Cisco Aironet 1552 Series for Hazardous Locations Installation Guide

April 2019

C O N T E N T S

Preface

This section describes the objectives, audience, organization, and conventions of the *Cisco Aironet 1552 Series for Hazardous Locations Installation Guide.*

Objectives

This publication explains the steps for installing the Cisco Aironet 1552 Series Outdoor Mesh Access Point for Hazardous Locations (called the *access point* in this document).

The 1552 model is a dual-radio platform that supports dual-band (2.4 GHz and 5 GHz) operation.

Audience

This publication is for the person installing and configuring an access point for the first time. The installer should be familiar with network structures, terms, and concepts.

⚠ **Warning** **Only trained and qualified personnel should be allowed to install, replace, or service this equipment.** Statement 1030

⚠ **Warning** **For Nordic countries (Norway, Finland, Sweden and Denmark) this system must be installed in a Restricted Access Location, where the voltage of the main ground connection of all equipment is the same (equipotential earth) and the system is connected to a grounded electrical outlet.** Statement 328

Organization

This guide contains the following sections:

Chapter	Title	Description
Chapter 1	Overview	Describes the major components and features of the access point.
Chapter 2	Before You Begin	Provides warnings, safety information, and mounting information you need to install your access point. The chapter contains a new section that provides information and procedures for mounting the access point in Class I, Division 2/Zone 2 hazardous locations.
Chapter 3	Installing the 1552 Series Access Points in Hazardous Locations	Describes the procedures for installing the different models of the access point.
Chapter 4	Troubleshooting	Provides basic troubleshooting procedures for the access point.
Appendix A	Translated Safety Warnings	Indicates how to access the document that provides translations of the safety warnings that appear in this publication.
Appendix B	Declarations of Conformity and Regulatory Information	Describes the regulatory conventions to which the access point conforms and provides guidelines for operating access points in Japan.
Appendix C	Channels and Power Levels	Indicates how to access the document that lists the access point radio channels and the maximum power levels supported by the world regulatory domains.
Appendix D	Access Point Specifications	Lists technical specifications for the access point.
Appendix E	Access Point Pinouts	Describes the connector pinouts for the access point.
Appendix F	Configuring DHCP Option 43	Describes the procedure to configure DHCP Option 43.

Conventions

This publication uses the following conventions:

Convention	Description
boldface font	Commands, command options, and keywords are in boldface.
italic font	Arguments for which you supply values are in italics.
[ ]	Elements in square brackets are optional.

Convention	Description
screen font	Terminal sessions and information the system displays are in screen font.
boldface screen font	Information you must enter is in boldface screen font.
italic screen font	Arguments for which you supply values are in italic screen font.
^	The symbol ^ represents the key labeled Control. For example, the key combination ^D in a screen display means hold down the Control key while you press the D key.
< >	Nonprinting characters, such as passwords, are in angle brackets.

Notes use the following conventions:

Note Means *reader take note.* Notes contain helpful suggestions or references to materials not contained in this manual.

Cautions use the following conventions:

Caution Means *reader be careful.* In this situation, you might do something that could result in equipment damage or loss of data.

Warnings use the following conventions:

Warning **IMPORTANT SAFETY INSTRUCTIONS**

This warning symbol means danger. You are in a situation that could cause bodily injury. Before you work on any equipment, be aware of the hazards involved with electrical circuitry and be familiar with standard practices for preventing accidents. Use the statement number provided at the end of each warning to locate its translation in the translated safety warnings that accompanied this device. Statement 1071

SAVE THESE INSTRUCTIONS

Related Documents

These documents provide complete information about the access point:

- *Release Notes for Cisco Wireless LAN Controllers and Lightweight Access Points*
- *Cisco Wireless LAN Controller Configuration Guide*
- *Cisco Aironet 1550 Series Outdoor Mesh Access Point Power Injector Installation Instructions*

Click this link to browse to the Cisco Wireless documentation home page:

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

To browse to the access point documentation, click **Cisco Aironet 1550 Series** listed under "Outdoor and Industrial Wireless." The documentation can be accessed from the Support box.

To browse to the Cisco Wireless LAN Controller documentation, click **Standalone Controllers** listed under "Wireless LAN Controllers." The documentation can be accessed from the Support box.

Finding the Product Serial Number

The access point serial number is on the bottom of the access point (refer to Figure 1).

Figure 1   *Location of Serial Number Label*
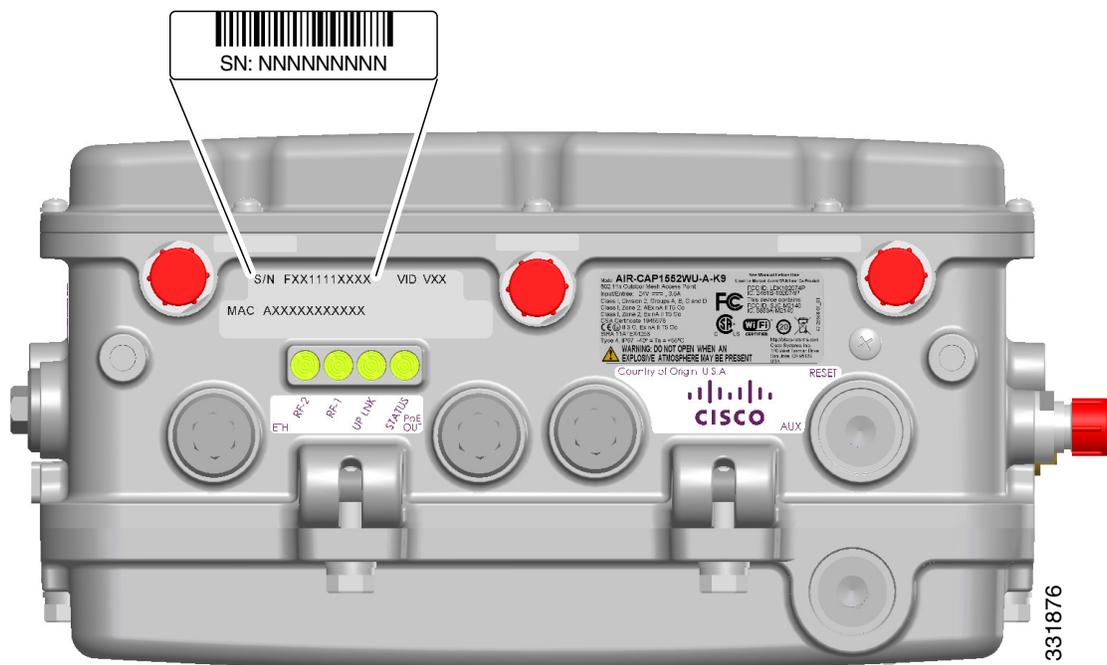
The access point serial number label contains the following information:

- Model number, such as AIR-CAP1552SA/SD-x-K9.
- Serial number, such as WCN0636279B (11 alphanumeric digits).
- Access point MAC address, for example 68BDABF54600 (12 hexadecimal digits). It is located under the serial number.

You will need your product serial number when requesting support.

Obtaining Documentation, Support, and Security Guidelines for the ISA100 Wireless and WirelessHART Multiprotocol Radio

The ISA100 Wireless and WirelessHART Multiprotocol Radio is supported by the Honeywell Process Solutions group. For support for this module, please contact Honeywell as per the information in the following link:

https://www.honeywellprocess.com/en-US/contact-us/customer-support-contacts/Pages/default.aspx

For information on obtaining documentation and support, providing documentation feedback, security guidelines, and recommended aliases and general Cisco documents, see the monthly *What's New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation, at:

http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html

To view all new wireless documentation, click on **Wireless**.

Obtaining Documentation, Support, and Security Guidelines for the WirelessHART Gateway

The WirelessHART Gateway is supported by Emerson Process Management.

Global Service Center

Software and Integration Support

1-800-833-8314 (United States)

+63-2-702-1111 (International)

Customer Central

Technical support, quoting, and order-related questions.

United States 1-800-999-9307 (7:00 am to 7:00 pm CST)

Asia Pacific +65-6777-8211

Europe/Middle East/ Africa +49-8153-9390

Outside of the United States, contact your local Emerson Process Management representative.

For information on obtaining documentation and support, providing documentation feedback, security guidelines, and recommended aliases and general Cisco documents, see the monthly *What's New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation, at:

http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html

To view all new wireless documentation, click on **Wireless**.

C H A P T E R 1

Overview

The Cisco Aironet 1552 Series Outdoor Mesh Access Point for Hazardous Locations (hereafter called the *access point* or *AP*) is a modularized wireless outdoor access point designed for use in a mesh network. The access point also supports wireless client access, point-to-point bridging, point-to-multipoint bridging, and point-to-multipoint mesh wireless connectivity.

About the Cisco 1552 Access Point

The 1552 access point supports two radios (2.4 GHz and 5 GHz) and provides client access without the need for a license. Depending on the radio, the access point can support 1 to 300 Mb/s data rates (for specific data rates, refer to Appendix D, "Access Point Specifications").

The 1552 access point supports the modularity of the 1520 series and allows flexibility in radio configuration. In addition to full interoperability with 802.11n clients, the 1552 access point interoperates with legacy clients and offers enhanced backhaul performance. The 1552 access point can also be configured with an integrated ISA100 Wireless and WirelessHART Multiprotocol Radio or WirelessHART Gateway.

The access point is a standalone unit that can be attached with a bracket or pole mounted with an optional kit. The access point can also operate as a relay node for other access points not directly connected to a wired network. Intelligent wireless routing is provided by the patented Cisco Adaptive Wireless Path Protocol (AWPP). This enables each 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 access point is configured, monitored, and operated through a Cisco wireless LAN controller (hereafter called a *controller*) as described in the *Cisco Wireless LAN Controller Configuration Guide*. The *Cisco Wireless Mesh Access Points, Design and Deployment Guide* describes how to plan and initially configure the Cisco mesh network, which supports wireless point-to-point, point-to-multipoint, and mesh deployments. The controllers use a browser-based management system, a command-line interface (CLI), or the Cisco Prime Network Management tool to manage the controller and the associated access points. The access point supports hardware-based advanced encryption standard (AES) encryption between wireless nodes to provide end-to-end security.

This chapter provides information on the following topics:

- Hardware Models, page 1-2
- Hardware Features, page 1-6
- Network Deployment Examples, page 1-21

Hardware Models

The model numbers (or part numbers) and configuration for the Cisco Aironet 1552 Outdoor Mesh Access Points for Hazardous Locations are described in Table 1-1. A detailed list of components supported by each 1552 access point model is shown in Table 1-2.

For a detailed description of the declarations of conformity and regulatory information for the 1552 access points refer to Appendix B, "Declarations of Conformity and Regulatory Information."

1552H Model

1552S Model

1552WU Model

Table 1-1   1552 Access Point Model Numbers and Descriptions

Model (or part number)	Configuration
AIR-CAP1552H-*x*-K9	Two-radio (2.4 GHz and 5 GHz) Hazardous Location (Haz Loc) version. This AP supports 3 external dual-band omnidirectional antennas. The antennas can be ordered with the model. An optional Small Form Factor Pluggable (SFP) fiber module can be ordered with the AP. The AP has the capability to receive and use an SFP fiber module. Countries (regulatory domains) represented by the variable *x* are described at:
	http://www.cisco.com/en/US/prod/collateral/wireless/ps5679/ps5861/product_data_sheet0900aecd80537b6a.html
	For specific regulatory domains supported by this model, refer to the product data sheet at:
	http://www.cisco.com/en/US/prod/collateral/wireless/ps5679/ps5861/product_data_sheet0900aecd80537b6a.html
AIR-CAP1552SA-x-K9 and AIR-CAP1552SD-x-K9	Two-radio (2.4 GHz and 5 GHz) modular version. This model supports three (3) external dual-band omnidirectional antennas. The antennas can be ordered with the model. This model also supports two ISA100 Wireless and WirelessHART Multiprotocol radios with 2 additional external omnidirectional antennas for connections to 802.15.4 sensor network transceivers. Countries (regulatory domains) represented by the variable *x* are described at:
	http://www.cisco.com/en/US/prod/collateral/wireless/ps5679/ps5861/product_data_sheet0900aecd80537b6a.html
	SA models support AC power input, and SD models require DC power.
	For specific regulatory domains supported by this model, refer to the product data sheet at:
	http://www.cisco.com/en/US/prod/collateral/wireless/ps5679/ps5861/product_data_sheet0900aecd80537b6a.html
AIR-CAP1552WU-x-K9	Two-radio (2.4 GHz and 5 GHz) modular version. This model supports six (6) external Wi-Fi antennas (Three 2.4 GHz and Three 5 GHz). This model also supports a WirelessHART radio for connections to 802.15.4 sensor network transceivers via a cable-attached 2.4 GHz antenna. Countries (regulatory domains) represented by the variable *x* are described at:
	http://www.cisco.com/en/US/prod/collateral/wireless/ps5679/ps5861/product_data_sheet0900aecd80537b6a.html
	For specific regulatory domains supported by this model, refer to the product data sheet at:
	http://www.cisco.com/en/US/prod/collateral/wireless/ps5679/ps5861/product_data_sheet0900aecd80537b6a.html

Table 1-2   Components of Each 1552 Access Point Model

	1552H	1552SA/1552SD	1552WU
Antennas	External	External	External
Fiber SFP	Yes	Yes	No
PoE Out Port **802.3af** (For example, an IP video camera or VOIP Phone)	When powered with PoE, the PoE Out port is not active.	Yes	Yes
Hazardous Locations Class 1 Div2/Zone2	Yes	Yes	Yes
Power Options	AC and PoE ✎ **Note** PoE In is not 802.3af. It cannot be powered by an IEEE 802.3af/at-based PoE Ethernet switch. It requires the dedicated Power Injector (AIR-PWRINJ1500-2=).	SA Model: AC SD Model: 24V DC	24 VDC

✎ **Note**   All models support 12 VDC power input, but this feature cannot be used in hazardous locations.

✎ **Note**   There is no battery backup option for these models.

Regulatory Domains

The "-*x*" in the 1552 model numbers represent the domain. For example, in AIR-CAP1552H-*x*-K9 the -*x* represents a regulatory domain for a specific country.

For specific regulatory domains supported by each 1552 access point model, refer to the Wireless LAN Compliance Status at:

http://www.cisco.com/en/US/prod/collateral/wireless/ps5679/ps5861/product_data_sheet0900aecd805 37b6a.html

To locate the 1552 access point models, click on **802.11abgn Mesh Access Points**.

Hardware Features

This section describes the hardware features of the 1552 access point models. The following hardware features are described in this section:

- Multiple Radio Operation, page 1-14
- Antenna Configurations, page 1-15
- Multiple Power Sources, page 1-19
- Ethernet (PoE) Ports, page 1-20
- Fiber Option, page 1-20
- Metal Enclosure, page 1-21
- Optional Hardware, page 1-21

Connectors

Figure 1-1 through Figure 1-6 show the access point connectors for each model. Figure 1-7 through Figure 1-9 show the external antenna Type N connectors.

✎ **Note**   The illustrations in this document show all available connections for the access point. Unused connections are capped with a connector plug to ensure the watertight integrity of the access point. Liquid-tight adapters are provided for connector openings, which can be installed before or after deploying the access point.

⚠ **Caution**   The liquid-tight adapter(s) supplied in the kit are IP68/69 certified with .200 to .350 diameter cables but not ATEX certified or hazardous locations compliant. The installer must use cable glands appropriate to the installation.

1552H

Figure 1-1   Access Point Model AIR-CAP1552H-x-K9 Bottom Connectors
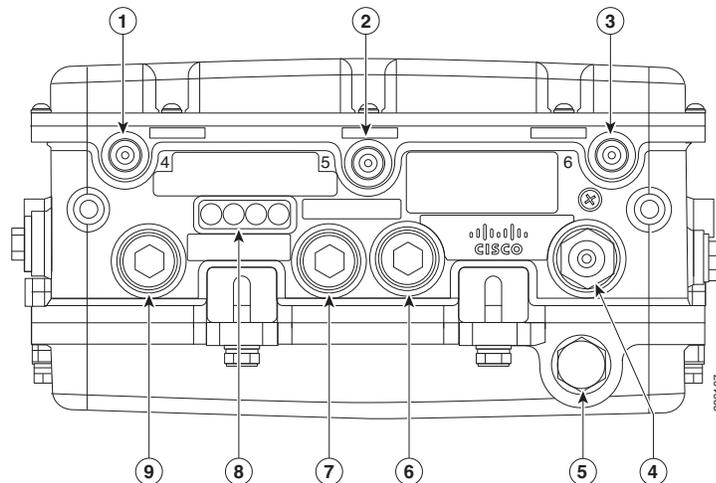
1	Antenna port 4	6	Fiber port (PG 13.5 thread)
2	Antenna port 5	7	PoE Out port (PG 13.5 thread)
3	Antenna port 6	8	LEDs (Status, Up Link, RF1, RF2)
4	AC power entry port (1/2-NPT thread) for model AIR-CAP1552H-*x*-K9 only or Cable Gland entry (1/2-NPT thread)	9	PoE In port (PG 13.5 thread) for data cable (outdoor cat 5 STP cable)
5	Not used		

Note   Antenna ports 1, 2, and 3 are not shown in Figure 1-1. These ports are reserved for future use and are located on the top of the access point.

1552SA/SD

Figure 1-2   Access Point Model AIR-CAP1552SA/SD-x-K9 Bottom Connectors
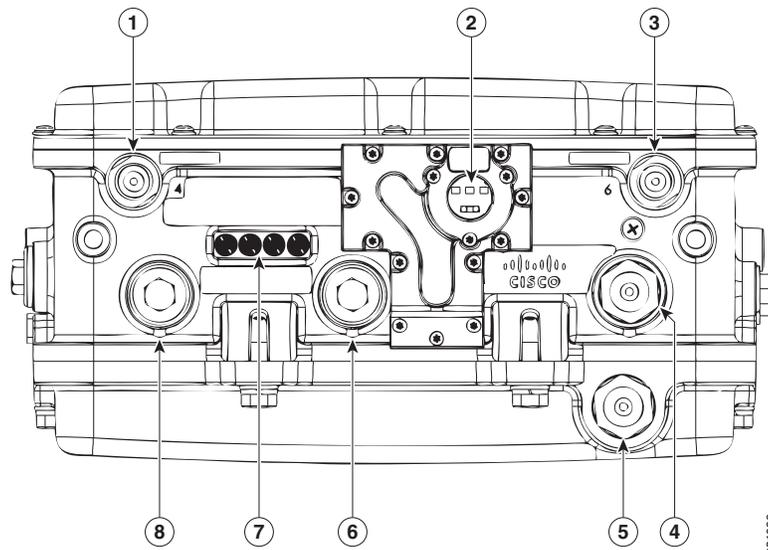
1	Antenna port 4 (ISA100 Wireless and WirelessHART)	5	Not used
2	IR window	6	PoE Out port - (PG13.5 Thread)
3	Antenna port 6 (ISA100 Wireless and WirelessHART RX)	7	LEDs (Status, Up Link, RF1, RF2)
4	AC (1552SA) or 24 VDC (1552SD) power input port and fiber backhaul port - (1/2NPT thread)	8	Copper Ethernet - (PG13.5 Thread)

1552WU

Figure 1-3   *Access Point Model AIR-CAP1552WUx-K9 Bottom Connectors*
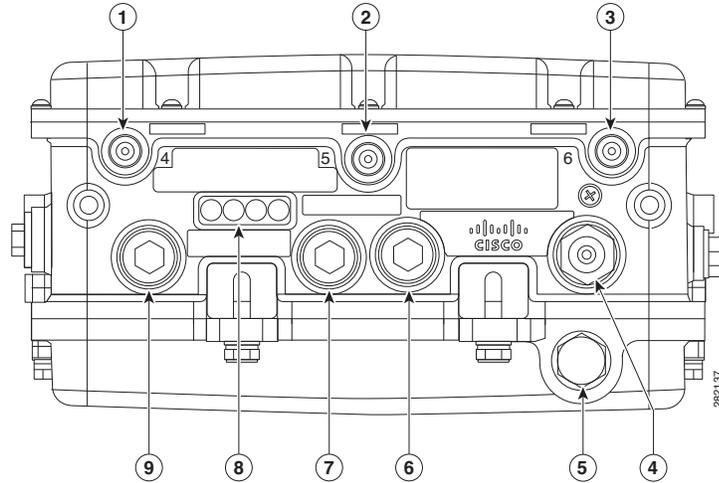
1	Antenna port 4 - 2.4 GHz Tx/Rx	6	Not Used
2	Antenna port 5- 2.4 GHz Rx	7	PoE Out port (PG 13.5 thread)
3	Antenna port 6- 2.4 GHz Tx/Rx	8	LEDs (Status, Up Link, RF1, RF2)
4	24 VDC power input port or Cable Gland entry (1/2-NPT thread)	9	Ethernet (PG 13.5 thread) for data cable (outdoor cat 5 STP cable)
5	Not used		

Console Connector

Figure 1-4   *Console Port for Access Point Model AIR-CAP1552H-x-K9 and*
                    AIR-CAP1552SA/SD-x-K9
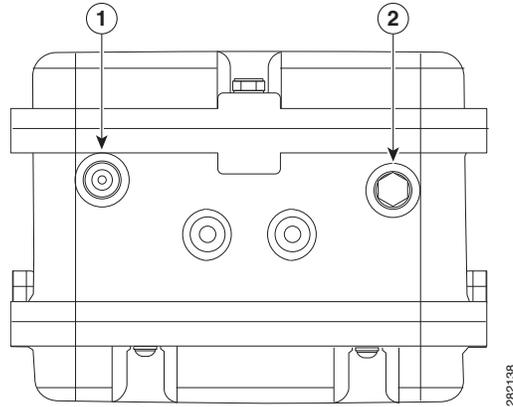
1	Console port	**2**	Not used on the H model, Fiber port on the S model. (5/8-24UNEF-2B)

Figure 1-5   *Console Port for Access Point Model AIR-CAP1552WU-x-K9*
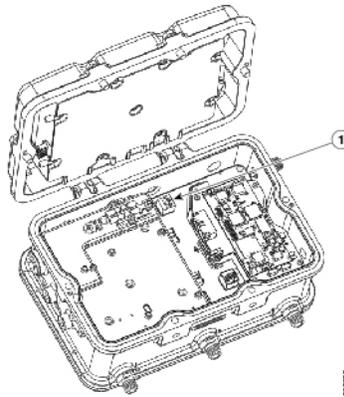
1	Console port (internal on the 1552WU)

DC Power Connector

Figure 1-6   *Access Point DC Power Connector and Ground Lug (All Models)*
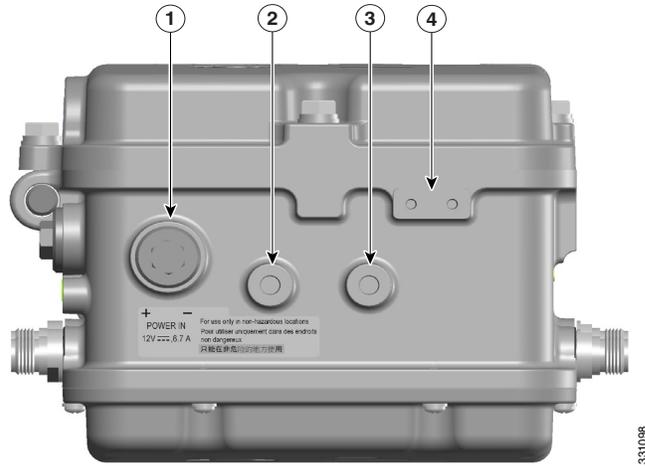
1	12 VDC non-hazardous locations input port (PG 13.5 thread size)	3	Bracket mounting hole (M8x1.25 x 12mm dp)
2	Bracket mounting hole (M8x1.25 x 12mm dp)	4	Ground lug location (connection for earth grounding (minimum VD 16 mm, 6 awg) (M4x.7 .30 THD Depth)

1552 Antenna Ports

Figure 1-7 shows the antenna port locations for model AIR-CAP1552H-*x*-K9.

Figure 1-7   External Antenna Port Locations for Access Point Model AIR-CAP1552H-x-K9
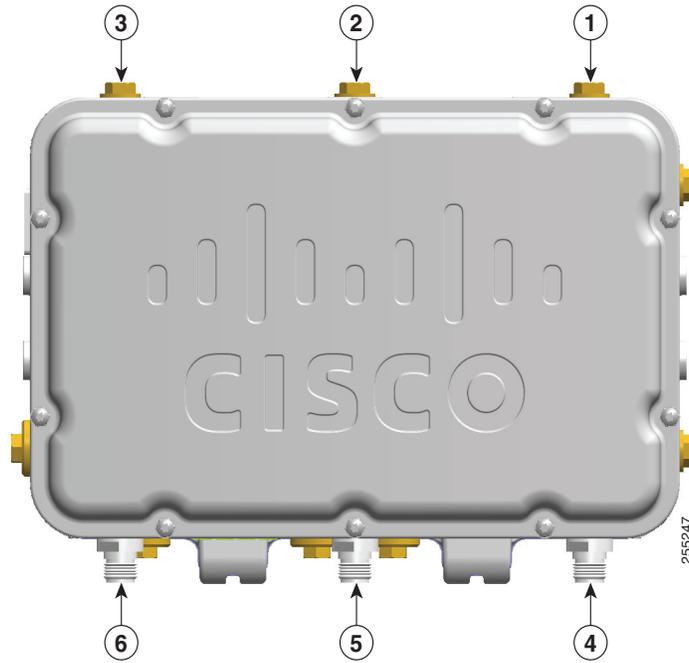
1	Not used	4	Antenna port 6- Type N connector 2.4/5 GHz Tx/Rx
2	Not used	5	Antenna port 5 - Type N connector 2.4/5 GHz Rx
3	Not used	6	Antenna port 4- Type N connector 2.4/5 GHz Tx/Rx

1552SA/SD Antenna Ports

Figure 1-8 shows the antenna port locations for model AIR-CAP1552SA/SD-*x*-K9.

Figure 1-8   *External Antenna Port Locations for Access Point Model AIR-CAP1552SA/SD-x-K9*

1	Antenna port 1- Type N connector Wi-Fi 2.4/5 GHz TX/RX	4	Antenna port 6- Type N connector ISA100 Wireless and WirelessHART 2.4 GHz TX/RX
2	Antenna port 2- Type N connector Wi-Fi 2.4/5 GHz RX	5	Antenna port 4- Type N connector ISA100 Wireless and WirelessHART 2.4 GHz RX
3	Antenna port 3- Type N connector Wi-Fi 2.4/5 GHz TX/RX		

1552WU Antenna Ports

Figure 1-9 shows the antenna port locations for model AIR-CAP1552WU-*x*-K9.

Figure 1-9   *External Antenna Port Locations for Access Point Model AIR-CAP1552WU-x-K9*
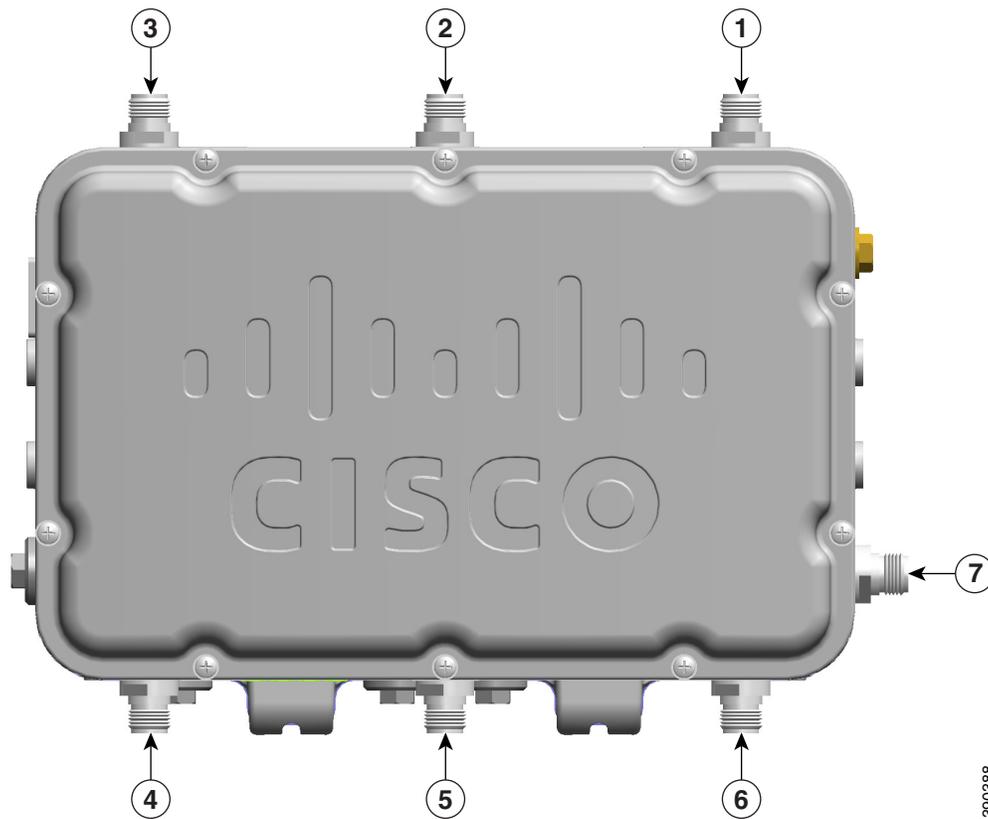
1	Antenna port 1 - Type N connector Single Band 5 GHz TX/RX	4	Antenna port 4 - Type N connector Single Band 2.4 GHz TX/RX
2	Antenna port 2 - Type N connector Single Band 5 GHz RX	5	Antenna port 5 - Type N connector Single Band 2.4 GHz RX
3	Antenna port 3 - Type N connector Single Band 5 GHz TX/RX	6	Antenna port 6 - Type N connector Single Band 2.4 GHz TX/RX
		7	WirelessHART Antenna port - Type N connector Single Band 2.4 GHz Omnidirectional WirelessHART Antenna TX/RX

Multiple Radio Operation

The 1552 access point supports simultaneous dual-radio operation using a 2.4 GHz 802.11b/g/n multiple input/multiple output (MIMO) radio and a 5 GHz 802.11a/n MIMO radio. The 2.4 GHz radio supports channels 1 to 11 in US, 1 to 13 in Europe, and 1 to 13 in Japan. It has two transmitters with a maximum total output power of 28 dBm for 802.11b/g/n operation. Output power is configurable to 5 levels. It has three receivers that enable maximum-ratio combining (MRC).

The 5 GHz radio operates in the UNII-2 band (5.25 – 5.35 GHz), UNII-2 Extended/ETSI band (5.47 – 5.725 GHz), and the upper ISM band (5.725 – 5.850 GHz). It has two transmitters with a maximum total output power of 22 dBm for the UNII-2 and UNII-2 Extended/ETSI bands. The total maximum output power for the upper UNII-3 band is 28 dBm. Output power is configurable for 5 power levels in 3 dB steps. The three receivers enables maximum-ratio combining (MRC).

Antenna Configurations

The 1552H, 1552SA/1552SD, and 1552WU models must always be operated with all the external antennas attached or the antenna connectors sealed with plugs. Figure 1-7, Figure 1-8, and Figure 1-9 show the antenna port locations.

Table 1-3   *Cisco Aironet Dual-Band Omnidirectional Antenna Supported Models and configuration information*

Part Number	Description	Gain	Number of Antennas		
			1552H	1552SA/ 1552SD	1552WU
AIR-ANT2547V-N-HZ	Dual Band 2.4/5 GHz Omnidirectional Wi-Fi Antenna	2.4 GHz: 4 dBi 5 GHz: 7 dBi	3	3	
AIR-ANT2450V-N-HZ	Single Band 2.4 GHz Omnidirectional ISA100 Wireless and WirelessHART Antenna	5 dBi		2	
AIR-ANT2480V-N	Single Band 2,4 GHz Omnidirectional Wi-Fi Antenna	8 dBi			3
AIR-ANT5180V-N	Single Band 5 GHz Omnidirectional Wi-Fi Antenna	8 dBi			3 See Note below
AIR-ANT5114P2M-N=	Single Band 5 GHz Directional Dual Polarized Patch Antenna	14 dBi			1 See Note below
(separately available from Emerson)	Single Band 2.4 GHz Omnidirectional WirelessHART Antenna	6 dBi			1

Note   Either the AIR-ANT5180V-N or the AIR-ANT5114P2M-N= antenna must be used, but not both on the 1552WU.

Note
- The WirelessHART Antenna must be installed a minimum of 3 feet from any other antenna, including the other Wi-Fi antennas attached to the Access Point.
- Follow all safety precautions when installing the antennas. For information on safety, refer to "Safety Precautions"section on page 1-18.

Figure 1-10   *Cisco Aironet Dual-Band Omnidirectional Antenna - Installed on Model AIR-CAP1552H-x-K9*

1	Antenna connected to antenna port 4 (Type N connector) (Wi-Fi TX/RX)
2	Antenna connected to antenna port 5 (Type N connector) (Wi-Fi RX)
3	Antenna connected to antenna port 6 (Type N connector) (Wi-Fi TX/RX)

Figure 1-11   *Cisco Aironet Dual-Band Omnidirectional Antenna and Cisco Aironet 2.4 GHz Omnidirectional Antenna - Installed on Model AIR-CAP1552SA/SD-x-K9*

1	Antenna port 1- Type N connector Wi-Fi 2.4/5 GHz TX/RX	4	Antenna port 6- Type N connector ISA100 Wireless and WirelessHART 2.4 GHz TX/RX
2	Antenna port 2- Type N connector Wi-Fi 2.4/5 GHz RX	5	Antenna port 4- Type N connector ISA100 Wireless and WirelessHART 2.4 GHz RX
3	Antenna port 3- Type N connector Wi-Fi 2.4/5 GHz TX/RX		

Figure 1-12   AIR-CAP1552WU-x-K9 Antenna Configurations.
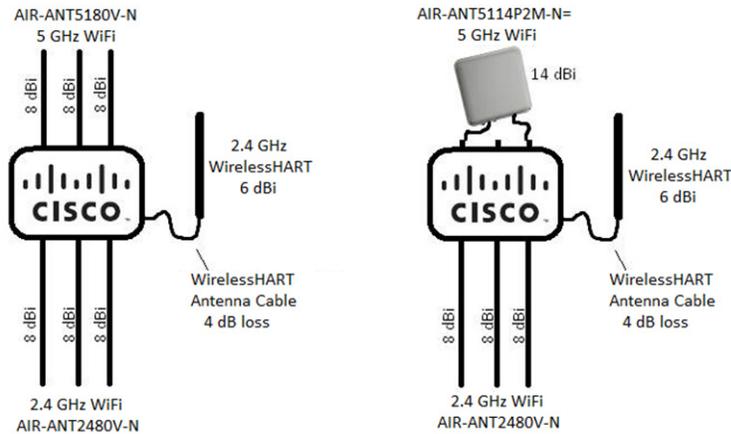
Safety Precautions

⚠️ **Warning**   Do not locate the antenna near overhead power lines or other electric light or power circuits, or where it can come into contact with such circuits. When installing the antenna, take extreme care not to come into contact with such circuits, as they may cause serious injury or death. For proper installation and grounding of the antenna, please refer to national and local codes (e.g. U.S.: NFPA 70, National Electrical Code, Article 810, Canada: Canadian Electrical Code, Section 54). Statement 280

For your safety, read and follow these safety precautions.

1. Before you install an antenna, contact your Cisco account representative to explain which mounting method to use for the size and type of antenna that you are about to install.

2. Select your installation site with safety, as well as best performance, in mind. Remember that electric power lines and phone lines look alike. For your safety, assume that any overhead line can kill you.

3. Contact your electric power company. Tell them your plans and ask them to come look at your proposed installation.

4. Plan your installation carefully and completely before you begin. Each person involved in an installation should be assigned to a specific task and should know what to do and when to do it. One person should be in charge of the operation to issue instructions and watch for signs of trouble.

5. When installing your antenna, follow these guidelines:

   – Do not use a metal ladder.

   – Do not work on a wet or windy day.

   – Do dress properly—wear shoes with rubber soles and heels, rubber gloves, and a long-sleeved shirt or jacket.

6. If the assembly starts to drop, move away from it and let it fall. Because the antenna, mast, cable, and metal guy wires are all excellent conductors of electrical current, even the slightest touch of any of these parts to a power line completes an electrical path through the antenna and the installer.

7. If any part of the antenna system should come in contact with a power line, do not touch it or try to remove it yourself. Call your local power company to have it removed safely.

8. If an accident should occur with the power lines, call for qualified emergency help immediately.

Multiple Power Sources

The 1552 series access point for hazardous locations support multiple power options. All models support 12 VDC, but not in a hazardous locations environment.

1552H and 1552SA

100 to 240 VAC, 50-60Hz

1552H

Power-over-Ethernet (PoE)—56 VDC power injector (AIR-PWRINJ1500-2=)

⚠️
Caution   Caution: Power injector (AIR-PWRINJ1500-2=) is not certified for installation within hazardous locations environments.

1552SD and 1552WU

24 VDC

⚠️
Warning   **Connect the unit only to DC power source that complies with the safety extra-low voltage (SELV) requirements in IEC 60950 based safety standards.** Statement 1033

✎
Note   This warning only applies to DC input sources and is not applicable if an AC power source is used.

The 1552 access point for hazardous locations can be connected to more than one power source. The access point detects the available power sources and switches to the preferred power source using the following priority:

1. AC power or 24 VDC, either but not both at the same time.

2. 12 VDC (not supported in hazardous locations environments)

3. Power over Ethernet (1552H only)

⚠️
Warning   **This unit might have more than one power supply connection. All connections must be removed to de-energize the unit.** Statement 1028

⚠️
Caution   To provide inline PoE, you must use the 1500 power injector (AIR-PWRINJ1500-2=). Other power injectors, PoE switches, and 802.3af/at power sources cannot provide adequate power, which can cause the access point to malfunction and cause over-current conditions at the power source.

⚠️
Caution   The 1500 power injector (AIR-PWRINJ1500-2=) must be used in an indoor environment only, and is not certified for installation within hazardous locations environments.

Note   The Ethernet cable from the power injector to the access point (PoE In port) must be at least 10 ft (3.1 m) in length.

Caution   When the access point is installed outdoors or in a wet or damp location, the AC branch circuit that is powering the access point should be provided with ground fault protection (GFCI), as required by Article 210 of the National Electrical Code (NEC). (1552H and 1552SA, not for 1552SD and 1552WU)

Ethernet (PoE) Ports

Caution   Power injector (AIR-PWRINJ1500-2=) is not certified for installation within hazardous locations environments.

Note   The 1552SA, 1552SD, and 1552WU access points do not support the PoE In port.

The 1552 hazardous location access points support an Ethernet uplink port and a downlink port (PoE Out). The 1552H access point also supports PoE In. The access point Ethernet ports use RJ-45 connectors (with a liquid tight adapter) to link the access point to the 10/100/1000BASE-T network. The Ethernet cable is used to send and receive Ethernet data and to optionally supply inline 56 VDC power from the power injector.

Note   When a 1552H access point is powered by PoE, the PoE Out port is not active.

The access point PoE Out (10/100/1000BASE-T) port uses an RJ-45 connector to provide LAN connectivity and IEEE 802.3af power to a single peripheral customer device, such as a camera or sensor gateway. The PoE Out port should not be connected to a switch or hub. The Ethernet MAC addresses are printed on the bottom of the access point under the LEDs.

Warning   **To reduce the risk of fire, use only No. 26 AWG or larger telecommunication line cord.** Statement 1023

The Ethernet cable must be a shielded outdoor rated Category 5e (CAT5e) or better cable. The access point senses the Ethernet and power signals and automatically switches internal circuitry to match the cable connections.

Caution   To provide inline PoE, you must use the 1500 power injector (AIR-PWRINJ1500-2=). Other power injectors, PoE switches, and 802.3af/at power sources cannot provide adequate power, which may cause the access point to malfunction and cause possible over-current conditions at the power source.

Fiber Option

Note   The 1552WU access point does not support Fiber.

Warning   **Class 1 laser product.** Statement 1008

The factory-orderable fiber option provides a fiber input and output capability. Fiber data is transmitted and received over a single or dual-strand fiber cable, depending on the SFP, which is connected to the access point using these SFP modules:

- 100BASE-BX10-U fiber rugged small-form factor pluggable (SFP) module
- 1000BASE-LX single-mode rugged SFP module
- 1000Base-SX multimode Rugged SFP module

Note   SFP modules are not hot-swappable.

The 1552H and 1552S have one SFP port for fiber use, located on the bottom of the unit. The 1552H is shown on Figure 1-1, and the 1552S is shown in Figure 1-2. Client data is passed to the network controller through the fiber connection via a fiber-capable switch or controller. Configuration information can be found in the controller configuration guide of the switch or controller you are using.

Metal Enclosure

The access point uses a metal enclosure that can accommodate both indoor or outdoor operating environments and an industrial temperature operating range of –40 to 131°F (–40 to 55°C). The access point complies with NEMA 4 and IP67 requirements.

Optional Hardware

Depending on the order configuration, the following optional access point hardware may be part of the shipment:

- Cisco Aironet Antennas
- Pole mount kits (AIR-ACCPMK1550=, AIR-ACCPMK1550HZM=)
- Band installation tool for pole mount kit (AIR-BAND-INS-TL=)
- Power injector (AIR-PWRINJ1500-2=)

Caution   Caution: Power injector (AIR-PWRINJ1500-2=) is not certified for installation within hazardous locations environments.

- 1000BASE-LX single-mode rugged SFP (GLC-LX-SM-RGD=)
- 1000BASE-SX multimode rugged SFP (GLC-SX-MM-RGD=)

Network Deployment Examples

The access point is a wireless device designed for wireless client access and point-to-point bridging, point-to-multipoint bridging, and point-to-multipoint mesh wireless connectivity. The access point provides 5 GHz backhaul capability to link with another access point to reach a wired network connection or to provide repeater operations for other access points.

The access point plays two primary radio roles: a root access point (RAP) or a mesh (non-root) access point (MAP), which is the default role of all access points. When the access point has a fiber or wired Ethernet or cable connector connection to the controller (through a switch), the radio role is called a

RAP. In order to be considered a RAP, the access point must be configured as a RAP. A RAP is a parent node to any bridging or mesh network. A controller can support one or more RAPs, each one parenting the same or different wireless networks. There can be more than one RAP for the same mesh network for redundancy. RAPs and MAPs can support wireless clients on the 2.4 GHz and 5 GHz band. Client access on 5 GHz is called universal client access.

When the access point does not have a wired Ethernet, fiber-optic, or cable connection to the controller, the radio role is called a MAP. The MAPs have a wireless connection (through the backhaul interface) to other MAPs and finally to a RAP with an Ethernet or cable connection through a switch to the controller. MAPs can also have a wired Ethernet connection to a local LAN and serve as a bridge endpoint for that LAN (using a point-to-point or point-to-multipoint bridge connection).

Wireless Backhaul

The access point supports wireless backhaul capability. Depending on the version of software being used, these links can utilize either 2.4 GHz or 5 GHz as of (8.2.100 and above) to bridge to another access point to reach a wired network connection to a controller (see Figure 1-13). The access point connected to the wired network is considered a RAP in this configuration. The remote access point is considered a MAP and transfers wireless client traffic to the RAP for transfer to the wired network. Control And Provisioning of Wireless Access Points (CAPWAP) control traffic is also transferred over this bridged link.

Figure 1-13   Access Point Backhaul Example
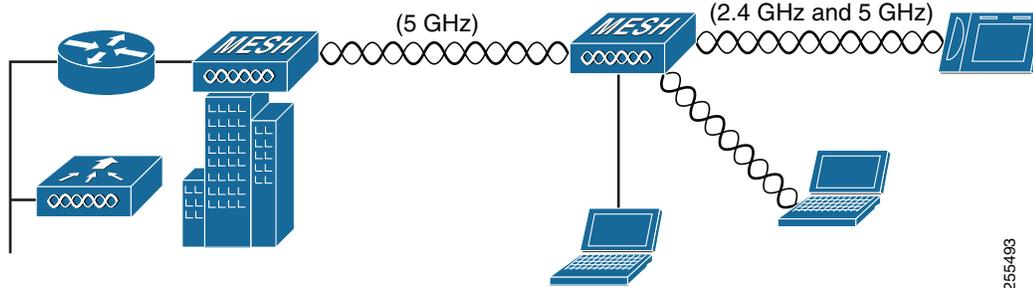
Point-to-Point Bridging

The access points can be used to extend a remote network by using the 2.4 GHz or 5 GHz backhaul radio to bridge the two network segments as shown in Figure 1-14. To support Ethernet bridging, you must enable bridging on the controller for each access point. By default this capability is turned-off for all access points.

Wireless client access is supported; however, if bridging between tall buildings, the 2.4 GHz wireless coverage area may be limited and possibly not suitable for direct wireless client access.

Figure 1-14   Access Point Point-to-Point Bridging Example
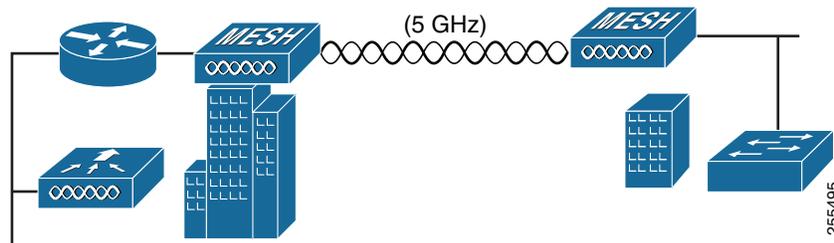
Point-to-Multipoint Bridging

The access points can be used as a RAP to connect multiple remote MAPs with their associated wired networks, or with 2.4 GHz or 5 GHz radio. By default this capability is turned-off for all access points. To support Ethernet bridging, you must enable bridging on the controller for each access point. Wireless client access can be provided over the bridging link; however, if bridging between tall buildings, the 2.4 GHz wireless coverage area may be limited and possibly not suitable for direct wireless client access. Figure 1-15 illustrates an example of access point-to-multipoint bridging.

Figure 1-15   Access Point to Multipoint Bridging Example
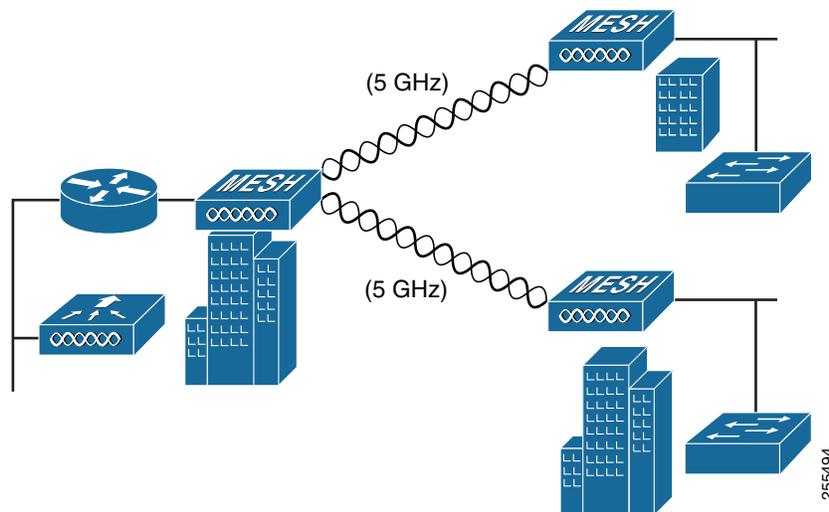
Point-to-Multipoint Mesh Network

The access point is typically deployed in a mesh network configuration. In a typical mesh deployment, one or more RAPs have a wired network connection through a switch to a controller. Other remote MAPs without wired network connections use the backhaul feature to optimally link to a RAP that is connected to the wired network. In the mesh network, the links between the access points are referred to as the *backhaul links*. Depending on the version of software being used, these links can utilize either 2.4 GHz or 5 GHz as of (8.2.100 and above).

Intelligent wireless routing is provided by the Adaptive Wireless Path protocol (AWPP). This enables each MAP to identify its neighbors and intelligently choose the optimal path to the RAP with the wired network connection by calculating the cost of each path in terms of signal strength and the number of hops required to get to a controller with signal strength given priority since signal strength determines the data rate available for backhaul.

Figure 1-16 illustrates a typical mesh configuration using MAPs and RAPs.

Figure 1-16   ***Typical Mesh Configuration Using Cisco 1552SA/1552SD Access Points with Sensors***
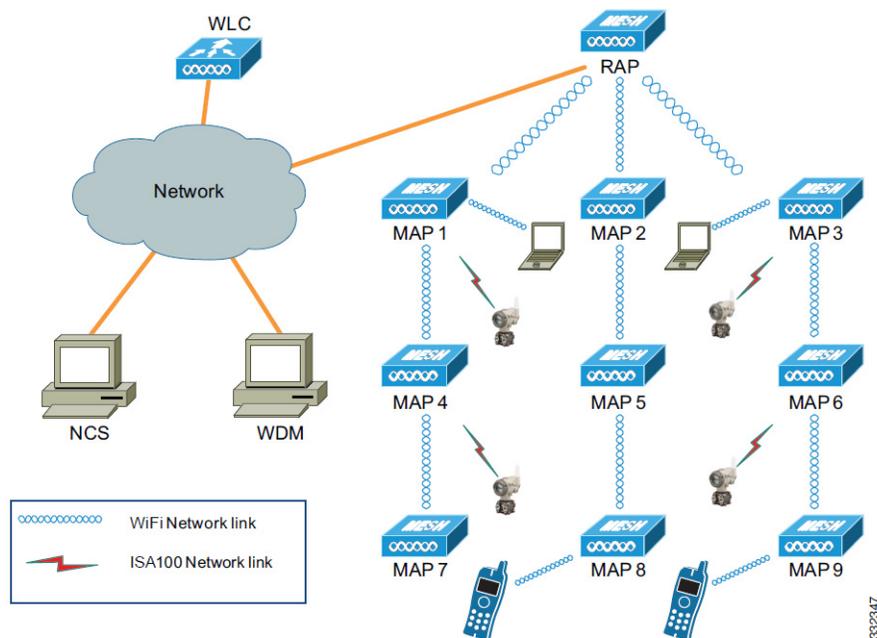
The Cisco 1552SA/1552SD is a universal and multifunctional outdoor wireless mesh network that supports not only Wi-Fi devices and applications, but also supports wireless field I/Os and actuators on both ISA100 Wireless and WirelessHART protocols.

Along with robust and reliable Cisco Outdoor Wi-Fi wireless mesh, it also creates parallel Industrial Wireless Automation Network to support field sensors and actuators running on either or both of the two protocols. The Multiprotocol Radio module manages and aggregates Industrial Wireless Data and passes it over to the Cisco Wireless Mesh backbone

Refer to Cisco Documentation for installation, configuration, best practices and troubleshooting guides.

Refer to to Honeywell OneWireless Network - Multiprotocol Wireless IO & System documentation for further details.

WirelessHART Gateway Configuration

This following information is abbreviated and is intended only to serve as a introduction. Refer to Emerson's WirelessHART Gateway documentation for complete details.

Figure 1-17   Typical Mesh Configuration Using Cisco 1552WU Access Points with Sensors
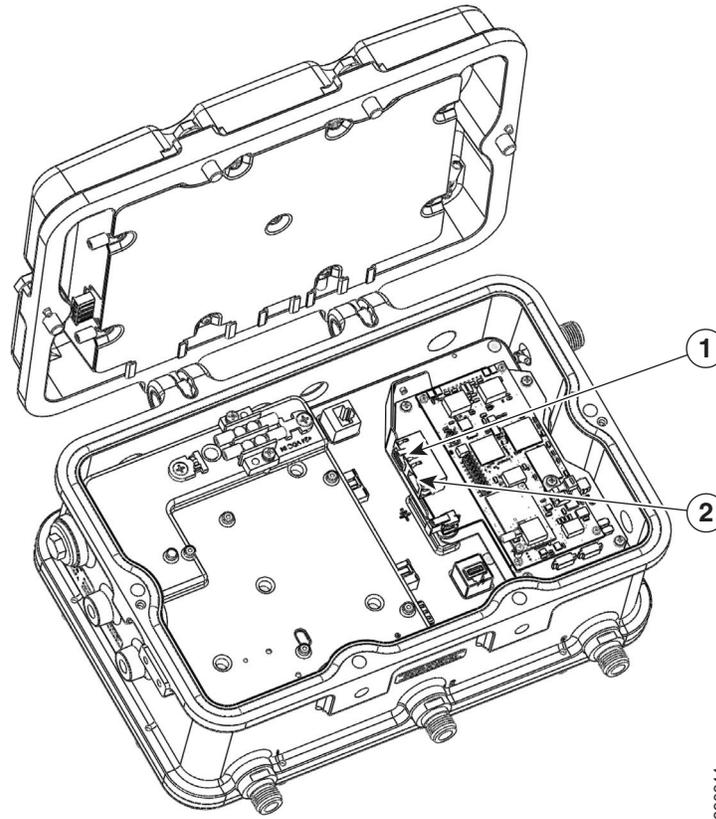
Table 1-4   The default IP addresses for the WirelessHART Gateway are:

	IP Address	Netmask	Notes
Ethernet 1	192.168.1.10	255.255.255.0	Connected to 1552WU internal interface GigabitEthernet2
Ethernet 2	192.168.2.10	255.255.255.0	User accessible. Can be used for connecting redundant WirelessHART Gateways.

The WirelessHART Gateway can be configured using a standard web browser and accessing the Gateway's internal webpage URL (https://192.168.1.10). For this to work, the 1552WU must be configured to pass traffic to the WirelessHART Gateway's IP address.

Table 1-5   Security Passwords

There are four role based user accounts for the gateway with varying levels of access. The table below describes this access.

Role	User Name	Web Interface Access
Executive	exec	Read-only access
Operator	oper	Read-only access
Maintenance	maint	Configure HART® device settings
		Configure Modbus communications
		Configure Modbus register mapping
		Configure OPC browse tree
		Configure Active Advertising
Administrator	admin	Includes all maintenance privileges
		Configure Ethernet network settings
		Configure WirelessHART network settings
		Set passwords
		Set time settings
		Set home page options
		Configure custom point pages
		Restart applications

Note   Each of the initial passwords for the user accounts is "default." It is recommended, for security purposes, that these passwords are changed. The administrator password should be appropriately noted when changed. If it is lost, please contact Emerson Process Management for technical support.

To change the User Accounts Passwords:

Step 1   Navigate to Setup>Security>User accounts.

Step 2   Set the new password for each role based user account, and confirm.

Step 3   Click Submit.

Layer 3 Network Operation

The access points support Layer 3 network operation. Access points and controllers in Layer 3 configurations use IP addresses and UDP packets, which can be routed through large networks. Layer 3 operation is scalable and recommended by Cisco.

Figure 1-18 illustrates a typical Layer-3 wireless network configuration containing access points and a controller.

Figure 1-18   Typical Layer 3 Access Point Network Configuration Example
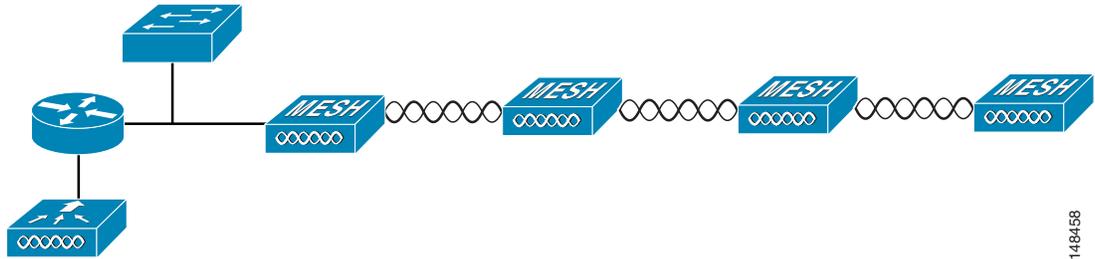
C H A P T E R **2**

Before You Begin

This chapter describes what steps you need to take before beginning the installation of your Access Point and contains the following sections:

- Unpacking the Access Point, page 2-30
- Tools and Hardware, page 2-30
- Warnings, page 2-32
- Safety Information, page 2-32
- Avoiding Damage to Radios in a Testing Environment, page 2-35
- Additional Considerations for Hazardous Locations, page 2-35
- Installation Guidelines, page 2-39

Unpacking the Access Point

When you are unpacking the access point, do not remove the foam blocks attached to the antenna connectors. The foam protects the antenna connectors during installation.

To unpack the access point, follow these steps:

Step 1   Open the shipping container and carefully remove the contents.

Step 2   Return all packing materials to the shipping container, and save it.

Step 3   Ensure that all items listed in "Package Contents" section on page 2-30 are included in the shipment. If any item is damaged or missing, notify your sales representative.

Package Contents

The typical access point package contains the following items:

- Access point
- Cisco product documentation and translated safety warnings
- Two-pin DC power connector
- Ground lug (Panduit PLCD6-10A-L) and screws with lock washers
- Watertight cable glands for Power-over-Ethernet (PoE) ports (depending on the 1552 access point model, 2 or 3 cable glands are provided)

> **Note**   These cable glands are **NOT** hazardous locations/Ex certified.

Tools and Hardware

The tools and hardware used to install the 1552 access point are described in:

Optional Tools and Hardware

The optional tools and hardware that can be obtained from Cisco are:

- Optional power injector (AIR-PWRINJ1500-2=)

> **⚠ Caution**   Caution: Power injector (AIR-PWRINJ1500-2=) is not certified for installation within hazardous locations environments.

- Antennas, 2.4/5 GHz (refer to the "Antenna Configurations" section on page 1-15)

- Optional pole mount kit (AIR-ACCPMK1550=, AIR-ACCPMK1550HZM=)
- Optional banding strap tool (BAND IT) (AIR-BAND-INST-TL=)

Optional Tools and Hardware That You Supply

Tools and materials that are user-supplied are:

- Ground lug crimping tool (Panduit CT-720 with CD-720-1 die)
- 6-AWG copper ground wire
- 13 mm box-end wrench or socket set
- Adjustable wrench, 22 mm socket, or Sealcon S-2200-WR socket wrench
- #8 Torx screwdriver
- Torque Wrench (ft-lbs)
- Small flat screwdriver for DC power connector
- Optional shielded outdoor-rated Ethernet (CAT5e or better) cable with 0.20 to 0.35 in (0.51 to 0.89 cm) diameter
- Optional Ethernet RJ-45 connector and installation tool
- Optional shielded outdoor-rated DC power cable with 0.20 to 0.35 inch (.0.51 to 0.89 cm) diameter
- Optional ground rod, as required by local regulations
- Optional ladder, power lift, rope, or other tools as required

Pole Installation Hardware and Tools

To install the access point on a vertical or horizontal metal, wood, or fiberglass pole, you need the following additional hardware and tools:

- Pole mount kit (AIR-ACCPMK1550=, AIR-ACCPMK1550HZM=)
  - Pole clamp bracket
  - Two gusset strap brackets
  - One mounting bracket
  - Twelve hex bolts (M8 x16)
  - One M8 flange nut
  - Six M8 flat washers
  - Ten M8 split lock washers
  - Two stainless steel mounting straps
- Customer banding strap tool (BAND IT)—(AIR-BAND-INST-TL=)
- Customer-supplied 13-mm and box-end wrench or socket set
- Customer-supplied adjustable wrench, 22 mm socket, or Sealcon S-2200-WR socket wrench

Warnings

Translated versions of all safety warnings are available in the safety warning document that shipped with your access point or on Cisco.com. To browse to the document on Cisco.com, refer to Appendix A, "Translated Safety Warnings" for instructions.

⚠
Warning   **IMPORTANT SAFETY INSTRUCTIONS**
This warning symbol means danger. You are in a situation that could cause bodily injury. Before you work on any equipment, be aware of the hazards involved with electrical circuitry and be familiar with standard practices for preventing accidents. Use the statement number provided at the end of each warning to locate its translation in the translated safety warnings that accompanied this device. Statement 1071
SAVE THESE INSTRUCTIONS

⚠
Caution   The installer is responsible for obtaining any required local or national safety inspections of the structural integrity of the installation by the local authority/inspection department.

⚠
Warning   **Do not operate the unit near unshielded blasting caps or in an explosive environment unless the device has been modified to be especially qualified for such use.** Statement 364

⚠
Caution   The cables specified in this installation guide that are used with the specified liquid-tight adapters provide protection against ingress of moisture for a Type 4/IP67 classified enclosure. If substitute cable are used, the installer must ensure that the size (OD) of the cable meets the acceptable range allowed by the liquid-type adapter.

⚠
Warning   **This equipment must be externally grounded using a customer-supplied ground wire before power is applied. Contact the appropriate electrical inspection authority or an electrician if you are uncertain that suitable grounding is available.** Statement 366

⚠
Warning   **Read the installation instructions before connecting the system to the power source.** Statement 1004

⚠
Warning   **Ultimate disposal of this product should be handled according to all national laws and regulations.** Statement 1040

Safety Information

Follow the guidelines in this section to ensure proper operation and safe use of the access point.

FCC Safety Compliance Statement

The FCC, with its action in ET Docket 96-8, has adopted a safety standard for human exposure to RF electromagnetic energy emitted by FCC-certified equipment. When used with approved Cisco Aironet antennas, Cisco Aironet products meet the uncontrolled environmental limits found in OET-65 and ANSI C95.1, 1991. Proper operation of this radio device according to the instructions in this publication results in user exposure substantially below the FCC recommended limits.

Safety Precautions

Warning   **Explosion Hazard—The area must be known to be nonhazardous before installing, servicing, or replacing the unit.** Statement 1082

Warning   **In order to comply with FCC radio frequency (RF) exposure limits, antennas should be located at a minimum of 7.9 inches (20 cm) or more from the body of all persons.** Statement 332

Warning   **The AC power supply has double pole/neutral fusing.** Statement 188

Warning   **Do not work on the system or connect or disconnect cables during periods of lightning activity.** Statement 1001

Warning   **Class 1 laser product.** Statement 1008

Warning   **A readily accessible two-poled disconnect device must be incorporated in the fixed wiring.** Statement 1022

Warning   **To reduce the risk of fire, use only No. 26 AWG or larger telecommunication line cord.** Statement 1023

Warning   **This unit might have more than one power supply connection. All connections must be removed to de-energize the unit.** Statement 1028

Warning   **Only trained and qualified personnel should be allowed to install, replace, or service this equipment.** Statement 1030

![warning] **Warning**   **When using a DC input voltage source, observe this warning statement:**
Connect the unit only to DC power source that complies with the safety extra-low voltage (SELV)
requirements in IEC 60950 based safety standards. Statement 1033

![warning] **Warning**   **When installing or replacing the unit, the ground connection must always be made first and**
disconnected last. Statement 1046.

![warning] **Warning**   **Do not locate the antenna near overhead power lines or other electric light or power circuits, or**
where it can come into contact with such circuits. When installing the antenna, take extreme care
not to come into contact with such circuits, because they may cause serious injury or death. For
proper installation and grounding of the antenna, please refer to national and local codes (for
example, U.S.:NFPA 70, National Electrical Code, Article 810, Canada: Canadian Electrical Code,
Section 54). Statement 1052

![caution] **Caution**   Before connecting or disconnecting a power cord, you must remove power from the power source using
a suitable service disconnect.

For safety and to achieve a good installation, please read and follow these safety precautions:

- Select your installation site with safety, as well as performance in mind. Remember: electric power
  lines and phone lines look alike. For safety, assume that any overhead line can kill.
- Call your electric power company. Tell them your plans, and ask them to come look at your proposed
  installation.
- Plan your installation carefully and completely before you begin. Successful raising of a mast or
  tower is largely a matter of coordination. Each person should be assigned to a specific task and
  should know what to do and when to do it. One person should be in charge of the operation to issue
  instructions and watch for signs of trouble.
- When installing the access point and antennas, remember:
  – Do not use a metal ladder.
  – Do not work on a wet or windy day.
  – Do dress properly—shoes with rubber soles and heels, rubber gloves, long sleeved shirt or
    jacket.
- Use a rope to lift the access point. If the assembly starts to drop, get away from it and let it fall.
- If any part of the antenna system should come in contact with a power line, do not touch it or try to
  remove it yourself. Call your local power company. They will remove it safely.

If an accident should occur, call for qualified emergency help immediately.

Avoiding Damage to Radios in a Testing Environment

The radios on outdoor units (bridges) have higher transmit power levels than radios on indoor units (access points). When you test high-power radios in a link, you must avoid exceeding the maximum receive input level for the receiver. At levels above the normal operating range, packet error rate (PER) performance is degraded. At even higher levels, the receiver can be permanently damaged. To avoid receiver damage and PER degradation, you can use one of the following techniques:

- Separate the omnidirectional antennas by at least 2 ft (0.6 m) to avoid receiver damage or by at least 25 ft (7.6 m) to avoid PER degradation.

Note These distances assume free space path loss and are conservative estimates. Required separation distances for damage and performance degradation levels in actual deployments are less if conditions are not non-line-of-sight.

- Reduce the configured transmit power to the minimum level.
- Use directional antennas, and keep them away from each other.
- Cable the radios together using a combination of attenuators, combiners, or splitters to achieve a total attenuation of at least 60 dB.

For a radiated test bed, the following equation describes the relationships among transmit power, antenna gain, attenuation, and receiver sensitivity:

```
txpwr + tx gain + rx gain - [attenuation due to antenna spacing] < max rx input level
Where:
txpwr = Radio transmit power level
tx gain = transmitter antenna gain
rx gain = receiver antenna gain
```

For a conducted test bed, the following equation describes the relationships among transmit power, antenna gain, and receiver sensitivity:

```
txpwr - [attenuation due to coaxial components] < max rx input level
```

Caution Under no circumstances should you connect the antenna port from one access point to the antenna port of another access point without using an RF attenuator. If you connect antenna ports, you must not exceed the maximum survivable receive level of 0 dBm. Never exceed 0 dBm, or damage to the access point can occur. Using attenuators, combiners, and splitters having a total of at least 60 dB of attenuation ensures that the receiver is not damaged and that PER performance is not degraded.

Additional Considerations for Hazardous Locations

This section describes special considerations for preparing the 1552H, 1552SA/1552SD and 1552WU access points for installation in Class I, Division 2/Zone 2 hazardous locations.

Note This document does not provide specific procedures for installing conduit. You must ensure that your installation techniques and procedures comply with Class I, Division 2/Zone 2 hazardous location installation regulations for your geographic location.

The access point hazardous location option complies with safety standards for Class I, Division 2/Zone 2 hazardous locations where ignitable concentrations of flammable gases, vapors, or liquids are not likely to exist under normal operation conditions.

When you select the hazardous location option as part of the ordering process, Cisco configures the system to contain the new components. Assembly instructions placed in the shipping box provide information and assembly procedures. The hazardous location option configures the access point as follows:

- Do not install a battery in a Hazardous Location environment. Battery packs are not approved for Hazardous Locations.

- The AC power connections are moved to the inside of the access point by installing an AC entry board containing a terminal block. To comply with hazardous location requirements, AC power must be installed through rigid metal conduit to the terminal block.

⚠️
Caution   The electrical rating for hazardous location installations has a lower voltage rating (100-240 VAC, 50/60 Hz, 1A) than a non-hazardous location installation (100-480 VAC).

⚠️
Caution   Do not use 12 VDC input connection in hazardous locations.

⚠️
Caution   Caution: Power injector (AIR-PWRINJ1500-2=) is not certified for installation within hazardous locations environments.

Warnings

⚠️
Warning   **Do not disconnect connections to this equipment unless power has been removed or you have verified that the area is nonhazardous. Secure any external connections that mate to this equipment by using screws, sliding latches, threaded connectors, or other means provided with this product. Substitution of components may impair suitability for Class I, Zone 2, Division 2.** Statement 1062

⚠️
Warning   **When used in a Class I, Zone 2, Division 2 hazardous location, this equipment must be mounted with a proper wiring method that complies with the governing electrical codes.** Statement 1069

⚠️
Warning   **If you connect or disconnect the console cable with power applied to the unit or any device on the network, an electrical arc can occur. This could cause an explosion in hazardous location installations. Be sure that power is removed or the area is nonhazardous before proceeding.**

To verify unit operation, perform POST on the device in a nonhazardous location before installation. Statement 1080

Warning   **In switch installations in a hazardous location, the DC power source could be located away from the vicinity of the switch. Before performing any of the following procedures, locate the DC circuit to ensure that the power is removed and cannot be turned on accidentally, or verify that the area is nonhazardous before proceeding.** Statement 1059

Warning   **Do not connect or disconnect cables to the ports while power is applied to the switch or any device on the network because an electrical arc can occur. This could cause an explosion in hazardous location installations. Be sure that power is removed from the switch and cannot be accidentally be turned on, or verify that the area is nonhazardous before proceeding.** Statement 1070

Compliance

The 1552H, 1552SA/1552SD, and 1552WU access points comply with the following versions of hazardous location certifications:

- IEC 60079-0 Edition 6.0
- IEC 60079-15 Edition 4.0
- CAN/CSA E60079-0: 11
- CAN/CSA E60079-15: 12
- UL 60079-0: Edition 6
- UL 60079-15: Edition 4
- EN 60079-0: 2012
- EN 60079-15: 2010

Table 2-1 interprets the information on the compliance labels.

Table 2-1   Interpreting the Hazardous Compliance Label

Label Text	Description

Class I, Division 2, Groups A, B, C, D	Defines the environment in which the access point can be used:
	 • Class I—Environment containing flammable gases, vapors, or liquids
	 • Division 2—Environmental classification used by the U.S. and Canada
	 • Groups A, B, C, D—Gas identification for the U.S. and Canada:
	  – A—Acetylene
	  – B—Hydrogen
	  – C—Ethylene
	  – D—Propane

Class I, Zone 2, Group II	Defines the environment in which the access point can be used:
	 • Class I—Environment containing flammable gases, vapors, or liquids
	 • Zone 2—Environment classification used in North America
	 • Group II—Gas identification for Zone II, which includes:
	  – IIa—Propane
	  – IIb—Ethylene
	  – IIc—Acetylene & Hydrogen

Table 2-1   Interpreting the Hazardous Compliance Label (continued)

Label Text	Description
Ex nA II T5	Defines parameters that the product complies with for U.S. Certification: • Ex —Denotes explosive atmosphere • nA —Non-sparking • II = Group II as defined previously • T5 = Temperature code < 100 degrees C, maximum surface temperature
CSA Certificate 1945576	Identifies the Canadian Standards Association (CSA) certificate number.
SIRA 11ATEX4253	Identifies Sira ATEX certificate number.
-40 ≤ Ta < +55C	The operating temperature range for the access point in all countries. **Note** Current safety certifications only include operation of this outdoor equipment down to -40C.
Type 4, IP67	Defines the enclosure degree of protection (Type 4 = indoor or outdoor use primarily to provide a degree of protection against windblown dust and rain, splashing water, hose-directed water, and damage from external ice formation. IP67 = Dust tight (dust, dirt, sand, and so forth) and protected against powerful water jets. Also, the unit can be immersed in water up to 1m for short periods of time (30min).

KOSHA Certificate Information (for Korean hazardous locations)

add in statements here when available

Installation Guidelines

Because the access point is a radio device, it is susceptible to common causes of interference that can reduce throughput and range. Follow these basic guidelines to ensure the best possible performance:

- For information on planning and initially configuring your Cisco Mesh network, refer to the *Cisco Wireless Mesh Access Points, Design and Deployment Guide.*
- Review the FCC guidelines for installing and operating outdoor wireless LAN devices at http://www.cisco.com/en/US/partner/prod/collateral/routers/ps272/data_sheet_c78-647116_ps11451_Products_Data_Sheet.html.
- Perform a site survey before beginning the installation.
- Install the access point in an area where structures, trees, or hills do not obstruct radio signals to and from the access point.

- The access points can be installed at any height, but best throughput is achieved when all the access points are mounted at the same height. Cisco recommends installing the access points no higher than 40 feet to allow support for wireless clients on the ground.

✎ **Note** To calculate path loss and to determine how far apart to install access points, consult an RF planning expert.

Site Surveys

Every network application is a unique installation. Before installing multiple access points, you should perform a site survey to determine the optimum use of networking components and to maximize range, coverage, and network performance.

Consider the following operating and environmental conditions when performing a site survey:

- Data rates—Sensitivity and range are inversely proportional to data bit rates. The maximum radio range is achieved at the lowest workable data rate. A decrease in receiver sensitivity occurs as the radio data increases.

- Antenna type and placement—Proper antenna configuration is a critical factor in maximizing radio range. As a general rule, range increases in proportion to antenna height. However, do not place the antenna higher than necessary, because the extra height also increases potential interference from other unlicensed radio systems and decreases the wireless coverage from the ground.

- Physical environment—Clear or open areas provide better radio range than closed or filled areas.

- Obstructions—Physical obstructions such as buildings, trees, or hills can hinder performance of wireless devices. Avoid locating the devices in a location where there is an obstruction between the sending and receiving antennas.

- Applications and type of devices to be used on the WLAN.

Before Beginning the Installation

Before you begin the installation process:

- Ensure that a site survey has been performed.

- Ensure that your network infrastructure devices are operational and properly configured.

- Ensure that your controllers are connected to switch trunk ports.

- Ensure that your switch is configured with untagged access ports for connecting your access points.

- Ensure that a DHCP server with Option 43 configured is reachable by your access points, or manually configure the controller information in the access point (for additional information, refer to the Appendix F, "Configuring DHCP Option 43").

- Become familiar with the access point installation components (see the "Becoming Familiar with Access Point Installation Components" section on page 2-41).

Becoming Familiar with Access Point Installation Components

The access point is designed to be installed in an outdoor environment, such as the exterior roof overhang of a tall building or a streetlight pole. Carefully review the following figures to become familiar with the system components, connectors, indicators, cables, system interconnection, and grounding:

- Components in a typical access point installation (see Figure 2-1)

- Pole mount installation (see Figure 2-2)

Note The illustrations in this document show all available connections for the access point. Unused connections must be capped with a connector plug to ensure the watertight integrity of the access point. Liquid-tight adapters are provided for connector openings, which can be installed before or after deploying the access point.

Caution The liquid-tight adapter(s) supplied in the kit are IP68/69 certified with .200 to .350 diameter cables but not ATEX certified or hazardous locations compliant. The installer must use cable glands appropriate to the installation.

Figure 2-1   Components in a Typical Access Point Installation
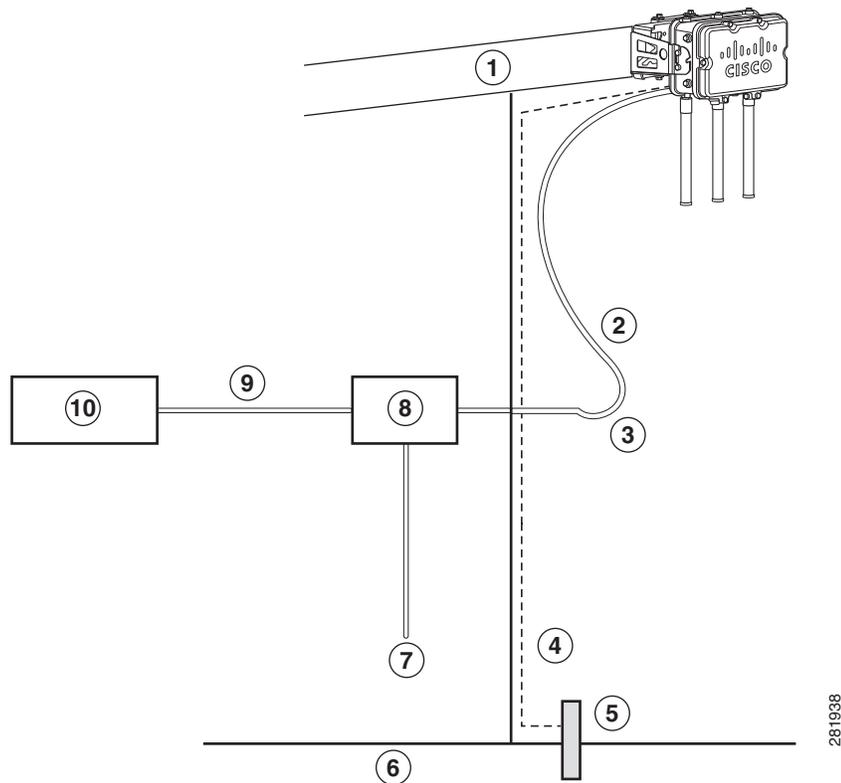
1	Building roof-overhang	6	Ground
2	Shielded outdoor-rated Ethernet (CAT5e or better) cable[1]	7	AC power cord[2]
3	Water drip loop	8	Power injector[3]
4	6-AWG copper grounding wire[1]	9	Shielded Ethernet (CAT5e or better) cable[1]
5	Ground rod[1]	10	Controller (through a switch)

1. User supplied.

2. The safety ground wire in the AC power cord must have a ground path to a grounding rod.

3. The shielded Ethernet cable has a ground path through the power injector and the safety ground wire in the AC power cord.

Note   The 1552 access point was designed with consideration for resistance to effects of lightning effects on the access point electronics. The 1552 access point employs lightning arrestor circuitry on the Ethernet and power ports. On the input Ethernet port, Gas Discharge Tubes (GDT) are used for the Power Entry Module (PEM) to mitigate lightning effect. On the AC power, GDTs are also used along with fuses to mitigate high-current condition. For the DC power, a fuse is used to mitigate high current condition.

While not a common practice, the user may want to consider using lightning protection at the antenna ports for added protection. To meet EN/IEC60950-22 (Clause 4.2) requirements, the installer must ensure that additional protection is provided external to this equipment to reduce transient surges from Overvoltage IV to Overvoltage Category II at the AC power input of the access point. The over-voltage and fault-current protection components used to achieve this protection must comply with the IEC 61643 series of standards. To meet CAN/CSA-C22.2 No. 60950-22-07/UL60950-22 requirements, the installer may use alternative components to provide this additional protection. Those components may comply with ANSI/IEEE C62.11, CSA Certification Notice No. 516, CSA C22.2 No. 1, or UL 1449. Suitability of the components for the application must be determined for the intended installation. (For example, some devices are suitable for installation on the load side of the service entrance only, and some are suitable for use with cord-connected equipment only.)

Warning   **Installation of the equipment must comply with local and national electrical codes.** Statement 1074

Figure 2-2   Pole Mount Installation
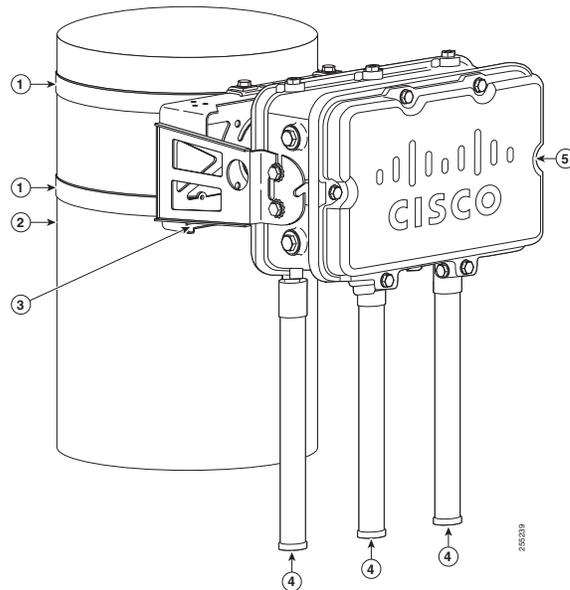
1	Stainless steel mounting straps (part of pole mount kit)	4	Cisco Aironet Dual-Band Omnidirectional Antennas. The dual-band antenna covers both the 2.4 GHz and 5 GHz bands.
2	Pole (wood, metal, or fiberglass) 2 to 16 in. (5.1 to 40.6 cm) diameter	5	1552 series access point
3	Mounting bracket (part of pole mount kit)		

Antenna N-Type Connector Locations

The access point antenna N-type connectors are located on the bottom of models AIR-CAP1552H-*x*-K9 and on the top and bottom of model AIR-CAP1552SA/SD/WU-*x*-K9. The N-type connectors support the Cisco Aironet Antennas listed in Antenna Configurations, page 1-15. Figure 1-7 and Figure 1-8 show the antenna port locations viewed from the RF cover side. The supported antennas can be directly attached to the access point or remotely located. When used in a Class 1, Zone 2, Division 2 hazardous location, this equipment must be mounted with proper RF cables (if required) and electrical wiring methods that comply with the governing electrical codes.

Adding the Access Point MAC Addresses to the Controller Filter List

Before installing your access points, configure your controller by adding the MAC addresses of the access points to the filter list. MAC address filtering is enabled by default. This enables the controller to respond to the listed access points. To add a MAC filter entry on the controller, follow these steps:

Step 1   Log into your controller using a web browser.

Step 2   Choose **SECURITY > MAC Filtering > New**.

Step 3   Enter the MAC address of the access point to the MAC Filter list; for example, 00:0B:91:21:3A:C7.

> ✎
>
> **Note**   The access point MAC address is located on the bottom of the unit. When two MAC addresses are shown, use the top MAC address.

Step 4   Select a WLAN ID or **Any WLAN** from the WLAN ID pop-up menu.

Step 5   Enter a description (32 characters maximum) of the access point in the Description field; for example, Fisher_Street_00.0B.91.21.3A.C7 shows the location and MAC address of the access point.

Step 6   Choose an interface from the Interface Name pop-up menu, and click **Apply**.

Step 7   Repeat Steps 2 to 6 to add other access points to the list.

Step 8   Log out of your controller, and close your web browser.

Configuring a RAP

The access point defaults to the mesh access point (MAP) radio role. One or more of your access points must be reconfigured as a root access point (RAP). The RAPs connect to a wired Ethernet link through a switch to the controller. The MAPs use their wireless backhaul interface to connect to a RAP to reach the controller.

To configure a RAP on the controller GUI, follow these steps:

Step 1   Log into your controller using a web browser.

Step 2   Click **Wireless**. When your access point associates to the controller, the name of the access point appears in the AP Name list.

Step 3   Double-click your access point name.

Step 4   Find Mesh Information, and choose **Root AP** by clicking the drop-down arrow in the AP Role field.

Step 5   Click **Apply**.

Step 6   Repeat Steps 2 through 5 for each RAP.

Step 7   Log out from your controller, and close your web browser.

C H A P T E R 3

Installing the 1552 Series Access Points in Hazardous Locations

This chapter describes how to install the 1552 access point for hazardous locations and contains the following sections:

Mounting on a Wall or a Pole

This section provides instructions for the physical installation of your access points. Personnel installing the access point must understand wireless access points and bridging techniques and grounding methods.

⚠ **Caution** All installation methods for mounting an access point on any wall surface is subject to the acceptance of local jurisdiction.

Installation Option

The Cisco Aironet 1552 Series Outdoor Mesh Access Point for Hazardous Locations are installed using the optional Pole Mount installation kit, which is used for pole or wall installations

⚠ **Warning** **Only trained and qualified personnel should be allowed to install, replace, or service this equipment.** Statement 1030

⚠

Warning   **Installation of the equipment must comply with local and national electrical codes.** Statement 1074

⚠

Caution   To provide inline PoE, you must use the power injector (AIR- PWRINJ1500-2=) specified for the access point. Other power injectors, PoE switches, and 802.3af power sources do not provide adequate power, which might cause the access point to malfunction and cause over-current conditions at the power source. You must ensure that the switch port connected to the access point has PoE turned off.

⚠

Caution   The power injector is not intended to be installed in a hazardous locations environment. If a PoE injector is required, it must be located in a non-hazardous locations environment.

Refer to these sections for installation details:

- Access Point Mounting Orientation, page 3-46
- Mounting the Access Point on a Wall, page 3-46
- Mounting the Access Point on a Pole, page 3-51

Access Point Mounting Orientation

When mounting an access point on a horizontal or vertical surface, you must ensure that the access point is oriented with the LED indicators pointing down (see Chapter 2, "Pole Mount Installation". This positioning allows the LEDs to be visible to someone on the ground below the access point.

You must also ensure the access point is mounted with the hinged access cover facing out.

✎

Note   Omnidirectional antennas are vertically polarized and should be mounted vertically.

Mounting the Access Point on a Wall

The optional pole mount kit contains a mounting bracket for wall mounting. You can use the mounting bracket as a template to mark the positions of the mounting holes for your installation. You then install the mounting plate, and attach the access point when you are ready. Table 3-1 lists the material that you will need to provide in addition to the pole mount kit.

Table 3-1   Material Needed to Mount Access Point to a Vertical Wall

Materials Required	In Kit
• Ground lug and screws (provided with access point)	Yes
• Crimping tool for ground lug, Panduit CT-720 with CD-720-1 die (http://onlinecatalog.panduit.com)	No
• Four M8 or 5/16 in. (31 mm) screws	No
• Four wall anchors (specified for wall material)	No
• Drill bit for wall anchors	No
• Electric drill and standard screwdriver	No
• #6-AWG ground wire	No
• Shielded outdoor-rated Ethernet (CAT5e or better) cable	No
• Grounding block	No
• Grounding rod	No
• 13-mm box-end wrench or socket set	No

⚠

Caution   The mounting surface, attaching screws, and optional wall anchors must be able to support a 50-lb (22.7 kg) static weight.

The mounting bracket can be used as a template to mark the screw hole locations, or you can refer to the following diagram:
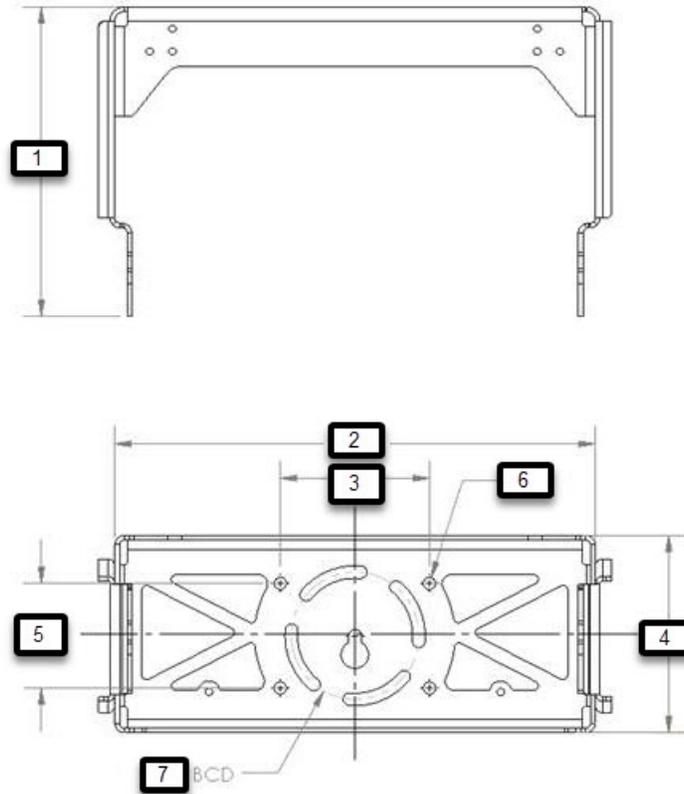
Note   BCD is Bolt Circle Diameter.

1	8.49 inches (21.56 cm)	**2**	13.17 inches (33.45 cm)
3	4.09 inches (10.38 cm)	**4**	5.41 inches (13.74 cm)
5	2.88 inches (7.32 cm)	**6**	0.335 inches (0.851 cm)
7	0.350 inches (0.889 cm)		

To mount the access point on a vertical wall, follow these instructions:

Step 1   Use the mounting bracket as a template to mark four screw hole locations on your mounting surface. See Figure 3-1 for the mounting bracket screw hole locations. You can optionally use the individual mounting holes or the mounting slots.

Figure 3-1   *Mounting Bracket for Wall Mounting*
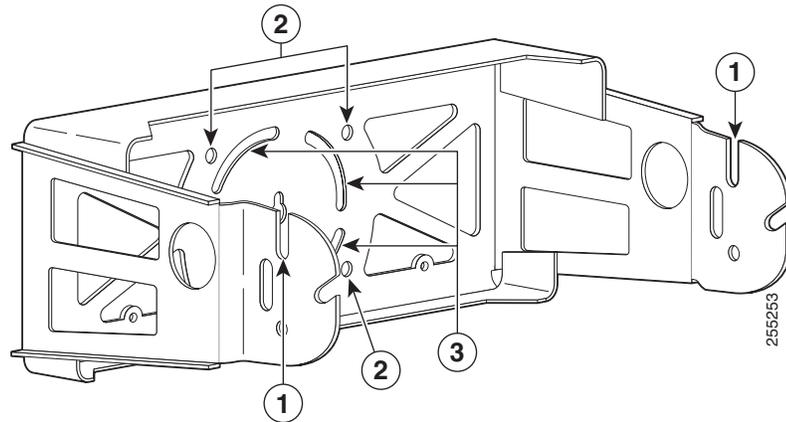
1	Access point quick mount notch	**3**	Mounting slots (allows bracket rotation)
2	Mounting holes		

Step 2   Use four customer-supplied screws and optional screw anchors to attach the mounting plate to the mounting surface.

> **Note**   If necessary, use suitable screw anchors and an exterior-grade plywood backboard to mount the access point to stucco, cement, or drywall.

Step 3   Screw a M8 x16 bolt in the top support bolt hole on each side the access point (see Figure 3-2). Do not screw the bolt all the way in; leave approximately a 0.25 inch (0.635 cm) space.

Figure 3-2   *Location of Access Point Top Support Bolt Hole*
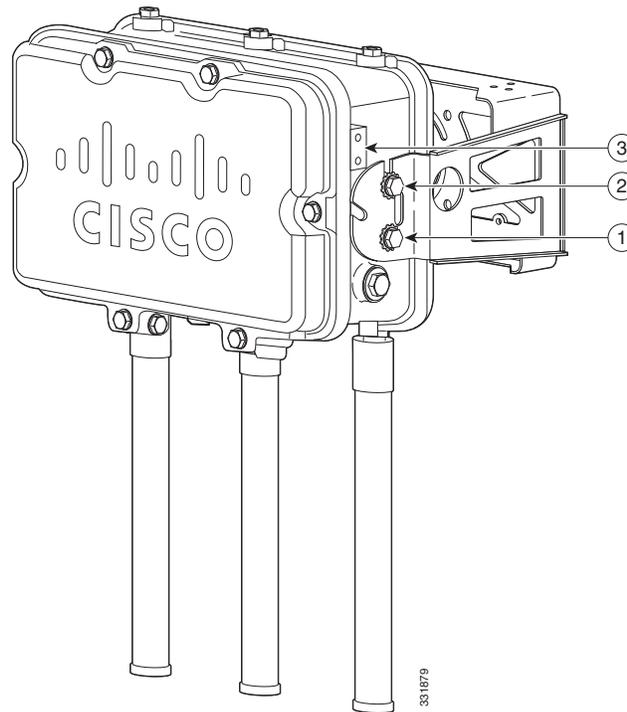
1	M8 x16 bolt (supplied with pole mount kit)	3	Ground lug location (M4 x .7)
2	M8 x16 bolt (supplied with pole mount kit)		

Step 4   Position the two bolts on the access point into the quick mount notches on each side of the mounting bracket (see Chapter 2, "Pole Mount Installation"). Ensure that the hinged door is facing out.

Step 5   Screw a M8 x16 bolt (with flat and lock washers) into the second bolt hole on each side of the access point.

Step 6   Ensure that the front of the access point is vertical, and tighten the four bolts to 13 to 15 ft lbs (17.6 to 20.3 Nm).

Step 7   When using the Cisco Aironet Dual-Band Omnidirectional Antennas, connect them to the access point as shown in Figure 3-2. Hand-tighten the antennas to the access point.

Step 8   Continue with the "Grounding the Access Point (all models)" section on page 3-60 and the "Powering the Access Point" section on page 3-71.

Mounting the Access Point on a Pole

When installing an access point on a vertical pole, mast, or a streetlight pole, you should use the optional Cisco pole mount kit. The kit supports metal, wood, or fiberglass poles from 2 to 16 inches in diameter.

Assembling the Pole Clamp Bracket and the Mounting Bracket

When installing an access point on a pole, mast, or a streetlight, you should use the optional Cisco pole mount kit. The kit supports metal, wood, or fiberglass poles from 2 to 16 inches in diameter.

The pole mount kit contains several parts that you must assemble prior to mounting on a pole. First you need to assemble two strap brackets on the pole clamp bracket that are positioned for the pole diameter you are using to mount the access point. Figure 3-3 illustrates the pole diameter indicators and bolt holes on the pole clamp bracket.

Figure 3-3   Pole Clamp Bracket Adjustment Hole Locations

1	Pole size indicators	2	Bolt holes for pole diameters
	• 2 to 6 inches (5.08 cm to 15.24 cm)		(11 to 16 inches (27.94 cm to 40.64 cm) indicated)
	• 6 to 11 inches (15.24 cm to 27.94 cm)		
	• 11 to 16 inches (27.94 cm to 40.64 cm)		

To assemble the pole clamp bracket, follow these steps:

Step 1 Position the strap brackets on the pole clamp bracket for the pole diameter you are using and secure each strap bracket with two M8 x16 bolts (with lock washers) (see Figure 3-4). Tighten the bolts to 13 to 15 ft lbs (17.6 to 20.3 Nm).

Figure 3-4   Assembled Pole Clamp Bracket and Strap Brackets
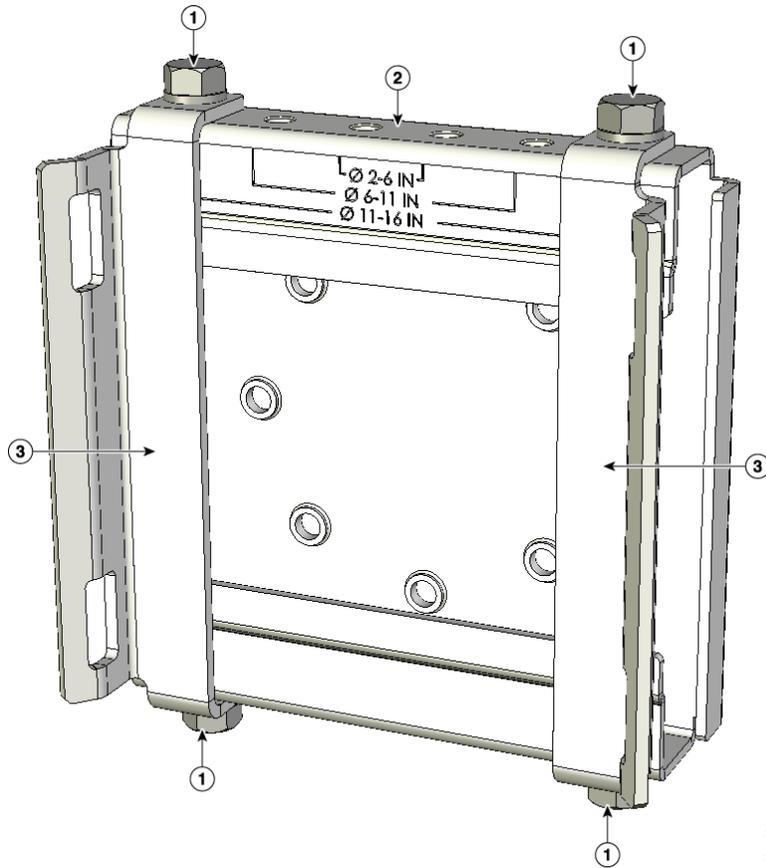
1	M8 x1.25x16 bolts (with lock washers)	3	Strap bracket (shown positioned for 11 to 16 inch diameter pole)
2	Pole clamp bracket		

Step 2 Screw the M8 nut onto the pole clamp bracket support bolt, and tighten just enough to prevent the bolt from falling off.

Step 3 Go to the "Pole Mounting" section on page 3-53.

Pole Mounting

The access point can be installed where power is available, without the need for a wired LAN connection. The access point uses intelligent wireless routing that is based on the Adaptive Wireless Path Protocol (AWPP). AWPP enables a remote access point to dynamically optimize the best route to the wired LAN network using another access point.

The 1552 access point uses the 5 GHz radio for the Mesh backhaul and connections. The 2.4 GHz radio is used for local wireless client access.

To mount your access point on a vertical pole or streetlight pole, you need to install two metal bands around the pole to support the access point. This process requires extra tools and material not provided in the pole mount kit (see Table 3-2).

Table 3-2   Material Needed to Mount Access Point on a Pole

Mounting Method	Materials Required	In Kit
Vertical or streetlight pole	• Two 0.75-in (1.9 cm) stainless steel bands	Yes
	• Banding strap tool (BAND IT) (Cisco AIR-BAND-INST-TL=)	No
	• Ground lug (provided with access point)	Yes
	• Crimping tool for ground lug, Panduit CT-720 with CD-720-1 die (http://onlinecatalog.panduit.com)	No
	• #6 AWG ground wire	No

To mount the access point onto a vertical pole or streetlight pole, follow these steps:

Step 1 Select a mounting location on the pole to mount the access point. You can attach the access point to any pole from 2 to 16 inch (5.1 to 40.6 cm) in diameter.

> **Note** If you will be using a streetlight power tap adapter, position the access point within 3 ft (1 m) of the outdoor light control.

Step 2 For poles larger than 3.5 inch (8.9 cm), mount the pole clamp bracket assembly to a pole (see Figure 3-5) using two metal straps. Following the instructions provided with the banding strap tool (BAND IT) (AIR-BAND-INST-TL=), loop each metal strap twice through the slots on the strap bracket.

> **Caution** Do not place the metal straps in the large open area between the pole clamp bracket and the strap brackets, because this does not properly secure the access point.

Figure 3-5   Clamp Bracket Assembly Mounted on Poles Larger than 3.5 inch (8.9 cm)
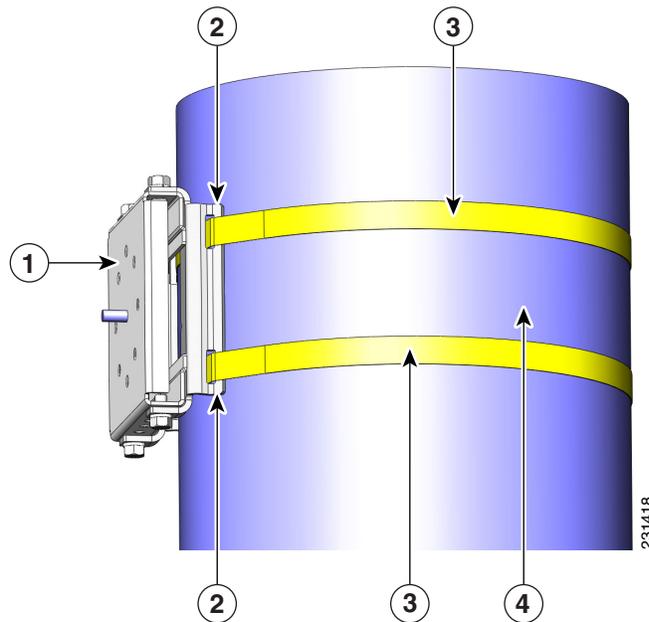
1	Pole clamp bracket	3	Metal mounting strap
2	Strap slot in strap bracket	4	Pole

Step 3   For pole diameters of 3.5 inch (8.9 cm) or less, mount the pole clamp bracket assembly to a pole using two metal straps looped through the space between the pole clamp bracket and the strap brackets (see Figure 3-6) to provide maximum holding strength for extreme environments. Following the instructions provided with the banding strap tool (BAND IT) (AIR-BAND-INST-TL=), loop each metal strap twice.

Figure 3-6   Metal Strap Open Space for 3.5 inch (8.9 cm) and Smaller Poles
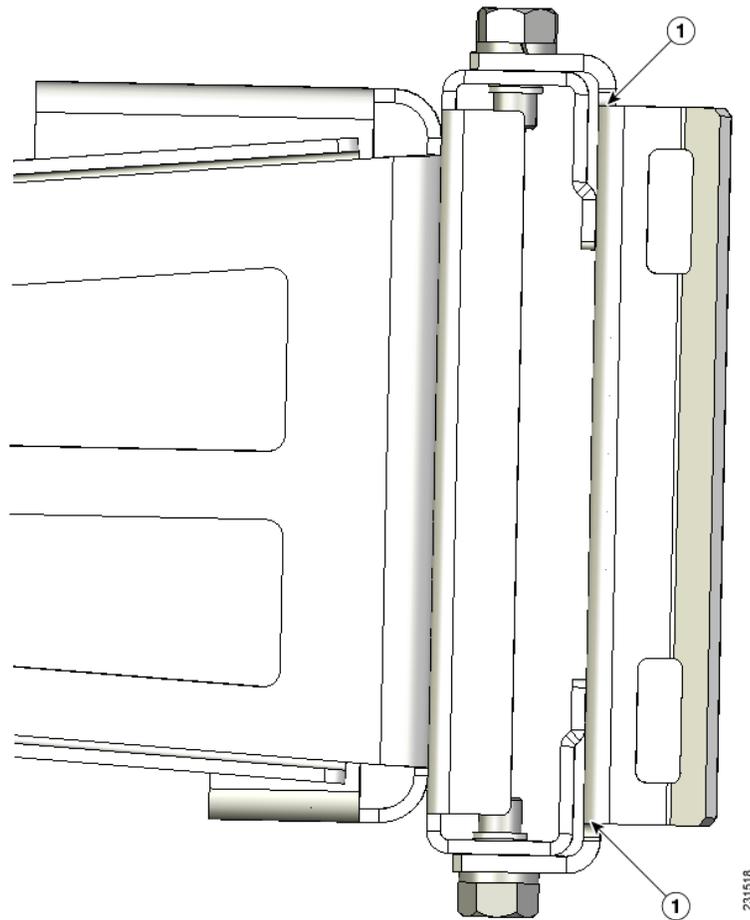
1	Metal strap open space

⚠️

Caution   Do not place the metal straps in the large open area between the pole clamp bracket and the strap brackets because this does not properly secure the access point.

Step 4   Position the pole clamp bracket on the pole as needed before tightening the metal bands.

✎

Note   When the metal bands are tightened to the full tension, the pole clamp bracket cannot be adjusted unless the metal bands are cut or disassembled.

Step 5   Tighten the metal bands using the banding strap tool (BAND IT) (Cisco AIR-BAND-INST-TL=) by following the operating instructions in the box with the tool. Ensure that the metal bands are as tight as possible.

Step 6   Place the mounting bracket onto the pole clamp bracket support bolt (see Figure 3-7).

Step 7   For vertical poles, position the mounting bracket as shown in Figure 3-7. For horizontal streetlight poles, rotate the mounting bracket 90$^{\text{o}}$ from the position shown in Figure 3-7.

Step 8   Install four M8 x16 bolts (with flat and lock washers) into the bolt holes.

Figure 3-7   *Screw Hole Locations on the Mounting Bracket and Pole Clamp Bracket Assembly*
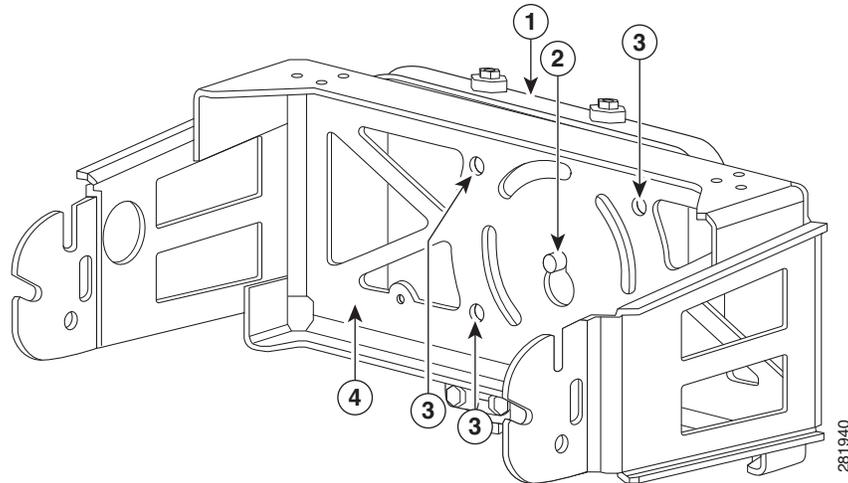
1	Pole clamp bracket assembly	3	Bolt holes
2	Access point support bolt (M8 flange nut not shown)	4	Mounting bracket

Step 9   Hand-tighten the bolts and the nut (do not overtighten).

Step 10   Adjust the top edge of the mounting bracket until it is horizontal and tighten the bolts and the flange nut (see Figure 3-7) to 13 to 15 ft lbs (17.6 to 20.3 Nm).

> ✎
>
> **Note**   The mounting bracket can be adjusted up to 45° to compensate for tilted horizontal streetlight poles.

Step 11   Screw a M8 x16 bolt (without a flat or lock washer) in the top support bolt hole on each side the access point (see Figure 3-8). Do not screw the bolt all the way in. Leave a gap of approximately 0.25 inch (0.635 cm).

Figure 3-8   Location of Access Point Top Support Bolt Holes
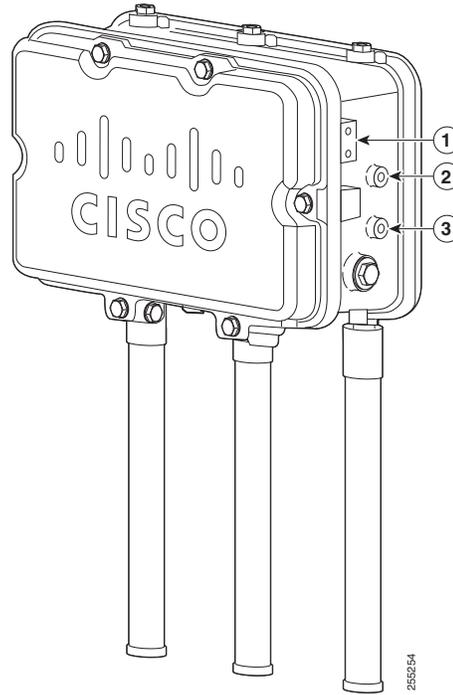
1	Ground lug screw holes location. M4x.7	**3**	Second M8 x16 bolt hole location
2	M8 x16 bolt hole (bolts are supplied with pole mount kit; install without flat or lock washers)		

Step 12   Position the two bolts on the access point into the access point quick-mount notch on the mounting bracket (see Figure 3-9).

Note   The access point should be positioned with the LEDs on the bottom to allow viewing from the ground and with the hinged cover facing out.

Figure 3-9   *Access Point Hanging in Mounting Bracket*
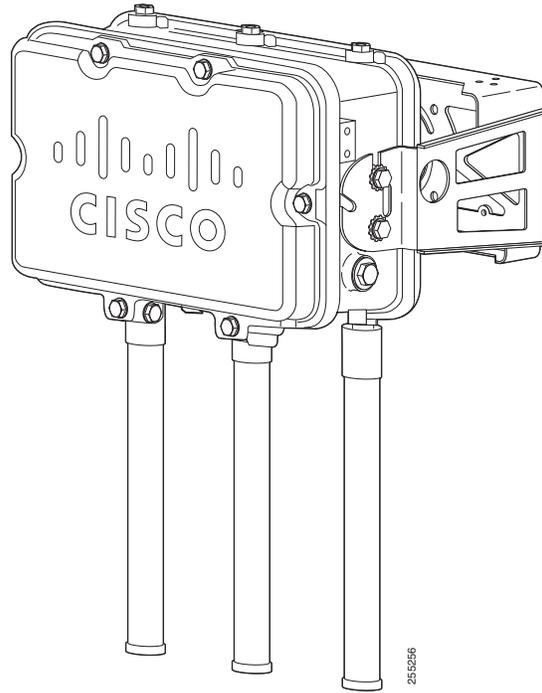
Step 13 Screw a M8 x16 bolt (with flat and lock washers) into the second bolt hole on each side of the access point (see Figure 3-9).

Step 14 Ensure that the front of the access point is vertical, and tighten the four bolts to 13 to 15 ft lbs (17.6 to 20.3 Nm).

Step 15 When using the Cisco Aironet Dual-Band Omnidirectional Antennas, connect them to the access point as shown in Figure 3-9. Hand-tighten the antennas to the access point.

Step 16 Continue with the "Grounding the Access Point (all models)" section on page 3-60 and the "Powering the Access Point" section on page 3-71.

Working with the Access Point Hinged Cover

This section details opening and closing the protective cover.

Opening the Access Point Hinged Cover

⚠

Caution   The hinged cover must not be opened unless the area is considered non-hazardous and the AP has been powered off.

You need to open the access point hinged cover to access the AC entry terminal block or 24 VDC terminal block, and when you are installing fiber-optic SFP module and fiber cable take-up reels.

To open the access point hinged cover, follow these steps:

Step 1   Use 0.5-in (13-mm) box-end wrench or socket set to unscrew and remove the four bolts on the front cover of the unit. Only unscrew the hinge bolts about 2 turns until they are easily turned by hand, do not remove the bolts on the hinge (Figure 3-10).

Step 2   The cover is hinged on the bottom. Carefully open the cover and remove the cover.

> **Note**   If the cover does not open easily, carefully loosen the hinge bolts again.

Figure 3-10   Access Point Front View of Hinged Cover

1	M8 x32 bolts	**2**	Cover hinge M8 x32 bolts

Closing the Access Point Hinged Cover

To close the access point cover, follow these steps:

Step 1   When closing the access point cover, be careful not to pinch internal wires.

Step 2   Carefully position the cover flush with all sides of the access point, then slowly hand-tighten each bolt.

Step 3   When all bolts are hand-tightened, use a 13-mm closed-end wrench or socket to partially tighten the bolts in the tightening sequence shown in Figure 3-11. Tighten each bolt to 3 to 4 ft lbs (0.34 to 0.45 Nm).

Step 4   Repeat Step 3 using the same tightening sequence to fully tighten each bolt to 6 to 7 ft lbs (0.68 to 0.79 Nm).

Figure 3-11   *Hinged Cover Bolt Tightening Sequence*
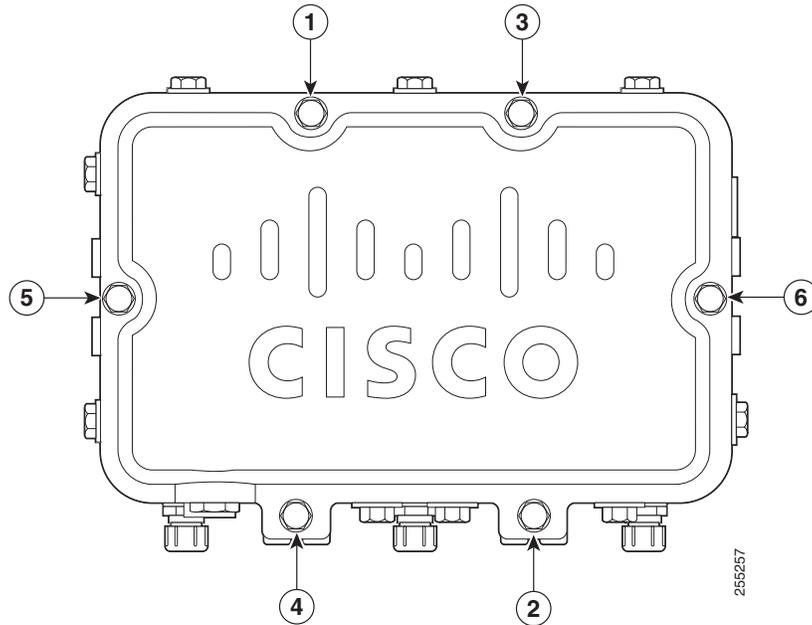
| 1 - 6 | Tighten the bolts in the numeric order shown, starting with 1. |

Grounding the Access Point (all models)

The access point must be grounded before connecting power.

Warning   **This equipment must be externally grounded using a customer-supplied ground wire before power is applied. Contact the appropriate electrical inspection authority or an electrician if you are uncertain that suitable grounding is available.** Statement 366

Warning   **Installation of the equipment must comply with local and national electrical codes.** Statement 1074

In all outdoor installations and when powering the access point with AC power, you must follow these instructions to properly ground the case:

Step 1   If using insulated 6-AWG copper ground wire, strip the insulation as required for the grounding lug.

Step 2   Use the appropriate crimping tool to crimp the bare 6-AWG copper ground wire to the supplied grounding lug (Panduit PLCD6-10A-L).

Note   The grounding lug and hardware used must comply with local and national electrical codes.

Step 3   Open the electrical joint compound (supplied), and apply a liberal amount over the metal surface where the ground strap screw holes are located (see Figure 3-8).

Step 4   Connect the grounding lug to the access point grounding screw holes (see Figure 3-8) using the supplied two Phillips head screws (M4 x10 mm) with lock washers. Tighten the grounding screw to 22 to 24 in. lbs (2.49 to 2.71 Nm).

Step 5   If necessary, strip the other end of the ground wire, and connect it to a reliable earth ground such as a grounding rod (see Chapter 2, "Components in a Typical Access Point Installation").

Installation Details for the 1552H Access Point

Note   There are differences in the port adapter sizes and threading between the different models. Be sure to review the connector details for the access point model you are installing in Connectors, page 1-7.

The fiber-optic kit (AIR-1520-FIB-REEL=) enables the 1552H access point to support fiber-optic network connections. The kit contains these parts:

- Eight screws (#2-56 x.75 in) to attach reels
- Two small take-up reels
- Two large take-up reels
- Liquid-tight adapter(s)—Accepts a cable diameter of 0.20 to 0.35 inches (0.51 to 0.89 cm)

Caution   The liquid-tight adapter(s) supplied in the kit AIR-1520-FIB-REEL= are IP68/69 certified with .200 to .350 diameter cables but not ATEX certified or hazardous locations compliant. The installer must use cable glands/adapters appropriate to the installation.

Note   The SFP module is a separate orderable item. Refer to the ordering guide for applicable SFP options.

Warning   **Class 1 laser product.** Statement 1008

Note   You need a customer-supplied outdoor-rated fiber-optic cable with an LC connector. The cable diameter must be 0.20 to 0.35 in. (5.1 to 8.9 mm). The diameter of the sheathing surrounding each individual fiber must be 0.040 in. (1.0 mm) or less.

Connecting a Fiber-Optic Cable to the 1552H Access Point

Note   Please refer to the Declarations of Conformity and Regulatory Information when the AIR-CAP1552H-Q-K9 (POE input configuration only) will be installed in an explosive area in Japan.

To connect a fiber-optic cable to the 1552H access point, follow these steps:

Step 1   Ensure that all power sources have been disconnected from the access point.

⚠

Warning   **This unit might have more than one power supply connection. All connections must be removed to de-energize the unit.** Statement 1028

Step 2   Open the hinged cover (see the "Opening the Access Point Hinged Cover" section on page 3-58 for instructions).

Step 3   Place the two large reels with the small reels on top as shown in Figure 3-12.

Step 4   Align the screw holes in the large and small reels, and insert four attachment screws in each of the reel pairs. Tighten the screws to 3 to 4 in. lbs (0.34 to 0.45 Nm).

Step 5   Remove the plug from the end of the SFP module, and insert the module into the SFP receptacle (see Figure 3-12).

Figure 3-12   Fiber-Optic Cable Components (1552H)
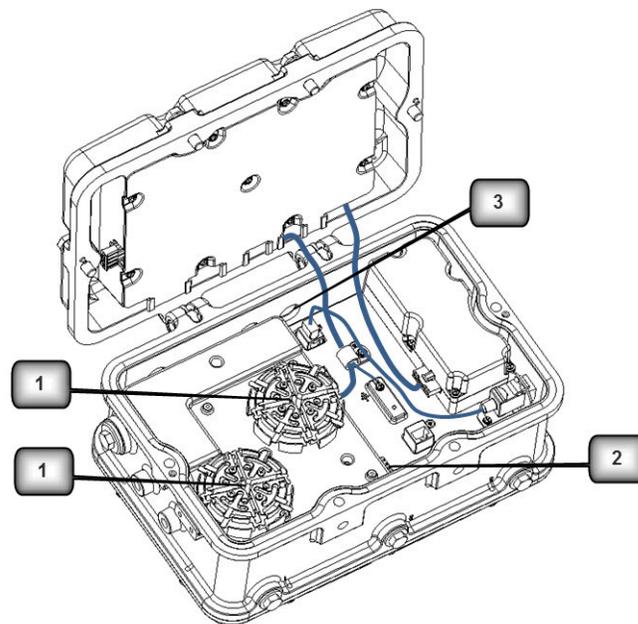
1	Fiber reels (large reel with small reel on top, 4 screws for each reel assembly)
2	SFP module slot
3	Fiber-optic connector port (1552H) Hole size is PG13.5

Step 6   Loosen the round end of the liquid-tight connector by turning counterclockwise, but do not remove (see Figure 3-13).

Figure 3-13   **Liquid -Tight Adapter**

1	Thread end	2	Round end

Step 7   Carefully screw the threaded end of the adapter into the access point and hand-tighten.

Step 8   Use an adjustable wrench, the 22 mm socket, or the Sealcon S-2200-WR wrench to tighten the threaded end of the adapter to 6 to 7 ft lbs (8.1 to 9.5 Nm).

Step 9   Carefully remove approximately 1 to 2 ft (30.5 cm) of the external jacket from the fiber-optic cable, exposing the inner strand.

Step 10   Carefully insert the fiber-optic LC cable connector into the rounded end of the liquid-tight adapter (see Figure 3-13), and push through the adapter.

Step 11   Wrap excess fiber-optic cable around the take-up reels in a figure eight (8) pattern.

Step 12   Insert the fiber-optic LC cable connector into the SFP module.

Step 13   Use an adjustable or open-end wrench to tighten the round end of the adapter to 2.7 to 3.2 ft lbs (3.66 to 4.34 Nm).

Step 14   Close the hinged cover (see the "Closing the Access Point Hinged Cover" section on page 3-59).

Installation Details for the 1552SA and 1552SD Access Point

Note   There are differences in the port adapter sizes and threading between the different models. Be sure to review the connector details for the access point model you are installing in Connectors, page 1-7.

The fiber-optic kit (AIR-1550S-FIB-KIT=) enables the 1552SA and 1552SD access points to support fiber-optic network connections. The kit contains these parts:

- Two take-up reels
- One bracket to support the reels

- Eight screws (#2-56 x .31 in) to attach the reels
- Two screws (#4-40 x .25 in) to attach the bracket
- One grommet
- One port adapter (5/8-24 to 1/2-14 NPT).

✎
Note   The adapter in this kit is EX compliant with the 1552S models.

The installation may require the use of junction boxes which have Ex certifications. Cisco does not supply these, but recommends either the GRT50 or ERT50 models as shown in Figure 3-14.

Figure 3-14   Junction Boxes

✎
Note   The SFP module is a separate orderable item. Refer to the ordering guide for applicable SFP options.

⚠
Warning   **Class 1 laser product.** Statement 1008

✎
Note   You need a customer-supplied outdoor-rated fiber-optic cable with an LC connector. The cable diameter must less than 0.40 in. (10.0 mm). The diameter of the sheathing surrounding each individual fiber must be less than 0.040 in. (1.0 mm).

Connecting a Fiber-Optic Cable to the 1552SA or 1552SD Access Point

Note If a fiber installation kit is required for the installation, please ensure you order the hazardous locations compliant kit, AIR-1550S-FIB-KIT, and follow the instructions on installing the adapter below.

To connect a fiber-optic cable to the 1552SA or 1552SD access point, follow these steps:

Step 1 Ensure that all power sources have been disconnected from the access point.

Warning **This unit might have more than one power supply connection. All connections must be removed to de-energize the unit.** Statement 1028

Step 2 Open the hinged cover (see the "Opening the Access Point Hinged Cover" section on page 3-58 for instructions).

Step 3 Align the reel bracket to the AP and attach via two screws (#4-40 x .25 in). Tighten the screws to 5.5 to 6.0 in. lbs (0.62 to 0.68 Nm). (See Figure 3-15.)

Step 4 Align each of the two reels to the installed bracket. Attach each reel to the bracket with four screws (#2-56 x .31 in). Tighten the screws to 3 to 4 in. lbs (0.34 to 0.45 Nm). (See Figure 3-15.)

Figure 3-15   Fiber-Optic Cable Kit Components (1552SD shown)
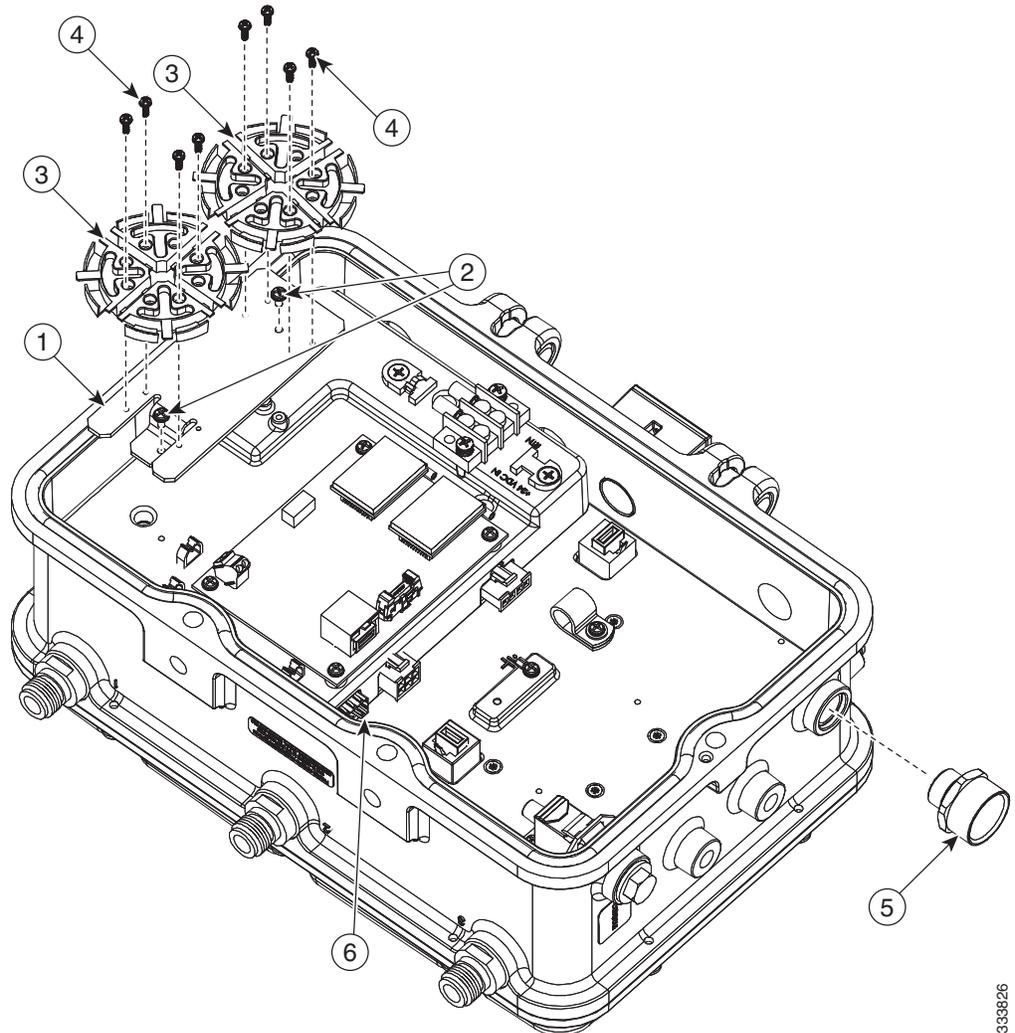
1	Reel bracket	2	Two screws for attaching reel bracket to AP (#4-40 x .25 in)
3	Two fiber reels	4	Eight screws, four to attach each reel to bracket (#2-56 x .31 in)
5	1/2-NPT port adapter from the kit. **Do not use in hazardous location deployments**.	6	SFP module slot

Note   Fiber and power can both be routed through the AC/DC port. If fiber and power are coming from the same area externally, route both through the AC/DC port. If fiber and power are coming from different areas externally, route them through one of the recommended junction boxes.
The rest of this procedure will show routing through an ETRT50 junction box.

Step 5   Attach the junction box to the chassis with a 1/2 NTP Male to Male connector. See Figure 3-16 and Figure 3-17.

Figure 3-16   ERT50 Junction Box Assembly
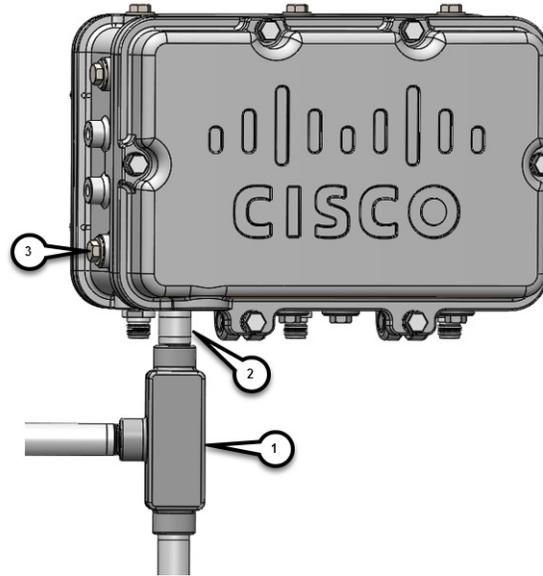
1	ERT50 Junction Box
2	AC/DC Port
3	5/8-24 Port

Step 6   Route the power cable and the fiber cable through the junction box using Figure 3-17 as an example.

Figure 3-17   Routing Detail
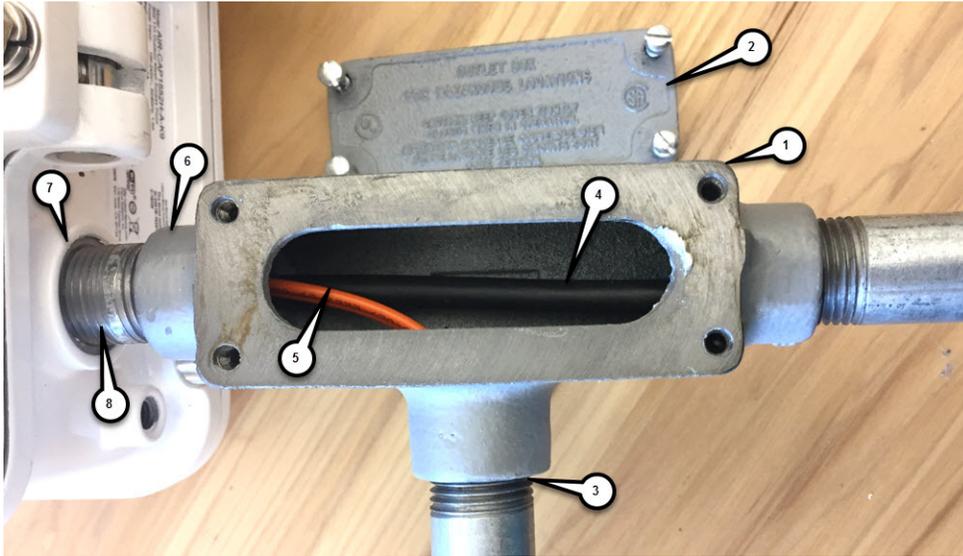
1	ERT50 Junction Box	**2**	ERT50 Junction Box Cover (removed)
3	1/2NPT	**4**	Power Cable
5	Fiber Cable	**6**	1/2NPT
7	1/2NPT	**8**	1/2NPT Male to Male

Step 7   Complete the connections inside the 1552 as shown in Figure 3-18.

Figure 3-18   Inside Connectivity
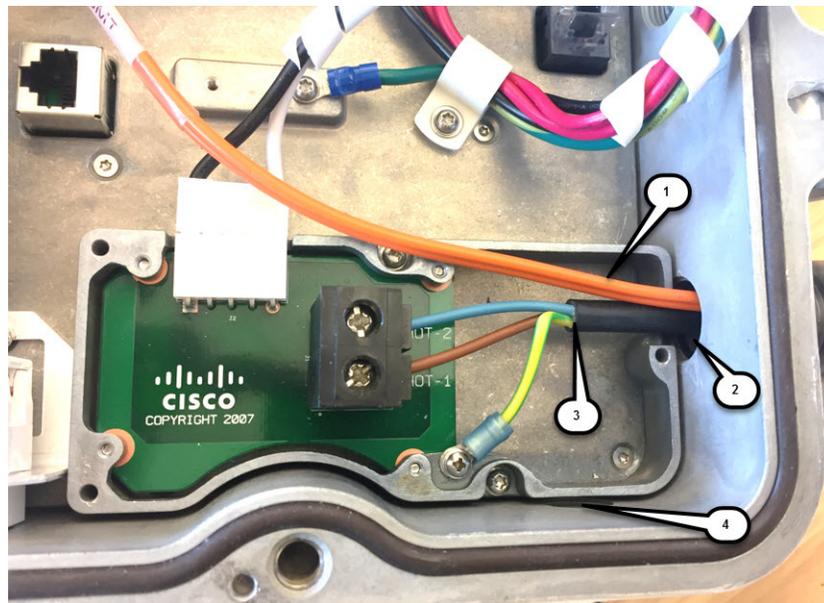
1	Duplex LC Fiber	2	AC/DC Entry Port
3	Power Cable	4	SCTE Port (shown for orientation purposes)

> **Note**   When installing the ½ NPT pipe or cable gland on the AP, the use of a thread sealant (for example, Loctite® 565) is required.

Step 8   Wrap excess fiber-optic cable around the take-up reels using industry-standard methods and cable routing.

Step 9   Insert the fiber-optic LC cable connector into the SFP module.

Step 10   Secure fiber cable inside enclosure using appropriate methods to avoid fiber damage.

Step 11   Close the cover to the junction box and the hinged cover (see Closing the Access Point Hinged Cover, page 3-59).

To complete the connectivity to a power source, go to Powering the Access Point, page 3-71.

Installation Details for the 1552WU Access Point

> **Note**   There are differences in the port adapter sizes and threading between the different models. Be sure to review the connector details for the access point model you are installing in Connectors, page 1-7.

> **Note**   The 1552WU does not support Fiber, therefore, there are no separate installation details for this model.

If installing the 1552WU with a WirelessHART antenna, read the "WirelessHART Gateway Configuration" procedure on page 1-26 before continuing.

Using the Reset Button

The access point has a reset button located on the bottom of the unit (see Figure 3-19). 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 these functions:

- Reset the access point—Press the reset button for less than 10 seconds.
- Disable battery backup power—Press the reset button for more than 10 seconds.

Figure 3-19   Reset Button Location - Models AIR-CAP1552SA/SD-x-K9 and AIR-CAP1552H-x-K9
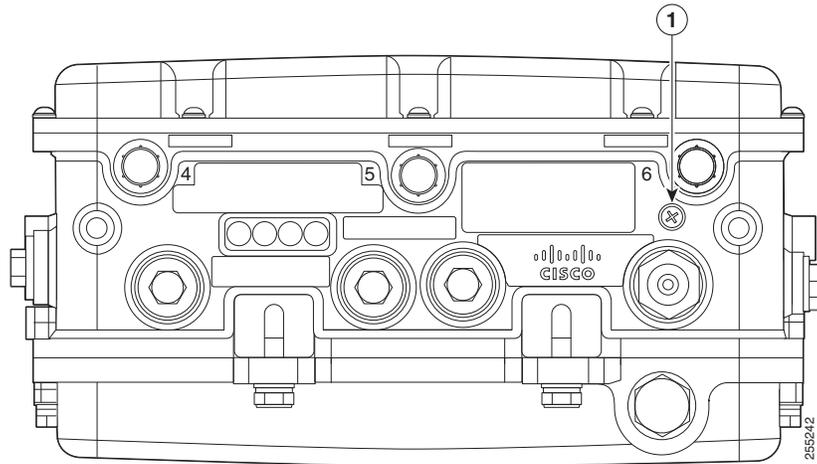
1	Reset button

⚠

Caution   Do not access the reset button in a Hazardous Location.

Rebooting the Access Point

To reboot (power cycle) the access point, follow these steps:

Step 1   Use a Phillips screwdriver to remove the reset button screw (Figure 3-19). Be careful not to lose the screw.

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

Powering the Access Point

Warning   **Explosion Hazard—The area must be known to be nonhazardous before installing, servicing, or replacing the unit.** Statement 1082

Note   Please refer to the Declarations of Conformity and Regulatory Information when the AIR-CAP1552H-Q-K9 (POE input configuration only) will be installed in an explosive area in Japan.

The access point can be powered by one of these methods:

1552H and 1552SA

100 to 240 VAC, 50-60Hz.

1552H

Power-over-Ethernet (PoE)—56 VDC power injector (AIR-PWRINJ1500-2=)

1552SD and 1552WU

24 VDC

Note   In all cases above, the AC branch circuit powering the access point must be limited to no more than 20A from the over-protection device supplied by the user. This branch power protection must meet all local and national electrical codes.

The 1552 access point for hazardous locations can be connected to more than one power source. The access point detects the available power sources and switches to the preferred power source using the following priority:

1. AC power
2. DC power
3. Power over Ethernet

Connecting a 1552H Series Power Injector

The power injector provides 56 VDC to the access point over the Ethernet cable and supports a total end-to-end Ethernet cable length of 100 m (328 ft) from the switch to the access point.

Note   The power injector is not intended to be installed in a hazardous locations environment. If a PoE injector is required, it must be located in a non-hazardous location environment.

Note   The 1552SA/SD and 1552WU do not support PoE In.

Note   The Ethernet cable from the power injector to the access point (PoE In port) must be at least 10 ft (3.1 m) in length.

Note   The PoE Out port is disabled when the access point is powered by the power injector.

When your access point is powered by an optional power injector, follow these steps to complete the installation:

Step 1   Before applying PoE to the access point, ensure that the access point is grounded (see the "Grounding the Access Point (all models)" section on page 3-60).

Step 2   Review Chapter 2, "Pole Mount Installation" to identify the components needed for the installation.

Note   It is recommended to install the injector in its own IP67 enclosure such as a Hoffman box, since the PoE injector is not weather proof.

Step 3   Connect a CAT5e or better Ethernet cable from your wired LAN network to the power injector.

Warning   **To reduce the risk of fire, use only No. 26 AWG or larger telecommunication line cord.** Statement 1023

Use only the 1500 power injector (AIR-PWRINJ1500-2=) for the access point. This power injector is designed to meet the power requirements of the access point and is a listed Class 2 limited power source (LPS).

Note   The installer is responsible for ensuring that powering the access point from this type of power injector is allowed by local and/or national safety and telecommunications equipment standards.

Tip   To forward bridge traffic, add a switch between the power injector and controller. Refer to the *Cisco Wireless Mesh Access Points, Design and Deployment Guide, Release 7.0* for more information.

Step 4   Ensure that the antennas are connected and that a ground is attached to the access point before you apply power to the access point.

Step 5   Connect a shielded outdoor-rated Ethernet (CAT5e or better) cable between the power injector and the PoE In connector of the access point (see Figure 3-20).

Step 6   Connect the Ethernet cable to the access point PoE In port (see "Connecting an Ethernet Cable to the Access Point (all models)" section on page 3-73).

Note   When a 1552H access point is powered by PoE, the PoE Out port is not active.

Step 7   Continue with the "What to Do Next" section on page 3-80.

Connecting an Ethernet Cable to the Access Point (all models)

✎

Note   Please refer to the Declarations of Conformity and Regulatory Information when the AIR-CAP1552H-Q-K9 (POE input configuration only) will be installed in an explosive area in Japan.

The following tools and materials are required:

- Shielded outdoor-rated Ethernet (CAT5e or better) cable with 0.2 to 0.35 in. (0.51 to 0.89 cm) diameter

  ✎

  Note   The Ethernet cable from the power injector to the access point must be at least 10 ft (3.05 m) long. The PoE Out port is disabled when the access point is powered by the power injector.

- RJ-45 connector and installation tool
- Adjustable wrench

To connect the shielded Ethernet cable to the access point, follow these steps:

Step 1   Disconnect power to the power injector, and ensure all power sources to the access point are turned off.

⚠

Warning   **This unit might have more than one power supply connection. All connections must be removed to de-energize the unit.** Statement 1028

Step 2   Ensure a 6 AWG ground wire is connected to the access point (see the "Grounding the Access Point (all models)" section on page 3-60).

Step 3   Use an adjustable wrench, a 22-mm socket, or the Sealcon S-2200-WR wrench to remove the Ethernet connector plug from the access point (see Figure 3-20 for the location).

Figure 3-20   *Location of Ethernet Liquid-Tight Adapters (Only Models AIR-CAP1552SA/SD-x-K9, AIR-CAP1552H-x-K9, and AIR-CAP1552WU-A-K9)*
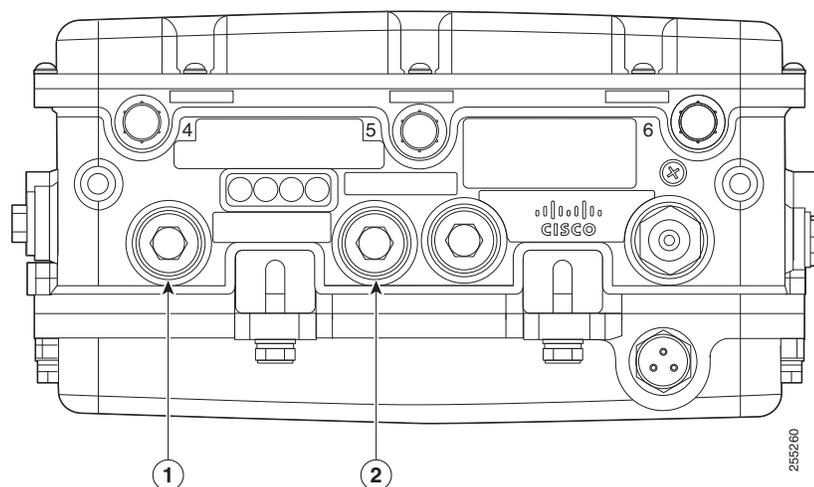
1	ETH port (1552SA/1552SD/1552WU) or PoE In port (1552H) Hole size PG13.5	2	PoE Out port Hole size PG13.5

✎

Note   For information on data cable entry, refer to Figure 1-1 on page 1-7

Step 4   Loosen the round end of the liquid-tight adapter by turning counterclockwise, but do not remove (see Figure 3-21).

Figure 3-21   *Liquid-tight Adapter*

1	Thread end	2	Round end

⚠

Caution   The liquid-tight adapter(s) supplied in the kit AIR-1520-FIB-REEL= are IP68/69 certified with .200 to .350 diameter cables but not ATEX certified or hazardous locations compliant. The installer must use cable glands and/or adapters appropriate to the installation.

Step 5   Insert the unterminated end of the Ethernet cable into the round end of the liquid-tight adapter (see Figure 3-21), and pull several inches of cable through the adapter.

Step 6   Install an RJ-45 connector on the unterminated end of the Ethernet cable using your Ethernet cable installation tool.

⚠

Warning   **To reduce the risk of fire, use only No. 26 AWG or larger telecommunication line cord.** Statement 1023

Step 7   Carefully insert the RJ-45 cable connector into the Ethernet port opening on the access point, and connect to the internal Ethernet connector (see Figure 3-22).

Figure 3-22   Inserting RJ-45 Connector into the Ethernet Port Opening in Case
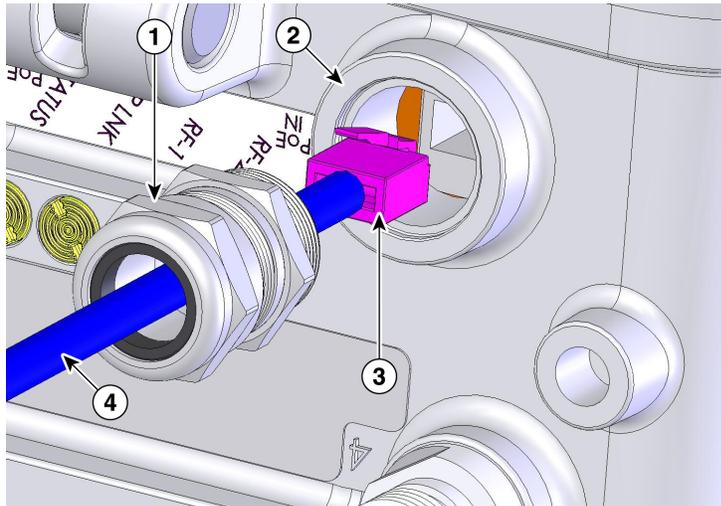
1	Liquid-tight adapter (PG 13.5 thread size)	3	RJ-45 connector
2	Ethernet port opening in access point case	4	Shielded outdoor-rated Ethernet (CAT5e or better) cable

Step 8 Slide the liquid-tight adapter towards the access point, and screw the threaded end of the adapter into the access point, and hand-tighten.

Step 9 Use an adjustable wrench, a 22-mm socket, or a Sealcon S-2200-WR wrench to tighten the threaded end of the adapter to 6 to 7 ft lbs (8.1 to 9.5 Nm).

Step 10 Use an adjustable wrench and tighten the round end of the adapter to 2.7 to 3.2 ft lbs (3.66 to 4.34 Nm).

Step 11 Ensure that the antennas are connected to the access point before you apply power to the access point.

Step 12 Route your Ethernet cable, and cut off any excess cable.

Step 13 Install an RJ-45 connector on the unterminated cable end, and insert it into the power injector. For typical installation components, see Chapter 2, "Components in a Typical Access Point Installation".

Step 14 Turn on power to the power injector.

Connecting a 24 VDC Power Cable to the Access Point

⚠️

Caution The DC branch circuit powering the access point must be limited to no more than 10A from the over-protection device supplied by the user. This branch power supplemental protection and all connecting conduit, must meet all local and national electrical codes.

To route and connect the 24 VDC power cable to the 1552SA/1552SD or 1552WU access point model, follow these steps:

Step 1   Open the access point hinged cover. See the "Opening the Access Point Hinged Cover" section on page 3-58 for instructions.

Figure 3-23   *24 VDC Power Installation—Model AIR-CAP1552SD-A-K9 and AIR-CAP1552WU-A-K9*

1	Terminal block	2	Customer-supplied harness
		3	Customer-supplied 1/2" NPT Pipe (North American/ATEX) or sheathed cable (ATEX only). The installer/integrator is responsible for supplying the appropriate certified components as part of the overall designed system and must maintain the access point environmental integrity of IP67 rating.

Step 2   Route the 24 VDC power cable through the 1/2-NPT port.

Step 3   Use a wire stripper tool to remove the insulation from each wire. Remove only enough wire to provide adequate crimp on to ring terminals (Cisco supplied).

Step 4   Remove terminal strip screw and square washer for connection labeled "RTN". Connect DC return line to terminal strip location labeled "RTN". Tighten terminal strip screw to secure ring terminal and wire.

Step 5   Remove terminal strip screw and square washer for connection labeled "+24 VDC IN". Connect +24 VDC hot line to terminal strip location labeled "+24 VDC IN". Tighten terminal strip screw to secure ring terminal and wire.

Step 6   Secure DC input cord to wire tie anchor adjacent to terminal strip.

Step 7   Check your work.

Step 8   Close the access point hinged cover. See the "Closing the Access Point Hinged Cover" section on page 3-59 for details.

Connecting Ground and AC Power

✎
Note   When you install the conduit, be sure to comply with the local electrical codes for your area.

Refer to "Table D-2Power Consumption Budget for the AIR-CAP1552H-x-K9, AIR-CAP1552SA/SD-x-K9, and AIR-CAP1552WU-A-K9 Access Point Configurations" section on page D-22 for Power distribution details.

To route and connect the ground and AC power cabling to the 1552H or 1552SA access point model, follow these steps:

⚠
Warning   **When installing or replacing the unit, the ground connection must always be made first and disconnected last.** Statement 1046

⚠
Caution   Always install the ground wire before connecting all power leads.

Step 1   Open the access point hinged cover. See the "Opening the Access Point Hinged Cover" section on page 3-58 for instructions.

Step 2   Use a Phillips head screwdriver to loosen the three captive screws that secure the AC entry module cover. (Figure 3-24).

Figure 3-24   AC Power Installation—Model AIR-CAP1552H-A-K9
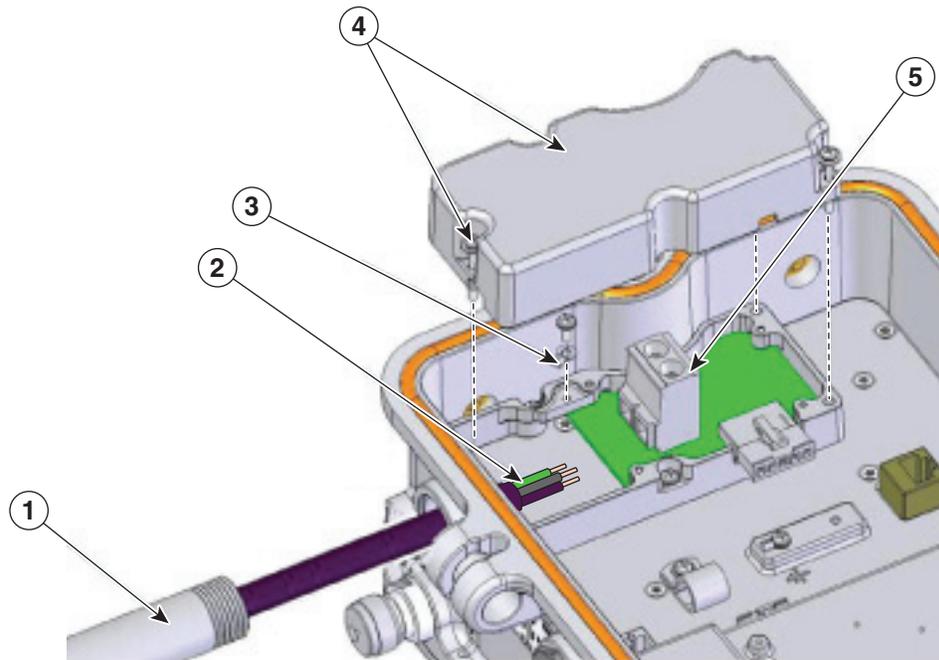
1	Customer-supplied 1/2" NPT Pipe (North American/ATEX) or sheathed cable (ATEX only).	4	AC Entry Cover • Loosen the captive screws (3x) to open cover. • Reattach after harness has been installed.
2	Customer-supplied harness	5	Terminal block
3	Attach GND wire to terminal ring. Attach terminal ring to chassis as shown.		

Notes	
1	The installer/integrator is responsible for supplying the appropriate certified components as part of the overall designed system and must maintain the access point environmental integrity of IP67 rating.
2	The water-tight gland device selected by the installer/integrator must be equal to or greater (better) than the specifications listed for device referenced as Sealcon CD-13AR-EX with a Buna-N O-ring.
3	The torque specification for water-tight glands are 6 to 7 ft-lbs (8.1 to 9.5 N.m).

Step 3   Remove the cover and set it aside.

Step 4   Route the AC power cable through the 1/2-NPT port.

Step 5   Use a wire stripper tool to remove the insulation from each wire. Remove only enough wire to provide a solid connection in the terminal block. The hot wires should have no bare wire exposed after the connection is made.

Step 6   Insert the ground wire into the provided ground lug and use a crimping tool to secure the connection.

Step 7   Install the ground lug and tighten the connection with a Phillips screwdriver. To prevent stripping the screw threads, do not overtighten.

Step 8   Insert each hot wire into the AC entry terminal block.

Step 9   Use a Phillips screwdriver to tighten the terminal block set screws to secure the wires in the terminal block.

Step 10   Verify that no bare wire is exposed. If wire is exposed, remove it from the terminal block, adjust the length, and reinstall.

Step 11   Check your work.

Step 12   Reinstall the AC entry module top cover and tighten the captive screws. Do not overtighten.

Step 13   Close the access point hinged cover. See the "Closing the Access Point Hinged Cover" section on page 3-59 for details.

Step 14   Install the Ethernet backhaul cable. See the next section for instructions.

Performing Maintenance

The access point requires minimal periodic or preventive maintenance as it has no moving parts, filters, lubricants, or mechanical contact components. However, when installed in a hazardous location, periodic inspections should be conducted in order to ensure that the access point is operating satisfactory. This section provides information about performing maintenance on an access point installed in a hazardous location.

Additional maintenance information can be found in Chapter 4, "Troubleshooting" and the *Troubleshooting a Mesh Network Guide.* The troubleshooting document is available at cisco.com at the following URL:

http://www.cisco.com/en/US/docs/wireless/access_point/1520/troubleshooting/guide/TrbleshtMesh.html

Warning   **Do not disconnect connections to this equipment unless power has been removed or you have verified that the area is nonhazardous. Secure any external connections that mate to this equipment by using screws, sliding latches, threaded connectors, or other means provided with this product. Substitution of components may impair suitability for Class I, Zone 2, Division 2.** Statement 1062

Warning   **If you connect or disconnect the console cable with power applied to the unit or any device on the network, an electrical arc can occur. This could cause an explosion in hazardous location installations. Be sure that power is removed or the area is nonhazardous before proceeding.**

To verify unit operation, perform POST on the device in a nonhazardous location before installation. Statement 1080

**Warning**   **When installing or replacing the unit, the ground connection must always be made first and disconnected last.** Statement 1046

Removing the Access Point from Service

When removing an access point from service, make sure you remove power from the access point before opening the cover and disconnecting the AC input wiring. When removing the AC wiring, the ground connection should be the last to be disconnected.

Conducting Periodic Inspections

The access point should be inspected periodically to ensure normal and airtight operation in the hazardous location environment. Table 3-3 lists the inspection routines and their periodicity.

Table 3-3   Periodic Inspection Table

Inspection Routine	Periodicity
Inspect O-ring seals and exterior electrical connections for aging, corrosion, and low ground resistance.	Every 3 years
Inspect cover and liquid-tight adapter gaskets for airtightness.	Every 5 years

Conducting Periodic Cleaning

The access point is designed to not require periodic cleaning.

What to Do Next

When you power up a MAP that is not connected to a wired Ethernet, fiber-optic, or cable network to the controller, the access point uses the Cisco Adaptive Wireless Path Protocol (AWPP) to bind to another mesh access point (MAP) with the best path to a root access point (RAP) connected to the wired network to a controller. The access point sends a discovery request when powered up. If you have configured the access point in the controller correctly, the controller sends back a discovery response to the access point. When that happens, the access point sends out a join request to the controller, and the controller responds with a join confirmation response. Then the access point establishes a Control And Provisioning of Wireless Access Points (CAPWAP) connection to the controller and gets the shared secret configured on the controller.

Refer to the *Cisco Wireless LAN Controller Configuration Guide* for more information on configuring, monitoring, and operating your access points.

Troubleshooting

This chapter provides troubleshooting procedures for basic problems with the access point. For the most up-to-date, detailed troubleshooting information, refer to the Cisco Technical Support and Documentation website at the following URL:

http://www.cisco.com/cisco/web/support/index.html

Sections in this chapter include:

Guidelines for Using the Access Points

You should keep these guidelines in mind when you use the access points:

- The access point can only communicate with controllers and cannot operate independently.

- The access point does not support Wireless Domain Services (WDS) and cannot communicate with WDS devices. However, the controller provides functionality equivalent to WDS when the access point associates to it.

- The access point only supports Layer 3 CAPWAP communications with the controllers.

  In Layer 3 operation, the access point and the controller can be on the same or different subnets. The access point communicates with the controller using standard IP packets. A Layer 3 access point on a different subnet than the controller requires a DHCP server on the access point subnet and a route to the controller. The route to the controller must have destination UDP ports 12222 and 12223 open for CAPWAP communications. The route to the primary, secondary, and tertiary controllers must allow IP packet fragments.

- Before deploying your access points, ensure that the following has been done:

  – Your controllers are connected to switch ports that are configured as trunk ports.

  – Your access points are connected to switch ports that are configured as untagged access ports.

  – A DHCP server is reachable by your access points and has been configured with Option 43. Option 43 provides the IP addresses of the management interfaces of your controllers. Typically, a DHCP server can be configured on a Cisco switch.

  – Optionally, a DNS server can be configured to enable CISCO-CAPWAP-CONTROLLER. Use *local domain* to resolve to the IP address of the management interface of your controller.

  – Your controllers are configured and reachable by the access points.

  – Your controllers are configured with the access point MAC addresses and the MAC filter list is enabled.

  – If layer 3 functionality is enabled on your switch, make sure that DHCP broadcast and request can be passed.

- The access point PoE Out port should be connected only to a single peripheral customer device, such as a camera or sensor gateway. We recommend that the PoE Out port not be connected to a switch or hub.

- After the access points are associated to the controller, you should change the bridge group name (BGN) from the default value. With the default BGN, the mesh access points (MAPs) can potentially try to connect with other mesh networks and slow down the convergence of the network.

Important Notes

Convergence Delays

During deployment, the access points can experience convergence delays due to various causes. The following list identifies some operating conditions that can cause convergence delays:

- A root access point (RAP) attempts to connect to a controller using any of the wired ports (cable, fiber-optic, PoE In, or PoE Out). If the wired ports are operational, the RAP can potentially spend several minutes on each port prior to connecting to a controller.

- If a RAP is unable to connect to a controller over the wired ports, it attempts to connect using the wireless network. This results in additional delays when multiple potential wireless paths are available.
- If a MAP is unable to connect to a RAP using a wireless connection, it then attempts to connect using any available wired port. The access point can potentially spend several minutes for each connection method, before attempting the wireless network again.

Bridge Loop

The access point supports packet bridging between wired and wireless network connections. The same network must never be connected to multiple wired ports on an access point or on two bridged access points. A bridge loop causes network routing problems.

Controller DHCP Server

The controller DHCP server only assigns IP addresses to lightweight access points, Ethernet bridging clients on the mesh access points, and wireless clients associated to an access point. It does not assign an IP address to other devices.

MAP Data Traffic

If the signal on the access point backhaul channel has a high signal-to-noise ratio, it is possible for a MAP to connect to the controller, via parent node, but not be able to pass data traffic, such as pinging the access point. This can occur because the default data rate for backhaul control packets is set to 6 Mb/s, and the backhaul data rate set to auto by the user.

Controller MAC Filter List

Before activating your access point, you must ensure that the access point MAC address has been added to the controller MAC filter list and that **Mac Filter List** is enabled.

Note   The access point MAC address and barcode is located on the bottom of the unit. When two MAC addresses are shown, use the top MAC address.

To view the MAC addresses added to the controller MAC filter list, you can use the controller CLI or the controller GUI:

- Controller CLI—Use the **show macfilter summary** controller CLI command to view the MAC addresses added to the controller filter list.
- Controller GUI—Log into your controller web interface using a web browser, and choose **SECURITY > AAA > MAC Filtering** to view the MAC addresses added to the controller filter list.

Using DHCP Option 43

You can use DHCP Option 43 to provide a list of controller IP addresses to the access points, enabling the access point to find and join a controller. Refer to the product documentation for your DHCP server for instructions on configuring DHCP Option 43. For additional information, refer to Appendix F, "Configuring DHCP Option 43".

Monitoring the Access Point LEDs

If your access point is not working properly, look at the LEDs on the bottom of the unit. You can use them to quickly assess the status of the unit. Figure 4-1 shows the location of the access point LEDs.

Figure 4-1   Access Point LEDs - Shown on the Bottom of Model AIR-CAP1552SA/SD-x-K9
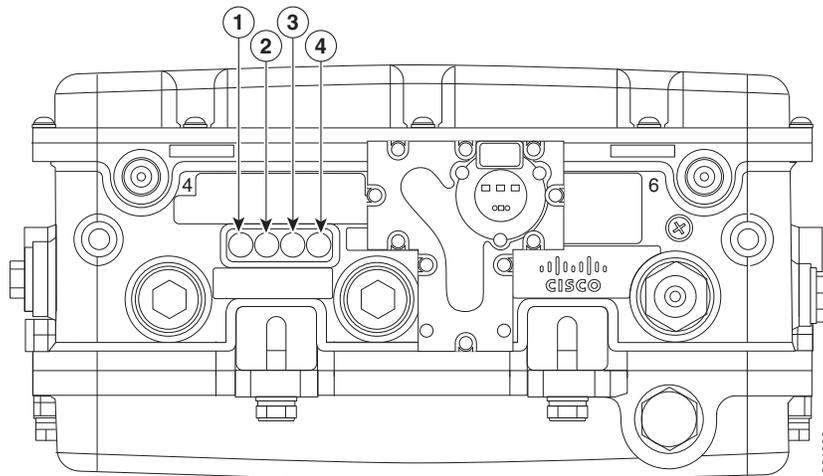
1	RF-2 LED—Status of the 5 GHz MIMO backhaul radio	**3**	Uplink LED—Ethernet, cable, or fiber status
2	RF-1 LED—Status of the 2.4 GHz MIMO access radio	**4**	Status LED—access point and software status

Note   It is expected that there will be small variations in LED color intensity and hue from unit to unit. This is within the normal range of the LED manufacturer specifications and is not a defect.

The access point LED signals are listed in Table 4-1.

Table 4-1   Access Point LED Signals

LED	Color[1, 2]	Meaning
Status	Black	No power applied or LED off.
	Steady green	Access point is operational.
	Blinking green	Download or upgrade of Cisco IOS image file in progress.
	Steady amber	Mesh neighbor access point discovery in progress.
	Blinking amber	Mesh authentication in progress.
	Blinking red / green /amber	CAPWAP discovery in progress.
	Steady red	Firmware failure. Contact your support organization for assistance.
Uplink	Black	All network ports down or LED off.
	Steady green	Uplink port is operational (cable, fiber optic, or Ethernet).
RF-1	Black	Radio turned off or LED off.
	Steady green	Radio is operational; network is good.
	Steady red	Firmware failure. Contact your support organization for assistance.
RF-2	Black	Radio is turned off or LED off.
	Steady green	Radio is operational; network is good.
	Steady red	Firmware failure. Contact your support organization for assistance.

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

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

Verifying Controller Association

To verify that your access point is associated to the controller, follow these steps:

Step 1   Log into your controller web interface using a web browser.

You can also use the controller CLI **show ap summary** command from the controller console port.

Step 2   Click **Wireless,** and verify that your access point MAC address is listed under Ethernet MAC.

Step 3   Log out of the controller, and close your web browser.

Changing the Bridge Group Name

The bridge group name (BGN) controls the association of the access points to a RAP. BGNs can be used to logically group the radios to avoid different networks on the same channel from communicating with each other. This setting is also useful if you have more than one RAP in your network in the same area.

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

The BGN is a string of ten characters maximum. A factory-set bridge group name (NULL VALUE) is assigned during manufacturing. It is not visible to you, but allows new access point radios to join a network of new access points. The BGN can be reconfigured from the Controller CLI and GUI. After configuring the BGN, the access point reboots.

After the access points are deployed and associated to the controller, the BGN should be changed from the default value to prevent the MAPs from attempting to associate to other mesh networks.

The BGN should be configured very carefully on a live network. You should always start with the most distant access point (last node) from the RAP and move towards the RAP. If you start configuring the BGN in a different location, then the access points beyond this point (farther away) are dropped, as they have a different BGN. MAPS with unconfigured BGNs will periodically join to RAPs with configured BGNs. This prevents the stranding of MAPs.

To configure the BGN for the access points using the controller GUI, follow these steps:

Step 1 Log into your controller using a web browser.

Step 2 Click **Wireless**. When access points associates to the controller, the access point name appears in the AP Name list.

Step 3 Click on an access point name.

Step 4 Find the Mesh Information section, and enter the new BGN in the Bridge Group Name field.

Step 5 Click **Apply**.

Step 6 Repeat Steps 2 through 5 for each access point.

Step 7 Log out from your controller, and close your web browser.

Connecting to the Access Point Locally

If you need to monitor the access point locally (without connecting the access point to a wired LAN), you can connect a PC to its console port using a DB-9 to RJ-45 serial cable.

Note The console port should only be used for debugging in a lab environment.

Follow these steps to open the CLI by connecting to the access point console port:

Step 1 Open the hinged cover of the access point (if necessary) (see "Working with the Access Point Hinged Cover" section on page 3-58 for instructions).

Connect a nine-pin, female DB-9 to RJ-45 serial cable to the RJ-45 console port on the access point and to the COM port on a computer (see Figure 4-2 for the console port locations).

Figure 4-2   Console Port Location on Access Point Models (AIR-CAP1552SA/SD-x-K9 Shown)

1	Console port	2	Not used
	✎ **Note** Not used for 1552WU. The 1552WU console is only available by opening the device and connecting to the internal console port.		

✎

Note   The Cisco part number for the DB-9 to RJ-45 serial cable is AIR-CONCAB1200. To order a serial cable, browse to:

http://www.cisco.com/pcgi-bin/marketplace/welcome.pl

Step 2   Set up a terminal emulator program on your PC to communicate with the access point. Use the following settings for the terminal emulator connection: 9600 baud, 8 data bits, no parity, 1 stop bit, and no flow control.

Step 3   When finished, remove your serial cable, and close the hinged cover (see the "Working with the Access Point Hinged Cover" section on page 3-58 for instructions).

Access Point Power Injector

The power injector (AIR-PWRINJ1500-2=) has three LEDs on the front end of the case (see Figure 4-3). For detailed information on the power injector, see the *Cisco Aironet 1550 Series Outdoor Mesh Access Point Power Injector Installation Instructions*.

⚠

Caution   Caution: Power injector (AIR-PWRINJ1500-2=) is not certified for installation within hazardous locations environments.

Figure 4-3   Power Injector Connectors and LEDs

1	Mounting tabs	4	AC POWER LED
2	AP POWER LED	5	TO AP—Ethernet connector (RJ-45) to access point (10/100/1000BASE-T)
3	FAULT LED	6	TO SWITCH—Ethernet connector (RJ-45) to switch (10/100/1000BASE-T)

Monitoring the Power Injector LEDs

You can use the power injector LEDs to check the power injector status. The LEDs provide the following status information:

- AP POWER—Turns solid green after successful discovery; indicates that power injector is supplying power to the access point.

- FAULT—Turns solid red when a fault occurs during discovery mode or power-up. Check Ethernet cables and connections before contacting your support organization for assistance.

- AC POWER—Turns solid green when power injector is receiving AC power and is ready to provide power to the access point.

Translated Safety Warnings

For translated safety warnings, refer to the safety warning document that shipped with your access point or that is available on Cisco.com.

To browse to the document on Cisco.com, follow these steps:

Step 1 Click this link and go to the Cisco Wireless documentation home page:

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

Step 2 Click **Support** and the Support and Documentation page displays.

Step 3 Click **Wireless** in the Find Product Support column**.**

Step 4 Click **1550**.

Step 5 Click **Install and Upgrade**.

Step 6 Click **Install and Upgrade Guides**.

Step 7 Click **Translated Safety Warnings for Cisco Aironet 1550 Series Outdoor Mesh Access Points**.

Declarations of Conformity and Regulatory Information

This appendix provides declarations of conformity and regulatory information for the Cisco Aironet 1552 Outdoor Mesh Access Point.

This appendix contains the following sections:

Manufacturers Federal Communication Commission Declaration of Conformity Statement

<div align="center">

FC **Tested To Comply With FCC Standards**

FOR HOME OR OFFICE USE

</div>

Models: **FCC Certification number:**

AIR-CAP1552SA/SD-A-K9   LDK102074P

AIR-CAP1552H-A-K9

AIR-CAP1552WU-x-K9

Manufacturer:

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

This device complies with Part 15 rules. Operation is subject to the following two conditions:

1. This device may not cause harmful interference, and

2. This device must accept any interference received, including interference that may cause undesired operation.

This equipment has been tested and found to comply with the limits of a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a residential environment. This equipment generates, uses, and radiates radio frequency energy, and if not installed and used in accordance with the instructions, may cause harmful interference. However, there is no guarantee that interference will not occur. If this equipment does cause interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to correct the interference by one of the following measures:

- Reorient or relocate the receiving antenna.

- Increase separation between the equipment and receiver.

- Connect the equipment to an outlet on a circuit different from which the receiver is connected.

- Consult the dealer or an experienced radio/TV technician.

⚠️

Caution   The Part 15 radio device operates on a non-interference basis with other devices operating at this frequency when using Cisco-supplied antennas. Any changes or modification to the product not expressly approved by Cisco could void the user's authority to operate this device.

⚠

Caution   To meet regulatory restrictions, the access point must be professionally installed.

Industry Canada

Models:	IC Certification Number:
AIR-CAP1552SA/SD-A-K9	2461B-102074P
AIR-CAP1552H-A-K9	
AIR-CAP1552WU-x-K9	

Canadian Compliance Statement

This Class B Digital apparatus meets all the requirements of the Canadian Interference-Causing Equipment Regulations.

Cet appareil numerique de la classe B respecte les exigences du Reglement sur le material broilleur du Canada.

This device complies with Class B Limits of Industry Canada. Operation is subject to the following two conditions:

1. This device may not cause harmful interference, and

2. This device must accept any interference received, including interference that may cause undesired operation.

Cisco Aironet Access Points are certified to the requirements of RSS-210. The use of this device in a system operating either partially or completely outdoors may require the user to obtain a license for the system according to the Canadian regulations. For further information, contact your local Industry Canada office.

The 1552H device has been designed to operate with antennas having a maximum gain of 4 dBi for 2.4 GHz and 7 dBi for 5 GHz. Antennas having a gain greater are strictly prohibited for use with this device. The required antenna impedance is 50 ohms.

The 1552SA/1552SD device has been designed to operate with antennas having a maximum gain of 4 dBi for 802.11 and 14 dBi for the sensor (802.15.4) radio in the 2.4 GHz band and 7 dBi in the 5 GHz band. Antennas having a gain greater are strictly prohibited for use with this device. The required antenna impedance is 50 ohms.

To reduce potential radio interference to other users, the antenna type and its gain should be so chosen that the equivalent isotropically radiated power (EIRP) is not more than necessary for successful communication.

Declaration of Conformity for RF Exposure

This access point product has been found to be compliant to the requirements set forth in CFR 47 Section 1.1307 addressing RF Exposure from radio frequency devices as defined in Evaluating Compliance with FCC Guidelines for Human Exposure to Radio Frequency Electromagnetic Fields.T he antennas should be positioned more than 7.9 in (20 cm) from the body of all persons.

This access point is also compliant to EN 50835 for RF exposure.

European Community, Switzerland, Norway, Iceland, and Liechtenstein

Access Point Models:

AIR-CAP1552H-E-K9

AIR-CAP1552SA-E-K9

AIR-CAP1552SD-E-K9

AIR-CAP1552WU-E-K9

Declaration of Conformity with regard to the R&TTE Directive 1999/5/EC & Medical Directive 93/42/EEC

This declaration is only valid for configurations (combinations of software, firmware, and hardware) provided and supported by Cisco Systems. The use of software or firmware not provided and supported by Cisco Systems may result in the equipment no longer being compliant with the regulatory requirements.

> The equipment is in compliance with the essential requirements and other relevant provisions of Directive 1999/5/EC.

The following standards were applied:

EMC—EN 301.489-1 v1.8.1; EN 301.489-17 v2.1.1

Health & Safety—EN60950-1: 2005; EN 50385: 2002

Radio—EN 300 328 v 1.7.1; EN 301.893 v 1.5.1

The conformity assessment procedure referred to in Article 10.4 and Annex III of Directive 1999/5/EC has been followed.

This device also conforms to the EMC requirements of the Medical Devices Directive 93/42/EEC.

Note This equipment is intended to be used in all EU and EFTA countries. Outdoor use may be restricted to certain frequencies and/or may require a license for operation. For more details, contact Cisco Corporate Compliance.

The product carries the CE Mark:

Operation of Cisco Aironet Access Points in Brazil

This section contains special information for operation of Cisco Aironet access points in Brazil.

Access Point Models

AIR-CAP1552H-E-K9

AIR-CAP1552SA-E-K9

AIR-CAP1552SD-E-K9

AIR-CAP1552WU-E-K9

Regulatory Information

Figure 1 contains Brazil regulatory information for the access point models identified in the previous section.

Figure 1   Brazil Regulatory Information

Declaration of Conformity for RF Exposure

The following is the declaration of conformity for RF exposure for the United States, Canada, European Union and Australia.

United States

This system has been evaluated for RF exposure for Humans in reference to ANSI C 95.1 (American National Standards Institute) limits. The evaluation was based on ANSI C 95.1 and FCC OET Bulletin 65C rev 01.01. The minimum separation distance from the antenna to general bystander is 7.9 inches (20cm) to maintain compliance.

Canada

This system has been evaluated for RF exposure for Humans in reference to ANSI C 95.1 (American National Standards Institute) limits. The evaluation was based on RSS-102 Rev 2. The minimum separation distance from the antenna to general bystander is 7.9 inches (20cm) to maintain compliance.

European Union

This system has been evaluated for RF exposure for Humans in reference to the ICNIRP (International Commission on Non-Ionizing Radiation Protection) limits. The evaluation was based on the EN 50385 Product Standard to Demonstrate Compliance of Radio Base stations and Fixed Terminals for Wireless Telecommunications Systems with basic restrictions or reference levels related to Human Exposure to Radio Frequency Electromagnetic Fields from 300 MHz to 40 GHz. The minimum separation distance from the antenna to general bystander is 20cm (7.9 inches).Dual antennas used for diversity operation are not considered co-located.

Australia

This system has been evaluated for RF exposure for Humans as referenced in the Australian Radiation Protection standard and has been evaluated to the ICNIRP (International Commission on Non-Ionizing Radiation Protection) limits. The minimum separation distance from the antenna to general bystander is 20cm (7.9 inches).

Guidelines for Operating Cisco Aironet Access Points in Japan

This section provides guidelines for avoiding interference when operating Cisco Aironet access points in Japan. These guidelines are provided in both Japanese and English.

Lightweight Access Point Model:

AIR-CAP1552SA/SD-Q-K9

AIR-CAP1552H-Q-K9 (POE input configuration only)

Japanese Translation

この機器の使用周波数帯では、電子レンジ等の産業・科学・医療用機器のほか工場の製造ライン等で使用されている移動体識別用の構内無線局（免許を要する無線局）及び特定小電力無線局（免許を要しない無線局）が運用されています。

1 この機器を使用する前に、近くで移動体識別用の構内無線局及び特定小電力無線局が運用されていないことを確認して下さい。

2 万一、この機器から移動体識別用の構内無線局に対して電波干渉の事例が発生した場合には、速やかに使用周波数を変更するか又は電波の発射を停止した上、下記連絡先にご連絡頂き、混信回避のための処置等(例えば、パーティションの設置など)についてご相談して下さい。

3 その他、この機器から移動体識別用の特定小電力無線局に対して電波干渉の事例が発生した場合など何かお困りのことが起きたときは、次の連絡先へお問い合わせ下さい。

連絡先：03-6434-6500

English Translation

This equipment operates in the same frequency bandwidth as industrial, scientific, and medical devices such as microwave ovens and mobile object identification (RF-ID) systems (licensed premises radio stations and unlicensed specified low-power radio stations) used in factory production lines.

1. Before using this equipment, make sure that no premises radio stations or specified low-power radio stations of RF-ID are used in the vicinity.

2. If this equipment causes RF interference to a premises radio station of RF-ID, promptly change the frequency or stop using the device; contact the number below and ask for recommendations on avoiding radio interference, such as setting partitions.

3. If this equipment causes RF interference to a specified low-power radio station of RF-ID, contact the number below.

Contact Number: 03-6434-6500

Japanese Translation

日本の防爆認定に関する指定注意事項は以下の通りです。(AIR-CAP1552H-Q-K9のみ)
1 装置に接続される各種ケーブルは65℃以上の耐熱ケーブルを使用してください。
2 本装置の入出力ポートには以下のケーブルグランド・ブラインドプラグを使用します。
（2017年1月現在の防爆認定指定部品）
　Fiber Port及びPoEポートのケーブルグランド
　　セフテック電装株式会社製 耐圧ケーブルグランドSFGU10-M-ES
　　セフテック電装株式会社製 ブラインドプラグPXN10-M20
3 アンテナの脱着は爆発性雰囲気中・危険場所では行わないでください。

English Translation

Specific notes on Japan explosion-proof certification are as follows. AIR-CAP1552H-Q-K9 (POE input configuration only).

1. Use a heat-resistant cable of 65 degree or higher for various cables connected to the equipment.

2. This model uses the following cable gland / blind plug for the input / output port of this unit.

    (TIIS Certified parts as of Jan/2017)

    For Cable ground of Fiber Port and PoE port

    Cable Grand: Ceftec Electric Co., Ltd. SFGU 10-M-ES

    Blind plug: Ceftec Electric Co., Ltd. PXN10-M20

3. Do not attach / detach the antenna in an explosive atmosphere or in a dangerous place.

VCCI Statement for Japan

⚠
Warning   **This is a Class B product based on the standard of the VCCI Council. If this equipment is used near a radio or television receiver in a domestic environment, it may cause radio interference. Install and use the equipment according to the instruction manual.**

警告   この装置は、クラスB情報技術装置です。この装置は、家庭環境で使用することを目的としていますが、この装置がラジオやテレビジョン受信機に近接して使用されると、受信障害を引き起こすことがあります。
取扱説明書に従って正しい取り扱いをして下さい。

ＶＣＣＩ－Ｂ

Administrative Rules for Cisco Aironet Access Points in Taiwan

This section provides administrative rules for operating Cisco Aironet Access Points in Taiwan. The rules are provided in both Chinese and English.

Chinese Translation

低功率電波輻射性電機管理辦法

第十二條　經型式認證合格之低功率射頻電機，非經許可，公司、商號或使用者均不得擅自變更頻率、加大功率或變更原設計之特性及功能。

第十四條　低功率射頻電機之使用不得影響飛航安全及干擾合法通信；經發現有干擾現象時，應立即停用，並改善至無干擾時方得繼續使用。

前項合法通信，指依電信法規定作業之無線電信。

低功率射頻電機須忍受合法通信或工業、科學及醫療用電波輻射性電機設備之干擾。

127048

English Translation

Administrative Rules for Low-power Radio-Frequency Devices

Article 12

For those low-power radio-frequency devices that have already received a type-approval, companies, business units or users should not change its frequencies, increase its power or change its original features and functions.

Article 14

The operation of the low-power radio-frequency devices is subject to the conditions that no harmful interference is caused to aviation safety and authorized radio station; and if interference is caused, the user must stop operating the device immediately and can't re-operate it until the harmful interference is clear.

The authorized radio station means a radio-communication service operating in accordance with the Communication Act.

The operation of the low-power radio-frequency devices is subject to the interference caused by the operation of an authorized radio station, by another intentional or unintentional radiator, by industrial, scientific and medical (ISM) equipment, or by an incidental radiator.

Chinese Translation

低功率射頻電機技術規範

4.7　　無線資訊傳輸設備

4.7.6　無線資訊傳輸設備須忍受合法通信之干擾且不得干擾合法通信；如造成干擾，應立即停用，俟無干擾之虞，始得繼續使用。

4.7.7　無線資訊傳輸設備的製造廠商應確保頻率穩定性，如依製造廠商使用手冊上所述正常操作，發射的信號應維持於操作頻帶中。

209139

English Translation

Low-power Radio-frequency Devices Technical Specifications

4.7

Unlicensed National Information Infrastructure

4.7.6

The U-NII devices shall accept any interference from legal communications and shall not interfere the legal communications. If interference is caused, the user must stop operating the device immediately and can't re-operate it until the harmful interference is clear.

4.7.7

Manufacturers of U-NII devices are responsible for ensuring frequency stability such that an emission is maintained within the band of operation under all conditions of normal operation as specified in the user manual.

Statement 371—Power Cable and AC Adapter

接続ケーブル、電源コード、AC アダプタ、バッテリーなどの部品は、
必ず添付品または指定品をご使用ください。添付品・指定品以外の部品を
ご使用になると故障や動作不良、火災の原因となります。また、電気用
品安全法により、当該法の認定（PSE とコードに表記）でなく UL 認定
（UL または CSA マークがコードに表記）の電源ケーブルは弊社が指定す
る製品以外の電気機器には使用できないためご注意ください。

English Translation

When installing the product, please use the provided or designated connection cables/power cables/AC adapters. Using any other cables/adapters could cause a malfunction or a fire. Electrical Appliance and Material Safety Law prohibits the use of UL-certified cables (that have the "UL" shown on the code) for any other electrical devices than products designated by CISCO. The use of cables that are certified by Electrical Appliance and Material Safety Law (that have "PSE" shown on the code) is not limited to CISCO-designated products.

Taiwan NCC Statement

English Translation

This product cannot be used unless installed and setup by professional staff, and may not be sold directly to the general consumer.

Chinese Translation

本器材須經專業工程人員安裝及設定，使得
設置使用，且不得直接販售給一般消費者。

English Translation

MPE standard value is 1mW / CM2, the assessment result is 0.19mW/CM2.

Chinese Translation

電磁波暴露量MPE 標準值1mW/cm^2，評估結果為__0.19__mW / CM2

EU Declaration of Conformity

All the Declaration of Conformity statements related to this product can be found at the following location:

http://www.ciscofax.com

Channels and Power Levels

For channel and maximum power level settings, refer to the *Channels and Maximum Power Settings for Cisco Aironet Lightweight Access Points and Bridges* document available on the Cisco Wireless documentation page of Cisco.com.

To browse to the document, follow these steps:

Step 1 Click this link and go to the Cisco Wireless documentation home page:
http://www.cisco.com/en/US/products/hw/wireless/index.html

Step 2 Click **Support**. The Support and Documentation page displays.

Step 3 Click **Wireless**

Step 4 Click **1550**.

Step 5 Click **Install and Upgrade**.

Step 6 Click **Install and Upgrade Guides**.

Step 7 Click **Channels and Maximum Power Settings for Cisco 1550 Series Outdoor Mesh Access Points** document.

APPENDIX D

Access Point Specifications

Table D-1 lists the technical specifications for the Cisco Aironet 1552 Outdoor Mesh Access Points for Hazardous Locations. For detailed specifications, refer to the *Cisco Aironet 1550 Series Outdoor Access Point* data sheet at:

http://www.cisco.com/en/US/prod/collateral/wireless/ps5679/ps11451/data_sheet_c78-641373.html

Table D-1   Access Point Specifications

Category	Specifications
Size	12.0 in. x 7.8 in. x 6.4 in. (30.48 cm x 19.81 cm x 16.26 cm) (including antenna mount)
Weight	• 1552SA/1552SD (AC): 18.5 lbs (8.4 kg) • 1552SA/1552SD (DC): 17.5 lbs (7.9) • 1552H: 17.6 lbs (8 kg) • 1552WU: 17.6 lbs (8 kg) • Pole mounting bracket: 6.1 lbs (2.8 kg)
Connector	• 1552H: Three Type N antenna connectors for 2.4 GHz radio and 5 GHz 802.11n radio (depends on configuration) • 1552S: Five Type N antenna connectors for 2.4 GHz radio and 5 GHz 802.11n radio (depends on configuration) • 1552WU: Seven Type N antenna connectors for 2.4 GHz radio and 5 GHz 802.11n radio (depends on configuration) • 1552S: Two Type N antenna connector (2.4 GHz ISA100 Wireless and WirelessHART Multiprotocol radio) • Internal PoE In or ETH connector (uplink port)—RJ-45 connector • Internal PoE Out connector (downlink port)—RJ-45 connector • 1552H and 1552S: Optional internal SFP fiber module—LC fiber connector • 1552WU: 2.4 GHz WirelessHART radio for communicating with sensor devices by a single Type N connector for the WirelessHART 2.4 GHz antenna. This antenna is intended to be connected using a low-loss coaxial cable.

Table D-1   Access Point Specifications (continued)

Category	Specifications
Power sources (see Table D-2 for power distribution budget)	• 100 to 240 VAC, 50–60 Hz (1552H and 1552SA only) • Power over Ethernet (PoE): 56 VDC (1552H only) • 12 VDC input (not supported in hazardous locations environment) • 24 VDC (1552SD and 1552WU)
Operating temperature	-40 to 55°C (-40 to 131°F) plus Solar Loading
Storage temperature	-50 to 85°C (-58 to 185°F)
Humidity	Access point: 0 to 100% condensing—access point (operating and nonoperating) Power injector: 10 to 90% noncondensing—power injector (operating)
Data rates	802.11a: 6, 9, 12, 18, 24, 36, 48, and 54 Mbps
	802.11b: 1, 2, 5.5, and 11 Mbps
	802.11g: 6, 9, 12, 18, 24, 36, 48, and 54 Mbps
	802.11n data rates (2.4 GHz and 5 GHz) - refer to Table D-3 for data rates
Environmental ratings	• IP67 (1552H, 1552SA/1552SD, and 1552WU) • NEMA Type 4X (1552H and 1552SA/1552SD) • NEMA Type 4 (1552WU)
Maximum elevation	6,561 ft (2,000 m) at 131ºF (55ºC)—Operating 16,000 ft (4,877 m) at –13ºF (–25ºC)—Non-operating
Wind resistance	Wind resistance: • Up to 100 MPH sustained winds • Up to 165 MPH wind gusts

Table D-1   *Access Point Specifications (continued)*

Category	Specifications

RF output power	2.4 GHz
	
	• 802.11b (CCK)
	    – 28 dBm with 2 antennas
	• 802.11g (non HT duplicate mode)
	    – 28 dBm with 2 antennas
	• 802.11n (HT20)
	    – 28 dBm with 2 antennas
	
	5 GHz
	
	• 802.11a
	    – 28 dBm with 2 antennas
	• 802.11n non-HT duplicate (802.11a duplicate) mode
	    – 28 dBm with 2 antennas
	• 802.11n (HT20)
	    – 27 dBm with 2 antennas
	• 802.11n (HT40)
	• 27 dBm with 2 antennas
	
	✎
	Note Maximum output depends on the regulatory domain in which the access point is installed. For additional information, refer to the Appendix C, "Channels and Power Levels".

Table D-1   *Access Point Specifications (continued)*

Category	Specifications
Frequency Band and 20-MHz Operating Channels	**-A Domain:** • 2.400 to 2.4835 GHz; 11 channels • 5.725 to 5.850 GHz; 5 channels **-B Domain:** • 2.400 to 2.4835 GHz, 11 channels • 5.260 to 5.320 GHz; 4 channels • 5.500 to 5.560 GHz, 4 channels • 5.680 to 5.720 GHz, 3 channels • 5.745 to 5.825 GHz, 5 channels **-C Domain:** • 2.400 to 2.4835 GHz; 13 channels • 5.725 to 5.850 GHz; 5 channels **-E Domain:** • 2.401 to 2.4835 GHz; 13 channels • 5.470 to 5.725 GHz; 8 channels **-K Domain:** • 2.400 to 2.4835 GHz; 11 channels • 5.250 to 5.825 GHz; 14 channels **-M Domain** • 2.400 to 2.4835 GHz; 13 channels • 5.470 to 5.850 GHz; 12 channels **-N Domain:** • 2.400 to 2.4835 GHz; 11 channels • 5.725 to 5.850 GHz; 5 channels **-Q Domain:** • 2.400 to 2.4835 GHz; 13 channels • 5.470 to 5.725 GHz; 11 channels **-R Domain:** • 2.400 to 2.4835 GHz; 13 channels • 5.250 to 5.725 GHz; 11 channels **-S Domain:** • 2.400 to 2.4835 GHz; 13 channels • 5.725 to 5.850 GHz; 5 channels **-T Domain:** • 2.400 to 2.4835 GHz; 11 channels • 5.470 to 5.850 GHz; 16 channels

Table D-1   Access Point Specifications (continued)

Category	Specifications
Immunity	• Less than or equal to 5 mJ for 6kV/3kA @ 8/20 ms waveform • ANSI/IEEE C62.41 • EN61000 4-5 Level 4 AC Surge Immunity • EN61000 4-4 Level 4 Electrical Fast Transient Burst Immunity • EN61000 4-3 Level 4 EMC Field Immunity • EN61000 4-2 Level 4 ESD Immunity
Safety	• IEC 60950-1 • UL 60950-1 • CSA 60950-1 • EN 60950-1
Hazardous Locations	• ANSI/ASA 12.12.01 • UL 60079-0 • UL 60079-15 • CSA C22.2 No. 213-M1987 • CAN/CSA E60079-15/-0 • EN 60079-0 • EN 60079-15 • IEC 60079-0 • IEC 60079-15 **Note** For more information about Hazardous Location Specifications, see Compliance, page 2-38.
Radio approvals	• FCC Parts 15.247, 90.210 • FCC Bulletin OET-65C • Canada RSS-210 and RSS-102 • AS/NZS 4268.2003

Table D-1   Access Point Specifications (continued)

Category	Specifications		
EMI and susceptibility 1552S and 1552H	Powered by AC (AP1552S): • FCC Part 15.107 and 15.109 Class B • ICES-003 Class B (Canada) • EN 55022 B • EN 60601-1-2:2001 • AS/NZS 3548 Class B • VCCI Class B • EN 301.489-1 • EN 301.489-17	Powered by power injector (AP1552S and AP1552H); Powered by AC (AP1552H): • FCC Part 15.107 and 15.109 Class A • ICES-003 Class A (Canada) • EN 55022 A • EN 60601-1-2:2001 • AS/NZS 3548 Class A • VCCI Class A • EN 301.489-1 • EN 301.489-17	
EMI and susceptibility 1552WU	• FCC part 15.107, 15.109 • ICES-003 • EN 301 489-1, -17		

Table D-2 lists the power distribution budget for 1552H/1552SA/1552SD/1552WU access point configurations.

Table D-2   Power Consumption Budget for the AIR-CAP1552H-x-K9, AIR-CAP1552SA/SD-x-K9, and AIR-CAP1552WU-A-K9 Access Point Configurations

Element	Nominal "H"/"S" Power (Watts)	Absolute "H"/"S" Max Power (Watts)
Total power budget when using DC power source	34/36	43/45
Total power budget when using AC power source	41/43	52/54
Optional components		
802.3af client connected	17	17
Fiber user as backhaul	1	1
Total Power Consumption		
Total Power Consumption When DC Powered	52/54	61/63
Total Power Consumption When AC Powered	59/61	70/72

Table D-3   *802.11n Data Rates (2.4 GHz and 5 GHz)*

MCS Index[1]	GI[2] = 800ns		GI = 400ns	
	20-MHz Rate (Mbps)	40-MHz Rate (Mbps)	20-MHz Rate (Mbps)	40-MHz Rate (Mbps)
0	6.5	13.5	7.2	15
1	13	27	14.4	30
2	19.5	40.5	21.7	45
3	26	54	28.9	60
4	39	81	43.3	90
5	52	108	57.8	120
6	58.5	121.5	65	135
7	65	135	72.2	150
8	13	27	14.4	30
9	26	54	28.9	60
10	39	81	43.3	90
11	52	108	57.8	120
12	78	162	86.7	180
13	104	216	115.6	240
14	117	243	130	270
15	130	270	144.4	300

APPENDIX E

Access Point Pinouts

This appendix describes the pin signals of the access point Ethernet connectors, and the power injector input and output connectors. Table E-1 describes the pin signals of the access point PoE Out connector.

Table E-1   Access Point PoE Out Ethernet Connector Pinouts

Pin Number	Signal Name
1	Ethernet signal pair (10/100/1000BASE-T)
2	
3	Ethernet signal pair (10/100/1000BASE-T)
6	
4	Ethernet signal pair (10/100/1000BASE-T) and 48 VDC (+)
5	
7	Ethernet signal pair (10/100/1000BASE-T) and 48 VDC return
8	
Shield	Chassis ground

Table E-2 describes the pin signals for the access point PoE In Ethernet connector.

Table E-2   Access Point PoE In Ethernet Connector Pinouts

Pin Number	Signal Name
1	Ethernet signal pair (10/100/1000BASE-T) and 56 VDC return
2	
3	Ethernet signal pair (10/100/1000BASE-T) and 56 VDC (+)
6	
4	Ethernet signal pair (1000BASE-T) and 56 VDC (+)
5	
7	Ethernet signal pair (1000BASE-T) and 56 VDC return
8	
Shield	Chassis ground

Table E-3 describes the pin signals for the power injector input connector (To Switch).

Table E-3   Power Injector Input Connector (To Switch) Pinouts

Pin Number	Signal Name
1	Ethernet signal pair (10/100/1000BASE-T)
2	
3	Ethernet signal pair 10/100/1000BASE-T)
6	
4	Ethernet signal pair (1000BASE-T)
5	
7	Ethernet signal pair (1000BASE-T)
8	
Shield	Chassis ground

Table E-4 describes the RJ-45 pin signals for the power injector output connector (To AP).

Table E-4   Power Injector Output Connector (To AP) Pinouts

Pin Number	Signal Name
1	Ethernet signal pair (10/100/1000BASE-T) and 56 VDC return
2	
3	Ethernet signal pair (10/100/1000BASE-T) and 56 VDC (+)
6	
4	Ethernet signal pair (1000BASE-T) and 56 VDC (+)
5	
7	Ethernet signal pair (1000BASE-T) and 56 VDC return
8	
Shield	Chassis ground

Note The power injector output connector (To AP) only supplies 56 VDC power when the Ethernet cable is connected to the 1550 PoE In connector.

Configuring DHCP Option 43

This appendix describes the steps needed to configure DHCP Option 43 on a DHCP server, such as a Cisco Catalyst 3750 series switch, for use with Cisco Aironet Hazardous Location Access Points. This appendix contains these sections:

Overview

This section contains a DHCP Option 43 configuration example on a DHCP server for use with Cisco Aironet Access Points. For other DHCP server implementations, consult DHCP server product documentation for configuring DHCP Option 43. In Option 43, use the IP address of the controller management interface.

✎ **Note**   DHCP Option 43 is limited to one access point type per DHCP pool. You must configure a separate DHCP pool for each access point type.

Cisco Aironet 1000, 1500, and 1552 access points use a comma-separated string format for DHCP Option 43. Other Cisco Aironet access points use the type-length-value (TLV) format for DHCP Option 43. DHCP servers must be programmed to return the option based on the access point DHCP Vendor Class Identifier (VCI) string (DHCP Option 60). The VCI strings for Cisco access points that can operate in lightweight mode are listed in Table F-1.

Table F-1   Lightweight Access Point VCI Strings

Access Point	Vendor Class Identifier (VCI)
Cisco Aironet 1000 series	Airespace.AP1200
Cisco Aironet 1100 series	Cisco AP c1100
Cisco Aironet 1130 series	Cisco AP c1130
Cisco Aironet 1200 series	Cisco AP c1200
Cisco Aironet 1240 series	Cisco AP c1240
Cisco Aironet 1250 series	Cisco AP c1250
Cisco Aironet 1300 series	Cisco AP c1300
Cisco Aironet 1500 series	Cisco AP c1500[1]
	Cisco AP.OAP1500[2], Cisco AP.LAP1510[2], or Cisco AP.LAP1505[2]
	Airespace.AP1200[3]
Cisco Aironet 1520 series	Cisco AP c1520
Cisco Aironet 1550 series	Cisco AP c1550

1. For controller release 4.1 or later.
2. For controller release 4.0, the VCI depends on the model.
3. For controller release 3.2.

The following is the format of the TLV block for 1100, 1130, 1200, 1240, 1250, 1300, 1520, and 1552 access points:

- Type: 0xf1 (decimal 241)
- Length: Number of controller IP addresses * 4
- Value: List of WLC management interfaces

Configuring Option 43 for 1100, 1130, 1200, 1240, 1250, 1300, 1520, and 1550 Series Access Points

To configure DHCP Option 43 for Cisco Aironet 1100, 1130, 1200, 1240, 1250, 1300, 1520, and 1550 series access points in the embedded Cisco IOS DHCP server, follow these steps:

Step 1 Enter configuration mode at the Cisco IOS CLI.

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

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

Where:
pool name is the name of the DHCP pool, such as AP1550
IP Network is the network IP address where the controller resides, such as 10.0.15.1
Netmask is the subnet mask, such as 255.255.255.0
Default router is the IP address of the default router, such as 10.0.0.1
DNS Server is the IP address of the DNS server, such as 10.0.10.2
```

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

```
option 60 ascii "VCI string"
```

For the VCI string, use the value from Table F-1. The quotation marks must be included.

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

```
option 43 hex hex string
```

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

Type + Length + Value

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

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

```
option 43 hex f1080a7e7e020a7f7f02
```

Configuring Option 43 for 1100, 1130, 1200, 1240, 1250, 1300, 1520, and 1550 Series Access Points

GLOSSARY

A

ad hoc network	A wireless network composed of stations without access points.
associated	A station is configured properly to allow it to wirelessly communicate with an access point.
AWPP	Adaptive Wireless Path Protocol.

B

beacon	A wireless LAN packet that signals the availability and presence of the wireless device. Beacon packets are sent by access points and base stations; however, client radio cards send beacons when operating in computer to computer (Ad Hoc) mode.
BOOTP	Boot Protocol. A protocol used for the static assignment of IP addresses to devices on the network.
BPSK	Binary phase shift keying is a modulation technique used by IEEE 802.11b-compliant wireless LANs for transmission at 1 Mb/s.

C

CAPWAP	Control And Provisioning of Wireless Access Points
CCK	Complementary Code Keying. A modulation technique used by IEEE 802.11b-compliant wireless LANs for transmission at 5.5 and 11 Mb/s.
CCKM	Cisco Centralized Key Management. Using CCKM, authenticated client devices can roam from one access point to another without any perceptible delay during reassociation. An access point on your network provides wireless domain services (WDS) and creates a cache of security credentials for CCKM-enabled client devices on the subnet. The WDS access point's cache of credentials dramatically reduces the time required for reassociation when a CCKM-enabled client device roams to a new access point.
CSMA	Carrier sense multiple access. A wireless LAN media access method specified by the IEEE 802.11 specification.

D

DFS Dynamic Frequency Selection. In some regulatory domains, 5 GHz radios are required to use DFS to avoid interfering with radar signals.

DHCP Dynamic host configuration protocol. A protocol available with many operating systems that automatically issues IP addresses within a specified range to devices on the network. The device retains the assigned address for a specific administrator-defined period.

DNS Domain Name System server. A server that translates text names into IP addresses. The server maintains a database of host alphanumeric names and their corresponding IP addresses.

DSSS Direct sequence spread spectrum. A type of spread spectrum radio transmission that spreads its signal continuously over a wide frequency band.

E

EAP Extensible Authentication Protocol. An optional IEEE 802.1x security feature ideal for organizations with a large user base and access to an EAP-enabled Remote Authentication Dial-In User Service (RADIUS) server.

I

infrastructure The wired Ethernet network.

isotropic An antenna that radiates its signal in a spherical pattern.

M

MAP Mesh Access Point

MBSSID Multiple basic SSID. Each multiple basic SSID is assigned a unique MAC address. You use multiple BSSIDs to assign a unique DTIM setting for each SSID and to broadcast SSIDs in beacons (one SSID per beacon).

MIMO Multiple Input/Multiple Output

multipath The echoes created as a radio signal bounces off of physical objects.

multicast packet A single data message (packet) sent to multiple addresses.

O

omni-directional   This typically refers to a primarily circular antenna radiation pattern.

OFDM   Orthogonal frequency division multiplex is a modulation technique used by IEEE 802.11a-compliant wireless LANs for transmission at 6, 9, 12, 18, 24, 36, 48, and 54 Mb/s.

P

packet   A basic message unit for communication across a network. A packet usually includes routing information, data, and sometimes error detection information.

Q

QPSK

Quadruple phase shift keying is a modulation technique used by IEEE 802.11b-compliant wireless LANs for transmission at 2 Mb/s.

R

range   A linear measure of the distance that a transmitter can send a signal.

RAP   Root Access Point

receiver sensitivity   A measurement of the weakest signal a receiver can receive and still correctly translate it into data.

RF   Radio frequency. A generic term for radio-based technology.

RP-TNC   A connector type unique to Cisco Aironet radios and antennas. Part 15.203 of the FCC rules covering spread spectrum devices limits the types of antennas that may be used with transmission equipment. In compliance with this rule, Cisco Aironet, like all other wireless LAN providers, equips its radios and antennas with a unique connector to prevent attachment of non-approved antennas to radios.

S

spread spectrum   A radio transmission technology that spreads the user information over a much wider bandwidth than otherwise required in order to gain benefits such as improved interference tolerance and unlicensed operation.

SSID   Service set identifier (also referred to as Radio Network Name). A unique identifier used to identify a radio network and which stations must use to be able to communicate with each other or to an access point. The SSID can be any alphanumeric entry up to a maximum of 32 characters.

U

UNII   Unlicensed National Information Infrastructure—regulations for UNII devices operating in the 5.15 to 5.35 GHz and 5.725 to 5.825 GHz frequency bands.

UNII-1   Regulations for UNII devices operating in the 5.15 to 5.25 GHz frequency band.

UNII-2   Regulations for UNII devices operating in the 5.25 to 5.35 GHz frequency band.

UNII-3   Regulations for UNII devices operating in the 5.725 to 5.825 GHz frequency band.

unicast packet   A single data message (packet) sent to a specific IP address.

W

WDS   Wireless Domain Services. An access point providing WDS on your wireless LAN maintains a cache of credentials for CCKM-capable client devices on your wireless LAN. When a CCKM-capable client roams from one access point to another, the WDS access point forwards the client's credentials to the new access point with the multicast key. Only two packets pass between the client and the new access point, greatly shortening the reassociation time.

WEP   Wired Equivalent Privacy. An optional security mechanism defined within the 802.11 standard designed to make the link integrity of wireless devices equal to that of a cable.

WLSE   Wireless LAN Solutions Engine. The WLSE is a specialized appliance for managing Cisco Aironet wireless LAN infrastructures. It centrally identifies and configures access points in customer-defined groups and reports on throughput and client associations. WLSE's centralized management capabilities are further enhanced with an integrated template-based configuration tool for added configuration ease and improved productivity.

WNM   Wireless Network Manager.

WPA   Wi-Fi Protected Access is a standards-based, interoperable security enhancement that strongly increases the level of data protection and access control for existing and future wireless LAN systems. It is derived from and will be forward-compatible with the upcoming IEEE 802.11i standard. WPA leverages TKIP (Temporal Key Integrity Protocol) for data protection and 802.1X for authenticated key management.