

Cisco Wireless Mesh Access Points, Design and Deployment Guide, Release 8.0

First Published: 2014-01-22

Last Modified: 2015-02-12

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-31337-01

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 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.

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

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at www.cisco.com/go/offices.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: https://www.cisco.com/c/en/us/about/legal/trademarks.html. Third-party trademarks mentioned 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. (1721R)

© 2014 Cisco Systems, Inc. All rights reserved.



CONTENTS

PREFACE

Preface xi

Audience xii

Organization xii

Conventions xii

Related Documentation xv

Obtaining Documentation and Submitting a Service Request xv

CHAPTER 1

Mesh Network Components 1

Mesh Access Points 1

Licensing for Mesh Access Points on a 5508, 5520 and 8540 Series Cisco Comptroller 1

Access Point Roles 2

Network Access 3

Network Segmentation 3

Cisco Indoor Mesh Access Points 4

Cisco Outdoor Mesh Access Points 5

Battery Backup Module (Optional) 6

Frequency Bands 7

Dynamic Frequency Selection 8

Antennas 9

Antenna Configurations for 1552 11

Client Access Certified Antennas (Third-Party Antennas) 13

Maximum Ratio Combining 13

Cisco 1500 Hazardous Location Certification 16

Cisco Wireless LAN Controllers 18

Cisco Prime Infrastructure 18

Architecture 18

Control and Provisioning of Wireless Access Points 18
CAPWAP Discovery on a Mesh Network 18
Dynamic MTU Detection 19
XML Configuration File 19
Adaptive Wireless Path Protocol 20
Traffic Flow 21
Mesh Neighbors, Parents, and Children 22

CHAPTER 2 **Mesh Deployment Modes 25**
Wireless Mesh Network 25
Wireless Backhaul 25
Universal Access 26
Point-to-Multipoint Wireless Bridging 26
Point-to-Point Wireless Bridging 26
Configuring Mesh Range (CLI) 27

CHAPTER 3 **Design Considerations 29**
Wireless Mesh Constraints 29
Wireless Backhaul Data Rate 29
ClientLink Technology 33
Configuring ClientLink (CLI) 34
Commands Related to ClientLink 36
Controller Planning 36

CHAPTER 4 **Site Preparation and Planning 39**
Site Survey 39
Pre-Survey Checklist 39
Outdoor Site Survey 40
Determining a Line of Sight 40
Weather 41
Fresnel Zone 41
Fresnel Zone Size in Wireless Mesh Deployments 42
Hidden Nodes Interference 42
Preferred Parent Selection 44

Preferred Parent Selection Criteria 44
Configuring a Preferred Parent 44
Related Commands 45
Co-Channel Interference 46
Wireless Mesh Network Coverage Considerations 46
Cell Planning and Distance 47
Assumptions for the Cisco Range Calculator 57
Collocating Mesh Access Points 59
Special Considerations for Indoor Mesh Networks 60
Wireless Propagation Characteristics 62
CleanAir 62
CleanAir AP Modes of Operation 63
Pseudo MAC (PMAC) and Merging 63
Event Driven Radio Resource Management and Persistence Device Avoidance 64
CleanAir Access Point Deployment Recommendations 65
CleanAir Advisor 66
Enabling CleanAir 66
Licensing 66
Wireless Mesh Mobility Groups 67
Multiple Controllers 67
Increasing Mesh Availability 67
Multiple RAPs 68
Indoor Mesh Interoperability with Outdoor Mesh 69

CHAPTER 5 **Overview** 71
Enhanced Feature Set Access Points 72
Adding Mesh Access Points to the Mesh Network 73
Adding MAC Addresses of Mesh Access Points to MAC Filter 74
Adding the MAC Address of the Mesh Access Point to the Controller Filter List (GUI) 74
Adding the MAC Address of the Mesh Access Point to the Controller Filter List (CLI) 75
Defining Mesh Access Point Role 75
General Notes about MAP and RAP Association With The Controller 75
Configuring the AP Role (GUI) 76
Configuring the AP Role (CLI) 76

Configuring Multiple Controllers Using DHCP 43 and DHCP 60 77
Backup Controllers 78
Configuring Backup Controllers (GUI) 78
Configuring Backup Controllers (CLI) 80
Configuring External Authentication and Authorization Using a RADIUS Server 82
Configuring RADIUS Servers 83
Enabling External Authentication of Mesh Access Points (GUI) 83
Enable External Authentication of Mesh Access Points (CLI) 85
View Security Statistics (CLI) 85
Mesh PSK Key Provisioning 85
Wireless Mesh Components Supported 86
Feature Configuration Step-by-Step 86
Mesh PSK GUI Configuration 87
Mesh PSK Provisioning with Controllers In Mobility Group 92
CLI Commands for PSK Provisioning 93
Configuring Global Mesh Parameters 93
Configuring Global Mesh Parameters (GUI) 93
Configuring Global Mesh Parameters (CLI) 97
Viewing Global Mesh Parameter Settings (CLI) 98
Mesh Backhaul at 5 and 2.4 Ghz in Release 8.2 99
Backhaul Client Access 104
Configuring Backhaul Client Access (GUI) 105
Configuring Backhaul Client Access (CLI) 105
Configuring Local Mesh Parameters 106
Configuring Wireless Backhaul Data Rate 106
Configuring Ethernet Bridging 108
Enabling Ethernet Bridging (GUI) 109
Configuring Native VLAN (GUI) 110
Configuring Native VLAN (CLI) 111
Configuring Bridge Group Names 111
Configuring Bridge Group Names (CLI) 112
Verifying Bridge Group Names (GUI) 112
Configuring Power and Channel Settings 112
Configuring Power and Channel Settings (GUI) 112

Configuring Antenna Gain 113
Configuring Antenna Gain (GUI) 113
Configuring Antenna Gain (CLI) 113
Configuring Dynamic Channel Assignment 113
Configuring Radio Resource Management on a Bridge Mode Access Point 116
Configuring Advanced Features 117
Configuring Ethernet VLAN Tagging 117
Ethernet Port Notes 118
VLAN Registration 119
Enabling Ethernet VLAN Tagging (GUI) 121
Configuring Ethernet VLAN Tagging (CLI) 122
Viewing Ethernet VLAN Tagging Configuration Details (CLI) 123
Workgroup Bridge Interoperability with Mesh Infrastructure 123
Configuring Workgroup Bridges 124
Guidelines for Configuration 127
Configuration Example 128
WGB Association Check 129
Link Test Result 131
WGB Wired/Wireless Client 132
Client Roaming 133
WGB Roaming Guidelines 133
Configuration Example 134
Troubleshooting Tips 134
Configuring Voice Parameters in Indoor Mesh Networks 135
Call Admission Control 135
Quality of Service and Differentiated Services Code Point Marking 135
Guidelines For Using Voice on the Mesh Network 140
Voice Call Support in a Mesh Network 141
Enabling Mesh Multicast Containment for Video 142
Viewing the Voice Details for Mesh Networks (CLI) 143
Enabling Multicast on the Mesh Network (CLI) 147
IGMP Snooping 147
Locally Significant Certificates for Mesh APs 148
Guidelines for Configuration 149

Differences Between LSCs for Mesh APs and Normal APs 149
Certificate Verification Process in LSC AP 149
Getting Certificates for LSC Feature 150
Configuring a Locally Significant Certificate (CLI) 151
LSC only MAP Authentication using wild card MAC 152
LSC-Related Commands 153
Controller GUI Security Settings 155
Deployment Guidelines 156
Configuring Antenna Band Mode 156
Information About Configuring Antenna Band Modes 156
Configuring Antenna Band Mode (GUI) 157
Configuring Antenna Band Mode (CLI) 157
Configuring Daisy Chaining on Cisco Aironet 1530 Series Access Points 158
Information About Daisy Chaining the Cisco Aironet 1530 Series Access Points 158
Configuring Daisy Chaining (GUI) 161
Configuring Daisy Chaining (CLI) 162
Configuring a Daisy-Chain 162
Configuring Mesh Convergence 164
Information About Mesh Convergence 164
Restrictions on Mesh Convergence 164
Configuring Mesh Convergence (CLI) 165
Switching Between LWAPP and Autonomous Images (AP CLI) 165

CHAPTER 6 **Checking the Health of the Network** 167
Show Mesh Commands 167
Viewing General Mesh Network Details 167
Viewing Mesh Access Point Details 169
Viewing Global Mesh Parameter Settings 170
Viewing Bridge Group Settings 171
Viewing VLAN Tagging Settings 171
Viewing DFS Details 171
Viewing Security Settings and Statistics 172
Viewing GPS Status 172
Viewing Mesh Statistics for a Mesh Access Point 173

Viewing Mesh Statistics for a Mesh Access Point (GUI) 173
Viewing Mesh Statistics for an Mesh Access Point (CLI) 178
Viewing Neighbor Statistics for a Mesh Access Point 179
Viewing Neighbor Statistics for a Mesh Access Point (GUI) 179
Viewing the Neighbor Statistics for a Mesh Access Point (CLI) 180

CHAPTER 7 **Troubleshooting Mesh Access Points** 183
Installation and Connections 183
Debug Commands 184
Remote Debug Commands 184
AP Console Access 185
Cable Modem Serial Port Access From an AP 185
Configuration 186
Mesh Access Point CLI Commands 188
Mesh Access Point Debug Commands 191
Defining Mesh Access Point Role 191
Backhaul Algorithm 191
Passive Beaconing (Anti-Stranding) 192
Dynamic Frequency Selection 193
DFS in RAP 194
DFS in MAP 194
Preparation in a DFS Environment 196
Monitoring DFS 197
Frequency Planning 197
Good Signal-to-Noise Ratios 198
Access Point Placement 198
Check Packet Error Rate 198
Bridge Group Name Misconfiguration 198
Misconfiguration of the Mesh Access Point IP Address 200
Misconfiguration of DHCP 200
Identifying the Node Exclusion Algorithm 201
Throughput Analysis 203

CHAPTER 8 **Managing Mesh Access Points with Cisco Prime Infrastructure** 205

Adding Campus Maps, Outdoor Areas, and Buildings with Cisco Prime Infrastructure 205
Adding Campus Maps 206
Adding Outdoor Areas 206
Adding a Building to a Campus Map 207
Adding Mesh Access Points to Maps with Cisco Prime Infrastructure 208
Monitoring Mesh Access Points Using Google Earth 209
Launching Google Earth in Cisco Prime Infrastructure 209
Viewing Google Earth Maps 210
Adding Indoor Mesh Access Points to Cisco Prime Infrastructure 212
Managing Mesh Access Points with Cisco Prime Infrastructure 213
Monitoring Mesh Networks Using Maps 213
Monitoring Mesh Link Statistics Using Maps 213
Monitoring Mesh Access Points Using Maps 214
Monitoring Mesh Access Point Neighbors Using Maps 215
Monitoring Mesh Health 216
Viewing Mesh Statistics for a Mesh Access Point 218
Viewing the Mesh Network Hierarchy 223
Using Mesh Filters to Modify Map Display of Maps and Mesh Links 224
Monitoring Workgroup Bridges 225
Multiple VLAN and QoS Support for WGB Wired Clients 227
Workgroup Bridge Guidelines 227
Configuring VLAN and QoS Support (CLI) 228
Workgroup Bridge Output 229
WGB Detail on Controller 229
Troubleshooting Tips 231
Viewing AP Last Reboot Reason 232



Preface

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

Mesh networking employs Cisco Aironet 1500 Series outdoor mesh access points and indoor mesh access points (Cisco Aironet 1040, 1130, 1140, 1240, 1250, 1260, 1600, 1700, 2600, 2700, 3500e, 3500i, 3600e, 3600i, and 3700 series access points) along with the Cisco Wireless LAN Controller, and Cisco Prime Infrastructure to provide scalable, central management, and mobility between indoor and outdoor deployments. Control and Provisioning of Wireless Access Points (CAPWAP) protocol manages the connection of mesh access points to the network.

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

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

- Cisco Aironet 1570 (1572) series outdoor mesh access points
- Cisco Aironet 1550 (1552) series outdoor mesh access points
- Cisco Aironet 1530 series outdoor mesh access points
- Cisco Aironet 1530 series outdoor mesh access points
- Cisco Aironet 1040, 1140, 1260, 1600, 1700, 2600, 2700, 3500e, 3500i, 3600e, 3600i, and 3700 series indoor mesh access points
- Mesh features in Cisco Wireless LAN Controller
- Mesh features in Cisco Prime Infrastructure

This chapter contains the following sections:

- Audience, on page xii
- Organization, on page xii
- Conventions, on page xii
- Related Documentation, on page xv
- Obtaining Documentation and Submitting a Service Request, on page xv

Audience

This document is for experienced network administrators who design and deploy mesh networks and configure and maintain Cisco mesh access points and Cisco wireless LAN controllers.

Organization

This guide is organized into these chapters:

Chapter Title	Description
Mesh Network Components	This chapter describes the components of a mesh network.
Mesh Deployment Modes	This chapter describes the various deployment modes of mesh access points.
Design Considerations	This chapter describes the design considerations involved in a mesh network.
Air Time Fairness in Mesh Deployments rel 8.4	This chapter describes the air time fairness in mesh deployments.
Site Preparation and Planning	This chapter describes the implementation details and configuration examples.
Connecting the Cisco 1500 Series Mesh Access Points to the Network	This chapter describes the procedures involved in connecting mesh access points to a network and configuring the mesh access points.
Checking the Health of the Network	This chapter describes the commands to enter to check the health of a mesh network.
Troubleshooting	This chapter describes the troubleshooting information.
Managing Mesh Access Points with Cisco Prime Infrastructure	This chapter describes information about managing access points with Cisco Prime Infrastructure.

Conventions

This document uses the following conventions:

Convention	Indication
bold font	Commands and keywords and user-entered text appear in **bold** font.
italic font	Document titles, new or emphasized terms, and arguments for which you supply values are in *italic* font.
[ ]	Elements in square brackets are optional.
{x | y | z }	Required alternative keywords are grouped in braces and separated by vertical bars.
[x | y | z]	Optional alternative keywords are grouped in brackets and separated by vertical bars.

Convention	Indication
string	A nonquoted set of characters. Do not use quotation marks around the string or the string will include the quotation marks.
`courier` font	Terminal sessions and information the system displays appear in `courier` font.
<>	Nonprinting characters such as passwords are in angle brackets.
[]	Default responses to system prompts are in square brackets.
!, #	An exclamation point (!) or a pound sign (#) at the beginning of a line of code indicates a comment line.



Note Means reader take note.



Tip Means the following information will help you solve a problem.



Caution Means reader be careful. In this situation, you might perform an action that could result in equipment damage or loss of data.



Warning 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. (To see translations of the warnings that appear in this publication, refer to the appendix "Translated Safety Warnings.")

Warning Title	Description
Waarschuwing	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 standaard maatregelen om ongelukken te voorkomen. (Voor vertalingen van de waarschuwingen die in deze publicatie verschijnen, kunt u het aanhangsel "Translated Safety Warnings" (Vertalingen van veiligheidsvoorschriften) raadplegen.)
Varoitus	Tämä varoitusmerkki merkitsee vaaraa. Olet tilanteessa, joka voi johtaa ruumiinvammaan. Ennen kuin työskentelet minkään laitteiston parissa, ota selvää sähkökytkentöihin liittyvistä vaaroista ja tavanomaisista onnettomuuksien ehkäisykeinoista. (Tässä julkaisussa esiintyvien varoitusten käännökset löydät liitteestä "Translated Safety Warnings" (käännetyt turvallisuutta koskevat varoitukset).)

Warning Title	Description
Attention	Ce symbole d'avertissement indique un danger. Vous vous trouvez dans une situation pouvant entraîner des blessures. Avant d'accéder à cet équipement, soyez conscient des dangers posés par les circuits électriques et familiarisez-vous avec les procédures courantes de prévention des accidents. Pour obtenir les traductions des mises en garde figurant dans cette publication, veuillez consulter l'annexe intitulée « Translated Safety Warnings » (Traduction des avis de sécurité).
Warnung	Dieses Warnsymbol bedeutet Gefahr. Sie befinden sich in einer Situation, die zu einer Körperverletzung führen könnte. Bevor Sie mit der Arbeit an irgendeinem Gerät beginnen, seien Sie sich der mit elektrischen Stromkreisen verbundenen Gefahren und der Standardpraktiken zur Vermeidung von Unfällen bewußt. (Übersetzungen der in dieser Veröffentlichung enthaltenen Warnhinweise finden Sie im Anhang mit dem Titel "Translated Safety Warnings" (Übersetzung der Warnhinweise).)
Avvertenza	Questo simbolo di avvertenza indica un pericolo. Si è in una situazione che può causare infortuni. Prima di lavorare su qualsiasi apparecchiatura, occorre conoscere i pericoli relativi ai circuiti elettrici ed essere al corrente delle pratiche standard per la prevenzione di incidenti. La traduzione delle avvertenze riportate in questa pubblicazione si trova nell'appendice, "Translated Safety Warnings" (Traduzione delle avvertenze di sicurezza).
Advarsel	Dette varselsymbolet betyr fare. Du befinner deg i en situasjon som kan føre til personskade. Før du utfører arbeid på utstyr, må du være oppmerksom på de faremomentene som elektriske kretser innebærer, samt gjøre deg kjent med vanlig praksis når det gjelder å unngå ulykker. (Hvis du vil se oversettelser av de advarslene som finnes i denne publikasjonen, kan du se i vedlegget "Translated Safety Warnings" [Oversatte sikkerhetsadvarsler].)
Aviso	Este símbolo de aviso indica perigo. Encontra-se numa situação que lhe poderá causar danos fisicos. Antes de começar a trabalhar com qualquer equipamento, familiarize-se com os perigos relacionados com circuitos eléctricos, e com quaisquer práticas comuns que possam prevenir possíveis acidentes. (Para ver as traduções dos avisos que constam desta publicação, consulte o apêndice "Translated Safety Warnings" - "Traduções dos Avisos de Segurança").
¡Advertencia!	Este símbolo de aviso significa peligro. Existe riesgo para su integridad física. Antes de manipular cualquier equipo, considerar los riesgos que entraña la corriente eléctrica y familiarizarse con los procedimientos estándar de prevención de accidentes. (Para ver traducciones de las advertencias que aparecen en esta publicación, consultar el apéndice titulado "Translated Safety Warnings.")
Varning	Denna varningssymbol 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 vanligt förfarande för att förebygga skador. (Se förklaringar av de varningar som förekommer i denna publikation i appendix "Translated Safety Warnings" [Översatta säkerhetsvarningar].)

Related Documentation

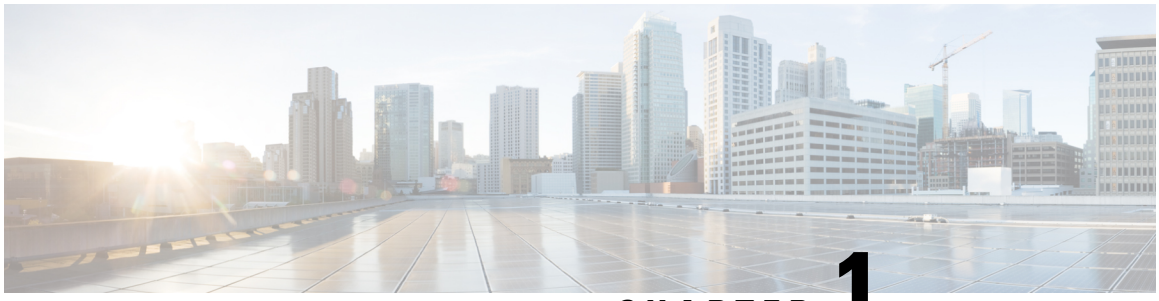
These documents provide complete information about the Cisco Unified Wireless Network solution:

- *Cisco Wireless LAN Controller Configuration Guide*
- *Cisco Wireless LAN Controller Command Reference*
- *Cisco Prime Infrastructure Configuration Guide*
- *Release Notes for Cisco Wireless LAN Controllers and Lightweight Access Points*

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, submitting a service request, and gathering additional information, see the monthly *What's New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation, at:

Subscribe to the *What's New in Cisco Product Documentation* as a Really Simple Syndication (RSS) feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service and Cisco currently supports RSS version 2.0.



CHAPTER 1

Mesh Network Components

This chapter describes the mesh network components.

The Cisco wireless mesh network has four core components:

- Cisco Aironet 15X0 series mesh access points

Note Cisco Aironet 1520 series mesh access points are not supported because of their End-of-Life status.

- Cisco Wireless LAN Controller (hereafter referred to as **controller**)
- Cisco Prime Infrastructure
- Mesh software architecture

This chapter contains the following sections:

- Mesh Access Points, on page 1
- Cisco Wireless LAN Controllers, on page 18
- Cisco Prime Infrastructure, on page 18
- Architecture, on page 18

Mesh Access Points

Licensing for Mesh Access Points on a 5508, 5520 and 8540 Series Cisco Comptroller

To use both mesh and non-mesh access points with a Cisco 5500 and 8500 Series Controller, only the base license is required from the 7.0 release and later releases. For more information about obtaining and installing licenses, see the *Cisco Wireless LAN Controller Configuration Guide* at http://www.cisco.com/en/US/products/ps10315/products_installation_and_configuration_guides_list.html.

Access Point Roles

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

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



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

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

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

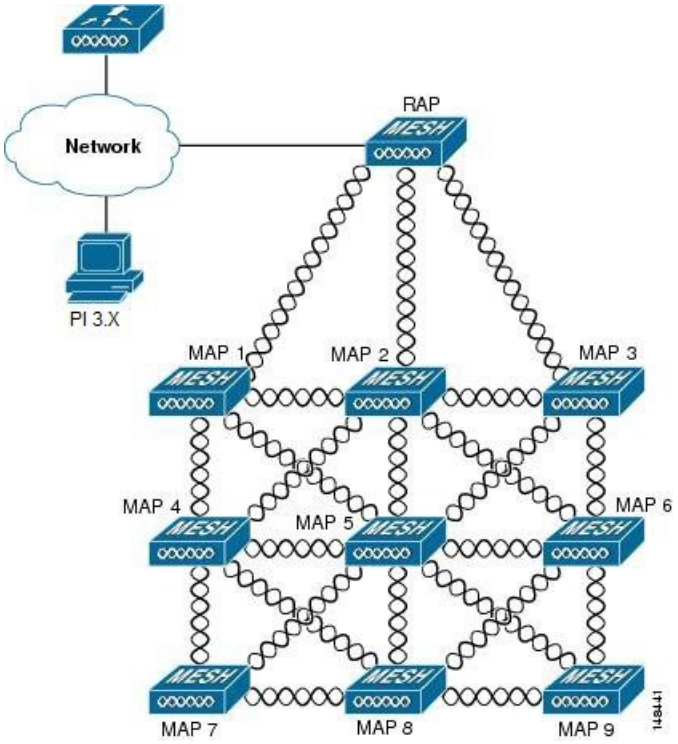
Bridge mode access points support CleanAir in mesh backhaul and provides only the interference device report (IDR) and Air Quality Index (AQI)reports.



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

Figure 1: Simple Mesh Network Hierarchy

This figure shows the relationship between RAPs and MAPs in a mesh network.



Network Access

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

- Wireless LAN client traffic
- MAP Ethernet port traffic

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

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

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

Network Segmentation

Membership to the wireless LAN mesh network for mesh access points is controlled by the bridge group names (BGNs). Mesh access points can be placed in similar bridge groups to manage membership or provide network segmentation.

Cisco Indoor Mesh Access Points

The following access point platforms are supported in this release:

- Cisco Aironet 1600 Series Access Points
- Cisco Aironet 1700 Series Access Points
- Cisco Aironet 2600 Series Access Points
- Cisco Aironet 2700 Series Access Points
- Cisco Aironet 3500 Series Access Points
- Cisco Aironet 3600 Series Access Points
- Cisco Aironet 3700 Series Access Points
- Cisco Aironet 1530 Series Access Points
- Cisco Aironet 1550 Series Access Points
- Cisco Aironet 1560 Series Access Points
- Cisco Aironet 1570 Series Access Points
- Cisco Industrial Wireless 3700 Series Access Points



Note In 8.4 release the following AP s will be supported.

- 1700
- 2700
- 3700



Note For more information about controller software support for access points, see the *Cisco Wireless Solutions Software Compatibility Matrix* at http://www.cisco.com/en/US/docs/wireless/controller/5500/tech_notes/Wireless_Software_Compatibility_Matrix.html.

Enterprise 11n/ac mesh is an enhancement added to the CUWN feature to work with the 802.11n/ac access points. Enterprise 11ac mesh features are compatible with non-802.11ac mesh but adds higher backhaul and client access speeds. The 802.11ac indoor access points are two-radio Wi-Fi infrastructure devices for select indoor deployments. One radio can be used for local (client) access for the access point and the other radio can be configured for wireless backhaul. If Universal Backhaul Access is enabled, the 5-GHz and 2.4–GHz radios in rel 8.2 can be used for local (client) access as well as a backhaul. Enterprise 11ac mesh supports P2P, P2MP, and mesh types of architectures.

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

You have a choice of ordering indoor access points directly into the bridge mode, so that these access points can be used directly as mesh access points. If you have these access points in a local mode (non-mesh), then you have to connect these access points to the controller and change the AP mode to the bridge mode (mesh). This scenario can become cumbersome particularly if the volume of the access points being deployed is large and if the access points are already deployed in the local mode for a traditional non-mesh wireless coverage.

The Cisco indoor mesh access points are equipped with the following two simultaneously operating radios:

- From rel 8.2 2.4 GHz radio used for data backhaul and client access if UBA is enable
- 5-GHz radio used for data backhaul and client access if Universal Backhaul Access is enabled

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

Cisco Outdoor Mesh Access Points

Cisco outdoor mesh access points comprise of the Cisco Aironet 1500 series access points. The 1500 series includes 1572 11ac outdoor access points, 1552 and 1532 11n outdoor mesh access points, and the 1560 11ac wave 2 series.1532 dual radio mesh access points .

Cisco 1500 series mesh access points are the core components of the wireless mesh deployment. AP1500s are configured by both the controller (GUI and CLI) and Cisco Prime Infrastructure. Communication between outdoor mesh access points (MAPs and RAPs) is over the 802.11a/n/ac radio backhaul. Client traffic is generally transmitted over the 802.11b/g/n radio (802.11a/n/ac can also be configured to accept client traffic).

The mesh access point can also operate as a relay node for other access points not directly connected to a wired network. Intelligent wireless routing is provided by the Adaptive Wireless Path Protocol (AWPP). This Cisco protocol enables each mesh access point to identify its neighbors and intelligently choose the optimal path to the wired network by calculating the cost of each path in terms9 of the signal strength and the number of hops required to get to a controller.

Uplinks support includes Gigabit Ethernet (1000BASE-T) and a small form-factor (SFP) slot that can be plugged for a fiber or cable modem interface. Both single mode and multimode SFPs up to 1000BASE-BX are supported. The cable modem can be DOCSIS 2.0 or DOCSIS/EuroDOCSIS 3.0 depending upon the type of mesh access point.

AP1550s are available in a hazardous location hardware enclosure. When configured, the AP1500 complies with safety standards for Class I, Division 2, Zone 2 hazardous locations.

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

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

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

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

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

Note For complete details and specification of all models of outdoor Mesh AP please visit this links below:

- http://www.cisco.com/c/en/us/products/collateral/wireless/aironet-1530-series/data_sheet_c78-728356.html
- http://www.cisco.com/c/en/us/products/collateral/wireless/aironet-1550-series/data_sheet_c78-641373.html
- http://www.cisco.com/c/en/us/td/docs/wireless/access_point/1550/installation/guide/1550hig/1550_ch1.html
- http://www.cisco.com/c/en/us/td/docs/wireless/access_point/1550/installation/guide/1550hig/1550_ch1.html
- http://wwwin.cisco.com/c/cec/prods-industry/selling-en/products/wireless/ap.html
- http://www.cisco.com/c/en/us/support/wireless/aironet-1572eac-outdoor-access-point/model.html
- http://www.cisco.com/c/dam/en/us/products/collateral/wireless/aironet-1570-series/datasheet-c78-732348.pdf

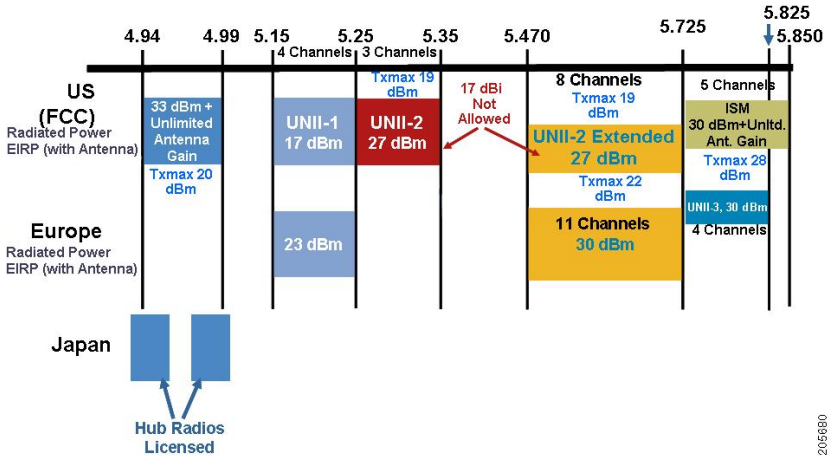
Battery Backup Module (Optional)

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

Frequency Bands

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

Figure 2: Frequency Bands Supported By 802.11a Radios on AP1500s



The 5-GHz band is a conglomerate of three bands in the USA: 5.150 to 5.250 (UNII-1), 5.250 to 5.350 (UNII-2), 5.470 to 5.725 (UNII-2 Extended), and 5.725 to 5.850 (ISM). UNII-1 and the UNII-2 bands are contiguous and are treated by 802.11a as being a continuous swath of spectrum 200-MHz wide, more than twice the size of the 2.4-GHz band (see Table 1: Frequency Band , on page 7).

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

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

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

Table 1: Frequency Band

Frequency Band Terms	Description	Model Support
UNII-1[1]	Regulations for UNII devices operating in the 5.15- to 5.25-GHz frequency band. Indoor operation and outdoor APs using the -B reg domain.	All 11n/ac Indoor APs and the 1572.
UNII-2	Regulations for UNII devices operating in the 5.25- to 5.35-GHz frequency band. DFS and TPC are mandatory in this band.	All 11n/ac indoor APs, 1532, 1552,1562 and 1572.

Frequency Band Terms	Description	Model Support
UNII-2 Extended	Regulations for UNII-2 devices operating in the 5.470 to 5.725 frequency band.	All 11n/ac indoor APs, 1532, 1552,1562 and 1572.
ISM[2]	Regulations for UNII devices operating in the 5.725 to 5.850 GHz frequency band.	All 11n/ac indoor APs, 1532, 1552,1562 and 1572.

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

Note For regulatory information, see http://www.cisco.com/en/US/prod/collateral/wireless/ps5679/ps5861/product_data_sheet0900aecd80537b6a.html.

Dynamic Frequency Selection

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

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

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

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

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

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

Figure 3: DFS and TPC Band Requirements



Antennas

Overview

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

- Directional
- Omnidirectional

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

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

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

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

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

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

Antenna Options

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

Table 2: External 2.4- and 5-GHz Antennas, on page 10 lists the supported external 2.4- and 5-GHz antennas for AP1500s.

Table 2: External 2.4- and 5-GHz Antennas

Part Number	Model	Gain (dBi)
AIR-ANT2450V-N	2.4-GHz compact omnidirectional[3]	5
AIR-ANT-2455V-N	2.4-GHz compact omnidirectional	5.5
AIR-ANT2480V-N	2.4-GHz omnidirectional	8.0
AIR-ANT5180V-N	5-GHz compact omnidirectional[4]	8.0
AIR-ANT5140V-N	5-GHz right-angle omnidirectional	4.0
AIR-ANT5114P-N	5-GHz patch2	14.0
AIR-ANT2547V-N	2.4 – 5-GHz dual-band omnidirectional	4 dBi at 2.4 GHz and 7 dBi at 5 GHz

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

See the *Cisco Aironet Antenna and Accessories Reference Guide* on Cisco antennas and accessories at http://www.cisco.com/en/US/prod/collateral/wireless/ps7183/ps469/product_data_sheet09186a008008883b.html

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

Table 3: Horizontal and Vertical Beamwidth for Cisco Antennas, on page 11 summarizes the horizontal and vertical beamwidth for Cisco antennas.

Table 3: Horizontal and Vertical Beamwidth for Cisco Antennas

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

N-Connectors

All external antennas are equipped with male N-connectors.

AP1552 E/H have three N-connectors to connect dual-band antennas.

AP1552 C/I have no N-connectors as they come with inbuilt antennas.

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

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

Antenna Configurations for 1552

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

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

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

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

Figure 4: 1552C Cable Mount

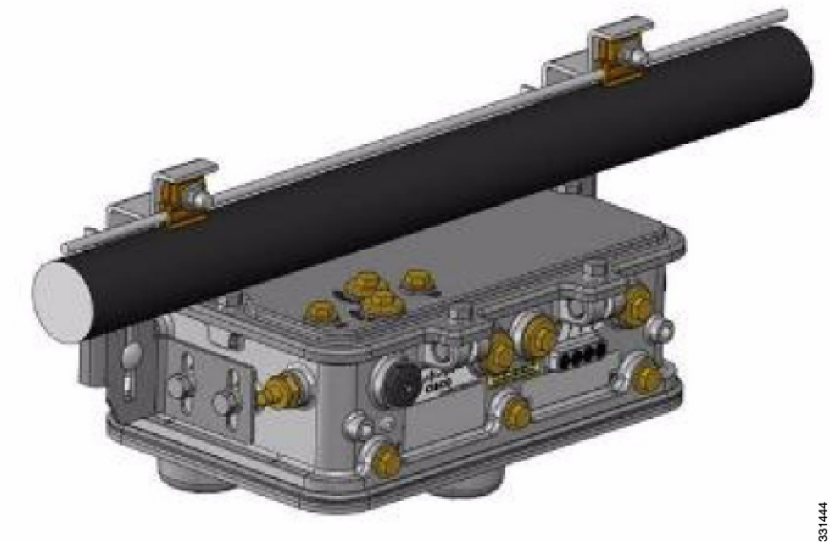
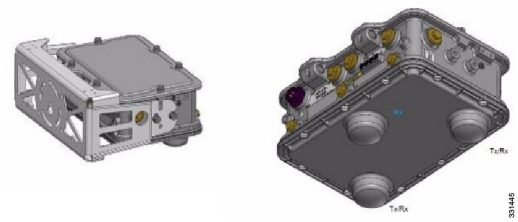


Figure 5: 1552I Pole/Wall Mount



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

Figure 6: 1552 E Pole/Wall Mount

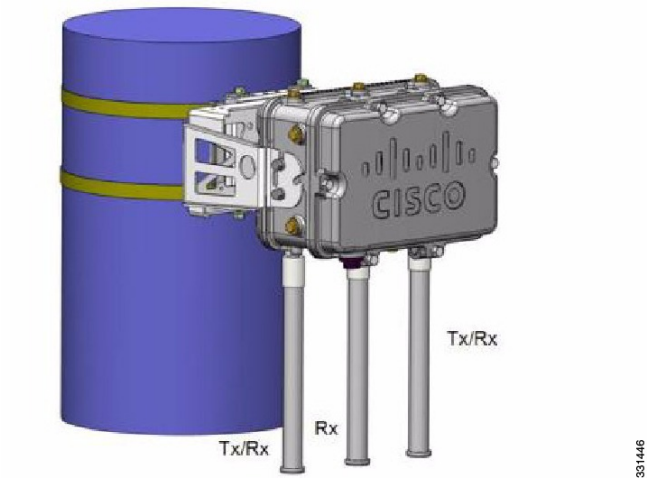
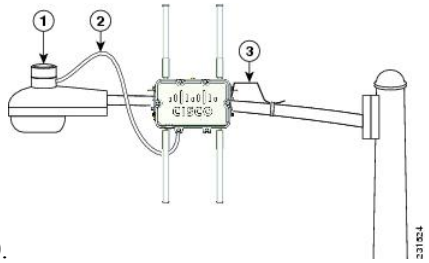


Figure 7: Outdoor Pole-top Installation of a Mesh Access Point

This figure shows one of the recommended installations of an outdoor



AP1500.

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

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

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

Client Access Certified Antennas (Third-Party Antennas)

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

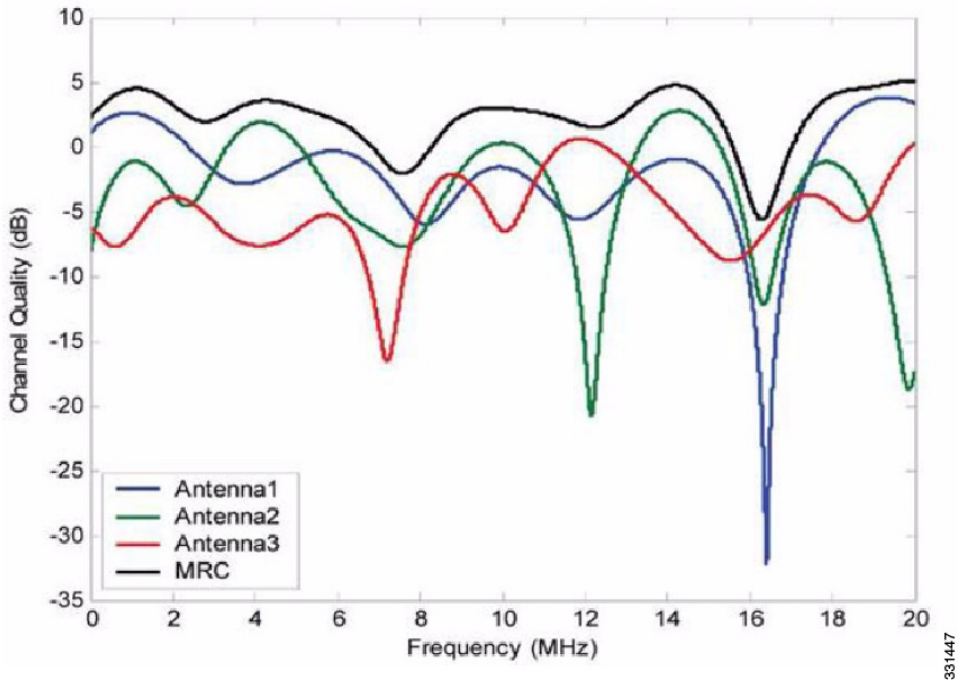
- Cisco does not track or maintain information about the quality, performance, or reliability of the noncertified antennas and cables.
- RF connectivity and compliance is the customer’s responsibility.
- Compliance is only guaranteed with Cisco antennas or antennas that are of the same design and gain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

Maximum Ratio Combining

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

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

Figure 8: Reinforcement of Received Signal via MRC Algorithm



For the 1550 Series

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

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

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

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

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

Table 4: AP1552 11a/g MRC Gain, on page 15 and Table 5: AP1552 11n MRC Gain, on page 15 list the MRC gain for the AP1552 11a/g and AP1552 11n respectively.

Table 4: AP1552 11a/g MRC Gain

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

Table 5: AP1552 11n MRC Gain

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

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

Cisco 1500 Hazardous Location Certification

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

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

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

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

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

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

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

Class 1, Division 1/Zone 1 is for environments with full-time ignitable concentrations of flammable gases, vapors, or liquids. To meet the requirements of the Div 1 > Div 2 and Zone 1 > Zone 2 locations, we recommend a TerraWave Solutions CSA certified protective Wi-Fi enclosure (see Table 6: TerraWave Enclosures, on page 17).

Table 6: TerraWave Enclosures

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

For more information about the TerraWave enclosures, see http://www.tessco.com/yts/partner/manufacturer_list/vendors/terrawave/pdf/terrawavehazardouesenclosuresjan08.pdf

Table 7: Hardware Features at a Glance, on page 17 lists the hardware features across different AP1500 models at a glance.

Table 7: Hardware Features at a Glance

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

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

Cisco Wireless LAN Controllers

The wireless mesh solution is supported on Cisco 2500, 3504, 5500, and 8500 Series Wireless LAN Controllers.

For more information about the Cisco 2500, 5500, and 8500 Series Wireless LAN Controllers, see http://www.cisco.com/en/US/products/ps6302/Products_Sub_Category_Home.html.

Cisco Prime Infrastructure

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

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

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

Architecture

Control and Provisioning of Wireless Access Points

Control and provisioning of wireless access points (CAPWAP) is the provisioning and control protocol used by the controller to manage access points (mesh and nonmesh) in the network.

CAPWAP Discovery on a Mesh Network

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

1. A mesh access point establishes a link before starting CAPWAP discovery, whereas a non mesh access point starts CAPWAP discovery using a static IP for the mesh access point, if any.
2. The mesh access point initiates CAPWAP discovery using a static IP for the mesh access point on the Layer 3 network or searches the network for its assigned primary, secondary, or tertiary controller. A maximum of 10 attempts are made to connect.

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

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

Dynamic MTU Detection

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

XML Configuration File

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

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

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

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

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

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

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

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

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

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

show invalid-config

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

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

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

Adaptive Wireless Path Protocol

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

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

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

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

AWPP automatically determines the best path back to the CAPWAP controller by calculating the cost of each path in terms of the signal strength and number of hops. After the path is established, AWPP continuously monitors conditions and changes routes to reflect changes in conditions. AWPP also performs a smoothing

function to signal condition information to ensure that the ephemeral nature of RF environments does not impact network stability.

Traffic Flow

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

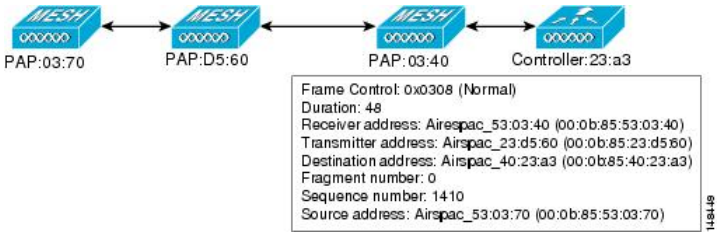
1. Overlay CAPWAP traffic that flows within a standard CAPWAP access point deployment; that is, CAPWAP traffic between the CAPWAP access point and the CAPWAP controller.
2. Wireless mesh data frame flow.
3. AWPP exchanges.

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

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

Figure 9: Wireless Mesh Frame, on page 21 shows an example of this type of framing. The source address of the frame is MAP:03:70, the destination address of this frame is the controller (the mesh network is operating in Layer 2 mode), the transmitter address is MAP:D5:60, and the receiver address is RAP:03:40.

Figure 9: Wireless Mesh Frame

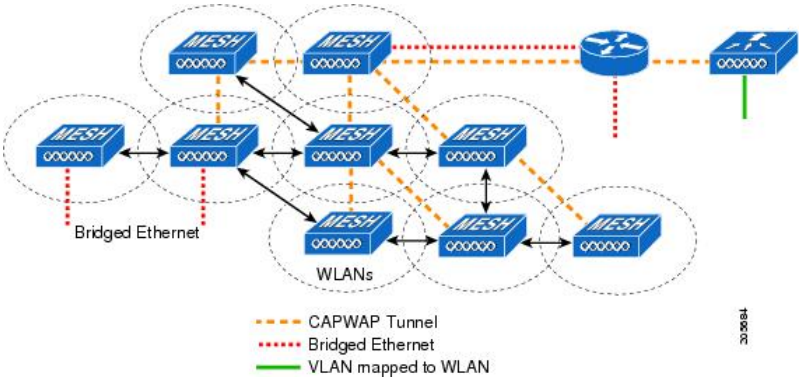


As this frame is sent, the transmitter and receiver addresses change on a hop-by-hop basis. AWPP is used to determine the receiver address at each hop. The transmitter address is known because it is the current mesh access point. The source and destination addresses are the same over the entire path.

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

Each mesh access point within the mesh forms an CAPWAP session with a controller. WLAN traffic is encapsulated inside CAPWAP and is mapped to a VLAN interface on the controller. Bridged Ethernet traffic can be passed from each Ethernet interface on the mesh network and does not have to be mapped to an interface on the controller (see Figure 10: Logical Bridge and WLAN Mapping, on page 22).

Figure 10: Logical Bridge and WLAN Mapping

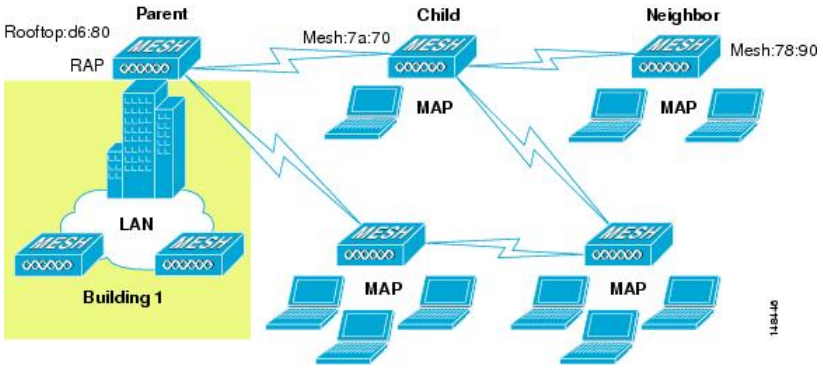


Mesh Neighbors, Parents, and Children

Relationships among mesh access points are as a parent, child, or neighbor (see Figure 11: Parent, Child, and Neighbor Access Points, on page 22).

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

Figure 11: Parent, Child, and Neighbor Access Points



Criteria to Choose the Best Parent

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

- A list of channels with neighbors is generated by passive scanning in the *scan* state, which is a subset of all backhaul channels.
- The channels with neighbors are sought by actively scanning in the *seek* state and the backhaul channel is changed to the channel with the best neighbor.

- The parent is set to the best neighbor and the parent-child handshake is completed in the *seek* state.
- Parent maintenance and optimization occurs in the *maintain* state.

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

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

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

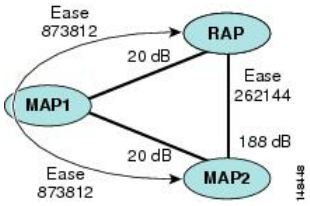
A parent mesh access point provides the best path back to a RAP. AWPP uses ease to determine the best path. Ease can be considered the opposite of cost, and the preferred path is the path with the higher ease.

Ease Calculation

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

Figure 12: Parent Path Selection, on page 23 shows the parent path selection where MAP2 prefers the path through MAP1 because the adjusted ease value (436906) though this path is greater then the ease value (262144) of the direct path from MAP2 to RAP.

Figure 12: Parent Path Selection



Parent Decision

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

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

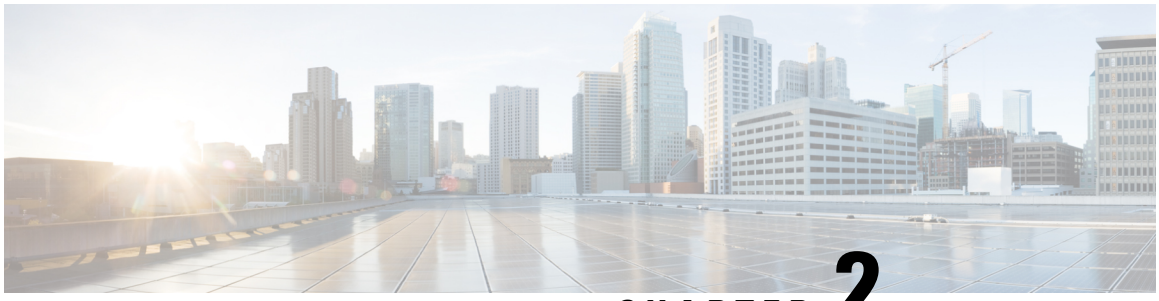
SNR Smoothing

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

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

Loop Prevention

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



CHAPTER 2

Mesh Deployment Modes

This chapter describes the mesh deployment modes and contains the following sections:

- Wireless Mesh Network, on page 25
- Wireless Backhaul, on page 25
- Point-to-Multipoint Wireless Bridging, on page 26
- Point-to-Point Wireless Bridging, on page 26

Wireless Mesh Network

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

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

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

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

Note CAPWAP over CAPWAP is not supported. AP in local mode connected on the RAP or MAP ethernet port is not a supported configuration.

Wireless Backhaul

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

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

Universal Access

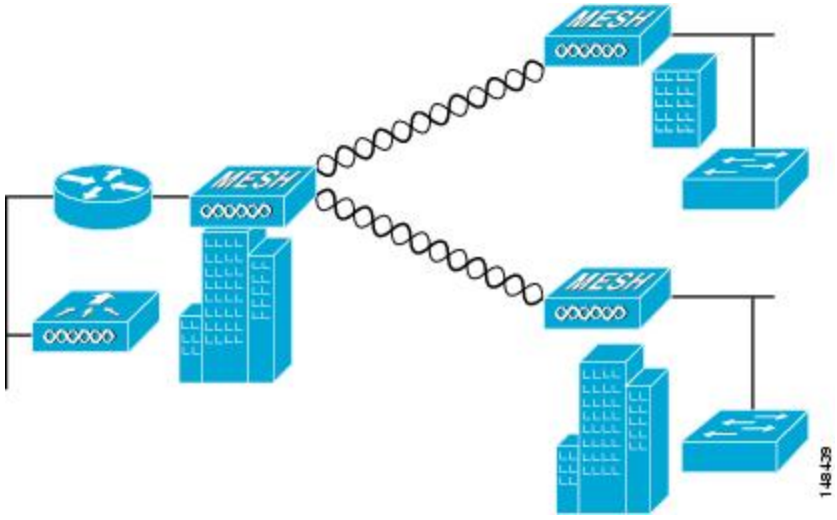
You can configure the backhaul on mesh access points to accept client traffic over its 802.11a radio. This feature is identified as Backhaul Client Access in the controller GUI (Monitor > Wireless). When this feature is disabled, backhaul traffic is transmitted only over the 802.11a or 802.11a/n radio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

Point-to-Multipoint Wireless Bridging

In the point-to-multipoint bridging scenario, a RAP acting as a root bridge connects multiple MAPs as non-root bridges with their associated wired LANs. By default, this feature is disabled for all MAPs. If Ethernet bridging is used, you must enable it on the controller for the respective MAP and for the RAP.

Figure 13: Point-to-Multipoint Bridging Example

This figure shows a simple deployment with one RAP and two MAPs, but this configuration is fundamentally a wireless mesh with no WLAN clients. Client access can still be provided with Ethernet bridging enabled, although if bridging between buildings, MAP coverage from a high rooftop might not be suitable for client access.

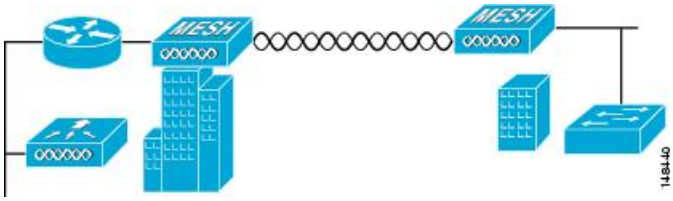


Point-to-Point Wireless Bridging

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

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

Figure 14: Point-to-Point Bridging Example



For security reasons the Ethernet port on the MAPs is disabled by default. It can be enabled only by configuring Ethernet bridging on the Root and the respective MAPs. To enable Ethernet bridging using the controller GUI, choose **Wireless** > **All APs** > **Details for the AP** page, click the **Mesh** tab, and then select the **Ethernet Bridging** check box.

Note The overall throughput of backhaul radio decreases by half for each hop of a mesh tree. When the Ethernet-bridged clients are used in MAPs and heavy traffic is passed, it may result in a high throughput consumption, which may cause the downlink MAPs to disassociate from the network due to throughput starvation.

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

When you want to use the mesh nodes as bridges.

When you want to connect Ethernet devices such as a video camera on the MAP using its Ethernet port.

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

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

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

Range: 150 to 132,000 feet

Configuring Mesh Range (CLI)

Procedure

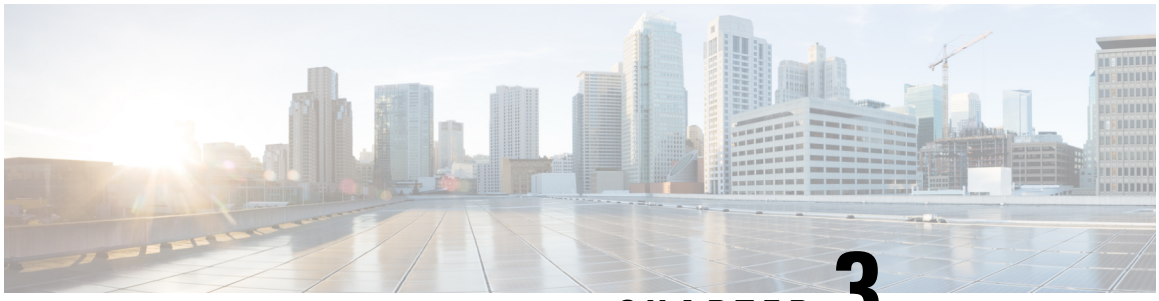
- To configure the distance between the nodes doing the bridging, enter the **config mesh range** command.

  APs reboot after you specify the range.

Note To estimate the range and the AP density, you can use range calculators that are available at:

Range Calculator for all access points: http://173.37.206.125/aspnet_client/system_web/2_0_50727/wng_coverage_capacity_calculator_v2.0_html/wng_coverage_capacity_calculator_v2.0.htm

- To view the mesh range, enter the **show mesh config** command.



CHAPTER 3

Design Considerations

This chapter describes important design considerations and provides an example of a wireless mesh design.

Each outdoor wireless mesh deployment is unique, and each environment has its own challenges with available locations, obstructions, and available network infrastructure. Design requirements driven by expected users, traffic, and availability needs are also major design criteria. This chapter contains the following sections:

- Wireless Mesh Constraints, on page 29
- ClientLink Technology, on page 33
- Controller Planning, on page 36

Wireless Mesh Constraints

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

Wireless Backhaul Data Rate

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

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

Data rates also affect the RF coverage and network performance. Lower data rates, for example 6 Mbps, can extend farther from the access point than can higher data rates, for example 1300 Mbps. As a result, the data rate affects cell coverage and consequently the number of access points required. Different data rates are achieved by sending a more redundant signal on the wireless link, allowing data to be easily recovered from noise. The number of symbols sent out for a packet at the 1-Mbps data rate is higher than the number of symbols used for the same packet at 11 Mbps. Therefore, sending data at the lower bit rates takes more time than sending the equivalent data at a higher bit rate, resulting in reduced throughput.

A lower bit rate might allow a greater distance between MAPs, but there are likely to be gaps in the WLAN client coverage, and the capacity of the backhaul network is reduced. An increased bit rate for the backhaul

network either requires more MAPs or results in a reduced SNR between MAPs, limiting mesh reliability and interconnection.

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

The required minimum LinkSNR for backhaul links per data rate is shown in Table 8: Backhaul Data Rates and Minimum LinkSNR Requirements, on page 30.

Table 8: Backhaul Data Rates and Minimum LinkSNR Requirements

802.11a Data Rate (Mbps)	Minimum Required LinkSNR (dB)
54	31
48	29
36	26
24	22
18	18
12	16
9	15
6	14

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

  Table 9: Backhaul Data Rates and Minimum LinkSNR Requirements for 802.11n, on page 30 summarizes the calculation by data rate.

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

  Minimum Required LinkSNR Calculations by Data Rate

Table 9: Backhaul Data Rates and Minimum LinkSNR Requirements for 802.11n

802.11n Date Rate (Mbps)	Spatial Stream	Minimum Required LinkSNR (dB)
15	1	9.3
30	1	11.3

802.11n Date Rate (Mbps)	Spatial Stream	Minimum Required LinkSNR (dB)
45	1	13.3
60	1	17.3
90	1	21.3
120	1	24.3
135	1	26.3
157.5	1	27.3
30	2	12.3
60	2	14.3
90	2	16.3
120	2	20.3
180	2	24.3
240	2	27.3
270	2	29.3
300	2	30.3

- If we take into account the effect of MRC for calculating Minimum Required Link SNR. Table 10: Required LinkSNR Calculations for 802.11a/g, on page 31 shows the required LinkSNR for 802.11a/g (2.4 GHz and 5 GHz) for AP1552 and 1522 with 3 Rx antennas (MRC gain).

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

Table 10: Required LinkSNR Calculations for 802.11a/g

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

If we consider only 802.11n rates, then Table 11: Requirements for LinkSNR with AP1552 for 2.4 and 5 GHz, on page 32 shows LinkSNR requirements with AP1552 for 2.4 and 5 GHz.

Table 11: Requirements for LinkSNR with AP1552 for 2.4 and 5 GHz

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

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

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

  The number of hops is recommended to be limited to three or four primarily to maintain sufficient backhaul throughput, because each mesh access point uses the same radio for transmission and reception of backhaul traffic, which means that throughput is approximately halved over every hop. For example, the maximum throughput for 24 Mbps is approximately 14 Mbps for the first hop, 9 Mbps for the second hop, and 4 Mbps for the third hop.

- Number of MAPs per RAP.

  There is no current software limitation on how many MAPs per RAP you can configure. However, it is suggested that you limit the number to 20 MAPs per RAP.

- Number of controllers
  - The number of controllers per mobility group is limited to 72.

- Number of mesh access points supported per controller.

ClientLink Technology

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

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

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

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

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

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

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

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

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

Although ClientLink is applied to legacy OFDM portions of packets, which refers to 11a/g rates (not 11b) for both indoor and outdoor 802.11n access points, there is one difference between ClientLink for indoor 11n and ClientLink for outdoor 11n. For indoor 11n access points, SW limits the affected rates to 24, 36, 48, and 54 Mbps. This is done to avoid clients sticking to a far away AP in an indoor environment. SW also does not allow ClientLink to work for those rates for 11n clients because the throughput gain is so minimal. However, there is a demonstrable gain for pure legacy clients. For outdoor 11n access points, we do need more coverage. Thus, three more additional legacy data rates lower than 24 Mbps have been added. ClientLink for outdoors is applicable to legacy data rates of 6, 9, 12, 18, 24, 36, 48, and 54 Mbps.



Note ClientLink is enabled by default.

Configuring ClientLink (CLI)

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

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

config {**802.11a** | **802.11b**} **disable network**

Step 2 Globally enable or disable beamforming on your 802.11a or 802.11g network by entering this command:

config {**802.11a** | **802.11b**} **beamforming global** {**enable** | **disable**}

The default value is disabled.

Note After you enable beamforming on the network, it is automatically enabled for all the radios applicable to that network type.

Step 3 Override the global configuration and enable or disable beamforming for a specific access point by entering this command:

config {**802.11a** | **802.11b**} **beamforming ap** *Cisco_AP* {**enable** | **disable**}

The default value is disabled if beamforming is disabled on the network and enabled if beamforming is enabled on the network.

Step 4 Reenable the network by entering this command:

config {**802.11a** | **802.11b**} **enable network**

Step 5 Save your changes by entering this command:

save config

Step 6 See the beamforming status for your network by entering this command:

show {**802.11a** | **802.11b**}

Information similar to the following appears:

```
802.11a Network.................................. Enabled
11nSupport....................................... Enabled
802.11a Low Band.......................... Enabled
802.11a Mid Band.......................... Enabled
802.11a High Band......................... Enabled
...
Pico-Cell-V2 Status.............................. Disabled
TI Threshold..................................... -50
Legacy Tx Beamforming setting................. Enabled
```

Step 7 See the beamforming status for a specific access point by entering this command:

show ap config {**802.11a** | **802.11b**} *Cisco_AP*

Information similar to the following appears:

```
Cisco AP Identifier.............................. 14
Cisco AP Name.................................... 1250-1
Country code..................................... US  - United States
Regulatory Domain allowed by Country............. 802.11bg:-A     802.11a:-A
...
Phy OFDM parameters
Configuration ............................. AUTOMATIC
Current Channel ........................... 149
Extension Channel ......................... NONE
Channel Width.............................. 20 Mhz
Allowed Channel List....................... 36,40,44,48,52,56,60,64,100,
.......................................... 104,108,112,116,132,136,140,
.......................................... 149,153,157,161,165
TI Threshold .............................. -50
```

```
Legacy Tx Beamforming Configuration ....... CUSTOMIZED
Legacy Tx Beamforming ..................... ENABLED
```

Commands Related to ClientLink

The following commands are related to ClientLink:

- The following commands are to be entered in the AP console:
  - To check the status of Beamforming on the AP, enter the **show controller d0/d1** command.
  - To find a client in the AP rbf table, enter the **show interface dot110** command.
  - To check the Beamforming rate assigned on the AP, enter the **debug d0 trace print rates** command.
- The following commands on the AP console are used for troubleshooting:
  - To show that ClientLink is enabled on a radio, enter the **show controllers | inc Beam** command.

    The output is displayed as follows:

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

  - To show that ClientLink is Beamforming to a particular client, enter the **show interface dot11radio 1 lbf rbf** command.

    The output is displayed as follows:

    ```
    RBF Table:
    Index      Client MAC      Reserved      Valid    Tx BF     Aging
     1       0040.96BA.45A0      Yes          Yes      Yes       No
    ```

Controller Planning

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

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

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

- Number of mesh access points (RAPs and MAPs) supported per controller. See Table 12: Mesh Access Point Support by Controller Model , on page 37.

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

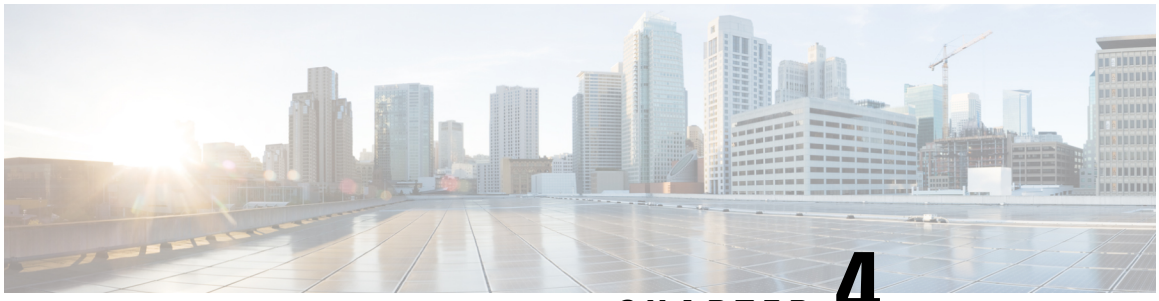
Table 12: Mesh Access Point Support by Controller Model

Controller Model	Local AP Support (nonmesh)[5]	Maximum Possible Mesh AP Support
5508[6]	500	500
2504[7]	50	50
WiSM2	500	500

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



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



CHAPTER 4

Site Preparation and Planning

This chapter describes the site preparation and planning for your mesh network and contains the following sections:

- Site Survey, on page 39
- Wireless Mesh Network Coverage Considerations, on page 46
- Indoor Mesh Interoperability with Outdoor Mesh, on page 69

Site Survey

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

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

Pre-Survey Checklist

Before attempting a site survey, determine the following:

- How long is your wireless link?
- Do you have a clear line of sight?
- What is the minimum acceptable data rate within which the link runs?
- Is this a point-to-point or point-to-multipoint link?
- Do you have the correct antenna?
- Can the access point installation area support the weight of the access point?
- Do you have access to both of the mesh site locations?
- Do you have the proper permits, if required?

- Do you have a partner? Never attempt to survey or work alone on a roof or tower.
- Have you configured the 1500 series before you go onsite? It is always easier to resolve configuration or device problems first.
- Do you have the proper tools and equipment to complete your task?



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

Outdoor Site Survey

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

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

Design recommendations for mesh links are as follows:

- MAP deployment cannot exceed 35 feet in height above the street.
- MAPs are deployed with antennas pointed down toward the ground.
- Typical 5-GHz RAP-to-MAP distances are 1000 to 4000 feet.
- RAP locations are typically towers or tall buildings.
- Typical 5-GHz MAP-to-MAP distances are 500 to 1000 feet.
- MAP locations are typically short building tops or streetlights.
- Typical 2.4-GHz MAP-to-client distances are 500 to 1000 feet (depends upon the type of access point).
- Clients are typically laptops, Smart Phones, Tablets, and CPEs. Most of the clients operate in the 2.4-GHz band.

Determining a Line of Sight

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

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

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

Weather

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

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

Fresnel Zone

A Fresnel zone is an imaginary ellipse around the visual line of sight between the transmitter and receiver. As radio signals travel through free space to their intended target, they could encounter an obstruction in the Fresnel area, degrading the signal. Best performance and range are attained when there is no obstruction of this Fresnel area. Fresnel zone, free space loss, antenna gain, cable loss, data rate, link distance, transmitter power, receiver sensitivity, and other variables play a role in determining how far your mesh link goes. Links can still occur as long as 60 percent to 70 percent of the Fresnel area is unobstructed, as illustrated in Figure 15: Point-to-Point Link Fresnel Zone, on page 41.

Figure 15: Point-to-Point Link Fresnel Zone

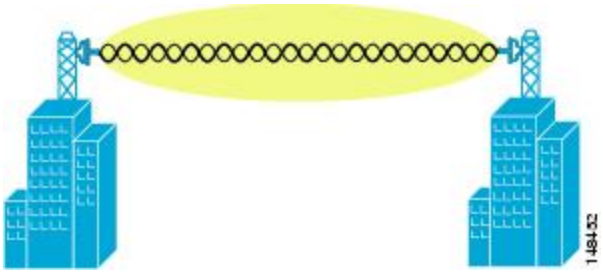
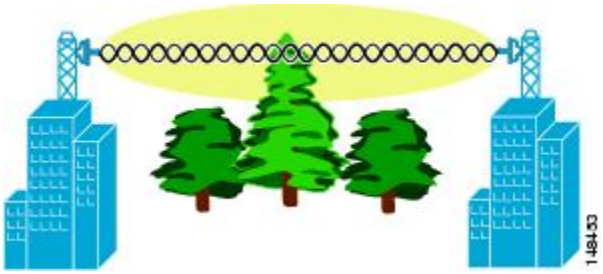


Figure 16: Typical Obstructions in a Fresnel Zone, on page 41 illustrates an obstructed Fresnel zone.

Figure 16: Typical Obstructions in a Fresnel Zone



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

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

where

F1 = the first Fresnel zone radius in feet

D = total path length in miles

F = frequency (GHz)

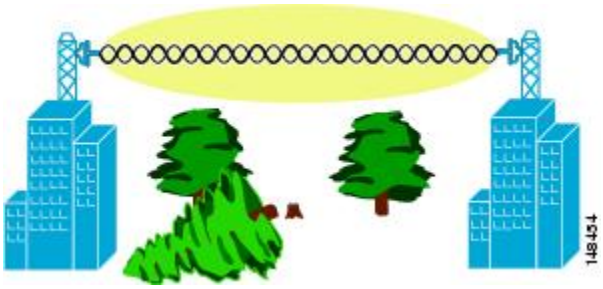
Normally, 60 percent of the first Fresnel zone clearance is recommended, so the above formula for 60 percent Fresnel zone clearance can be expressed as follows:

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

These calculations are based on a flat terrain.

Figure 17: Removing Obstructions in a Fresnel Zone, on page 42 shows the removal of an obstruction in the Fresnel zone of the wireless signal.

Figure 17: Removing Obstructions in a Fresnel Zone



Fresnel Zone Size in Wireless Mesh Deployments

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

Hidden Nodes Interference

The mesh backhaul uses the same 802.11a channel for all nodes in that mesh, which can introduce hidden nodes into the WLAN backhaul environment.

Figure 18: Hidden Nodes

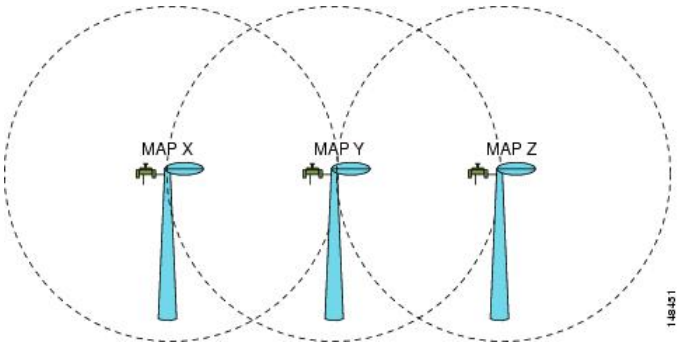


Figure 18: Hidden Nodes, on page 43 shows the following three MAPs:

- MAP X
- MAP Y
- MAP Z

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

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

Both the hidden node problem and the exposed node problem are inherent to wireless mesh networks because mesh access points share the same backhaul channel. Because these two problems can affect the overall network performance, the Cisco mesh solution seeks to mitigate these two problems as much as possible. For example, the AP1500s have at least two radios: one for backhaul access on a 5-GHz channel and the other for 2.4-GHz client access. In addition, the radio resource management (RRM) feature, which operates on the 2.4-GHz radio, enables cell breathing and automatic channel change, which can effectively decrease the collision domains in a mesh network.

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

Preferred Parent Selection

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

Preferred Parent Selection Criteria

The child AP selects the preferred parent based on the following criteria:

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

Configuring a Preferred Parent

To configure a preferred parent, enter the following command:

```
(Cisco Controller) > config mesh parent preferred AP_name MAC
```

where:

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



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

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

```
(Cisco Controller) > config mesh parent preferred MAP1SB 00:24:13:0f:92:0f
```

To configure a preferred parent using the controller GUI, follow these steps:

1. Choose **Wireless** > **Access Points** > **AP_NAME** > **Mesh**.

2. Enter the MAC address of the preferred parent in the **Preferred Parent** text box.



Note To clear the Preferred Parent value, enter **none** in the Preferred Parent Text box.

3. Click **Apply**.



Note When the preferred parent is entered, no other mesh configurations can be made at the same time. You must apply the changes and wait for 90 seconds before other mesh changes can be made.

Related Commands

The following commands are related to preferred parent selection:

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

```
(Cisco Controller) > config mesh parent preferred AP_name none
```

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

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

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

```
(Cisco Controller) > show ap config general MAP1

Cisco AP Identifier.............................. 9
Cisco AP Name.................................... MAP1
Country code..................................... US - United States
Regulatory Domain allowed by Country............. 802.11bg:-A 802.11a:-A
AP Country code.................................. US - United States
AP Regulatory Domain............................. 802.11bg:-A 802.11a:-A
Switch Port Number .............................. 1
MAC Address...................................... 12:12:12:12:12:12
IP Address Configuration......................... DHCP
IP Address....................................... 209.165.200.225
IP NetMask....................................... 255.255.255.224
CAPWAP Path MTU.................................. 1485
Domain.......................................
Name Server...................................
Telnet State..................................... Disabled
Ssh State........................................ Disabled
Cisco AP Location................................ default location
Cisco AP Group Name.............................. default-group
Primary Cisco Switch Name........................ 4404
Primary Cisco Switch IP Address.................. 209.165.200.230
Secondary Cisco Switch Name.....................
Secondary Cisco Switch IP Address................ Not Configured
Tertiary Cisco Switch Name....................... 4404
```

```
Tertiary Cisco Switch IP Address..... 3.3.3.3
Administrative State ..... ADMIN_ENABLED
Operation State ..... REGISTERED
Mirroring Mode ..... Disabled
AP Mode ..... Local
Public Safety ..... Global: Disabled, Local: Disabled
AP subMode ..... WIPS
Remote AP Debug ..... Disabled
S/W  Version ..... 5.1.0.0
Boot  Version ..... 12.4.10.0
Mini IOS Version ..... 0.0.0.0
Stats Reporting Period ..... 180
LED State..... Enabled
PoE Pre-Standard Switch..... Enabled
PoE Power Injector MAC Addr..... Disabled
Power Type/Mode..... PoE/Low Power (degraded mode)
Number Of Slots..... 2
AP Model..... AIR-LAP1252AG-A-K9
IOS Version..... 12.4(10:0)
Reset Button..... Enabled
AP Serial Number..... serial_number
AP Certificate Type..... Manufacture Installed
Management Frame Protection Validation..... Enabled (Global MFP Disabled)
AP User Mode..... CUSTOMIZED
AP username..... maria
AP Dot1x User Mode..... Not Configured
AP Dot1x username..... Not Configured
Cisco AP system logging host..... 255.255.255.255
AP Up Time..... 4 days, 06 h 17 m 22 s
AP LWAPP Up Time..... 4 days, 06 h 15 m 00 s
Join Date and Time..... Mon Mar 3 06:19:47 2008

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

Co-Channel Interference

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

Wireless Mesh Network Coverage Considerations

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

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

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

Cell Planning and Distance

For the Cisco 1500 Series Access Points

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

We recommend the following values for cell planning and distance in nonvoice networks:

- RAP-to-MAP ratio—Recommended maximum ratio is 20 MAPs per RAP.
- AP-to-AP distance—A spacing of no more than of 2000 feet (609.6 meters) between each mesh access point is recommended. When you extend the mesh network on the backhaul (no client access), use a cell radius of 1000 feet (304.8 meters).
- Hop count—Three to four hops.
    - One square mile in feet (52802), is nine cells and you can cover one square mile with approximately three or four hops (see Figure 19: Cell Radius of 1000 Feet and Access Point Placement for Nonvoice Mesh Networks, on page 47 and Figure 20: Path Loss Exponent 2.3 to 2.7, on page 48.)
- For 2.4 GHz, the local access cell size radius is 600 feet (182.88 meters). One cell size is around 1.310 x 106, so there are 25 cells per square mile. (See Figure 21: Cell Radius of 600 Feet and Access Point Placement for Nonvoice Mesh Networks, on page 48 and Figure 22: Path Loss Exponent 2.5 to 3.0, on page 49.)

Figure 19: Cell Radius of 1000 Feet and Access Point Placement for Nonvoice Mesh Networks

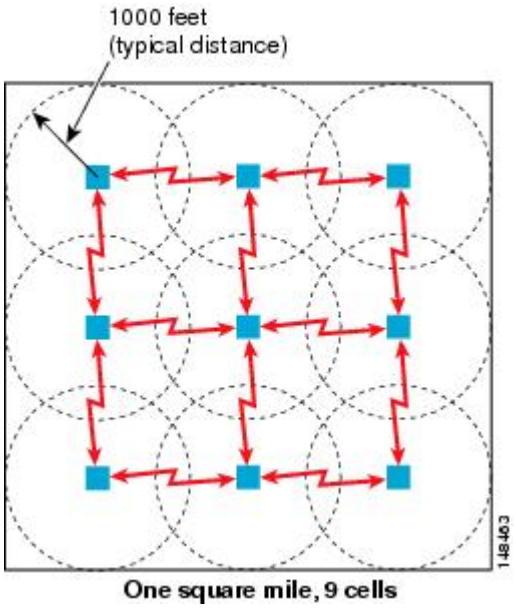


Figure 20: Path Loss Exponent 2.3 to 2.7

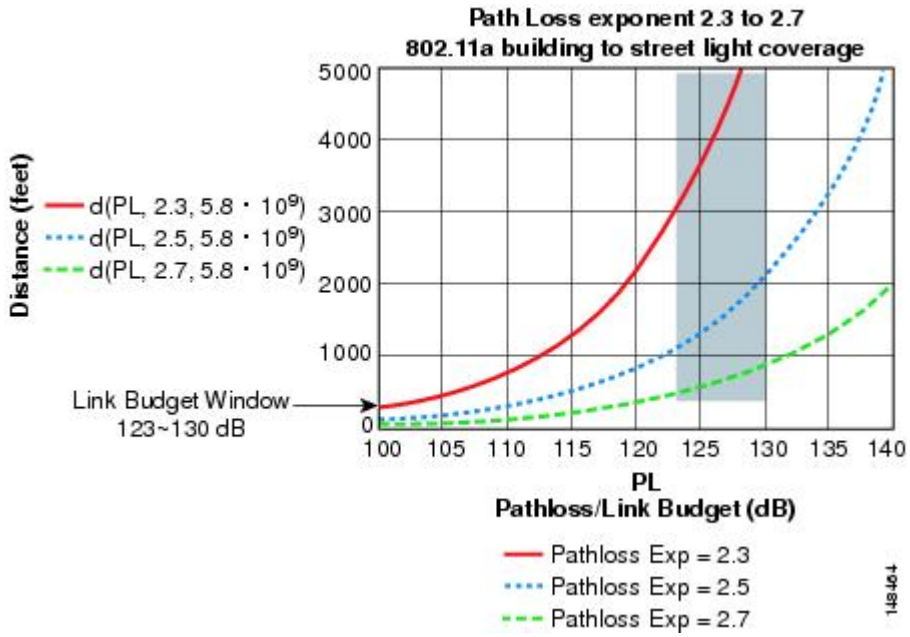


Figure 21: Cell Radius of 600 Feet and Access Point Placement for Nonvoice Mesh Networks

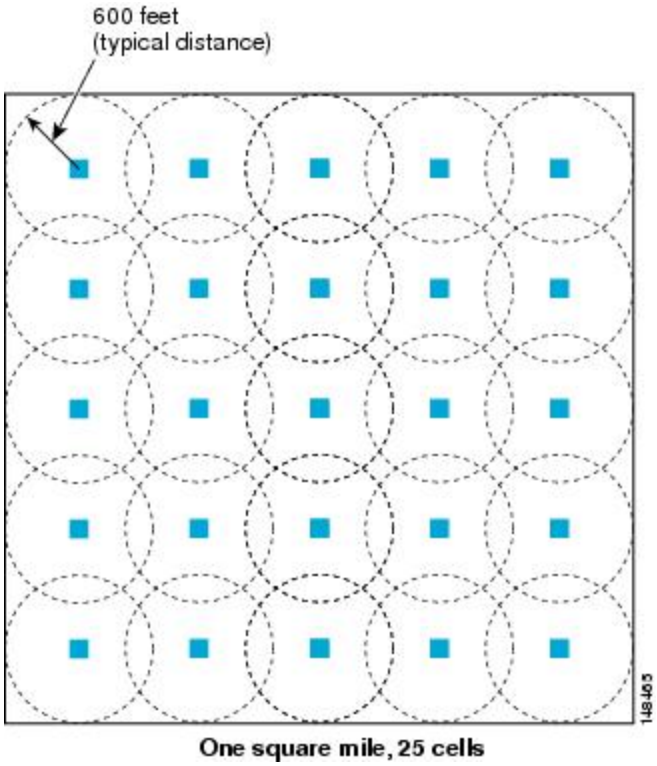
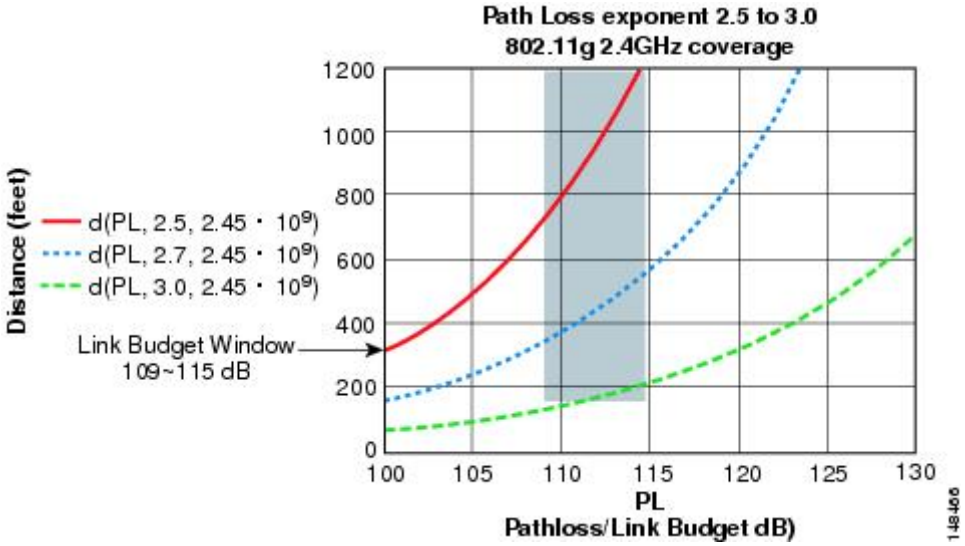


Figure 22: Path Loss Exponent 2.5 to 3.0



For the Cisco 1550 Series Access Points

As seen in the previous section, we recommend a cell radius of 600 feet, and an AP to AP distance of 1200 feet. Normally, an AP to AP distance that is twice the AP to client distance is recommended. That is, if we halve the AP to AP distance, we will get the approximate cell radius.

The AP1550 series offers comparatively better range and capacity as it has the 802.11n functionality. It has advantages of ClientLink (Beamforming) in downstream, better receiver sensitivities because of MRC in upstream, multiple transmitter streams and a few other advantages of 802.11n such as channel combining and so on. The 1552 access points can provide comparatively larger and higher capacity cells.

Note Link budgets are different for different country domains. The discussion in this section takes into account the most widely distributed and large country domains: -A and -E.

Comparison of Link Budgets of AP1572 Series and AP1552 Series in 2.4- and 5-GHz Bands (-A Domain)

See Table 13: Link Budget Comparison for the 2.4-GHz band in -A/-B Domain, on page 49.

Table 13: Link Budget Comparison for the 2.4-GHz band in -A/-B Domain

Parameter	Cisco 1552 (-A domain)	Cisco 1532 (-A Domain)	Cisco 1572 (-B Domain)
Frequency Band	2412 – 2462 MHz	2412 – 2462 MHz	2412 – 2462 MHz
Air Interface	802.11b/g/n	802.11b/g/n	802.11b/g/n
Channel Bandwidth	20 MHz	20 MHz	20 MHz
No. of Tx Spatial Streams	2	3SS for 1532I, 2SS for 1532E	3SS

Parameter	Cisco 1552 (-A domain)	Cisco 1532 (-A Domain)	Cisco 1572 (-B Domain)
PHY Data Rates	Up to 144 Mbps[8]	Up to 216 Mbps with 3SS 144 Mbps for 2SS	Up to 216 Mbps
Tx Power Conducted	28 dBm, Composite[9]	29 dBm	30 dBm
Rx Sensitivity	–94 dBm at 6 Mbps –79 dBm at 54 Mbps –73 dBm at 150 Mbps	–95 dBm at 6 Mbps –75 dBm at 54 Mbps –69 dBm at 216 Mbps	–93 dBm at 6 Mbps –81 dBm at 54 Mbps –76 dBm at 216 Mbps
No. of Receive Channels	3	3	4
Rx Diversity	MRC	MRC	MRC
Antenna Cable loss	0.5 dB, with external antenna	0.5 dB	0.5 dB

[8] 40-MHz channel bonding in 2.4 GHz is not applicable. Therefore, the maximum data rate is 144 Mbps.
[9] Composite power is the power when we have two Tx streams enabled in AP1552.

For the 5-GHz band, see Table 14: Link Budget Comparison for the 5-GHz band in -A/-B Domain, on page 50.

Table 14: Link Budget Comparison for the 5-GHz band in -A/-B Domain

Parameter	Cisco 1552 (-A Domain)	Cisco 1532 (-A Domain)	Cisco 1572 (-B Domain)
Frequency Band	5745 – 5825 MHz	5.280 – 5.320 GHz 5.500 – 5.560 GHz 5.680 – 5.700 GHz 5.745 – 5.825 GHz	5.180 – 5.240 GHz 5.260 – 5.320 GHz 5.500 – 5.560 GHz 5.680 – 5.720 GHz 5.745 – 5.825 GHz
Air Interface	802.11a/n	802.11a/n	802.11a/n/ac
Channel Bandwidth	20 MHz, 40 MHz	20 MHz, 40 MHz	20 MHz, 40 MHz, 80 MHz
No. of Tx Spatial Streams	2	2	3
PHY Data Rates	Up to 300 Mbps	Up to 300 Mbps	Up to 1.3 Gbps
Tx Power Conducted	28 dBm, Composite	27 dBm	30 dBm
Rx Sensitivity	–92 dBm at 6 Mbps –76 dBm at 54 Mbps –72 dBm at 300 Mbps	–92 dBm at 6 Mbps –72 dBm at 54 Mbps –68 dBm at 300 Mbps	–92 dBm at 6 Mbps –80 dBm at 54 Mbps –60 dBm at 1300 Mbps

The 20-MHz channel bonding to form a 40-MHz channel is available in 5 GHz. Therefore, we can go up to a data rate of 300 Mbps.

As discussed in the previous section, Path Loss Exponents (PLE) and Link Budget windows work together. For a full clear path, PLE is 2.0. For AP to AP, there is comparatively more clearance than AP to client. For AP to AP, PLE can be taken as 2.3 because it can be assumed that the height of both APs is about 10 meters, which means a good line of sight (but without Fresnel zone clearance).

For AP to client, PLE should be greater than or equal to 2.5 because the client is only 1 meter high. Therefore, there will be less Fresnel zone clearance. This applies to both the 2.4-GHz and 5-GHz bands.

Let us consider AP to AP link budget in 5 GHz for -A domain because 5 GHz is used as a backhaul for mesh. We can take a legacy data rate of 9 Mbps to estimate the range (see Table 15: AP to AP RF Link Budget, 5.8 GHz: 9 Mbps (-A domain), on page 51).

Note This is the lowest data rate for outdoor 802.11n APs, which carries the Cisco's ClientLink (Beamforming for Legacy clients) advantage. It provides a gain of up to 4 dB in the downlink direction.

Table 15: AP to AP RF Link Budget, 5.8 GHz: 9 Mbps (-A domain)

Parameter	Cisco 1552 I/C	Cisco 1552 E/H
Tx Power Conducted at 9 Mbps, 20 MHz bandwidth	28 dBm, Composite	26 dBm, Composite
Tx Antenna Cable Loss	0 dB	0.5 dB
Tx Antenna Gain	4 dBi (inbuilt antenna)	7 dBI
Tx Beam Forming (BF)	4 dB	4 dB
Tx EIRP	36 dBm	36.5 dBm
Rx Antenna Gain	4 dBi	7 dBI
Rx Antenna Cable Loss	0 dB	0.5 dB
Rx Sensitivity	–91 dBm at 9 Mbps	–91 dBm at 9 Mbps
System Gain	131 dB	134 dB
Fade Margin	9 dB	9 dB
Range between APs (LOS, PLE = 2.3)	829 meters (2722 feet)	1120 meters (3675 feet)

A fade margin of 9 dB is assumed, which is inconsistent with the assumption to calculate the required SNR values in the *Wireless Mesh Constraints* section.

Link Budget Analysis for AP to Client (–A Domain)

This section contains a link budget analysis for the AP to the Client, so that you know how far away a client can go from the AP with a system gain value in each band. In this analysis, the focus is on the system gain

for upstream and downstream. A link should be balanced for upstream and downstream, but it might not happen. Generally, there is a higher antenna gain and higher Tx power available on the AP rather than on the client. But, this can also be opposite in a few regulatory domains because of different EIRP limit requirements. Therefore, the lowest of both upstream and downstream should be taken to calculate the AP to the client distance because that will be the decision factor. For example, if there is a higher downstream gain than upstream, the upstream should be the decision maker for the cell size because the upstream system gain allows only the client to connect to the AP.

The regulatory domain values of Tx EIRP and Rx sensitivities decide whether upstream or downstream has the lower system gain. The cell size should be determined by upstream and not downstream.

Because most of the clients available are 2.4-GHz clients, the focus is on the 2.4-GHz AP to the.

For the AP to client link budget in 2.4 GHz, let us assume a client Tx power of 20 dB and an antenna gain of 0 dBi (see Table 16: Outdoor 11n AP-to-Client, at 2.4 GHz: 9 Mbps Data Rate (–A domain), on page 52). For the –A domain EIRP limit is 36 dBm for 2.4- and 5-GHz bands.

.

Table 16: Outdoor 11n AP-to-Client, at 2.4 GHz: 9 Mbps Data Rate (–A domain)

Parameter	Cisco 1552 I/C		Cisco 1552 E/H		Comments
	DS	US	DS	US	
Tx Power Conducted	28 dBm (AP)	20 dBm (Client)	28 dBm (AP)	20 dBm (Client)	Composite power at 9 Mbps, 20 MHz bandwidth
Tx Antenna Gain	2 dBi (AP)	0 dBi (Client)	4 dBi (AP)	0 dBi (Client)	
Tx Beam Forming (BF)	4 dB (AP)	0 dB (Client)	4 dB (AP)	0 dB (Client)	Legacy Rate ClientLink. Helps only in DS.
Tx EIRP	34 dBm	20 dBm	36 dBm	20 dBm	
Rx Antenna Gain	0 dBi (Client)	2 dBi (AP)	0 dBi (Client)	4 dBi (AP)	
Rx Sensitivity	–90 dBm (Client)	–94 dBm (AP)	–90 dBm (Client)	–94 dBm (AP)	Includes 4.7 dB MRC gain for AP1552
System Gain	124 dB	116 dB	126 dB	118 dB	
Range (AP to Client)		268 meters (881 feet)		323 meters (1058 feet)	LOS, PLE = 2.5

The –A domain AP to client link budget in 2.4 GHz band is limited by upstream. That is, the upstream has lower system gain, and therefore, the decision factor will be upstream.

Cell sizes for AP to Client in 2.4 GHz for different AP1552 models can be decided by picking the lowest of the following two:

- AP to Client distance in the 2.4-GHz band (from Table 16: Outdoor 11n AP-to-Client, at 2.4 GHz: 9 Mbps Data Rate (–A domain), on page 52)
- Half of the distance between AP to AP on the 5-GHz backhaul (from Table 14: Link Budget Comparison for the 5-GHz band in -A/-B Domain, on page 50)

Because most of the clients available are 2.4-GHz clients, we recommend the cell size taking 2.4 GHz values into consideration (see Table 17: Lowest of AP to Client and Half of AP to AP Backhaul Distance, on page 53).

Table 17: Lowest of AP to Client and Half of AP to AP Backhaul Distance

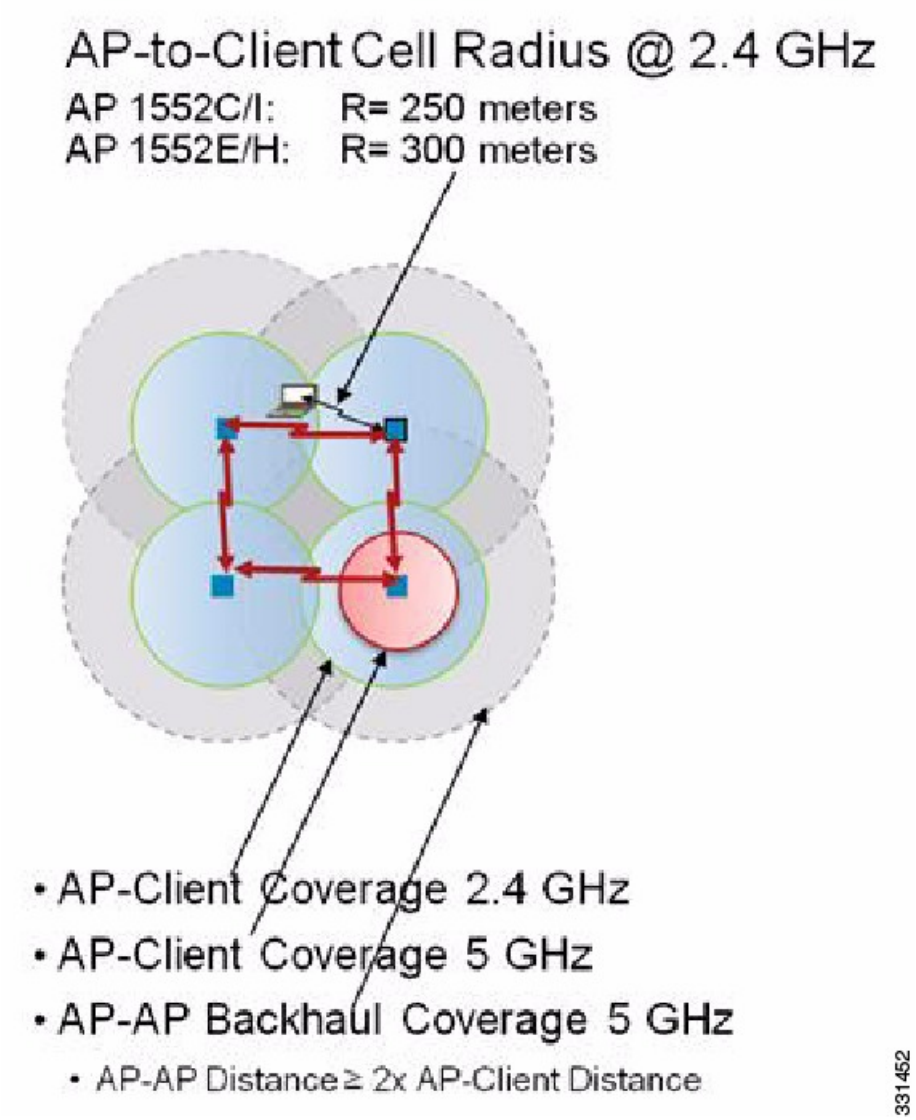
AP Type (-A Domain)	AP to Client 2.4 GHz	Half of AP to AP backhaul Distance in 5 GHz
1552 C/I	250 meters (800 feet)	415 meters (1360 feet)
1552 E/H	300 meters (1000 feet)	560 meters (1840 feet)

For the AP to the AP distance, you can take double the AP to the client distance (see Table 18: Recommendations for Cell Radius, on page 53).

Table 18: Recommendations for Cell Radius

AP Type (-A Domain)	AP to Client	AP to AP
1552 C/I	250 meters (800 feet)	500 meters (1600 feet)
1552 E/H	300 meters (1000 feet)	600 meters (2000 feet)

Figure 23: AP-to-Client Cell Radius at 2.4 GHz



The following assumptions are made:

- Height: APs are at 33 feet (10 meters); Client at 3.3 feet (1 meter)
- Throughput greater than 1 Mbps
- Decreasing AP-to-AP distance improves coverage
- Near LoS. For Less LoS scenarios, you must reduce the distance assumptions
- Flat Terrain Environment

AP Densities result as follows:

- AP1552C and AP1552I: 14 AP/sq. mile = 5.3 AP/sq. km
- AP1552E and AP1552H: 9 AP/sq. mile = 3.5 AP/sq. km

With these recommendations, the likelihood of getting healthy cells is more.

Note For 5-GHz clients, the cell radius is comparatively smaller because higher the frequency, higher is the attenuation. The 2.4-GHz band has almost 13 dB better link budget than 5 GHz.

Comparison of Link Budgets of AP1520 Series and AP1552 Series in 2.4- and 5-GHz Bands (-E Domain)

In the -E Domain, EIRP limits are comparatively much lower. EIRP limit for 2.4 Ghz is 20 dBm and for 5 GHz is 30 dBm.

Let us consider 5 GHz because it is used as a backhaul for mesh. We can take a legacy data rate of 9 Mbps to estimate the range.

Note PLE is 2.3 for backhaul.

AP to AP RF Link Budget, 5.6 GHz: 9 Mbps (-E domain)

Table 19: AP to AP RF Link Budget, 5.6 GHz: 9 Mbps (-E domain)

Parameter	Cisco 1552 I/C	Cisco 1552 E/H
Tx Power Conducted at 9 Mbps, 20 MHz bandwidth	22 dBm, Composite	19 dBm, Composite
Tx Antenna Cable Loss	0 dB	0.5 dB
Tx Antenna Gain	4 dBi (inbuilt antenna)	7 dBI
Tx Beamforming (BF)	4 dB	4 dB
Tx EIRP	30 dBm	30.5 dBm
Rx Antenna Gain	4 dBi	7 dBI
Rx Antenna Cable Loss	0 dB	0.5 dB
Rx Sensitivity	–91 dBm at 9 Mbps	–91 dBm at 9 Mbps
System Gain	125 dB	127 dB
Fade Margin	9 dB	9 dB
Range between APs (LOS, PLE = 2.3)	471 meters (1543 feet)	575 meters (1888 feet)

The AP1552 models with inbuilt antennas (1552C/I) have the same system gain as AP1522s for 5 GHz backhaul giving the AP to AP distance of 1543 feet.

Link Budget Analysis for AP to Client (-E Domain)

This section contains link budget analysis for AP to Client in the 2.4-GHz band. In this analysis, the focus is on the system gain for upstream and downstream. Ideally, the link should be balanced for upstream and

downstream, but practically it may not happen. Therefore, the decision factor for the cell radius will be the lowest of both upstream and downstream.

For AP to client link budget in 2.4 GHz, let us assume a client Tx power of 20 dB and an antenna gain of 0 dBi.

For -E domain, the EIRP limit is 20 dBm for the 2.4-GHz band and 30 dBm for the 5-GHz band.

Table 20: Outdoor 11n AP-to-Client, at 2.4 GHz: 9 Mbps Data Rate (-E domain)

Parameter	Cisco 1552 I/C		Cisco 1552 E/H		Comments
	DS	US	DS	US	
Tx Power Conducted	15 dBm (AP)	20 dBm (Client)	13 dBm (AP)	20 dBm (Client)	Composite power at 9 Mbps, 20 MHz bandwidth
Tx Antenna Gain	2 dBi (AP)	0 dBi (Client)	4 dBi (AP)	0 dBi (Client)	
Tx Beamforming (BF)	3 dB (AP)	0 dB (Client)	3 dB (AP)	0 dB (Client)	Legacy Rate ClientLink. Helps only in DS.
Tx EIRP	20 dBm	20 dBm	20 dBm	20 dBm	
Rx Antenna Gain	0 dBi (Client)	2 dBi (AP)	0 dBi (Client)	4 dBi (AP)	
Rx Sensitivity	–91 dBm (Client)	–94 dBm (AP)	–91 dBm (Client)	–94 dBm (AP)	Includes 4.7 dB MRC gain for AP1552
System Gain	111 dB	116 dB	111 dB	118 dB	
Range (AP to Client)	173 meters (567 feet)		173 meters (567 feet)		LOS, PLE = 2.5 (5 dB fade margin)

The AP to client link budget in the 2.4-GHz band on the -E domain is limited by downstream. Therefore, downstream has a lower system gain. Thus, the decision factor will be downstream.

Cell sizes for AP to Client in 2.4 GHz for different AP1552 models can be decided by picking the lowest of the following two:

- AP to Client distance in 2.4 GHz band (from Table 20: Outdoor 11n AP-to-Client, at 2.4 GHz: 9 Mbps Data Rate (-E domain), on page 56)
- Half of the distance between AP to AP on 5 GHz backhaul (from Table 19: AP to AP RF Link Budget, 5.6 GHz: 9 Mbps (-E domain), on page 55)

Because most of the clients available are 2.4-GHz clients, we recommend the cell size taking 2.4 GHz values into consideration (see Table 21: Lowest of AP to Client and Half of AP to AP Backhaul Distance, on page 57).

Table 21: Lowest of AP to Client and Half of AP to AP Backhaul Distance

AP Type (-E Domain)	AP to Client 2.4 GHz	Half of AP to AP backhaul Distance in 5 GHz
1552 C/I	180 meters (600 feet)	235 meters (770 feet)
1552 E/H	180 meters (600 feet)	288 meters (944 feet)

For AP to AP distance we can take double the AP to Client distance (see Table 22: Recommendations for Cell Radius, on page 57).

Table 22: Recommendations for Cell Radius

AP Type (-E Domain)	AP to Client	AP to AP
1552 C/I	180 meters (600 feet)	360 meters (1200 feet)
1552 E/H	180 meters (600 feet)	360 meters (1200 feet)



Note To estimate the range and the AP density, you can use range calculators that are available at

- Range Calculator for all Cisco access points: http://173.37.206.125/aspnet_client/system_web/2_0_50727/wng_coverage_capacity_calculator_v2.0_html/wng_coverage_capacity_calculator_v2.0.htm.

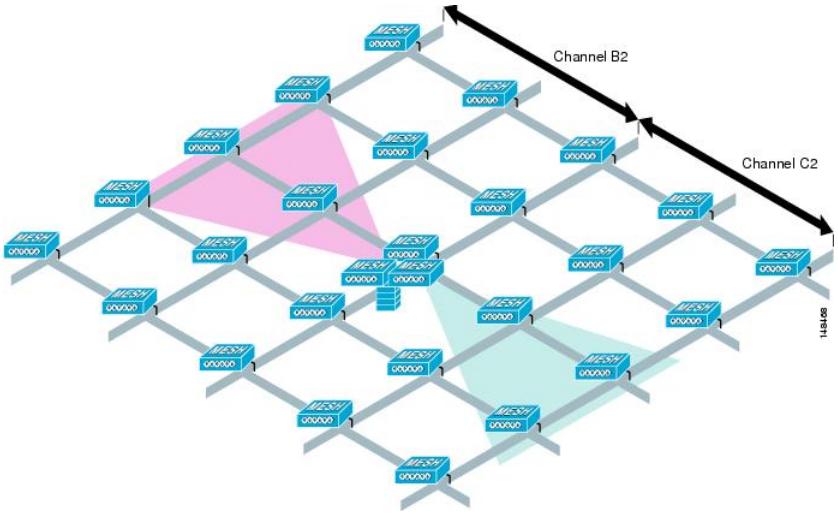
Assumptions for the Cisco Range Calculator

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

- You can only select only valid power levels.

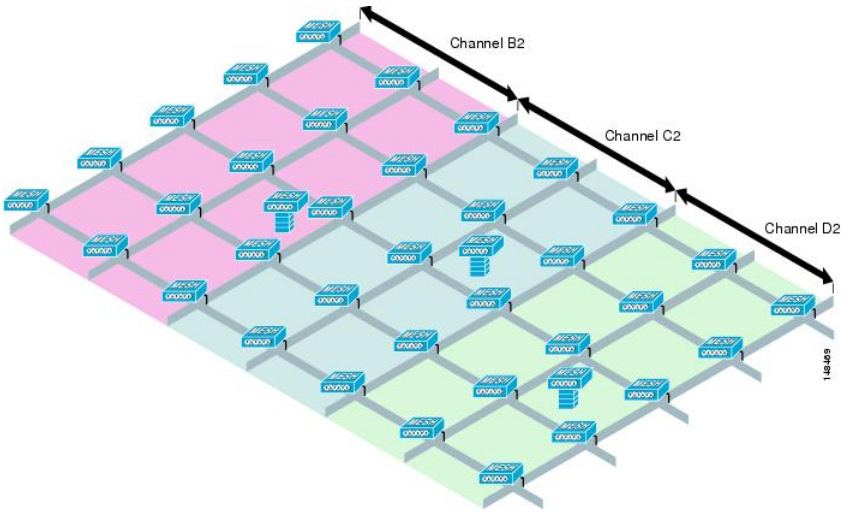
The RAPs shown in Figure 24: PoP with Multiple RAPs, on page 58 are simply a starting point. The goal is to use the RAP location in combination with the RF antenna design to ensure that there is a good RF link to the MAP within the core of the cell, which means that the physical location of the RAPs can be on the edge of the cell, and a directional antenna is used to establish a link into the center of the cell. Therefore, the wired network location of a RAP might play host to the RAP of multiple cells, as shown in Figure 24: PoP with Multiple RAPs, on page 58.

Figure 24: PoP with Multiple RAPs



When the basic cell composition is settled, the cell can be replicated to cover a greater area. When replicating the cells, a decision needs to be made whether to use the same backhaul channel on all cells or to change backhaul channels with each cell. In the example shown in Figure 25: Multiple RAP and MAP Cells, on page 58, various backhaul channels (B2, C2, and D2) per cell have been chosen to reduce the co-channel interference between cells.

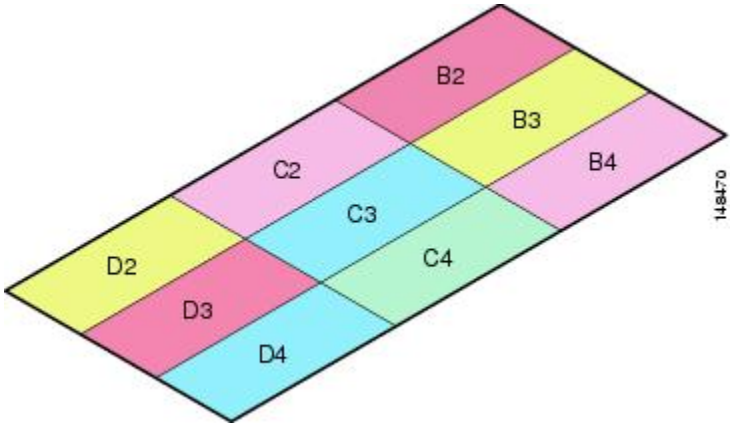
Figure 25: Multiple RAP and MAP Cells



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

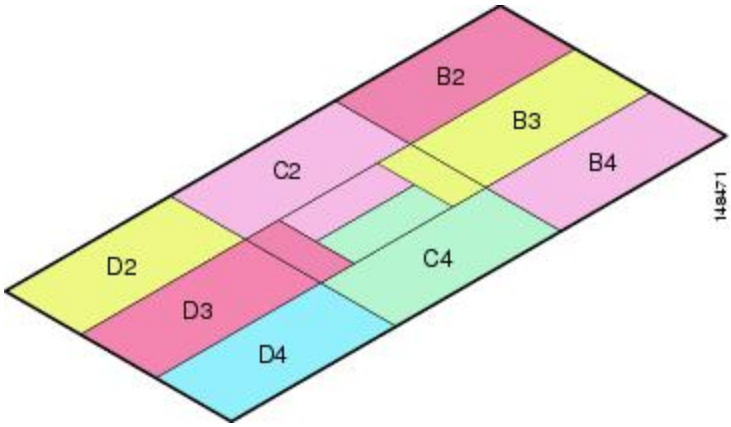
When you lay out multiple cells, use channel planning similar to standard WLAN planning to avoid overlapping channels, as shown in Figure 26: Laying out Various Cells, on page 59.

Figure 26: Laying out Various Cells



If possible, the channel planning should also minimize channel overlap in cases where the mesh has expanded to cover the loss of a RAP connection, as shown in Figure 27: Failover Coverage, on page 59.

Figure 27: Failover Coverage



Collocating Mesh Access Points

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

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

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

Collocating AP1500s on Adjacent Channels

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

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

Collocating AP1500s on Alternate Adjacent Channels

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

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

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

Special Considerations for Indoor Mesh Networks

Note these considerations for indoor mesh networks:

- For outdoors, voice is supported on a best-effort basis on a mesh infrastructure.
- Quality of Service (QoS) is supported on the local 2.4-GHz client access radio and on the 5-GHz.
- Cisco also supports static Call Admission Control (CAC) in CCXv4 clients, which provides CAC between the access point and the client.
- RAP-to-MAP ratio—The recommended ratio is 3 to 4 MAPs per RAP.
- AP-to-AP distance:
  - For 11n and 11ac mesh APs, a spacing of no more than 250 feet between each mesh AP with a cell radius of 125 feet is recommended.
- Hop count—For data, the maximum is 4 hops. No more than 2 hops is recommended for voice.
- RF considerations for client access on voice networks:
  - Coverage hole of 2 to 10 percent
  - Cell coverage overlap of 15 to 20 percent
  - Voice needs RSSI and SNR values that are at least 15 dB higher than data requirements
  - RSSI of -67 dBm for all data rates should be the goal for 11b/g/n and 11a/n
  - SNR should be 25 dB for the data rate used by client to connect to the AP
  - Packet error rate (PER) should be configured for a value of one percent or less

- Channel with the lowest utilization (CU) must be used

  Check the CU when no traffic is running

- Radio resource manager (RRM) can be used to implement the recommended RSSI, PER, SNR, CU, cell coverage, and coverage hole settings on the 802.11b/g/n radio (RRM is not available on 802.11a/n radio).

Figure 28: Cell Radius of 100 Feet (30.4 meters) and Access Point Placement for Voice Mesh Networks

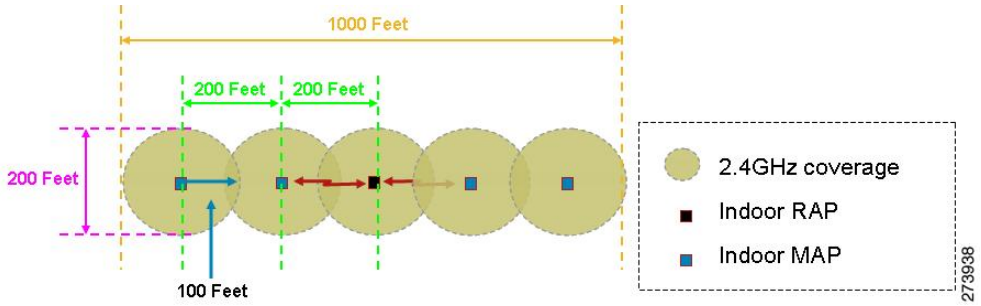
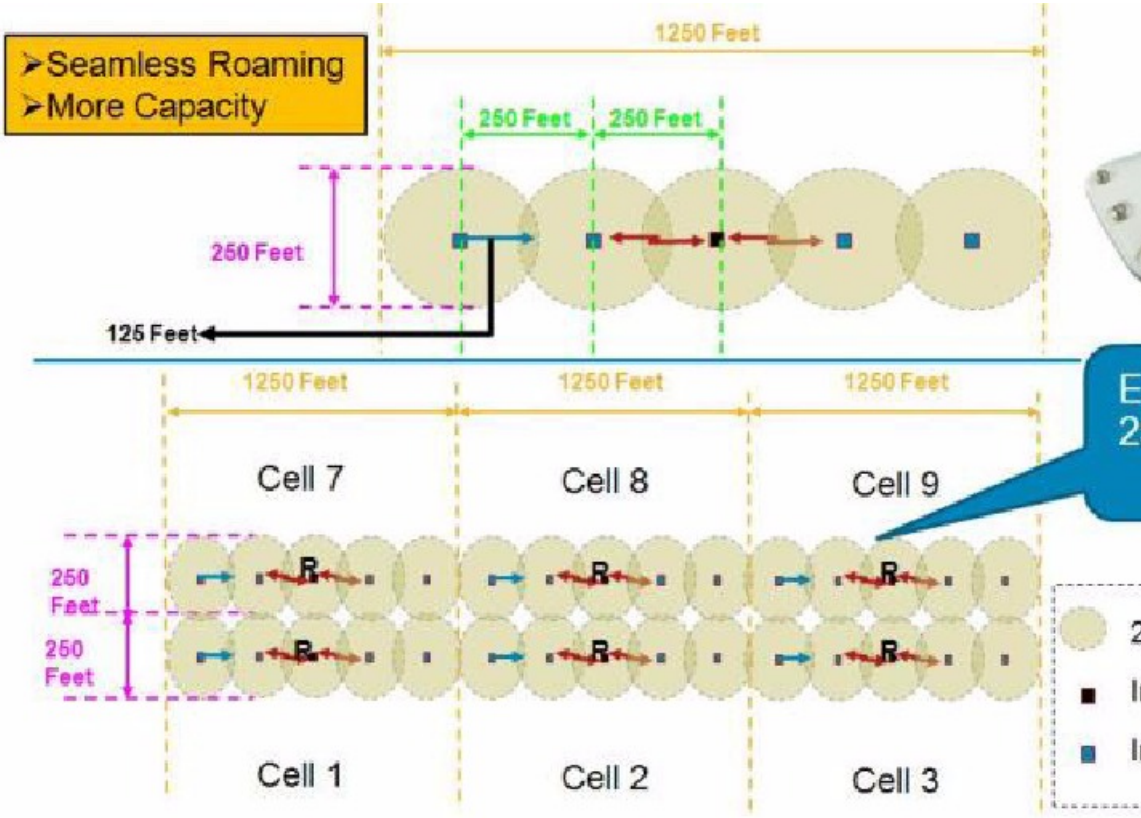


Figure 29: Cell Radius of 125 Feet (38 meters) and Access Point Placement for Indoor 11n Mesh Networks



Note Although you can use directional antenna and have an AP-to-AP distance longer than 250 feet (76.2 meters), for seamless roaming, we recommend that you have an AP-to-AP distance no more than 250 feet.

Wireless Propagation Characteristics

Table 23: Comparison of 2.4-GHz and 5-GHz Bands, on page 62 provides a comparison of the 2.4-GHz and 5-GHz bands.

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

Table 23: Comparison of 2.4-GHz and 5-GHz Bands

2.4-GHz Band Characteristics	5-GHz Band Characteristics
3 channels	22 channels (-A/-B regulatory domain)
More prone to co-channel interference	No co-channel interference
Lower power	Higher power
Lower SNR requirements given lower data rates	Higher SNR requirements given higher data rates
Better propagation characteristics than 5 GHz but more susceptible to noise and interference	Worse propagation characteristics than 2.4 GHz but less susceptible to noise and interference
Unlicensed band. Widely available throughout the world.	Not as widely available in the world as 2.4-GHz. Licenses in some countries.

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

CleanAir

The 1550/1570 series access points contain the CleanAir chipset, allowing full CleanAir support.

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

CleanAir AP Modes of Operation

Bridge (Mesh) Mode AP—CleanAir capable access points offer complete CleanAir functionality in the 2.4 GHz band and CleanAir advisor on the 5 GHz radio. This is across all access points that operate in Bridge mode.

Tight silicon integration with the Wi-Fi radio allows the CleanAir hardware to listen between traffic on the channel that is currently being served with no penalty to throughput of attached clients. That is, line rate detection without interrupting client traffic.

Bridge mode access points support Radio Resource Management (RRM) on the 2.4 GHz band, which helps to mitigate the interference from WiFi interferers. RRM is only available on the 5 GHz band, if a Bridge mode RAP has no child MAPs.

A CleanAir Mesh AP only scans one channel of each band continuously. In a normal deployment density, there should be many access points on the same channel, and at least one on each channel, assuming RRM is handling channel selection. In 2.4 GHz, access points have sufficient density to ensure at least three points of classification. An interference source that uses narrow band modulation (operates on or around a single frequency) is only detected by access points that share the frequency space. If the interference is a frequency hopping type (uses multiple frequencies—generally covering the whole band), it is detected by every access point that can hear it operating in the band.

Monitor Mode AP (MMAP)—A CleanAir monitor mode AP is dedicated and does not serve client traffic. The monitor mode ensures that all bands-channels are routinely scanned. The monitor mode is not available for access points in bridge (mesh) mode because in a mesh environment, access points also talk to each other on the backhaul. If a mesh AP (MAP) is in the monitor mode, then it cannot perform mesh operation.

Local Mode AP— When an outdoor access point is operating in local mode, it can preform full CleanAir and RRM on both the 2.4 GHz and 5 GHz channels. It will predominately scan its primary channel, but will periodically go off-channel to scan the rest of the spectrum. Enhanced Local Mode (ELM) wIPS detection is not available on the 1532, 1550, or 1570.

Spectrum Expert Connect Mode (optional) (SE Connect)—An SE Connect AP is configured as a dedicated spectrum sensor that allows connection of the Cisco Spectrum Expert application running on a local host to use the CleanAir AP as a remote spectrum sensor for the local application. This mode allows viewing of the raw spectrum data such as FFT plots and detailed measurements. This mode is intended for only remote troubleshooting.

Pseudo MAC (PMAC) and Merging

PMAC and Merging phenomenon is similar to the one for Generation 2 access points in local mode. A PMAC is calculated as part of the device classification and included in the interference device record (IDR). Each AP generates the PMAC independently. While it is not identical for each report (at a minimum the measured RSSI of the device is likely different at each AP), it is similar. The function of comparing and evaluating PMACs is called merging. The PMAC is not exposed to customer interfaces. Only the results of merging are available in the form of a cluster ID.

The same device can be detected by multiple APs. All the PMACs and IDRs are analyzed on the controller and a report is generated called a device cluster, which shows the APs detecting the device and the device cluster showing the AP which is hearing the device as strongest.

In this merging spatial proximity, RF proximity (RF neighbor relationship) work together. If there are six similar IDRs with 5 APs nearby and another one from an AP that is far away, it is unlikely that it is the same interferer. Therefore, a cluster is formed taking all these into account. MSE and the controller first rely on RF Neighbor lists to establish spatial proximity in a merge.

PMAC Convergence and Merging depends upon the following factors:

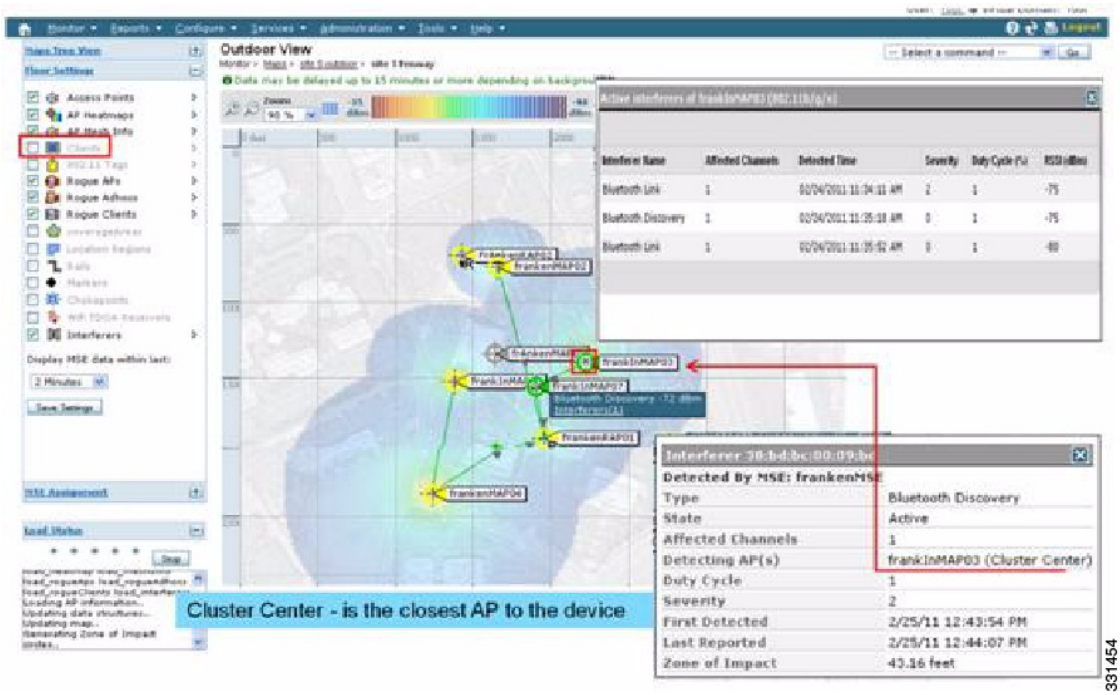
- Density of the sensors
- Quality of the observed classification
- RSSI from the interferer to the APs
- RF neighbor list at the APs

So RRM on 2.4 GHz in mesh also plays a key role in deciding the merging aspect. APs should be RF neighbors for any possibility of Merging. RF Neighbor list is consulted and spatial relationships for IDRs are taken into account for Merging.

Because there is no Monitor Mode in mesh, a single controller merging occurs on the controller. The result of a controller merge is forwarded to the MSE (if present) along with all of the supporting IDRs.

For more than one WLC (possible in outdoor deployments), merging occurs on the MSE. MSE does more advanced merging and extracts location and historical information for interferers. No Location is performed on controller merged interferers. Location is done on the MSE.

Figure 30: Pseudo MAC Merging in Outdoors



After PMAC signature merging, you can identify which AP can hear the device, and which AP is the center of a cluster. In the figure above, the values are relevant to the band selected. The label R on AP indicates that the AP is a RAP and the line between APs shows the mesh relationship.

Event Driven Radio Resource Management and Persistence Device Avoidance

There are two key mitigation features that are present with CleanAir. Both rely directly on information that can only be gathered by CleanAir. Event Driven Radio Resource Management (EDRRM) and Persistence Device Avoidance (PDA). For mesh networks, they work exactly the same way as for nonmesh networks in the 2.4-GHz band.

Note EDRRM and PDA are only available in a Greenfield installation and configured off by default.

CleanAir Access Point Deployment Recommendations

CleanAir is a passive technology that does not affect the normal operation of Wi-Fi networks. There is no inherent difference between a CleanAir deployment and a mesh deployment.

Locating a non-Wi-Fi device has a lot of variables to consider. Accuracy increases with power, duty cycle, and the number of channels hearing the device. This is advantageous because higher power, higher duty cycle, and devices that impact multiple channels are considered to be severe with respect to interference to networks.

Note There is no guarantee of accuracy for location of non- Wi-Fi devices.

There are a lot of variables in the world of consumer electronics and unintentional electrical interference. Any expectation of accuracy that is derived from current Client or Tag location accuracy models does not apply to non-Wi-Fi location and CleanAir features.

Important notes to consider:

- CleanAir mesh AP supports the assigned channel only.
- Band Coverage is implemented by ensuring that channels are covered.
- The CleanAir mesh AP can hear very well, and the active cell boundary is not the limit.
- For Location solutions, the RSSI cutoff value is –75 dBm.
- A minimum of three quality measurements is required for location resolution.

In most deployments, it is difficult to have a coverage area that does not have at least three APs nearby on the same channel in the 2.4-GHz band. In locations where there is minimal density, while the location resolution is likely not supported, the active user channel is protected.

Deployment considerations are dependent upon planning the network for desired capacity and ensuring that you have the correct components and network paths in place to support CleanAir functions. RF proximity and the importance of RF Neighbor Relations cannot be understated. It is important to keep in mind the PMAC and the merging process. If a network does not have a good RF design, the neighbor relations is affected, which in turn affects CleanAir performance.

The AP Density recommendations for CleanAir remain the same as normal mesh AP deployment.

Location resolution in the Outdoors is to the nearest AP. Devices are located near the AP which is physically closest to the device. It is advisable to assume closest AP resolution.

It is possible to deploy a few 1530 APs (non-CleanAir) with an installation that consists of 1552 APs and 1572 APs (CleanAir). This deployment can work from a client and coverage standpoint as these access points are fully interoperable with each other. The complete CleanAir functionality depends on all access points being CleanAir enabled. Detection can be affected, and mitigation is not recommended.

A CleanAir AP actively serving clients can only monitor the assigned channel that it is serving. In an area where you have multiple access points serving clients in close proximity, the channels being served by CleanAir

access points can drive CleanAir features. Legacy non-CleanAir access points rely on RRM, and mitigate interference issues, but not report the type and severity as CleanAir access points do to the system level.

For more information about mixed systems, see http://www.cisco.com/en/US/products/ps10315/products_tech_note09186a0080b4bdc1.shtml

CleanAir Advisor

If CleanAir is enabled on a backhaul radio, CleanAir Advisor is activated. CleanAir Advisor generates Air Quality Index (AQI) and Interferer Detection Reports (IDR) but the reports are only displayed in the controller. No action is taken through event driven RRM (ED-RRM). CleanAir Advisor is only present on the 5-GHz backhaul radio of the 1552 access points in Bridge mode. In all other AP modes, the 5-GHz backhaul radio of the 1552 access points operates in CleanAir mode.

Enabling CleanAir

To enable CleanAir functionality in the system, you first need to enable CleanAir on the controller through **Wireless > 802.11a/b > CleanAir**. Although CleanAir is disabled by default, CleanAir is enabled by default on the AP interface.

After you enable CleanAir, it takes 15 minutes to propagate air quality information because the default reporting interval is 15 minutes. However, you can see the results instantly at the CleanAir detail level on the radio by going to **Monitor > Access Points > 802.11a/n** or **802.11b/n**.

Licensing

A CleanAir system requires a CleanAir AP and a controller that is running release 7.0 or later releases. Adding the Cisco Prime Infrastructure allows the displays to be enhanced and additional information to be correlated within the system. Adding the MSE further enhances the available features and provides the history and location of specific interference devices. There is no additional license requirement for the CleanAir feature because the CleanAir AP is the license. Adding the Prime Infrastructure can be done with a basic license. Adding the MSE to the system requires a Prime Infrastructure Plus license and a context-aware license selection for the MSE.

For purposes of interference location with the MSE, each interference device counts as a location target in Context-Aware. One hundred Permanent Interferer licenses are embedded in the MSE. Interferer Licenses open as CleanAir APs are detected, in stages of five licenses per CleanAir AP. This process is applicable to AP1552. An Interference device is the same as a client or a tag from a license quantity standpoint. Only a small percentage of the available licenses are used because there should be far less interference devices than clients or tags to track. Users do have control over what types of interference devices to detect and located from the controller configuration menus.

Cisco context-aware licenses can be managed and limited by the class of target (client, tag, interference), which gives users complete control over how licenses are used.



Note Each interference device requires one context-aware service (CAS) license.

If you have too many Bluetooth devices, it is advisable to switch off the tracing of these devices because they might take up too many CAS licenses.

Wireless Mesh Mobility Groups

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

Multiple Controllers

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

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

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

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

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

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

Increasing Mesh Availability

In the Cell Planning Distance section, a wireless mesh cell of one square mile was created and then built upon. This wireless mesh cell has similar properties to the cells used to create a cellular phone network because the smaller cells (rather than the defined maximum cell size) can be created to cover the same physical area, providing greater availability or capacity. This process is done by adding a RAP to the cell. Similar to the larger mesh deployment, the decision is whether to use RAP on the same channel, as shown in Figure 31: Two RAPs per Cell with the Same Channel, on page 68, or to use RAPs placed on different channels, as shown in Figure 32: Two RAPs per Cell on Different Channels, on page 68. The addition of RAPs into an area adds capacity and resilience to that area.

Figure 31: Two RAPs per Cell with the Same Channel

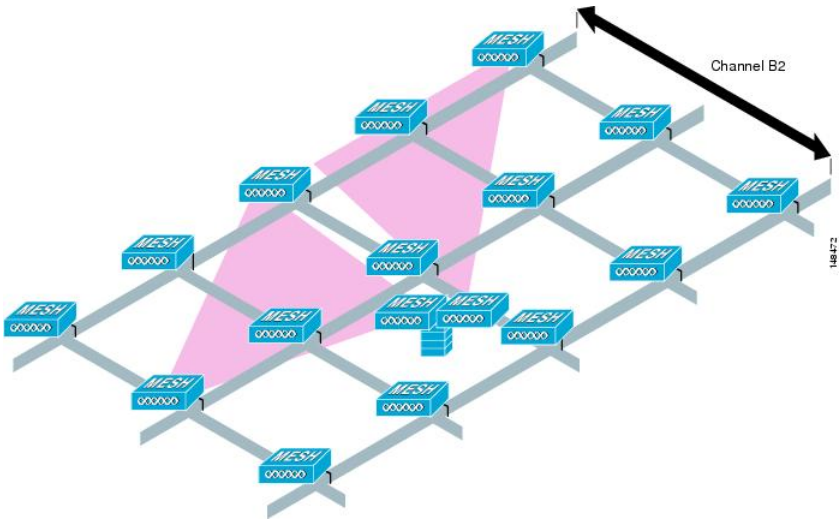
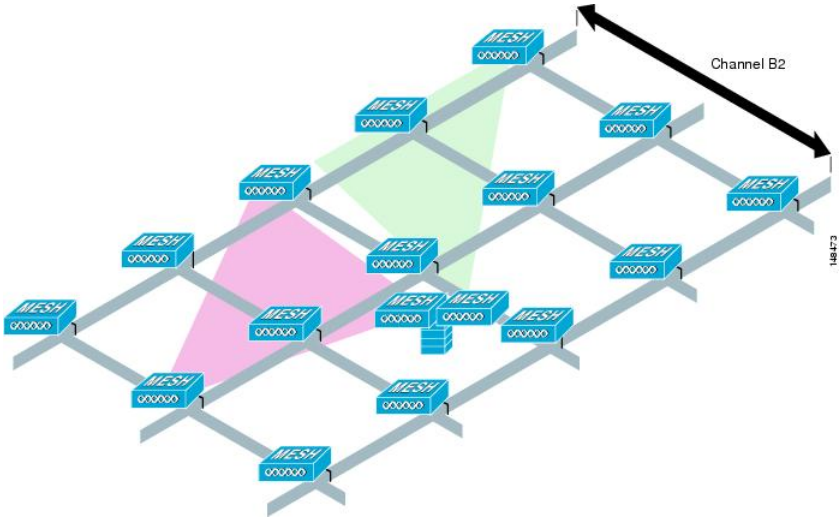


Figure 32: Two RAPs per Cell on Different Channels



Multiple RAPs

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

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

Adding a second RAP on a different channel also reduces the collision domain through channel planning or through RAP cell splitting. Channel planning allocates different nonoverlapping channels to mesh nodes in the same collision domain to minimize the collision probability. RAP cell splitting is a simple, yet effective, way to reduce the collision domain. Instead of deploying one RAP with omnidirectional antennas in a mesh

network, two or more RAPs with directional antennas can be deployed. These RAPs collocate with each other and operate on different frequency channels. This process divides a large collision domain into several smaller ones that operate independently.

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

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

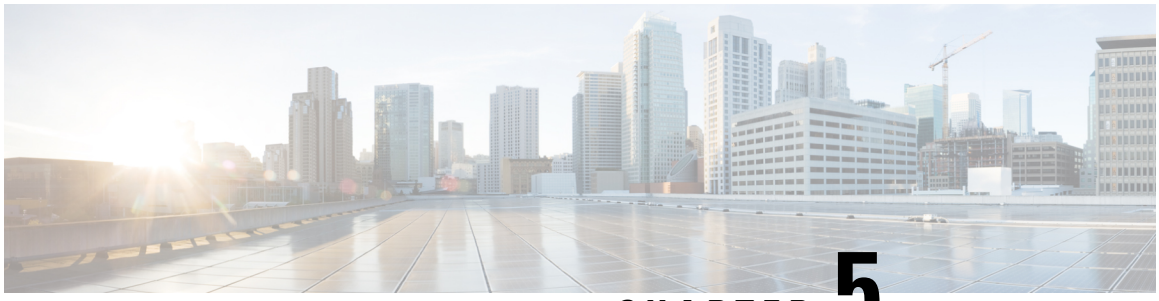
Indoor Mesh Interoperability with Outdoor Mesh

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



Caution The indoor access points in a third-party outdoor enclosure can be deployed for limited outdoor deployments, such as a simple short haul extension from an indoor WLAN to a hop in a parking lot. The 1260, 1600, 1700, 2600, 2700, 3500e, 3600, and 3700 access points in an outdoor enclosure is recommended because of its robust environmental and temperature specifications. Additionally, the indoor access points have connectors to support articulated antennas when the AP is within an outdoor enclosure. Exercise caution with the SNR values as they may not scale and long-term fades may take away the links for these APs when compared to a more optimized outdoor 1500 series access point.

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



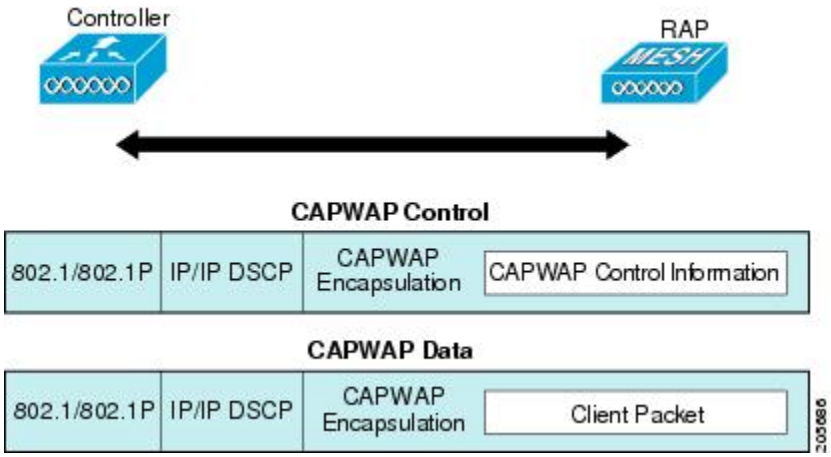
CHAPTER 5

Overview

This chapter describes how to connect the Cisco mesh access points to the network.

The wireless mesh terminates on two points on the wired network. The first location is where the RAP attaches to the wired network, and where all bridged traffic connects to the wired network. The second location is where the CAPWAP controller connects to the wired network; this location is where the WLAN client traffic from the mesh network connects to the wired network (see Figure 33: Mesh Network Traffic Termination, on page 71). The WLAN client traffic from CAPWAP is tunneled at Layer 2, and matching WLANs should terminate on the same switch VLAN where the controllers are collocated. The security and network configuration for each of the WLANs on the mesh depend on the security capabilities of the network to which the controller is connected.

Figure 33: Mesh Network Traffic Termination



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

For more information about upgrading to a new controller software release, see the *Release Notes for Cisco Wireless LAN Controllers and Lightweight Access Points* at http://www.cisco.com/en/us/products/ps10315/prod_release_notes_list.html.

For more information about mesh and controller software releases and the compatible access points, see the *Cisco Wireless Solutions Software Compatibility Matrix* at http://www.cisco.com/en/US/docs/wireless/controller/5500/tech_notes/Wireless_Software_Compatibility_Matrix.html.

This chapter contains the following sections:

- Enhanced Feature Set Access Points , on page 72
- Adding Mesh Access Points to the Mesh Network, on page 73
- Mesh PSK Key Provisioning , on page 85
- Configuring Global Mesh Parameters, on page 93
- Mesh Backhaul at 5 and 2.4 Ghz in Release 8.2 , on page 99
- Backhaul Client Access, on page 104
- Configuring Local Mesh Parameters, on page 106
- Configuring Antenna Gain, on page 113
- Configuring Dynamic Channel Assignment, on page 113
- Configuring Radio Resource Management on a Bridge Mode Access Point, on page 116
- Configuring Advanced Features, on page 117

Enhanced Feature Set Access Points

Enhanced Feature Set is the support for PMIPv6 MAG , IPv6, and PPPoE on Cisco 1500 series mesh access points.

The latest version of the 1500 series outdoor mesh access points with 128 MB RAM has Enhanced Feature Set enabled by default. It is disabled in the older versions of 1500 series outdoor mesh access points with 64MB RAM.

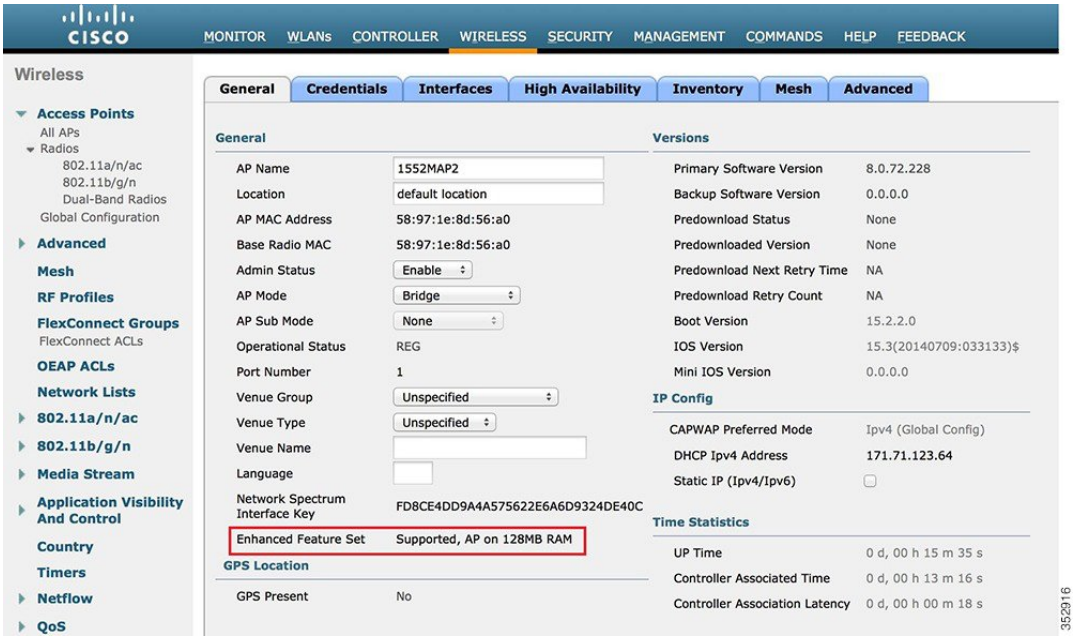
To display the Enhanced Feature Set information, use the command **show ap summary**.

```
(Cisco Controller)> show mesh ap summary

AP Name         AP Model           BVI MAC            CERT MAC          Hop  Bridge Group
Name  Enhanced Feature Set
-------------------------------------------------------------------------------------------------
RAP-1550-128MB  AIR-CAP1552H-C-K9  34:a8:4e:51:a0:00  34:a8:4e:51:a0:1e  0   cisco
      Supported, 128MB RAM
MAP-1550-64MB   AIR-CAP1552H-C-K9  34:a8:4e:51:7e:c0  34:a8:4e:51:7e:de  1   cisco
      Not Supported, 64MB RAM
```

You can also view the Enhanced Feature Set information by clicking on the AP name from **Wireless** > **Access Points** > **All Access Points**.

Figure 34: Enhanced Feature Set



Adding Mesh Access Points to the Mesh Network

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

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

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

Step 1 Add the MAC address of the mesh access point to the controller's MAC filter. See the Adding MAC Addresses of Mesh Access Points to MAC Filter section.

Step 2 Define the role (RAP or MAP) for the mesh access point. See the Defining Mesh Access Point Role section.

Step 3 Verify that Layer 3 is configured on the controller. See the Verifying Layer 3 Configuration section.

Step 4 Configure a primary, secondary, and tertiary controller for each mesh access point. See the Configuring Multiple Controllers Using DHCP 43 and DHCP 60 section.

Configure a backup controller. See the Configuring Backup Controllers section.

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

Step 6 Configure global mesh parameters. See the Configuring Global Mesh Parameters section.

Step 7 Configure backhaul client access. See the Configuring Advanced Features section.

Step 8 Configure local mesh parameters. See the Configuring Local Mesh Parameters section.

Step 9 Configure antenna parameters. See the Configuring Antenna Gain section.

Step 10 Configure channels for serial backhaul. This step is applicable only to serial backhaul access points. See the Backhaul Channel Deselection on Serial Backhaul Access Point section.

Step 11 Configure the DCA channels for the mesh access points. See the Configuring Dynamic Channel Assignment section.

Step 12 Configure mobility groups (if desired) and assign controllers. See the Configuring Mobility Groups chapter in the *Cisco Wireless Controller Configuration Guide*.

Step 13 Configure Ethernet bridging (if desired). See the Configuring Ethernet Bridging section.

Step 14 Configure advanced features such as Ethernet VLAN tagging network, video, and voice. See the Configuring Advanced Features section.

Adding MAC Addresses of Mesh Access Points to MAC Filter

You must enter the radio MAC address for all mesh access points that you want to use in the mesh network into the appropriate controller. A controller only responds to discovery requests from outdoor radios that appear in its authorization list. MAC filtering is enabled by default on the controller, so only the MAC addresses need to be configured. If the access point has an SSC and has been added to the AP Authorization List, then the MAC address of the AP does not need to be added to the MAC Filtering List.

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

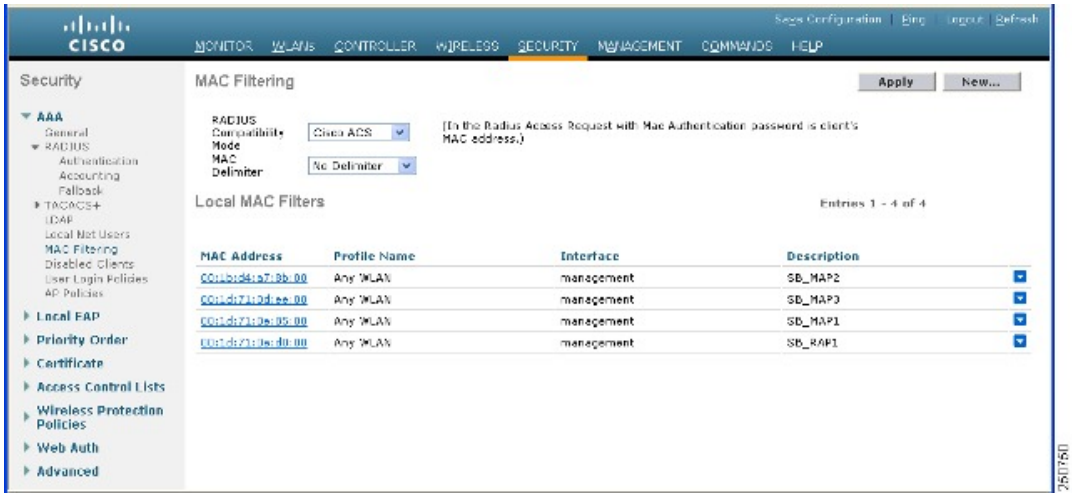
Note You can also download the list of mesh access point MAC addresses and push them to the controller using Cisco Prime Infrastructure.

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

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

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

Figure 35: MAC Filtering Page



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

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

Note For 1500 series outdoor mesh access points, specify the BVI MAC address of the mesh access point into the controller as a MAC filter. For indoor mesh access points, enter the Ethernet MAC. If the required MAC address does not appear on the exterior of the mesh access point, enter the following command at the access point console to display the BVI and Ethernet MAC addresses: **sh int** | **i** *hardware*.

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

Step 5 In the Description field, specify a description of the mesh access point. The text that you enter identifies the mesh access point on the controller.

Note You might want to include an abbreviation of its name and the last few digits of the MAC address, such as ap1522:62:39:10. You can also note details on its location such as *roof top*, *pole top*, or its cross streets.

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

Step 7 Click **Apply** to commit your changes. The mesh access point now appears in the list of MAC filters on the MAC Filtering page.

Step 8 Click **Save Configuration** to save your changes.

Step 9 Repeat this procedure to add the MAC addresses of additional mesh access points to the list.

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

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

Step 1 To add the MAC address of the mesh access point to the controller filter list, enter this command:

config macfilter add *ap_mac wlan_id interface* [*description*]

A value of zero (0) for the *wlan_id* parameter specifies any WLAN, and a value of zero (0) for the *interface* parameter specifies none. You can enter up to 32 characters for the optional *description* parameter.

Step 2 To save your changes, enter this command:

save config

Defining Mesh Access Point Role

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

General Notes about MAP and RAP Association With The Controller

The general notes are as follows:

- A MAP always sets the Ethernet port as the *primary backhaul* if it is UP, and secondarily the 802.11a/n/ac radio. This gives the network administrator time to reconfigure the mesh access point as a RAP, initially.

For faster convergence on the network, we recommend that you do not connect any Ethernet device to the MAP until it has joined the mesh network.

- A MAP that fails to connect to a controller on a UP Ethernet port, sets the 802.11a/n/ac radio as the primary backhaul. If a MAP fails to find a neighbor or fails to connect to a controller through a neighbor, the Ethernet port is set as the primary backhaul again.
- A MAP connected to a controller over an Ethernet port does not build a mesh topology (unlike a RAP).
- A RAP always sets the Ethernet port as the primary backhaul.
- If the Ethernet port is DOWN on a RAP, or a RAP fails to connect to a controller on a UP Ethernet port, the 802.11a/n/ac radio is set as the primary backhaul for 15 minutes. Failing to find a neighbor or failing to connect to a controller via any neighbor on the 802.11a/n/ac radio causes the primary backhaul to go into the *scan* state. The primary backhaul begins its scan with the Ethernet port.

Configuring the AP Role (GUI)

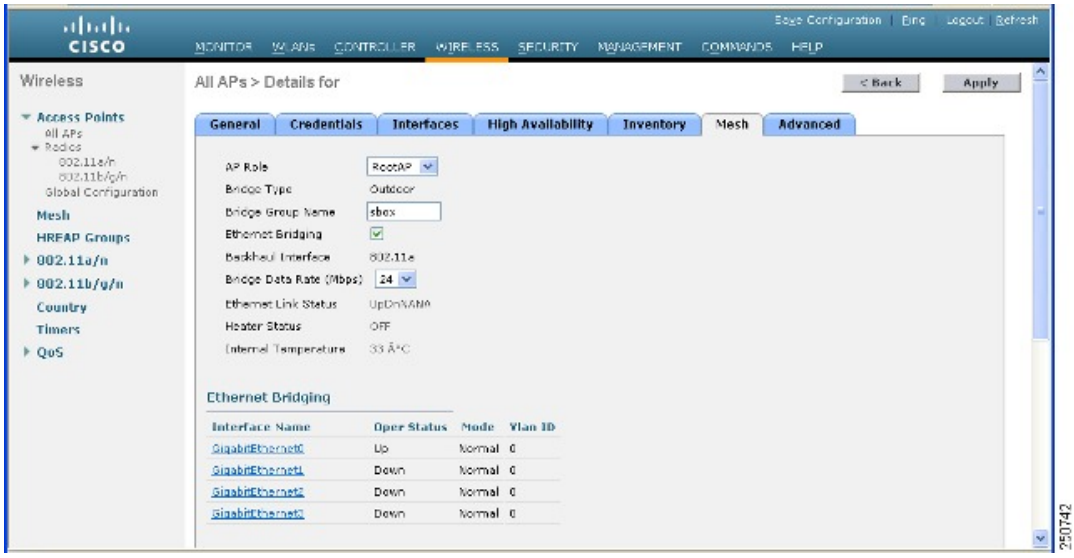
To configure the role of a mesh access point using the GUI, follow these steps:

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

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

Step 3 Click the **Mesh** tab.

Figure 36: All APs > Details for (Mesh) Page



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

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

Configuring the AP Role (CLI)

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

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

Configuring Multiple Controllers Using DHCP 43 and DHCP 60

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

Step 1 Enter configuration mode at the Cisco IOS CLI.

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

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

where:

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

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

```
option 60 ascii “VCI string”
```

For the VCI string, use one of the values below. The quotation marks must be included.

```
For Cisco 1550 series access points, enter “Cisco AP c1550”
For Cisco 1520 series access points, enter “Cisco AP c1520”
For Cisco 1240 series access points, enter “Cisco AP c1240”
For Cisco 1130 series access points, enter “Cisco AP c1130”
```

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

```
option 43 hex hex string
```

The hex string is assembled by concatenating the TLV values 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
```

Backup Controllers

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

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



Note The fast heartbeat timer is not supported on access points in bridge mode. The fast heartbeat timer is configured only on access points in local and FlexConnect modes.

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



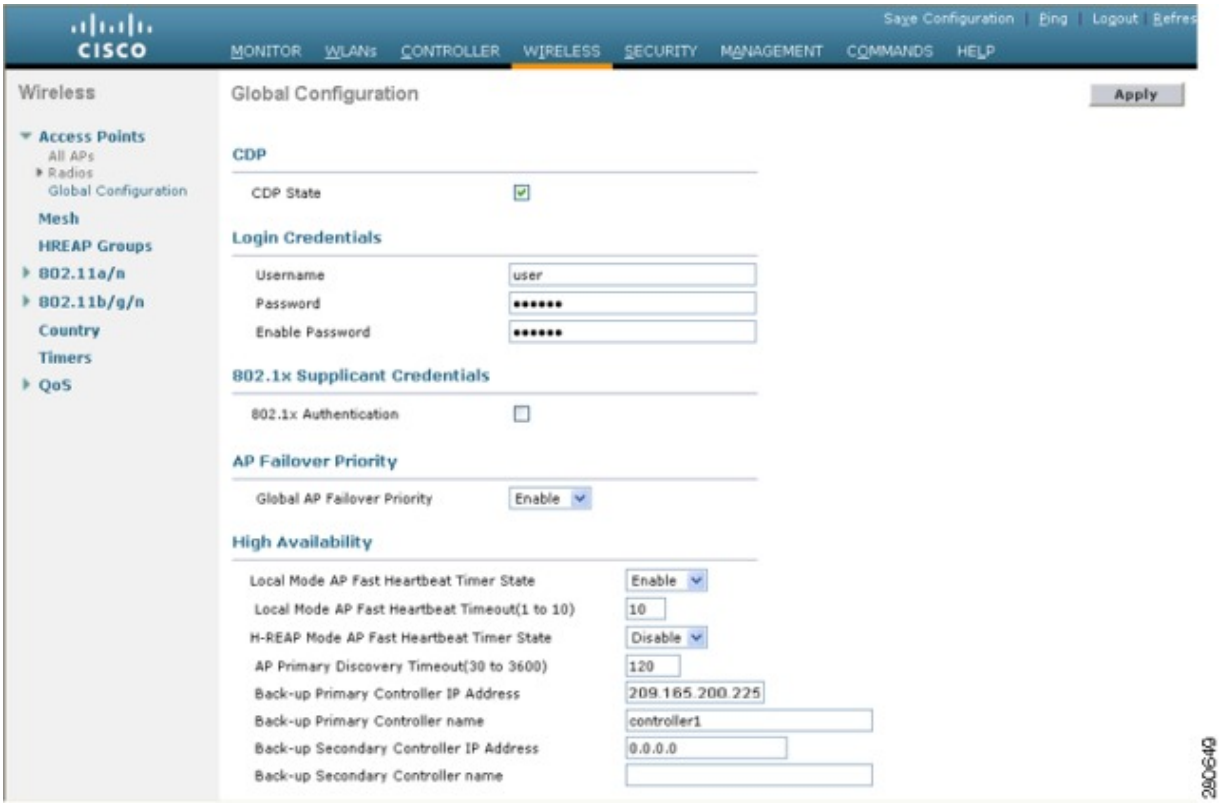
Note When a mesh access point's primary controller comes back online, the mesh access point disassociates from the backup controller and reconnects to its primary controller. The mesh access point falls back to its primary controller and not to any secondary controller for which it is configured. For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

Configuring Backup Controllers (GUI)

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

Step 1 Choose **Wireless > Access Points > Global Configuration** to open the Global Configuration page (see Figure 37: Global Configuration Page, on page 79).

Figure 37: Global Configuration Page



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

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

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

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

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

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

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

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

a) Choose **Access Points** > **All APs** to open the All APs page.
b) Click the name of the access point for which you want to configure primary, secondary, and tertiary backup controllers.
c) Click the **High Availability** tab.
d) If desired, specify the name and IP address of the primary backup controller for this access point in the Primary Controller fields.

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

e) If desired, specify the name and IP address of the secondary backup controller for this mesh access point in the Secondary Controller fields.
f) If desired, specify the name and IP address of the tertiary backup controller for this mesh access point in the Tertiary Controller fields.
g) No change is required to the AP Failover Priority value. The default value for mesh access points is critical and it cannot be modified.
h) Click **Apply** to commit your changes.

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

Configuring Backup Controllers (CLI)

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

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

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

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

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

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

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

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

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

config advanced backup-controller primary *backup_controller_name backup_controller_ip_address*

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

config advanced backup-controller secondary *backup_controller_name backup_controller_ip_address*

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

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

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

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

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

config advanced timers ap-discovery-timeout *interval*

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

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

config advanced timers auth-timeout *interval*

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

Step 9 To save your changes, enter this command:

save config

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

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

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

```
Cisco AP Identifier.............................. 1
Cisco AP Name.................................... AP5
Country code..................................... US  - United States
Regulatory Domain allowed by Country............. 802.11bg:-AB    802.11a:-AB
AP Country code.................................. US  - United States
AP Regulatory Domain............................. 802.11bg:-A    802.11a:-N
Switch Port Number .............................. 1
MAC Address...................................... 00:13:80:60:48:3e
IP Address Configuration......................... DHCP
IP Address....................................... 1.100.163.133
...
Primary Cisco Switch Name........................ 1-5520
Primary Cisco Switch IP Address.................. 2.2.2.2
Secondary Cisco Switch Name...................... 2-5520
Secondary Cisco Switch IP Address................ 2.2.2.2
Tertiary Cisco Switch Name....................... 3-5520
Tertiary Cisco Switch IP Address................. 1.1.1.4
```

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

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

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

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

```
AP Primary Discovery Timeout (seconds)..... 120
```

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

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

Configuring External Authentication and Authorization Using a RADIUS Server

External authorization and authentication of mesh access points using a RADIUS server such as Cisco ACS (4.1 and later) is supported in release 5.2 and later releases. The RADIUS server must support the client authentication type of EAP-FAST with certificates.

Before you employ external authentication within the mesh network, ensure that you make these changes:

- The RADIUS server to be used as an AAA server must be configured on the controller.
- The controller must also be configured on the RADIUS server.
- Add the mesh access point configured for external authorization and authentication to the user list of the RADIUS server.
    - For additional details, see the Adding a Username to a RADIUS Server section.
- Configure EAP-FAST on the RADIUS server and install the certificates. EAP-FAST authentication is required if mesh access points are connected to the controller using an 802.11a interface; the external RADIUS servers need to trust Cisco Root CA 2048. For information about installing and trusting the CA certificates, see the Configuring RADIUS Servers section.

Note If mesh access points connect to a controller using a Fast Ethernet or Gigabit Ethernet interface, only MAC authorization is required.

Note This feature also supports local EAP and PSK authentication on the controller.

Configuring RADIUS Servers

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

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

- https://www.cisco.com/security/pki/certs/crca2048.cer
- https://www.cisco.com/security/pki/certs/cmca.cer

Step 2 Install the certificates as follows:

a) From the CiscoSecure ACS main menu, click **System Configuration** > **ACS Certificate Setup** > **ACS Certification Authority Setup**.
b) In the **CA certificate file** box, type the CA certificate location (path and name). For example: C:\Certs\crca2048.cer.
c) Click **Submit**.

Step 3 Configure the external RADIUS servers to trust the CA certificate as follows:

a) From the CiscoSecure ACS main menu, choose **System Configuration** > **ACS Certificate Setup** > **Edit Certificate Trust List**. The Edit Certificate Trust List appears.
b) Select the check box next to the **Cisco Root CA 2048 (Cisco Systems)** certificate name.
c) Click **Submit**.
d) To restart ACS, choose **System Configuration** > **Service Control**, and then click **Restart**.

For additional configuration details on Cisco ACS servers, see the following:

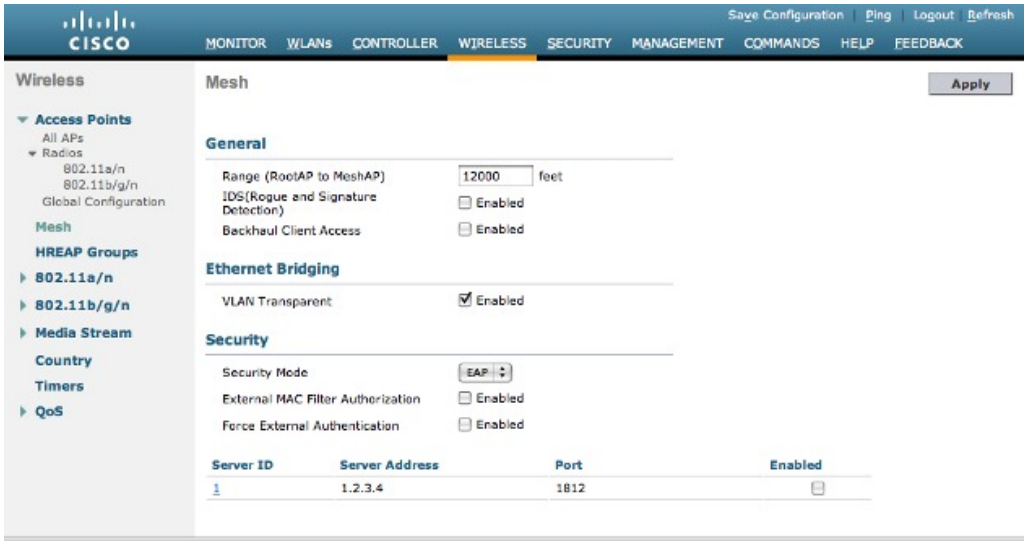
- http://www.cisco.com/en/US/products/sw/secursw/ps2086/products_installation_and_configuration_guides_list.html(Windows)
- http://www.cisco.com/en/US/products/sw/secursw/ps4911/(UNIX)

Enabling External Authentication of Mesh Access Points (GUI)

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

Step 1 Choose **Wireless** > **Mesh**. The Mesh page appears (see Figure 38: Mesh Page, on page 84).

Figure 38: Mesh Page



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

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

Step 4 Click **Apply**.

Step 5 Click **Save Configuration**.

Adding a Username to a RADIUS Server

Add MAC addresses of mesh access point that are authorized and authenticated by external RADIUS servers to the user list of that server *prior* to enabling RADIUS authentication for a mesh access point.

For remote authorization and authentication, EAP-FAST uses the manufacturer's certificate (CERT) to authenticate the child mesh access point. Additionally, this manufacturer certificate-based identity serves as the username for the mesh access point in user validation.

For Cisco IOS-based mesh access points, in addition to adding the MAC address to the user list, you need to enter the *platform_name_string–MAC_address* string to the user list (for example, c1240-001122334455). The controller first sends the MAC address as the username; if this first attempt fails, then the controller sends the *platform_name_string–MAC_address* string as the username.

Note The Authentication MAC address is different for outdoor versus indoor APs. Outdoor APs use the AP's BVI MAC address, whereas indoor APs use the AP's Gigabit Ethernet MAC address.

RADIUS Server Username Entry

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

- platform_name_string-MAC_address

User: c1570-aabbccddeeff

Password: cisco

- Hyphen Delimited MAC Address

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

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



Note The AP1552 platform uses a platform name of c1550. The AP1532 platform uses a platform name of ap1g3. The AP1572 uses a platform name of c1570.

Enable External Authentication of Mesh Access Points (CLI)

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

Step 1 **config mesh security eap**

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

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

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

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

View Security Statistics (CLI)

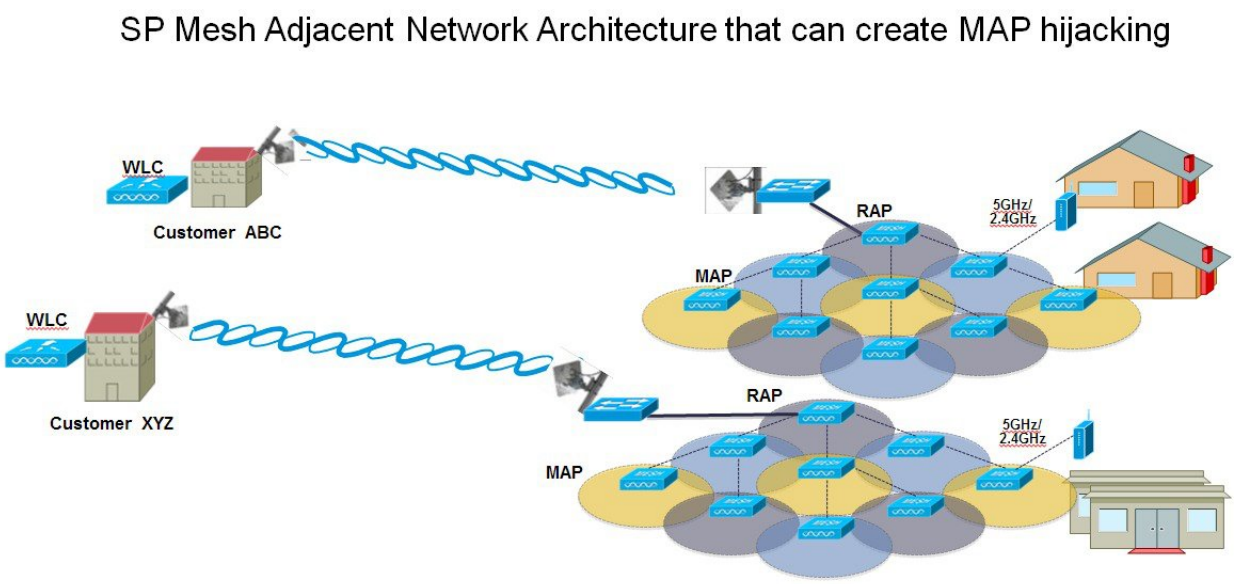
To view security statistics for mesh access points using the CLI, enter the following command:

show mesh security-stats *Cisco_AP*

Use this command to display packet error statistics and a count of failures, timeouts, and association and authentication successes as well as reassociations and reauthentications for the specified access point and its child.

Mesh PSK Key Provisioning

Customers with Cisco Mesh deployment will see their Mesh Access Points (MAP) possibly moving out of their network and joining another Mesh network when both of these Mesh Deployments use AAA with wild card MAC filtering to allow MAPs association. As Mesh APs security may use EAP-FAST this cannot be controlled since for EAP security combination of MAC address and type of AP is used and there is no controlled configuration is available. PSK option with default passphrase also presents security risk and hijack possibility. This issue will be prominently seen in overlapping deployments of two different SPs when the MAPs are used in a moving vehicle (public transportations, ferry, ship and so on.). This way, there is no restriction on MAPs to 'stick' to the SPs mesh network and MAPs can be hijacked / getting used by another SPs network / and cannot serve intended customers of SPs in a deployment.



The new feature introduced in 8.2 release will enable a provision-able PSK functionality from WLC which will help make a controlled mesh deployment and enhance MAPs security beyond default **'cisco'** PSK used today. With this new feature the MAPs which are configured with a custom PSK, will use this key to do their authentication with their RAPs and WLC. A special precaution should be taken when upgrading from Controller Software release 8.1 and below or downgrading from release 8.2. Admin needs to understand the implications when MAP software is moving in and out of PSK support.

If a mesh PSK mismatch occurs, we recommend that you do any one of the following three tasks to address the issue:

1. Delete the PSK key from the MAP as follows:
   a. With MAP in connected state, move the MAP to EAP.
   b. On the controller UI, navigate to the Mesh tab and delete the PSK key for the MAP.
2. Have a wired connection between MAP and the controller and then clear the configuration on the MAP.
3. Clear the configuration from the MAP console.

Wireless Mesh Components Supported

- WiSM2, 5508, Flex 7510 and 8510 Wireless LAN Controller
- Mesh AP 1550, 1530 or 1570 series and all indoor Mesh supported APs.
- Wireless clients (tablets, smartphones and so on.)

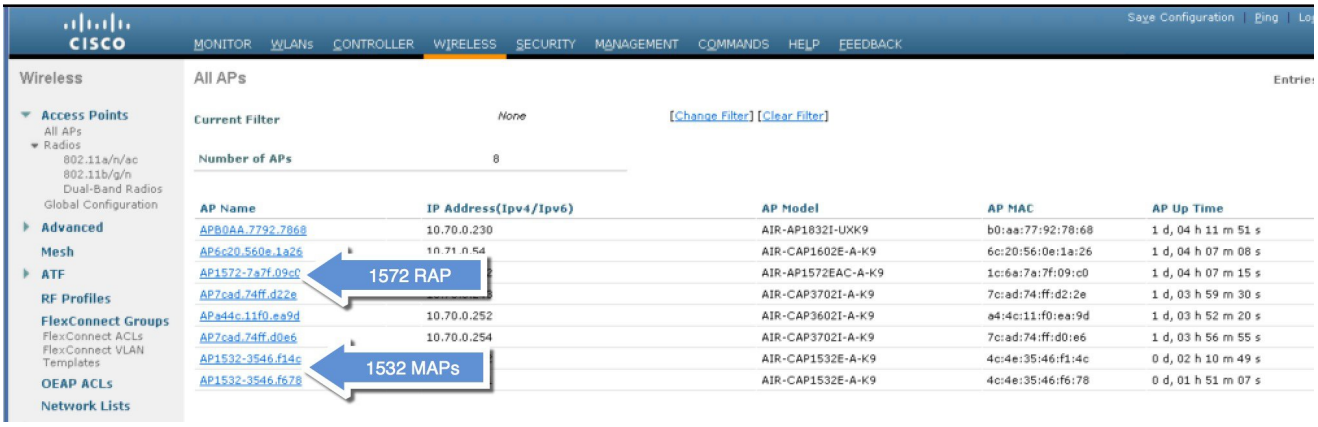
Feature Configuration Step-by-Step

Admin shall set security mode as PSK and optionally configure a new PSK. If there is no PSK configured MAPs will be able to join with default PSK key '**cisco**'.

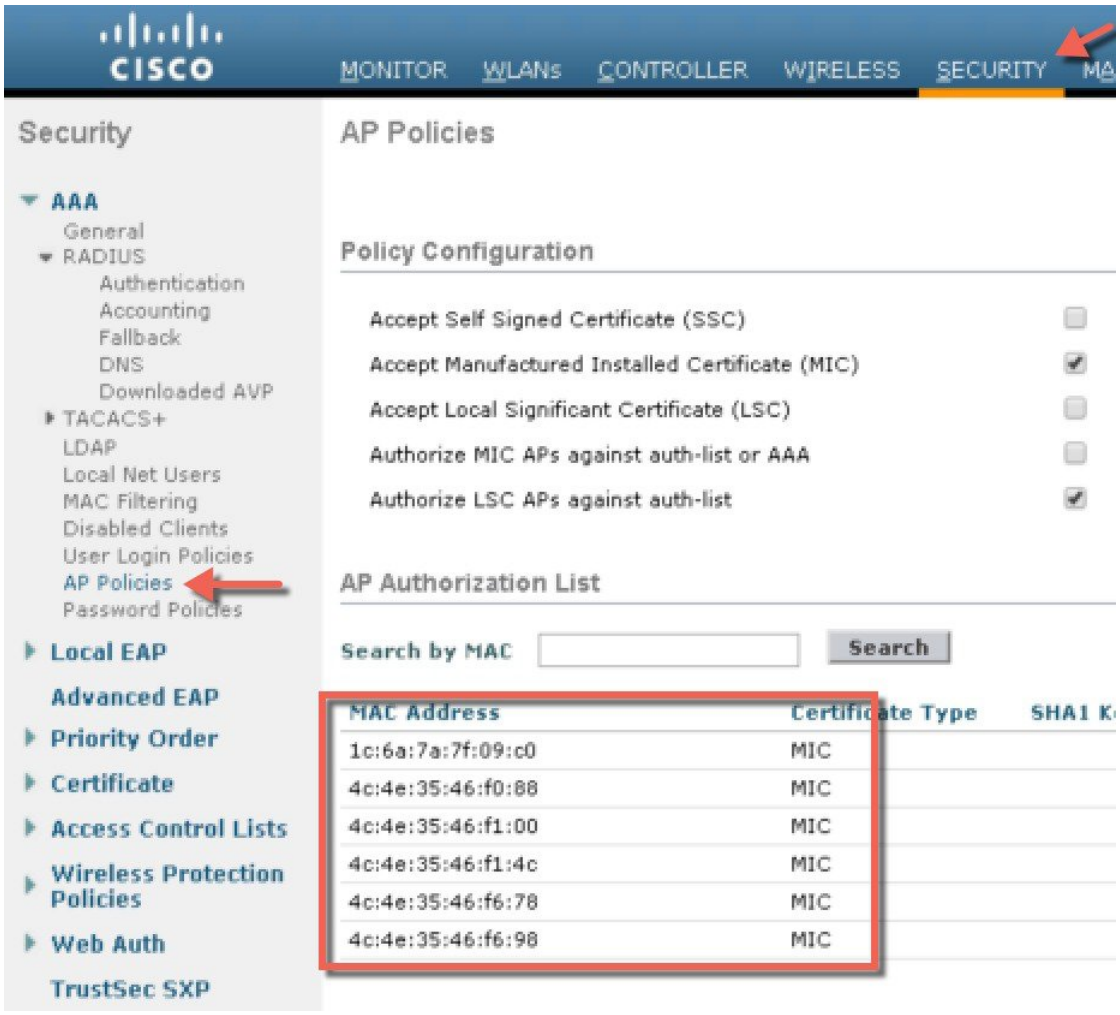
- Provisioning shall be local to each WLC
- Need to be in 'enabled' state to allow local provisioning
- Key strength as followed in WLC (Alphanumeric with special characters combination of lower, upper case, length 3-32 characters, special characters supported, redundant passwords not supported.
- Provisioned PSK is encrypted at WLC, stored, and sent to APs in encrypted format.

Mesh PSK GUI Configuration

Step 1 Connect a RAP to the controller as documented in the above sections of this Deployment Guide. As shown in the Configuration illustration example below two 1532 MAPs are connected to the RAP 1572.

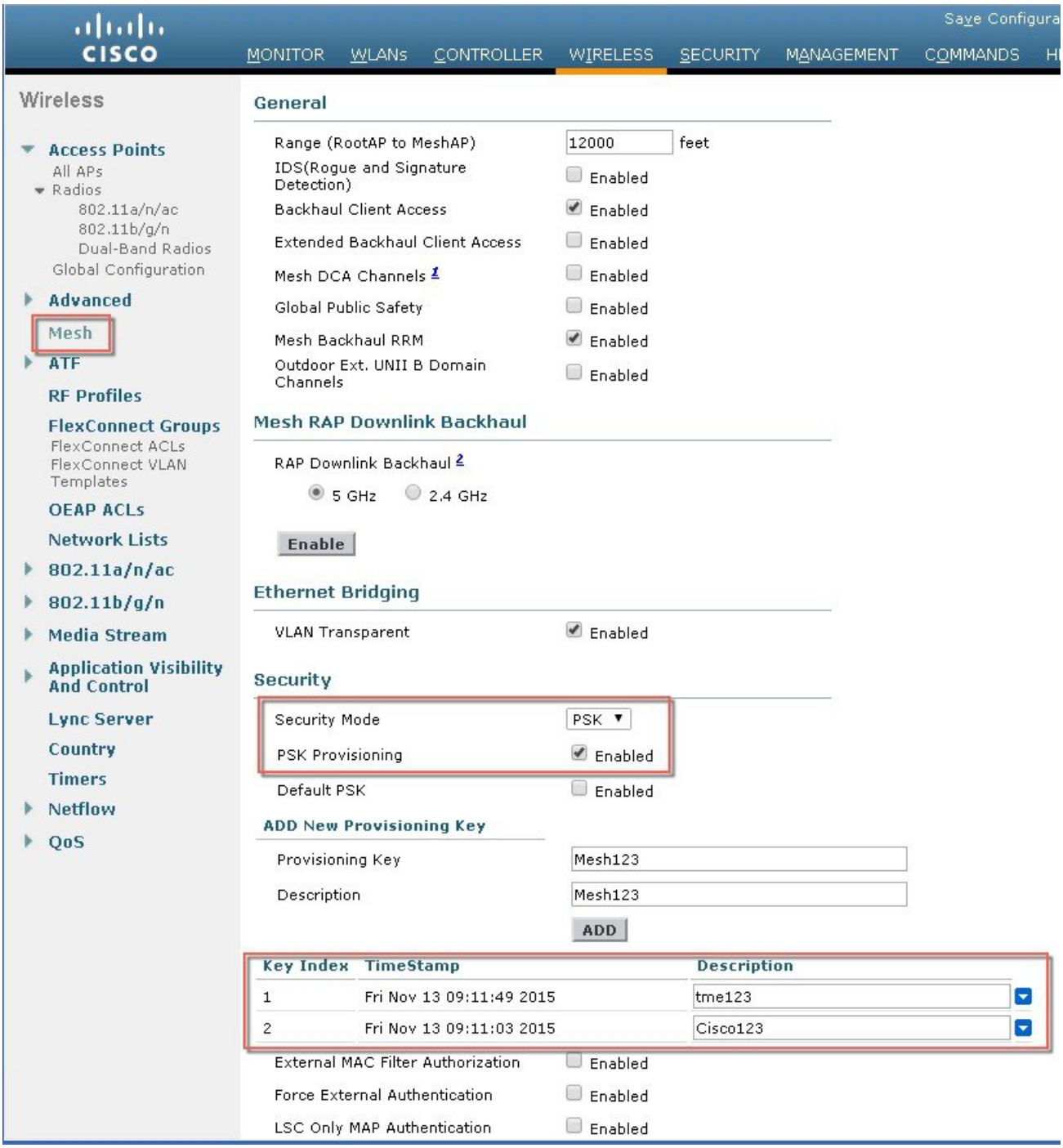


As indicated in the deployment guide one of the options for the MAPs initial connection the MAP MAC addresses have to be entered on the controller for them to be connected to the RAP as indicated in the screen shot.



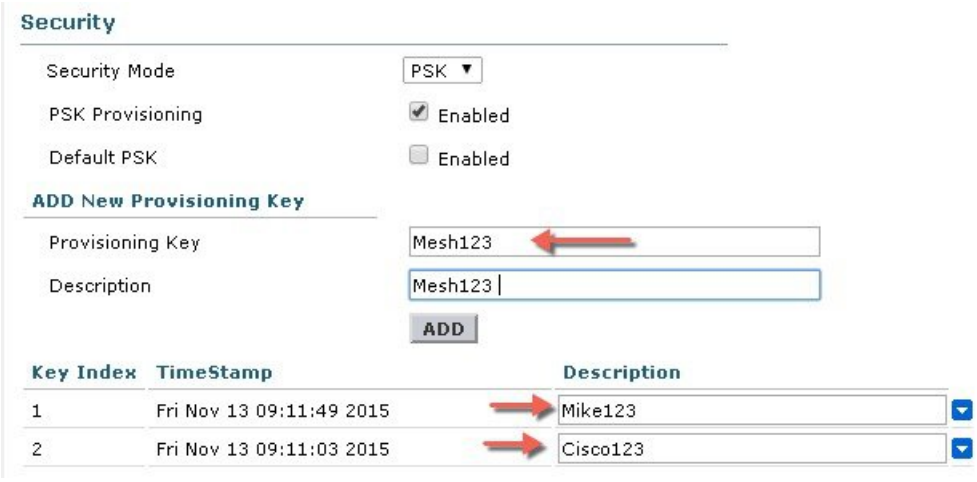
Step 2 From Wireless > Mesh menu, choose Security Mode as PSK and enable PSK provisioning.

Prior to release 8.2 MAC, AAA authentication with wild card character or EAP authentication were the only three methods where EAP was basically used with default internal authentication and MAC address provisioning was not reliable enough in certain installations especially when Mesh installations from different customers were overlapping and there was a strong probability of Mesh APs being accidently hijacked from one Mesh network to another. That could create many issues and coverage holes in the Mesh deployments. For that reason in release 8.2 a PSK MAP provisioning was introduced. As indicated above the PSK key has to be created on the wireless controller.



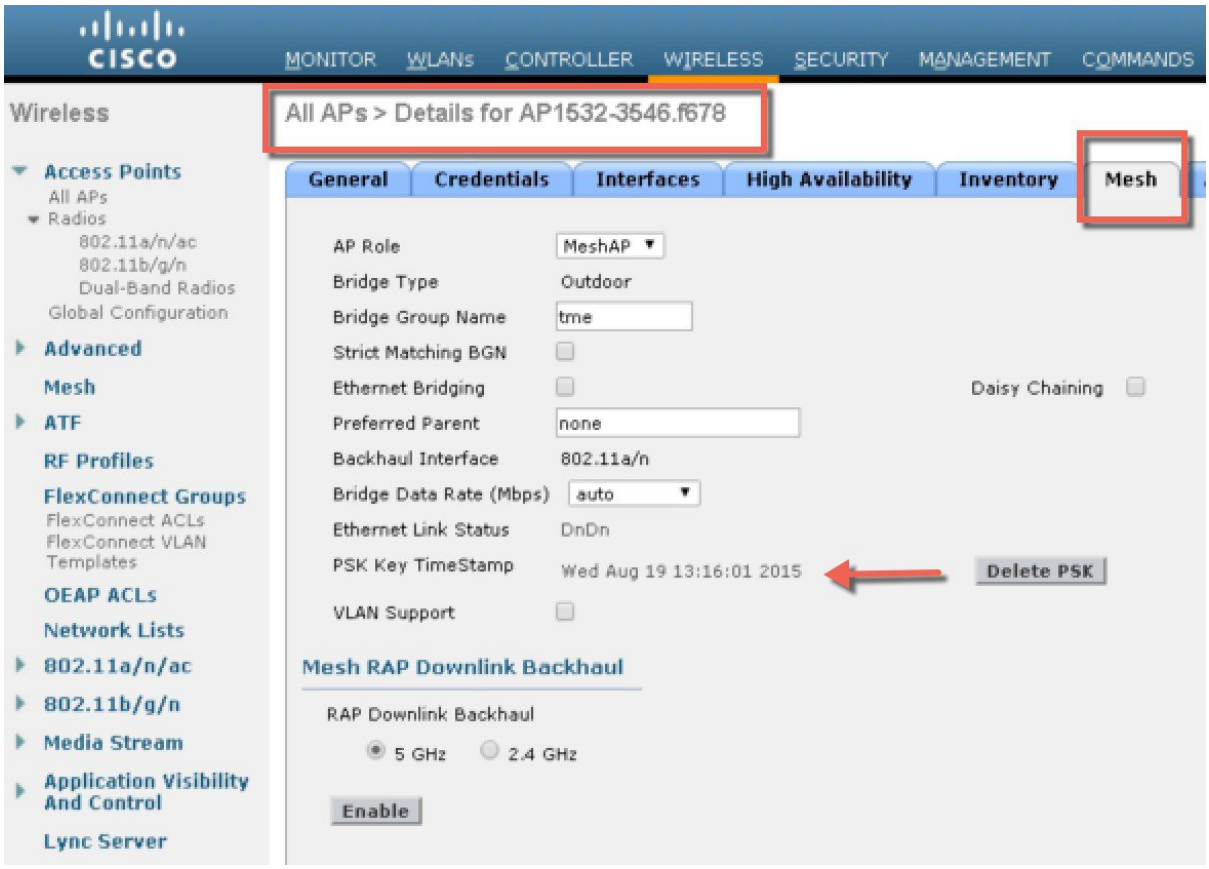
Step 3 Enter Provisioning Key as shown in the example and hit ADD to apply the entered value.

The Key value will not show in the list but only the Index of the key with a time stamp when that key was provisioned on the controller. Up to 5 keys can be entered on the controller for MAPs to be used for provisioning. Any of those 5 keys that are always stored in flash on the controller, can be used by MAP for provisioning. MD5 cryptographic algorithm (128-bit) is used to encrypt a provisioned PSK and sent down to APs during new key configuration.

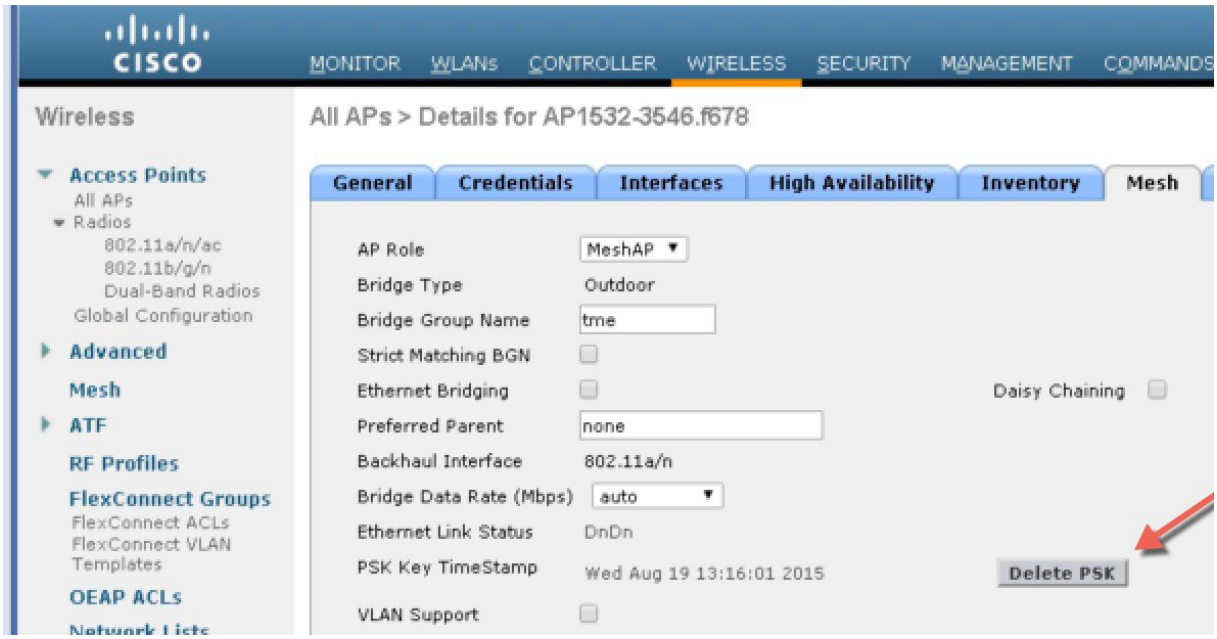


Step 4 Once the controller has the PSK key configured and enabled the key will be provisioned on the RAP and propagated to all MAPs connected to that RAP. The same key will be also propagated to all other children MAPs in the mesh network. There is no need to do anything on the MAPs in order for them to receive PSK key and authenticate to the RAP/MAP network

As shown in the example when observing one specific MAP that connected to the RAP, under the Mesh tab - you can see that MAP has been provisioned using PSK key with index 1 and Time Stamp from August 19th.



Step 5 The provisioned PSK key can be deleted from MAP or RAP in case PSK key was compromised or deleted on the controller intentionally.



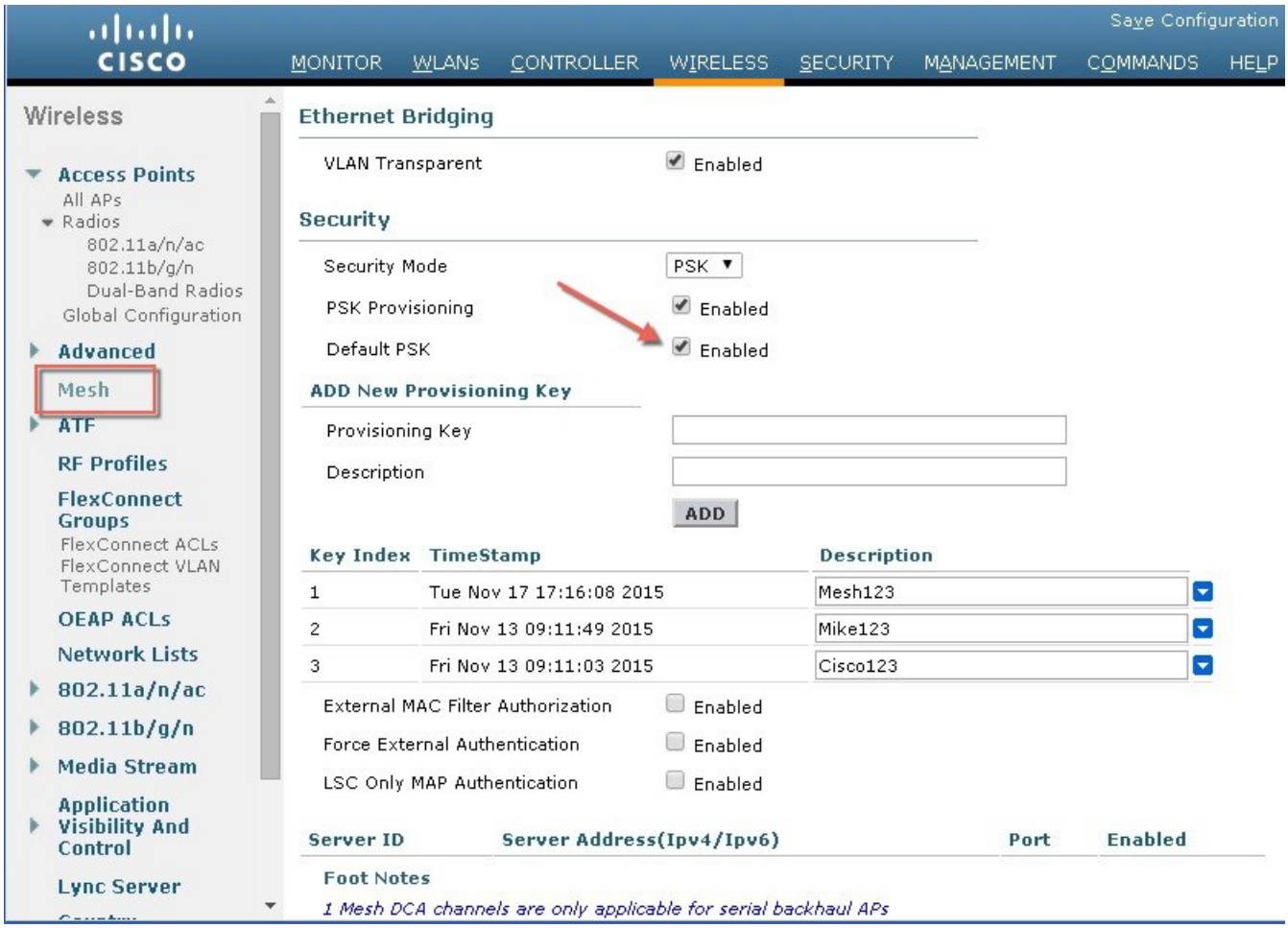
Step 6 If MAP accidently connected to the wrong network and obtained Key from there, admin has an option to delete that wrong PSK key. In addition, "Delete PSK" for PSK timestamp in WLC GUI interface can be used to remove a provisioned PSK of AP when it joined via EAP security. This option is sort of Mesh AP recovery option when AP has been stranded with staled or not valid PSK and EAP security was used to rejoin a stranded Mesh AP. When PSK key is deleted from the MAP, it will go back to using its default PSK key "cisco".

Note

- Configuring a PSK with passphrase ‘cisco’ does NOT mean that its equivalent to ‘Default cisco PSK’. Provisioned PSK works independent of ‘Default PSK’
- Deleting PSK key on the RAP does not apply unless RAP becomes a MAP.

However, note that if the PSK key is still configured on the controller and in turn on the RAP/MAP, then the MAP without a matching PSK key will not be able to connect to the Mesh network. For un-provisioned MAP to connect to the PSK enabled mesh network on the controller the Provisioning Window has to be enabled.

As shown in the example when Provisioning Window is manually enabled the MAP will be allowed to connect using default "cisco" PSK key and at the same time obtain new PSK key.



Note It is important for Mesh administrator to disable default provisioning Window so that MAPs with default PSK key don't connect to the provisioned Mesh network.

Note the following scenarios can cause Mesh AP to get stranded, make sure avoiding these configuration mistakes:

- Out-of-the-box APs trying to join using default PSK, but default or "PSK Provisioning Window" option is not enabled in WLC
- Forgotten the provisioned PSKs in WLC —always write description of the PSK to remind you later and save provisioned PSK or recovery will have to be performed on AP.

Mesh PSK Provisioning with Controllers In Mobility Group

In case there is a configuration of RAPs in the Mobility Group it is always advised to use the same PSK Keys or one of the 5 allowable PSK keys on all controllers in the Mobility Group; this way when MAPs coming from a different controllers they will be able to authenticate. By looking at the time stamp of the PSK you can find out where the MAP and PSK Key came from.

The following are recommendations when configuring Mesh APs with PSK or EAP security in a multi-controller configuration:

- All Controllers should have the same PSKs. WLCs with different keys will result in unexpected behavior if RAPs and MAPs move between them, and may even cause extended outages.
- All controllers should be set for the same security method – mixed EAP and PSK (with provisioning enabled and PSK(s) created) is not recommended..

  All controllers should be set for the same security method – mixed EAP and PSK (with provisioning enabled and PSK(s) created) is not recommended

CLI Commands for PSK Provisioning

- **config mesh security psk provisioning** {**enable** | **disable**}
- **config mesh security psk provisioning key** *pre-shared-key*
- **config mesh security psk provision window** {**enable** | **disable**}
- **config mesh security psk provisioning delete_psk** {**ap** *ap-name* |**wlc** *psk_index*}

Configuring Global Mesh Parameters

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

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

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

Configuring Global Mesh Parameters (GUI)

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

Step 1 Choose **Wireless > Mesh**.

Step 2 Modify the mesh parameters as appropriate.

Table 24: Global Mesh Parameters

Parameter	Description
Range (RootAP to MeshAP)	The optimum distance (in feet) that should exist between the root access point (RAP) and the mesh access point (MAP). This global parameter applies to all mesh access points when they join the controller and all existing mesh access points in the network. **Range:** 150 to 132,000 feet **Default:** 12,000 feet **Note** After this feature is enabled, all mesh access points reboot.
IDS (Rogue and Signature Detection)	When you enable this feature, IDS reports are generated for all traffic on the client access only and not on the backhaul. When you disable this feature, no IDS reports are generated, which preserves bandwidth on the backhaul. You have to use the following command to enable or disable it on the mesh APs: `config mesh ids-state {enable | disable}` **Note** 2.4GHz IDS is activated with the global IDS settings on the controller.
Backhaul Client Access	**Note** This parameter applies to mesh access points with two or more radios (1552, 1532, 1240, 1130, and 11n indoor mesh APs). When Backhaul Client Access is enabled, it allows wireless client association over the backhaul radio. Generally, backhaul radio is a 5 GHz radio for most of the mesh access points. This means that a backhaul radio can carry both backhaul traffic and client traffic. When Backhaul Client Access is disabled, only backhaul traffic is sent over the backhaul radio and client association is only over the second radio(s). **Default:** Disabled **Note** After this feature is enabled, all mesh access points reboot.

Parameter	Description
VLAN Transparent	This feature determines how a mesh access point handles VLAN tags for Ethernet bridged traffic. **Note** See the Configuring Advanced Features section for overview and additional configuration details. If VLAN Transparent is enabled, then VLAN tags are not handled and packets are bridged as untagged packets. **Note** No configuration of Ethernet ports is required when VLAN transparent is enabled. The Ethernet port passes both tagged and untagged frames without interpreting the frames. If VLAN Transparent is disabled, then all packets are handled according to the VLAN configuration on the port (trunk, access, or normal mode). **Note** If the Ethernet port is set to Trunk mode, then Ethernet VLAN tagging must be configured. See the Enabling Ethernet Bridging (GUI) section. **Note** For an overview of normal, access, and trunk Ethernet port use, see the Ethernet Port Notes section. **Note** To use VLAN tagging, you must uncheck the VLAN Transparent check box. **Note** VLAN Transparent is enabled as a default to ensure a smooth software upgrade from 4.1.192.xxM releases to release 5.2. Release 4.1.192.xxM does not support VLAN tagging. **Default:** Enabled.
Security Mode	Defines the security mode for mesh access points: Pre-Shared Key (PSK) or Extensible Authentication Protocol (EAP). **Note** EAP must be selected if external MAC filter authorization using a RADIUS server is configured. **Note** Local EAP or PSK authentication is performed within the controller if the External MAC Filter Authorization parameter is disabled (check box unchecked). **Options:** PSK or EAP **Default:** EAP

Parameter	Description

External MAC Filter Authorization	MAC filtering uses the local MAC filter on the controller by default.
	
	When external MAC filter authorization is enabled, if the MAC address is not found in the local MAC filter, then the MAC address in the external RADIUS server is used.
	
	This protects your network against rogue mesh access points by preventing mesh access points that are not defined on the external server from joining.
	
	Before employing external authentication within the mesh network, the following configuration is required:
	
	• The RADIUS server to be used as an AAA server must be configured on the controller.
	
	• The controller must also be configured on the RADIUS server.
	
	• The mesh access point configured for external authorization and authentication must be added to the user list of the RADIUS server.
	
	  • For remote authorization and authentication, EAP-FAST uses the manufacturer's certificate (CERT) to authenticate the child mesh access point. Additionally, this manufacturer certificate-based identity serves as the username for the mesh access point in user validation.
	
	  • For IOS-based mesh access points (1130, 1240), the platform name of the mesh access point is located in front of its Ethernet address within the certificate; therefore, their username for external RADIUS servers is *platform_name_string–Ethernet MAC address* such as *c1520-001122334455*.
	
	• The certificates must be installed and EAP-FAST must be configured on the RADIUS server.
	
	Note When this capability is not enabled, by default, the controller authorizes and authenticates mesh access points using the MAC address filter.
	
	Default: Disabled.

Parameter	Description
Force External Authorization	When enabled along with *EAP* and *External MAC Filter Authorization* parameters, external authorization and authentication of mesh access points is done by default by an external RADIUS server (such as Cisco 4.1 and later). The RADIUS server overrides local authentication of the MAC address by the controller which is the default. **Default:** Disabled.

Step 3 Click **Apply**.

Step 4 Click **Save Configuration**.

Configuring Global Mesh Parameters (CLI)

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



Note See the Configuring Global Mesh Parameters (GUI) section for descriptions, valid ranges, and default values of the parameters used in the CLI commands.

Step 1 To specify the maximum range (in feet) of all mesh access points in the network, enter this command:

config mesh range *feet*

To see the current range, enter the **show mesh range** command.

Step 2 To enable or disable IDS reports for all traffic on the backhaul, enter this command:

config mesh ids-state {**enable** | **disable**}

Step 3 To specify the rate (in Mbps) at which data is shared between access points on the backhaul interface, enter this command:

config ap bhrate {*rate* | **auto**} *Cisco_AP*

Step 4 To enable or disable client association on the primary backhaul (802.11a) of a mesh access point, enter these commands:

config mesh client-access {**enable** | **disable**}

config ap wlan {**enable** | **disable**} **802.11a** *Cisco_AP*

config ap wlan {**add** | **delete**} **802.11a** *wlan_id Cisco_AP*

Step 5 To enable or disable VLAN transparent, enter this command:

config mesh ethernet-bridging VLAN-transparent {**enable** | **disable**}

Step 6 To define a security mode for the mesh access point, enter one of the following commands:

a) To provide local authentication of the mesh access point by the controller, enter this command:

config mesh security {**eap** | **psk**}

b) To store the MAC address filter in an external RADIUS server for authentication instead of the controller (local), enter these commands:

config macfilter mac-delimiter colon

config mesh security rad-mac-filter enable

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

c) To provide external authentication on a RADIUS server and define a local MAC filter on the controller, enter these commands:

config mesh security eap

config macfilter mac-delimiter colon

config mesh security rad-mac-filter enable

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

config mesh security force-ext-auth enable

d) To provide external authentication on a RADIUS server using a MAC username (such as c1520-123456) on the RADIUS server, enter these commands:

config macfilter mac-delimiter colon

config mesh security rad-mac-filter enable

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

config mesh security force-ext-auth enable

Step 7 To save your changes, enter this command:

save config

Viewing Global Mesh Parameter Settings (CLI)

Use these commands to obtain information on global mesh settings:

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

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

```
(Cisco Controller)> show mesh client-access
Backhaul with client access status: enabled
```

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

```
(Cisco Controller)> show mesh ids-state
Outdoor Mesh IDS(Rogue/Signature Detect): .... Disabled
```

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

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

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

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

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

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

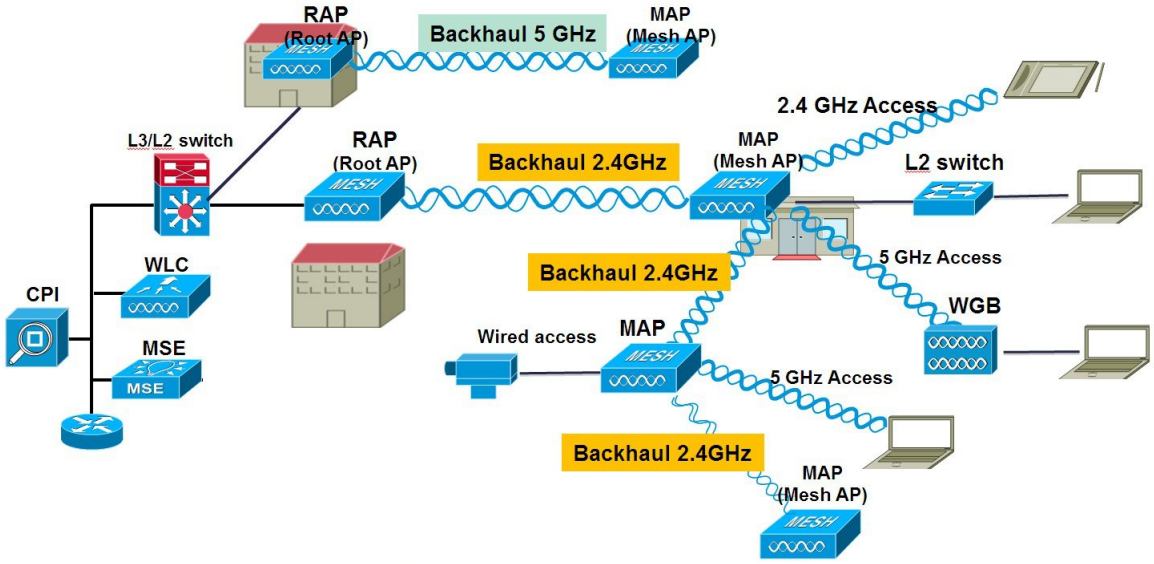
Mesh Backhaul at 5 and 2.4 Ghz in Release 8.2

Prior to release 8.2 Wireless Mesh Backhaul was supported only at 5GHz. In release 8.2 Wireless Mesh backhaul is supported at 5 and 2.4 GHz.

In certain countries it is not allowed to use Mesh Network with 5 Ghz backhaul network or even in the courtiers when 5Ghz is permitted customer may prefer to use 2.4 Ghz radio frequencies to achieve much larger Mesh or Bridge distances.

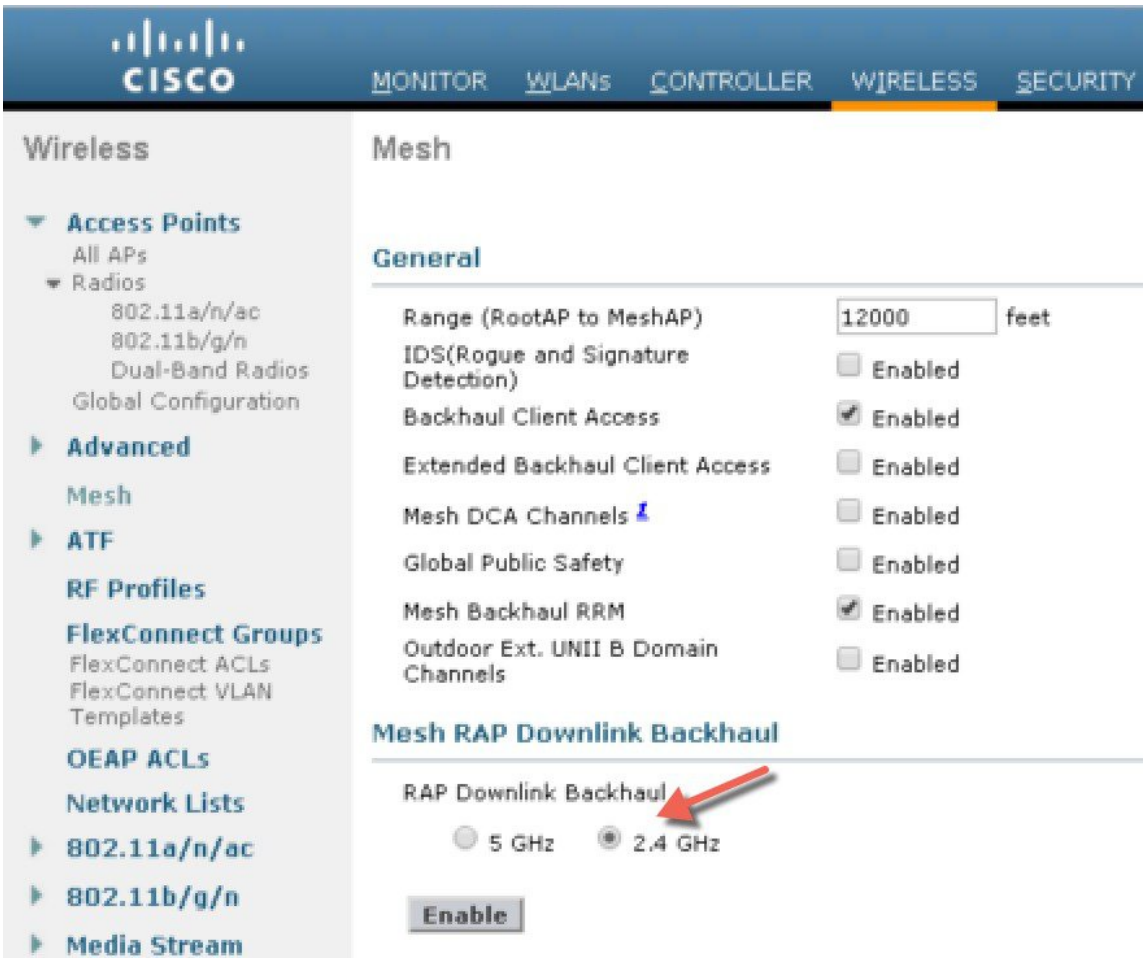
When a RAP gets change of the configuration from 5 to 2.4 Ghz that selection gets propagated from RAP to all MAPs and they will disconnect from 5Ghz network and get reconnected at 2.4 Ghz. Please note if configuring 2.4Ghz make sure all Controllers are configured with version 8.2 so that 2.4 Ghz backhaul is recognized.

Note Only RAPs are configured with the backhaul frequency of 5 or 2.4GHz. Once RAP is configured that frequency selection will propagate down the branch to all MAPs.



Step 1 To configure Mesh Backhaul to 2.4 Ghz one simple step is required on the controller. As illustrated configure the RAP Downlink Backhaul to 2.4 Ghz and hit Enable.

Note In the example below a Controller Global 2.4 GHz configuration is shown. When it is done on the global configuration it will apply to all Mesh RAPs. Chanel provisioning can be done also on individual RAP in that case the Chanel provisioning will apply only to that specific RAP branch of parents and children



From the CLI you can issue "show mesh ap tree" and "show mesh backhaul <ap-name> to see the backhaul connection.

```
(5520-MA1) >show mesh ap tree

 ========================================================
||   AP Name [Hop Counter, Link SNR, Bridge Group Name] ||
 ========================================================

[Sector 1]
----------
AP1572-7a7f.09c0[0,0,tme]
  |-AP1532-3546.f14c[1,37,tme]
  |-AP1532-3546.f678[1,28,tme]

--------------------------------------------------------
Number of Mesh APs.............................. 3
Number of RAPs.................................. 1
Number of MAPs.................................. 2
--------------------------------------------------------

(5520-MA1) >show mesh backhaul ?

<Cisco AP>     Enter the name of the Cisco AP.

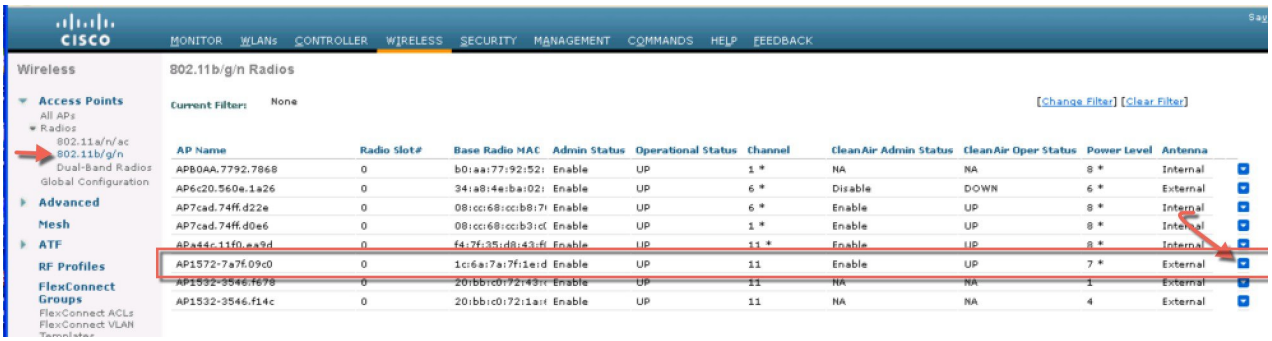
(5520-MA1) >show mesh backhaul AP1532-3546.f14c

Current Backhaul Slot(s)........................ 1

Basic Attributes for Slot  1
    Radio Type.................................. RADIO_TYPE_80211n-5
    Radio Subband............................... RADIO_SUBBAND_ALL
    Radio Role.................................. UPDOWNLINK ACCESS
    Administrative State ....................... ADMIN_ENABLED
    Operation State ............................ UP
      Current Tx Power Level ................... 1
      Current Channel ..........................  149
      Antenna Type................................ EXTERNAL_ANTENNA
      External Antenna Gain (in .5 dBm units).... 0

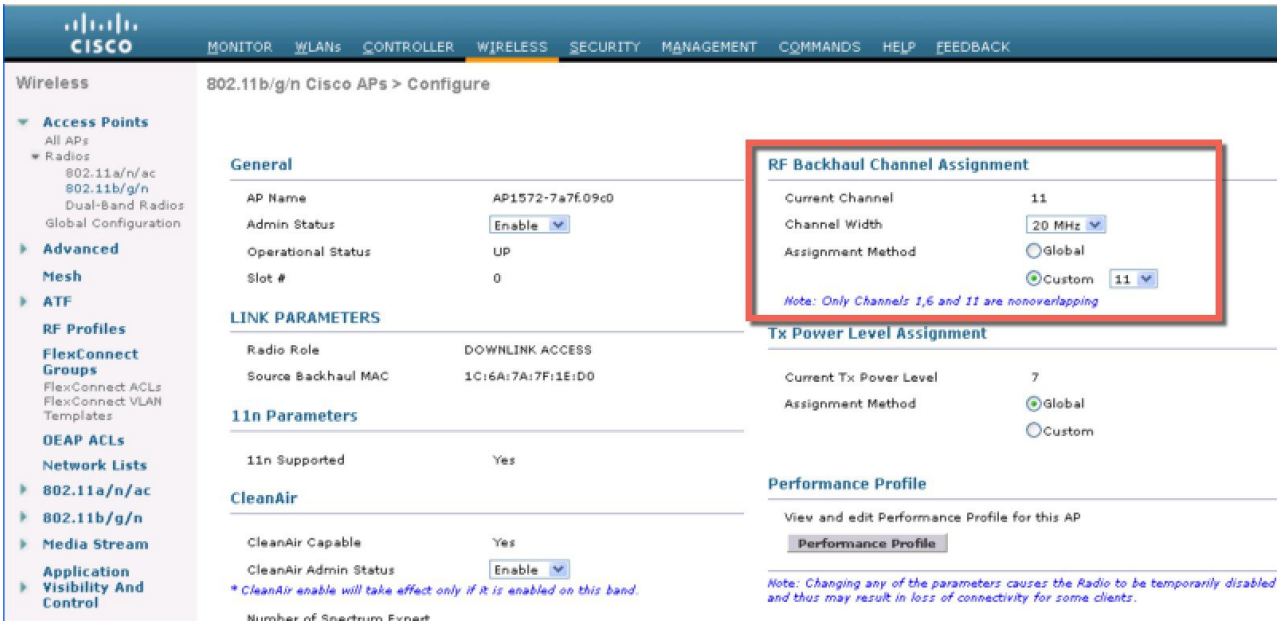
(5520-MA1) >
```

Step 2 On the RAP the channel has to be changed to 2.4GHz and channel has to be custom selected and that selection will be propagated to all MAPs and "children" in the Branch of that RAP.



After Channel is selected under the Custom option that channel will be used for the RAP Backhaul.

Note RAPs can participate in the RRM process with other RAPs in the same RF domain, however MAP only inherit the same channel from RAP and stick with it.



After the Channel change on the RAP as illustrated in the example below, the channel on the MAP has changed to CH11 in 2.4 GHz band.

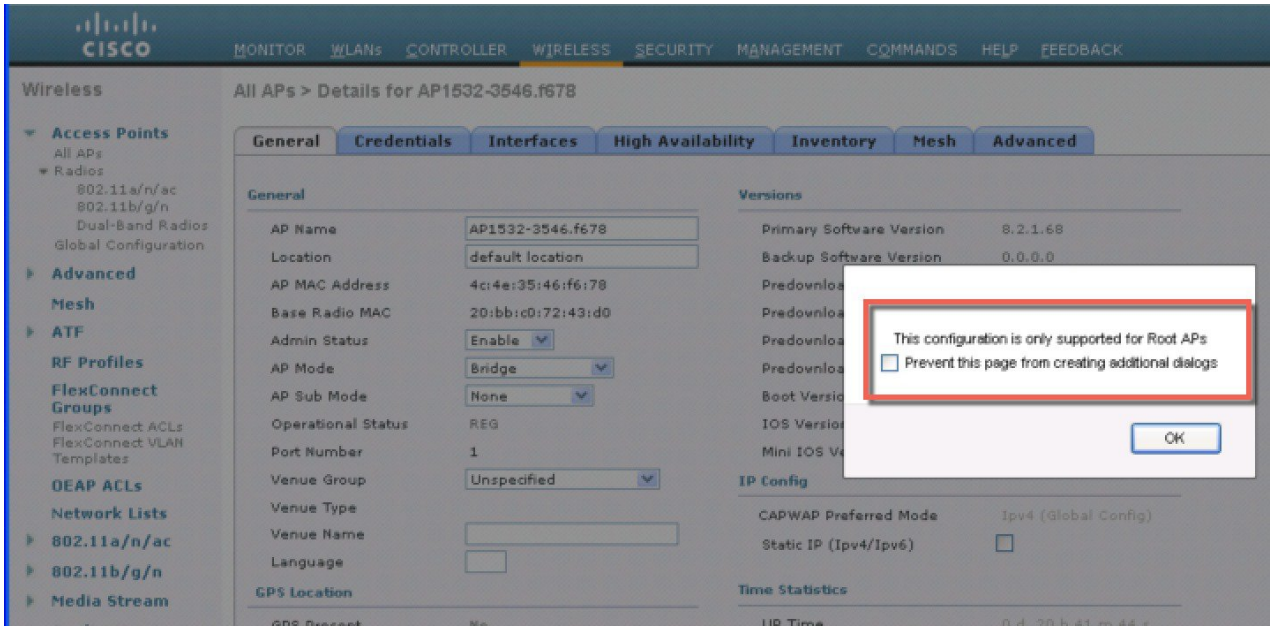
Example of the MAP CLI command: show mesh backhaul <ap-name>

```
(5520-MA1) >show mesh backhaul AP1572-7a7f.09c0

Current Backhaul Slot(s)..................... 0

Basic Attributes for Slot  0
    Radio Type.............................. RADIO_TYPE_80211n-2.4
    Radio Role.............................. DOWNLINK ACCESS
    Administrative State ................... ADMIN_ENABLED
    Operation State ........................ UP
      Current Tx Power Level ............... 7
      Current Channel ...................... 11
      Antenna Type.......................... EXTERNAL_ANTENNA
      External Antenna Gain (in .5 dBm units).... 0
```

If for example you would try to change the Backhaul channel on the MAP you will get an error message since this functionality is not supported on the MAPs. MAPs and “map children” receive their Channel assignments from the upstream parent RAP. An example of the error message from the MAP is as shown.



Backhaul Client Access

When Backhaul Client Access is enabled, it allows wireless client association over the backhaul radio. The backhaul radio is a 5-GHz radio. This means that a backhaul radio can carry both backhaul traffic and client traffic.

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

Note Backhaul Client Access is disabled by default. After this feature is enabled, all mesh access points, except subordinate AP and its child APs in Daisy-chained deployment, reboot.

This feature is applicable to mesh access points with two radios (1552, 1532, 1540, 1560, 1572, and Indoor APs in Bridge mode).

Configuring Backhaul Client Access (GUI)

Step 1 Choose **Wireless** > **Mesh** to navigate to the **Mesh** page.

Step 2 In the **General** section, check the **Backhaul Client Access** check box.

Step 3 Save the configuration.

What to do next

In a Flex+Bridge deployment, after you enable Backhaul Client Access globally, for the 5-GHz radios to beacon as expected, you must enable the **Install mapping on radio backhaul** option for the root APs operating in Flex+Bridge mode.

For more information about enabling the **Install mapping on radio backhaul** option, see the "Configuring Flex+Bridge Mode (GUI)" section.

Configuring Backhaul Client Access (CLI)

Use the following command to enable Backhaul Client Access:

```
(Cisco Controller)> config mesh client-access enable
```

The following message is displayed:

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

What to do next

In a Flex+Bridge deployment, after you enable Backhaul Client Access globally, for the 5-GHz radios to beacon as expected, you must enable the **Install mapping on radio backhaul** option for the root APs operating in Flex+Bridge mode.

For more information about enabling the **Install mapping on radio backhaul** option, see the "Configuring Flex+Bridge Mode (CLI)" section.

Configuring Local Mesh Parameters

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

- Backhaul Data Rate.
- Ethernet Bridging.
- Bridge Group Name.
- Workgroup Bridge.
- Power and Channel Setting.
- Antenna Gain Settings.
- Dynamic Channel Assignment.

Configuring Wireless Backhaul Data Rate

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

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

Data rates also affect the RF coverage and network performance. Lower data rates, for example 6 Mbps, can extend farther from the access point than can higher data rates, for example 1300 Mbps. As a result, the data rate affects cell coverage and consequently the number of access points required. Different data rates are achieved by sending a more redundant signal on the wireless link, allowing data to be easily recovered from noise. The number of symbols sent out for a packet at the 1-Mbps data rate is higher than the number of symbols used for the same packet at 11 Mbps. Therefore, sending data at the lower bit rates takes more time than sending the equivalent data at a higher bit rate, resulting in reduced throughput.

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

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

We recommend that you configure the mesh backhaul to Auto.

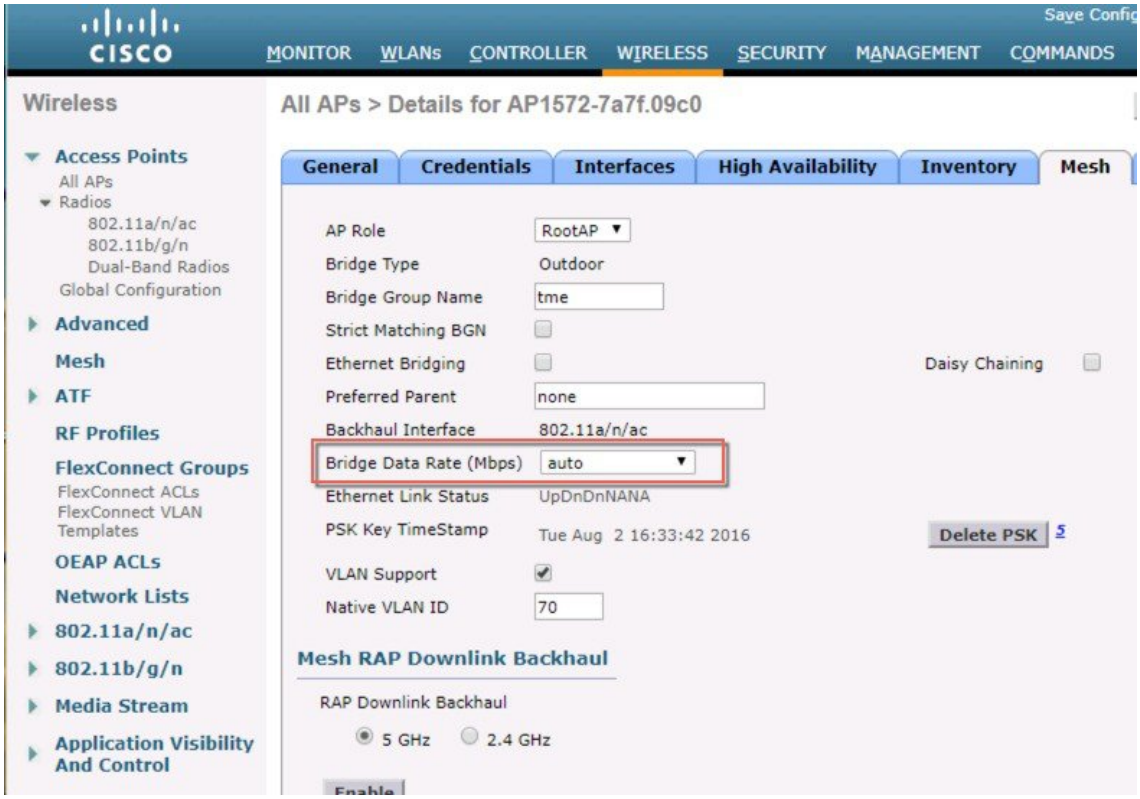
For example, if mesh backhaul chose 48 Mbps, then this decision is taken after ensuring that we cannot use 54 Mbps as there is not enough SNR for 54 and not because some just turned the microwave oven on which affects all rates.

A lower bit rate might allow a greater distance between MAPs, but there are likely to be gaps in the WLAN client coverage, and the capacity of the backhaul network is reduced. An increased bit rate for the backhaul

network either requires more MAPs or results in a reduced SNR between MAPs, limiting mesh reliability and interconnection.

This figure shows the RAP using the "auto" backhaul data rate, and it is currently using 54 Mbps with its child MAP.

Figure 39: Bridge Rate Set to Auto



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

Related Commands

Use these commands to obtain information about backhaul:

Command	Description
config ap bhrate—Configures the Cisco Bridge backhaul Tx rate. The syntax is as follows: `(controller) > config ap bhrate backhaul-rate ap-name`	

Command	Description

Note Preconfigured data rates for each AP (RAP=18 Mbps, MAP1=36 Mbps) are preserved after the upgrade to 6.0 or later software releases.??Before you upgrade to the 6.0 release, if you have the backhaul data rate configured to any data rate, then the configuration is preserved.

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

```
(controller) > config ap bhrate 36000 HPRAP1
```

show ap bhrate—Displays the Cisco Bridge backhaul rate.

The syntax is as follows:

```
(controller) > show ap bhrate ap-name
```

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

Example:

```
(controller) > show mesh neigh summary HPRAP1

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

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

Configuring Ethernet Bridging

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

When Ethernet bridging is enabled:

- VLAN ID 0 can be configured as a native VLAN and an access VLAN, but not as non-native VLAN.
- All native VLANs can be configured as a non-native VLANs also and vice-versa.
- Deleting a native VLAN from the allowed VLAN list does not interfere with the native VLAN.
- An old native VLAN will not be automatically added to the allowed VLAN list.

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

- Spanning Tree Protocol (STP)
- Address Resolution Protocol (ARP)
- Control and Provisioning of Wireless Access Points (CAPWAP)
- Bootstrap Protocol (BOOTP) packets

Enable Spanning Tree Protocol (STP) on all connected switch ports to avoid Layer 2 looping.

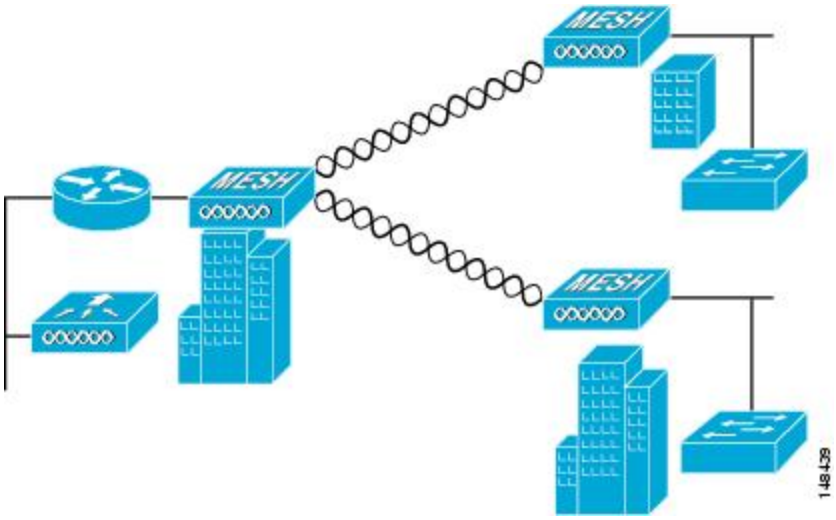
Ethernet bridging has to be enabled for two scenarios:

1. When you want to use the mesh nodes as bridges.

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

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

Figure 40: Point-to-Multipoint Bridging



Enabling Ethernet Bridging (GUI)

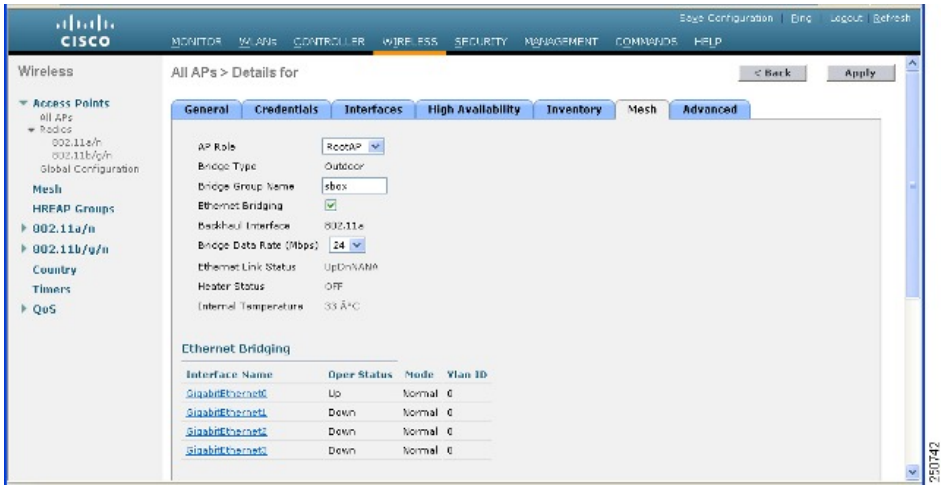
To enable Ethernet bridging on a RAP or MAP using the GUI, follow these steps:

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

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

Step 3 At the details page, select the **Mesh** tab (see Figure 41: All APs > Details for (Mesh) Page, on page 110).

Figure 41: All APs > Details for (Mesh) Page



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

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

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

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

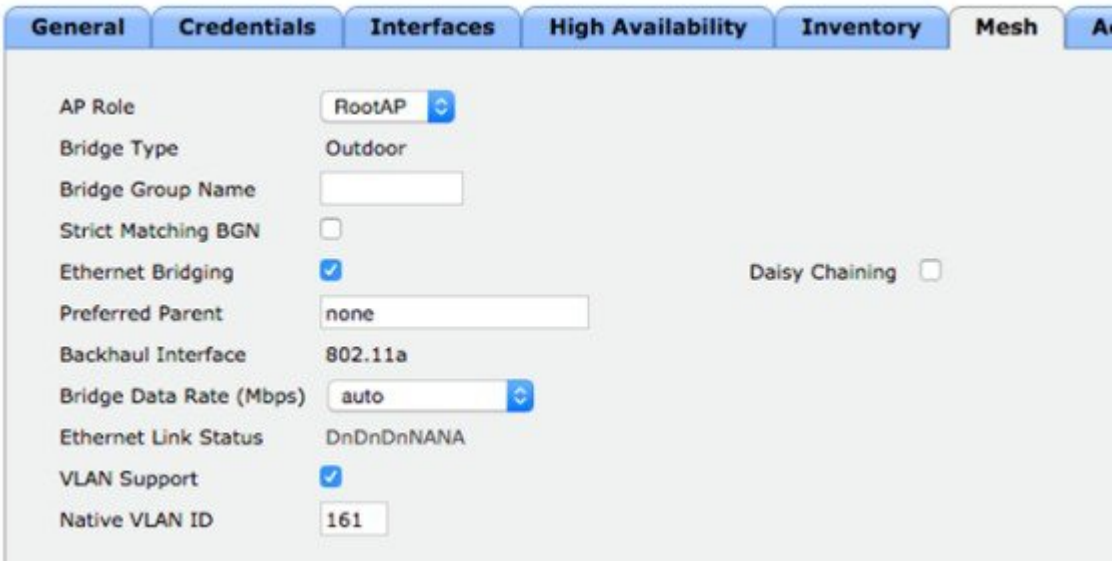
Configuring Native VLAN (GUI)

Note Prior to 8.0, the Native VLAN on the wired backhaul was set as VLAN 1. Starting with the 8.0 release, the Native VLAN can be set.

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

Step 2 Choose the mesh access point on which you would like to configure the Native VLAN.

Step 3 Check the **VLAN Support** checkbox on the AP.



Step 4 Assign a Native VLAN.

Note It is important that this Native VLAN matches the Native VLAN configured on the switch port of the connected switch.

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

Configuring Native VLAN (CLI)

Note Prior to 8.0, the Native VLAN on the wired backhaul was set as VLAN 1. Starting with the 8.0 release, the Native VLAN can be set.

1. Set the Native VLAN on the wired backhaul port using the command **config ap vlan-trunking native *vlan-id ap-name***.

   This applies the Native VLAN configuration to the access point.

Configuring Bridge Group Names

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

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

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

When Strict Match BGN is enabled on the mesh AP, it will scan ten times to find the matched BGN parent. After ten scans, if the AP does not find the parent with matched BGN, it will connect to the non-matched BGN and maintain the connection for 15 minutes. After 15 minutes the AP will again scan ten times and this cycle continues. The default BGN functionalities remain the same when Strict Match BGN is enabled.

Configuring Bridge Group Names (CLI)

Step 1 To set a bridge group name (BGN), enter this command:

config ap bridgegroupname set *group-name ap-name*

Note The mesh access point reboots after a BGN configuration.

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

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

show ap config general *ap-name*

Verifying Bridge Group Names (GUI)

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

Step 2 Click the **Mesh** tab. Details for the mesh access point including the BGN appears.

Configuring Power and Channel Settings

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

Configuring Power and Channel Settings (GUI)

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

Note Radio slots are displayed for each radio.

Step 2 Select **configure** from the Antenna drop-down list for the 802.11a/n radio. The Configure page is displayed.

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

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

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

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

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

Step 6 From the 802.11a/n Radios page, verify that channel assignments were made correctly.

Configuring Antenna Gain

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

Configuring Antenna Gain (GUI)

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

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

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

Note Only external antennas have configurable gain settings.

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

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

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

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

Configuring Antenna Gain (CLI)

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

config 802.11a antenna extAntGain *antenna_gain AP_name*

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

Configuring Dynamic Channel Assignment

Using the controller GUI, follow these steps to specify the channels that the dynamic channel assignment (DCA) algorithm considers when selecting the channels to be used for RRM scanning. This functionality is

helpful when you know that the clients do not support certain channels because they are legacy devices or they have certain regulatory restrictions.

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

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

a) Choose **Wireless > 802.11a/n or 802.11b/g/n > Network** to open the 802.11a (or 802.11b/g) Global Parameters page.
b) Deselect the **802.11a** (or **802.11b/g**) **Network Status** check box.
c) Click **Apply** to commit your changes.

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

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

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

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

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

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

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

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

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

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

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

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

- **High**—The DCA algorithm is highly sensitive to environmental changes.

The default value is **Medium**.

Table 25: DCA Sensitivity Thresholds

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

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

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

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

This page also shows the following nonconfigurable channel parameter settings:

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

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

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

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

Note These extended UNII-2 channels in the 802.11a band do not appear in the channel list: 100, 104, 108, 112, 116, 132, 136, and 140. If you have Cisco Aironet 1500 series mesh access points in the -E regulatory domain, you must include these channels in the DCA channel list before you start operation. If you are upgrading from a previous release, verify that these channels are included in the DCA channel list. To include these channels in the channel list, select the **Extended UNII-2 Channels** check box.

Step 12 If you are using AP1500s in your network, you must set the 4.9-GHz channels in the 802.11a band on which they are to operate. The 4.9-GHz band is for public safety client access traffic only. To choose a 4.9-GHz channel, select its check box in the Select column. To exclude a channel, deselect its check box.

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

Default:?802.11a—20, 26

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

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

a) Click **Wireless > 802.11a/n** or **802.11b/g/n > Network** to open the 802.11a (or 802.11b/g) Global Parameters page.
b) Select the **802.11a** (or **802.11b/g**) **Network Status** check box.
c) Click **Apply** to commit your changes.

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

Note To see why the DCA algorithm changed channels, click **Monitor** and then **View All** under Most Recent Traps. The trap provides the MAC address of the radio that changed channels, the previous channel and the new channel, the reason why the change occurred, the energy before and after the change, the noise before and after the change, and the interference before and after the change. Dynamic Channel Assignment on 5 GHz radio is supported only on outdoor access points in local or flexconnect mode.

Configuring Radio Resource Management on a Bridge Mode Access Point

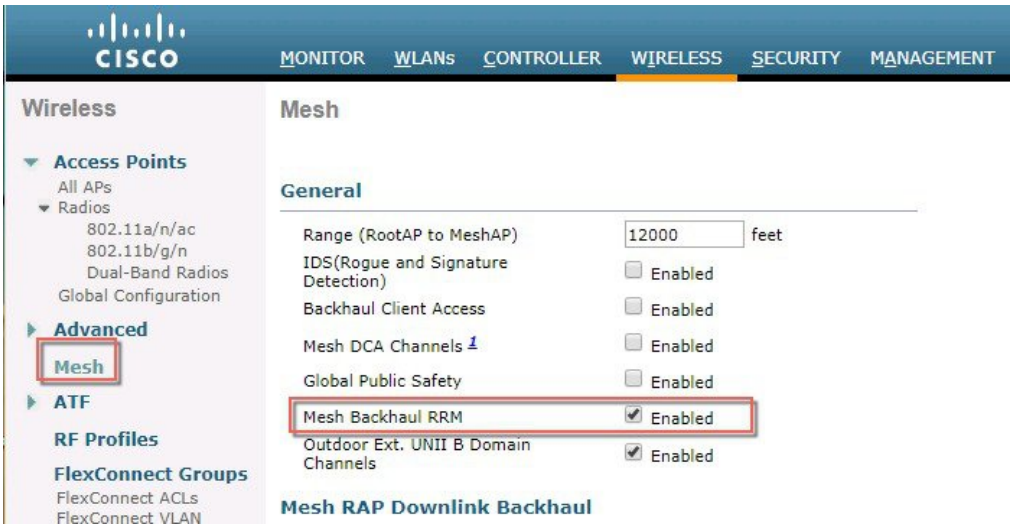
Radio Resource Management (RRM) can be enabled on the backhaul radio of a bridge mode access point if:

- AP is a root AP (RAP)
- RAP has a wired Ethernet link to a WLC
- RAP has no child Mesh APs connected to it

Once these conditions are met, full RRM will be established, including transmit power control (TPC), Dynamic Channel Assignment (DCA), and Coverage Hole Detection and Mitigation (CHDM). If a Mesh AP needs to re-join a RAP participating in RRM, the RAP will immediately stop all RRM functionality.

The following commands enable RRM:

- **config mesh backhaul rrm <*enable*|*disable*>** — To enable RRM on the mesh backhaul radio
- **Config mesh backhaul rrm <*auto-rf global*|*off*>** — To enable/disable dynamic channel assignment only



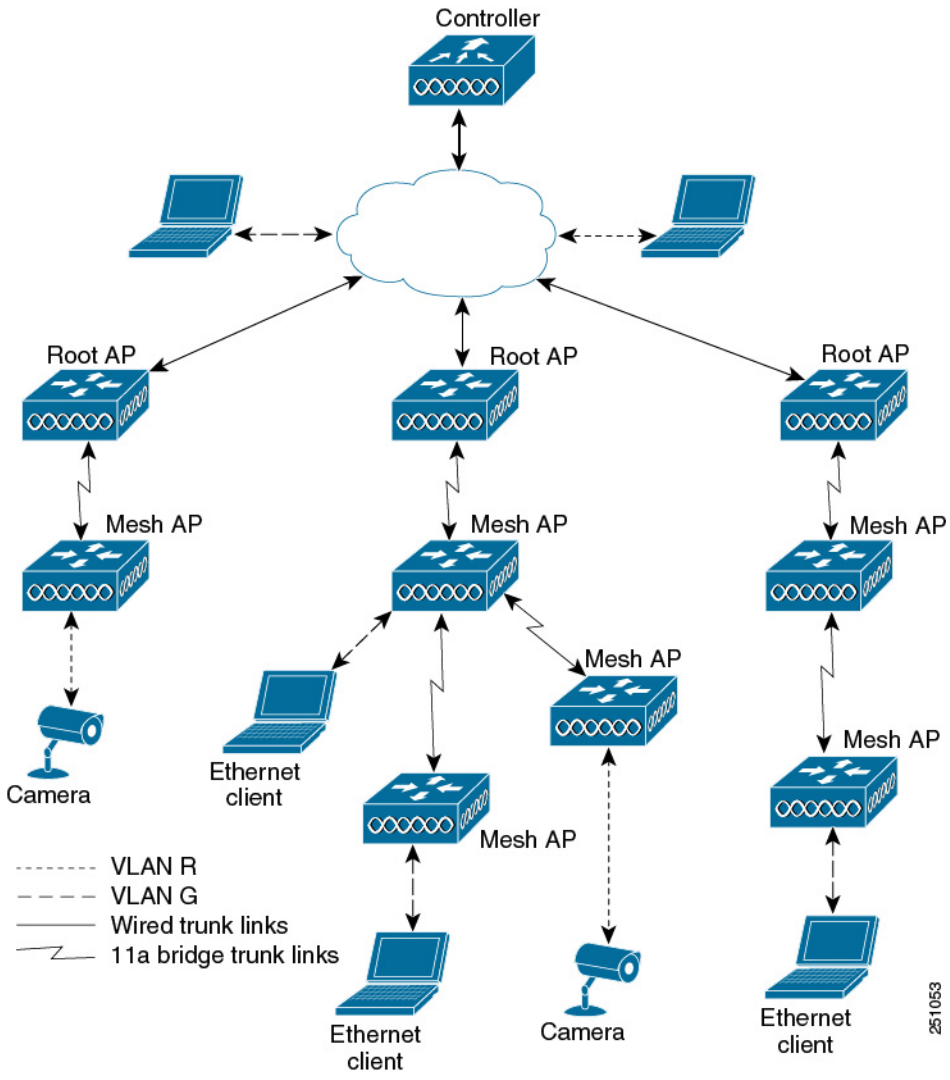
Configuring Advanced Features

Configuring Ethernet VLAN Tagging

Ethernet VLAN tagging allows specific application traffic to be segmented within a wireless mesh network and then forwarded (bridged) to a wired LAN (access mode) or bridged to another wireless mesh network (trunk mode).

A typical public safety access application that uses Ethernet VLAN tagging is the placement of video surveillance cameras at various outdoor locations within a city. Each of these video cameras has a wired connection to a MAP. The video of all these cameras is then streamed across the wireless backhaul to a central command station on a wired network.

Figure 42: Ethernet VLAN Tagging



Ethernet Port Notes

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

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

- Access Mode—In this mode, only untagged packets are accepted. All incoming packets are tagged with user-configured VLANs called access-VLANs.

  Use the access mode for applications in which information is collected from devices connected to the MAP, such as cameras or PCs, and then forwarded to the RAP. The RAP then applies tags and forwards traffic to a switch on the wired network.

- Trunk mode—This mode requires the user to configure a native VLAN and an allowed VLAN list (no defaults). In this mode, both tagged and untagged packets are accepted. Untagged packets are accepted and are tagged with the user-specified native VLAN. Tagged packets are accepted if they are tagged with a VLAN in the allowed VLAN list.

- Use the trunk mode for bridging applications such as forwarding traffic between two MAPs that reside on separate buildings within a campus.

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

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

In the 7.2 and 7.4 releases, the Root Access Point (RAP) native VLAN is not forwarded out of Mesh Access Point (MAP) Ethernet ports with Mesh Ethernet Bridging and VLAN Transparent enabled. This behavior is changed starting 7.6, where the native VLAN is forwarded by the MAP when VLAN transparent is enabled.

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

VLAN Registration

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

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

VLAN registration is summarized below:

1. Whenever an Ethernet port on a mesh access point is configured with a VLAN, the port requests its parent to support that VLAN.
2. If the parent is able to support the request, it creates a bridge group for the VLAN and propagates the request to its parent. This propagation continues until the RAP is reached.

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

Ethernet VLAN Tagging Guidelines

Follow these guidelines for Ethernet tagging:

- For security reasons, the Ethernet port on a mesh access point (RAP and MAP) is disabled by default. It is enabled by configuring Ethernet bridging on the mesh access point port.
- Ethernet bridging must be enabled on all the mesh access points in the mesh network to allow Ethernet VLAN tagging to operate.
- VLAN mode must be set as non-VLAN transparent (global mesh parameter). See the Configuring Global Mesh Parameters (CLI) section. VLAN transparent is enabled by default. To set as non-VLAN transparent, you must unselect the VLAN transparent option on the Wireless > Mesh page.
- VLAN tagging can only be configured on Ethernet interfaces as follows:
  - On AP1500s, three of the four ports can be used as secondary Ethernet interfaces: port 0-PoE in, port 1-PoE out, and port 3- fiber. Port 2 - cable cannot be configured as a secondary Ethernet interface.
  - In Ethernet VLAN tagging, port 0-PoE in on the RAP is used to connect to the trunk port of the switch of the wired network. Port 1-PoE out on the MAP is used to connect to external devices such as video cameras.
- Backhaul interfaces (802.11a radios) act as primary Ethernet interfaces. Backhauls function as trunks in the network and carry all VLAN traffic between the wireless and wired network. No configuration of primary Ethernet interfaces is required.
- For indoor mesh networks, the VLAN tagging feature functions as it does for outdoor mesh networks. Any access port that is not acting as a backhaul is *secondary* and can be used for VLAN tagging.
- VLAN tagging cannot be implemented on RAPs because the RAPs do not have a secondary Ethernet port, and the primary port is used as a backhaul. However, VLAN tagging can be enabled on MAPs with a single Ethernet port because the Ethernet port on a MAP does not function as a backhaul and is therefore a secondary port.
- No configuration changes are applied to any Ethernet interface acting as a backhaul. A warning displays if you attempt to modify the backhaul's configuration. The configuration is only applied after the interface is no longer acting as a backhaul.
- No configuration is required to support VLAN tagging on any 802.11a backhaul Ethernet interface within the mesh network as follows:

- This includes the RAP uplink Ethernet port. The required configuration occurs automatically using a registration mechanism.
- Any configuration changes to an 802.11a Ethernet link acting as a backhaul are ignored and a warning results. When the Ethernet link no longer functions as a backhaul, the modified configuration is applied.

- VLAN configuration is not allowed on port-02-cable modem port of AP1500s (wherever applicable). VLANs can be configured on ports 0 (PoE-in), 1 (PoE-out), and 3 (fiber).
- Up to 16 VLANs are supported on each sector. The cumulative number of VLANs supported by a RAP's children (MAP) cannot exceed 16.
- The switch port connected to the RAP must be a trunk:
  - The trunk port on the switch and the RAP trunk port must match.
  - The RAP must always connect to the native VLAN ID 1 on a switch. The RAP's primary Ethernet interface is by default the native VLAN of 1.
  - The switch port in the wired network that is attached to the RAP (port 0–PoE in) must be configured to accept tagged packets on its trunk port. The RAP forwards all tagged packets received from the mesh network to the wired network.
  - No VLANs, other than those destined for the mesh sector, should be configured on the switch trunk port.
- A configured VLAN on a MAP Ethernet port cannot function as a Management VLAN.
- Configuration is effective only when a mesh access point is in the CAPWAP RUN state and VLAN-Transparent mode is disabled.
- Whenever there roaming or a CAPWAP restart, an attempt is made to apply configuration again.

Enabling Ethernet VLAN Tagging (GUI)

You must enable Ethernet bridging before you can configure VLAN tagging.

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

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

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

Step 3 On the details page, select the **Mesh** tab.

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

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

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

  Select **access** from the mode drop-down list.

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

  Click **Apply**.

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

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

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

  Select **trunk** from the mode drop-down list.

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

  Click **Apply**.

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

  Specify a trunk VLAN ID for *outgoing* packets:

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

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

  Click **Add** to add the trunk VLAN ID to the allowed VLAN list. The newly added VLAN displays under the Configured VLANs section on the page.

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

Step 5 Click **Apply**.

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

Configuring Ethernet VLAN Tagging (CLI)

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

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

where *AP1500-MAP* is the variable *AP_name* and *50* is the variable *access_vlan ID*

To configure a RAP or MAP *trunk* port, enter this command:

config ap ethernet 0 mode trunk enable *AP1500-MAP 60*

where *AP1500-MAP* is the variable *AP_name* and *60* is the variable *native_vlan ID*

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

config ap ethernet 0 mode trunk add *AP1500-MAP3 65*

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

Viewing Ethernet VLAN Tagging Configuration Details (CLI)

Procedure

- To view VLAN configuration details for Ethernet interfaces on a specific mesh access point (*AP Name*) or all mesh access points (*summary*), enter this command:

  show ap config ethernet *ap-name*

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

  show mesh config

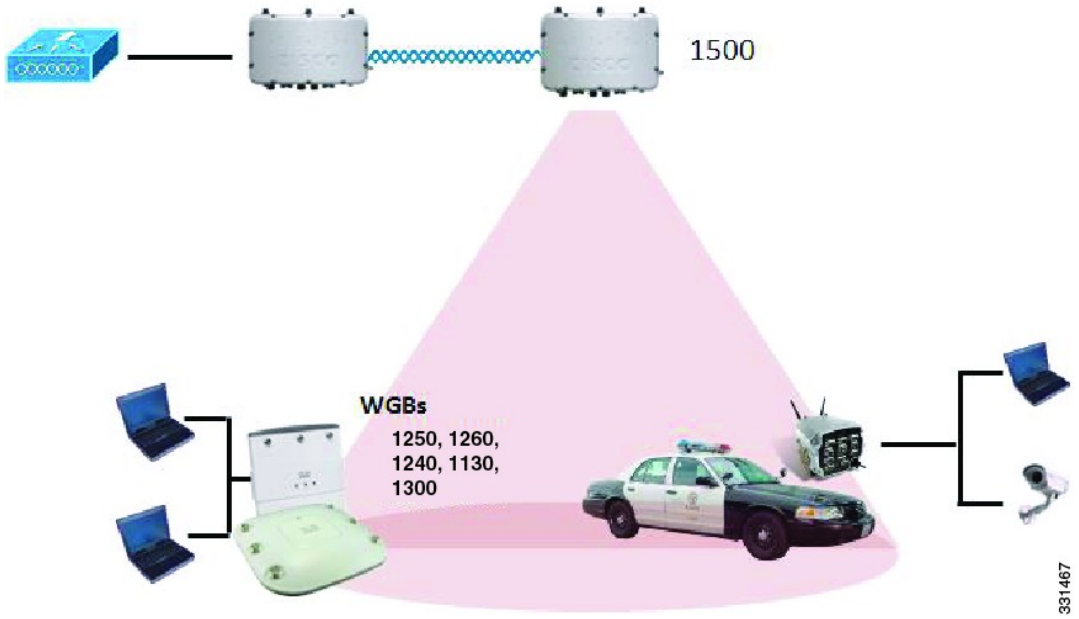
Workgroup Bridge Interoperability with Mesh Infrastructure

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

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

WGB association is supported on all radios of every mesh access point.

Figure 43: WGB Example



In the current architecture, while an autonomous AP functions as a workgroup bridge, only one radio interface is used for controller connectivity, Ethernet interface for wired client connectivity, and other radio interface for wireless client connectivity. dot11radio 1 (5 GHz) can be used to connect to a controller (using the mesh

infrastructure) and Ethernet interface for wired clients. dot11radio 0 (2.4 GHz) can be used for wireless client connectivity. Depending on the requirement, dot11radio 1 or dot11radio 0 can be used for client association or controller connectivity.

With the 7.0 release, a wireless client on the second radio of the WGB is not dissociated by the WGB upon losing its uplink to a wireless infrastructure or in a roaming scenario.

With two radios, one radio can be used for client access and the other radio can be used for accessing the access points. Having two independent radios performing two independent functions provides you better control and lowers the latency. Also, wireless clients on the second radio for the WGB do not get disassociated by the WGB when an uplink is lost or in a roaming scenario. One radio has to be configured as a Root AP (radio role) and the second radio has to be configured as a WGB (radio role).



Note If one radio is configured as a WGB, then the second radio cannot be a WGB or a repeater.

The following features are not supported for use with a WGB:

- Idle timeout
- Web authentication—If a WGB associates to a web-authentication WLAN, the WGB is added to the exclusion list, and all of the WGB-wired clients are deleted (web-authentication WLAN is another name for a guest WLAN).
- For wired clients behind the WGB, MAC filtering, link tests, and idle timeout

Configuring Workgroup Bridges

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

WGB association is supported on both the 2.4-GHz (802.11b/g) and 5-GHz (802.11a) radios on all Cisco APs.

Supported platforms are autonomous 1600, 1700, 2600, 2700, 3600, 3700, 1530, 1550, and 1570, which are configured as WGBs can associate with a mesh access point. See the “Cisco Workgroup Bridges” section in *Cisco Wireless LAN Controller Configuration Guide* for configuration steps at https://www.cisco.com/c/en/us/support/wireless/8500-series-wireless-controllers/products-installation-and-configuration-guides-list.html

The supported WGB modes and capacities are as follows:

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



Note If your mesh access point has two radios, you can only configure workgroup bridge mode on one of the radios. We recommend that you disable the second radio. Workgroup bridge mode is not supported on access points with three radios.

- Client mode WGB (BSS) is supported; however, infrastructure WGB is not supported. The client mode WGB is not able to trunk VLAN as in an infrastructure WGB.
- Multicast traffic is not reliably transmitted to WGB because no ACKs are returned by the client. Multicast traffic is unicast to infrastructure WGB, and ACKs are received back.
- If one radio is configured as a WGB in a Cisco IOS access point, then the second radio cannot be a WGB or a repeater.
- Mesh access points can support up to 200 clients including wireless clients, WGB, and wired clients behind the associated WGB.
- A WGB cannot associate with mesh access points if the WLAN is configured with WPA1 (TKIP) +WPA2 (AES), and the corresponding WGB interface is configured with only one of these encryptions (either WPA1 or WPA2):

Figure 44: WPA Security Settings for a WGB

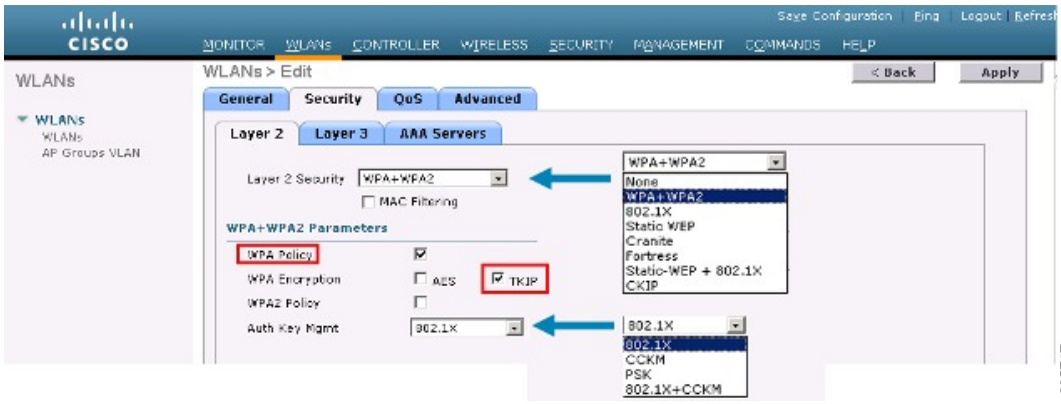
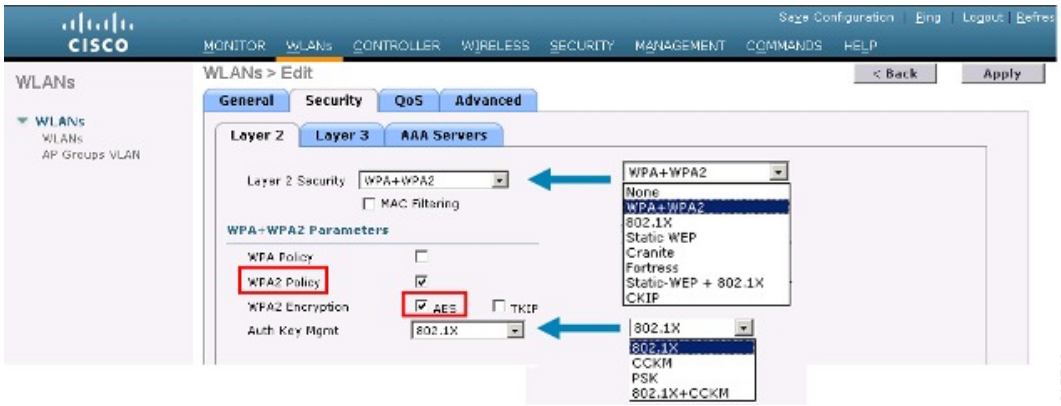


Figure 45: WPA-2 Security Settings for a WGB



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

Step 1 Choose **Monitor > Clients**.

Step 2 On the client summary page, click on the MAC address of the client or search for the client using its MAC address.

Step 3 In the page that appears, note that the client type is identified as a *WGB* (far right).

Figure 46: Clients are Identified as a WGB



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

- For a wireless client, the page seen in **Monitor** > **Clients** > **Detail Page (Wireless WGB Client)** is displayed.
- For a wired client, the page seen in **Monitor** > **Clients** > **Detail Page (Wireless WGB Client)** is displayed.

Figure 47: Monitor > Clients > Detail Page (Wireless WGB Client)

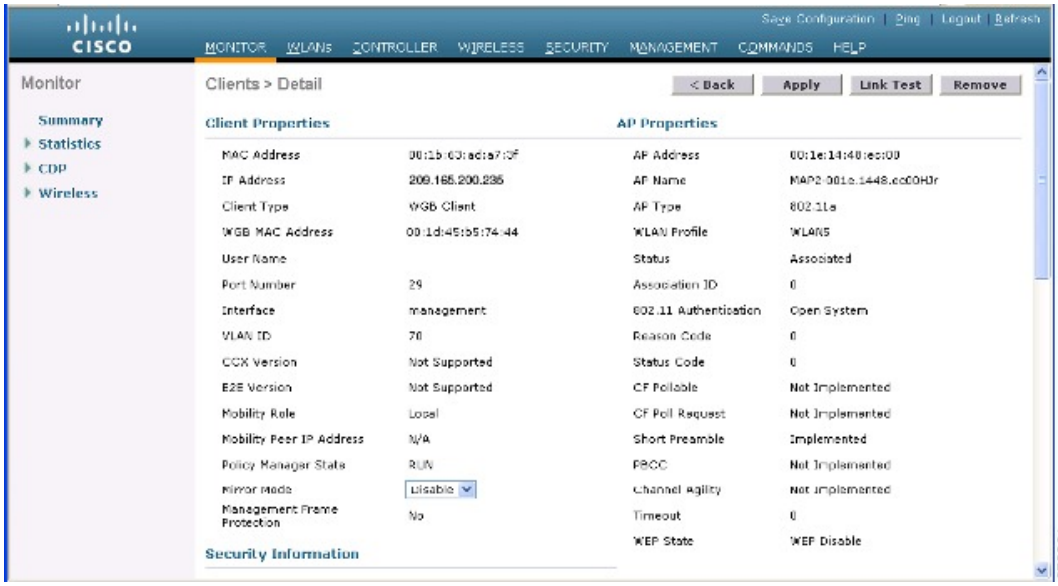
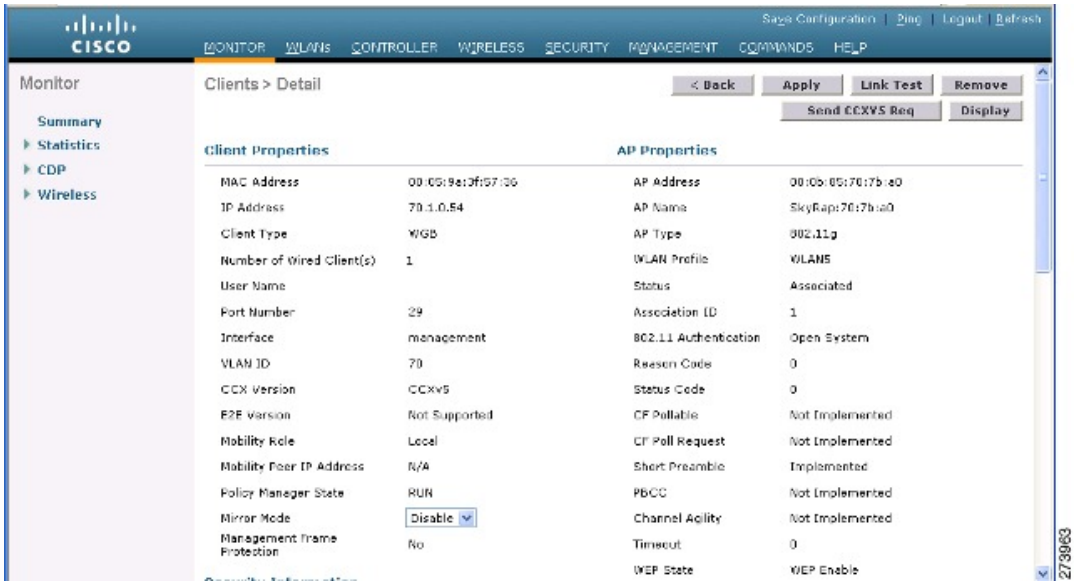


Figure 48: Monitor > Clients > Detail Page (Wired WGB Client)



Guidelines for Configuration

Follow these guidelines when you configure:

- We recommend using a 5-GHz radio for the uplink to Mesh AP infrastructure so you can take advantage of a strong client access on two 5-GHz radios available on mesh access points. A 5-GHz band allows more Effective Isotropic Radiated Power (EIRP) and is less polluted. In a two-radio WGB, configure 5-GHz radio (radio 1) mode as WGB. This radio will be used to access the mesh infrastructure. Configure the second radio 2.4-GHz (radio 0) mode as Root for client access.
- On the Autonomous access points, only one SSID can be assigned to the native VLAN. You cannot have multiple VLANs in one SSID on the autonomous side. SSID to VLAN mapping should be unique because this is the way to segregate traffic on different VLANs. In a unified architecture, multiple VLANs can be assigned to one WLAN (SSID).
- Only one WLAN (SSID) for wireless association of the WGB to the access point infrastructure is supported. This SSID should be configured as an infrastructure SSID and should be mapped to the native VLAN.
- A dynamic interface should be created in the controller for each VLAN configured in the WGB.
- A second radio (2.4-GHz) on the access point should be configured for client access. You have to use the same SSID on both radios and map to the native VLAN. If you create a separate SSID, then it is not possible to map it to a native VLAN, due to the unique VLAN/SSID mapping requirements. If you try to map the SSID to another VLAN, then you do not have multiple VLAN support for wireless clients.
- All Layer 2 security types are supported for the WLANs (SSIDs) for wireless client association in WGB.
- This feature does not depend on the AP platform. On the controller side, both mesh and nonmesh APs are supported.
- There is a limitation of 20 clients in the WGB. The 20-client limitation includes both wired and wireless clients. If the WGB is talking to autonomous access points, then the client limit is very high.

- The controller treats the wireless and wired clients behind a WGB in the same manner. Features such as MAC filtering and link test are not supported for wireless WGB clients from the controller.
- If required, you can run link tests for a WGB wireless client from an autonomous AP.
- Multiple VLANs for wireless clients associated to a WGB are not supported.
- Up to 16 multiple VLANs are supported for wired clients behind a WGB from the 7.0 release and later releases.
- Roaming is supported for wireless and wired clients behind a WGB. The wireless clients on the other radio will not be dissociated by the WGB when an uplink is lost or in a roaming scenario.

We recommend that you configure radio 0 (2.4 GHz) as a Root (one of the mode of operations for Autonomous AP) and radio 1 (5 GHz) as a WGB.

Configuration Example

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

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

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

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

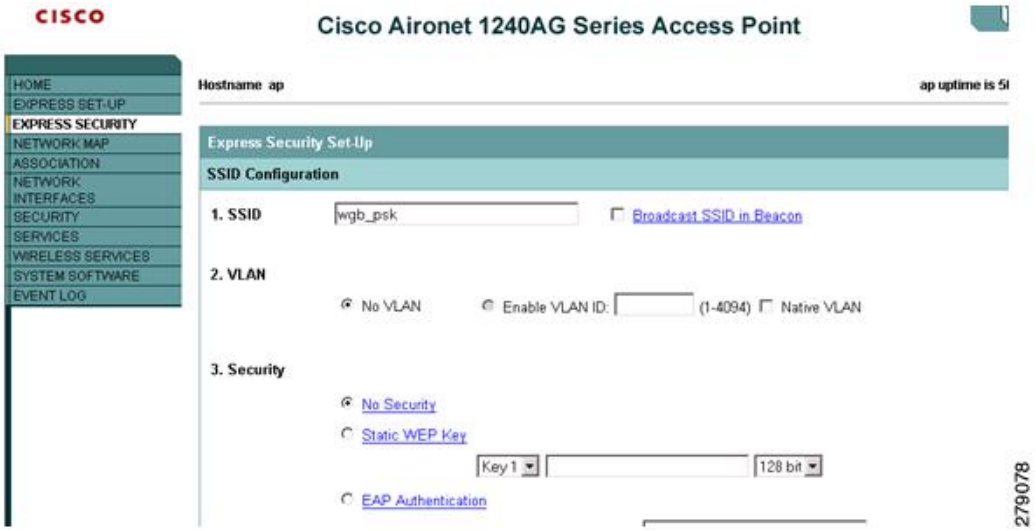
In the following example, one SSID (WGBTEST) is used in both radios, and the SSID is the infrastructure SSID mapped to NATIVE VLAN 51. All radio interfaces are mapped to bridge group -1.

```
WGB1#config t
WGB1(config)#interface Dot11Radio1.51
WGB1(config-subif)#encapsulation dot1q 51 native
WGB1(config-subif)#bridge-group 1
WGB1(config-subif)#exit
WGB1(config)#interface Dot11Radio0.51
WGB1(config-subif)#encapsulation dot1q 51 native
WGB1(config-subif)#bridge-group 1
WGB1(config-subif)#exit
WGB1(config)#dot11 ssid WGBTEST
WGB1(config-ssid)#VLAN 51
WGB1(config-ssid)#authentication open
WGB1(config-ssid)#infrastructiure-ssid
WGB1(config-ssid)#exit
WGB1(config)#interface Dot11Radio1
WGB1(config-if)#ssid WGBTEST
WGB1(config-if)#station-role workgroup-bridge
WGB1(config-if)#exit
WGB1(config)#interface Dot11Radio0
```

```
WGB1(config-if)#ssid WGBTEST
WGB1(config-if)#station-role root
WGB1(config-if)#exit
```

You can also use the GUI of an autonomous AP for configuration. From the GUI, subinterfaces are automatically created after the VLAN is defined.

Figure 49: SSID Configuration Page



WGB Association Check

Both the WGB association to the controller and the wireless client association to WGB can be verified by entering the **show dot11 associations client** command in autonomous AP.

```
WGB#show dot11 associations client

802.11 Client Stations on Dot11Radio1:

SSID [WGBTEST] :
```

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

From the controller, choose **Monitor > Clients**. The WGB and the wireless/wired client behind the WGB are updated and the wireless/wired client are shown as the WGB client.

Figure 50: Updated WGB Clients



Figure 51: Updated WGB Clients

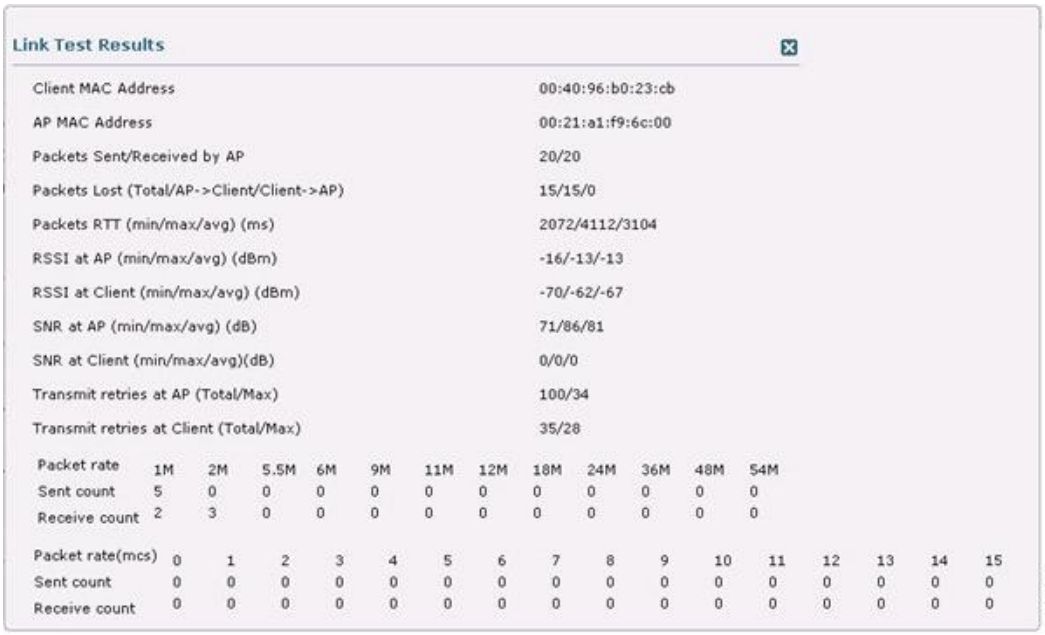


Figure 52: Updated WGB Clients



Link Test Result

Figure 53: Link Test Results



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

```
(Cisco Controller) > linktest client mac-address
```

Link tests from the controller are only limited to the WGB, and they cannot be run beyond the WGB from the controller to a wired or wireless client connected to the WGB. You can run link tests for the wireless client connected to the WGB from the WGB itself using the following command:

```
ap#dot11 dot11Radio 0 linktest target client-mac-address
Start linktest to 0040.96b8.d462, 100 512 byte packets
ap#
```

POOR (4% lost)	Time (msec)	Strength (dBm)		SNR Quality		Retries	
		In	Out	In	Out	In	Out
Sent: 100	Avg. 22	-37	-83	48	3	Tot. 34	35
Lost to Tgt: 4	Max. 112	-34	-78	61	10	Max. 10	5
Lost to Src: 4	Min. 0	-40	-87	15	3		

```
Rates (Src/Tgt)     24Mb 0/5  36Mb 25/0  48Mb 73/0  54Mb 2/91
Linktest Done in 24.464 msec
```

WGB Wired/Wireless Client

You can also use the following commands to know the summary of WGBs and clients associated with a Cisco lightweight access point:

```
(Cisco Controller) > show wgb summary
Number of WGBs..................................... 2
```

MAC Address	IP Address	AP Name	Status	WLAN	Auth	Protocol	Clients
00:1d:70:97:bd:e8	209.165.200.225	c1240	Assoc	2	Yes	802.11a	2
00:1e:be:27:5f:e2	209.165.200.226	c1240	Assoc	2	Yes	802.11a	5

```
(Cisco Controller) > show client summary

Number of Clients.................................. 7
```

MAC Address	AP Name	Status	WLAN/Guest-Lan	Auth	Protocol	Port	Wired
00:00:24:ca:a9:b4	R14	Associated	1	Yes	N/A	29	No
00:24:c4:a0:61:3a	R14	Associated	1	Yes	802.11a	29	No
00:24:c4:a0:61:f4	R14	Associated	1	Yes	802.11a	29	No
00:24:c4:a0:61:f8	R14	Associated	1	Yes	802.11a	29	No
00:24:c4:a0:62:0a	R14	Associated	1	Yes	802.11a	29	No
00:24:c4:a0:62:42	R14	Associated	1	Yes	802.11a	29	No
00:24:c4:a0:71:d2	R14	Associated	1	Yes	802.11a	29	No

```
(Cisco Controller) > show wgb detail 00:1e:be:27:5f:e2

Number of wired client(s): 5
```

MAC Address	IP Address	AP Name	Mobility	WLAN	Auth
00:16:c7:5d:b4:8f	Unknown	c1240	Local	2	No

00:21:91:f8:e9:ae	209.165.200.232	c1240	Local	2	Yes
00:21:55:04:07:b5	209.165.200.234	c1240	Local	2	Yes
00:1e:58:31:c7:4a	209.165.200.236	c1240	Local	2	Yes
00:23:04:9a:0b:12	Unknown	c1240	Local	2	No

Client Roaming

High-speed roaming of Cisco Compatible Extension (CX), version 4 (v4) clients is supported at speeds up to 70 miles per hour in outdoor mesh deployments. An example application might be maintaining communication with a terminal in an emergency vehicle as it moves within a mesh public network.

Three Cisco CX v4 Layer 2 client roaming enhancements are supported:

- Access point assisted roaming—Helps clients save scanning time. When a Cisco CX v4 client associates to an access point, it sends an information packet to the new access point listing the characteristics of its previous access point. Roaming time decreases when the client recognizes and uses an access point list built by compiling all previous access points to which each client was associated and sent (unicast) to the client immediately after association. The access point list contains the channels, BSSIDs of neighbor access points that support the client's current SSID(s), and time elapsed since disassociation.
- Enhanced neighbor list—Focuses on improving a Cisco CX v4 client's roam experience and network edge performance, especially when servicing voice applications. The access point provides its associated client information about its neighbors using a neighbor-list update unicast message.
- Roam reason report—Enables Cisco CX v4 clients to report the reason why they roamed to a new access point. It also allows network administrators to build and monitor a roam history.

Note Client roaming is enabled by default. For more information, see the Enterprise Mobility Design Guide at http://www.cisco.com/en/US/docs/solutions/Enterprise/Mobility/emob41dg/eMob4.1.pdf

WGB Roaming Guidelines

Follow these guidelines for WGB roaming:

- Configuring a WGB for roaming—If a WGB is mobile, you can configure it to scan for a better radio connection to a parent access point or bridge. Use the ap(config-if)#**mobile station period 3 threshold 50** command to configure the workgroup bridge as a mobile station.

  When you enable this setting, the WGB scans for a new parent association when it encounters a poor Received Signal Strength Indicator (RSSI), excessive radio interference, or a high frame-loss percentage. Using these criteria, a WGB configured as a mobile station searches for a new parent association and roams to a new parent before it loses its current association. When the mobile station setting is disabled (the default setting), a WGB does not search for a new association until it loses its current association.

- Configuring a WGB for Limited Channel Scanning—In mobile environments such as railroads, a WGB instead of scanning all the channels is restricted to scan only a set of limited channels to reduce the hand-off delay when the WGB roams from one access point to another. By limiting the number of channels, the WGB scans only those required channels; the mobile WGB achieves and maintains a continuous wireless LAN connection with fast and smooth roaming. This limited channel set is configured using the ap(config-if)#**mobile station scan** *set of channels*.

  This command invokes scanning to all or specified channels. There is no limitation on the maximum number of channels that can be configured. The maximum number of channels that can be configured is restricted only by the number of channels that a radio can support. When executed, the WGB scans only this limited channel set. This limited channel feature also affects the known channel list that the WGB receives from the access point to which it is currently associated. Channels are added to the known channel list only if they are also part of the limited channel set.

Configuration Example

The following example shows how to configure a roaming configuration:

```
ap(config)#interface dot11radio 1
ap(config-if)#ssid outside
ap(config-if)#packet retries 16
ap(config-if)#station role workgroup-bridge
ap(config-if)#mobile station
ap(config-if)#mobile station period 3 threshold 50
ap(config-if)#mobile station scan 5745 5765
```

Use the **no mobile station scan** command to restore scanning to all the channels.

Troubleshooting Tips

If a wireless client is not associated with a WGB, use the following steps to troubleshoot the problem:

1. Verify the client configuration and ensure that the client configuration is correct.
2. Check the **show bridge** command output in autonomous AP, and confirm that the AP is reading the client MAC address from the right interface.
3. Confirm that the subinterfaces corresponding to specific VLANs in different interfaces are mapped to the same bridge group.
4. If required, clear the bridge entry using the **clear bridge** command (remember that this command will remove all wired and wireless clients associated in a WGB and make them associate again).
5. Check the **show dot11 association** command output and confirm that the WGB is associated with the controller.
6. Ensure that the WGB has not exceeded its 20-client limitation.

In a normal scenario, if the **show bridge** and **show dot11 association** command outputs are as expected, wireless client association should be successful.

Configuring Voice Parameters in Indoor Mesh Networks

You can configure call admission control (CAC) and QoS on the controller to manage voice and video quality on the mesh network.

The indoor mesh access points are 802.11e capable, and QoS is supported on the local 2.4 and 5-Ghz access radio and the 2.4 and 5 Ghz access radio and the 2.4 and 5 Ghz backhaul radio. CAC is supported on the backhaul and the CCXv4 clients (which provides CAC between the mesh access point and the client)

Note Voice is supported only on indoor mesh networks. Voice is supported on a best-effort basis in the outdoors in a mesh network.

Call Admission Control

Call Admission Control (CAC) enables a mesh access point to maintain controlled quality of service (QoS) when the wireless LAN is experiencing congestion. The Wi-Fi Multimedia (WMM) protocol deployed in CCXv3 ensures sufficient QoS as long as the wireless LAN is not congested. However, to maintain QoS under differing network loads, CAC in CCXv4 or later is required.

Note CAC is supported in Cisco Compatible Extensions (CCX) v4 or later. See Chapter 6 of the *Cisco Wireless LAN Controller Configuration Guide* at http://www.cisco.com/en/US/docs/wireless/controller/7.0/configuration/guide/c70sol.html

Two types of CAC are available for access points: bandwidth-based CAC and load-based CAC. All calls on a mesh network are bandwidth-based, so mesh access points use only bandwidth-based CAC.

Bandwidth-based, or static CAC enables the client to specify how much bandwidth or shared medium time is required to accept a new call. Each access point determines whether it is capable of accommodating a particular call by looking at the bandwidth available and compares it against the bandwidth required for the call. If there is not enough bandwidth available to maintain the maximum allowed number of calls with acceptable quality, the mesh access point rejects the call.

Quality of Service and Differentiated Services Code Point Marking

Cisco supports 802.11e on the local access and on the backhaul. Mesh access points prioritize user traffic based on classification, and therefore all user traffic is treated on a best-effort basis.

Resources available to users of the mesh vary, according to the location within the mesh, and a configuration that provides a bandwidth limitation in one point of the network can result in an oversubscription in other parts of the network.

Similarly, limiting clients on their percentage of RF is not suitable for mesh clients. The limiting resource is not the client WLAN, but the resources available on the mesh backhaul.

Similar to wired Ethernet networks, 802.11 WLANs employ Carrier Sense Multiple Access (CSMA), but instead of using collision detection (CD), WLANs use collision avoidance (CA), which means that instead of each station trying to transmit as soon as the medium is free, WLAN devices will use a collision avoidance mechanism to prevent multiple stations from transmitting at the same time.

The collision avoidance mechanism uses two values called CWmin and CWmax. CW stands for contention window. The CW determines what additional amount of time an endpoint should wait, after the interframe space (IFS), to attend to transmit a packet. Enhanced distributed coordination function (EDCF) is a model that allows end devices that have delay-sensitive multimedia traffic to modify their CWmin and CWmax values to allow for statically greater (and more frequent) access to the medium.

Cisco access points support EDCF-like QoS. This provides up to eight queues for QoS.

These queues can be allocated in several different ways, as follows:

- Based on TOS / DiffServ settings of packets
- Based on Layer 2 or Layer 3 access lists
- Based on VLAN
- Based on dynamic registration of devices (IP phones)

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

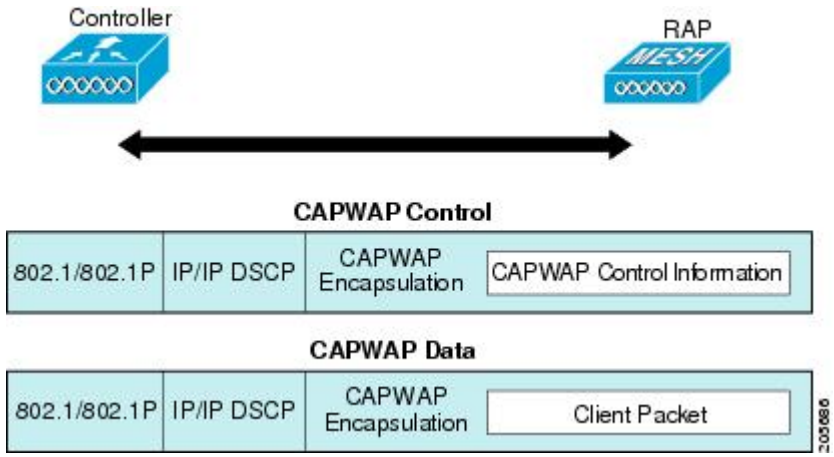
When the queue capacity has been reached, additional frames are dropped (tail drop).

Encapsulations

Several encapsulations are used by the mesh system. These encapsulations include CAPWAP control and data between the controller and RAP, over the mesh backhaul, and between the mesh access point and its client(s). The encapsulation of bridging traffic (noncontroller traffic from a LAN) over the backhaul is the same as the encapsulation of CAPWAP data.

There are two encapsulations between the controller and the RAP. The first is for CAPWAP control, and the second is for CAPWAP data. In the control instance, CAPWAP is used as a container for control information and directives. In the instance of CAPWAP data, the entire packet, including the Ethernet and IP headers, is sent in the CAPWAP container.

Figure 54: Encapsulations

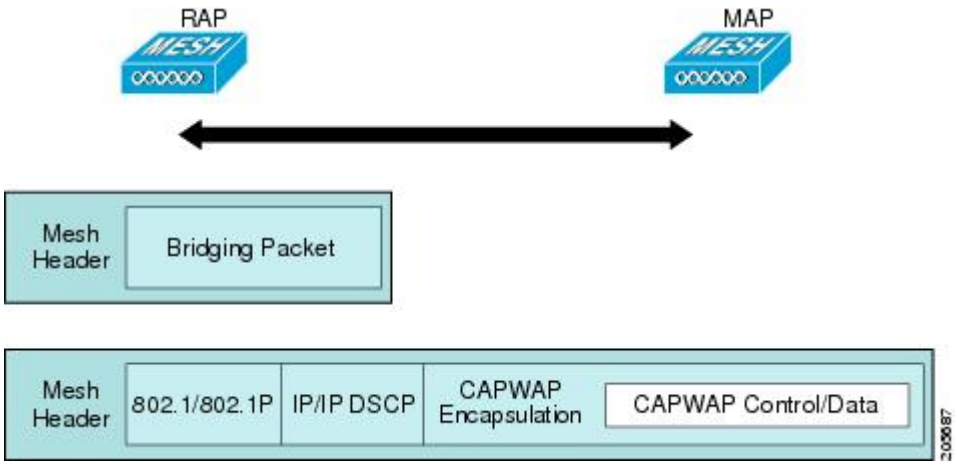


For the backhaul, there is only one type of encapsulation, encapsulating mesh traffic. However, two types of traffic are encapsulated: bridging traffic and CAPWAP control and data traffic. Both types of traffic are encapsulated in a proprietary mesh header.

In the case of bridging traffic, the entire packet Ethernet frame is encapsulated in the mesh header.

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

Figure 55: Encapsulating Mesh Traffic



Note Mesh Data DTLS encryption is only supported on the wave 2 Mesh AP such as 1540 and 1560 models only.

Queuing on the Mesh Access Point

The mesh access point uses a high speed CPU to process ingress frames, Ethernet, and wireless on a first-come, first-serve basis. These frames are queued for transmission to the appropriate output device, either Ethernet or wireless. Egress frames can be destined for either the 802.11 client network, the 802.11 backhaul network, or Ethernet.

AP1500s support four FIFOs for wireless client transmissions. These FIFOs correspond to the 802.11e platinum, gold, silver, and bronze queues, and obey the 802.11e transmission rules for those queues. The FIFOs have a user configurable queue depth.

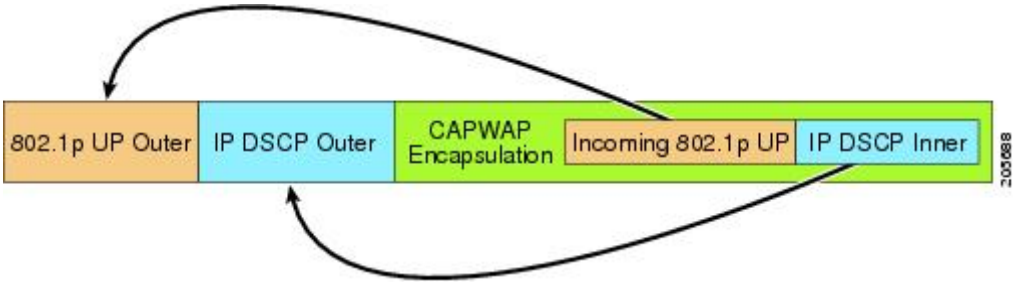
The backhaul (frames destined for another outdoor mesh access point) uses four FIFOs, although user traffic is limited to gold, silver, and bronze. The platinum queue is used exclusively for CAPWAP control traffic and voice, and has been reworked from the standard 802.11e parameters for CWmin, CWmax,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

The 802.11e parameters for CWmin, CWmax, and so on, for the gold queue have been reworked to provide lower latency at the expense of slightly higher error rate and aggressiveness. The purpose of these changes is to provide a channel that is more conducive to video applications.

Frames that are destined for Ethernet are queued as FIFO, up to the maximum available transmit buffer pool (256 frames). There is support for a Layer 3 IP Differentiated Services Code Point (DSCP), so marking of the packets is there as well.

In the controller to RAP path for the data traffic, the outer DSCP value is set to the DSCP value of the incoming IP frame. If the interface is in tagged mode, the controller sets the 802.1Q VLAN ID and derives the 802.1p UP (outer) from 802.1p UP incoming and the WLAN default priority ceiling. Frames with VLAN ID 0 are not tagged.

Figure 56: Controller to RAP Path



For CAPWAP control traffic the IP DSCP value is set to 46, and the 802.1p user priority is set to 7. Prior to transmission of a wireless frame over the backhaul, regardless of node pairing (RAP/MAP) or direction, the DSCP value in the outer header is used to determine a backhaul priority. The following sections describe the mapping between the four backhaul queues the mesh access point uses and the DSCP values shown in Backhaul Path QoS.

Table 26: Backhaul Path QoS

DSCP Value	Backhaul Queue
2, 4, 6, 8 to 23	Bronze
26, 32 to 63	Gold
46 to 56	Platinum
All others including 0	Silver

Note The platinum backhaul queue is reserved for CAPWAP control traffic, IP control traffic, and voice packets. DHCP, DNS, and ARP requests are also transmitted at the platinum QoS level. The mesh software inspects each frame to determine whether it is a CAPWAP control or IP control frame in order to protect the platinum queue from use by non-CAPWAP applications.

For a MAP to the client path, there are two different procedures, depending on whether the client is a WMM client or a normal client. If the client is a WMM client, the DSCP value in the outer frame is examined, and the 802.11e priority queue is used.

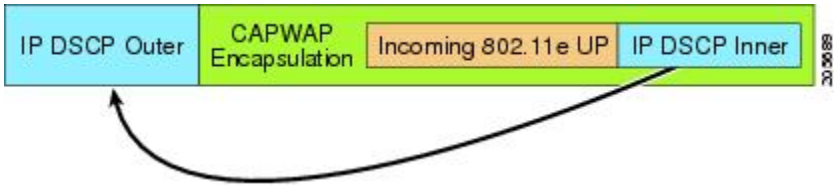
Table 27: MAP to Client Path QoS

DSCP Value	Backhaul Queue
2, 4, 6, 8 to 23	Bronze
26, 32 to 45, 47	Gold
46, 48 to 63	Platinum
All others including 0	Silver

If the client is not a WMM client, the WLAN override (as configured at the controller) determines the 802.11e queue (bronze, gold, platinum, or silver), on which the packet is transmitted.

For a client of a mesh access point, there are modifications made to incoming client frames in preparation for transmission on the mesh backhaul or Ethernet. For WMM clients, a MAP illustrates the way in which the outer DSCP value is set from an incoming WMM client frame.

Figure 57: MAP to RAP Path



The minimum value of the incoming 802.11e user priority and the WLAN override priority is translated using the information listed in Table 28: DSCP to Backhaul Queue Mapping, on page 139 to determine the DSCP value of the IP frame. For example, if the incoming frame has as its value a priority indicating the gold priority, but the WLAN is configured for the silver priority, the minimum priority of silver is used to determine the DSCP value.

Table 28: DSCP to Backhaul Queue Mapping

DSCP Value	802.11e UP	Backhaul Queue	Packet Types
2, 4, 6, 8 to 23	1, 2	Bronze	Lowest priority packets, if any
26, 32 to 34	4, 5	Gold	Video packets
46 to 56	6, 7	Platinum	CAPWAP control, AWPP, DHCP/DNS, ARP packets, voice packets
All others including 0	0, 3	Silver	Best effort, CAPWAP data packets

If there is no incoming WMM priority, the default WLAN priority is used to generate the DSCP value in the outer header. If the frame is an originated CAPWAP control frame, the DSCP value of 46 is placed in the outer header.

With the 5.2 code enhancements, DSCP information is preserved in an AWPP header.

All wired client traffic is restricted to a maximum 802.1p UP value of 5, except DHCP/DNS and ARP packets, which go through the platinum queue.

The non-WMM wireless client traffic gets the default QoS priority of its WLAN. The WMM wireless client traffic may have a maximum 802.11e value of 6, but it must be below the QoS profile configured for its WLAN. If admission control is configured, WMM clients must use TSPEC signaling and get admitted by CAC.

The CAPWAPP data traffic carries wireless client traffic and has the same priority and treatment as wireless client traffic.

Now that the DSCP value is determined, the rules described earlier for the backhaul path from the RAP to the MAP are used to further determine the backhaul queue on which the frame is transmitted. Frames transmitted

from the RAP to the controller are not tagged. The outer DSCP values are left intact, as they were first constructed.

Bridging Backhaul Packets

Bridging services are treated a little differently from regular controller-based services. There is no outer DSCP value in bridging packets because they are not CAPWAP encapsulated. Therefore, the DSCP value in the IP header as it was received by the mesh access point is used to index into the table as described in the path from the mesh access point to the mesh access point (backhaul).

Bridging Packets from and to a LAN

Packets received from a station on a LAN are not modified in any way. There is no override value for the LAN priority. Therefore, the LAN must be properly secured in bridging mode. The only protection offered to the mesh backhaul is that non-CAPWAP control frames that map to the platinum queue are demoted to the gold queue.

Packets are transmitted to the LAN precisely as they are received on the Ethernet ingress at entry to the mesh.

The only way to integrate QoS between Ethernet ports on AP1500 and 802.11a is by tagging Ethernet packets with DSCP. AP1500s take the Ethernet packet with DSCP and places it in the appropriate 802.11e queue.

AP1500s do not tag DSCP itself:

- On the ingress port, the AP1500 sees a DSCP tag, encapsulates the Ethernet frame, and applies the corresponding 802.11e priority.
- On the egress port, the AP1500 decapsulates the Ethernet frame, and places it on the wire with an untouched DSCP field.

Ethernet devices, such as video cameras, should have the capability to mark the bits with DSCP value to take advantage of QoS.



Note QoS only is relevant when there is congestion on the network.

Guidelines For Using Voice on the Mesh Network

Follow these guidelines when you use voice on the mesh network:

- Voice is supported only on indoor mesh networks. For outdoors, voice is supported on a best-effort basis on a mesh infrastructure.
- When voice is operating on a mesh network, calls must not traverse more than two hops. Each sector must be configured to require no more than two hops for voice.
- RF considerations for voice networks are as follows:
  - Coverage hole of 2 to 10 percent
  - Cell coverage overlap of 15 to 20 percent
  - Voice needs RSSI and SNR values that are at least 15 dB higher than data requirements
  - RSSI of -67 dBm for all data rates should be the goal for 11b/g/n and 11a/n

- SNR should be 25 dB for the data rate used by client to connect to the AP
- Packet error rate (PER) should be configured for a value of one percent or less
- Channel with the lowest utilization (CU) must be used

- On the **802.11a/n/ac** or **802.11b/g/n** > *Global* parameters page, do the following:
  - Enable dynamic target power control (DTPC).
  - Disable all data rates less than 11 Mbps.
- On the **802.11a/n/ac** or **802.11b/g/n** > *Voice* parameters page, do the following:
  - Load-based CAC must be disabled.
  - Enable admission control (ACM) for CCXv4 or v5 clients that have WMM enabled. Otherwise, bandwidth-based CAC does not operate properly.
  - Set the maximum RF bandwidth to 50 percent.
  - Set the reserved roaming bandwidth to 6 percent.
  - Enable traffic stream metrics.
- On the **802.11a/n/ac** or **802.11b/g/n** > *EDCA* parameters page, you should do the following:
  - Set the EDCA profile for the interface as voice optimized.
  - Disable low latency MAC.
- On the **QoS** > *Profile* page, you should do the following:
  - Create a voice profile and select 802.1Q as the wired QoS protocol type.
- On the **WLANs** > *Edit* > *QoS* page, you should do the following:
  - Select a QoS of platinum for voice and gold for video on the backhaul.
  - Select allowed as the WMM policy.
- On the **WLANs** > *Edit* > *QoS* page, you should do the following:
  - Select CCKM for authorization (*auth*) key management (*mgmt*) if you want to support fast roaming.
- On the **x** > *y* page, you should do the following:
  - Disable voice active detection (VAD).

Voice Call Support in a Mesh Network

Table 29: Calls Possible with 1550 Series in 802.11a/n 802.11b/g/n Radios, on page 142 shows the actual calls in a clean, ideal environment.

Table 29: Calls Possible with 1550 Series in 802.11a/n 802.11b/g/n Radios

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

[10] Traffic was bidirectional 64K voice flows. VoCoder type: G.711, PER <= 1%. Network setup was daisy-chained with no calls traversing more than 2 hops. No external interference.

While making a call, observe the MOS score of the call on the 7921 phone. A MOS score between 3.5 and 4 is acceptable.

Table 30: MOS Ratings

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

Enabling Mesh Multicast Containment for Video

You can use the controller CLI to configure three mesh multicast modes to manage video camera broadcasts on all mesh access points. When enabled, these modes reduce unnecessary multicast transmissions within the mesh network and conserve backhaul bandwidth.

Mesh multicast modes determine how bridging-enabled access points MAP and RAP send multicasts among Ethernet LANs within a mesh network. Mesh multicast modes manage non-CAPWAP multicast traffic only. CAPWAP multicast traffic is governed by a different mechanism.

The three mesh multicast modes are as follows:

- **Regular mode**—Data is multicast across the entire mesh network and all its segments by bridging-enabled RAP and MAP.
- **In-only mode**—Multicast packets received from the Ethernet by a MAP are forwarded to the RAP's Ethernet network. No additional forwarding occurs, which ensures that non-CAPWAP multicasts received by the RAP are not sent back to the MAP Ethernet networks within the mesh network (their point of origin), and MAP to MAP multicasts do not occur because they are filtered out.



Note When an HSRP configuration is in operation on a mesh network, we recommend the In-Out multicast mode be configured.

- **In-out mode**—The RAP and MAP both multicast but in a different manner:
  - In-out mode is the default mode.
  - If multicast packets are received at a MAP over Ethernet, they are sent to the RAP; however, they are not sent to other MAP over Ethernet, and the MAP to MAP packets are filtered out of the multicast.
  - If multicast packets are received at a RAP over Ethernet, they are sent to all the MAPs and their respective Ethernet networks. When the in-out mode is in operation, it is important to properly partition your network to ensure that a multicast sent by one RAP is not received by another RAP on the same Ethernet segment and then sent back into the network.

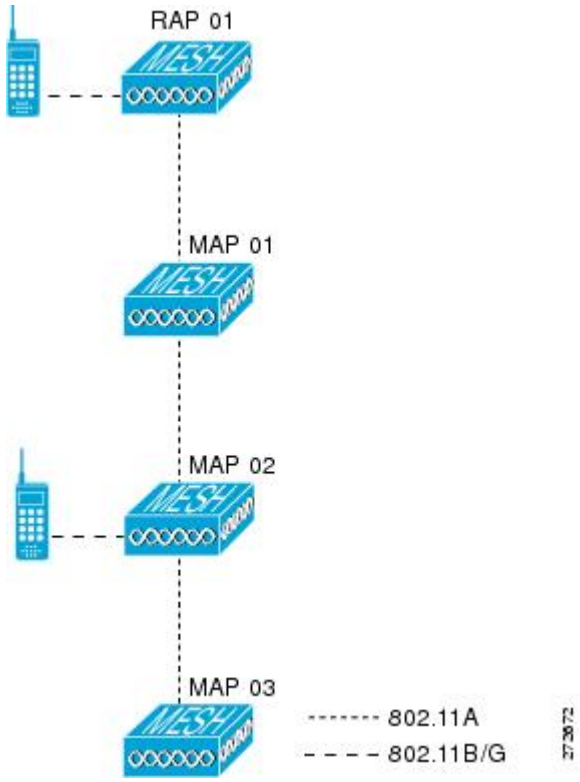


Note If 802.11b clients need to receive CAPWAP multicasts, then multicast must be enabled globally on the controller as well as on the mesh network (using the **config network multicast global enable** CLI command). If multicast does not need to extend to 802.11b clients beyond the mesh network, the global multicast parameter should be disabled (using the **config network multicast global disable** CLI command).

Viewing the Voice Details for Mesh Networks (CLI)

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

Figure 58: Mesh Network Example



- To view the total number of voice calls and the bandwidth used for voice calls on each RAP, enter this command:

  show mesh cac summary

  Information similar to the following appears:

```
AP Name           Slot#   Radio  BW Used/Max  Calls
------------     -------  -----  -----------  -----
SB_RAP1              0    11b/g     0/23437    0
                     1    11a       0/23437    2
SB_MAP1              0    11b/g     0/23437    0
                     1    11a       0/23437    0
SB_MAP2              0    11b/g     0/23437    0
                     1    11a       0/23437    0
SB_MAP3              0    11b/g     0/23437    0
                     1    11a      0/23437    0?
```

- To view the mesh tree topology for the network and the bandwidth utilization (used/maximum available) of voice calls and video links for each mesh access point and radio, enter this command:

  show mesh cac bwused {**voice** | **video**} *AP_name*

  Information similar to the following appears:

```
AP Name        Slot#    Radio      BW Used/Max
-------------- -------  -----      -----------
SB_RAP1          0      11b/g       1016/23437
```

```
                1       11a         3048/23437
|SB_MAP1        0       11b/g       0/23437
                1       11a         3048/23437
||  SB_MAP2     0       11b/g       2032/23437
                1       11a         3048/23437
||| SB_MAP3     0       11b/g       0/23437
                1       11a         0/23437
```

Note The bars (|) to the left of the AP Name field indicate the number of hops that the MAP is from its RAP.

Note When the radio type is the same, the backhaul bandwidth utilization (bw used/max) at each hop is identical. For example, mesh access points *map1*, *map2*, *map3*, and *rap1* are all on the same radio backhaul (802.11a) and are using the same bandwidth (3048). All of the calls are in the same interference domain. A call placed anywhere in that domain affects the others.

- To view the mesh tree topology for the network and display the number of voice calls that are in progress by mesh access point radio, enter this command:

  show mesh cac access *AP_name*

```
Information similar to the following appears:

AP Name             Slot#   Radio     Calls
-------------      -------  -----    -----
SB_RAP1              0      11b/g      0
                     1      11a        0
|   SB_MAP1          0      11b/g      0
                     1      11a        0
||  SB_MAP2          0      11b/g      1
                     1      11a        0
||| SB_MAP3          0      11b/g      0
                     1      11a        0
```

Note Each call received by a mesh access point radio causes the appropriate calls summary column to increment by one. For example, if a call is received on the 802.11b/g radio on map2, then a value of one is added to the existing value in that radio's *calls* column. In this case, the new call is the only active call on the 802.11b/g radio of map2. If one call is active when a new call is received, the resulting value is two.

- To view the mesh tree topology for the network and display the voice calls that are in progress, enter this command:

  show mesh cac callpath *AP_name*

```
Information similar to the following appears:
```

```
AP Name             Slot#   Radio     Calls
-------------      -------  -----    -----
SB_RAP1              0      11b/g      0
                     1      11a        1
|   SB_MAP1          0      11b/g      0
                     1      11a        1
||  SB_MAP2          0      11b/g      1
                     1      11a        1
||| SB_MAP3          0      11b/g      0
                     1      11a        0
```



Note The *calls* column for each mesh access point radio in a call path increments by one. For example, for a call that initiates at map2 (**show mesh cac call path** *SB_MAP2*) and terminates at rap1 by way of map1, one call is added to the map2 802.11b/g and 802.11a radio *calls* column, one call to the map1 802.11a backhaul radio *calls* column, and one call to the rap1 802.11a backhaul radio *calls* column.

- To view the mesh tree topology of the network, the voice calls that are rejected at the mesh access point radio due to insufficient bandwidth, and the corresponding mesh access point radio where the rejection occurred, enter this command:

  show mesh cac rejected *AP_name*

  Information similar to the following appears:

```
AP Name             Slot#   Radio     Calls
-------------      -------  -----    -----
SB_RAP1              0      11b/g      0
                     1      11a        0
|   SB_MAP1          0      11b/g      0
                     1      11a        0
||  SB_MAP2          0      11b/g      1
                     1      11a        0
||| SB_MAP3          0      11b/g      0
                     1      11a        0
```



Note If a call is rejected at the map2 802.11b/g radio, its *calls* column increments by one.

- To view the number of bronze, silver, gold, platinum, and management queues active on the specified access point, enter this command. The peak and average length of each queue are shown as well as the overflow count.

  show mesh queue-stats *AP_name*

  Information similar to the following appears:

```
Queue Type  Overflows  Peak length  Average length
 ----------  ---------  -----------  --------------
 Silver      0          1            0.000
 Gold        0          4            0.004
```

```
Platinum    0          4            0.001
Bronze      0          0            0.000
Management  0          0            0.000
```

Overflows—The total number of packets dropped due to queue overflow.

Peak Length—The peak number of packets waiting in the queue during the defined statistics time interval.

Average Length—The average number of packets waiting in the queue during the defined statistics time interval.

Enabling Multicast on the Mesh Network (CLI)

Note

- Cisco Aironet 1540 and 1560 Series Outdoor Access Points support in-out mode only.
- Cisco Aironet 1530, 1550, and 1570 Series Outdoor Access Points support all the modes.

Procedure

- To enable multicast mode on the mesh network to receive multicasts from beyond the mesh networks, enter these commands:

  config network multicast global enable

  config mesh multicast {**regular** | **in-only** | **in-out**}

- To enable multicast mode only the mesh network (multicasts do not need to extend to 802.11b clients beyond the mesh network), enter these commands:

  config network multicast global disable

  config mesh multicast {**regular** | **in-only** | **in-out**}

Note Multicast for mesh networks cannot be enabled using the controller GUI.

IGMP Snooping

IGMP snooping delivers improved RF usage through selective multicast forwarding and optimizes packet forwarding in voice and video applications.

A mesh access point transmits multicast packets only if a client is associated with the mesh access point that is subscribed to the multicast group. So, when IGMP snooping is enabled, only that multicast traffic relevant to given hosts is forwarded.

To enable IGMP snooping on the controller, enter the following command:

configure network multicast igmp snooping enable

A client sends an IGMP *join* that travels through the mesh access point to the controller. The controller intercepts the *join* and creates a table entry for the client in the multicast group. The controller then proxies the IGMP *join* through the upstream switch or router.

You can query the status of the IGMP groups on a router by entering the following command:

```
router# show ip gmp groups
IGMP Connected Group Membership

Group Address    Interface   Uptime  Expires    Last Reporter
233.0.0.1        Vlan119     3w1d    00:01:52   10.1.1.130
```

For Layer 3 roaming, an IGMP query is sent to the client's WLAN. The controller modifies the client's response before forwarding and changes the source IP address to the controller's dynamic interface IP address.

The network hears the controller's request for the multicast group and forwards the multicast to the new controller.

For more information about video, see the following:

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

Locally Significant Certificates for Mesh APs

Until the 7.0 release, mesh APs supported only the Manufactured Installed Certificate (MIC) to authenticate and get authenticated by controllers to join the controller. You might have had to have your own public key infrastructure (PKI) to control CAs, to define policies, to define validity periods, to define restrictions and usages on the certificates that are generated, and get these certificates installed on the APs and controllers. After these customer-generated or locally significant certificates (LSCs) are present on the APs and controllers, the devices start using these LSCs, to join, authenticate, and derive a session key. Cisco supported normal APs from the 5.2 release and later releases and extended the support for mesh APs as well from the 7.0 release.

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

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

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

- Over the air provisioning of MAPs.

Guidelines for Configuration

Follow these guidelines when using LSCs for mesh APs:

- This feature does not remove any preexisting certificates from an AP. It is possible for an AP to have both LSC and MIC certificates.
- After an AP is provisioned with an LSC, it does not read in its MIC certificate on boot-up. A change from an LSC to an MIC will require the AP to reboot. APs do it for a fallback if they cannot be joined with an LSC.
- Provisioning an LSC on an AP does not require an AP to turn off its radios, which is vital for mesh APs, which may get provisioned over-the-air.
- Because mesh APs need a dot1x authentication, a CA and ID certificate is required to be installed on the server in the controller.
- LSC provisioning can happen over Ethernet and over-the-air in case of MAPs.You have to connect the mesh AP to the controller through Ethernet and get the LSC certificate provisioned. After the LSC becomes the default, an AP can be connected over-the-air to the controller using the LSC certificate.

Differences Between LSCs for Mesh APs and Normal APs

CAPWAP APs use LSC for DTLS setup during a JOIN irrespective of the AP mode. Mesh APs also use the certificate for mesh security, which involves a dot1x authentication with the controller through the parent AP. After the mesh APs are provisioned with an LSC, they need to use the LSC for this purpose because MIC will not be read in.

Mesh APs use a statically configured dot1x profile to authenticate.

This profile is hardcoded to use "cisco" as the certificate issuer. This profile needs to be made configurable so that vendor certificates can be used for mesh authentication (enter the **config local-auth eap-profile cert-issuer vendor "prfMaP1500LlEAuth93"** command).

You must enter the **config mesh lsc enable/disable** command to enable or disable an LSC for mesh APs. This command will cause all the mesh APs to reboot.



Note An LSC on mesh is open for very specific Oil and Gas customers with the 7.0 release. Initially, it is a hidden feature. The **config mesh lsc enable/disable** is a hidden command. Also, the **config local-auth eap-profile cert-issuer vendor "prfMaP1500LlEAuth93"** command is a normal command, but the "prfMaP1500LlEAuth93" profile is a hidden profile, and is not stored on the controller and is lost after the controller reboot.

Certificate Verification Process in LSC AP

LSC-provisioned APs have both LSC and MIC certificates, but the LSC certificate will be the default one. The verification process consists of the following two steps:

1. The controller sends the AP the MIC device certificate, which the AP verifies with the MIC CA.
2. The AP sends the LSC device certificate to the controller, which the controller verifies with the LSC CA.

Getting Certificates for LSC Feature

To configure LSC, you must first gather and install the appropriate certificates on the controller. The following steps show how to accomplish this using Microsoft 2003 Server as the CA server.

To get the certificates for LSC, follow these steps:

Step 1 Go to the CA server (http://<ip address of caserver/crtsrv) and login.

Step 2 Get the CA certificate as follows:

a) Click the Download a CA certificate link, certificate chain, or CRF.
b) Choose the encoding method as DER.
c) Click the Download CA certificate link and use the save option to download the CA certificate on to your local machine.

Step 3 To use the certificate on the controller, convert the downloaded certificate to PEM format. You can convert this in a Linux machine using the following command:

openssl x509 -in <input.cer> -inform DER -out <output.cer> -outform PEM

Step 4 Configure the CA certificate on the controller as follows:

a) Choose **COMMANDS > Download File**.
b) Choose the file type as Vendor CA Certificate from the File Type drop-down list.
c) Update the rest of the fields with the information of the TFTP server where the certificate is located.
d) Click **Download**.

Step 5 To install the Device certificate on the WLC, login to the CA server as mentioned in Step 1 and do the following:

a) Click the Request a certificate link.
b) Click the advanced certificate request link.
c) Click Create and submit a request to this CA link.
d) Go to the next screen and choose the Server Authentication Certificate from the Certificate Template drop-down list.
e) Enter a valid name, email, company, department, city, state, and country/region. (Remember it in case you want the cap method to check the username against its database of user credentials).

Note The e-mail is not used.

f) Enable Mark keys as exportable.
g) Click **Submit**.
h) Install the certificate on your laptop.

Step 6 Convert the device certificate obtained in the Step 5. To get the certificate, go to your internet browser options and choose exporting to a file. Follow the options from your browser to do this. You need to remember the password that you set here.

To convert the certificate, use the following command in a Linux machine:

openssl pkcs12 -in <input.pfx> -out <output.cer>

Step 7 On the controller GUI, choose **Command > Download File**. Choose Vendor Device Certificate from the File Type drop-down list. Update the rest of the fields with the information of the TFTP server where the certificate is located and the password you set in the previous step and click **Download**.

Step 8 Reboot the controller so that the certificates can then be used.

Step 9 You can check that the certificates were successfully installed on the controller using this command:

show local-auth certificates

Configuring a Locally Significant Certificate (CLI)

To configure a locally significant certificate (LSC), follow these steps:

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

Step 2 Enter the following command:

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

Step 3 Turn on the feature by entering the following command:

config mesh lsc {**enable** | **disable**}

Step 4 Connect the mesh AP through Ethernet and provision for an LSC certificate.

Step 5 Let the mesh AP get a certificate and join the controller using the LSC certificate.

Figure 59: Local Significant Certificate Page

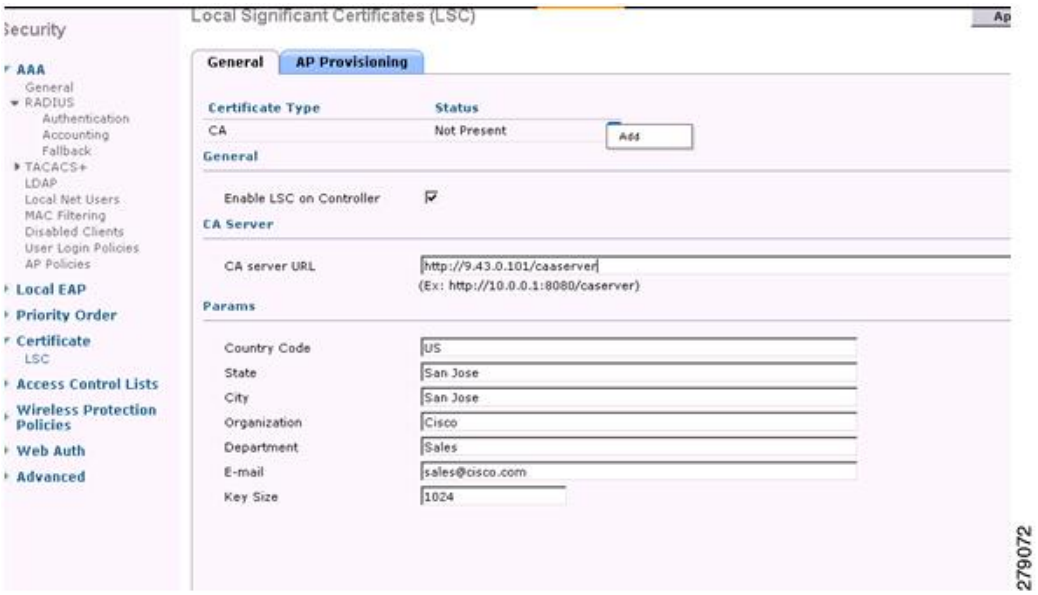
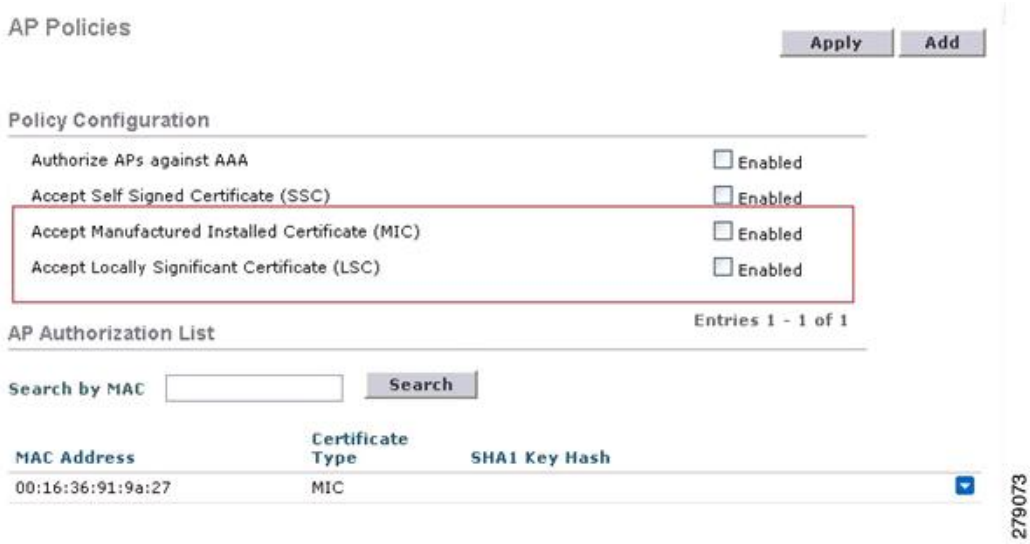


Figure 60: AP Policy Configuration



LSC only MAP Authentication using wild card MAC

Information about LSC-Only MAP Authentication using wild card MAC

The 8.0 release supports LSC only authentication using a wild card MAC address thus disabling the MAC filter. To ensure only authorized access points authenticate, the Cisco WLC must be able to force the EAP with LSC authentication.

The table shows the different forms of LSC authentication.

Table 31: MAP Authentication Methods

Operation	MAC Filter	LSC Only Authentication
LSC-Only MAP Authentication enabled	disabled	enabled
LSC-Only MAP Authentication disabled	enabled	disabled
Security mode: EAP & PSK	EAP or PSK can be used	Only EAP with LSC should be used
Certificates: MIC & LSC	MIC or LSC can be used	Only EAP with LSC should be used

WLC includes the wildcard MAC address in mac filter list and allows all APs to join the WLC. MAC authorization is disabled automatically. EAP security mode provides valid security with LSC. During EAP-FAST, the AP gets authenticated using LSC and gets the MSK key from WLC. Any rogue APs are filtered out. Using these keys message handshake happens and the PTK key is generated. The Mesh AP joins the WLC using LSC only.

The PSK security mode leads to security threat. As the MSK key is hardcoded inside the code of the mesh AP, any AP even a rogue AP can join the WLC. Using these keys, message handshake happens and the PTK

key is generated. The Mesh AP joins the WLC using LSC only. Wildcard with PSK must be used only for the debugging purposes.

Configuring LSC-Only Authentication for Mesh Access Points (GUI)

Mesh access points must authenticate before associating with the Cisco WLC. It is not feasible to enter every AP MAC address into every Cisco WLC filter list. Service providers have locally significant certificates (LSC), which you can use to bypass MAC authentication and use only LSC.

Step 1 Choose **Security** > **Certificate** > **LSC** .

The **Locally Significant Certificates** page is displayed.

Step 2 Select the **AP Provisioning** tab.

Step 3 Select the **Enable LSC on Controller** check box.

Step 4 Select the **General** tab.

Step 5 Select the **Enable** check box in the **AP Provisioning** group.

Step 6 Choose **Wireless** > **Mesh**.

The **Mesh** page is displayed.

Step 7 Select or unselect the **LSC Only MAP Authentication** check box.

Step 8 Click **Apply**.

Step 9 Click **Save Configuration**.

Configuring LSC-Only Authentication for Mesh Access Points (CLI)

Mesh access points must authenticate before associating with the Cisco WLC. It is not feasible to enter every AP MAC address into every Cisco WLC filter list. Service providers have locally significant certificates (LSC), which you can use to bypass MAC authentication and use only LSC.

Procedure

- Configure LSC-only authentication for mesh access points by entering this command:
  config mesh security lsc-only-auth {**enable** | **disable**}

LSC-Related Commands

The following commands are related to LSCs:

- **config certificate lsc** {**enable** | **disable**}
  - **enable**—To enable an LSC on the system.
  - **disable**—To disable an LSC on the system. Use this keyword to remove the LSC device certificate and send a message to an AP, to do the same and disable an LSC, so that subsequent joins could be made using the MIC/SSC. The removal of the LSC CA cert on the WLC should be done explicitly by using the CLI to accommodate any AP that has not transitioned back to the MIC/SSC.
- **config certificate lsc ca-server url-path** *ip-address*

Following is the example of the URL when using Microsoft 2003 server:

http:<ip address of CA>/sertsrv/mscep/mscep.dll

This command configures the URL to the CA server for getting the certificates. The URL contains either the domain name or the IP address, port number (typically=80), and the CGI-PATH.

http://ipaddr:port/cgi-path

Only one CA server is allowed to be configured. The CA server has to be configured to provision an LSC.

- **config certificate lsc ca-server delete**

  This command deletes the CA server configured on the controller.

- **config certificate lsc ca-cert** {**add** | **delete**}

  This command adds or deletes the LSC CA certificate into/from the controller's CA certificate database as follows:

  - **add**—Queries the configured CA server for a CA certificate using the SSCEP getca operation, and gets into the WLC and installs it permanently into the WLC database. If installed, this CA certificate is used to validate the incoming LSC device certificate from the AP.
  - **delete**—Deletes the LSC CA certificate from the WLC database.

- **config certificate lsc subject-params** *Country State City Orgn Dept Email*

  This command configures the parameters for the device certificate that will be created and installed on the controller and the AP.

  All of these strings have 64 bytes, except for the Country that has a maximum of 3 bytes. The Common Name is automatically generated using its Ethernet MAC address. This should be given prior to the creation of the controller device certificate request.

  The above parameters are sent as an LWAPP payload to the AP, so that the AP can use these parameters to generate the certReq. The CN is automatically generated on the AP using the current MIC/SSC "Cxxxx-MacAddr" format, where xxxx is the product number.

- **config certificate lsc other-params** *keysize*

  The default keysize value is 2048 bits.

- **config certificate lsc ap-provision** {**enable** | **disable**}

  This command enables or disables the provisioning of the LSCs on the APs if the APs just joined using the SSC/MIC. If enabled, all APs that join and do not have the LSC will get provisioned.

  If disabled, no more automatic provisioning will be done. This command does not affect the APs, which already have LSCs in them.

- **config certificate lsc ra-cert** {**add** | **delete**}

  We recommend this command when the CA server is a Cisco IOS CA server. The controller can use the RA to encrypt the certificate requests and make communication more secure. RA certificates are not currently supported by other external CA servers, such as MSFT.

  - **add**—Queries the configured CA server for an RA certificate using the SCEP operation and installs it into the controller database. This keyword is used to get the certReq signed by the CA.

- **delete**—Deletes the LSC RA certificate from the WLC database.

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

  After getting the LSC, an AP tries to join the controller. Before the AP tries to join the controller, you must mandatorily enter this command on the controller console. By default, the **config auth-list ap-policy lsc** command is in the disabled state, and the APs are not allowed to join the controller using the LSC.

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

  After getting the MIC, an AP tries to join the controller. Before the AP tries to join the controller, you must mandatorily enter this command on the controller console. By default, the **config auth-list ap-policy mic** command is in the enabled state. If an AP cannot join because of the enabled state, this log message on the controller side is displayed: LSC/MIC AP is not allowed to join.

- **show certificate lsc summary**

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

- **show certificate lsc ap-provision**

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

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

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

Controller GUI Security Settings

Although the settings are not directly related to the feature, it might help you in achieving the desired behavior with respect to APs provisioned with an LSC.

- Case 1—Local MAC Authorization and Local EAP Authentication

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

  Example:

```
(Cisco Controller) > config macfilter mac-delimiter colon
(Cisco Controller) > config macfilter add 00:0b:85:60:92:30 0 management
```

- Case 2—External MAC Authorization and Local EAP authentication

  Enter the following command on the WLC:

```
(Cisco Controller) > config mesh security rad-mac-filter enable
```

  or

  Check only the external MAC filter authorization on the GUI page and follow these guidelines:

  - Do not add the MAC address of the RAP/MAP to the controller MAC filter list.
  - Configure the external radius server details on the WLC.

- Enter the **config macfilter mac-delimiter colon** command configuration on the WLC.
- Add the MAC address of the RAP/MAP in the external radius server in the following format:

  User name: 11:22:33:44:55:66 Password : 11:22:33:44:55:66

- Case 3—LSC Only MAP Authentication

  Enter the following command on the WLC:

```
(Cisco Controller) > config mesh security lsc-only-auth enable
```

  or

  Check LSC Only MAP Authentication on the GUI page. This message will be displayed:

```
Warning: Enabling LSC Only MAP Authentication will provision LSC Certificate into MAP
(if MAP are being provisioned for first time). Please make sure MAP is connected to WLC using Ethernet
cable to avoid security risk.
Are you sure you want to continue? (Y/N)
```

Deployment Guidelines

- When using local authorization, the controller should be installed with the vendor's CA and device certificate.
- When using an external AAA server, the controller should be installed with the vendor’s CA and device certificate.
- Mesh security should be configured to use ‘vendor’ as the cert-issuer.
- MAPs cannot move from an LSC to an MIC when they fall back to a backup controller.

The **config mesh lsc** {**enable** | **disable**} command is required to enable or disable an LSC for mesh APs. This command causes all the mesh APs to reboot.

Configuring Antenna Band Mode

Information About Configuring Antenna Band Modes

You can configure the antenna band modes for mesh access points as either of the following:

- Dual Antenna Band Mode—The bottom two ports, port 1 and port 2, are used for dual band 2.4-GHz and 5-GHz dual radiating element (DRE) antennas.
- Single Antenna Band Mode—The top two ports, port 3 and port 4, are used for 5-GHz single radiating element (SRE) antennas and the bottom two ports, port 1 and port 2, are used for 2.4-GHz SRE antennas.

Restrictions for Configuring Antenna Band Modes

The antenna band mode configuration is available on the Cisco Aironet 1532E and 1572EC/EAC access point models.

Note The Cisco Aironet 1532I access point model has internal antenna and does not require additional antennas.

Configuring Antenna Band Mode (GUI)

Before you begin

Ensure that the physical antennas are correctly configured before changing the antenna band mode. If the antenna band mode is incorrectly configured, the mesh AP could be stranded.

Step 1 Choose **Wireless** > **Access Points** > **All APs**.
A list of APs is displayed.

Step 2 Click the AP name.
The configuration details for the AP are displayed.

Step 3 Click the **Advanced** tab.

Step 4 From the **Antenna Band Mode** drop-down list, choose from the following options:

- **Single**
- **Dual**

A warning message is displayed prompting you that changing the antenna band mode may strand mesh APs. Click **OK**.

Step 5 Click **Apply**.

Step 6 Click **Save Configuration**.

Configuring Antenna Band Mode (CLI)

Before you begin

Ensure that the physical antennas are correctly configured before changing the antenna band mode. If the antenna band mode is incorrectly configured, the mesh AP could be stranded.

Procedure

- Configure antenna band mode for a mesh AP by entering this command on the Cisco WLC CLI:
  config ap antenna-band-mode {**single** | **dual**} *mesh-ap-name*
- View the status of the antenna band mode by entering this command:
  show ap config general *mesh-ap-name*

Configuring Antenna Band Mode (AP CLI)

Procedure

- Configure antenna band mode on the mesh AP CLI by entering this command on the AP console:
  capwap ap ant-band-mode {**dual** | **single**}

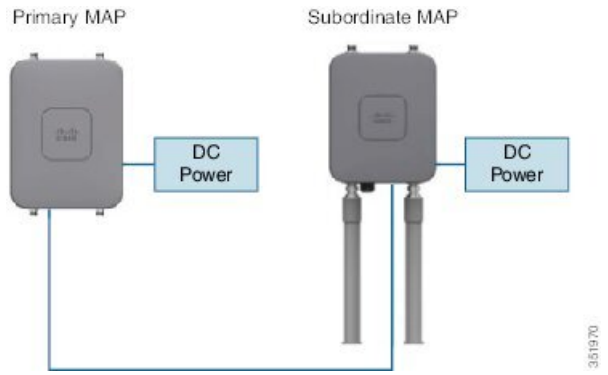
Configuring Daisy Chaining on Cisco Aironet 1530 Series Access Points

Information About Daisy Chaining the Cisco Aironet 1530 Series Access Points

The Cisco Aironet 1530 Series Access Points have the capability to "daisy chain" access points when they function as mesh APs (MAPs). The "daisy chained" MAPs can either operate the access points as a serial backhaul, allowing different channels for uplink and downlink access thus improving backhaul bandwidth, or extend universal access. Extending universal access allows you to connect a local mode or FlexConnect mode Cisco AP1530 to the Ethernet port of a MAP, thus extending the network to provide better client access.

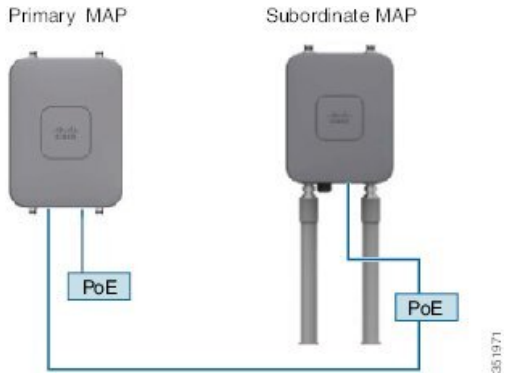
Daisy chained access points must be cabled differently depending on how the APs are powered. If the access point is powered using DC power, an Ethernet cable must be connected directly from the LAN port of the primary AP to the PoE in port of the subordinate AP.

Figure 61: Daisy Chained APs using DC Power



If the access point is powered using PoE, an Ethernet cable must be connected from the LAN port of the primary AP into the PoE Injector, which powers the subordinate AP.

Figure 62: Daisy Chained APs using PoE Injector



Daisy Chaining with the 1572

One of the key features of the 1572 access point (AP) is the ability to “daisy chain” APs while they are operating as Mesh APs (MAPs). By “daisy chaining” MAPs, customers can either operate the APs as a serial backhaul, allowing different channels for uplink and downlink access thus improving backhaul bandwidth, or to extend universal access. Extending universal access allows a customer to connect a local mode or

flexconnect mode 1572 AP to the Ethernet port of a MAP, thus extending the network to provide better client access. These features are explained in detail in the following sections.

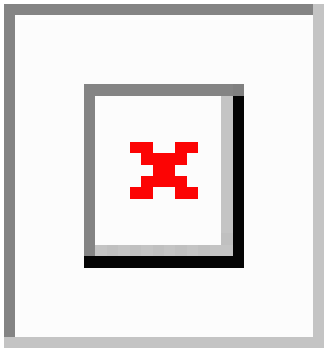
In the 8.0MR release, when the 1572 is configured as a primary AP, the following APs are supported as subordinate APs:

- 1572EAC
- 1572EC
- 1572IC
- 1552
- 1532E/I
- 3700P

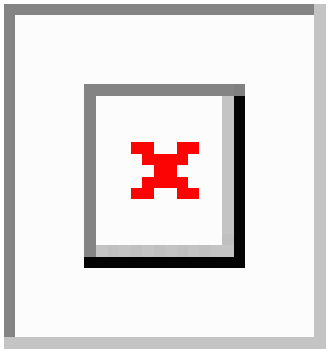
Daisy-chained access points need to be cabled differently depending on the AP type of their terminating subordinate AP.

If both the primary AP and subordinate APs are 1572s, there should be an Ethernet cable from the primary AP's Ethernet port to the subordinate AP's Ethernet port. Daisy chaining should be enabled on both APs.

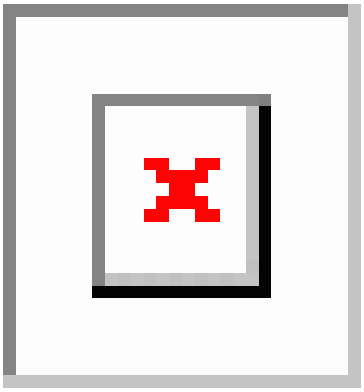
Caution We recommend that you connect Ethernet Bridged wired clients or Daisy-chained APs to either the Ethernet port or PoE-Out port only. Ethernet Bridged wired clients should never be connected to PoE-in port.



If the primary AP is a 1570 and the subordinate AP is a 1532 or 3700P, the Ethernet cable connects the PoE-Out port of the primary AP to the PoE-In port of the subordinate AP.



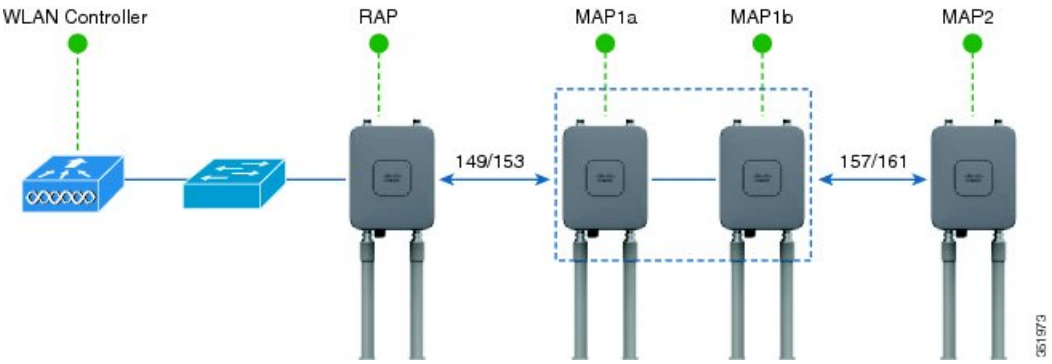
If the primary AP is a 1570 and the subordinate AP is a 1520 or 1550, the Ethernet cable connects the 1572's Ethernet port to any Ethernet port on the 1552.



Serial Backhaul on the Cisco Aironet 1530/1572 Series Access Points

Daisy chaining on the Cisco Aironet Access Points can be used to provide a serial-backhaul mesh. MAP1a is the primary MAP and has a preferred parent selected as the RAP. MAP1b is the subordinate MAP and has no preferred parent selected. MAP1b is configured in “Bridge” AP mode with “RootAP” role. Daisy chaining is enabled for MAP1b. MAP2 has preferred parent selected as MAP1b.

Figure 63: Daisy Chaining with Serial-Backhaul Mesh



High gain directional antenna must be used in typical serial-backhaul deployments. Additionally, preferred parent configurations must be used to create serial-backhaul mesh networks.

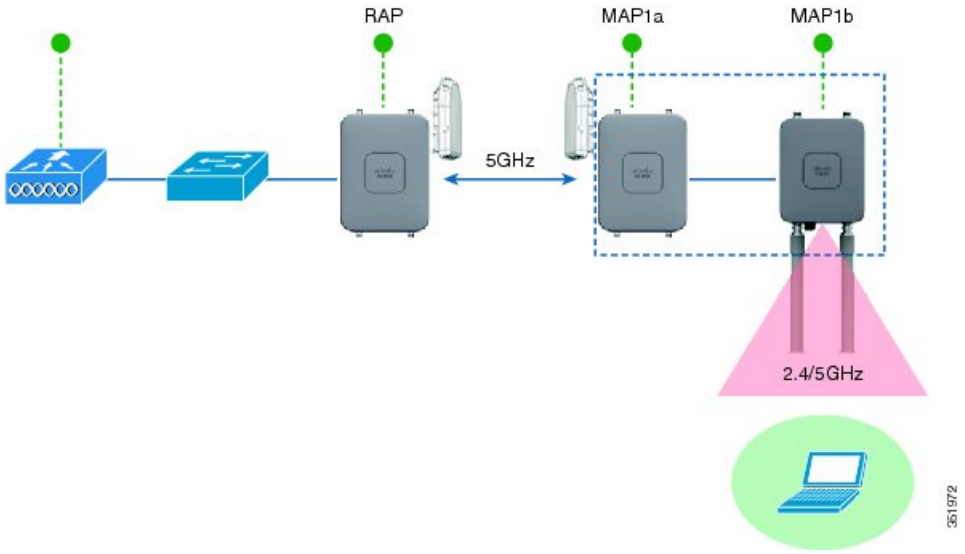
The child AP selects the preferred parent based on the following conditions:

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

Extended Universal Access

Daisy chaining on the Cisco Aironet 1530 Series Access Points can be used to extend Universal Access across a mesh network. In this example MAP1a is the primary MAP, it is backhauled wirelessly with the RAP. MAP1b, the subordinate MAP is operating in local/Flex-connect mode and is providing client access on both the 2.4GHz and 5GHz radio.

Figure 64: Daisy Chaining to Extend Universal Access



Important Points to Note When Configuring Daisy Chaining the Cisco Aironet 1530/1570 Series Access Points

- Only Mesh Access Points (MAPs) can operate as a daisy chained APs.
- The uplink daisy-chained AP is considered the primary AP; the connected AP is considered as the subordinate AP.
- The connecting Ethernet cable must go from the LAN port of the primary AP to the PoE in port of the subordinate AP.
- There must be a preferred parent set for each daisy-chained mesh hop; the primary MAP should have a preferred parent.
- Daisy chaining must be enabled on the subordinate AP in the Bridge mode through Cisco WLC GUI or CLI or on the AP console.
- Directional antennas must be used when you create a daisy chain; the antennas must be used to guide the mesh tree formation to suit your needs.
- Directional antenna must have a physical separation of 3 meters.
- Ethernet bridging must be enabled on all the APs in the Bridge mode.

Configuring Daisy Chaining (GUI)

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

A list of APs is displayed.

Step 2 Click the name of the AP.
The configuration details of the AP are displayed.

Step 3 Click the **Mesh** tab.

Step 4 Select or unselect the **Daisy Chaining** check box.
If the AP is used in a serial-backhaul deployment, specify a **Preferred Parent** for the AP.

Step 5 Click **Apply**.

Step 6 Click **Save Configuration**.

Configuring Daisy Chaining (CLI)

Procedure

- Configure daisy chaining by entering this command:
  config ap daisy-chaining {**enable** | **disable**} *cisco-mesh-ap*
- Configure the preferred parent for each serial-backhaul AP by entering this command:
  config mesh parent preferred *cisco-ap parent-mac-address*
- View the status of daisy chaining and the preferred parent that is configured by entering this command:
  show ap config general *cisco-ap*

Configuring Daisy Chaining (AP CLI)

Procedure

- Configure daisy chaining on the AP by entering this command on the AP console:
  capwap ap daisy-chaining {**enable** | **disable**}

Configuring a Daisy-Chain

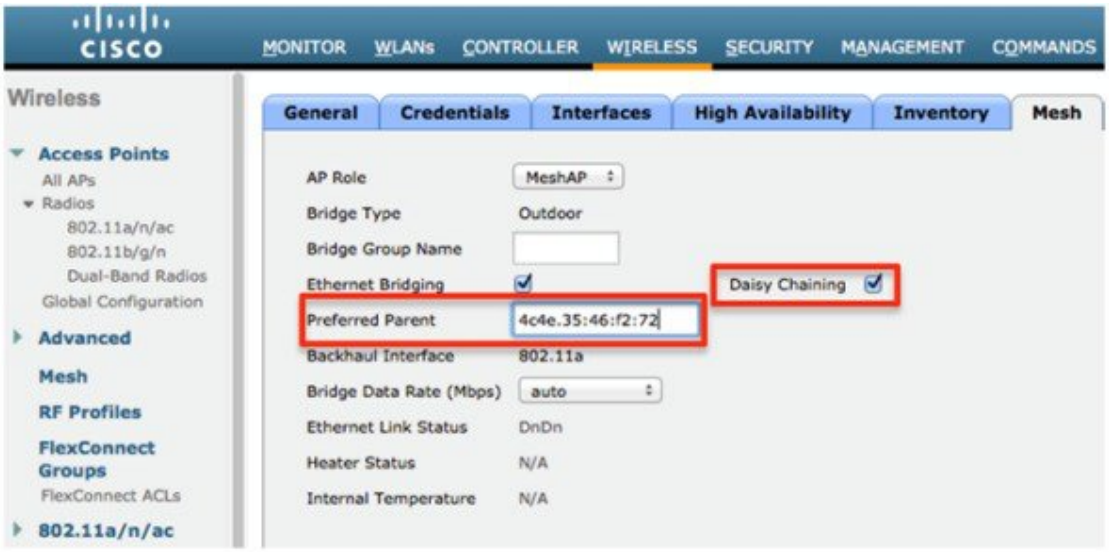
There are a few key components to address when configuring a daisy-chaining deployment:

- Only Mesh Access Points (MAPs) can operate as a daisy chained AP.
- The uplink daisy-chained AP is considered the primary AP, and the connected AP is considered the subordinate AP.
- There must be a preferred parent set for each daisy-chained mesh hop. The primary MAP should have a preferred parent.
- Daisy-chaining must be enabled on the AP, either via WLC GUI, WLC CLI, or AP CLI.
- Directional antennas should be used when creating a daisy-chain, which guides the mesh tree formation to the customer needs.

Enabling Daisy-Chaining using the WLC GUI

To enable Daisy-Chaining from the controller GUI, go to **Wireless > Access Point > (AP_NAME) > Mesh**, and then check the **Daisy-Chaining** check box. If the AP is used in a serial-backhaul solution, a **Preferred Parent** must be selected.

Note Daisy-chaining should only be enabled on the subordinate RAP. The primary MAP should have daisy-chaining as disabled.



Enabling Daisy-Chaining using the WLC CLI

To enable Daisy-Chaining from the WLC CLI, issue the command:

```
(Cisco Controller) >config ap daisy-chaining [enable/disable] <ap_name>
```

The daisy chaining feature must be enabled on a per access point basis:

```
(Cisco Controller) >show ap config general <ap_name>
```

Then scroll down the Daisy Chaining entry

```
Daisy Chaining ................................ Disabled
```

Enabling Daisy-Chaining using the AP CLI

To enable Daisy-Chaining from the AP CLI, issue the command:

```
AP#capwap ap daisy-chaining <enable/disable>
```

Setting a Preferred Parent for each Serial-Backhaul AP

To set up a preferred parent for each serial-backhaul AP, issue the command:

```
(Cisco Controller) >config mesh parent preferred <ap_name> <PARENT_MAC_ADDRESS>
```

An access point's preferred parent can be seen by issuing:

```
Cisco Controller) >show ap config general <ap_name>
```

Then scroll down the Mesh preferred parent entry

```
Mesh preferred parent ..... 00:24:13:0f:92:00
```

Note For more details, see this page.

Configuring Mesh Convergence

Information About Mesh Convergence

Using Cisco WLC, you can configure mesh convergence methods per mesh AP (MAP) or for all mesh APs. This enables you to choose the convergence methods based on deployment without affecting the existing convergence mechanism. The default setting is the existing convergence mechanism.

Mesh Convergence	Parent Loss Detection / Keep Alive Timers	Channel Scan / Seek	DHCP / CAPWAP Information
Standard	21 / 3 seconds	Scan/Seek all 5-GHz channels	Renew/Restart CAPWAP
Fast	7 / 3 seconds	Scan/Seek only preset channels	Maintain DHCP and CAPWAP
Very Fast	4 / 1.5 seconds	Scan/Seek only preset channels	Maintain DHCP and CAPWAP

Restrictions on Mesh Convergence

In Cisco Wave 2 APs, the convergence settings are as follows:

Table 32: Frequency to Seek Parent

Convergence Setting	Frequency to Seek Parent
Very Fast	Every 500 milliseconds
Fast	Every 750 milliseconds
Standard	Every 1 second

The frequency to seek neighbors for all convergence settings is 15 seconds.

If the AP fails to respond 8 times, the parent or the neighbor is assumed lost.

Table 33: Totaly Time Taken to Calculate Parent Loss

Convergence Setting	Total Time Taken
Very Fast	4 seconds

Convergence Setting	Total Time Taken
Fast	6 seconds
Standard	8 seconds

The neighbor (non-parent), loss time is 2 minutes.

In fast and very fast convergence, a subset channel seek is performed. The AP maintains a list of channels supported by neighboring parents and directly seeks those channels than going for a channel scan. For standard convergence, a channel scan is performed when the parent is lost.

Configuring Mesh Convergence (CLI)

Procedure

- Configure mesh convergence on the Cisco WLC CLI by entering this command:
  config mesh convergence {**fast** | **standard** | **very-fast**} **all**

Note The **all** keyword denotes all MAP nodes.

- Mesh convergence commands on the AP console:
  a) To see the current subset list of channels:
     show mesh convergence
  b) To debug mesh convergence:
     debug mesh convergence
  c) To set convergence method at the AP:
     test mesh convergence {**fast** | **standard** | **very_fast**}

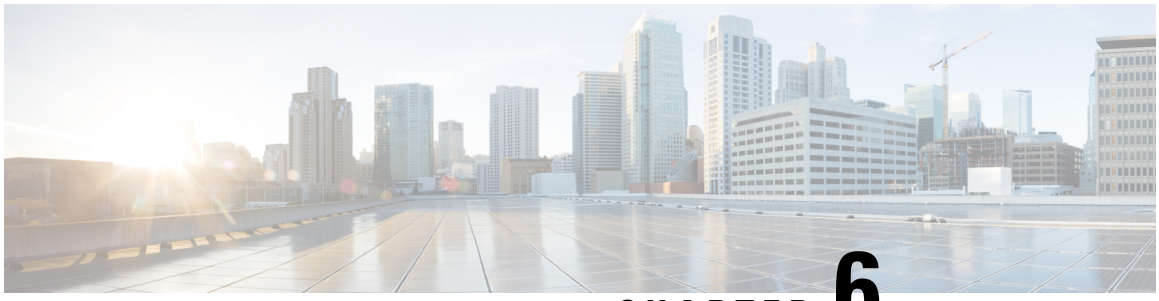
Switching Between LWAPP and Autonomous Images (AP CLI)

By default, the Cisco AP1532 and AP1572 are set to unified mode.

Procedure

- Switch the access point from LWAPP mode to autonomous mode (aIOS) by entering this command on the AP console:
  capwap ap autonomous

Note This command should be used only once, during initial priming of the access point. For information about switching back from autonomous mode to LWAPP mode, see https://supportforums.cisco.com/docs/DOC-14960.



CHAPTER 6

Checking the Health of the Network

- Show Mesh Commands, on page 167
- Viewing Mesh Statistics for a Mesh Access Point, on page 173
- Viewing Neighbor Statistics for a Mesh Access Point, on page 179

Show Mesh Commands

The **show mesh** commands are grouped under the following sections:

- Viewing General Mesh Network Details
- Viewing Mesh Access Point Details
- Viewing Global Mesh Parameter Settings
- Viewing Bridge Group Settings
- Viewing VLAN Tagging Settings
- Viewing DFS Details
- Viewing Security Settings and Statistics
- Viewing GPS Status

Viewing General Mesh Network Details

To view general mesh network details, enter these commands:

- **show mesh env** {**summary** | *AP_name*}—Shows the temperature, heater status, and Ethernet status for either all access points (summary) or a specific access point (AP_name). The access point name, role (RootAP or MeshAP), and model are also shown.
  - The temperature is shown in both Fahrenheit and Celsius.
  - The heater status is ON or OFF.
  - The Ethernet status is UP or DOWN.

Note The battery status appears as N/A (not applicable) in the **show mesh env** *AP_name* status display because it is not provided for access points.

```
(Cisco Controller) > show mesh env summary

AP Name             Temperature(C/F)  Heater  Ethernet  Battery
------------------  ----------------  ------  --------  -------
SB_RAP1              39/102           OFF     UpDnNANA  N/A
SB_MAP1              37/98            OFF     DnDnNANA  N/A
SB_MAP2              42/107           OFF     DnDnNANA  N/A
SB_MAP3              36/96            OFF     DnDnNANA  N/A

(Cisco Controller > show mesh env SB_RAP1
AP Name..................................... SB_RAP1
AP Model.................................... AIR-LAP1522AG-A-K9
AP Role..................................... RootAP

Temperature................................. 39 C, 102 F
Heater...................................... OFF
Backhaul.................................... GigabitEthernet0
GigabitEthernet0 Status..................... UP
    Duplex.................................. FULL
    Speed................................... 100
    Rx Unicast Packets...................... 988175
    Rx Non-Unicast Packets.................. 8563
    Tx Unicast Packets...................... 106420
    Tx Non-Unicast Packets.................. 17122
GigabitEthernet1 Status..................... DOWN
POE Out..................................... OFF
Battery..................................... N/A
```

- **show mesh ap summary**—Revised to show the CERT MAC field that shows a MAC address within an AP certificate that can be used to assign a username for external authentication.

```
(Cisco Controller) > show mesh ap summary
AP Name AP Model           BVI MAC            CERT MAC          Hop Bridge Group Name
------- ---------------    -----------------  ----------------- ---- ------------------
R1      LAP1520            00:0b:85:63:8a:10  00:0b:85:63:8a:10 0    y1
R2      LAP1520            00:0b:85:7b:c1:e0  00:0b:85:7b:c1:e0 1    y1
H2      AIR-LAP1522AG-A-K9 00:1a:a2:ff:f9:00  00:1b:d4:a6:f4:60 1
Number of Mesh APs.............................. 3
Number of RAP................................... 2
Number of MAP................................... 1
```

- **show mesh path**—Displays MAC addresses, access point roles, SNR ratios (dBs) for uplink and downlink (SNRUp, SNRDown) and link SNR for a particular path.

```
(Cisco Controller) > show mesh path mesh-45-rap1
AP Name/Radio Mac Channel Snr-Up Snr-Down Link-Snr Flags State
----------------- ------- ------ -------- -------- ------ -------
mesh-45-rap1      165     15     18       16       0x86b UPDATED NEIGH PARENT BEACON
mesh-45-rap1 is a Root AP.
```

- **show mesh neighbor summary**—Displays summary information about mesh neighbors. Neighbor information includes MAC addresses, parent-child relationships, and uplink and downlink (SNRUp, SNRDown).

```
(Cisco Controller) > show mesh neighbor summary ap1500:62:39:70
AP Name/Radio Mac Channel Snr-Up Snr-Down Link-Snr Flags  State
mesh-45-rap1      165     15     18       16       0x86b  UPDATED NEIGH PARENT BEACON
00:0B:85:80:ED:D0 149     5      6        5        0x1a60 NEED UPDATE BEACON DEFAULT
00:17:94:FE:C3:5F 149     7      0        0        0x860  BEACON
```



Note After review of the **show mesh** commands above, you should be able to see the relationships between the nodes of your network and verify the RF connectivity by seeing the SNR values for every link.

- **show mesh ap tree**—Displays mesh access points within a tree structure (hierarchy).

```
(Cisco Controller) > show mesh ap tree
R1(0,y1)
|-R2(1,y1)
|-R6(2,y1)
|-H2(1,default)
Number of Mesh APs.............................. 4
Number of RAP................................... 1
Number of MAP................................... 3
```

Viewing Mesh Access Point Details

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

- **show ap config general** *Cisco_AP*—Displays system specifications for a mesh access point.

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

- **show mesh astools stats** [*Cisco_AP*]—Displays anti-stranding statistics for all outdoor mesh access points or a specific mesh access point.

```
(Cisco Controller) > show mesh astools stats

Total No of Aps stranded : 0
> (Cisco Controller) > show mesh astools stats sb_map1

Total No of Aps stranded : 0
```

- **show advanced backup-controller**—Displays configured primary and secondary backup controllers.

```
(Cisco Controller) > show advanced backup-controller
AP primary Backup Controller ..................... controller1 10.10.10.10
AP secondary Backup Controller ..............  0.0.0.0
```

- **show advanced timer**—Displays settings for system timers.

```
(Cisco Controller) > show advanced timer
Authentication Response Timeout (seconds)........ 10
Rogue Entry Timeout (seconds)..................... 1300
AP Heart Beat Timeout (seconds).................. 30
AP Discovery Timeout (seconds)................... 10
AP Primary Discovery Timeout (seconds)........... 120
```

- **show ap slots**—Displays slot information for mesh access points.

```
(Cisco Controller) > show ap slots
Number of APs.................................... 3
AP Name Slots AP Model            Slot0    Slot1   Slot2    Slot3
------------------------------  ------  -------  ------   ------
R1       2    LAP1520            802.11A  802.11BG
H1       3    AIR-LAP1521AG-A-K9 802.11BG 802.11A  802.11A
H2       4    AIR-LAP1521AG-A-K9 802.11BG 802.11A  802.11A 802.11BG
```

Viewing Global Mesh Parameter Settings

Use this command to obtain information on global mesh settings:

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

```
(Cisco Controller) > show mesh config
Mesh Range....................................... 12000
Backhaul with client access status............... disabled
Background Scanning State........................ enabled
Mesh Security
Security Mode.................................. EAP
External-Auth.................................. disabled
Use MAC Filter in External AAA server......... disabled
Force External Authentication.................. disabled
Mesh Alarm Criteria
Max Hop Count.................................. 4
Recommended Max Children for MAP............... 10
Recommended Max Children for RAP............... 20
Low Link SNR................................... 12
High Link SNR.................................. 60
Max Association Number......................... 10
```

```
Association Interval.......................... 60 minutes
Parent Change Numbers......................... 3
Parent Change Interval........................ 60 minutes
Mesh Multicast Mode........................... In-Out
Mesh Full Sector DFS.......................... enabled
Mesh Ethernet Bridging VLAN Transparent Mode..... enabled
```

Viewing Bridge Group Settings

Use these commands to view bridge group settings:

- **show mesh forwarding table**—Shows all configured bridges and their MAC table entries.
- **show mesh forwarding interfaces**—Displays bridge groups and the interfaces within each bridge group. This command is useful for troubleshooting bridge group membership.

Viewing VLAN Tagging Settings

Use these commands to view VLAN tagging settings:

- **show mesh forwarding VLAN mode**—Shows the configured VLAN Transparent mode (enabled or disabled).
- **show mesh forwarding VLAN statistics**—Displays statistics for the VLAN and the path.
- **show mesh forwarding vlans**—Displays supported VLANs.
- **show mesh ethernet VLAN statistics**—Displays statistics for the Ethernet interface.

Viewing DFS Details

Use this command to view DFS details:

- **show mesh dfs history**—Displays a history of radar detections by channels and resulting outages.

```
(Cisco Controller) > show mesh dfs history
ap1520#show mesh dfs history
Channel 100 detects radar and is unusable (Time Elapsed: 18 day(s), 22 hour(s), 10
minute(s), 24 second(s)).
Channel is set to 136 (Time Elapsed: 18 day(s), 22 hour(s), 10 minute(s), 24 second(s)).
Channel 136 detects radar and is unusable (Time Elapsed: 18 day(s), 22 hour(s), 9
minute(s), 14 second(s)).
Channel is set to 161 (Time Elapsed: 18 day(s), 22 hour(s), 9 minute(s), 14 second(s)).
Channel 100 becomes usable (Time Elapsed: 18 day(s), 21 hour(s), 40 minute(s), 24
second(s)).
Channel 136 becomes usable (Time Elapsed: 18 day(s), 21 hour(s), 39 minute(s), 14
second(s)).
Channel 64 detects radar and is unusable (Time Elapsed: 0 day(s), 1 hour(s), 20 minute(s),
 52 second(s)).
Channel 104 detects radar and is unusable (Time Elapsed: 0 day(s), 0 hour(s), 47
minute(s), 6 second(s)).
Channel is set to 120 (Time Elapsed: 0 day(s), 0 hour(s), 47 minute(s), 6 second(s)).
```

- **show mesh dfs channel** *channel number*—Displays a history of radar detections and outages for a specified channel.

```
(Cisco Controller) > show mesh dfs channel 104
ap1520#show mesh dfs channel 104
Channel 104 is available
Time elapsed since radar last detected: 0 day(s), 0 hour(s), 48 minute(s), 11 second(s).
```

Viewing Security Settings and Statistics

Use this command to view security settings and statistics:

- **show mesh security-stats** *AP_name*—Shows packet error statistics and a count of failures, timeouts, and successes with respect to associations and authentications as well as reassociations and reauthentications for the specified access point and its child.

```
(Cisco Controller) > show mesh security-stats ap417

AP MAC : 00:0B:85:5F:FA:F0
Packet/Error Statistics:
----------------------------
Tx Packets 14, Rx Packets 19, Rx Error Packets 0
Parent-Side Statistics:
-------------------------
Unknown Association Requests 0
Invalid Association Requests 0
Unknown Re-Authentication Requests 0
Invalid Re-Authentication Requests 0
Unknown Re-Association Requests 0
Invalid Re-Association Requests 0
Unknown Re-Association Requests 0
Invalid Re-Association Requests 0
Child-Side Statistics:
-------------------------
Association Failures 0
Association Timeouts 0
Association Successes 0
Authentication Failures 0
Authentication Timeouts 0
Authentication Successes 0
Re-Association Failures 0
Re-Association Timeouts 0
Re-Association Successes 0
Re-Authentication Failures 0
Re-Authentication Timeouts 0
Re-Authentication Successes 0
```

Viewing GPS Status

Procedure

- See location summary of all APs by entering this command:

  show ap gps location summary

```
(Site5_AMC_02) >show ap gps location summary

AP Name             GPS Present   Latitude       Longitude       Altitude        GPS
location Age
------------------  -----------   ------------   -------------   -------------
------------------------
SJC24-RAP-EAST      NO            N/A            N/A             N/A             N/A
SJC21-RAP-NORTH     NO            N/A            N/A             N/A             N/A
SJC21-RAP-SOUTH     NO            N/A            N/A             N/A             N/A
Site5_21-17         NO            N/A            N/A             N/A             N/A
SJC22-ROOF-MAP      NO            N/A            N/A             N/A             N/A
Site5_21-28         NO            N/A            N/A             N/A             N/A
SJC-24-RAP-WEST     YES           37.42034194    -121.91973098   25.10  meters   000
days, 00 h 00 m 19 s
Site5_24-02         YES           37.41970399    -121.92051996   10.00  meters   000
days, 00 h 00 m 12 s
Site5_22-30         NO            N/A            N/A             N/A             N/A
Site5_23-200        NO            N/A            N/A             N/A             N/A
Site5_25-18         NO            N/A            N/A             N/A             N/A
Site5_22-15         NO            N/A            N/A             N/A             N/A
Site5_25-05         NO            N/A            N/A             N/A             N/A
```

- See a location summary of all mesh APs by entering this command:

  show mesh gps location summary

- See the location information for a particular mesh AP by entering this command:

  show mesh gps location *ap-name*

Viewing Mesh Statistics for a Mesh Access Point

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

Note You can modify the Statistics Timer interval setting on the **All APs > Details** page of the controller GUI.

Viewing Mesh Statistics for a Mesh Access Point (GUI)

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

Step 2 To view statistics for a specific mesh access point, hover the mouse over the blue drop-down arrow for the desired mesh access point and choose **Statistics**. The **All APs** > *AP Name* > **Statistics** page for the selected mesh access point appears.

This page shows the role of the mesh access point in the mesh network, the name of the bridge group to which the mesh access point belongs, the backhaul interface on which the access point operates, and the number of the physical switch port. It also displays a variety of mesh statistics for this mesh access point.

Table 34: Mesh Access Point Statistics

Statistics	Parameter	Description
Mesh Node Stats	Malformed Neighbor Packets	The number of malformed packets received from the neighbor. Examples of malformed packets include malicious floods of traffic such as malformed or short DNS packets and malformed DNS replies.
	Poor Neighbor SNR Reporting	The number of times the signal-to-noise ratio falls below 12 dB on the backhaul link.
	Excluded Packets	The number of packets received from excluded neighbor mesh access points.
	Insufficient Memory Reporting	The number of insufficient memory conditions.
	Rx Neighbor Requests	The number of broadcast and unicast requests received from the neighbor mesh access points.
	Rx Neighbor Responses	The number of responses received from the neighbor mesh access points.
	Tx Neighbor Requests	The number of unicast and broadcast requests sent to the neighbor mesh access points.
	Tx Neighbor Responses	The number of responses sent to the neighbor mesh access points.
	Parent Changes Count	The number of times a mesh access point (child) moves to another parent.
	Neighbor Timeouts Count	The number of neighbor timeouts.

Statistics	Parameter	Description
Queue Stats	Gold Queue	The average and peak number of packets waiting in the gold (video) queue during the defined statistics time interval.
	Silver Queue	The average and peak number of packets waiting in the silver (best effort) queue during the defined statistics time interval.
	Platinum Queue	The average and peak number of packets waiting in the platinum (voice) queue during the defined statistics time interval.
	Bronze Queue	The average and peak number of packets waiting in the bronze (background) queue during the defined statistics time interval.
	Management Queue	The average and peak number of packets waiting in the management queue during the defined statistics time interval.

Statistics	Parameter	Description
Mesh Node Security Stats	Transmitted Packets	The number of packets transmitted during security negotiations by the selected mesh access point.
	Received Packets	The number of packets received during security negotiations by the selected mesh access point.
	Association Request Failures	The number of association request failures that occur between the selected mesh access point and its parent.
	Association Request Timeouts	The number of association request timeouts that occur between the selected mesh access point and its parent.
	Association Requests Successful	The number of successful association requests that occur between the selected mesh access point and its parent.
	Authentication Request Failures	The number of failed authentication requests that occur between the selected mesh access point and its parent.
	Authentication Request Timeouts	The number of authentication request timeouts that occur between the selected mesh access point and its parent.
	Authentication Requests Successful	The number of successful authentication requests between the selected mesh access point and its parent.
	Reassociation Request Failures	The number of failed reassociation requests between the selected mesh access point and its parent.
	Reassociation Request Timeouts	The number of reassociation request timeouts between the selected mesh access point and its parent.
	Reassociation Requests Successful	The number of successful reassociation requests between the selected mesh access point and its parent.
	Reauthentication Request Failures	The number of failed reauthentication requests between the selected mesh access point and its parent.
	Reauthentication Request Timeouts	

Statistics	Parameter	Description
		The number of reauthentication request timeouts that occur between the selected mesh access point and its parent.
	Reauthentication Requests Successful	The number of successful reauthentication requests that occur between the selected mesh access point and its parent.
	Unknown Association Requests	The number of unknown association requests received by the parent mesh access point from its child. The unknown association requests often occur when a child is an unknown neighbor mesh access point.
	Invalid Association Requests	The number of invalid association requests received by the parent mesh access point from the selected child mesh access point. This state may occur when the selected child is a valid neighbor but is not in a state that allows association.

Statistics	Parameter	Description
Mesh Node Security Stats (continued)	Unknown Reauthentication Requests	The number of unknown reauthentication requests received by the parent mesh access point node from its child. This state may occur when a child mesh access point is an unknown neighbor.
	Invalid Reauthentication Requests	The number of invalid reauthentication requests received by the parent mesh access point from a child. This state may occur when a child is a valid neighbor but is not in a proper state for reauthentication.
	Unknown Reassociation Requests	The number of unknown reassociation requests received by the parent mesh access point from a child. This state may occur when a child mesh access point is an unknown neighbor.
	Invalid Reassociation Requests	The number of invalid reassociation requests received by the parent mesh access point from a child. This state may occur when a child is a valid neighbor but is not in a proper state for reassociation.

Viewing Mesh Statistics for an Mesh Access Point (CLI)

Use these commands to view mesh statistics for a specific mesh access point using the controller CLI:

- To view packet error statistics, a count of failures, timeouts, and successes with respect to associations and authentications, and reassociations and reauthentications for a specific mesh access point, enter this command:

  show mesh security-stats *AP_name*

  Information similar to the following appears:

```
AP MAC : 00:0B:85:5F:FA:F0
Packet/Error Statistics:
----------------------------
x Packets 14, Rx Packets 19, Rx Error Packets 0

Parent-Side Statistics:
-------------------------
Unknown Association Requests 0
Invalid Association Requests 0
Unknown Re-Authentication Requests 0
Invalid Re-Authentication Requests 0
```

```
Unknown Re-Association Requests 0
Invalid Re-Association Requests 0
Unknown Re-Association Requests 0
Invalid Re-Association Requests 0

Child-Side Statistics:
--------------------------
Association Failures 0
Association Timeouts 0
Association Successes 0
Authentication Failures 0
Authentication Timeouts 0
Authentication Successes 0
Re-Association Failures 0
Re-Association Timeouts 0
Re-Association Successes 0
Re-Authentication Failures 0
Re-Authentication Timeouts 0
Re-Authentication Successes 0
```

- To view the number of packets in the queue by type, enter this command:

  show mesh queue-stats *AP_name*

  Information similar to the following appears:

```
Queue Type  Overflows  Peak length  Average length
 ----------  ---------  -----------  --------------
 Silver      0          1            0.000
 Gold        0          4            0.004
 Platinum    0          4            0.001
 Bronze      0          0            0.000
 Management  0          0            0.000
```

  Overflows—The total number of packets dropped due to queue overflow.

  Peak Length—The peak number of packets waiting in the queue during the defined statistics time interval.

  Average Length—The average number of packets waiting in the queue during the defined statistics time interval.

Viewing Neighbor Statistics for a Mesh Access Point

This section describes how to use the controller GUI or CLI to view neighbor statistics for a selected mesh access point. It also describes how to run a link test between the selected mesh access point and its parent.

Viewing Neighbor Statistics for a Mesh Access Point (GUI)

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

Step 2 To view neighbor statistics for a specific mesh access point, hover the mouse over the blue drop-down arrow for the desired mesh access point and choose **Neighbor Information**. The All APs > *Access Point Name* > Neighbor Info page for the selected mesh access point appears.

This page lists the parent, children, and neighbors of the mesh access point. It provides each mesh access point's name and radio MAC address.

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

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

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

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

Step 4 To view the details for any of the mesh access points on this page, follow these steps:

a) Hover the mouse over the blue drop-down arrow for the desired mesh access point and choose **Details**. The **All APs** > *Access Point Name* > **Link Details** > *Neighbor Name* page appears.

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

Step 5 To view statistics for any of the mesh access points on this page, follow these steps:

a) Hover the mouse over the blue drop-down arrow for the desired mesh access point and choose **Stats**. The **All APs** > *Access Point Name* > **Mesh Neighbor Stats** page appears.

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

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

Use these commands to view neighbor statistics for a specific mesh access point using the controller CLI.

- To view the mesh neighbors for a specific mesh access point, enter this command:

  show mesh neigh {**detail** | **summary**} *AP_Name*

  Information similar to the following appears when you request a summary display:

```
AP Name/Radio Mac   Channel Snr-Up Snr-Down Link-Snr Flags  State
-----------------  ------- ------ -------- -------- ------  -------
mesh-45-rap1       165     15     18       16       0x86b  UPDATED NEIGH PARENT BEACON
00:0B:85:80:ED:D0  149      5      6        5       0x1a60  NEED UPDATE BEACON DEFAULT
00:17:94:FE:C3:5F  149    7      0        0      0x860      BEACON
```

- To view the channel and signal-to-noise ratio (SNR) details for a link between a mesh access point and its neighbor, enter this command:

  show mesh path *AP_Name*

  Information similar to the following appears:

```
AP Name/Radio Mac  Channel Snr-Up Snr-Down Link-Snr Flags  State
-----------------  ------- ------ -------- -------- ------  -------
mesh-45-rap1       165     15     18       16       0x86b  UPDATED NEIGH PARENT BEACON
mesh-45-rap1 is a Root AP.
```

- To view the percentage of packet errors for packets transmitted by the neighbor mesh access point, enter this command:

  show mesh per-stats *AP_Name*

  Information similar to the following appears:

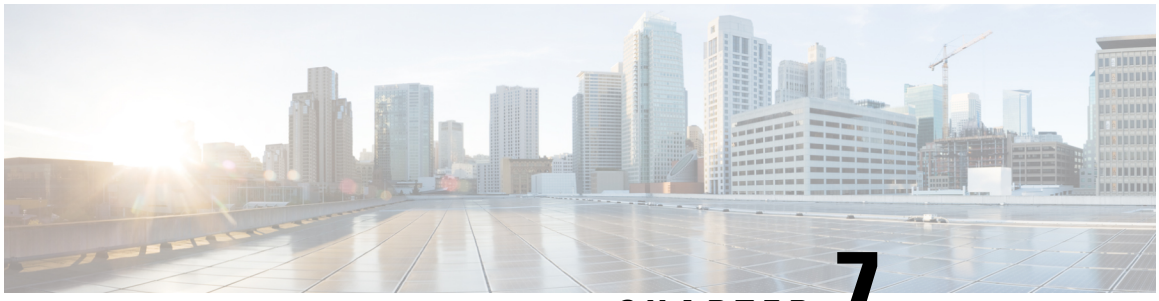
```
Neighbor MAC Address 00:0B:85:5F:FA:F0
Total Packets transmitted: 104833
Total Packets transmitted successfully: 104833
Total Packets retried for transmission: 33028

Neighbor MAC Address 00:0B:85:80:ED:D0
Total Packets transmitted: 0
Total Packets transmitted successfully: 0
Total Packets retried for transmission: 0

Neighbor MAC Address 00:17:94:FE:C3:5F
Total Packets transmitted: 0
Total Packets transmitted successfully: 0
Total Packets retried for transmission: 0
```



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



CHAPTER 7

Troubleshooting Mesh Access Points

• Installation and Connections, on page 183

Installation and Connections

Step 1 Connect the mesh access point that you want to be the RAP to the controller.

Step 2 Deploy the radios (MAP) at the desired locations.

Step 3 On the controller CLI, enter the **show mesh ap summary** command to see all MAPs and RAPs on the controller.

Figure 65: Show Mesh AP Summary Page

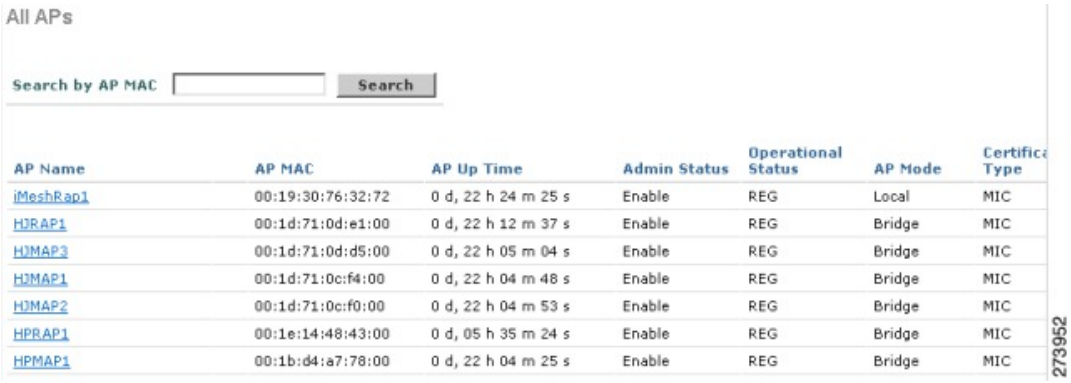
```
(Cisco Controller) >show mesh ap summary

AP Name                AP Model             BVI MAC            CERT MAC       Hop  Bridge Group Name  Enhanced Feature Set
-----------------  ------------------  -----------------  -----------------  ---  -----------------  --------------------
1532MAP2-DaisyChained  AIR-CAP1532E-A-K9    4c:4e:35:46:f2:72  4c:4e:35:46:f2:72  0    default            N/A
1532RAP1             AIR-CAP1532E-A-K9    4c:4e:35:46:f2:64  4c:4e:35:46:f2:64  0    default            N/A
1532MAP1             AIR-CAP1532E-A-K9    4c:4e:35:46:f1:4e  4c:4e:35:46:f1:4e  1    default            N/A
1524PSRAP1           AIR-LAP1524PS-A-K9   00:22:be:41:23:00  00:22:be:41:23:00  0    MESHDEMO1          N/A
1522MAP2             AIR-LAP1522AG-A-K9   00:22:be:42:fe:00  00:22:be:42:fe:00  1    MESHDEMO1          N/A

Number of Mesh APs.............................. 3
Number of RAPs.................................. 2
Number of MAPs.................................. 1
Number of Flex+Bridge APs....................... 2
Number of Flex+Bridge RAPs...................... 1
Number of Flex+Bridge MAPs...................... 1
```

Step 4 On the controller GUI, click **Wireless** to see the mesh access point (RAP and MAP) summary.

Figure 66: All APs Summary Page



Step 5 Click **AP Name** to see the details page and then select the **Interfaces** tab to see the active radio interfaces.

The radio slot in use, radio type, subband in use, and operational status (UP or DOWN) are summarized.

- All APs supports 2 radio slots: slot 0—2.4 GHz and slot 1—5 GHz.

  If you have more than one controller connected to the same mesh network, then you must specify the name of the primary controller using global configuration for every mesh access point or specify the primary controller on every node, otherwise the least loaded controller is the preferred controller. If the mesh access points were previously connected to a controller, they already have learned a controller's name.

  After configuring the controller name, the mesh access point reboots.

Step 6 Click **Wireless > AP Name** to check the mesh access point's primary controller on the AP details page.

Debug Commands

The following two commands are very helpful to see the messages being exchanged between mesh access points and the controller.

```
(Cisco Controller) > debug capwap events enable
(Cisco Controller) > debug disable-all
```

You can use the **debug** command to see the flow of packet exchanges that occur between the mesh access point and the controller. The mesh access point initiates the discovery process. An exchange of credentials takes place during the join phase to authenticate that the mesh access point is allowed to join the mesh network.

Upon a successful join completion, the mesh access point sends a CAPWAP configuration request. The controller responds with a configuration response. When a Configure Response is received from the controller, the mesh access point evaluates each configuration element and then implements them.

Remote Debug Commands

You can log on to the mesh access point console for debugging either through a direct connection to the AP console port or through the remote debug feature on the controller.

To invoke remote debug on the controller, enter the following commands:

```
(Cisco Controller) > debug ap enable ap-name
(Cisco Controller) > debug ap command command ap-name
```

AP Console Access

AP1500s have a console port. A console cable is not shipped with the mesh access point. For the 1550 series access points, console ports are easily accessible and you need not open the access point box.

The AP1500s have console access security embedded in the code to prevent unauthorized access on the console port and provide enhanced security.

The **login ID** and **password** for console access are configured from the controller. You can use the following commands to push the username/password combination to the specified mesh access point or all access points:

```
<Cisco Controller> config ap username cisco password cisco ?

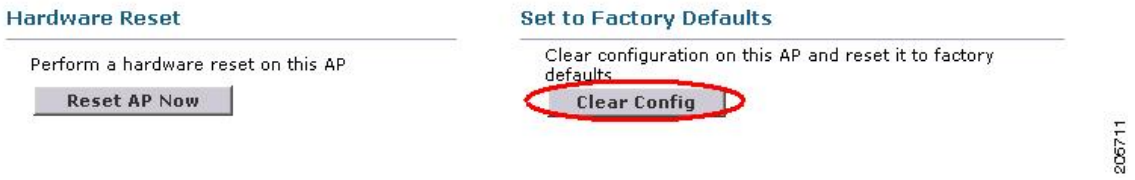
all           Configures the Username/Password for all connected APs.
<Cisco AP>    Enter the name of the Cisco AP.

<Cisco Controller> config ap username cisco password cisco all
```

You must verify whether the username/password pushed from the controller is used as *user-id* and *password* on the mesh access point. It is a nonvolatile setting. Once set, a *login ID* and *password* are saved in the private configuration of the mesh access point.

Once you have a successful login, the trap is sent to the Cisco Prime Infrastructure. If a user fails to log on three times consecutively, login failure traps are sent to the controller and Cisco Prime Infrastructure.

Caution A mesh access point must be reset to the factory default settings before moving from one location to another.



Cable Modem Serial Port Access From an AP

Commands can be sent to the cable modem from the privileged mode of the CLI. Use the command to take a text string and send it to the cable modem UART interface. The cable modem interprets the text string as one of its own commands. The cable modem response is captured and displayed on the Cisco IOS console. Up to 9600 characters are displayed from the cable modem. Any text that is greater than 4800 characters is truncated.

The modem commands are only operational on mesh APs that have devices connected to the UART port originally intended for the cable modem. If the commands are used on a mesh AP that does not have a cable modem (or any other device connected to the UART), the commands are accepted, however, but they do not produce any returned output. No errors are explicitly flagged.

Configuration

Enter the following command from the privileged mode of the MAP:

```
AP#send cmodem timeout-value modem-command
```

The modem command is any command or text to send to the cable modem. The range of timeout value is 1 to 300 seconds. However, if the captured data equals 9600 characters, any text beyond that is truncated and the response, irrespective of the timeout value and is immediately displayed on the AP console.

Figure 67: Cable Modem Console Access Command

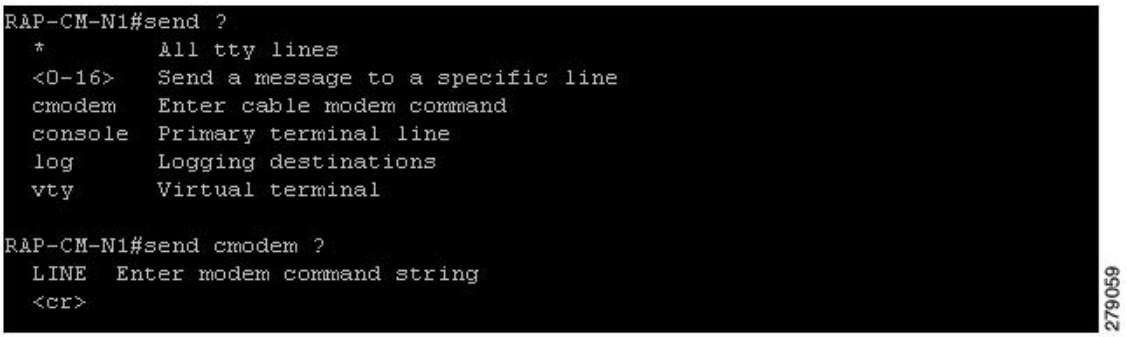
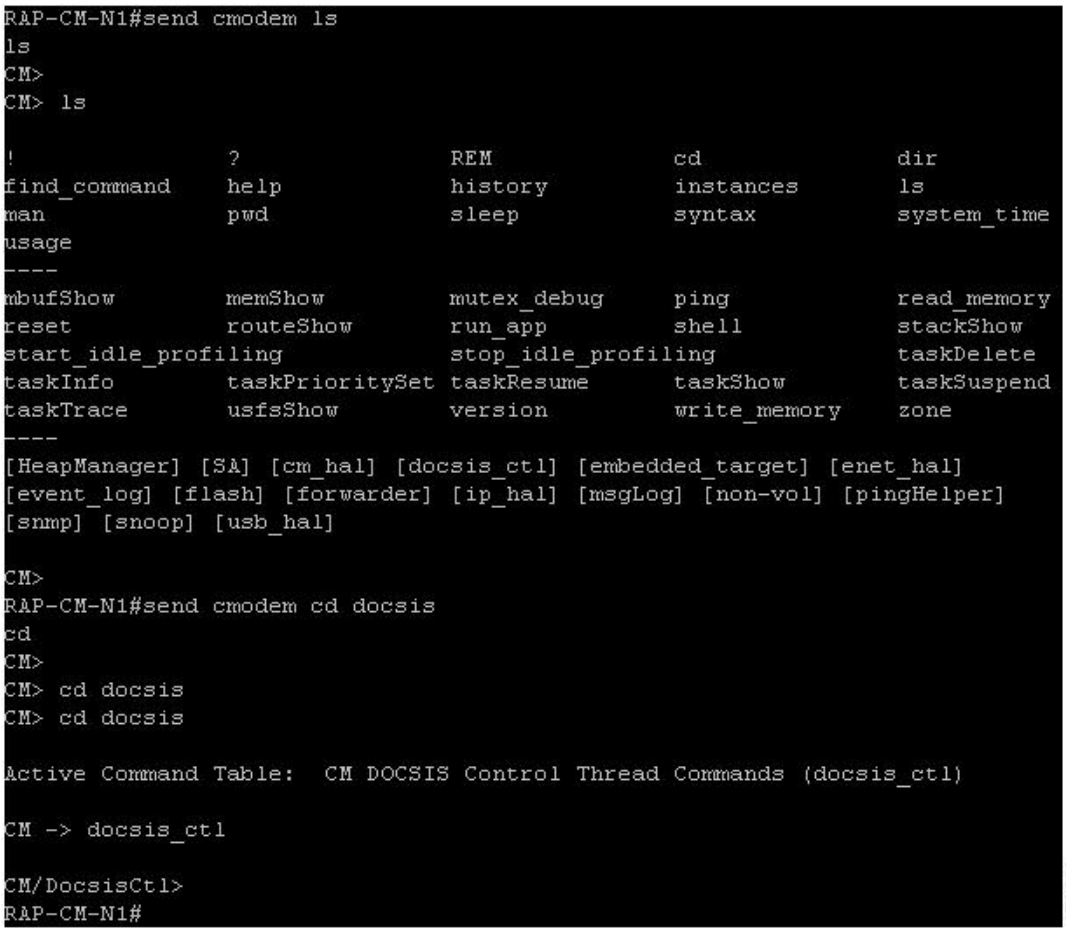


Figure 68: Cable Modem Console Access Command



Caution The question mark (?) and the exclamation point (!) should not be used in the **send cmodem** command. These characters have immediate interpreted use in the Cisco IOS CLI. Therefore, they cannot be sent to the modem.

Enabling the Cable Modem Console Port

By default, the Cable Modem console port is disabled. This is to prevent users from accessing the console through their residential cable modem. In the AP1572IC, AP1572EC, and AP1552C model, the cable modem console is connected directly to the access point. The console port is required for signaling between the AP and the cable modem. There are two methods to enable the cable modem console port, either through SNMP or by adding the command to the configuration .cm file on the CMTS.

Note For the AP1572EC, AP1572IC, AP1552C, and AP1552CU, the cable modem must be enabled.

- Enable the cable modem console port through SNMP by entering this command to the IP address of the cable modem:

```
snmpset –c private IP_ADDRESS cmConsoleMode.0 i N
```

Using the OID, enter this command:

```
snmpset –c private IP_ADDRESS
1.3.6.1.4.1.1429.77.1.4.7.0 i N
```

Where IP_ADDRESS is any IPv4 address and N is an integer, 2 to enable read-write, 1 for read-only, or 0 to disable.

Example:

```
snmpset –c private 209.165.200.224 cmConsoleMode.0 i 2
```

- Enable the cable modem console port through the configuration file. The configuration file (with a .cm extension) is loaded into the cable modem head end. It is pushed to the cable modem as part of the join process. Enter the following line to the cable modem configuration file:

  ```
  SA-CM-MIB::cmConsoleMode.0 = INTEGER: readWrite(2)
  ```

  Using the OID, enter this line:

  ```
  SA-CM-MIB::cmConsoleMode.0 = INTEGER: readWrite(2)
  ```

Resetting the AP1572xC/AP1552C Through the Cable Modem

An AP can be reset by entering an SNMP command to the Cable Modem, which resides inside the access point. For this feature to work, you must enable the cable modem console port.

Reset the AP by entering this snmpset command:

```
Snmpset -v2c -c public IP ADDRESS 1.3.6.1.4.1.1429.77.1.3.17.0 i 1
```

Where the IP ADDRESS is the IPv4 address of the cable modem.

Mesh Access Point CLI Commands

You can enter these commands directly on the mesh access point using the AP console port or you can use the remote debug feature from the controller:

```
Hl •shou lllBSh ?
  adjacency   l'ESH Adjacency
  astools     l'ESH Anti-strand tools
  backhaul    l'ESH backhaul
  channel     l'ESH channel
  canfig      l'ESH config paranenter
  dfs         l'ESH dfs lnfornatIon
  ethernet    sllou nesh Erthernet bridging
  foruarding  l'ESH Foruarding
  irwenlory   platforn inventory
  linktest    l'ESH linktest stats
  nmule       l'ESH nodule detail
  np!rf       l'ESH BN tool
  security    l'ESH  Security  shou        !2
  simulation  flESH sinul ated configLration ih
  status      l'ESH status
                                           Ul
```

```
HJRAPllleliou nesh config
rtsfhresliold l la 0, eHs 0, a.11in 0, c:o.11ex 0
rtsfhresholdl llbg 0, aifs 0, a.1Hin 0, a.11ax 0
huRetrles O. llri<Rate O qOepth O
8O2.11MAt ient Statistics Push Int.......al: 3
range paraneter: 12000
nesh security node: 0
Universal Client Access: disabled
publ ic safety global state: enabled
Battery backup state: enabled
nul ticast node: in-out
Ful l Sector DFS: enabled
```

```
HJRAPlllehou caplolBp client mb
Adnin5tate                          ADHIN ENABLED
SuVer                               S.2.98.0
NunFll ledSlots                     2
Nane                                HJRAPl
Location                            default location
Huarllame                           SEYf-CllffROLLER
Huarrlp                             209.165.200.227
Huartt.Ner                          0.0.0.0
ApHocle                              Brld!JE!
ApSubl'lode                         Not [:mf igured
OperationState                      UP
CAPllN'Path nru                     1485
Link!U:liting                       disabled
ApRole                              RootAP
ApBac:khaul                         802.1 la
Ap8ac:khaulthannel                  5805
ApBac:khaulSlot                     1
ApBac:khaul 11gEnabled              0
ApBac:l<haullxRate                  24000
Ethernet Brldglrg State             0
Public Safety State                 enabled
```

```
HJHAPlllehoi.I nesh adjacency ?
  alI      HESH Adjacency AlI
  child    HESH Adjacency Child
  parent MESH Adjacency Parent
                                                    01
```

```
HJMap4#shou mesh status
 shou MESH Status
 MeshAP in state Maint
 Uplink Backbone: Virtual-DotllRadio0
 Dounlink Backbone: Dot11Radiol
 Configured BGN: HuckJr
       rxNeighReq 129790 rxNeighRsp 66976 txNeighReq 33938 txNeighRsp 129790
       rxNeighRsp 147275 txNeighUpd 202060
       nextchan 0 nextant 0 downAnt 0 downChan 0 curAnts 0
       nextNeigh 1. malformedNeighPackets 4.poorNeighSnr 1
       blacklistPackets 0,insufficientMemory 0, authenticationFailures 0
       Parent Changes 3, Neighbor Timeouts 0
       Vector through 0017.94fe.c3bf:
              Vector ease 1 -1, FWD: 0017.94fe.c3bf
                                                    273949
```

```
HJNap4#shou mesh forwarding link
 Current mesh links:
----------------------
 End Point  : 0017.94fe.c3bf
 Adjacency  : Exists
 Channel    : 161 on Dot11Radiol
 Type       : 2
 State      : 4
 Bundle     : member
 Bridge     : 1
 swidb      : Virtual-Dot11Radio0
 port state : OPEN
                                                    273950
```

Mesh Access Point Debug Commands

You can enter these commands directly on the mesh access point using the AP console port or you can use the remote debug feature from the controller.

- **debug mesh ethernet bridging**—Debugs Ethernet bridging.
- **debug mesh ethernet config**—Debugs access and trunk port configuration associated with VLAN tagging.
- **debug mesh ethernet registration**—Debugs the VLAN registration protocol. This command is associated with VLAN tagging.
- **debug mesh forwarding table**—Debugs the forwarding table containing bridge groups.
- **debugs mesh forwarding packet bridge-group**—Debugs the bridge group configuration.

Defining Mesh Access Point Role

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

Backhaul Algorithm

A **backhaul** is used to create only the wireless connection between mesh access points.

The backhaul interface by default is 802.11a. You cannot change the backhaul interface to 802.11b/g.

The "auto" data rate is selected by default for AP1500s.

The backhaul algorithm has been designed to fight against stranded mesh access point conditions. This algorithm also adds a high-level of resiliency for each mesh node.

The algorithm can be summarized as follows:

- A MAP always sets the Ethernet port as the **primary backhaul** if it is UP; otherwise, it is the 802.11a radio (this feature gives the network administrator the ability to configure it as a RAP the first time and recover it in-house). For fast convergence of the network, we recommend that you do not connect any Ethernet device to the MAP for its initial joining to the mesh network.
- A MAP failing to connect to a WLAN controller on an Ethernet port that is UP, sets the 802.11a radio as the **primary backhaul**. Failing to find a neighbor or failing to connect to a WLAN controller via any neighbor on the 802.11a radio causes the **primary backhaul** to be UP on the Ethernet port again. A MAP gives preference to the parent which has the same BGN.
- A MAP connected to a controller over an Ethernet port does not build a mesh topology (unlike a RAP).
- A RAP always sets the Ethernet port as the **primary backhaul**.



Note Cisco Wave 2 APs operating as RAPs can fall back on Ethernet sooner than 15 minutes if the RAPs cannot find any valid uplink on the radio in 5 minutes' time. In such a case, the RAPs clear the blocked-listing on the wired port and try to fall back on the wired port.

- If the Ethernet port on a RAP is DOWN, or a RAP fails to connect to a controller on an Ethernet port that is UP, the 802.11a radio is set as the **primary backhaul**. Failing to find a neighbor or failing to connect to a controller via any neighbor on the 802.11a radio makes the RAP go to the SCAN state after 15 minutes and starts with the Ethernet port first.

Keeping the roles of mesh nodes distinct using the above algorithm greatly helps to avoid a mesh access point from being in an unknown state and becoming stranded in a live network.

Passive Beaconing (Anti-Stranding)

When enabled, passive beaconing allows a stranded mesh access point to broadcast its debug messages over-the-air using a 802.11b/g radio. A neighboring mesh access point that is listening to the stranded mesh access point and has a connection to a controller, can pass those messages to the controller over CAPWAP. Passive beaconing prevents a mesh access point that has no wired connection from being stranded.

Debug logs can also be sent as distress beacons on a nonbackhaul radio so that a neighboring mesh access point can be dedicated to listen for the beacons.

The following steps are automatically initiated at the controller when a mesh access point loses its connection to the controller:

- Identifies the MAC address of a stranded mesh access point
- Finds a nearby neighbor that is CAPWAP connected
- Sends commands through remote debug
- Cycles channels to follow the mesh access point

You only have to know the MAC address of the stranded AP to make use of this feature.

A mesh access point is considered stranded if it goes through a lonely timer reboot. When the lonely timer reboot is triggered, the mesh access point, which is now stranded, enables passive beaconing, the anti-stranding feature.

This feature can be divided into three parts:

- Strand detection by stranded mesh access point
- Beacons sent out by stranded mesh access point
    - Latch the 802.11b radio to a channel (1,6,11)
    - Enable debugs
    - Broadcast the standard debug messages as distress beacons
    - Send Latest Crash info file
- Receive beacons (neighboring mesh access point with remote debugging enabled)

Deployed mesh access points constantly look for stranded mesh access points. Periodically, mesh access points send a list of stranded mesh access points and SNR information to the controller. The controller maintains a list of the stranded mesh access points within its network.

When the **debug mesh astools troubleshoot** *mac-addr* **start** command is entered, the controller runs through the list to find the MAC address of the stranded mesh access point.

A message is sent to the best neighbor to start listening to the stranded access point. The listening mesh access point gets the distress beacons from the stranded mesh access point and sends it to the controller.

Once a mesh access point takes the role of a listener, it does not purge the stranded mesh access point from its internal list until it stops listening to the stranded mesh access point. While a stranded mesh access point is being debugged, if a neighbor of that mesh access point reports a better SNR to the controller than the current listener by some percentage, then the listener of the stranded mesh access point is changed to the new listener (with better SNR) immediately.

End-user commands are as follows:

- **config mesh astools** [**enable** | **disable**]—Enables or disables the astools on the mesh access points. If disabled, APs no longer sends a stranded AP list to the controller.
- **show mesh astools stats**—Shows the list of stranded APs and their listeners if they have any.
- **debug mesh astools troubleshoot** *mac-addr* **start**—Sends a message to the best neighbor of the *mac-addr* to start listening.
- **debug mesh astools troubleshoot** *mac-addr* **stop**—Sends a message to the best neighbor of the *mac-addr* to stop listening.
- **clear mesh stranded** [**all** | *mac of b/g radio*]—Clears stranded AP entries.

The controller console is swamped with debug messages from stranded APs for 30 minutes.

Dynamic Frequency Selection

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

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

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

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

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



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

Figure 69: DFS and TPC Band Requirements



DFS in RAP

The RAP performs the following steps as a response to radar detection:

1. The RAP sends a message to the controller that the channel is infected with radar. The channel is marked as infected on the RAP and on the controller.
2. The RAP blocks the channel for 30 minutes. This 30-minute period is called the nonoccupancy period.
3. The controller sends a TRAP, which indicates that the radar has been detected on the channel. A TRAP remains until the nonoccupancy period expires.
4. The RAP has 10 seconds to move away from the channel. This period is called the channel move time, which is defined as the time for the system to clear the channel and is measured from the end of the radar burst to the end of the final transmission on the channel.
5. The RAP enters the quiet mode. In the quiet mode, the RAP stops data transmissions. Beacons are still generated and probe responses are still delivered. The quiet mode exists until the channel move time is over (10 seconds).
6. The controller picks up a new random channel and sends the channel information to the RAP.
7. The RAP receives the new channel information and sends channel change frames (unicast, encrypted) to the MAP, and each MAP sends the same information to its lower children down the sector. Each mesh access point sends the channel change frames once every 100 msecs for a total of five times.
8. The RAP tunes to the new channel and enters into the silent mode. During the silent mode, only the receiver is ON. The RAP keeps scanning the new channel for any radar presence for 60 seconds. This process is called channel availability check (CAC).
9. The MAP tunes to the new channel and enters into the silent mode. During the silent mode, only the receiver is ON. The MAP keeps scanning the new channel for any radar presence for 60 seconds.
10. If radar is not detected, the RAP resumes full functionality on this new channel and the whole sector tunes to this new channel.

DFS in MAP

The MAP performs the following steps as a response to radar detection:

1. The MAP sends a radar seen indication to the parent and ultimately to the RAP indicating that the channel is infected. The RAP sends this message to the controller. The message appears to be coming from the RAP. The MAP, RAP, and controller mark the channel as infected for 30 minutes.
2. The MAP blocks the channel for 30 minutes. This 30-minute period is called the nonoccupancy period.
3. The controller sends a TRAP, which indicates that the radar has been detected on the channel. The TRAP remains until the nonoccupancy period expires.
4. The MAP has 10 seconds to move away from the channel. This is called the channel move time, which is defined as the time for the system to clear the channel and is measured from the end of the radar burst to the end of the final transmission on the channel.
5. The MAP enters the quiet mode. In the quiet mode, the MAP stops data transmissions. Beacons are still generated and probe responses are still delivered. The quiet mode exists until the channel move time is over (10 seconds).
6. The controller picks up a new random channel and sends the channel to the RAP.
7. The RAP receives the new channel information and sends channel change frames (unicast, encrypted) to a MAP, and each MAP sends the same information to its lower children down the sector. Each mesh access point sends the channel change frames once every 100 msecs for a total of five times.
8. Each mesh access point tunes to the new channel and enters into the silent mode. During the silent mode, only the receiver is ON. There is no packet transmission. An AP keeps scanning the new channel for any radar presence for 60 seconds. This process is called the channel availability check (CAC). The MAP should not disconnect from the controller. The network should remain stable during this one-minute period.

DFS functionality allows a MAP that detects a radar signal to transmit that up to the RAP, which then acts as if it has experienced radar and moves the sector. This process is called the coordinated channel change. This functionally can be turned on or off on the controller. The coordinated channel change is enabled by default.

To enable DFS, enter the following command:

```
(Cisco Controller) > config mesh full-sector-dfs enable
```

To verify that DFS is enabled on the network, enter the following command:

```
(Cisco Controller) > show network summary
```



Note A MAP that detects radar should send a message to the RAP, unless the parent has a different BGN, in which case it does not send messages for a coordinated sector change. Instead, the MAP reenters the SCAN state and searches on nonradar seen channels for a new parent.



Note Ensure that none of your mesh access points are using a default BGN.

Note A repeated radar event on the MAP (radar triggers once, and then almost immediately again), causes the MAP to disconnect.

Preparation in a DFS Environment

This section describes how to prepare in a DFS environment:

- To verify that your controller is set to the correct country domain, enter the following command:

```
(Cisco Controller) > show country
```

- To check the mesh access point country and the channel setting on the controller, enter the following command:

```
(Cisco Controller)> show ap config 802.11a ap-name
```

- To identify channels available for mesh, enter the following command:

```
(Cisco Controller)> show ap config 802.11a ap-name
```

  Look for the allowed channel list.

```
Allowed Channel List..................... 100,104,108,112,116,120,124,
..................................... 128,132,136,140
```

- To identify channels available for mesh on the AP console (or use remote debug from the controller, enter the following command:

```
ap1520-rap # show mesh channels

HW: Dot11Radio1, Channels:
100, 104, 108, 112, 116, 120, 124, 128, 132, 136, 140
```

  An asterisk next to a channel indicates that radar has been seen on the channel.

- To invoke remote debug, enter the following commands:

```
(Cisco Controller) > debug ap enable ap-name
(Cisco Controller) > debug ap command command ap-name
```

- Debug commands to see radar detection and past radar detections on the DFS channel are as follows:

```
show mesh dfs channel channel-number
show mesh dfs history
```

  Information similar to the following appears.

ap1520-rap # **show mesh dfs channel** 132

```
Channel 132 is available
Time elapsed since radar last detected: 0 day(s), 7 hour(s), 6 minute(s), 51 second(s).
```

The RAP should be run through the channels to determine whether there is active radar on each of the channels.

```
ap1520-rap # show mesh dfs channel 132

Radar detected on channel 132, channel becomes unusable (Time Elapsed: 0 day(s), 7
hour(s), 7 minute(s), 11 second(s)).
Channel is set to 100 (Time Elapsed: 0 day(s), 7 hour(s), 7 minute(s), 11 second(s)).
Radar detected on channel 116, channel becomes unusable (Time Elapsed: 0 day(s), 7
hour(s), 6 minute(s), 42 second(s)).
Channel is set to 64 (Time Elapsed: 0 day(s), 7 hour(s), 6 minute(s), 42 second(s)).
Channel 132 becomes usable (Time Elapsed: 0 day(s), 6 hour(s), 37 minute(s), 10
second(s)).
Channel 116 becomes usable (Time Elapsed: 0 day(s), 6 hour(s), 36 minute(s), 42
second(s)).
```

Monitoring DFS

The DFS history should be run every morning or more frequently to detect the radar. This information does not get erased and is stored on the mesh access point flash. Therefore, you only need to match the times.

```
ap1520-rap # show controller dot11Radio 1
```

Information similar to the following appears:

```
interface Dot11Radio1
Radio Hammer 5, Base Address 001c.0e6c.9c00, BBlock version 0.00, Software version 0.05.30
Serial number: FOC11174XCW
Number of supported simultaneous BSSID on Dot11Radio1: 16
Carrier Set: ETSI (OFDM) (EU) (-E)
Uniform Spreading Required: Yes
Current Frequency: 5540 MHz Channel 108 (DFS enabled)
Allowed Frequencies: *5500(100) *5520(104) *5540(108) *5560(112) *5580(116) *560
0(120) *5620(124) *5640(128) *5660(132) *5680(136) *5700(140)
* = May only be selected by Dynamic Frequency Selection (DFS)
Listen Frequencies: 5180(36) 5200(40) 5220(44) 5240(48) 5260(52) 5280(56) 5300(6
0) 5320(64) 5500(100) 5520(104) 5540(108) 5560(112) 5580(116) 5660(132) 5680(136
) 5700(140) 5745(149) 5765(153) 5785(157) 5805(161) 5825(165) 4950(20) 4955(21)
4960(22) 4965(23) 4970(24) 4975(25) 4980(26)
```

Note An asterisk indicates that this channel has DFS enabled.

Frequency Planning

Use alternate adjacent channels in adjacent sectors. If you have two RAPs deployed at the same location, you must leave one channel in between.

Weather radars operate within the 5600- to 5650-MHz band, which means that channels 124 and 128 might be affected, but also channels 120 and 132 might suffer from weather radar activity.

If the mesh access point does detect radar, the controller and the mesh access point both will retain the channel as the configured channel. The controller retains it in volatile memory associated with the mesh access point, and the mesh access point has it stored in its flash as configuration. After the 30 minute quiet period, the controller returns the mesh access point to the static value, regardless of whether the mesh access point has been configured with a new channel or not. In order to overcome this, configure the mesh access point with a new channel, and reboot the mesh access point.

Once radar is reliably detected on a channel, that channel, and the two surrounding channels, should be added to the RRM exclusion list, as follows:

```
(Cisco Controller) > config advanced 802.11a channel delete channel
```

A mesh access point goes to a new channel that is picked by RRM, and it does not consider excluded channels.

If a radar is detected on channel 124, for instance, channels 120, 124, and 128 should be added to the exclusion list. In addition, do not configure RAP to operate on those channels.

Good Signal-to-Noise Ratios

For European installations, the minimum recommendation is increased to 20 dB of signal-to-noise ratio (SNR). The extra dBs are used to mitigate the effects of radar interference with packet reception, which is not observed in non-DFS environments.

Access Point Placement

Collocated mesh access points should have a minimum of 10 feet (3.048 meters) of vertical separation or 100 (30.48 meters) feet of horizontal separation.

Check Packet Error Rate

Mesh access points that have an high error rate, greater than 1 percent, should have mitigation applied to them, by changing the channels for noise and interference, adding additional mesh access points in the transmission path, moving the mesh access points to different sectors, or adding additional mesh access points.

Bridge Group Name Misconfiguration

A mesh access point can be wrongly provisioned with a *bridgegroupname* and placed in a group other than it was intended. Depending on the network design, this mesh access point might or might not be able to reach out and find its correct sector or tree. If it cannot reach a compatible sector, the mesh access point can become stranded.

To recover a stranded mesh access point, the concept of default bridgegroupname has been introduced in the software. When a mesh access point is unable to connect to any other mesh access point with its configured bridgegroupname, it attempts to connect with the bridgegroupname of *default*.

The algorithm of detecting this strand condition and recovery is as follows:

1. Passively scans and finds all neighbor nodes regardless of their bridgegroupname.
2. The mesh access point attempts to connect to the neighbors heard with *my own bridgegroupname* using AWPP.

3. If Step 2 fails, attempts to connect with default bridgegroupname using AWPP.
4. For each failed attempt in Step 3, it adds the neighbor to an exclusion list and attempts to connect the next best neighbor.
5. If the AP fails to connect with all neighbors in Step 4, it reboots the mesh access point.
6. If connected with a *default* bridgegroupname for 15 minutes, the mesh access point goes into a scan state.

When an mesh access point is able to connect with the default bridgegroupname, the parent node reports the mesh access point as a default child/node/neighbor entry on the controller, so that a network administrator is Cisco Prime Infrastructure. Such a mesh access point behaves as a normal (nonmesh) access point and accepts any client, other mesh nodes as its children, and it passes any data traffic through.

Note Do not confuse an unassigned BGN (null value) with DEFAULT, which is a mode that the access point uses to connect when it cannot find its own BGN.

To check the current state of a mesh access point's BGN, enter the following command:

```
(Cisco Controller)> show mesh path Map3:5f:ff:60
00:0B:85:5F:FA:60 state UPDATED NEIGH PARENT DEFAULT (106B), snrUp 48, snrDown 48, linkSnr
 49
00:0B:85:5F:FB:10 state UPDATED NEIGH PARENT BEACON (86B) snrUp 72, snrDown 63, linkSrn 57
00:0B:85:5F:FA:60 is RAP
```

To check the current state of a mesh access point's BGN, check the neighbor information for the mesh access point (GUI) as follows:

Choose **Wireless > All APs** > *AP Name* > *Neighbor info* .

Figure 70: Neighbor Information for a Child

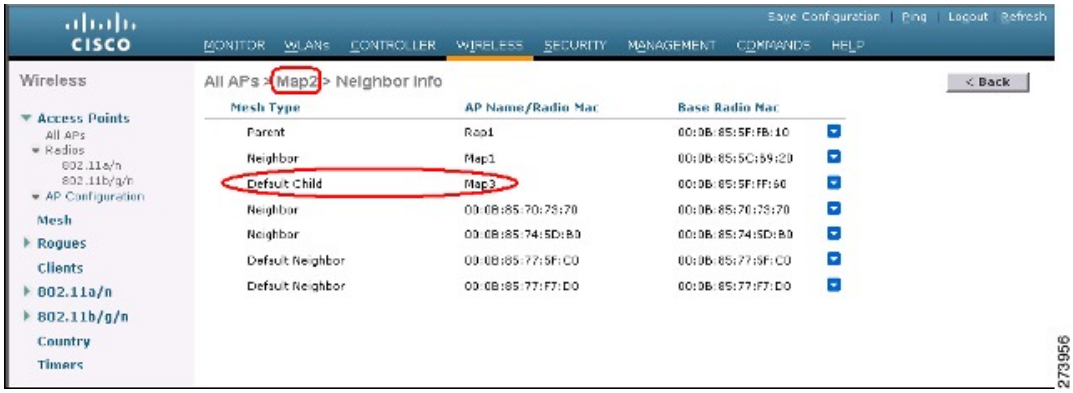
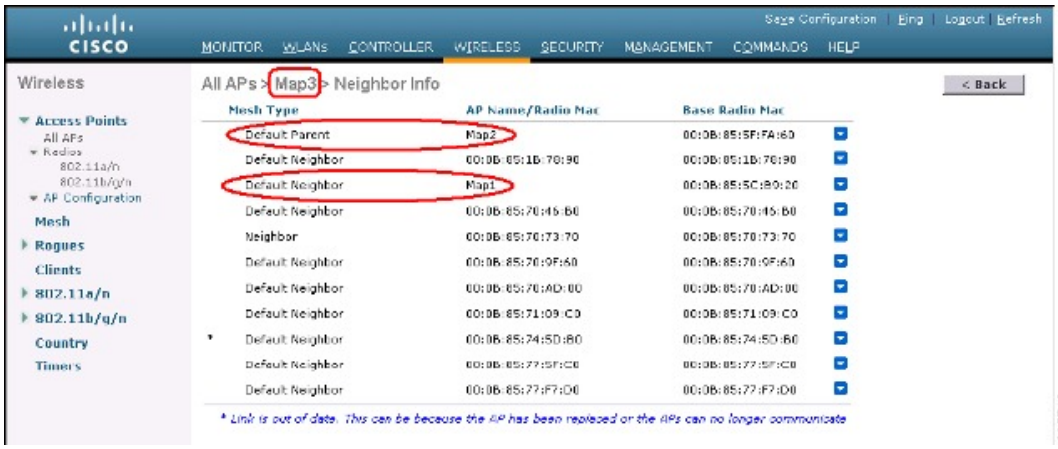


Figure 71: Neighbor Information for a Parent



Misconfiguration of the Mesh Access Point IP Address

Although most Layer 3 networks are deployed using DHCP IP address management, some network administrators might prefer the manual IP address management and allocating IP addresses statically to each mesh node. Manual mesh access point IP address management can be a nightmare for large networks, but it might make sense in small to medium size networks (such as 10 to 100 mesh nodes) because the number of mesh nodes are relatively small compared to client hosts.

Statically configuring the IP address on a mesh node has the possibility of putting a MAP on a wrong network, such as a subnet or VLAN. This mistake could prevent a mesh access point from successfully resolving the IP gateway and failing to discover a WLAN controller. In such a scenario, the mesh access point falls back to its DHCP mechanism and automatically attempts to find a DHCP server and obtains an IP address from it. This fallback mechanism prevents a mesh node from being potentially stranded from a wrongly configured static IP address and allows it to obtain a correct address from a DHCP server on the network.

When you are manually allocating IP addresses, we recommend that you make IP addressing changes from the furthest mesh access point child first and then work your way back to the RAP. This recommendation also applies if you relocate equipment. For example, if you uninstall a mesh access point and redeploy it in another physical location of the mesh network that has a different addressed subnet.

Another option is to take a controller in Layer 2 mode with a RAP to the location with the misconfigured MAP. Set the bridge group name on the RAP to match the MAP that needs the configuration change. Add the MAP's MAC address to the controller. When the misconfigured MAP comes up in the mesh access point summary detail, configure it with an IP address.

Misconfiguration of DHCP

Despite the DHCP fallback mechanism, there is still a possibility that a mesh access point can become stranded, if any of the following conditions exist:

- There is no DHCP server on the network.
- There is a DHCP server on the network, but it does not offer an IP address to the AP, or if it gives a wrong IP address to the AP (for example, on a wrong VLAN or subnet).

These conditions can strand a mesh access point that is configured with or without a wrong static IP address or with DHCP. Therefore, you must ensure that when a mesh access point is unable to connect after exhausting all DHCP discovery attempts or DHCP retry counts or IP gateway resolution retry counts, it attempts to find a controller in Layer 2 mode. In other words, a mesh access point attempts to discover a controller in Layer 3 mode first and in this mode, attempts with both static IP (if configured) or DHCP (if possible). The AP then attempts to discover a controller in Layer 2 mode. After finishing a number of Layer 3 and Layer 2 mode attempts, the mesh access point changes its parent node and re-attempts DHCP discovery. Additionally, the software exclusion-lists notes the parent node through which it was unable to obtain the correct IP address.

Identifying the Node Exclusion Algorithm

Depending on the mesh network design, a node might find another node "best" according to its routing metric (even recursively true), yet it is unable to provide the node with a connection to the correct controller or correct network. It is the typical honeypot access point scenario caused by either misplacement, provisioning, design of the network, or by the dynamic nature of an RF environment exhibiting conditions that optimize the AWPP routing metric for a particular link in a persistent or transient manner. Such conditions are generally difficult to recover from in most networks and could blackhole or sinkhole a node completely, taking it out from the network. Possible symptoms include, but are not limited to the following:

- A node connects to the honeypot but cannot resolve the IP gateway when configured with the static IP address, or cannot obtain the correct IP address from the DHCP server, or cannot connect to a WLAN controller.
- A node ping-pongs between a few honeypots or circles between many honeypots (in worst-case scenarios).

Cisco mesh software resolves this difficult scenario by using a sophisticated node exclusion-listing algorithm. This node exclusion-listing algorithm uses an exponential backoff and advance technique much like the TCP sliding window or 802.11 MAC.

The basic idea relies on the following five steps:

1. Honeypot detection—The honeypots are first detected via the following steps:

   A parent node is set by the AWPP module by:

   - A static IP attempt in CAPWAP module.
   - A DHCP attempt in the DHCP module.
   - A CAPWAP attempt to find and connect to a controller fails.

2. Honeypot conviction—When a honeypot is detected, it is placed in a exclusion-list database with its conviction period to remain on the list. The default is 32 minutes. Other nodes are then attempted as parents in the following order, falling back to the next, upon failing the current mechanism:

   - On the same channel.
   - Across different channels (first with its own bridgegroupname and then with default).
   - Another cycle, by clearing conviction of all current exclusion-list entries.
   - Rebooting the AP.

3. Nonhoneypot credit—It is often possible that a node is not a really a honeypot, but appears to be due to some transient back-end condition, such as the following:

- The DHCP server is either not up-and-running yet, has failed temporarily, or requires a reboot.
- The WLAN controller is either not up-and-running yet, has failed temporarily, or requires a reboot.
- The Ethernet cable on the RAP was accidentally disconnected.

  Such nonhoneypots must be credited properly from their serving times so that a node can come back to them as soon as possible.

4. Honeypot expiration—Upon expiration, an exclusion-list node must be removed from the exclusion-list database and return to a normal state for future consideration by AWPP.
5. Honeypot reporting—Honeypots are reported to the controller via an LWAPP mesh neighbor message to the controller, which shows these on the Bridging Information page. A message is also displayed the first-time an exclusion-listed neighbor is seen. In a subsequent software release, an SNMP trap is generated on the controller for this condition so that Cisco Prime Infrastructure can record the occurrence.

Figure 72: Excluded Neighbor



Because many nodes might be attempting to join or rejoin the network after an expected or unexpected event, a hold-off time of 16 minutes is implemented, which means that no nodes are exclusion-listed during this period of time after system initialization.

This exponential backoff and advance algorithm is unique and has the following properties:

- It allows a node to correctly identify the parent nodes whether it is a true honeypot or is just experiencing temporary outage conditions.
- It credits the good parent nodes according to the time it has enabled a node to stay connected with the network. The crediting requires less and less time to bring the exclusion-list conviction period to be very low for real transient conditions and not so low for transient to moderate outages.
- It has a built-in hysteresis for encountering the initial condition issue where many nodes try to discover each other only to find that those nodes are not really meant to be in the same network.
- It has a built-in memory for nodes that can appear as neighbors sporadically so they are not accidentally considered as parents if they were, or are supposed to be, on the exclusion-list database.

The node exclusion-listing algorithm guards the mesh network against serious stranding. It integrates into AWPP in such a way that a node can quickly reconverge and find the correct network.

Throughput Analysis

Throughput depends on packet error rate and hop count.

Capacity and throughput are orthogonal concepts. Throughput is one user's experience at node N and the total area capacity is calculated over the entire sector of N-nodes and is based on the number of ingress and egress RAP, assuming separate noninterfering channels.

For example, 4 RAPs at 10 Mbps each deliver 40 Mbps total capacity. So, one user at 2 hops out, logically under each RAP, could get 5 Mbps each of TPUT, but consume 40 Mbps of the backhaul capacity.

With the Cisco Mesh solution, the per-hop latency is less than 10 msecs, and the typical latency numbers per hop range from 1 to 3 msecs. Overall jitter is also less than 3 msecs.

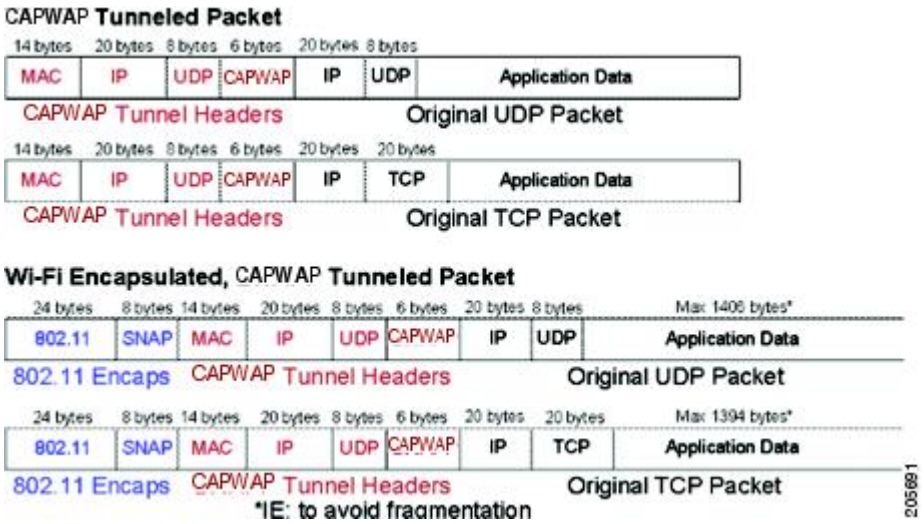
Throughput depends on the type of traffic being passed through the network: User Datagram Protocol (UDP) or Transmission Control Protocol (TCP). UDP sends a packet over Ethernet with a source and destination address and a UDP protocol header. It does not expect an acknowledgement (ACK). There is no assurance that the packet is delivered at the application layer.

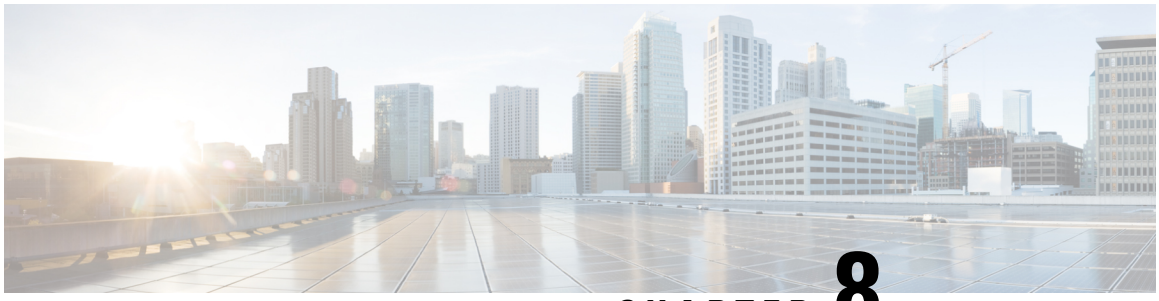
TCP is similar to UDP but it is a reliable packet delivery mechanism. There are packet acknowledgments and a sliding window technique is used to allow the sender to transmit multiple packets before waiting for an ACK. There is a maximum amount of data the client transmits (called a TCP socket buffer window) before it stops sending data. Sequence numbers track packets sent and ensure that they arrive in the correct order. TCP uses cumulative ACKs and the receiver reports how much of the current stream has been received. An ACK might cover any number of packets, up to the TCP window size.

TCP uses slow start and multiplicative decrease to respond to network congestion or packet loss. When a packet is lost, the TCP window is cut in half and the back-off retransmission timer is increased exponentially. Wireless is subject to packet loss due to interference issues and TCP reacts to this packet loss. A slow start recovery algorithm is also used to avoid swamping a connection when recovering from packet loss. The effect of these algorithms in a lossy network environment is to lessen the overall throughput of a traffic stream.

By default, the maximum segment size (MSS) of TCP is 1460 bytes, which results in a 1500-byte IP datagram. TCP fragments any data packet that is larger than 1460 bytes, which can cause at least a 30-percent throughput drop. In addition, the controller encapsulates IP datagrams in the 48-byte CAPWAP tunnel header as shown in Figure 73: CAPWAP Tunneled Packets, on page 204. Any data packet that is longer than 1394 bytes is also fragmented by the controller, which results in up to a 15-percent throughput decrease.

Figure 73: CAPWAP Tunneled Packets





CHAPTER 8

Managing Mesh Access Points with Cisco Prime Infrastructure

Cisco Prime Infrastructure is a complete platform for enterprise-wide WLAN systems management. It provides a wide range of tools for visualizing and controlling the mesh, including histograms of signal-to-noise ratio, mesh detail information, mesh access point neighbor and link information, seven-day temporal link information, and tools to identify and avoid RF interference.

This section addresses the following Prime Infrastructure monitoring capabilities:

- Monitoring Mesh Networks Using Maps
- Monitoring Mesh Health
- Viewing Mesh Statistics for a Mesh Access Point
- Viewing the Mesh Network Hierarchy
- Using Mesh Filters to Modify Map Display of Maps and Mesh Links

- Adding Campus Maps, Outdoor Areas, and Buildings with Cisco Prime Infrastructure, on page 205
- Adding Mesh Access Points to Maps with Cisco Prime Infrastructure, on page 208
- Monitoring Mesh Access Points Using Google Earth, on page 209
- Adding Indoor Mesh Access Points to Cisco Prime Infrastructure, on page 212
- Managing Mesh Access Points with Cisco Prime Infrastructure, on page 213
- Monitoring Workgroup Bridges, on page 225
- Viewing AP Last Reboot Reason, on page 232

Adding Campus Maps, Outdoor Areas, and Buildings with Cisco Prime Infrastructure

For mesh networks, maps and items on those maps (buildings and mesh access points) are added to Cisco Prime Infrastructure in the following order:

Step 1 Add a campus map.

Step 2 Add an outdoor area map.

Step 3 Add buildings.

Step 4 Add mesh access points.

Detailed steps for adding these maps and components are noted below.

Adding Campus Maps

To add a single campus map to the Cisco Prime Infrastructure database, follow these steps:

Step 1 Save the map in .PNG, .JPG, .JPEG, or .GIF format.

Note The map can be any size because the Prime Infrastructure automatically resizes the map to fit its working areas.

Step 2 Browse to and import the map from anywhere in your file system.

Step 3 Choose **Monitor > Maps** to display the Maps page.

Step 4 From the Select a command drop-down list, choose **New Campus** and click **GO**.

Step 5 On the Maps > New Campus page, enter the campus name and campus contact name.

Step 6 Browse to and choose the image filename containing the map of the campus and click **Open**.

Step 7 Select the **Maintain Aspect Ratio** check box to prevent length and width distortion when the Prime Infrastructure resizes the map.

Step 8 Enter the horizontal and vertical span of the map in feet.

Note The horizontal and vertical span should be larger than any building or floor plan to be added to the campus.

Step 9 Click **OK** to add this campus map to the Prime Infrastructure database. The Prime Infrastructure displays the Maps page, which lists maps in the database, map types, and campus status.

Adding Outdoor Areas

To add an outdoor area to a campus map, follow these steps:



Note You can add outdoor areas to a campus map in the Cisco Prime Infrastructure database regardless of whether you outdoor area maps are in the database.

Step 1 If you want to add a map of the outdoor area to the database, save the map in .PNG, .JPG, .JPEG, or .GIF format. Then browse to and import the map from anywhere in your file system.

Note You do not need a map to add an outdoor area. You can simply define the dimensions of the area to add it to the database. The map can be any size because Cisco Prime Infrastructure automatically resizes the map to fit the workspace.

Step 2 Choose **Monitor** > **Maps** to display the Maps page.

Step 3 Click the desired campus. Cisco Prime Infrastructure displays the Maps > Campus Name page.

Step 4 From the Select a command drop-down list, choose **New Outdoor Area** and click **GO**.

Step 5 On the Campus Name > New Outdoor Area page, follow these steps to create a manageable outdoor area:

a) Enter the outdoor area name.
b) Enter the outdoor area contact name.
c) If desired, enter or browse to the filename of the outdoor area map.
d) Enter an approximate outdoor horizontal span and vertical span (width and depth on the map) in feet.

Tip Tip You can also use **Ctrl-click** to resize the bounding area in the upper left corner of the campus map. As you change the size of the bounding area, the Horizontal Span and Vertical Span parameters of the outdoor area change to match your actions.

e) Click **Place** to put the outdoor area on the campus map. Cisco Prime Infrastructure creates an outdoor area rectangle scaled to the size of the campus map.
f) Click on the outdoor area rectangle and drag it to the desired position on the campus map.
g) Click **Save** to save this outdoor area and its campus location to the database. Cisco Prime Infrastructure saves the outdoor area name in the outdoor area rectangle on the campus map.

Note A hyperlink associated with the outdoor area takes you to the corresponding Map page

Step 6 Click **Save**.

Adding a Building to a Campus Map

You can add buildings to the Cisco Prime Infrastructure database regardless of whether you have added campus maps to the database. This section explains how to add a building to a campus map or a standalone building (one that is not part of a campus) to the Prime Infrastructure database.

To add a building to a campus map in the Prime Infrastructure database, follow these steps:

Step 1 Choose **Monitor > Maps** to display the Maps page.

Step 2 Click the desired campus. Cisco Prime Infrastructure displays the Maps > Campus Name page.

Step 3 From the Select a command drop-down list, choose **New Building** and click **Go**.

Step 4 On the Campus Name > New Building page, follow these steps to create a virtual building in which to organize related floor plan maps:

a) Enter the building name.
b) Enter the building contact name.
c) Enter the number of floors and basements.
d) Enter an approximate building horizontal span and vertical span (width and depth on the map) in feet.

Tip The horizontal and vertical span should be larger than or the same size as any floors that you might add later. You can also use **`Ctrl-click`** to resize the bounding area in the upper left corner of the campus map. As you change the size of the bounding area, the Horizontal Span and Vertical Span parameters of the building change to match your actions.

e) Click **Place** to put the building on the campus map. Cisco Prime Infrastructure creates a building rectangle scaled to the size of the campus map.

f) Click on the building rectangle and drag it to the desired position on the campus map.

Note After adding a new building, you can move it from one campus to another without having to recreate it.

g) Click **Save** to save this building and its campus location to the database. Cisco Prime Infrastructure saves the building name in the building rectangle on the campus map.

Note A hyperlink associated with the building takes you to the corresponding Map page.

Step 5 Click **Save**.

Adding Mesh Access Points to Maps with Cisco Prime Infrastructure

After you add the .PNG, .JPG, .JPEG, or .GIF format floor plan and outdoor area maps to the Cisco Prime Infrastructure database, you can position mesh access point icons on the maps to show where they are installed in the buildings.

To add mesh access points to floor plan and outdoor area maps, follow these steps:

Step 1 Click the desired floor plan or outdoor area map in the Coverage Areas component of the **General** tab. Cisco Prime Infrastructure displays the associated coverage area map.

Step 2 From the Select a command drop-down list, choose **Add Access Points** and click **GO**.

Step 3 On the Add Access Points page, choose the mesh access points to add to the map.

Step 4 Click **OK** to add the mesh access points to the map and display the Position Access Points map.

Note The mesh access point icons appear in the upper left area of the map.

Step 5 Click and drag the icons to indicate their physical locations.

Step 6 Click each icon and choose the antenna orientation in the sidebar.

Figure 74: Antenna Sidebar



The antenna angle is relative to the map's X axis. Because the origin of the X (horizontal) and Y (vertical) axes is in the upper left corner of the map, 0 degrees points side A of the mesh access point to the right, 90 degrees points side A down, 180 degrees points side A to the left, and so on. The antenna elevation is used to move the antenna vertically, up or down, to a maximum of 90 degrees.

Make sure each mesh access point is in the correct location on the map and has the correct antenna orientation. Accurate mesh access point positioning is critical when you use the maps to find coverage holes and rogue access points.

See this location for further information about the antenna elevation and azimuth patterns:

http://www.cisco.com/en/US/products/hw/wireless/ps469/tsd_products_support_series_home.html

Step 7 Click **Save** to store the mesh access point locations and orientations. Cisco Prime Infrastructure computes the RF prediction for the coverage area. These RF predictions are popularly known as heat maps because they show the relative intensity of the RF signals on the coverage area map.

Note This display is only an approximation of the actual RF signal intensity because it does not take into account the attenuation of various building materials, such as drywall or metal objects. It also does not display the effects of RF signals bouncing off obstructions.

Monitoring Mesh Access Points Using Google Earth

Cisco Prime Infrastructure supports both Google Earth Map Plus or Pro and displays, when present, mesh access points and their links.

Launching Google Earth in Cisco Prime Infrastructure

Cisco Prime Infrastructure supports both Google Earth Map Plus or Pro and displays, when present, mesh access points and their links.

To launch Google Earth maps, follow these steps:

Step 1 Launch Google Earth plus or pro and add a new folder.

Step 2 Create a mesh access points placemark on Google Earth plus or pro.

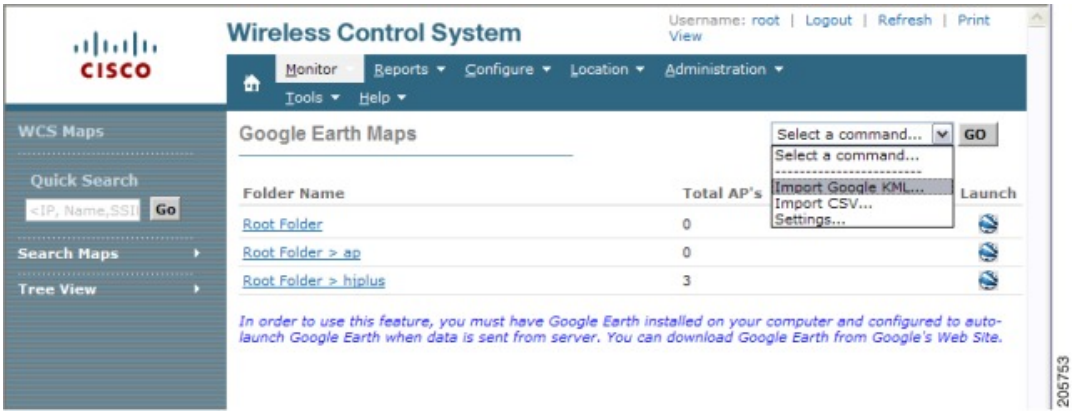
Note You must use the exact name of the mesh access point when creating the placement mark to ensure Prime Infrastructure can recognize these mesh access points.

Step 3 Place the mesh access point placemarks in the new folder. Save the folder as a .KML file.

Step 4 In the Prime Infrastructure, choose **Monitor > Google Earth Maps**. Select Import Google KML from the Select a command drop-down list.

Step 5 Import the new Google KML folder. It displays in the folder name summary.

Figure 75: Importing New Folder into Google Earth



Step 6 Click the launch icon next to the new folder to launch the Google Earth map from the Prime Infrastructure.

Viewing Google Earth Maps

You can view campus maps, mesh access point and link information using Google maps.

To view Google Earth maps, follow these steps:

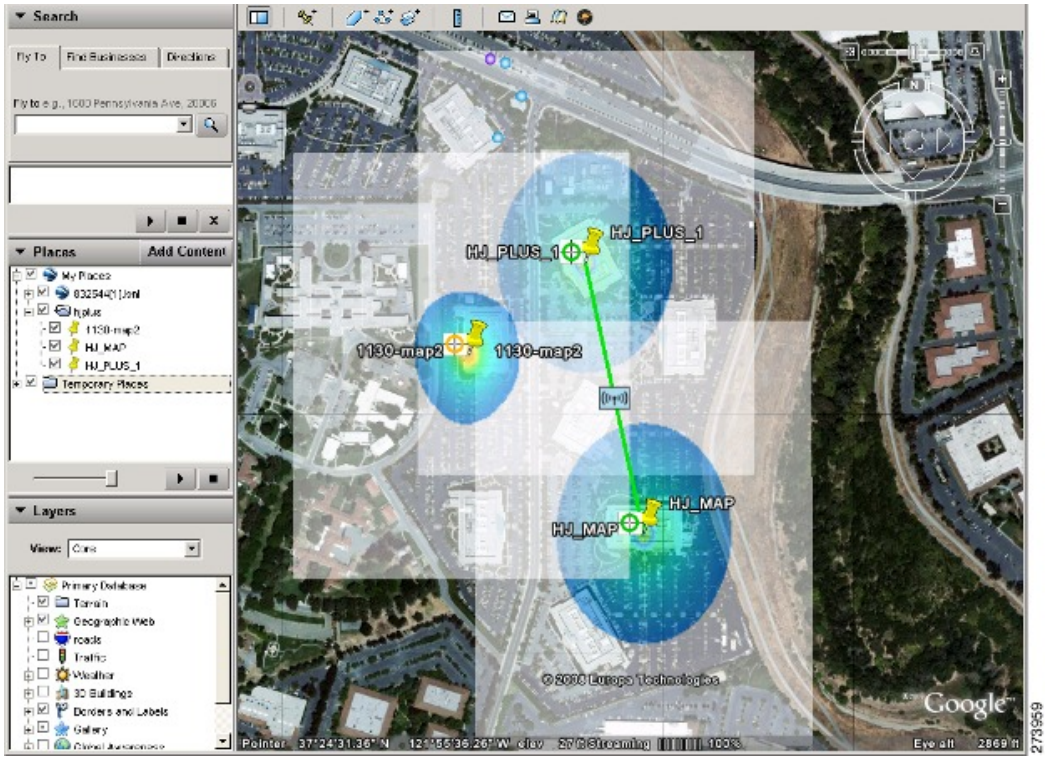
Step 1 Log on to Cisco Prime Infrastructure.

Step 2 Choose **Monitor > Google Earth Maps**. The Google Earth Maps page displays all folders and the number of mesh access points included within each folder.

Step 3 Click **Launch** for the map you want to view. Google Earth opens in a separate window and displays the location and its mesh access points.

Note To use this feature, you must have Google Earth installed on your computer and configured to auto-launch when data is sent from the server. You can download Google Earth from Google's website.

Figure 76: Google Earth Map Page



Step 4 Click **Launch** for the map you want to view. Google Earth opens in a separate window and displays the location and its mesh access points.

Note To use this feature, you must have Google Earth installed on your computer and configured to auto-launch when data is sent from the server. You can download Google Earth from Google's website.

Figure 77: Google Earth Map With Mesh Access Point Details

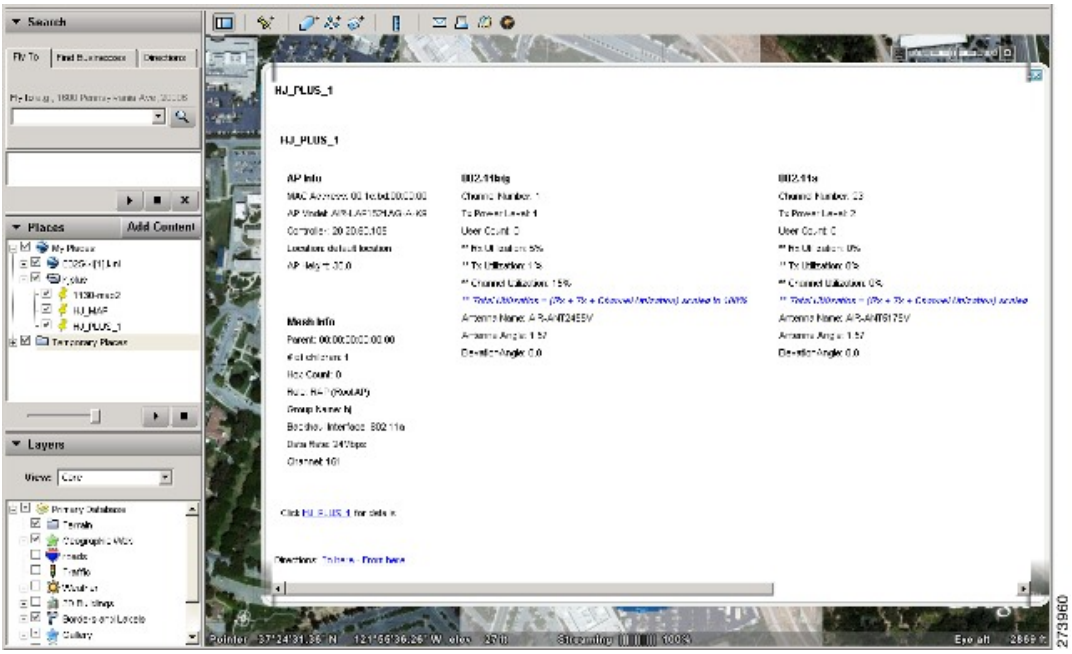


Figure 78: Google Earth Map With Mesh Link Details



To view details for a Google Earth Map folder, follow these steps:

Step 5 From the Google Earth Map page, click the folder name to open the details page for this folder. The Google Earth Details page provides the mesh access point names and MAC or IP addresses.

Note To delete a mesh access point, select the applicable check box and click **Delete**.?To delete the entire folder, select the check box next to Folder Name and click **Delete**. Deleting a folder also deletes all subfolders and mesh access points inside the folder.

Step 6 Click **Cancel** to close the details page.

Adding Indoor Mesh Access Points to Cisco Prime Infrastructure

You have a choice of ordering indoor access points directly into the bridge mode, so that these access points can be used directly as mesh access points. If you have these access points in a local mode (nonmesh), then you have to connect these access points to the controller and change the radio role to the bridge mode (mesh). This task can become cumbersome particularly if the volume of the access points being deployed is large and if the access points are already deployed in the local mode for a traditional nonmesh wireless coverage.

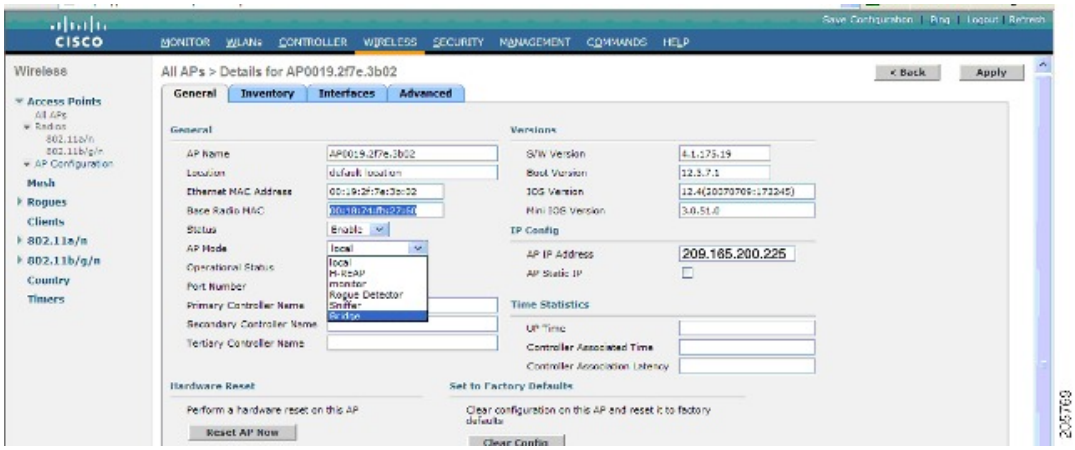
For local mode indoor access points prior to a mesh installation, you must first connect all indoor mesh access points to the controller and change the mode to *bridge* mode.

To do so, connect all the indoor access points to the Layer 3 network on the same subnet as the Management IP address.

Add the MAC address of the indoor mesh access points into the MAC filter list on the controller. All indoor access points will then join the controller in local mode.

You can then change local mode to bridge mode in the controller for every indoor access point.

Figure 79: All APs > AP Details Controller Page



After changing the indoor access points to bridge mode on the controller, add these indoor mesh access points into the Prime Infrastructure.

You cannot initially configure indoor mesh access points into bridge mode from the Prime Infrastructure.

Managing Mesh Access Points with Cisco Prime Infrastructure

Cisco Prime Infrastructure is a complete platform for enterprise-wide WLAN systems management. It provides a wide range of tools for visualizing and controlling the mesh, including histograms of signal-to-noise ratio, mesh detail information, mesh access point neighbor and link information, seven-day temporal link information, and tools to identify and avoid RF interference.

This section addresses the following Prime Infrastructure monitoring capabilities:

- Monitoring Mesh Networks Using Maps
- Monitoring Mesh Health
- Viewing Mesh Statistics for a Mesh Access Point
- Viewing the Mesh Network Hierarchy
- Using Mesh Filters to Modify Map Display of Maps and Mesh Links

Monitoring Mesh Networks Using Maps

You can access and view details for the following elements from a mesh network map in the Cisco Prime Infrastructure.:

- Mesh Link Statistics
- Mesh Access Points
- Mesh Access Point Neighbors

Details on how this information is accessed and the information displayed for each of these items is detailed in the following sections.

Monitoring Mesh Link Statistics Using Maps

You can view the SNR for a specific mesh network link, view the number of packets transmitted and received on that link, and initiate a link test from the Monitor > Maps display.

To view details on a specific mesh link between two mesh access points or a mesh access point and a root access point, follow these steps:

Step 1 In Cisco Prime Infrastructure, choose **Monitor > Maps**.

Step 2 Click the **Map Name** that corresponds to the outdoor area, campus, building, or floor you want to monitor.

Step 3 Move the cursor over the link arrow for the target link. A Mesh Link page appears.

Note The AP Mesh Info check box under the Layers drop-down list must be selected for links to appear on the map.

Step 4 Click either **Link Test, Child to Parent** or **Link Test, Parent to Child**. After the link test is complete, a results page appears.

Note A link test runs for 30 seconds.

Note You cannot run link tests for both links (child-to-parent and parent-to-child) at the same time.

Step 5 To view a graphical representation of SNR statistics over a period of time, click the arrow on the link. A page with multiple SNR graphs appears.

The following graphs are displayed for the link:

- SNR Up—Plots the RSSI values of the neighbor from the perspective of the mesh access point.
- SNR Down—Plots the RSSI values that the neighbor reports to the mesh access point.
- Link SNR—Plots a weighed and filtered measurement based on the SNR Up value.
- The Adjusted Link Metric —Plots the value used to determine the least cost path to the root mesh access point. This value is the ease to get to the rooftop access point and accounts for the number of hops. The lower the ease value, the less likely the path is used.
- The Unadjusted Link Metric —Plots the least cost path to get to the root access point unadjusted by the number of hops. The higher the value for the unadjusted link indicates the better the path.

Monitoring Mesh Access Points Using Maps

You can view the following summary information for a mesh access point from a mesh network map:

- Parent
- Number of children
- Hop count
- Role
- Group name
- Backhaul interface
- Data Rate
- Channel



Note This information is in addition to the information shown for all mesh access points (MAC address, mesh access point model, controller IP address, location, height of mesh access point, mesh access point up time, and CAPWAP up time).

To view summary and detailed configuration information for a mesh access point from a mesh network map, follow these steps:

Step 1 On the GUI of Cisco Prime Infrastructure, choose **Monitor > Maps**.

Step 2 Click the **Map Name** that corresponds to the outdoor area, campus, building, or floor location of the mesh access point you want to monitor.

Step 3 To view summary configuration information for a mesh access point, move the cursor over the mesh access point that you want to monitor. A page with configuration information for the selected mesh access point appears.

Step 4 To view detailed configuration information for a mesh access point, click the arrow portion of the mesh access point label. The configuration details for the mesh access point appears.

Note If the mesh access point has an IP address, a Run Ping Test link is also visible at the bottom of the mesh access point panel.

Step 5 On the Access Point configuration page, follow these steps to view configuration details for the mesh access point:

a) Choose the **General** tab to view the overall configuration of the mesh access point such as AP name, MAC address, AP Up time, associated controllers (registered and primary) operational status, and software version.

Note The software version for mesh access points is appended the letter *m* and the word *mesh* in parentheses.

b) Choose the **Interface** tab to view configuration details for the interfaces supported on the mesh access point. Interface options are radio and Ethernet.

c) Choose the **Mesh Links** tab to view parent and neighbors' details (name, MAC address, packet error rate, and link details) for the mesh access point. You can also initiate link tests from this panel.

d) Choose the **Mesh Statistics** tab to view details on the bridging, queue, and security statistics for the mesh access point. For more details on mesh statistics, see the Viewing Mesh Statistics for a Mesh Access Point section.

Monitoring Mesh Access Point Neighbors Using Maps

To view details on neighbors of a mesh access point from a mesh network map, follow these steps:

Step 1 Choose **Monitor > Maps**.

Step 2 Click the **Map Name** that corresponds to the outdoor area, campus, building, or floor you want to monitor.

Step 3 To view detailed information on mesh links for a mesh access point, click the arrow portion of the access point label. The Access Points screen appears.

Step 4 Click the **Mesh Links** tab.

Note You can also mesh link details for neighbors of a selected mesh access point by clicking on the View Mesh Neighbors link on the mesh access point configuration summary panel that displays when you mouse over a mesh access point on a map.

Note Signal-to-noise ratio (SNR) only appears on the View Mesh Neighbors panel.

Note In addition to listing the current and past neighbors in the panel that displays, labels are added to the mesh access points map icons to identify the selected mesh access point, the neighbor mesh access point, and the child mesh access point. Select the clear link of the selected mesh access point to remove the relationship labels from the map.

Note The drop-down lists at the top of the mesh neighbors page indicate the resolution of the map (100%) displayed and how often the information displayed is updated (5 minutes). You can modify these default values.

Monitoring Mesh Health

Mesh Health monitors the overall health of outdoor and indoor mesh access points, except as noted. Tracking this environmental information is particularly critical for mesh access points that are deployed outdoors. The following factors are monitored:

- Temperature—Displays the internal temperature of the mesh access point in Fahrenheit and Celsius (AP1500s only).
- Heater status—Displays the heater as on or off (AP1500s only).
- AP Up time—Displays how long the mesh access point has been active to receive and transmit.
- CAPWAP Join Taken Time—Displays how long it took to establish the CAPWAP connection.
- CAPWAP Up Time—Displays how long the CAPWAP connection has been active.

Mesh Health information is displayed in the General Properties panel for mesh access points.

To view the mesh health details for a specific mesh access point, follow these steps:

Step 1 Choose **Monitor > Access Points**. A listing of access points appears.

Note You can also use the New Search button to display the mesh access point summary shown below. With the New Search option, you can further define the criteria of the access points that display. Search criteria include AP Type, AP Mode, Radio Type, and 802.11n Support.

Step 2 Click the **AP Name** link to display details for that mesh access point. The General Properties panel for that mesh access point appears.



Note You can also access the General properties panel for a mesh access point from a Cisco Prime Infrastructure map page. To display the panel, click the arrow portion of the mesh access point label. A tabbed panel appears and displays the General properties panel for the selected access point.

To add, remove, or reorder columns in the table, click the **Edit View** link. Table 35: Monitor Access Points Additional Search Results Parameters, on page 216 displays optional access point parameters available from the Edit View page.

Table 35: Monitor Access Points Additional Search Results Parameters

Column	Options
AP Type	Indicates the type of access point (unified or autonomous).
Antenna Azim. Angle	Indicates the horizontal angle of the antenna.

Column	Options
Antenna Diversity	Indicates if antenna diversity is enabled or disabled. Antenna diversity refers to the access point sampling the radio signal from two integrated antenna ports in order to choose the preferred antenna.
Antenna Elev. Angle	Indicates the elevation angle of the antenna.
Antenna Gain	Indicates the peak gain of the dBi of the antenna for directional antennas and the average gain in dBi for omnidirectional antennas connected to the wireless network adapter. The gain is in multiples of 0.5 dBm. An integer value 4 means 4 x 0.5 - 2 dBm of gain.
Antenna Mode	Indicates the antenna mode such as omni, directional, or nonapplicable.
Antenna Name	Indicates the antenna name or type.
Antenna Type	Indicates whether the antenna is internal or external.
Audit Status	Indicates one of the following audit statuses: • Mismatch—Config differences were found between Cisco Prime Infrastructure and controller during the last audit. • Identical—No config differences were found during the last audit. • Not Available—Audit status is unavailable.
Bridge Group Name	Indicates the name of the bridge group used to group the access points, if applicable.
CDP Neighbors	Indicates all directly connected Cisco devices.
Channel Control	Indicates whether the channel control is automatic or custom.
Channel Number	Indicates the channel on which the Cisco radio is broadcasting.
Controller Port	Indicates the number of controller ports.
Node Hops	Indicates the number of hops between access point.

Column	Options
POE Status	Indicates the Power-over-Ethernet status of the access point. The possible values are as follows: • Low—The access point draws low power from the Ethernet. • Lower than 15.4 volts—The access point draws lower than ?15.4 V from the Ethernet. • Lower than 16.8 volts—The access point draws lower than ?16.8 V from the Ethernet. • Normal—The power is high enough for the operation of the access point. • Not Applicable—The power source is not from the Ethernet.
Primary Controller	Indicates the name of the primary controller for this access point.
Radio MAC	Indicates the radio's MAC address.
Reg. Domain Supported	Indicates whether or not the regulatory domain is supported.
Serial Number	Indicates the access point's serial number.
Slot	Indicates the slot number.
Tx Power Control	Indicates whether the transmission power control is automatic or custom.
Tx Power Level	Indicates the transmission power level.
Up Time	Indicates how long the access point has been up in days, hours, minutes, and seconds.
WLAN Override Names	Indicates the WLAN override profile names.
WLAN Override	Indicates whether WLAN Override is enabled or disabled. Each access point is limited to 16 WLAN profiles. Each access point broadcasts all WLAN profiles unless the WLAN override feature is enabled. The WLAN override feature allows you to disable any of the 16 WLAN profiles per access point.

Viewing Mesh Statistics for a Mesh Access Point

Mesh Statistics are reported when a child mesh access point authenticates or associates with a parent mesh access point.

Security entries are removed and no longer displayed when the child mesh access point disassociates from the controller.

The following mesh security statistics are displayed for mesh access points:

- Bridging
- Queue
- Security

To view the mesh statistics for a specific mesh access point, follow these steps:

Step 1 Choose **Monitor > Access Points**. A listing of access points appears.

Note You can also use the New Search button to display the access point summary. With the New Search option, you can further define the criteria of the access points that display. Search criteria include AP Name, IP address, MAC address, Controller IP or Name, Radio type, and Outdoor area.

Step 2 Click the **AP Name** link of the target mesh access point.

A tabbed panel appears and displays the General Properties page for the selected mesh access point.

Step 3 Click the **Mesh Statistics** tab. A three-tabbed Mesh Statistics panel appears.

Note The Mesh Statistics tab and its subordinate tabs (Bridging, Queue and Security) only appear for mesh access points. The Mesh Link Alarms and Mesh Link Events links are accessible from each of the three tabbed panels.

Note You can also access the Mesh Securities panel for a mesh access point from a Cisco Prime Infrastructure map. To display the panel, click the arrow portion of the mesh access point label.

Summaries of the Bridging, Queue and Security Statistics and their definitions are provided in the following tables.

Table 36: Bridging Mesh Statistics

Parameter	Description
Role	The role of the mesh access point. Options are mesh access points (MAPs) and root access points (RAPs).
Bridge Group Name (BGN)	The name of the bridge group to which the MAP or RAP is a member. Assigning membership in a BGN is recommended. If one is not assigned, a MAP is by default assigned to a default BGN.
Backhaul Interface	The radio backhaul for the mesh access point.
Routing State	The state of parent selection. Values that display are seek, scan, and maint. Maint displays when parent selection is complete.
Malformed Neighbor Packets	The number of malformed packets received from the neighbor. Examples of malformed packets include malicious floods of traffic such as malformed or short DNS packets and malformed DNS replies.

Parameter	Description
Poor Neighbor SNR	The number of times the signal-to-noise ratio falls below 12 dB on the backhaul link.
Excluded Packets	The number of packets received from excluded neighbor mesh access points.
Insufficient Memory	The number of insufficient memory conditions.
RX Neighbor Requests	The number of broadcast and unicast requests received from the neighbor mesh access points.
RX Neighbor Responses	The number of responses received from the neighbor mesh access points.
TX Neighbor Requests	The number of unicast and broadcast requests sent to the neighbor mesh access points.
TX Neighbor Responses	The number of responses sent to the neighbor mesh access points.
Parent Changes	The number of times a mesh access point (child) moves to another parent.
Neighbor Timeouts	The number of neighbor timeouts.
Node Hops	The number of hops between the MAP and the RAP. Click the value link to display a subpanel that enables you to configure details of what is reported, how often the node hop value is updated, and view a graphical representation of the report.

Table 37: Queue Mesh Statistics

Parameter	Description
Silver Queue	The average and peak number of packets waiting in the silver (best effort) queue during the defined statistics time interval. Packets dropped and queue size are also summarized.
Gold Queue	The average and peak number of packets waiting in the gold (video) queue during the defined statistics time interval. Packets dropped and queue size are also summarized.
Platinum Queue	The average and peak number of packets waiting in the platinum (voice) queue during the defined statistics time interval. Packets dropped and queue size are also summarized.

Parameter	Description
Bronze Queue	The average and peak number of packets waiting in the bronze (background) queue during the defined statistics time interval. Packets dropped and queue size are also summarized.
Management Queue	The average and peak number of packets waiting in the management queue during the defined statistics time interval. Packets dropped and queue size are also summarized.

Table 38: Security Mesh Statistics

Parameter	Description
Association Request Failures	Summarizes the total number of association request failures that occur between the selected mesh access point and its parent.
Association Request Success	Summarizes the total number of successful association requests that occur between the selected mesh access point and its parent.
Association Request Timeouts	Summarizes the total number of association request time outs that occur between the selected mesh access point and its parent.
Authentication Request Failures	Summarizes the total number of failed authentication requests that occur between the selected mesh access point and its parent.
Authentication Request Success	Summarizes the total number of successful authentication requests between the selected mesh access point and its parent mesh node.
Authentication Request Timeouts	Summarizes the total number of authentication request timeouts that occur between the selected mesh access point and its parent.
Invalid Association Request	Summarizes the total number of invalid association requests received by the parent mesh access point from the selected child mesh access point. This state might occur when the selected child is a valid neighbor but is not in a state that allows association.
Invalid Reassociation Request	Summarizes the total number of invalid reassociation requests received by the parent mesh access point from a child. This state might occur when a child is a valid neighbor but is not in a proper state for reassociation.

Parameter	Description
Invalid Reauthentication Request	Summarizes the total number of invalid reauthentication requests received by the parent mesh access point from a child. This state might occur when a child is a valid neighbor but is not in a proper state for reauthentication.
Packets Received	Summarizes the total number of packets received during security negotiations by the selected mesh access point.
Packets Transmitted	Summarizes the total number of packets transmitted during security negotiations by the selected mesh access point.
Reassociation Request Failures	Summarizes the total number of failed reassociation requests between the selected mesh access point and its parent.
Reassociation Request Success	Summarizes the total number of successful reassociation requests between the selected mesh access point and its parent.
Reassociation Request Timeouts	Summarizes the total number of reassociation request timeouts between the selected mesh access point and its parent.
Reauthentication Request Failures	Summarizes the total number of failed reauthentication requests between the selected mesh access point and its parent.
Reauthentication Request Success	Summarizes the total number of successful reauthentication requests that occurred between the selected mesh access point and its parent.
Reauthentication Request Timeouts	Summarizes the total number of reauthentication request timeouts that occurred between the selected mesh access point and its parent.
Unknown Association Requests	Summarizes the total number of unknown association requests received by the parent mesh access point from its child. The unknown association requests often occur when a child is an unknown neighbor mesh access point.
Unknown Reassociation Request	Summarizes the total number of unknown reassociation requests received by the parent mesh access point from a child. This state might occur when a child mesh access point is an unknown neighbor.
Unknown Reauthentication Request	Summarizes the total number of unknown reauthentication requests received by the parent mesh access point node from its child. This state might occur when a child mesh access point is an unknown neighbor.

Viewing the Mesh Network Hierarchy

You can view the parent-child relationship of mesh access points within a mesh network in an easily navigable display. You can also filter which mesh access points display on the Map view, by selecting only mesh access points of interest.

To view the mesh network hierarchy for a selected network, follow these steps:

Step 1 Choose **Monitor** > **Maps**.

Step 2 Select the map that you want to be displayed.

Step 3 Click the Layers arrow to expand that menu.

Step 4 Select the **AP Mesh Info** check box if it is not already checked.

Note The AP Mesh Info check box can be selected only if mesh access points are present on the map. It must be checked to view the mesh hierarchy.

Step 5 Click the AP Mesh Info arrow to display the mesh parent-child hierarchy.

Step 6 Click the plus (+) sign next to a mesh access point to display its children.

All subordinate mesh access points are displayed when a negative (-) sign displays next to the parent mesh access point entry.

Step 7 Move the cursor over the colored dot next to each mesh access point child to view details on the link between it and its parent. Table 39: Bridging Link Information, on page 223 summarizes the parameters that display.

The color of the dot also provides a quick reference point of the SNR strength.

- A green dot represents a high SNR (above 25 dB).
- An amber dot represents an acceptable SNR (20 to 25 dB).
- A red dot represents a low SNR (below 20 dB).
- A black dot indicates a root access point.

Table 39: Bridging Link Information

Parameter	Description
Information fetched on	Date and time that information was compiled.
Link SNR	Link signal-to-noise ratio (SNR).
Link Type	Hierarchical link relationship.
SNR Up	Signal-to-noise radio for the uplink (dB).
SNR Down	Signal-to-noise radio for the downlink (dB).
PER	Packet error rate for the link.
Tx Parent Packets	TX packets to a node while acting as a parent.
Rx Parent Packets	RX packets to a node while acting as a parent.

Parameter	Description
Time of Last Hello	Date and time of last hello.

Using Mesh Filters to Modify Map Display of Maps and Mesh Links

In the mesh hierarchical page, you can also define mesh filters to determine which mesh access points display on the map based on hop values as well as what labels display for mesh links.

Mesh access points are filtered by the number of hops between them and their root access point.

To use mesh filtering, follow these steps:

Step 1 To modify what label and color displays for a mesh link, do the following:

In the Mesh Parent-Child Hierarchical View, select an option from the Link Label drop-down list. Options are None, Link SNR, and Packet Error Rate.

In the Mesh Parent-Child Hierarchical View, select an option from the Link Color drop-down list to define which parameter (Link SNR or Packet Error Rate) determines the color of the mesh link on the map.

Note The color of the link provides a quick reference point of the SNR strength or Packet Error Rate.

Table 40: Definition for SNR and Packet Error Rate Link Color

Link Color	Link SNR	Packet Error Rate (PER)
Green	Represents an SNR above 25 dB (high value)	Represents a PER of one percent (1%) or lower
Amber	Represents an SNR between 20 and 25 dB (acceptable value)	Represents a PER that is less than ten percent (10%) and greater than one percent (1%)
Red	Represents an SNR below 20 dB (low value)	Represents a PER that is greater than ten percent (10%)

Note The Link label and color settings are reflected on the map immediately. You can display both SNR and PER values simultaneously.

Step 2 To modify which mesh access points display based on the number of hops between them and their parents, do the following:

In the Mesh Parent-Child Hierarchical View, click the Quick Selections drop-down list.

Select the appropriate option from the list.

Table 41: Quick Selection Options

Parameter	Description

Select only Root APs	Choose this setting if you want the map view to display root access points only.
Select up to 1st hops	Choose this setting if you want the map view to display 1st hops only.
Select up to 2nd hops	Choose this setting if you want the map view to display 2nd hops only.
Select up to 3rd hops	Choose this setting if you want the map view to display 3rd hops only.
Select up to 4th hops	Choose this setting if you want the map view to display 4th hops only.
Select All	Select this setting if you want the map view to display all access points.

Click Update Map View to refresh the screen and redisplay the map view with the selected options.

Note Map view information is retrieved from the Cisco Prime Infrastructure database and is updated every 15 minutes.

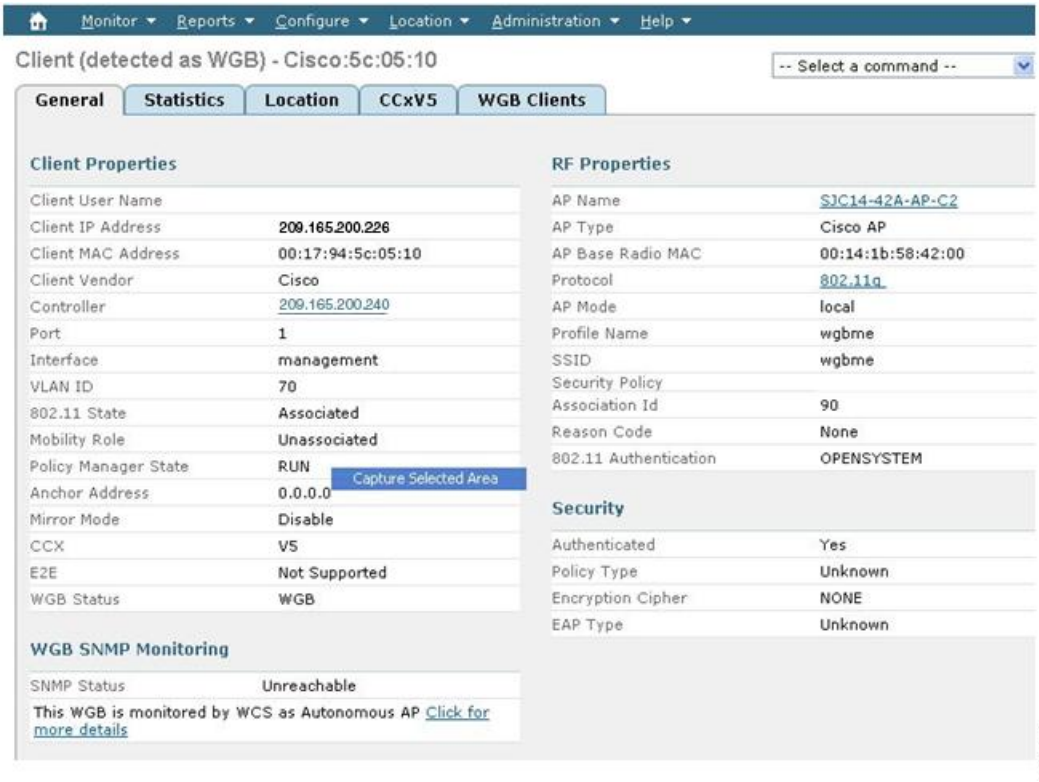
Note You can also select or deselect the check boxes of mesh access points in the mesh hierarchical view to modify which mesh access points are displayed. For a child access point to be visible, the parent access point to root access point must be selected.

Monitoring Workgroup Bridges

You can monitor workgroup bridge (WGB) clients separately.

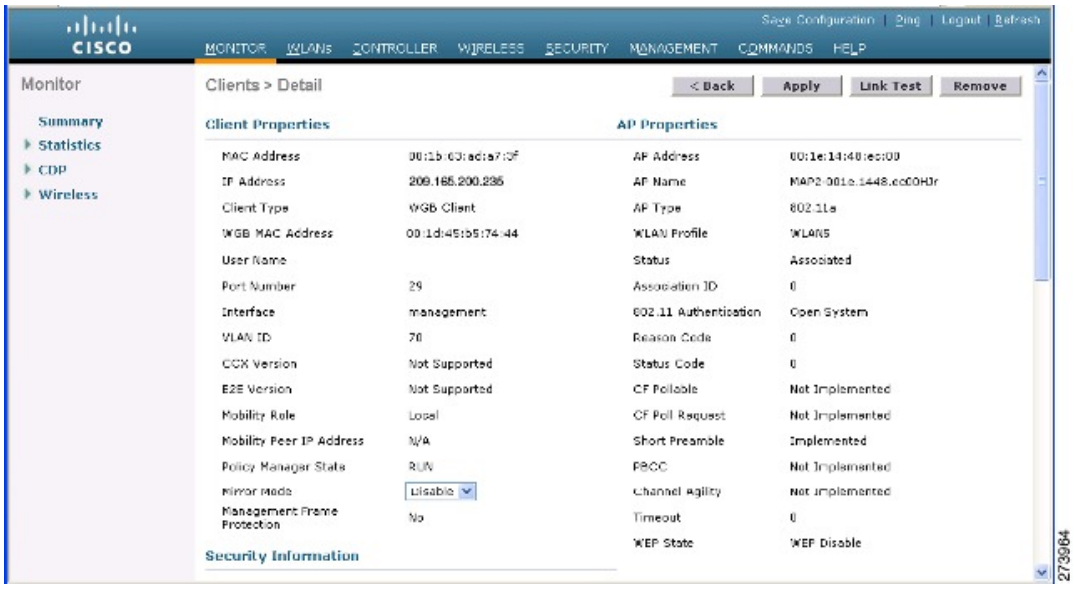
Step 1 On the Cisco Prime Infrastructure GUI, choose **Monitor > WGBs**.

Figure 80: Monitor > WGBs



Step 2 Click the WGB Clients tab to see a summary of WGB clients.

Figure 81: Monitor > WGBs > WGB Clients Panel



Multiple VLAN and QoS Support for WGB Wired Clients

A WGB is a small standalone unit that can provide a wireless infrastructure connection for Ethernet-enabled devices. Devices that do not have a wireless client adapter to connect to the wireless network can be connected to the WGB through the Ethernet port. The WGB associates with the root AP through the wireless interface, which means that wired clients get access to the wireless network.

This feature provides the segregation of traffic based on VLANs for different applications running on different devices connected to a switch behind a WGB. Traffic from WGB clients are sent in the right priority queue in the mesh backhaul based on DSCP/dot1p values.



Note You need a special autonomous image on the autonomous access points being used as a WGB for interoperability with the Unified CAPWAP infrastructure. This image will be merged with the next official autonomous release.

The WGB informs the WLC about the wired-client VLAN information in an IAPP association message. The WGB removes the 802.1Q header from the packet while sending to the WLC. The WLC sends the packet to the WGB without the 802.1Q tag and the WGB adds 802.1Q header to packets that go to the wired switch based on the destination MAC address.

The WLC treats the WGB client as a VLAN client and forwards the packet in the right VLAN interface based on the source MAC address.

You must enable the WGB unified client for multiple VLAN support on the WGB by entering the workgroup-bridge unified-VLAN-client command. This WGB unified client is disabled by default.

You have to configure subinterfaces on the WGB that corresponds to the VLANs on the switch ports to which the wired clients are connected.

Workgroup Bridge Guidelines

Follow these guidelines when configuring WGBs:

- A dynamic interface should be created in the controller for each VLAN that is configured in the WGB.
- Only one WLAN (SSID) for a wireless association of the WGB to the access point infrastructure is supported. This SSID should be configured as an infrastructure SSID and should be mapped to the native VLAN. The WGB drops everything that is not in the native VLAN in the mesh infrastructure.
- We recommend that you configure the same native VLAN in the switch that connects the WLC, WGB, and in the switch behind the WGB.

  All native VLAN clients on the WGB Ethernet side are part of the same VLAN in which the WGB is associated. The WGB is part of the VLAN to which the WLAN (in which the WGB has associated) is mapped.

  For example, if in the WGB, the 5-GHz radio (dot11radio 1) is mapped to a native VLAN 184, and the switch behind WGB has wired clients only in VLAN 185 and 186, then you may not require the native VLAN to be identical to the native VLAN on the WGB (VLAN 184).

  But, if you add one wired client in VLAN 184 and this VLAN client in the WGB belongs to a native VLAN, you must define the same native VLAN on the switch.
- Intersubnet mobility is supported with this feature for VLAN clients behind the WGB with a limitation that the dynamic interface for all VLANs of the WGB should be configured in all the controllers.

- Interoperability with a VLAN-pooling feature is not supported. When the VLAN-pooling feature is enabled, the WGB and its native VLAN clients become part of the same VLAN.
- AAA-override for WGB clients is not supported, but AAA-override for the WGB is supported.
- Only Layer 3 multicast is provided for WGB VLAN clients and there is no support for Layer 2 multicast.
- There is a 20-client limitation in WGB that includes wireless clients.
- Link testing for WGB wired clients is not supported.
- Roaming is supported for wireless and wired clients behind WGB.
- Multicast is supported for wired clients behind WGB.
- Broadcast is supported.
- Non-Cisco workgroup bridges are supported on Mesh access points.

Configuring VLAN and QoS Support (CLI)

In the following example, VLANs 184 and 185 exist on the wired switch behind WGB. WGB's native VLAN is 184. SSID is auto-wgb mapped to native VLAN 184. Radio 1 (5 GHz) radio is used to connect to the CAPWAP infrastructure using this SSID.

```
ap#config t
ap(config)#workgroup-bridge unified-VLAN-client
ap(config)#int FastEthernet0.184
ap(config-subif)#encapsulation dot1q 184 native
ap(config-subif)#bridge-group 1
ap(config-subif)#exit
ap(config)#int FastEthernet0.185
ap(config-subif)#encapsulation dot1q 185
ap(config-subif)#bridge-group 185
ap(config-subif)#exit
ap(config)#int Dot11Radio 1.185
ap(config-subif)#encapsulation dot1q 185
ap(config-subif)#bridge-group 185
ap(config-subif)#exit
ap(config)#int Dot11Radio 1.184
ap(config-subif)#encapsulation dot1q 184 native
ap(config-subif)#bridge-group 1
ap(config-subif)#exit
ap(config)#dot11 ssid auto-wgb
ap(config-ssid)#authentication open
ap(config-ssid)#infrastructure-ssid
ap(config-ssid)#VLAN 184
ap(config-ssid)#exit
ap(config)#int Dot11Radio 1
ap(config-if)#station-role workgroup-bridge
ap(config-if)#ssid auto-wgb
ap(config-if)#exit
ap(config)#bridge irb
```

```
ap(config)#hostname WGB
```

The **bridge irb** command is used to enable integrated routing and bridging, which the Auto AP code has retained from other higher end platforms.

You have to create dynamic interfaces 184 and 185 on the WLC for the above configuration to work. The WGB updates the WLC about the wired-client VLAN information in the IAPP association message. The WLC treats the WGB client as a VLAN-client and forwards the packet in the right VLAN interface based on the source MAC address. In the upstream direction, the WGB removes the 802.1Q header from the packet and sends it to the WLC. In the downstream direction, the WLC sends the packet to the WGB without the 802.1Q tag and the WGB adds the 802.1Q header based on the destination MAC address, while forwarding the packet to the switch that connects the wired client.

Workgroup Bridge Output

Enter the following command:

```
WGB#sh bridge
Total of 300 station blocks, 292 free
Codes: P - permanent, S - self

Bridge Group 1:
```

Address	Action	Interface	Age	RX count	TX count
0023.049a.0b12	forward	Fa0.184	0	2	0
0016.c75d.b48f	forward	Fa0.184	0	21	0
0021.91f8.e9ae	forward	Fa0.184	0	110	16
0017.59ff.47c2	forward	Vi0.184	0	23	22
0021.5504.07b5	forward	Fa0.184	0	18	6
0021.1c7b.38e0	forward	ViO.184	0	6	0

```
Bridge Group 185:
```

0016.c75d.b48f	forward	Fa0.185	0	10	0
001e.5831.c74a	forward	Fa0.185	0	9	0

WGB Detail on Controller

To display WGB details about the controller, enter the following command:

(Cisco Controller) > **show wgb summary**
Number of WGBs..... 2

MAC Address	IP Address	AP Name	Status	WLAN	Auth	Protocol	Clients
00:1d:70:97:bd:e8	209.165.200.225	c1240	Assoc	2	Yes	802.11a	2
00:1e:be:27:5f:e2	209.165.200.226	c1240	Assoc	2	Yes	802.11a	5

Cisco Controller) > **show client summary**
Number of Clients..... 7

MAC Address	AP Name	Status	WLAN/Guest-Lan	Auth	Protocol	Port	Wired
00:00:24:ca:a9:b4	R14	Associated	1	Yes	N/A	29	No
00:24:c4:a0:61:3a	R14	Associated	1	Yes	802.11a	29	No
00:24:c4:a0:61:f4	R14	Associated	1	Yes	802.11a	29	No
00:24:c4:a0:61:f8	R14	Associated	1	Yes	802.11a	29	No
00:24:c4:a0:62:0a	R14	Associated	1	Yes	802.11a	29	No
00:24:c4:a0:62:42	R14	Associated	1	Yes	802.11a	29	No
00:24:c4:a0:71:d2	R14	Associated	1	Yes	802.11a	29	No

(Cisco Controller) > **show wgb detail** *00:1e:be:27:5f:e2*
Number of wired client(s): 5

MAC Address	IP Address	AP Name	Mobility	WLAN	Auth
00:16:c7:5d:b4:8f	Unknown	c1240	Local	2	No
00:21:91:f8:e9:ae	209.165.200.232	c1240	Local	2	Yes
00:21:55:04:07:b5	209.165.200.234	c1240	Local	2	Yes
00:1e:58:31:c7:4a	209.165.200.236	c1240	Local	2	Yes
00:23:04:9a:0b:12	Unknown	c1240	Local	2	No

```
WGB_1#sh ip int brief
```

Interface	IP Address	OK?	Method	Status	Protocol
BVI1	209.165.200.225	YES	DHCP	up	up
Dot11Radio0	unassigned	YES	unset	admindown	down
Dot11Radio1	unassigned	YES	TFTP	up	up
Dot11Radio1.184	unassigned	YES	other	up	up
Dot11Radio1.185	unassigned	YES	unset	up	up
FastEthernet0	unassigned	YES	other	up	up
FastEthernet0.184	unassigned	YES	unset	up	up
FastEthernet0.185	unassigned	YES	unset	up	up
Virtual-Dot11Radio0	unassigned	YES	TFTP	up	up
Virtual-Dot11Radio0.184	unassigned	YES	unset	up	up
Virtual-Dot11Radio0.185	unassigned	YES	unset	up	up

Troubleshooting Tips

If a WGB client does not associate with the WGB, note these tips to troubleshoot the problem:

- The native VLAN that is configured on the WGB needs to be the same VLAN on the switch to which the WGB is connected. The switch port connected to the WGB should be Trunk.
- Verify the client configuration and ensure that the client configuration is correct.
- Check the show bridge command output in the autonomous AP and confirm that the AP is reading the client MAC address in the right interface.
- Confirm that the subinterfaces that correspond to specific VLANs and different subinterfaces are mapped to the bridge group.
- WGB reads the switch port behind as a client in its MAC address table.
- If required, clear the bridge entry using the clear bridge command (remember that this command will remove all the wired and wireless clients associated with the WGB and make them associated again).
- Ensure that the WGB has not exceeded its 20-client limitation.

Viewing AP Last Reboot Reason

Cisco Prime Infrastructure reports the reason for the most recent reboot on the general panel of the access point details page (**Monitor** > **Access Points** > *AP Name*).

Listed below is a summary of each of the possible Last Reboot Reasons that might be reported and its definition:

- none–Access point reported a reboot reason unknown to the controller
- dot11gModeChange–Change of 802.11g mode change occurred
- ipAddressSet–Set of static IP address
- ip AddressReset–Reset of static IP address
- rebootFromController–Reboot of access point initiated from the controller
- dhcpFallbackFail–Fallback to DHCP did not occur
- discoveryFail–Discovery was not sent
- noJoinResponse–Join response was not received
- denyJoin–Join attempt at the controller was denied
- noConfigResponse–Config Response was not received
- configController–Configured or primary controller found
- imageUpgrade Success–Upgrade of image successful
- imageOpcodeInvalid–Invalid image data opcode
- imageCheckSumInvalid–Invalid image md 5 checksum
- imageDataTimeout–Image data message timed-out
- configFileInvalid–Invalid config file
- imageDownloadError–Process error during the image download
- rebootFromConsole–Reboot command initiated from AP console
- rapOverAir–Root access point (RAP) is connected over the air
- brownout–Power failure caused reboot
- powerLow–Low power caused a reboot
- crash–Software failure caused crash
- powerHigh–Power spike caused reboot
- powerLoss–Power loss caused reboot
- powerCharge–Change in power source caused reboot
- componentFailure–Component failure caused reboot
- watchdog–Watch dog timer reset caused reboot



INDEX

A

Access Point Roles 2, 72, 75, 191
  Defining 75, 191
  Enhanced Feature Set Access Points 72

B

Backup Controllers 78
Base License 37
Beamwidth 9

C

CAC 135
  in mesh networks 135
CAPWAP 18
Cell Planning and Distance 47, 49
  AP1520 Series 47
  AP1550 Series 49
CleanAir 63, 65, 66
  Access Point Deployment Recommendations 65
  Advisor 66
  Licensing 66
  Modes of Operation 63
ClientLink Technology 33, 36
  Related Commands 36
configuring ClientLink (CLI) 34
Controller Planning 36

D

Dynamic Frequency Selection 8, 193

F

Frequency Bands 7
Fresnel Zone 39, 41

G

Google Earth Map 209
Google Earth Maps 210
  Viewing 210

H

Hazardous Location Certification 16

I

Indoor Mesh Access Points 4

L

LinkSNR Requirements 30, 31
Locally Significant Certificates 148
LSC-Only MAP Authentication using wild card MAC 152

M

Maximum Ratio Combining 14
  For the 1550 Series 14
mesh 178
  statistics 178
    viewing for an access point using the GUI 178
Mesh Range 27
  Configuring 27
Monitoring Mesh Health 216
Monitoring Mesh Link Statistics Using Maps 213

N

N-Connectors 11

P

Polarization 10
Pre-Survey Checklist 39
Preferred Parent 44
  Configuring 44
  Selection Criteria 44
Pseudo MAC and Merging 63

U

Universal Access 26
Upgrade Controller Software 71

W

Wireless Backhaul 25
Wireless Backhaul Data Rate 106
Wireless Bridging 26
    Point-to-Multipoint 26
Wireless Bridging *(continued)*
    Point-to-Point 26
Wireless Software Compatibility Matrix 72
Workgroup Bridges 225
    Monitoring 225
WPlus License 37