No.	Description
1	Status LED—Access point and software status
2	Uplink LED—Ethernet, cable, or fiber status
3	RF-1 LED—Status of the radio in slot 0 (2.4 GHz) and slot 2 (5.8 GHz for 1524SB and 4.9 GHz for 1524PS)).
4	RF-2 LED—Status of the radio in slot 1 (5.8 GHz) and the radio in slot 3[1].

1. Slot 3 is disabled.

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

Table 8-3 lists the Access Point LED signals.

Table 8-3 Access Point LED Signals

LED	Color[1]	Meaning
Status	Off	Access is point is not powered on.
	Green	Access point is operational.
	Blinking green	Download or upgrade of Cisco IOS image file is in progress.
	Amber	Mesh neighbor access point discovery is in progress.
	Blinking amber	Mesh authentication is in progress.
	Blinking red/green/amber	CAPWAP discovery is in progress.
	Red	Firmware failure. Contact your support organization for assistance.
Uplink	Off	No physical connector is present. The uplink port is not operational.
	Green	Uplink network is operational (cable, fiber optic, or Ethernet).
RF-1 Slot 0 2.4-GHz radio	Off	Radio is turned off.
	Green	Radio is operational.
	Red	Firmware failure. Contact your support organization for assistance.
RF-1 Slot 2 802.11a radio	Off	Radio is turned off.
	Green	Radio is operational.
	Red	Firmware failure. Contact your support organization for assistance.
RF-2 Slot 1 802.11a radio	Off	Radio is turned off.
	Green	Radio is operational.
	Red	Firmware failure. Contact your support organization for assistance.
RF-2 Slot 3	Disabled in this release.	—

1. If all LEDs are off, the access point has no power.
When the access point power supply is initially turned on, all LEDs are amber.

1570

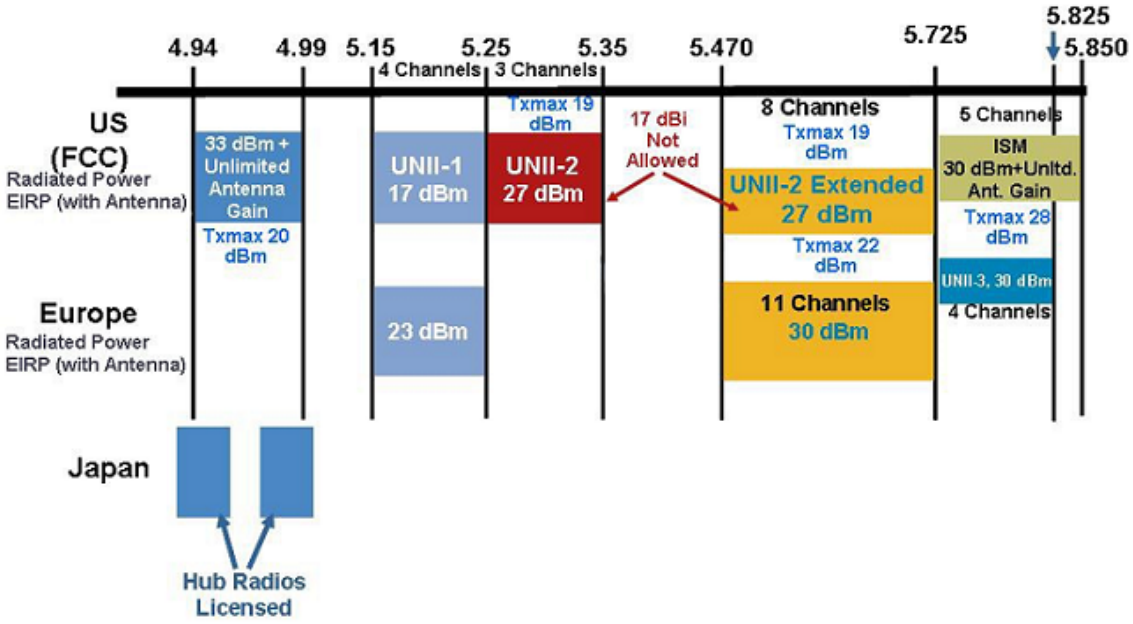
For more information, please refer the following guides:

- AP-1570 Hardware Installation Guide
- AP-1570 Deployment Guide

Frequency Bands

Both the 2.4-GHz and 5-GHz frequency bands are supported on the indoor and outdoor access points.

Figure 8-6 Frequency Bands Supported by 802.11a Radios on AP1500s



The 5-GHz band is a conglomerate of three bands in the USA: 5.150 to 5.250 (UNII-1), 5.250 to 5.350 (UNII-2), 5.470 to 5.725 (UNII-2 Extended), and 5.725 to 5.850 (ISM). UNII-1 and the UNII-2 bands are contiguous and are treated by 802.11a as being a continuous swath of spectrum 200-MHz wide, more than twice the size of the 2.4-GHz band (see Table 8-4)

The -D domain, which is the country domain for India, supports the following:

- 20-MHz channels—169 (5.845 GHz) and 173 (5.865 GHz)
- 40-MHz channels—The channel pair 169/173 (5.855 GHz)

Note The frequency depends on the regulatory domain in which the access point is installed. For additional information, see the Channels and Power Levels Document.

Table 8-4 lists the frequency band.

Table 8-4 Frequency Band

Frequency Band Terms	Description	Model Support
UNII-1[1]	Regulations for UNII devices operating in the 5.15- to 5.25 GHz frequency band. Indoor operation and outdoor APs using the -B reg domain.	All 11n/ac Indoor APs and the 1572.
UNII-2	Regulations for UNII devices operating in the 5.25- to 5.35 GHz frequency band. DFS and TPC are mandatory in this band.	All 11n/ac indoor APs, 1532, 1552, and 1572.
UNII-2 Extended	Regulations for UNII-2 devices operating in the 5.470 to 5.725 frequency band.	All 11n/ac indoor APs, 1532, 1552, and 1572.
ISM5[2]	Regulations for UNII devices operating in the 5.725 to 5.850 GHz frequency band.	All 11n/ac indoor APs, 1532, 1552, and 1572.

1. UNII refers to the Unlicensed National Information Infrastructure.
2. ISM refers to Industrial, Scientific and Medical.

Note For regulatory information, see Wireless LAN Compliance Status.

Dynamic Frequency Selection

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

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

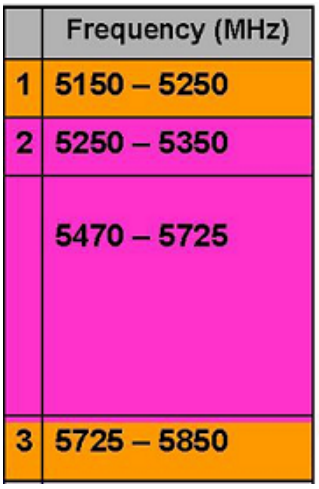
The AP performs a DFS scan on the new DFS channel for 60 seconds. However, if a neighboring AP is already using that new DFS channel, the AP does not perform the DFS scan.

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

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

Note DFS is mandatory in the USA for 5250 to 5350 and 5470 to 5725 frequency bands. DFS and TPC are mandatory for these same bands in Europe.

Figure 8-7 DFS and TPC Band Requirements



Antennas

Overview

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

- Directional
- Omni-directional

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

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

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

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

Note An 8-dBi antenna transmits with a horizontal beamwidth of 360 degrees, causing the radio waves to disperse power in all directions. Therefore, radio waves from an 8-dBi antenna do not go nearly as far as those radio waves sent from a 14-dBi patch antenna (or a third-party dish) that has a more narrow beamwidth (less than 360 degrees).

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

Antenna Options

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

Table 8-5 lists the supported external 2.4- and 5-GHz antennas for AP1500s.

Table 8-5 External 2.4- and 5-GHz Antennas

Part Number	Model	Gain (dBi)
AIR-ANT2450V-N	2.4-GHz compact omni-directional[1]	5
AIR-ANT-2455V-N	2.4-GHz compact omni-directional	5.5
AIR-ANT2480V-N	2.4-GHz omni-directional	8.0
AIR-ANT5180V-N	5-GHz compact omni-directional[2]	8.0
AIR-ANT5140V-N	5-GHz right-angle omni-directional	4.0
AIR-ANT5114P-N	5-GHz patch2	14.0
AIR-ANT2547V-N	2.4 - 5-GHz dual-band omni-directional	4 dBi at 2.4 GHz and 7 dBi at 5 GHz

1. The compact omni-directional antennas mount directly on the access point.
2. The compact omni-directional antennas mount directly on the access point.

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

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

Table 8-6 summarizes the horizontal and vertical beamwidth for Cisco antennas.

Table 8-6 Horizontal and Vertical Beamwidth for Cisco Antennas

Antenna	Horizontal Beam-width (degrees)	Vertical Beam-width (degrees)
AIR-ANT5180V-N	360	16
AIR-ANT5114P-N	25	29
AIR-ANT2547V-N	360	30

N-Connectors

- All external antennas are equipped with male N-connectors.

- AP1552 E/H have three N-connectors to connect dual-band antennas. AP1552 C/I have no N-connectors as they come with inbuilt antennas.
- Each radio has at least one TX/RX port. Each radio must have an antenna connected to at least one of its available TX/RX ports.
- Antenna locations for 5.8 GHz and 2.4 GHz are fixed and labeled.

Antenna Configurations for 1552

The 1552 access point supports the following two types of antennas designed for outdoor use with radios operating in the 2.4-GHz and 5-GHz frequency:

- Cisco Aironet Low Profile Dual-Band 2.4/5 GHz Dipole Antenna Array (CPN 07-1123-01), an integrated array of three dual-band dipole antennas.
- Cisco Aironet Dual-Band Omnidirectional Antenna (AIR-ANT2547V-N), referred to as "stick" antennas.

Two types of mounting configurations are available: the cable strand mount and the pole mount.

The 1552 models C and I access points are equipped with three new integrated dual-band antennas, with 2 dBi gain at 2.4 GHz and 4 dBi gain at 5 GHz. The antenna works in cable strand mount, low cost and has low profile applications.

Figure 8-8 1552C Cable Mount

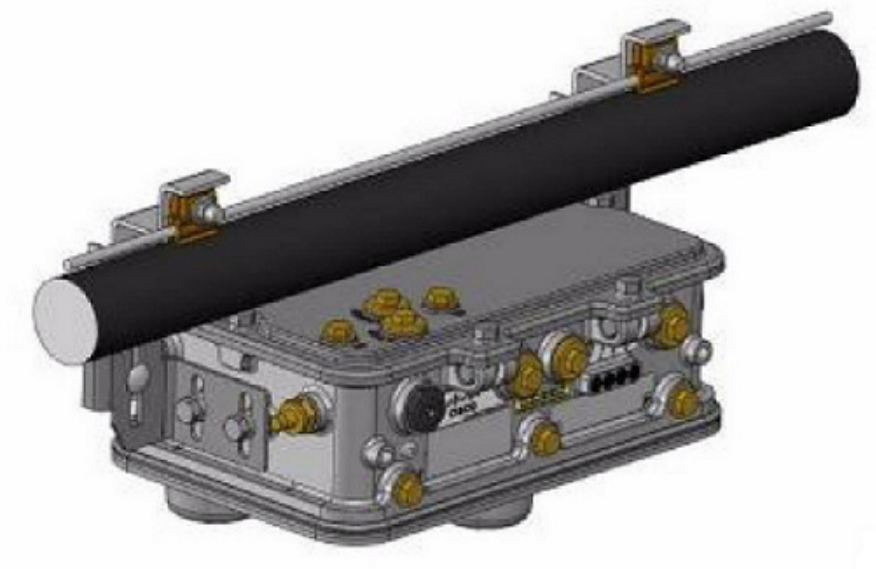
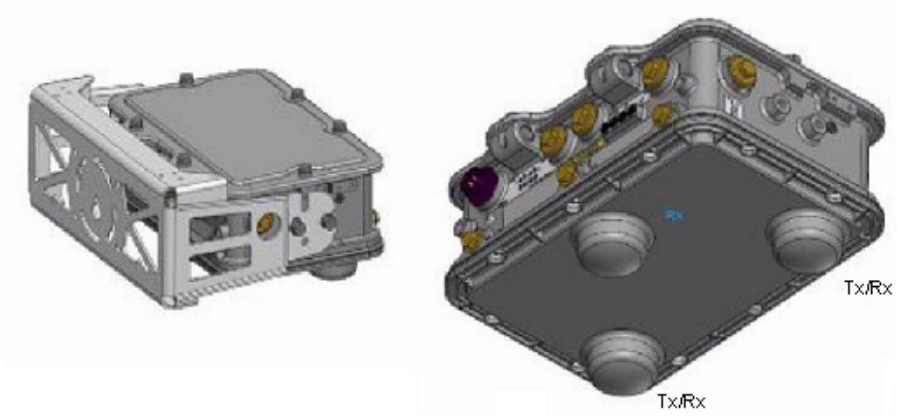


Figure 8-9 1552I Pole/Wall Mount



The 1552 E and H access points are equipped with three N-type radio frequency (RF) connectors (antenna ports 4, 5, and 6) on the bottom of the unit for external antennas to support multiple input multiple output (MIMO) operation as shown in the figure below. When using the optional Cisco Aironet AIR-ANT2547V-N Dual-Band Omni-directional Antenna, the 2.4- and 5-GHz antennas connect directly to the access point. These antennas have 4 dBi gain at 2.4 GHz and 7 dBi gain at 5 GHz.

Figure 8-10 1552 E Pole/Wall Mount

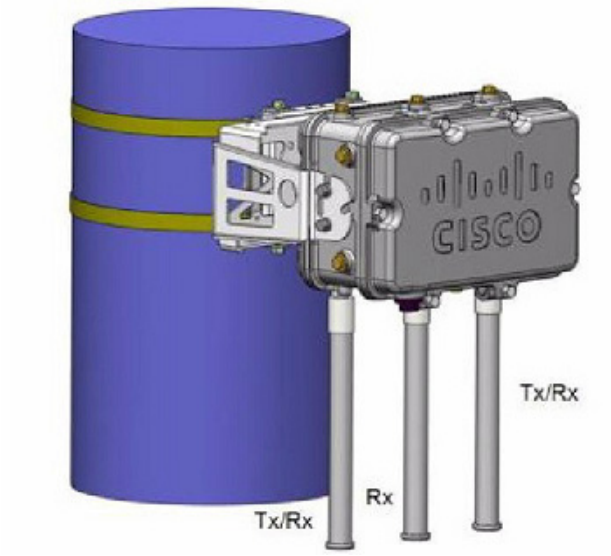
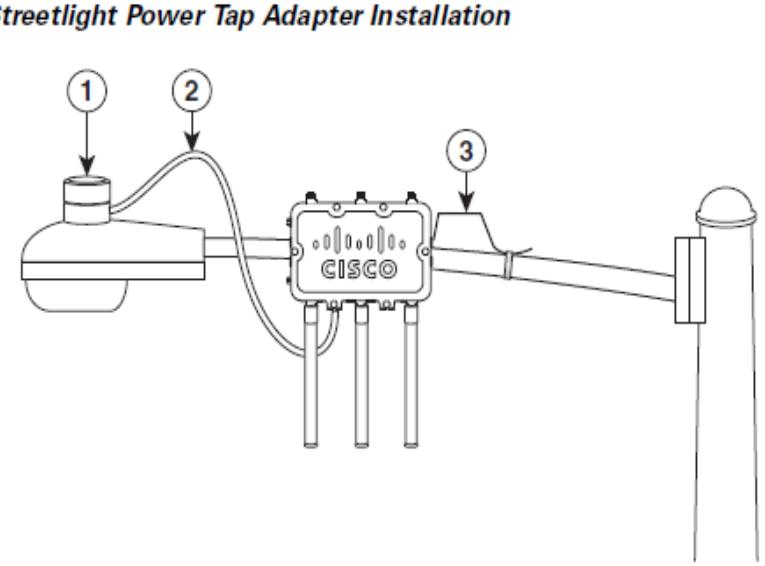


Figure 8-11 shows one of the recommended installations of an outdoor AP1500.

Figure 8-11 Outdoor Pole-top Installation of a Mesh Access Point



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

The AP1500 series was designed building on the long experience we have had in deploying outdoor access points over the past few years. This includes consideration for resistance to lightning effects. The AP1500 series employs some lightning arrestor circuitry on the Ethernet & Power ports. On input Ethernet port, Gas Discharge Tubes (GDT) are used on the Power Entry Module (PEM) to mitigate lightning effect. On the AC Power, GDTs are also used along with fuses to mitigate a high-current condition. For the DC power, a fuse is used to mitigate a high-current condition.

While not a common practice, users may want to consider adding additional lightning protection at the antenna ports for added protection.

Client Access Certified Antennas (Third-Party Antennas)

You can use third-party antennas with AP1500s. However, note the following:

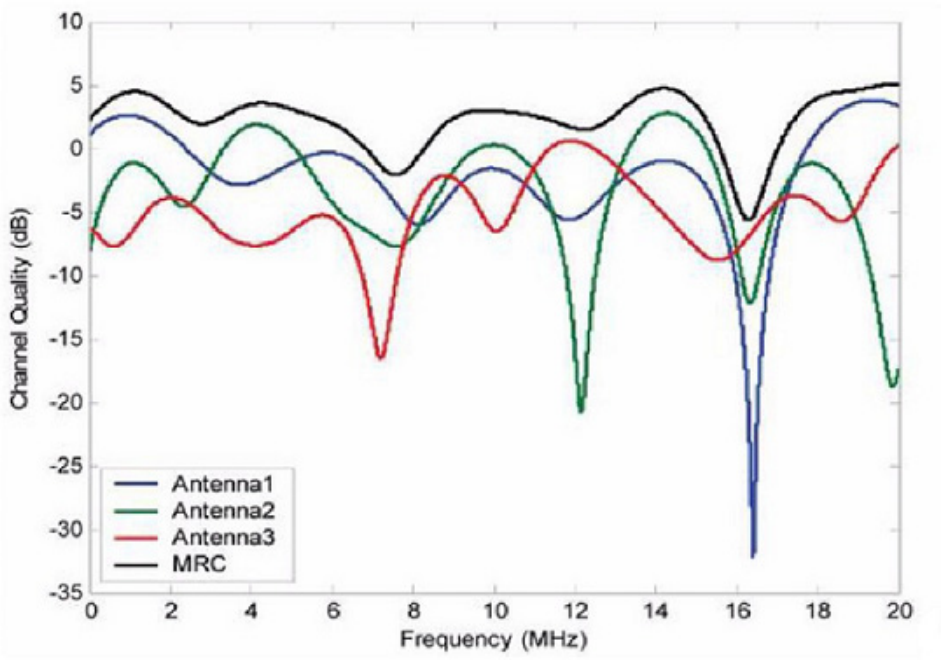
- Cisco does not track or maintain information about the quality, performance, or reliability of the non-certified antennas and cables.
- RF connectivity and compliance is the customer's responsibility.
- Compliance is only guaranteed with Cisco antennas or antennas that are of the same design and gain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

Maximum Ratio Combining

To understand how this works, consider a single transmitter 802.11a/g client sending an uplink packet to an 802.11n access point with multiple transceivers. The access point receives the signal on each of its three receive antennas.

Each received signal has a different phase and amplitude based on the characteristics of the space between the antenna and the client. The access point processes the three received signals into one reinforced signal by adjusting their phases and amplitudes to form the best possible signal. The algorithm used, called maximum ratio combining (MRC), is typically used on all 802.11n access points. MRC only helps in the uplink direction, enabling the access point to "hear" the client better.

Figure 8-12 Reinforcement of Received Signal via MRC Algorithm



For the 1550 Series

In the 1552 series mesh access point, MRC gain is different from the 1520 series mesh access points. The 1520 series access points do not have 802.11n functionality. The 2.4-GHz band has only one transmitter and up to three receivers. Therefore, it is SIMO (Single in Multiple out) in 2.4 GHz. In the 5-GHz band, it has only one transmitter and one receiver. Therefore, it is SISO (Single in Single out) in the 5-GHz band. The MRC gain is important only for the 2.4-GHz radio in the 1552 access points. The MRC is not available for the 5-GHz radio. The 2.4-GHz radio has one Tx and up to three Rx antennas depending on the AP configuration.

In the 1522 access points, users have an option to use one, two, or three 2.4-GHz Rx antennas. With this option, users get around 3 dB MRC gain with 2 Rx antennas and a 4.5-dB MRC gain with 3 Rx antennas for data rates of 24 Mbps or higher.

For the 1552 access points, both the 2.4- and 5-GHz radios are 2x3 MIMO. Therefore, they have two transmitters and three receivers. Because the antennas are dual band and there is no option to have less than three Rx antennas, the MRC is added to the RX sensitivity always as it is embedded into the baseband chipset.

The number for typical Rx sensitivity in our customer data sheet assume 3 Rx antennas for both the 1520 and the 1550 series access points.

With the chipset used in the AP1520 series radios, there was a start-of-packet problem at lower data rates that wiped out the gain. Therefore, the MRC gain became useful from a data rate of 12 Mbps onwards in the 1520 series access points. This problem has been corrected in the current chipset used in the 1552 access points. The MRC gain has improved for lower data rates as well in the 1552 access points. You get a 4.7-dB improvement in sensitivity with the 2x3 MIMO radio over a 1x1 SISO implementation.

Table 8-7 lists the AP1552 11a/g MRC Gain, and Table 8-8 lists the AP1552 11n MRC gain

Table 8-7 AP1552 11a/g MRC Gain

11a/g MCS (Mbps)	Modulation	MRC Gain from 3 RXs (dB)
6	BPSK 1/2	4.7
9	BPSK 3/4	4.7
12	QPSK 1/2	4.7
18	QPSK 3/4	4.7
24	16QAM 1/2	4.7
36	16QAM 3/4	4.7
48	64QAM 2/3	4.7
54	64QAM 3/4	4.7

Table 8-8 AP1552 11n MRC Gain

No. of Spatial Streams	11n MCS	Modulation	MRC Gain from 3 RXs (dB)
1	MCS 0	BPSK 1/2	4.7
1	MCS 1	QPSK 1/2	4.7
1	MCS 2	QPSK 3/4	4.7
1	MCS 3	16QAM 1/2	4.7
1	MCS 4	16QAM 3/4	4.7
1	MCS 5	64QAM 2/3	4.7
1	MCS 6	64QAM 3/4	4.7
1	MCS 7	64QAM 5/6	4.7
2	MCS 8	BPSK 1/2	1.7
2	MCS 9	QPSK 1/2	1.7
2	MCS 10	QPSK 3/4	1.7
2	MCS 11	16QAM 1/2	1.7
2	MCS 12	16QAM 3/4	1.7
2	MCS 13	64QAM 2/3	1.7
2	MCS 14	64QAM 3/4	1.7
2	MCS 15	64QAM 5/6	1.7

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 is 3 SS with 3 RX, then the MRC gain will be zero.

Cisco 1500 Hazardous Location Certification

The standard AP1500 enclosure is a ruggedized, hardened enclosure that supports the NEMA 4X and IP67 standards for protection to keep out dust, damp and water.

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

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

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

Cisco has Hazardous Certified SKU for USA and EU: AIR-LAP1552H-x-K9. This SKU is modified, as per the certification requirements. The hazardous locations certificate requires that all electrical power cables be run through conduit piping to protect against accidental damage to the electrical wiring that could cause a spark and possible explosion. Access points for hazardous locations contain an internal electrical mounting connect that receives discrete wires from a conduit interface coupler entering from the side of the housing. After the electrical wiring is installed, a cover housing is installed over the electrical connector to prevent exposure to the electrical wiring. The outside of the housing has a hazardous location certification label (CSA, ATEX, or IEC) that identifies the type of certifications and environments that the equipment is approved for operation.

Note Power entry module for CSA (USA and Canada) is Power Entry Module, Groups A, B, C, and D with T5v(120° C) temp code. Power Entry Module for ATEX (EU) is Power entry module Groups IIC, IIB, IIA with T5 (120° C) temperature code.

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

Class 1, Division 1/Zone 1 is for the environments with full-time ignitable concentrations of flammable gases, vapors, or liquids. To meet the requirements of the Div 1 > Div 2 and Zone 1 > Zone 2 locations, we recommend a TerraWave Solutions CSA certified protective Wi-Fi enclosure (see Table 8-9 for TerraWave Enclosures).

Table 8-9 TerraWave Enclosures

Access Points	Enclosure Part No	Description
Indoor Mesh Access Points	Example: TerraWave XEP1242 for 1240 series.	18 x12 x8 Protective Wi-Fi Enclosure that includes the Cisco 1242 Access Point
Outdoor Mesh Access Points (1552)	Example: TerraWave Part Number: XEP1522	18 x 12 x8 Protective Wi-Fi Enclosure that includes the Cisco 1522 Access Point

For more information, see Terrawave Enclosures.

Table 8-10 lists the hardware features across different AP1500 models at a glance.

Table 8-10 Hardware Features at a Glance

Features	1552E	1552H	1552C	1552I
Number of radio	2	2	2	2
External Antennas	Yes	Yes	—	—
Internal Antennas	—	—	Yes	Yes
CleanAir 2.4-GHz radio	Yes	Yes	Yes	Yes
CleanAir 5-GHz radio	—	—	—	—
Beam Forming (ClientLink)	Yes	Yes	Yes	Yes
Fiber SFP	Yes	Yes	—	—
802.3af PoE out port	Yes	Yes	—	—
DOCSIS 3.0 Cable Modem	—	—	Yes	—
HazLoc Class 1 Div 2/Zone 2	—	Yes	—	—
Battery backup option	Yes	Yes	—	—
Power options	AC, DC, Power Injector	AC, DC, Power Injector	40 to 90 VAC Power over Cable	AC, DC
Console Port Ext. Access	Yes	Yes	Yes	Yes

Note PoE-in is not 802.3af and does not work with PoE 802.3af-capable Ethernet switch. It requires Power Injector.

Cisco Wireless LAN Controllers

The wireless mesh solution is supported on Cisco 2500, 5500, and 8500 Series Wireless LAN Controllers. For more information, see Wireless LAN Controller.

Cisco Prime Infrastructure

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

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

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

Architecture

Control and Provisioning of Wireless Access Points

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

Note CAPWAP significantly reduces capital expenditures (CapEx) and operational expenses (OpEx), which enables the Cisco wireless mesh networking solution to be a cost-effective and secure deployment option in enterprise, campus, and metropolitan networks.

CAPWAP Discovery on a Mesh Network

The process for CAPWAP discovery on a mesh network is as follows:

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

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

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

Step 3 If Step 2 fails after 10 attempts, the mesh access point falls back to DHCP and attempts to connect in 10 tries.

Step 4 If both Step 2 and Step 3 fail and there is no successful CAPWAP connection to a controller, then the mesh access point falls back to LWAPP.

Step 5 If there is no discovery after attempting Step 2, Step 3, and Step 4, the mesh access point tries the next link.

Dynamic MTU Detection

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

XML Configuration File

Mesh features within the controller's boot configuration file are saved in an XML file in ASCII format. The XML configuration file is saved in the flash memory of the controller.

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

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

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

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

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

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

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

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

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

```
show invalid-config
```

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

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

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

Adaptive Wireless Path Protocol

The Adaptive Wireless Path Protocol (AWPP) is designed specifically for wireless mesh networking to provide ease of deployment, fast convergence, and minimal resource consumption.

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

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

To optimize the route, a MAP actively solicits neighbor MAP. During the solicitation, the MAP learns all of the available neighbors back to a RAP, determines which neighbor offers the best path, and then synchronizes with that neighbor. The path decisions of AWPP are based on the link quality and the number of hops.

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

Traffic Flow

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

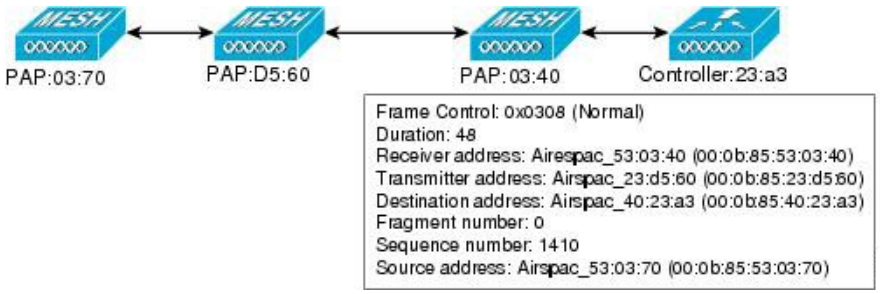
- Overlay CAPWAP traffic that flows within a standard CAPWAP access point deployment; that is, CAPWAP traffic between the CAPWAP access point and the CAPWAP controller.
- Wireless mesh data frame flow.
- AWPP exchanges.

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

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

Figure 8-13 shows an example of this type of framing. The source address of the frame is MAP:03:70, the destination address of this frame is the controller (the mesh network is operating in Layer 2 mode), the transmitter address is MAP:D5:60, and the receiver address is RAP:03:40.

Figure 8-13 Wireless Mesh Frame

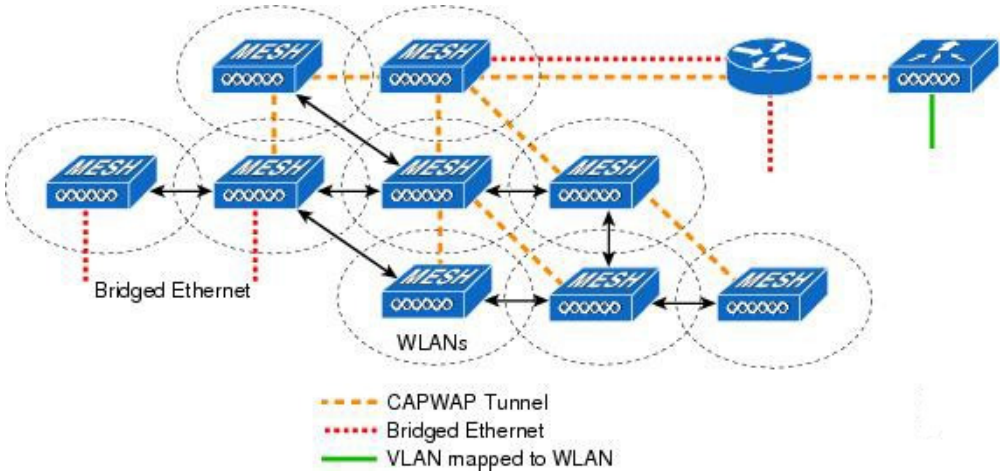


As this frame is sent, the transmitter and receiver addresses change on a hop-by-hop basis. AWPP is used to determine the receiver address at each hop. The transmitter address is known because it is the current mesh access point. The source and destination addresses are the same over the entire path.

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

Each mesh access point within the mesh forms an CAPWAP session with a controller. WLAN traffic is encapsulated inside CAPWAP and is mapped to a VLAN interface on the controller. Bridged Ethernet traffic can be passed from each Ethernet interface on the mesh network and does not have to be mapped to an interface on the controller (see Figure 8-14.)

Figure 8-14 Logical Bridge and WLAN Mapping

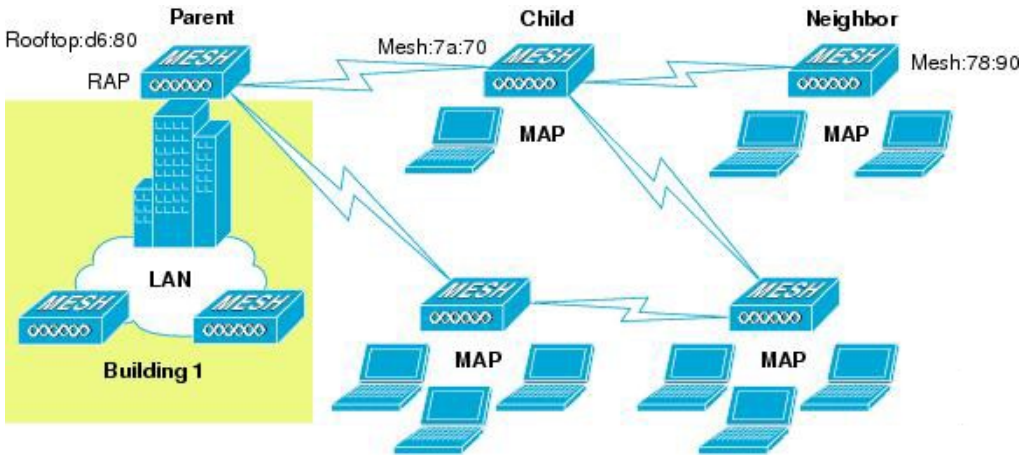


Mesh Neighbors, Parents, and Children

Relationships among mesh access points are as a parent, child, or neighbor (see Figure 8-15).

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

Figure 8-15 Parent, Child, and Neighbor Access Points



Criteria to Choose the Best Parent

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

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

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

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

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

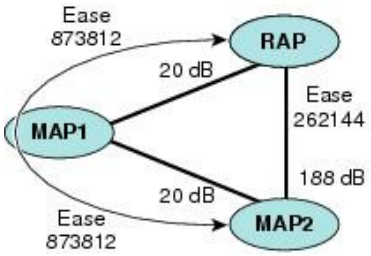
A parent mesh access point provides the best path back to a RAP. AWPP uses Ease to determine the best path. Ease can be considered the opposite of cost, and the preferred path is the path with the higher ease.

Ease Calculation

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

Figure 8-16 shows the parent path selection where MAP2 prefers the path through MAP1 because the adjusted ease value (436906) though this path is greater then the ease value (262144) of the direct path from MAP2 to RAP.

Figure 8-16 Parent Path Selection



Parent Decision

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

adjusted ease = min (ease at each hop) Hop count

SNR Smoothing

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

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

Loop Prevention

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

Mesh Deployment Modes

In a Cisco wireless outdoor mesh network, multiple mesh APs comprise a network that provides secure, scalable outdoor wireless LAN.

The three RAPs are connected to the wired network at each location and are located on the building roof. All the downstream APs 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 APs in 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 APs but it is not a mandatory requirement because CAPWAP sessions can be back hauled to a controller over a wide-area network (WAN).

Wireless Backhaul

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

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

Only 5 GHz backhaul is possible on all mesh APs except 1522 in which either 2.4 or 5 GHz radio can be configured as a backhaul radio (*see* Configuring Advanced Features).

Universal Access

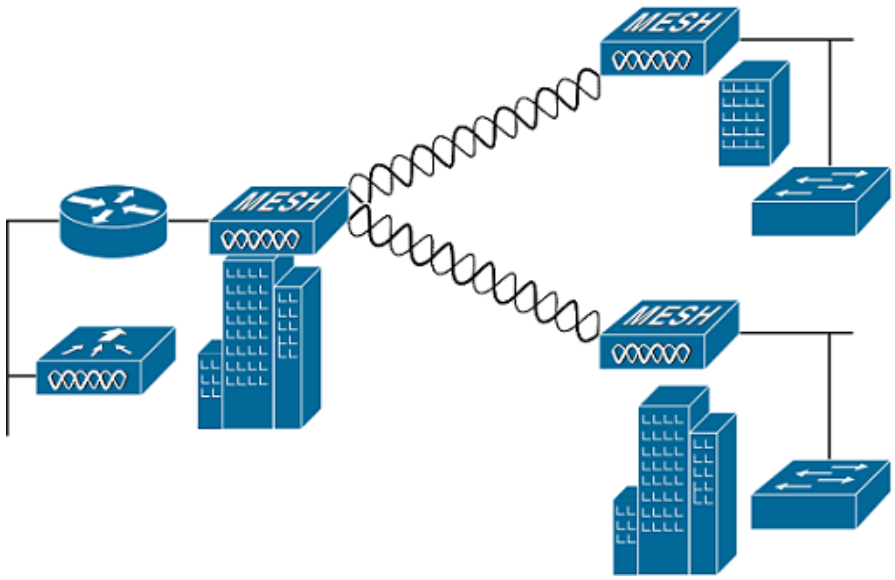
You can configure the backhaul on mesh APs to accept client traffic over its 802.11a radio. This feature is identified as Backhaul Client Access in the controller GUI (**Monitor > Wireless**). When this feature is disabled, backhaul traffic is transmitted only over the 802.11a or 802.11a/n radio and client association is allowed only over the 802.11b/g or 802.11b/g/n radio. For more information about the configuration, *see* Configuring Advanced Features.

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 8-17 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 8-17 Point-to-Multipoint 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. To enable Ethernet bridging using the controller GUI, choose **Wireless > All APs > Details** from the AP page, click the **Mesh** tab, and then check the **Ethernet Bridging** check box.

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

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

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.

To configure range parameters for longer links, choose **Wireless > Mesh**. Optimum distance (in feet) should exist between the root AP (RAP) and the farthest mesh AP (MAP). Range from the RAP bridge to the MAP bridge has to be mentioned in feet.

The following global parameter applies to all mesh APs when they join the controller and all existing mesh APs in the network:

- Range: 150 to 132,000 feet
- Default: 12,000 feet

Wireless Backhaul Data Rate

Backhaul is used to create only the wireless connection between the APs. The backhaul interface by default is 802.11a or 802.11a/n depending upon the AP. 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 AP than can higher data rates, for example 300 Mbps. As a result, the data rate affects cell coverage and consequently the number of APs 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.

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 technology can help to 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 Multiple-input multiple-output (MIMO) beamforming, transmit beamforming, 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. This 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. We intend to lead in this area going forward.

We realized that 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. In other words, for 802.11 a/g clients, some of the capabilities of the extra transmit path was lying idle. In addition, we realized that for many networks, the performance of the installed 802.11 a/g client base would be a limiting factor on the network.

To take advantage of this fallow capacity and greatly enhance overall network capacity by bringing 802.11 a/g clients up to a higher performance level, we created an innovation in transmit beamforming technology, called ClientLink.

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 AP to optimize the SNR exactly at the position where the client is placed. 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 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, ClientLink increases the overall capacity of the system, which means an efficient use of spectrum resources.

ClientLink in the 1552 APs is based on ClientLink capability available in AP3500s. Therefore, the AP has the ability to beamform well to nearby clients and to update beamforming information on 802.11ACKs. Therefore, even if there is no dedicated uplink traffic, the 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 APs.

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 APs, there is one difference between ClientLink for indoor 11n and ClientLink for outdoor 11n. For indoor 11n APs, SW limits the affected rates to 24, 36, 48, and 54 Mbps. This is done to avoid clients sticking to a faraway 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 APs, we do need more coverage. Thus, three more additional legacy data rates lower than 24 Mbps have been added. ClientLink for outdoors is applicable to legacy data rates of 6, 9, 12, 18, 24, 36, 48, and 54 Mbps.

Controller Planning

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

- Mesh APs (RAPs and MAPs) in the network.

- The wired network that connects the RAP and controllers can affect the total number of APs supported in the network. If this network allows the controllers to be equally available to all APs without any impact on WLAN performance, the APs 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 APs and coverage are reduced.
- Number of mesh APs (RAPs and MAPs) supported per controller.

For clarity, non-mesh APs are referred to as local APs in this document.

Table 8-11 Mesh AP Support by Controller Model

Controller Model	Local AP Support (nonmesh)[1]	Maximum Possible Mesh AP Support
5508[2]	500	500
2504[3]	50	50
WiSM2	500	500
5520	1500	1500
8510 & 8540	6k	6k

1. Local AP support is the total number of nonmesh APs supported on the controller model.
2. For 5508, controllers, the number of MAPs is equal to (local AP support - number of RAPs).
3. For 2504, controllers, the number of MAPs is equal to (local AP support - number of RAPs).

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.

Wireless Mesh Network Coverage Considerations

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

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

We always recommend that you perform a site survey before taking any real estimations for the area and creating a bill of materials.

Cell Planning and Distance

For the Cisco 1520 Series Access Points

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

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

- RAP-to-MAP ratio—Recommended maximum ratio is 20 MAPs per RAP.

- AP-to-AP distance—A spacing of no more than of 2000 feet (609.6 meters) between each mesh AP is recommended. When you extend the mesh network on the backhaul (no client access), use a cell radius of 1000 feet (304.8 meters).
- Hop count—Three to four hops. One square mile in feet (52802), is nine cells and you can cover one square mile with approximately three or four hops.
- For 2.4 GHz, the local access cell size radius is 600 feet (182.88 meters). One cell size is around 1.310 x 106, so there are 25 cells per square mile.

Collocating Mesh Access Points

The following recommendations provide guidelines to determine the required antenna separation when you collocate AP1500s on the same tower. The recommended minimum separations for antennas, transmit powers, and channel spacing are addressed.

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

You must follow antenna proximity requirements, which depend upon the adjacent and alternate adjacent channel usage.

Collocating AP1500s on Adjacent Channels

If two collocated AP1500s operate on adjacent channels such as channel 149 (5745 MHz) and channel 152 (5765 MHz), the minimum vertical separation between the two AP1500s is 40 feet (12.192 meters) (the requirement applies for mesh APs equipped with either 8 dBi omni-directional or 17 dBi high-gain directional patch antennas).

If two collocated AP1500s operate on channels 1, 6, or 11 (2412 to 2437 MHz) with a 5.5-dBi omni-directional antenna, then the minimum vertical separation is 8 feet (2.438 meters).

Collocating AP1500s on Alternate Adjacent Channels

If two collocated AP1500s operate on alternate adjacent channels such as channel 149 (5745 MHz) and channel 157 (5785 MHz), the minimum vertical separation between the two AP1500s is 10 feet (3.048 meters) (the requirements applies for mesh APs equipped with either 8-dBi omni-directional or 17-dBi high-gain directional patch antennas).

If two collocated AP1500s operate on alternate adjacent channels 1 and 11 (2412 MHz and 2462 MHz) with a 5.5-dBi omni-directional antenna, then the minimum vertical separation is 2 feet (0.609 meters).

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

CleanAir

The 1550 series leverages 802.11n technology with integrated radio and internal/external antennas. The 1550 series APs are based on the same chipset as the present CleanAir capable Aironet 3500 APs. In other words, the 1550 series APs are capable of doing CleanAir.

With the 7.3.101.0 Release, 2600 series APs can mesh with each other and can also provide CleanAir functionality.

With the 7.2.103.0 Release, 3600 series APs can mesh with each other and can also provide CleanAir functionality.

With the 7.0.116.0 Release, 3500 series APs can mesh with each other and can also provide CleanAir functionality.

CleanAir in mesh (1552, 2600, 3500 and 3600) can be implemented on the 2.4-GHz radio and provides clients complete 802.11n data rates while detecting, locating, classifying, and mitigating radio frequency (RF) interference. This provides a carrier class management and customer experience and ensures that you have control over the spectrum in the deployed location. CleanAir enabled RRM technology on the outdoor 11n platform detects, quantifies, and mitigates Wi-Fi and non-Wi-Fi interference on 2.4-GHz radios. AP1552 supports CleanAir in 2.4 GHz client access mode.

CleanAir Advisor

If CleanAir is enabled on a backhaul radio, CleanAir Advisor is activated. CleanAir Advisor generates Air Quality Index (AQI) and Interferer Detection Reports (IDR) but the reports are only displayed in the controller. No action is taken through event driven RRM (ED-RRM). CleanAir Advisor is only present on the 5-GHz backhaul radio of APs in bridge mode.

Wireless Mesh Mobility Groups

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

Multiple Controllers

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

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

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

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

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

The CAPWAP model used in the wireless mesh network is designed for campus networks; that is, it expects a high-speed, low-latency network between the CAPWAP mesh APs and the CAPWAP controller.

Increasing Mesh Availability

In the Cell Planning and Distance section, a wireless mesh cell of one square mile was created and then built upon. This wireless mesh cell has similar properties to the cells used to create a cellular phone network because the smaller cells (rather than the defined maximum cell size) can be created to cover the same physical area, providing greater availability or capacity. This process is done by adding a RAP to the cell. Similar to the larger mesh deployment, the decision is whether to use RAP on the same channel, as shown in Figure 8-18 or to use RAPs placed on different channels, as shown in Figure 8-19. The addition of RAPs into an area adds capacity and resilience to that area.

Figure 8-18 Two RAPs per Cell with the Same Channel

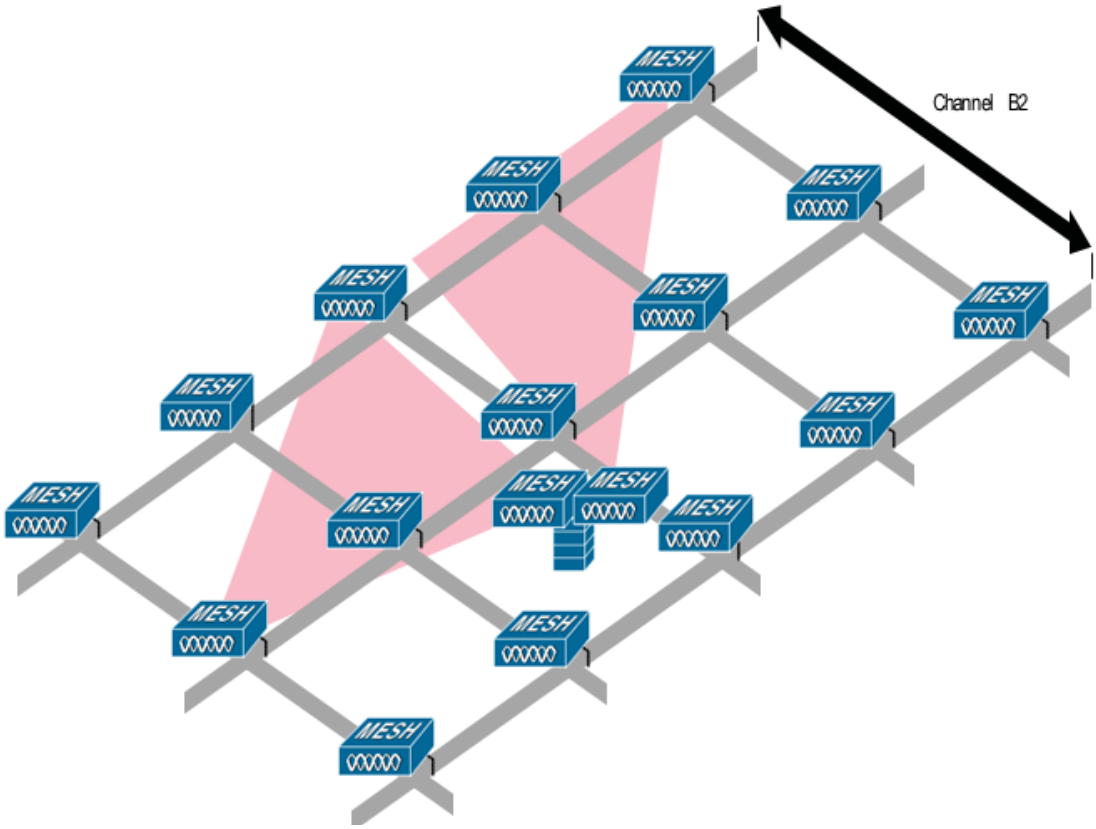
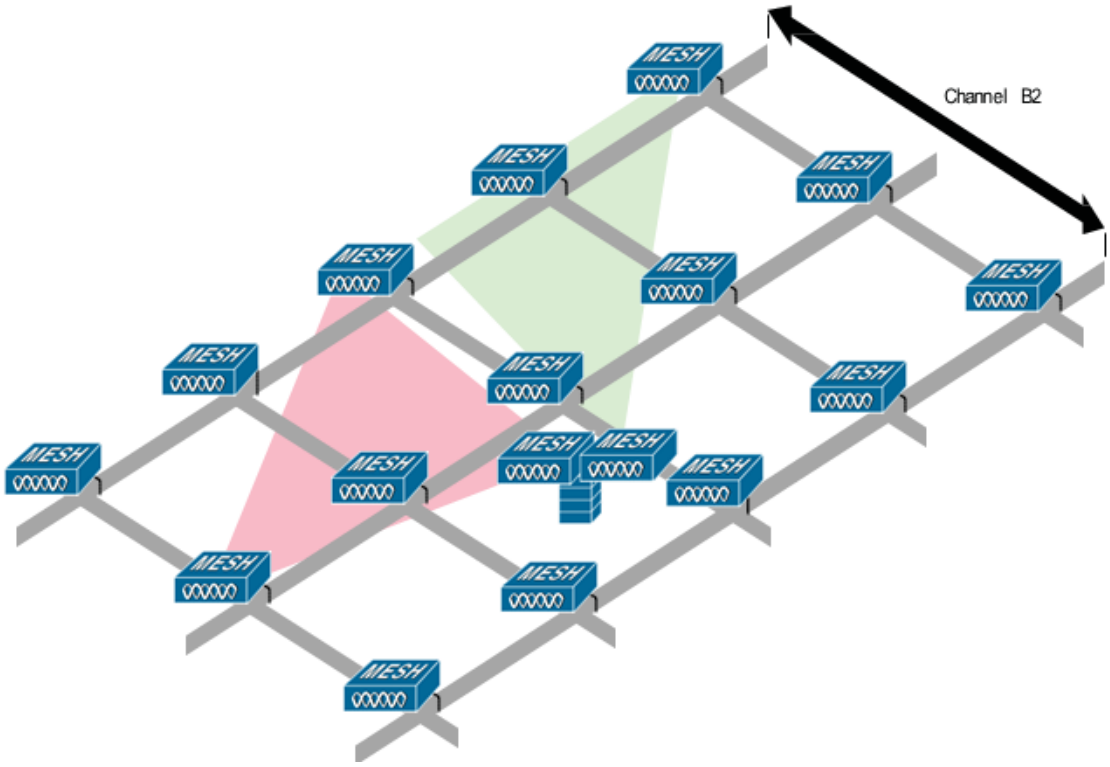


Figure 8-19 Two RAPs per Cell on Different Channels



Multiple RAPs

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

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

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

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

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

Indoor Mesh Interoperability with Outdoor Mesh

Complete interoperability of indoor mesh APs with the outdoor ones is supported. It helps to bring coverage from outdoors to indoors. We recommend indoor mesh APs for indoor use only, and these APs should be deployed outdoors only under limited circumstances as described below.

Caution The indoor APs in a third-party outdoor enclosure can be deployed for limited outdoor deployments, such as a simple short haul extension from an indoor WLAN to a hop in a parking lot. The 1240, 1250, 1260, 2600, 3500e, and 3600 APs in an outdoor enclosure is recommended because of its robust environmental and temperature specifications. Additionally, the indoor APs have connectors to support articulated antennas when the AP is within an outdoor enclosure. Exercise caution with the SNR values as they may not scale and long-term fades may take away the links for these APs when compared to a more optimized outdoor 1500 series AP.

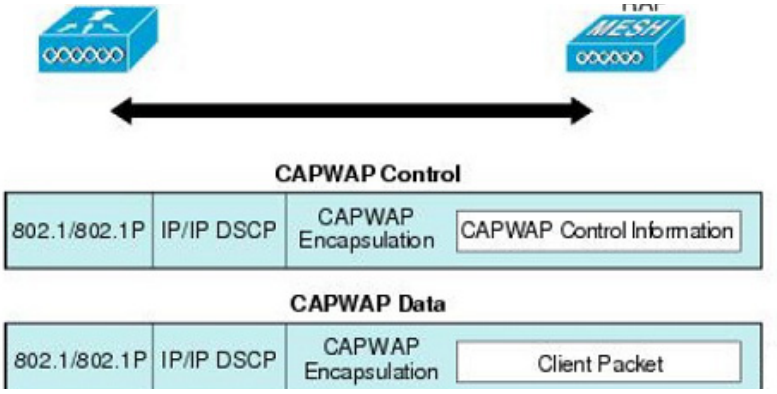
Mobility groups can be shared between outdoor mesh networks and indoor WLAN networks. It is also possible for a single controller to control indoor and outdoor mesh APs simultaneously. The same WLANs are broadcast out of both indoor and outdoor mesh APs.

Connecting the Cisco 1500 Series Mesh APs to the Network

This section describes how to connect the Cisco 1500 Series mesh APs to the network.

The wireless mesh terminates on two points on the wired network. The first location is where the RAP attaches to the wired network, and where all bridged traffic connects to the wired network. The second location is where the CAPWAP controller connects to the wired network; this location is where the WLAN client traffic from the mesh network connects to the wired network (see Figure 8-20). The WLAN client traffic from CAPWAP is tunneled at Layer 2, and matching WLANs should terminate on the same switch VLAN where the controllers are collocated. The security and network configuration for each of the WLANs on the mesh depend on the security capabilities of the network to which the controller is connected.

Figure 8-20 Mesh Network Traffic Termination



Note When an HSRP configuration is in operation on a mesh network, we recommend that the In-Out multicast mode be configured. For more details on multicast configuration, refer to the Cisco Mesh Access Points, Design and Deployment Guide.

Adding Mesh APs to the Mesh Network

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

Note The controller ports that connect to the mesh APs should be untagged.

Before adding a mesh AP to a network, perform the following:

Step 1 Add the MAC address of the mesh AP to the controller's MAC filter.

Step 2 Define the role (RAP or MAP) for the mesh AP.

Step 3 Verify that Layer 3 is configured on the controller.

Step 4 Configure a primary, secondary, and tertiary controller for each mesh AP. Configure a backup controller.

Step 5 Configure external authentication of MAC addresses using an external RADIUS server. See the Configuring External Authentication and Authorization Using a RADIUS Server.

Step 6 Configure global mesh parameters.

Step 7 Configure universal client access.

Step 8 Configure local mesh parameters.

Step 9 Configure antenna parameters.

Step 10 Configure channels for serial backhaul. This step is applicable only to serial backhaul APs.

Step 11 Configure the DCA channels for the mesh APs.

Step 12 Configure mobility groups (if desired) and assign controllers.

Step 13 Configure Ethernet bridging (if desired).

Step 14 Configure advanced features such as Ethernet VLAN tagging network, video, and voice.