



REVIEW DRAFT – CISCO CONFIDENTIAL



Cisco Aironet 1520 Series Outdoor Mesh Access Point Hardware Installation Guide

March, 2008

Americas Headquarters

Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
<http://www.cisco.com>
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

Text Part Number: OL-12632-03

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The following information is for FCC compliance of Class A devices: This equipment has been tested and found to comply with the limits for a Class A 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 commercial environment. This equipment generates, uses, and can radiate radio-frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case users will be required to correct the interference at their own expense.

The following information is for FCC compliance of Class B devices: The equipment described in this manual generates and may radiate radio-frequency energy. If it is not installed in accordance with Cisco's installation instructions, it may cause interference with radio and television reception. This equipment has been tested and found to comply with the limits for a Class B digital device in accordance with the specifications in part 15 of the FCC rules. These specifications are designed to provide reasonable protection against such interference in a residential installation. However, there is no guarantee that interference will not occur in a particular installation.

Modifying the equipment without Cisco's written authorization may result in the equipment no longer complying with FCC requirements for Class A or Class B digital devices. In that event, your right to use the equipment may be limited by FCC regulations, and you may be required to correct any interference to radio or television communications at your own expense.

You can determine whether your equipment is causing interference by turning it off. If the interference stops, it was probably caused by the Cisco equipment or one of its peripheral devices. If the equipment causes interference to radio or television reception, try to correct the interference by using one or more of the following measures:

- Turn the television or radio antenna until the interference stops.
- Move the equipment to one side or the other of the television or radio.
- Move the equipment farther away from the television or radio.
- Plug the equipment into an outlet that is on a different circuit from the television or radio. (That is, make certain the equipment and the television or radio are on circuits controlled by different circuit breakers or fuses.)

Modifications to this product not authorized by Cisco Systems, Inc. could void the FCC approval and negate your authority to operate the product.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

CCSP, the Cisco Square Bridge logo, Follow Me Browsing, and StackWise are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn, and i Study are service marks of Cisco Systems, Inc.; and Access Registrar, Aironet, ASIST, BPX, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Empowering the Internet Generation, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, FormShare, GigaDrive, GigaStack, HomeLink, Internet Quotient, IOS, IP/TV, iQ Expertise, the iQ logic Net Readiness Scorecard, LightStream, Linksys, MeetingPlace, MGX, the Networkers logo, Networking Academy, Network Registrar, Packet, PIX, Post-Routing, Pre-Rout ProConnect, RateMUX, ScriptShare, SlideCast, SMARTnet, StrataView Plus, SwitchProbe, TeleRouter, The Fastest Way to Increase Your Internet Quotient, TransPath, and are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0501R)

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

Book Title

©2007 Cisco Systems, Inc. All rights reserved.



REVIEW DRAFT - CISCO CONFIDENTIAL

CONTENTS

Preface VII

- Objectives I-VII
- Audience I-VII
- Organization I-VII
- Conventions I-VIII
- Related Publications I-XIII
 - Finding the Product Serial Number I-XIV
- Obtaining Documentation, Obtaining Support, and Security Guidelines I-XIV

CHAPTER 1

Overview 1-1

- Hardware Features 1-2
 - Connectors 1-5
 - Antenna Connector Locations 1-5
 - Dual Radio Operation 1-7
 - External Antennas 1-7
 - Multiple Power Sources 1-8
 - Ethernet Ports 1-9
 - Cable Modem 1-10
 - Metal Enclosure 1-10
 - Optional Hardware 1-10
- Network Deployment Examples 1-11
 - Wireless Backhaul 1-12
 - Point-to-Point Bridging 1-12
 - Point-to-Multipoint Bridging 1-13
 - Mesh Network 1-14
 - Layer 3 Network Operation 1-15

CHAPTER 2

Mounting Instructions 2-1

- Unpacking the Access Point 2-2
 - Package Contents 2-2
- Tools and Materials that You Supply 2-2
 - Pole Installation 2-3
 - Cable Strand Installation 2-3
- Warnings 2-4

REVIEW DRAFT – CISCO CONFIDENTIAL

- Safety Information 2-4
 - FCC Safety Compliance Statement 2-4
 - Safety Precautions 2-5
- Avoiding Damage to Radios in a Testing Environment 2-7
- Installation Guidelines 2-8
 - Site Surveys 2-8
 - Before Beginning the Installation 2-9
 - Becoming Familiar with Access Point Installation Components 2-9
 - Antenna Connector Locations 2-13
 - Adding the Access Point MAC Addresses to the Controller Filter List 2-14
 - Configuring a RAP 2-15
 - Configuring a Bridge Group Name 2-15
- Mounting the Access Point 2-16
 - Installation Options 2-16
 - Access Point Mounting Orientation 2-17
 - Mounting the Access Point on a Wall 2-17
 - Mounting the Access Point on a Pole 2-21
 - Assembling the Pole Clamp Bracket and the Mounting Bracket 2-21
 - Pole Mounting 2-24
 - Cable Strand Mounting 2-30
 - Opening the Access Point Hinged Cover 2-38
 - Closing the Access Point Hinged Cover 2-39
 - Using the Reset Button 2-41
 - Reboot the Access Point 2-41
 - Disabling Backup Battery Power 2-42
- Grounding the Access Point 2-42
- Connecting a Fiber-Optic Cable to the Access Point 2-43
- Powering the Access Point 2-46
 - Connecting a 1520 Series Power Injector 2-46
 - Connecting an Ethernet Cable to the Access Point 2-47
 - Connecting Streetlight AC Power 2-51
 - Connecting an AC Power Cable to the Access Point 2-54
 - Connecting a DC Power Cable to the Access Point 2-55
 - Connecting a Cable POC Power to the Access Point 2-59
 - What to Do Next 2-61

CHAPTER 3

Troubleshooting 3-1

- Guidelines for Using the Access Points 3-2
- Important Notes 3-2

REVIEW DRAFT—CISCO CONFIDENTIAL

Convergence Delays	3-2
Bridge Loop	3-3
Controller DHCP Server	3-3
MAP Data Traffic	3-3
Controller MAC Filter List	3-3
Using DHCP Option 43	3-4
Monitoring the Access Point LEDs	3-4
Verifying Controller Association	3-5
Changing the Bridge Group Name	3-6
Cable Modem LEDs	3-7
Connecting to the Access Point Locally	3-8
Access Point Power Injector	3-9
Monitoring the Power Injector LEDs	3-10

CHAPTER 4**Installing or Replacing the Backup Battery 4-1**

Before Beginning the Installation or Replacement	4-2
Opening the Access Point Radio Cover	4-3
Removing a Backup Battery	4-4
Installing a New Backup Battery	4-5
Connecting the Backup Battery Cable and Closing the Radio Cover	4-6
What to do Next	4-6

APPENDIX A**Translated Safety Warnings A-1****APPENDIX B****Declarations of Conformity and Regulatory Information B-1**

Manufacturers Federal Communication Commission Declaration of Conformity Statement for Model LAP1522	B-2
VCCI Statement for Japan	B-3
Department of Communications—Canada	B-3
Canadian Compliance Statement	B-3
Declaration of Conformity for RF Exposure	B-4
European Community, Switzerland, Norway, Iceland, and Liechtenstein	B-4
Declaration of Conformity with Regard to the 1999/5/EC (R&TTE Directive)	B-5
Declaration of Conformity for RF Exposure	B-7
Guidelines for Operating Cisco Aironet Access Points in Japan	B-7
Japanese Translation	B-8
English Translation	B-8
Administrative Rules for Cisco Aironet Access Points in Taiwan	B-8

REVIEW DRAFT – CISCO CONFIDENTIAL

Chinese Translation **B-9**

English Translation **B-9**

Declaration of Conformity Statements for Model LAP1522 **B-10**

Declaration of Conformity Statements for European Union Countries **B-10**

Manufacturers Federal Communication Commission Declaration of Conformity Statement for Model LAP1524 **B-12**

Overview **B-12**

Industry Canada **B-14**

Canadian Compliance Statement **B-14**

Declaration of Conformity for RF Exposure **B-14**

APPENDIX C **Access Point Specifications** **C-1**

APPENDIX D **Channels and Power Levels** **D-1**

APPENDIX E **Access Point Pinouts** **E-1**

APPENDIX F **Configuring DHCP Option 43** **F-1**

Overview **F-2**

Configuring Option 43 for 1000 and 1500 Series Access Points **F-3**

Configuring Option 43 for 1100, 1130, 1200, 1240, 1250, 1300, and 1520 Series Access Points **F-4**

INDEX



REVIEW DRAFT - CISCO CONFIDENTIAL

Preface

This section describes the objectives, audience, organization, and conventions of the *Cisco Aironet 1520 Series Outdoor Mesh Access Point Hardware Installation Guide*.

Objectives

This publication explains the steps for installing the Cisco Aironet 1520 Series Outdoor Mesh Access Point (hereafter called the *access point*). The access point is available in two models: The LAP1522 and LAP1524. The LAP1522 model supports dual band (2.4- and 5-GHz) operation. The LAP1524 supports dual band (2.4- and 5-GHz) operation and the 4.9-GHz public safety band.

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

Organization

This guide contains the following sections:

[Chapter 1, “Overview,”](#) describes the major components and features of the access point.

[Chapter 2, “Mounting Instructions,”](#) provides warnings, safety information, and mounting information needed during the installation of your access point.

[Chapter 3, “Troubleshooting,”](#) provides basic troubleshooting procedures for the access point.

[Chapter 4, “Installing or Replacing the Backup Battery,”](#) describes the procedures to install or replace the backup battery in 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.

REVIEW DRAFT – CISCO CONFIDENTIAL

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, “Access Point Specifications,” lists technical specifications for the access point.

Appendix D, “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’s regulatory domains.

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 to convey instructions and information:

- Commands and keywords are in **boldface** type.



Note

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



Caution

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



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

Waarschuwing

BELANGRIJKE VEILIGHEIDSINSTRUCTIES

Dit waarschuwingssymbool betekent gevaar. U verkeert in een situatie die lichamelijk letsel kan veroorzaken. Voordat u aan enige apparatuur gaat werken, dient u zich bewust te zijn van de bij elektrische schakelingen betrokken risico's en dient u op de hoogte te zijn van de standaard praktijken om ongelukken te voorkomen. Gebruik het nummer van de verklaring onderaan de waarschuwing als u een vertaling van de waarschuwing die bij het apparaat wordt geleverd, wilt raadplegen.

BEWAAR DEZE INSTRUCTIES

REVIEW DRAFT – CISCO CONFIDENTIAL

Varoitus	TÄRKEITÄ TURVALLISUUSOHJEITA Tämä varoitusmerkki merkitsee vaaraa. Tilanne voi aiheuttaa ruumiillisia vammoja. Ennen kuin käsittelet laitteistoa, huomioi sähköpiirien käsittelemiseen liittyvät riskit ja tutustu onnettomuuksien yleisiin ehkäisytapoihin. Turvallisuusvaroitusten käännökset löytyvät laitteen mukana toimitettujen käännettyjen turvallisuusvaroitusten joukosta varoitusten lopussa näkyvien lausuntonumeroiden avulla. SÄILYTÄ NÄMÄ OHJEET
Attention	IMPORTANTES INFORMATIONS DE SÉCURITÉ Ce symbole d'avertissement indique un danger. Vous vous trouvez dans une situation pouvant entraîner des blessures ou des dommages corporels. Avant de travailler sur un équipement, soyez conscient des dangers liés aux circuits électriques et familiarisez-vous avec les procédures couramment utilisées pour éviter les accidents. Pour prendre connaissance des traductions des avertissements figurant dans les consignes de sécurité traduites qui accompagnent cet appareil, référez-vous au numéro de l'instruction situé à la fin de chaque avertissement. CONSERVEZ CES INFORMATIONS
Warnung	WICHTIGE SICHERHEITSHINWEISE Dieses Warnsymbol bedeutet Gefahr. Sie befinden sich in einer Situation, die zu Verletzungen führen kann. Machen Sie sich vor der Arbeit mit Geräten mit den Gefahren elektrischer Schaltungen und den üblichen Verfahren zur Vorbeugung vor Unfällen vertraut. Suchen Sie mit der am Ende jeder Warnung angegebenen Anweisungsnummer nach der jeweiligen Übersetzung in den übersetzten Sicherheitshinweisen, die zusammen mit diesem Gerät ausgeliefert wurden. BEWAHREN SIE DIESE HINWEISE GUT AUF.
Avvertenza	IMPORTANTI ISTRUZIONI SULLA SICUREZZA Questo simbolo di avvertenza indica un pericolo. La situazione potrebbe causare infortuni alle persone. Prima di intervenire su qualsiasi apparecchiatura, occorre essere al corrente dei pericoli relativi ai circuiti elettrici e conoscere le procedure standard per la prevenzione di incidenti. Utilizzare il numero di istruzione presente alla fine di ciascuna avvertenza per individuare le traduzioni delle avvertenze riportate in questo documento. CONSERVARE QUESTE ISTRUZIONI
Advarsel	VIKTIGE SIKKERHETSINSTRUKSJONER Dette advarselssymbolet betyr fare. Du er i en situasjon som kan føre til skade på person. Før du begynner å arbeide med noe av utstyret, må du være oppmerksom på farene forbundet med elektriske kretser, og kjenne til standardprosedyrer for å forhindre ulykker. Bruk nummeret i slutten av hver advarsel for å finne oversettelsen i de oversatte sikkerhetsadvarslene som fulgte med denne enheten. TA VARE PÅ DISSE INSTRUKSJONENE

REVIEW DRAFT – CISCO CONFIDENTIAL

Aviso INSTRUÇÕES IMPORTANTES DE SEGURANÇA

Este símbolo de aviso significa perigo. Você está em uma situação que poderá ser causadora de lesões corporais. Antes de iniciar a utilização de qualquer equipamento, tenha conhecimento dos perigos envolvidos no manuseio de circuitos elétricos e familiarize-se com as práticas habituais de prevenção de acidentes. Utilize o número da instrução fornecido ao final de cada aviso para localizar sua tradução nos avisos de segurança traduzidos que acompanham este dispositivo.

GUARDE ESTAS INSTRUÇÕES

¡Advertencia! INSTRUCCIONES IMPORTANTES DE SEGURIDAD

Este símbolo de aviso indica peligro. Existe riesgo para su integridad física. Antes de manipular cualquier equipo, considere los riesgos de la corriente eléctrica y familiarícese con los procedimientos estándar de prevención de accidentes. Al final de cada advertencia encontrará el número que le ayudará a encontrar el texto traducido en el apartado de traducciones que acompaña a este dispositivo.

GUARDE ESTAS INSTRUCCIONES

Varning! VIKTIGA SÄKERHETSANVISNINGAR

Denna varningssignal signalerar fara. Du befinner dig i en situation som kan leda till personskada. Innan du utför arbete på någon utrustning måste du vara medveten om farorna med elkretsar och känna till vanliga förfaranden för att förebygga olyckor. Använd det nummer som finns i slutet av varje varning för att hitta dess översättning i de översatta säkerhetsvarningar som medföljer denna anordning.

SPARA DESSA ANVISNINGAR

Figyelem FONTOS BIZTONSÁGI ELOÍRÁSOK

Ez a figyelmeztető jel veszélyre utal. Sérülésveszélyt rejte helyzetben van. Mielőtt bármely berendezésen munkát végezte, legyen figyelemmel az elektromos áramkörök okozta kockázatokra, és ismerkedjen meg a szokásos balesetvédelmi eljárásokkal. A kiadványban szereplő figyelmeztetések fordítása a készülékhez mellékelt biztonsági figyelmeztetések között található; a fordítás az egyes figyelmeztetések végén látható szám alapján kereshető meg.

ORIZZE MEG EZEKET AZ UTASÍTÁSOKAT!

Предупреждение ВАЖНЫЕ ИНСТРУКЦИИ ПО СОБЛЮДЕНИЮ ТЕХНИКИ БЕЗОПАСНОСТИ

Этот символ предупреждения обозначает опасность. То есть имеет место ситуация, в которой следует опасаться телесных повреждений. Перед эксплуатацией оборудования выясните, каким опасностям может подвергаться пользователь при использовании электрических цепей, и ознакомьтесь с правилами техники безопасности для предотвращения возможных несчастных случаев. Воспользуйтесь номером заявления, приведенным в конце каждого предупреждения, чтобы найти его переведенный вариант в переводе предупреждений по безопасности, прилагаемом к данному устройству.

СОХРАНИТЕ ЭТИ ИНСТРУКЦИИ

REVIEW DRAFT – CISCO CONFIDENTIAL

警告 重要的安全性说明

此警告符号代表危险。您正处于可能受到严重伤害的工作环境中。在您使用设备开始工作之前，必须充分意识到触电的危险，并熟练掌握防止事故发生的标准工作程序。请根据每项警告结尾提供的声明号码来找到此设备的安全性警告说明的翻译文本。

请保存这些安全性说明

警告 安全上の重要な注意事項

「危険」の意味です。人身事故を予防するための注意事項が記述されています。装置の取り扱い作業を行うときは、電気回路の危険性に注意し、一般的な事故防止策に留意してください。警告の各国語版は、各注意事項の番号を基に、装置に付属の「Translated Safety Warnings」を参照してください。

これらの注意事項を保管しておいてください。

주의 중요 안전 지침

이 경고 기호는 위험을 나타냅니다. 작업자가 신체 부상을 일으킬 수 있는 위험한 환경에 있습니다. 장비에 작업을 수행하기 전에 전기 회로와 관련된 위험을 숙지하고 표준 작업 관례를 숙지하여 사고를 방지하십시오. 각 경고의 마지막 부분에 있는 경고문 번호를 참조하여 이 장치와 함께 제공되는 번역된 안전 경고문에서 해당 번역문을 찾으십시오.

이 지시 사항을 보관하십시오.

Aviso INSTRUÇÕES IMPORTANTES DE SEGURANÇA

Este símbolo de aviso significa perigo. Você se encontra em uma situação em que há risco de lesões corporais. Antes de trabalhar com qualquer equipamento, esteja ciente dos riscos que envolvem os circuitos elétricos e familiarize-se com as práticas padrão de prevenção de acidentes. Use o número da declaração fornecido ao final de cada aviso para localizar sua tradução nos avisos de segurança traduzidos que acompanham o dispositivo.

GUARDE ESTAS INSTRUÇÕES

Advarsel VIGTIGE SIKKERHEDSANVISNINGER

Dette advarselssymbol betyder fare. Du befinder dig i en situation med risiko for legemeskade. Før du begynder arbejde på udstyr, skal du være opmærksom på de involverede risici, der er ved elektriske kredsløb, og du skal sætte dig ind i standardprocedurer til undgåelse af ulykker. Brug erklæringsnummeret efter hver advarsel for at finde oversættelsen i de oversatte advarsler, der fulgte med denne enhed.

GEM DISSE ANVISNINGER

تحذير

إرشادات الأمان الهامة

يوضح رمز التحذير هذا وجود خطر. وهذا يعني أنك متواجد في مكان قد ينتج عنه التعرض لإصابات. قبل بدء العمل، احذر مخاطر التعرض للصدمات الكهربائية وكن على علم بالإجراءات القياسية للحيلولة دون وقوع أي حوادث. استخدم رقم البيان الموجود في أحر كل تحذير لتحديد مكان ترجمته داخل تحذيرات الأمان المترجمة التي تأتي مع الجهاز. قم بحفظ هذه الإرشادات

REVIEW DRAFT – CISCO CONFIDENTIAL

Upozorenje **VAŽNE SIGURNOSNE NAPOMENE**

Ovaj simbol upozorenja predstavlja opasnost. Nalazite se u situaciji koja može prouzročiti tjelesne ozljede. Prije rada s bilo kojim uređajem, morate razumjeti opasnosti vezane uz električne sklopove, te biti upoznati sa standardnim načinima izbjegavanja nesreća. U prevedenim sigurnosnim upozorenjima, priloženima uz uređaj, možete prema broju koji se nalazi uz pojedino upozorenje pronaći i njegov prijevod.

SAČUVAJTE OVE UPUTE

Upozornění **DŮLEŽITÉ BEZPEČNOSTNÍ POKYNY**

Tento upozorňující symbol označuje nebezpečí. Jste v situaci, která by mohla způsobit nebezpečí úrazu. Před prací na jakémkoliv vybavení si uvědomte nebezpečí související s elektrickými obvody a seznamte se se standardními opatřeními pro předcházení úrazům. Podle čísla na konci každého upozornění vyhledejte jeho překlad v přeložených bezpečnostních upozorněních, která jsou přiložena k zařízení.

USCHOVEJTE TYTO POKYNY

Προειδοποίηση **ΣΗΜΑΝΤΙΚΕΣ ΟΔΗΓΙΕΣ ΑΣΦΑΛΕΙΑΣ**

Αυτό το προειδοποιητικό σύμβολο σημαίνει κίνδυνο. Βρίσκεστε σε κατάσταση που μπορεί να προκαλέσει τραυματισμό. Πριν εργαστείτε σε οποιοδήποτε εξοπλισμό, να έχετε υπόψη σας τους κινδύνους που σχετίζονται με τα ηλεκτρικά κυκλώματα και να έχετε εξοικειωθεί με τις συνήθειες πρακτικές για την αποφυγή ατυχημάτων. Χρησιμοποιήστε τον αριθμό δήλωσης που παρέχεται στο τέλος κάθε προειδοποίησης, για να εντοπίσετε τη μετάφρασή της στις μεταφρασμένες προειδοποιήσεις ασφαλείας που συνοδεύουν τη συσκευή.

ΦΥΛΑΞΤΕ ΑΥΤΕΣ ΤΙΣ ΟΔΗΓΙΕΣ

אזהרה

הוראות בטיחות חשובות

סימן אזהרה זה מסמל סכנה. אתה נמצא במצב העלול לגרום לפציעה. לפני שתעבוד עם ציוד כלשהו, עליך להיות מודע לסכנות הכרוכות במעגלים חשמליים ולהכיר את הנהלים המקובלים למניעת תאונות. השתמש במספר ההוראה המסופק בסופה של כל אזהרה כדי לאתר את התרגום באזהרות הבטיחות המתורגמות שמצורפות להתקן.

שמור הוראות אלה

Opomena **ВАЖНИ БЕЗБЕДНОСНИ НАПАТСТВИЈА**

Симболот за предупредување значи опасност. Се наоѓате во ситуација што може да предизвика телесни повреди. Пред да работите со опремата, бидете свесни за ризикот што постои кај електричните кола и треба да ги познавате стандардните постапки за спречување на несреќни случаи. Искористете го бројот на изјавата што се наоѓа на крајот на секое предупредување за да го најдете неговиот период во prevedените безбедносни предупредувања што се испорачани со уредот.

ЧУВАЈТЕ ГИ ОБИЕ НАПАТСТВИЈА

REVIEW DRAFT – CISCO CONFIDENTIAL

Ostrzeżenie WAŻNE INSTRUKCJE DOTYCZĄCE BEZPIECZEŃSTWA

Ten symbol ostrzeżenia oznacza niebezpieczeństwo. Zachodzi sytuacja, która może powodować obrażenia ciała. Przed przystąpieniem do prac przy urządzeniach należy zapoznać się z zagrożeniami związanymi z układami elektrycznymi oraz ze standardowymi środkami zapobiegania wypadkom. Na końcu każdego ostrzeżenia podano numer, na podstawie którego można odszukać tłumaczenie tego ostrzeżenia w dołączonym do urządzenia dokumencie z tłumaczeniami ostrzeżeń.

NINIEJSZE INSTRUKCJE NALEŻY ZACHOWAĆ

Upozornenie DÔLEŽITÉ BEZPEČNOSTNÉ POKYNY

Tento varovný symbol označuje nebezpečenstvo. Nachádzate sa v situácii s nebezpečenstvom úrazu. Pred prácou na akomkoľvek vybavení si uvedomte nebezpečenstvo súvisiace s elektrickými obvodmi a oboznámte sa so štandardnými opatreniami na predchádzanie úrazom. Podľa čísla na konci každého upozornenia vyhľadajte jeho preklad v preložených bezpečnostných upozorneniach, ktoré sú priložené k zariadeniu.

USCHOVAJTE SI TENTO NÁVOD

Related Publications

These documents provide complete information about the access point:

- *Release Notes for Cisco Wireless LAN Controllers and Lightweight Access Points*
- *Quick Start Guide: Cisco Aironet 1520 Series Lightweight Outdoor Mesh Access Points*
- *Cisco Wireless LAN Controller Configuration Guide*

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

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

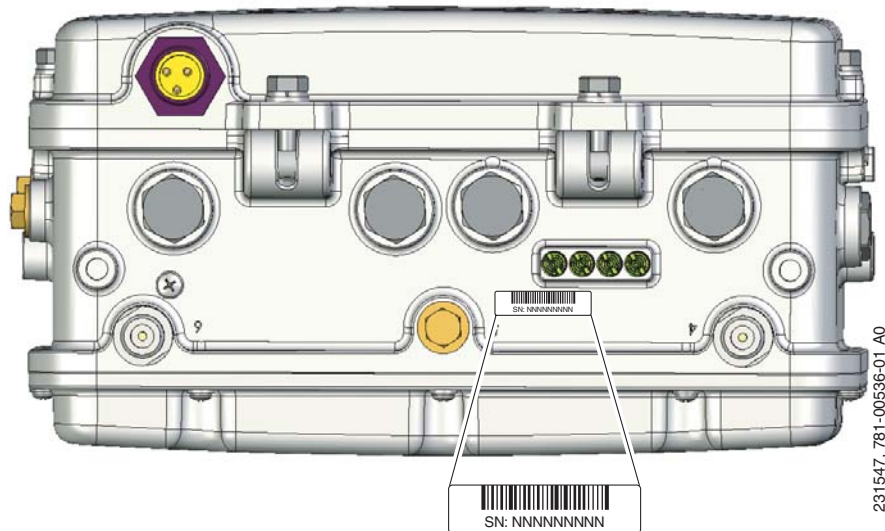
To browse to the access point documentation, click **Cisco Aironet 1520 Series** listed under “Outdoor Wireless.” The documentation can be accessed from the Support box.

To browse to the Cisco Wireless LAN Controller documentation, click **Cisco 4400 Series Wireless LAN Controllers** or **Cisco 2100 Series Wireless LAN Controllers** listed under “Wireless LAN Controllers.” The documentation can be accessed from the Support box.

REVIEW DRAFT – CISCO CONFIDENTIAL**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 - Need New picture



The access point serial number label contains the following information:

- Model number, such as *AIR-LAP1521G-A-k9* or *AIR-LAP1522AG-A-k9*.
- Serial number, such as *WCN0636279B* (11 alphanumeric digits).
- Access point MAC address, such as *00abc65094f3* (12 hexadecimal digits). It is located to the right of the serial number.
- Cable modem MAC address for cable configuration, such as *00abc7d094f9* (12 hexadecimal digits). The cable modem MAC address is only available on the access point cable configuration. It is located below the serial number.

You need your product serial number when requesting support from the Cisco Technical Assistance Center.

Obtaining Documentation, Obtaining Support, and Security Guidelines

For information on obtaining documentation, obtaining support, providing documentation feedback, security guidelines, and also 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>



Overview

The Cisco Aironet 1520 Series Outdoor Wireless Mesh Access Point (hereafter called the *access point*) is a wireless device designed for wireless client access, point-to-point bridging, point-to-multipoint bridging, and point-to-multipoint mesh wireless connectivity. The access point is a standalone unit that can be mounted on a streetlight pole, building wall, overhang, or a cable strand.access point

The access point model LAP1522 supports two radios (2.4-GHz and 5-GHz). The access point provides client access and without the need for a license. The 5-GHz radio is dedicated to backhaul operations to reach a wired network and the 2.4-GHz radio is used for wireless clients. The access point can support 6 to 54 Mbps data rates.

The access point model LAP1524 supports up to four radios operating in the 2.4-GHz, 4.9-GHz, and 5-GHz frequency bands. The access point provides client access and without the need for a license. The 5-GHz and 4.9-GHz radios are dedicated to backhaul operations to reach a wired network and the 2.4-GHz radio is used for wireless clients. The access point can support 6 to 54 Mbps data rates.

The access point is manufactured in three configurations: cable, pole mount, and mesh. The cable configuration has three antenna connectors on the top of the unit, can be mounted to a cable strand, and supports power-over-cable (POC). The pole mount configuration supports two antennas on the top and bottom of the unit. It can be mounted to a pole or building wall and supports fiber-optic networks and several power options. The Mesh configuration has two antennas on the top and bottom of the unit. It can be powered by AC and only supports wireless backhaul communications to reach the wired network. It does not support hard-wired communications (cable, fiber-optic, or Ethernet) to a wired network.

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 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 *Deployment Guide: Cisco Mesh Networking Solution* 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 Wireless Control System (WCS) network management system 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 Features, page 1-2](#)
- [Network Deployment Examples, page 1-11](#)

REVIEW DRAFT – CISCO CONFIDENTIAL

Hardware Features

This section describes the hardware features of the access point. [Figure 1-1](#), [Figure 1-2](#), and [Figure 1-3](#) show the access point connectors.



Note

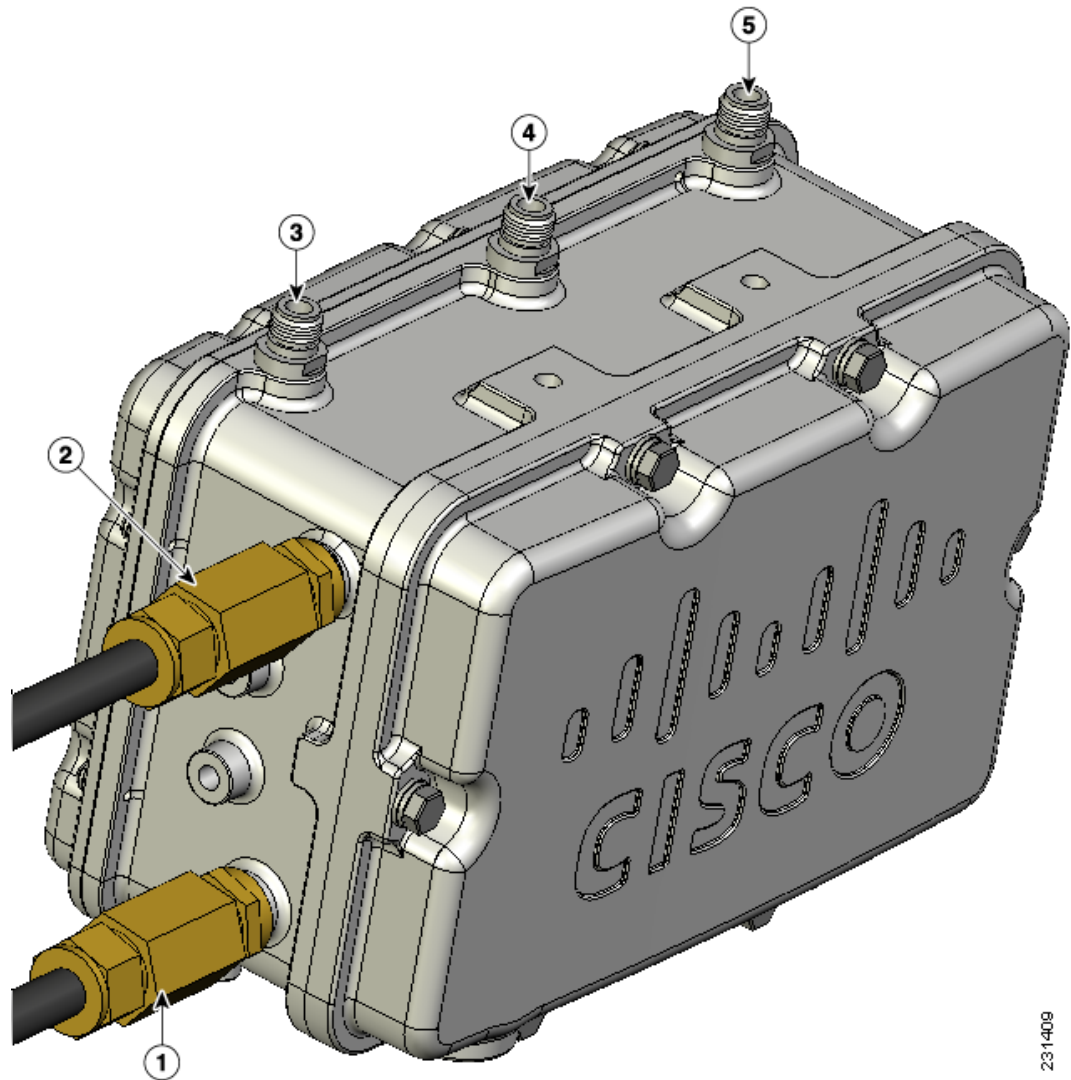
The illustrations in this document show all available connections for the access point. Unused connections are capped with a connector plug to ensure the access point’s watertight integrity. Liquid tight adapters are provided for connector openings, which can be installed before or after deploying the access point. The illustrations do not show antenna port 5, which is reserved for future use.

Figure 1-1 Access Point Bottom Connectors



1	AC power connector ¹ (optional)	5	PoE-Out connector ²
2	Reserved for future use	6	LEDs
3	Antenna connector ³ (Type N)	7	Antenna connector ³ (Type N)
4	Alternate fiber-optic connector location (optional)	8	PoE-In connector ^{1, 2}

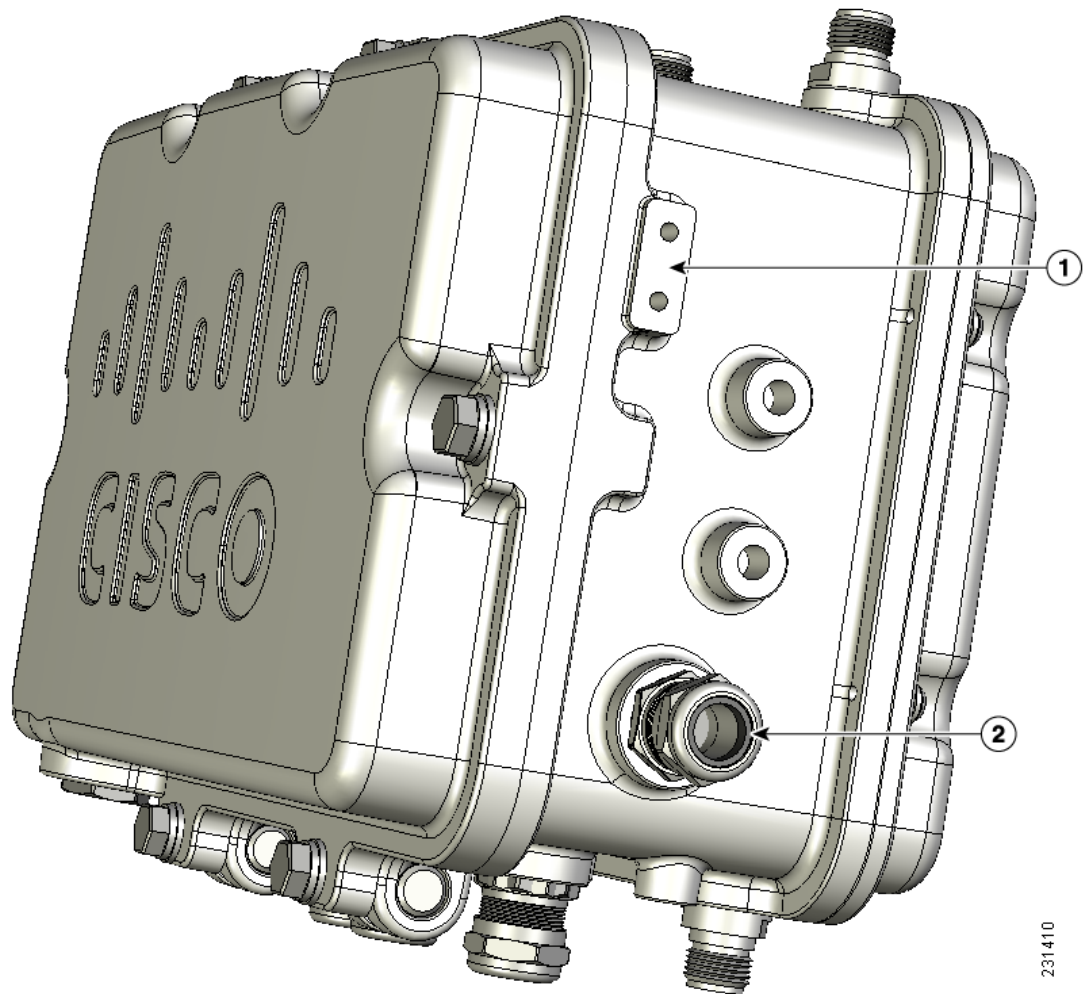
1. Only one power source is usually configured.
2. PoE = Power over Ethernet
3. Antenna locations depend upon access point configuration (see the [“Antenna Connector Locations”](#) section on page 1-5).

REVIEW DRAFT – CISCO CONFIDENTIAL**Figure 1-2 Cable, Fiber-Optic, and Antenna Connector Locations**

231408

1	Cable POC connector (optional) ¹	4	Antenna connector ² (Type N)
2	Fiber-optic connector ³ (optional)	5	Antenna connector ² (Type N)
3	Antenna connector ² (Type N)		

1. Stinger connector shown is user supplied.
2. Antenna locations depend upon access point configuration (see the “[Antenna Connector Locations](#)” section on page 1-5).
3. Liquid tight adapter not shown.

REVIEW DRAFT – CISCO CONFIDENTIAL**Figure 1-3 DC Power Connector and Ground Screw Holes**

231410

1	Ground screw holes	2	DC power connector
---	--------------------	---	--------------------

Some of the access point's hardware features are listed below:

- Two radios (2.4- and 5-GHz)—see the “Dual Radio Operation” section on page 1-7
- External radio antennas—see the “External Antennas” section on page 1-7
- Multiple power sources—see the “Multiple Power Sources” section on page 1-8
- Ethernet ports—see the “Ethernet Ports” section on page 1-9
- Rugged metal enclosure—see the “Metal Enclosure” section on page 1-10
- Optional cable modem—see the “Cable Modem” section on page 1-10
- Optional hardware—see the “Optional Hardware” section on page 1-10

REVIEW DRAFT – CISCO CONFIDENTIAL

Connectors

The optional features of the access point support these connectors (see [Figure 1-1](#)):

- PoE-in connector—internal RJ-45 with liquid tight adapter for waterproofing
- PoE-out connector—internal RJ-45 with liquid tight adapter for waterproofing
- Three or four antenna connectors (Type N)—depends on access point configuration
- Fiber-optic connector—internal small form-factor pluggable (SFP) transceiver with LC connector
- Power-over-cable (POC) stinger connector—customer provided
- AC power connector (3-pin Remke Mini-Link 50908)
- DC power connector—internal 2-pin connector

Antenna Connector Locations

The access point is manufactured in three configurations, cable, mesh, and pole mount. These configurations support specific locations for the access point antennas, as shown in [Table 1-1](#).

Table 1-1 **Antenna Locations per Access Point Configuration**

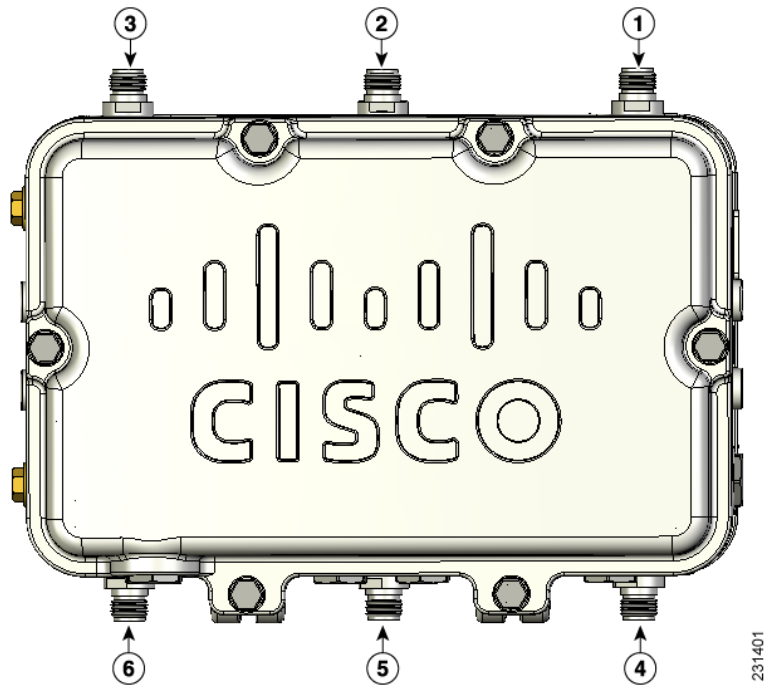
Antenna Port	Access Point Configurations	
	Cable	Mesh and Pole Mount
1	2.4-GHz antenna connector (RX)	5-GHz antenna connector (TX/RX)
2	5-GHz antenna connector (TX/RX)	– ¹
3	2.4-GHz antenna connector (TX/RX)	2.4-GHz antenna connector (RX)
4	– ¹	2.4-GHz antenna connector (RX)
5	– ¹	– ¹
6	– ¹	2.4-GHz antenna connector (TX/RX)

1. Reserved for future use. A plug is installed.

REVIEW DRAFT – CISCO CONFIDENTIAL

Figure 1-4 shows the antenna port locations viewed from the hinged cover side.

Figure 1-4 Antenna Port Locations



1	Antenna port 1	4	Antenna port 4
2	Antenna port 2	5	Antenna port 5 ¹
3	Antenna port 3	6	Antenna port 6

1. Reserved for future use. A plug is installed.

REVIEW DRAFT – CISCO CONFIDENTIAL

Dual Radio Operation

The access point supports 2.4-GHz and 5-GHz radios using external antennas (see “[External Antennas](#)”).

The LAP1522 model supports simultaneous dual-radio operation using a 2.4-GHz 802.11b/g radio and a 5-GHz 802.11a radio. The 5-GHz radio can operate in either the upper industrial, scientific and medical (ISM) 5.8-GHz band or the public safety 4.9-GHz band. The 5-GHz radio supports one antenna and is used for backhaul operations to the controller.

**Note**

The 4.9-GHz band requires a license and can only be used by qualified public safety operators as defined in section 90.20 of the FCC rules.

The 2.4-GHz radio supports two or three antennas for multi-input, single output (MISO) operation. The access point uses two or three receivers to support maximum ratio combining (MRC) to enhance receiver performance. MRC is a technique that combines the signals from multiple receivers in a manner to optimize the signals. MRC can provide up to 3 dB of increased receive signal strength with two receive antennas or up to 5 dB with three antennas.

External Antennas

The access point supports up to three N-type radio frequency (RF) antenna connectors on the top of the unit and two on the bottom of the unit. The number of active antenna connectors depends upon the access point configuration (see [Antenna Connector Locations, page 1-5](#)). All access point configurations supports multiple 2.4-GHz antennas for MISO operation, but only one 5-GHz antenna.

When using the optional Cisco compact omnidirectional antennas, the 2.4- and 5-GHz antennas connect directly to the access point. The Cisco omnidirectional antennas use vertical polarization.

**Warning**

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

The access point has been designed to operate with the antennas listed below and with a maximum gain of 8 dBi for 2.4 GHz and 17 dBi for 5 GHz. Antennas not in this list or with a higher gain are strictly prohibited for use with the access point. The required antenna impedance is 50 ohms.

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

**Caution**

For directly mounted antennas, you must not add weatherproofing around the antenna connectors because the antenna drain holes might be blocked and damage the antenna.

REVIEW DRAFT – CISCO CONFIDENTIAL

Table 1-2 and Table 1-3 list the supported external antennas for the access point.

Table 1-2 External 5-GHz Antennas

Part Number	Model ¹	Gain (dBi)
AIR-ANT5180V-N	5-GHz compact omnidirectional	8
AIR-ANT58G10SSA-N	5-GHz sector	9.5
AIR-ANT5114P-N	5-GHz patch	14
AIR-ANT5117S-N	5-GHz 90-degree sector	17

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

Table 1-3 External 2.4-GHz Antennas

Part Number	Model	Gain (dBi)
AIR-ANT2450V-N	2.4-GHz compact omnidirectiona	5.5
AIR-ANT2480V-N	2.4 GHz omnidirectional	8

Multiple Power Sources

The access point supports these power sources:

- PoE—power injector (AIR-PWRINJ1500-2=)
- AC power—100 to 480 VAC (standard power source for the pole mount configuration)
- POC—40 to 90 VAC (quasi-square wave AC), (standard power source for the cable configuration)
- External 12 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

- Internal battery

The access point 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 default prioritization:

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



Warning

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

REVIEW DRAFT – CISCO CONFIDENTIAL**Caution**

To provide inline PoE, you must use the 1520 power injector (AIR-PWRINJ1500-2=). Other power injectors, PoE switches, and 802.3af 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 1520 power injector (AIR-PWRINJ1500-2=) must be used in an indoor environment only.

**Note**

In the cable configuration, the cable modem is activated only when the access point is powered by POC or external 12 VDC power. When using only PoE power, the cable modem is deactivated.

**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).

The Ethernet cable from the power injector to the access point (PoE-in port) must be not less than 10 ft (3.1 m).

The AC power cord options are listed below:

- 40-ft (15.2-m) power cord for light pole installations in the US and Canada. One end of the power cord is terminated with an access point AC power connector, and the other end is terminated with an AC plug (AIR-CORD-R3P-40NA=).
- 4-ft (1.2-m) streetlight power tap adapter for light pole installations in the US and Canada (AIR-PWR-ST-LT-R3P=).

Ethernet Ports

The access point supports a PoE-in port and a PoE-out port. The access point's PoE-in port uses an RJ-45 connector (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.

The access point's PoE-out (10/100/1000BASE-T) port uses an RJ-45 connector (with a liquid tight adapter) 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.

**Note**

The PoE-out port is disabled when the access point is powered by the power injector.

The Ethernet MAC addresses is printed on the bottom of the access point under the LEDs (refer to the [“Finding the Product Serial Number”](#) section on page XIV).

**Warning**

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

REVIEW DRAFT – CISCO CONFIDENTIAL

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 1520 power injector (AIR-PWRINJ1500-2=). Other power injectors, PoE switches, and 802.3af power sources cannot provide adequate power, which may cause the access point to malfunction and cause possible over-current conditions at the power source.

Cable Modem

The access point cable configuration contains an internal cable modem for connection to the cable network from the pole-mounted cable lines. The access point can be powered using the 40-to 90-VAC (quasi-square wave AC) power provided by the cable network.

**Note**

The access point uses a Scientific Atlanta DPC2100 cable modem board and 4015821 RF splitter.

The cable modem supports these main features:

- Data Over Cable Service Interface Specifications (DOCSIS) 2.0
- Backward compatibility with existing DOCSIS 1.1 and 1.0 networks

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

Some of the access point hardware options are listed below:

- Fiber-optic module and take-up reel kit (GLC-FE-100BX-URGD=)—Small form-factor pluggable (SFP) module for connection to fiber-optic lines. The take-up reels are used to store excess fiber-optic cable by wrapping the cable around the reels.
 - Single strand fiber bidirectional optical transceiver
 - 1.3 (transmit) /1.5 (receive) micrometer wavelength division multiplexing (WDM) function
 - 100 Mb/s data rates
 - LC receptacle
 - Supports up to 15.5 mi (25 km) of fiber-optic cable.
- Pole mount kit (AIR-ACCPMK1520=)—provides hardware for mounting the access point to a metal or wood pole, such as a streetlight pole.
- Strand mount kit (AIR-ACCSMK1520=)—provides hardware for mounting the access point to a cable strand.

REVIEW DRAFT—CISCO CONFIDENTIAL

- Streetlight power tap adapter (AIR-PWR-ST-LT-R3P=)—connects to the light control connector on a streetlight pole and provides AC power to the access point.
- 1520 power injector (AIR-PWRINJ1500-2=)—provides PoE to the access point.
- 40-ft (12.2-m) power cord for light pole installations in the US and Canada (AIR-CORD-R3P-40NA=)—provides AC power to the access point. One end of the power cord is terminated with an access point AC power connector, and the other end is terminated with an AC plug.
- Battery backup module (AIR-1520-BATT-6AH). The integrated battery can be used for temporary backup power during external power interruptions.
 - 3-hour access point operation using two radios at 77°F (25°C)—with PoE output port off
 - 2-hour access point operation using two radios at 77°F (25°C)—with PoE output port on
- Strap hand tool (AIR-BAND-INST-TL=)—used to install the metal straps used in pole mounting.

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 one of two primary radio roles: a root access point (hereafter called a *RAP*) or the access points that relay their wireless connections to the controller are called *mesh access points (MAPs)*. When the access point has a wired Ethernet, fiber-optic, or cable connection to the controller (through a switch), the radio role is called 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. Both *RAP* and *MAP* access points can support wireless clients using the 2.4-GHz radio.



Note

The access point must be configured as a *RAP* in the controller, whereas the *MAP* role is a default setting.

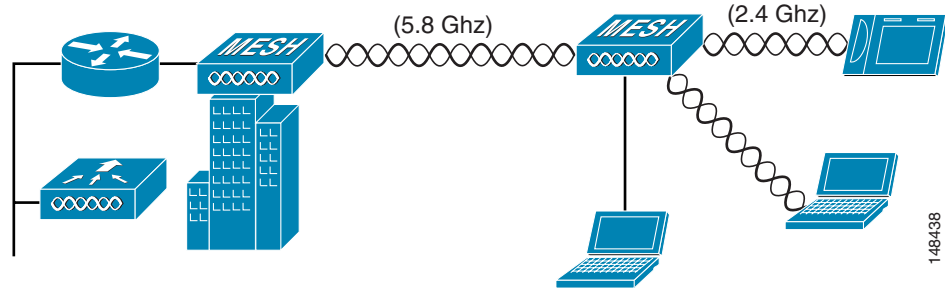
When the access point does not have a wired Ethernet, fiber-optic, or cable connection to the controller, the radio role is called a *MAP*. The *MAPs* have a wireless connection (through the backhaul interface) to other *MAPs* and finally to a *RAP* with an Ethernet or cable connection through a switch 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).

REVIEW DRAFT – CISCO CONFIDENTIAL

Wireless Backhaul

The access point supports wireless backhaul capability using the 5-GHz radio to bridge to another access point to reach a wired network connection to a controller (see Figure 1-5). 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. Lightweight access point protocol (LWAPP) control traffic is also transferred over this bridged link.

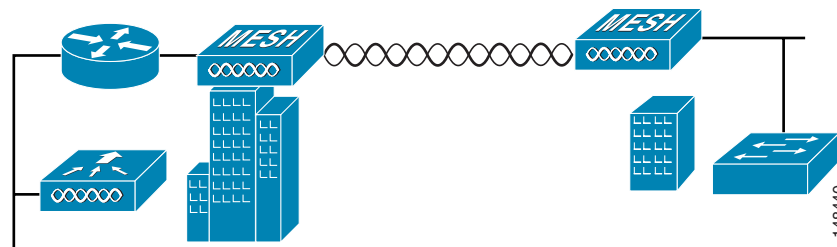
Figure 1-5 Access Point Backhaul Example



Point-to-Point Bridging

The access points can be used to extend a remote network by using the 5-GHz backhaul radio to bridge the two network segments as shown in Figure 1-6. To support Ethernet bridging, you must enable bridging on the controller for each access point.

Figure 1-6 Access Point Point-to-Point Bridging Example



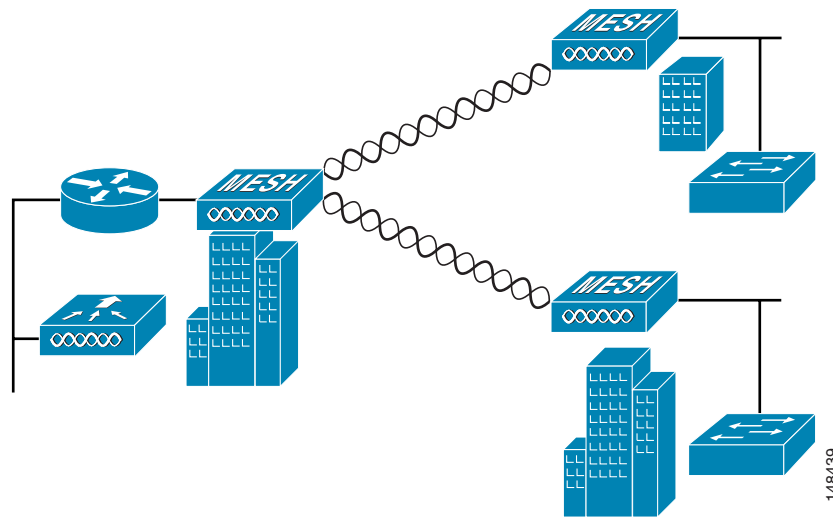
REVIEW DRAFT – CISCO CONFIDENTIAL

Point-to-Multipoint Bridging

The access points can be used as a RAP to connect multiple remote MAPs with their associated wired networks (see [Figure 1-7](#)). 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 might be limited and possibly not suitable for direct wireless client access.

Figure 1-7 Access Point Point to Multipoint Bridging Example



REVIEW DRAFT – CISCO CONFIDENTIAL

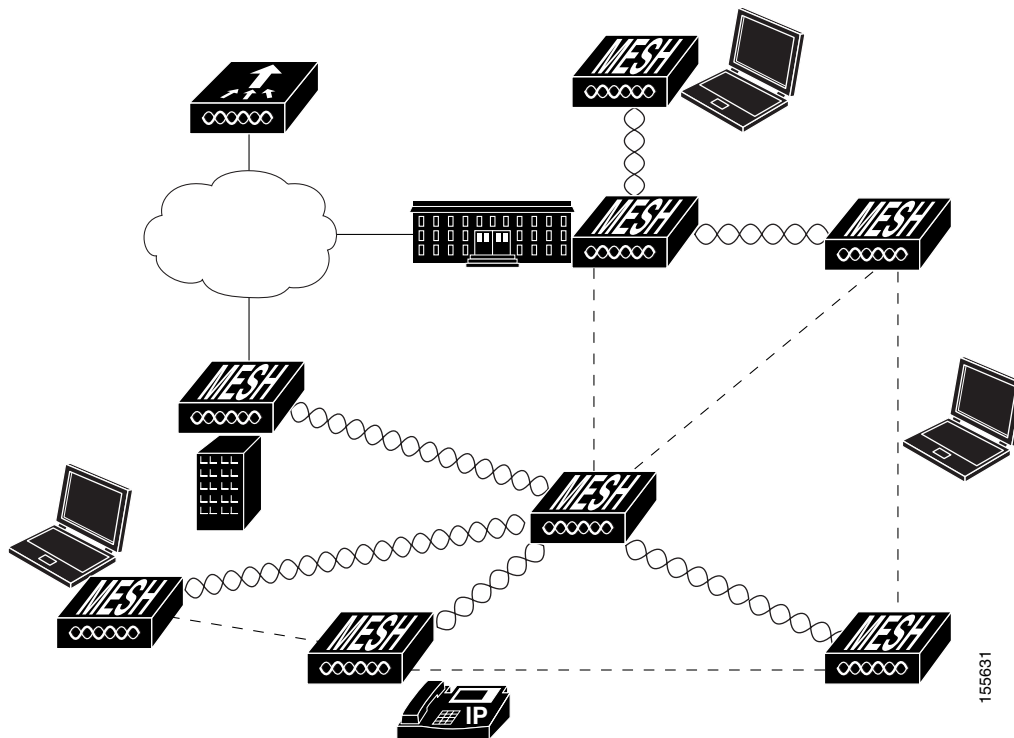
Mesh Network

The access points are 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*.

Intelligent wireless routing is provided by the patented 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.

Figure 1-8 illustrates a typical mesh configuration using MAPs and RAPs.

Figure 1-8 Typical Mesh Configuration Using Access Points



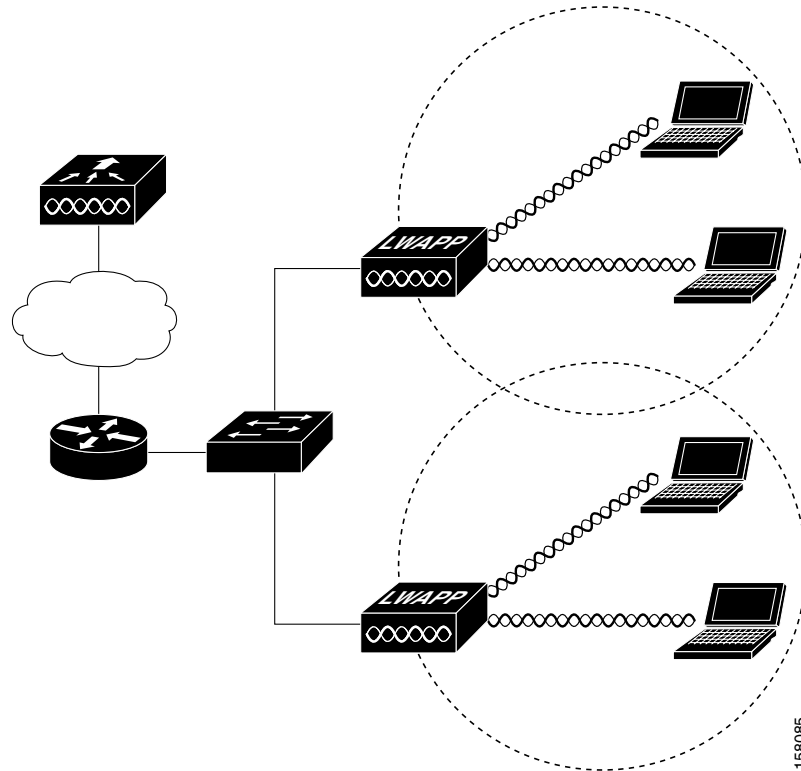
REVIEW DRAFT – CISCO CONFIDENTIAL

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 1-9 illustrates a typical Layer-3 wireless network configuration containing access points and a controller.

Figure 1-9 Typical Layer 3 Access Point Network Configuration Example



REVIEW DRAFT – CISCO CONFIDENTIAL



REVIEW DRAFT – CISCO CONFIDENTIAL

CHAPTER **2**

Mounting Instructions

This chapter describes warnings, safety information, and mounting information needed during the installation of your access point. The chapter contains these sections:

- [Unpacking the Access Point, page 2-2](#)
- [Tools and Materials that You Supply, page 2-2](#)
- [Warnings, page 2-4](#)
- [Safety Information, page 2-4](#)
- [Avoiding Damage to Radios in a Testing Environment, page 2-7](#)
- [Installation Guidelines, page 2-8](#)
- [Mounting the Access Point, page 2-16](#)
- [Installing the Access Point in Hazardous Locations, page 2-42](#)
- [Grounding the Access Point, page 2-46](#)
- [Connecting a Fiber-Optic Cable to the Access Point, page 2-46](#)
- [Powering the Access Point, page 2-50](#)

REVIEW DRAFT – CISCO CONFIDENTIAL

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.

Follow these steps to unpack the access point:

-
- 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](#) are included in the shipment. If any item is damaged or missing, notify your authorized Cisco sales representative.
-

Package Contents

Each access point package contains the following items:

- Access point
- Cisco product documentation and translated safety warnings
- Grounding lug with two screws and lock washers
- Three liquid tight adapters
- Two-pin DC power connector
- Ground lug (Panduit PLCD6-10A-L) and screws with lock washers

Tools and Materials that You Supply

- 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
- Small flat screwdriver for DC power connector
- Optional power injector (AIR-PWRINJ1500-2=)
- Optional AC power cord
 - 40-ft (12.2-m) power cord (AIR-CORD-R3P-40NA=) for light pole installations in the US and Canada
 - 4-ft (1.2-m) streetlight power tap adapter (AIR-PWR-ST-LT-R3P=) for light pole installations in the US and Canada
- Antennas, 2.4 and 5 GHz (refer to the [“External Antennas”](#) section on page 1-7)
- Optional pole mount kit (AIR-ACCPMK1520=)
- Optional strand mount kit (AIR-ACCSMK1520=)
- Optional strap hand tool (AIR-BAND-INST-TL=)

REVIEW DRAFT – CISCO CONFIDENTIAL

- Optional fiber-optic 100BASE-BX10-U SFP, fiber-optic take-up reels, and liquid tight adapter (GLC-FE-100BX-URGD=)
- Optional outdoor-rated fiber-optic cable with 0.20 to 0.35 in. (0.51 to 0.89 cm) diameter
- 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 in. (.0.51 to 0.89 cm) diameter
- Optional cable Stinger connector
- Optional ground rod, as required by local regulations
- Optional ladder, power lift, rope, or other tools as required

Pole Installation

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

- Pole mount kit (AIR-ACCPMK1520=)
 - 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 supplied metal strap tool—(AIR-BAND-IT-TOOL=)
- 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

Cable Strand Installation

To install the access point on a cable strand, you need the following additional parts:

- Cable strand mount kit (AIR-ACCSMK1520=)
 - Strand mounting bracket
 - Strand clamp bracket
 - Four cable clamps
 - Four M8 flange nuts
 - Four hex bolts (M8 x16)
 - Four M8 split lock washers and six M8 flat washers
- Customer supplied 13-mm box-end wrench or socket set

REVIEW DRAFT – CISCO CONFIDENTIAL

- 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**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

**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.

REVIEW DRAFT – CISCO CONFIDENTIAL**Safety Precautions**

-  **Warning** In order to comply with radio frequency (RF) exposure limits, the antennas for this product should be positioned no less than 6.56 ft (2 m) from your body or nearby persons. Statement 339
-  **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** There is the danger of explosion if the battery is replaced incorrectly. Replace the battery only with the same or equivalent type recommended by the manufacturer. Dispose of used batteries according to the manufacturer's instructions. Statement 1015
-  **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** 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** When installing or replacing the unit, the ground connection must always be made first and disconnected last. Statement 1046.

REVIEW DRAFT – CISCO CONFIDENTIAL**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**

Before connecting or disconnecting a power cord, you must remove AC power from the power cord using a suitable service disconnect.

For additional important safety instructions for AC power cords, refer to the *AC Power Cords for Cisco Aironet 1520 Series Outdoor Mesh Access Points* document that shipped with your AC power cords.

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

1. 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.
2. Call your electric power company. Tell them your plans, and ask them to come look at your proposed installation.
3. 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.
4. When installing the access point and antennas, remember:
 - a. Do not use a metal ladder.
 - b. Do not work on a wet or windy day.
 - c. Do dress properly—shoes with rubber soles and heels, rubber gloves, long sleeved shirt or jacket.
5. Use a rope to lift the access point. If the assembly starts to drop, get away from it and let it fall.
6. 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.

REVIEW DRAFT – CISCO CONFIDENTIAL

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 receiver's maximum receive input level. 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:

$$\text{txpwr} + \text{tx gain} + \text{rx gain} - [\text{attenuation due to antenna spacing}] < \text{max rx input level}$$

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:

$$\text{txpwr} - [\text{attenuation due to coaxial components}] < \text{max rx input level}$$

**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.

REVIEW DRAFT – CISCO CONFIDENTIAL

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 *Deployment Guide: Cisco Mesh Networking Solution*.
- 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. We 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.

REVIEW DRAFT – CISCO CONFIDENTIAL

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 [“Configuring DHCP Option 43”](#) section on page F-1).
- Become familiar with the access point installation components (see the [“Becoming Familiar with Access Point Installation Components”](#) section on page 2-9).

Becoming Familiar with Access Point Installation Components

The access point is designed to be installed in an indoor or outdoor environment, such as an interior wall or ceiling or 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:

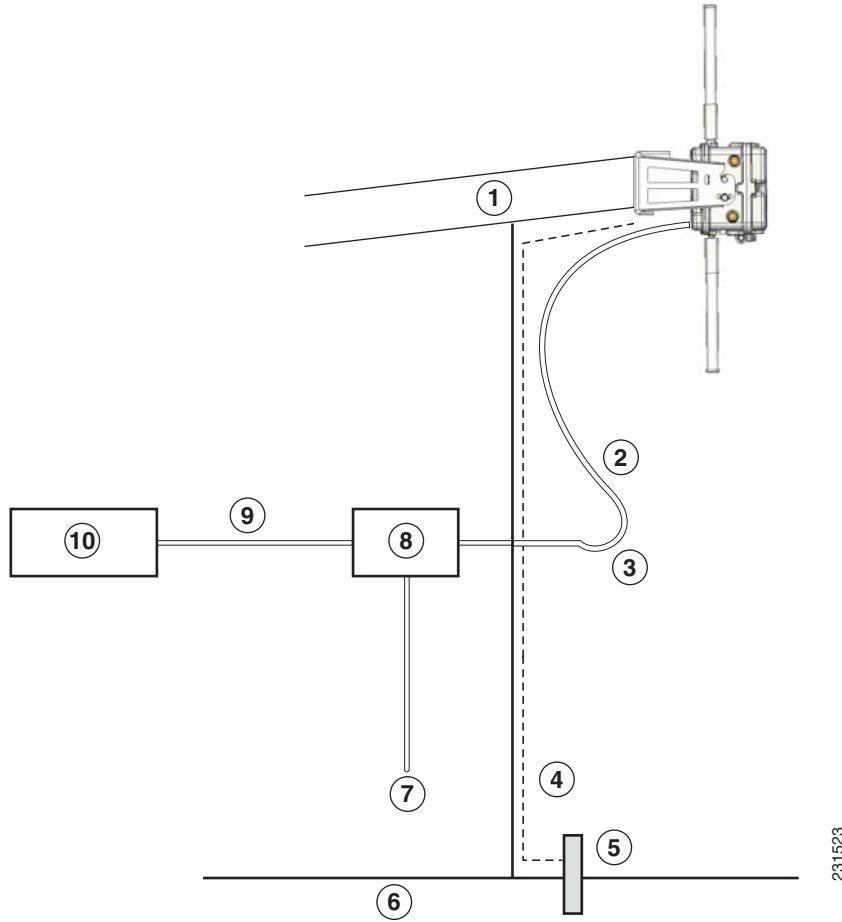
- Components in a typical access point installation (see [Figure 2-1](#))
- Pole mount installation (see [Figure 2-2](#))
- Cable strand mount installation (see [Figure 2-3](#))
- Streetlight power tap installation (see [Figure 2-4](#))

**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 access point’s watertight integrity. liquid tight adapters are provided for connector openings, which can be installed before or after deploying the access point. The illustrations do not show antenna port 5, which is reserved for future use.

REVIEW DRAFT – CISCO CONFIDENTIAL

Figure 2-1 Components in a Typical Access Point Installation



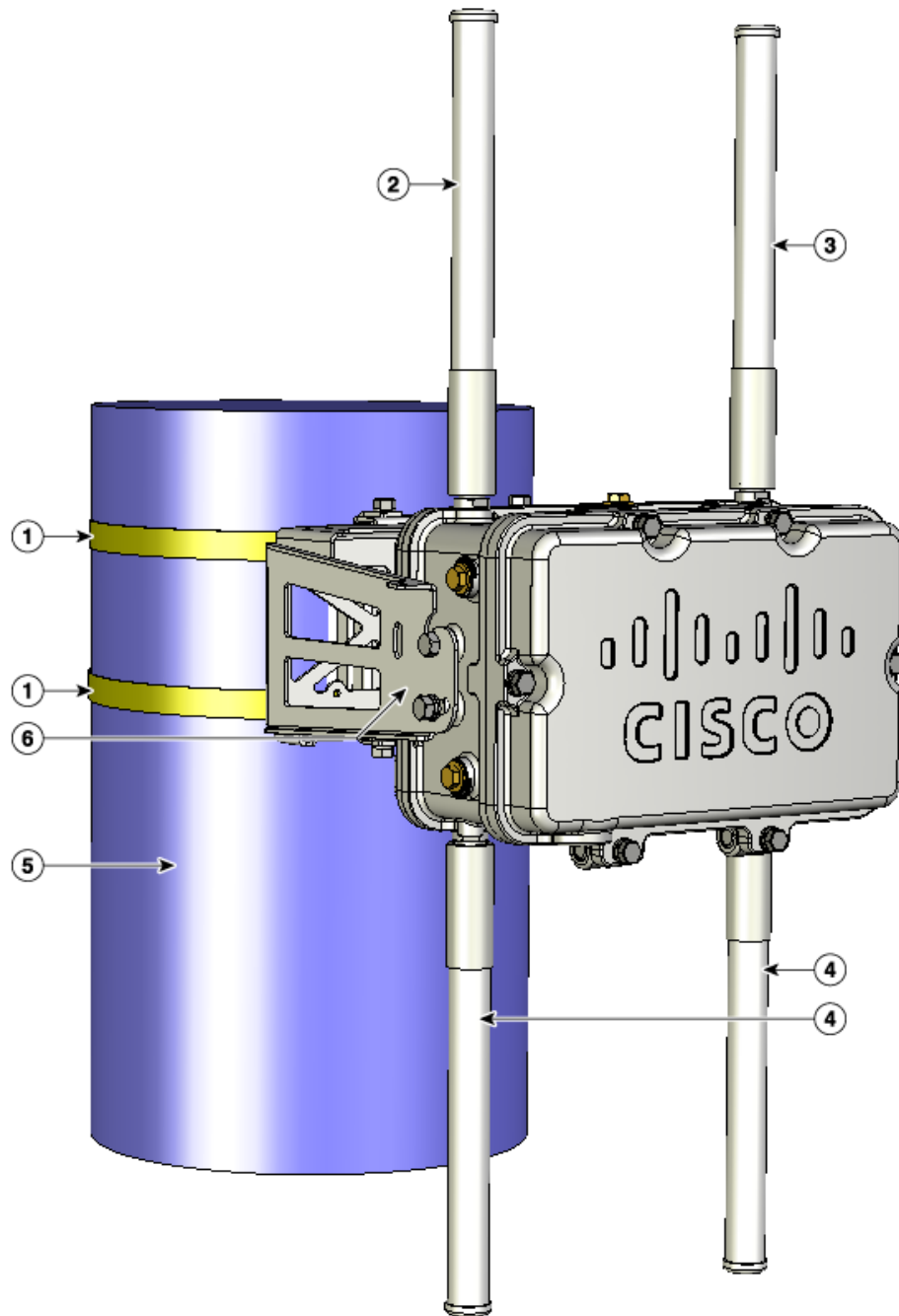
1	Building roof-overhang	6	Ground
2	Shielded outdoor-rated Ethernet (CAT5e or better) cable ¹	7	AC power cord ²
3	Water drip loop	8	Power injector ³
	6-AWG copper grounding wire ¹	9	Shielded Ethernet (CAT5e or better) cable ¹
5	Ground rod ¹	10	Controller (through a switch)

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.



Warning

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

REVIEW DRAFT – CISCO CONFIDENTIAL**Figure 2-2 Pole Mount Installation**

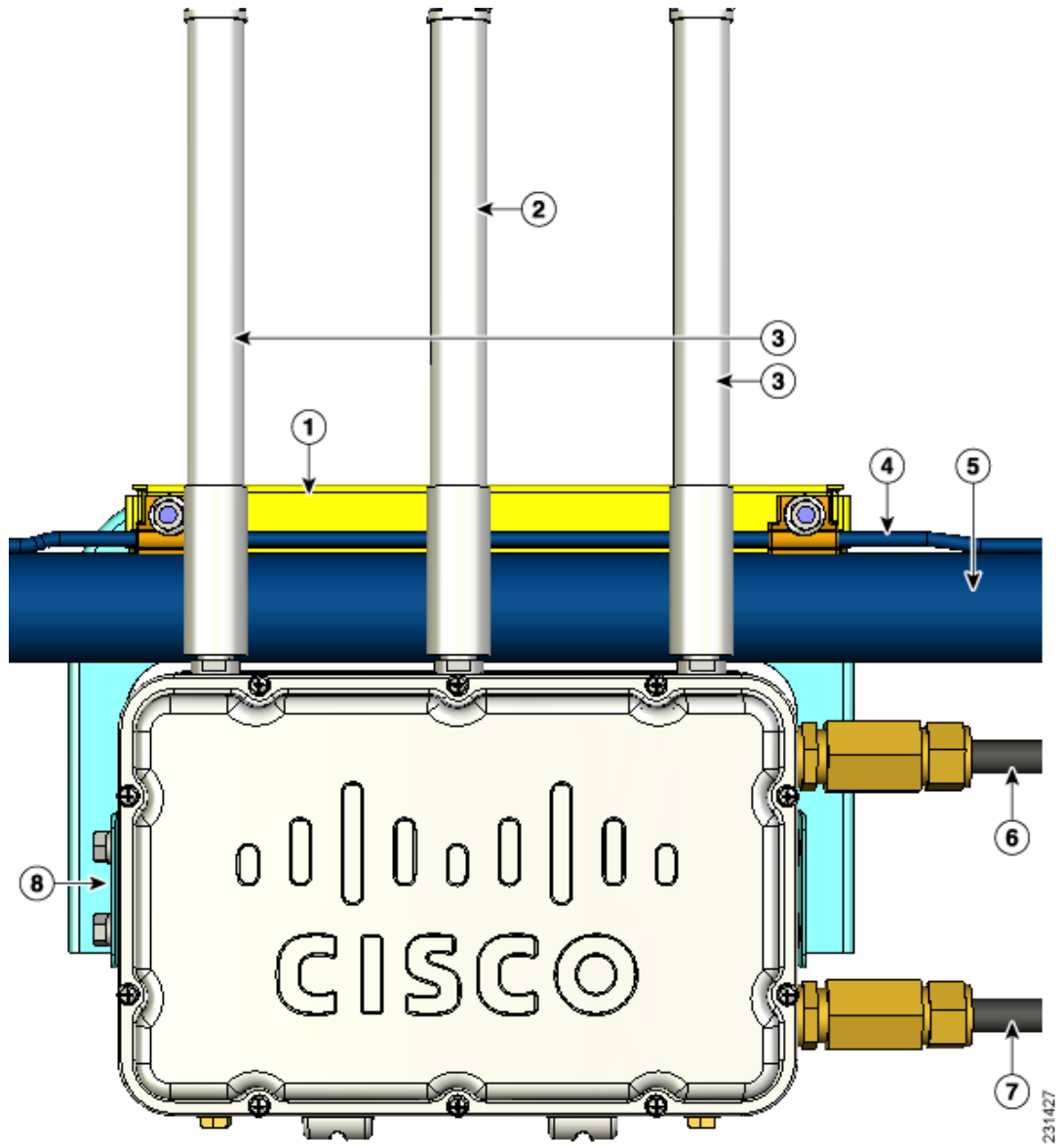
231420

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

1. Illustration shows antennas for an access point with two radios.

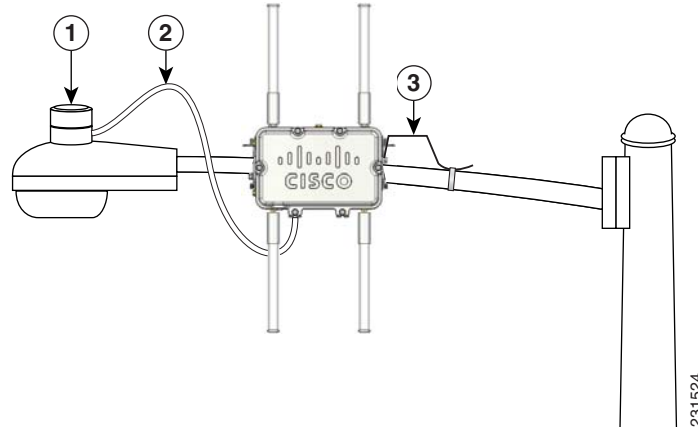
REVIEW DRAFT – CISCO CONFIDENTIAL

Figure 2-3 Cable Strand Mounting



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

- 1. Illustration shows antennas for an access point with two radios.
- 2. Liquid tight connector not shown.
- 3. Stinger connector shown is user supplied.

REVIEW DRAFT – CISCO CONFIDENTIAL**Figure 2-4 Streetlight Power Tap Adapter Installation**

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

Antenna Connector Locations

The access point is manufactured in three configurations, cable, pole mount, and mesh. These configurations support specific locations for the access point antennas as shown in [Table 2-1](#).

Table 2-1 Antenna Locations for Each Access Point Configuration¹

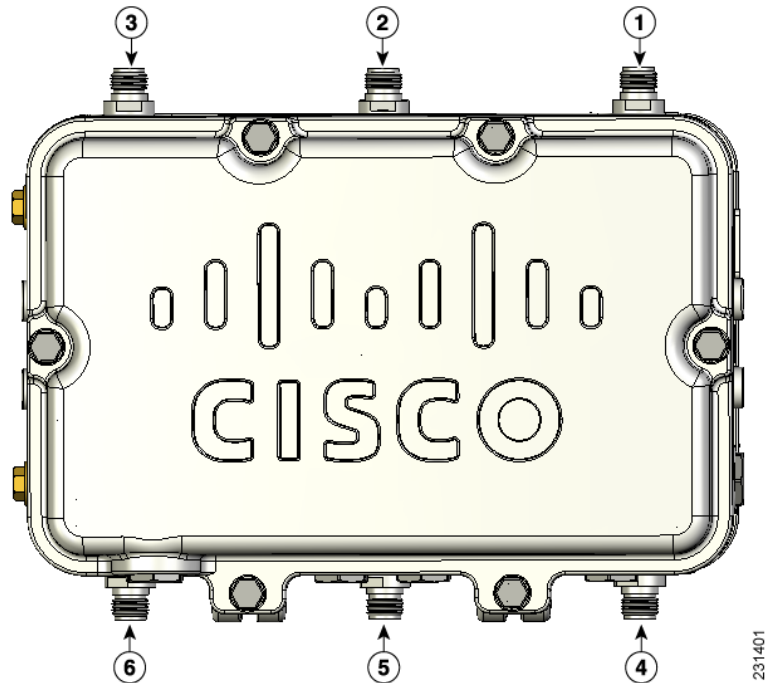
Antenna Port	Access Point Configurations	
	Cable	Pole Mount and Mesh
1	2.4-GHz antenna connector (RX)	5-GHz antenna connector (TX/RX)
2	5-GHz antenna connector (TX/RX)	– ²
3	2.4-GHz antenna connector (TX/RX)	2.4-GHz antenna connector (RX)
4	– ²	2.4-GHz antenna connector (RX)
5	– ²	– ²
6	– ¹	2.4-GHz antenna connector (TX/RX)

1. Antenna locations specified for a two radio access point.
2. Reserved for future use. A plug is installed.

REVIEW DRAFT – CISCO CONFIDENTIAL

Figure 2-5 shows the antenna port locations viewed from the hinged cover side.

Figure 2-5 Antenna Port Locations



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. Follow these steps to add a MAC filter entry on the controller:

-
- 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.

REVIEW DRAFT – CISCO CONFIDENTIAL

- 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 MAP radio role. One or more of your access points must be reconfigured as a 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.

Follow these steps to configure a RAP on the controller GUI:

- Step 1** Log into your controller using a web browser.
 - Step 2** Click **Wireless**. When your access point associates to the controller, your access point's name appears in the AP Name list.
 - Step 3** Double-click your access point's 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.
-

Configuring a 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 the same BGN, but 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.

The BGN should be configured very carefully on a live network. You should always start from the farthest node (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.

REVIEW DRAFT – CISCO CONFIDENTIAL

To configure the BGN for the access points using the 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's name appears in the AP Name list.
 - Step 3** Double-click on an access point's name.
 - Step 4** Find Mesh Information, 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.
-

Mounting the Access Point

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



Caution

All mounting methods on any wall surface is subject to the acceptance of local jurisdiction.

Installation Options

There are two optional installation kits:

- Pole mount kit—used for pole, wall, or streetlight installations
- Strand mount kit—used for cable strand 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.

REVIEW DRAFT – CISCO CONFIDENTIAL

Refer to these sections for installation details.

- [Access Point Mounting Orientation, page 2-17](#)
- [Mounting the Access Point on a Wall, page 2-17](#)
- [Mounting the Access Point on a Pole, page 2-21](#)
- [Cable Strand Mounting, page 2-30](#)

Access Point Mounting Orientation

When installing 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 [Figure 2-2](#), [Figure 2-3](#), and [Figure 2-4](#)). 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 contain 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 2-2](#) lists the material that you will need to provide in addition to the pole mount kit.

Table 2-2 *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.

REVIEW DRAFT – CISCO CONFIDENTIAL

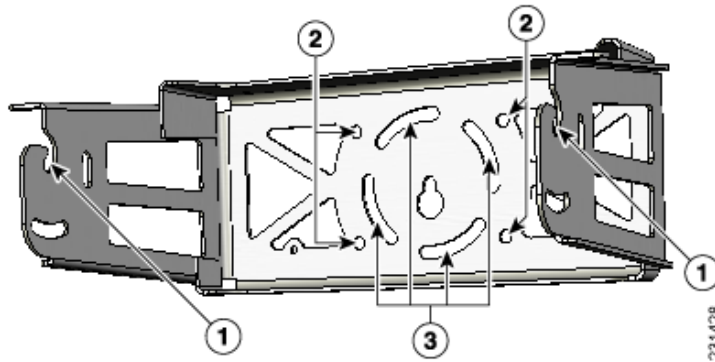
To mount the access point on a vertical wall, follow these instructions:

- Step 1** Use the mounting bracket as a template to mark four screw hole locations on your mounting surface. See [Figure 2-6](#) for the mounting bracket screw hole locations. You can optionally use the individual mounting holes or the mounting slots.

**Caution**

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

Figure 2-6 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.

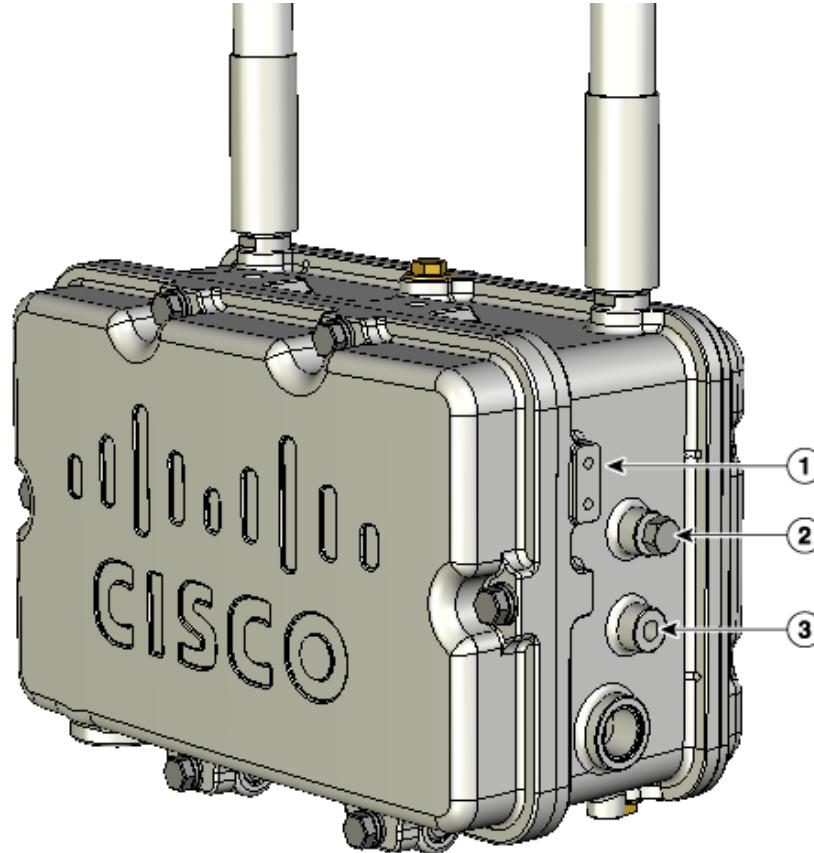


Note If necessary, use suitable screw anchors and an exterior-grade plywood backboard to mount the access point to stucco, cement, or drywall.

REVIEW DRAFT – CISCO CONFIDENTIAL

- Step 3** Screw a M8 x16 bolt in the top support bolt hole on each side the access point (see [Figure 2-7](#)). Do not screw the bolt all the way in; leave approximately a 0.25 in. (0.635 cm) space.

Figure 2-7 Location of Access Point Top Support Bolt Hole

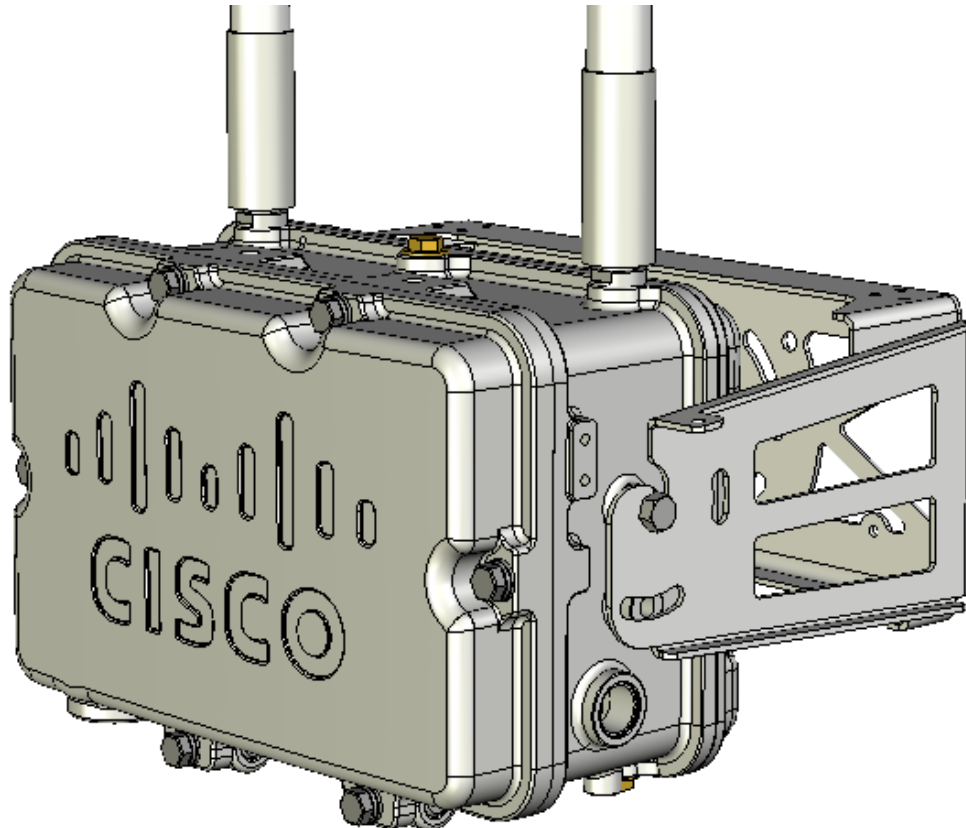


1	Ground lug location	3	Second bolt hole location
2	M8 x16 bolt (supplied with pole mount kit)		

REVIEW DRAFT – CISCO CONFIDENTIAL

- Step 4** Position the two bolts on the access point into the quick mount notches on each side of the mounting bracket (see [Figure 2-8](#)). Ensure that the hinged door is facing out.

Figure 2-8 Access Point Hanging in Mounting Bracket



231405

- 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** (Optional) When using the optional Cisco external omnidirectional antennas, connect them to the access point as shown in [Figure 2-2](#). Hand-tighten the antennas to the access point.



Note Some access point configurations might support two or three of the 2.4-GHz antennas.

- Step 8** Continue with the “[Grounding the Access Point](#)” section on page 2-46 and the “[Powering the Access Point](#)” section on page 2-50.